Panduan Administrasi

AWS AppFabric

AWS AppFabric: Panduan Administrasi

Table of Contents

Apa itu AWS AppFabric?

AWS AppFabric dengan cepat menghubungkan aplikasi perangkat lunak sebagai layanan (SaaS) di seluruh organisasi Anda, sehingga tim TI dan keamanan dapat dengan mudah mengelola dan mengamankan aplikasi menggunakan skema standar, dan karyawan dapat menyelesaikan tugas sehari-hari lebih cepat menggunakan AI generatif.

Topik

Produk

Jelajahi dua aspek AWS AppFabric: AppFabric untuk keamanan, dirancang untuk manajemen dan keamanan yang efisien, dan AppFabric untuk produktivitas (pratinjau), ditingkatkan dengan kemampuan AI generatif. Untuk informasi selengkapnya, lihat topik berikut.

- Apa itu AWS AppFabric untuk keamanan?
- Apa AWS AppFabric untuk produktivitas?

Manfaat

Anda dapat menggunakan AppFabric untuk melakukan hal berikut:

- Hubungkan aplikasi Anda dalam hitungan menit, dan kurangi biaya operasional.
- Tingkatkan visibilitas di seluruh data aplikasi SaaS untuk meningkatkan postur keamanan Anda.
- Secara otomatis memfasilitasi tugas di seluruh aplikasi dengan AI generatif.

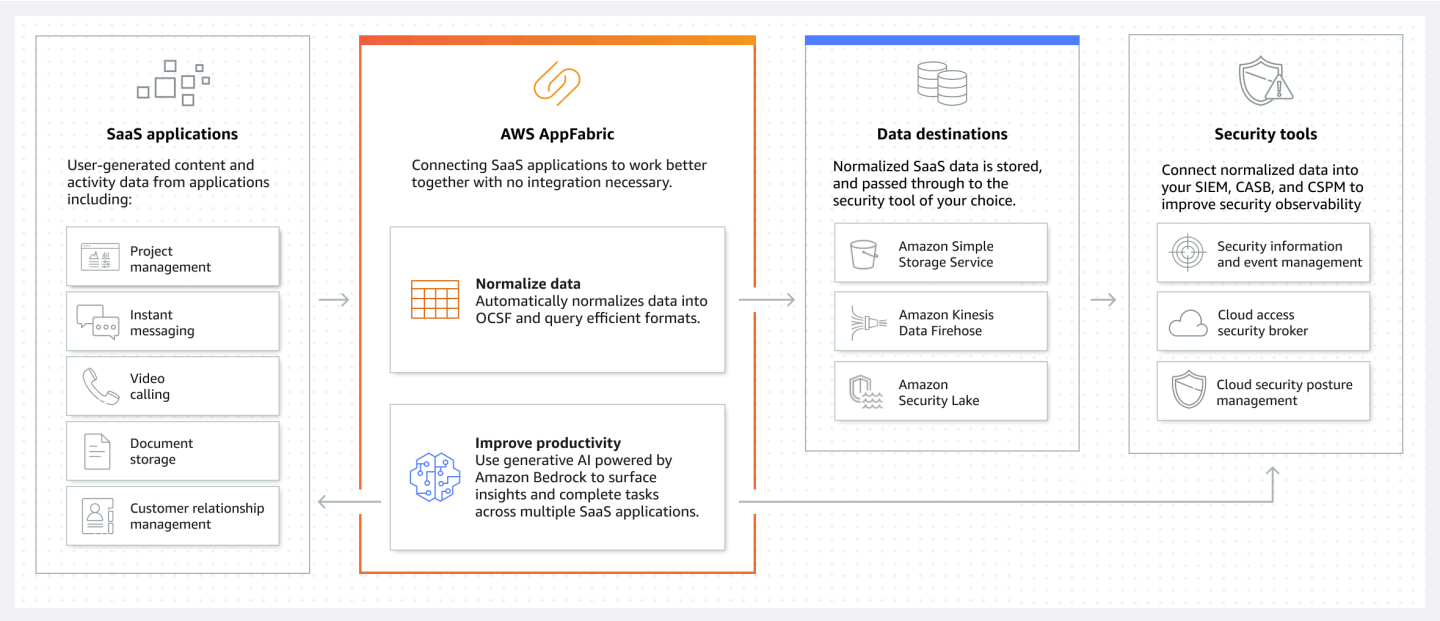
Kasus penggunaan

Anda dapat menggunakan AppFabric untuk:

- Hubungkan aplikasi SaaS Anda dengan cepat
  - AppFabric untuk keamanan secara native menghubungkan produktivitas SaaS teratas dan aplikasi keamanan satu sama lain, menyediakan solusi interoperabilitas SaaS yang dikelola sepenuhnya.
- Tingkatkan postur keamanan Anda
  - Data aplikasi dinormalisasi secara otomatis, memungkinkan administrator untuk menetapkan kebijakan umum, menstandarisasi peringatan keamanan, dan mengelola akses pengguna dengan mudah di beberapa aplikasi.
- Bayangkan kembali produktivitas
  - Dengan asisten AI generatif yang umum, AppFabric untuk produktivitas memberdayakan karyawan untuk mendapatkan jawaban dengan cepat, mengotomatiskan manajemen tugas, dan menghasilkan wawasan di seluruh aplikasi produktivitas SaaS mereka.

Bagaimana cara AppFabric kerja

AppFabric dengan cepat menghubungkan beberapa aplikasi SaaS tanpa pengkodean yang diperlukan untuk meningkatkan produktivitas dan keamanan. Diagram berikut menunjukkan manfaat dari AppFabric.



> **Note**
>
> AppFabric untuk produktivitas saat ini diluncurkan sebagai pratinjau dan tersedia di AS Timur (Virginia N.) Wilayah AWS. Untuk informasi selengkapnya Wilayah AWS, lihat AWS AppFabric titik akhir dan kuota di. Referensi Umum AWS

Harga

Untuk detail dan contoh AppFabric harga, lihat AWS AppFabric Harga.

Ketersediaan

Untuk melihat AWS Wilayah dan titik akhir yang saat ini didukung AppFabric, lihat AWS AppFabric titik akhir dan kuota di Referensi Umum.AWS

Apa itu AWS AppFabric untuk keamanan?

AWS AppFabric untuk keamanan dengan cepat menghubungkan aplikasi perangkat lunak sebagai layanan (SaaS) di seluruh organisasi Anda, sehingga tim TI dan keamanan dapat dengan mudah mengelola dan mengamankan aplikasi menggunakan skema standar.

Topik

Manfaat

Anda dapat menggunakan keamanan AppFabric untuk melakukan hal berikut:

- Hubungkan aplikasi Anda dalam hitungan menit, dan kurangi biaya operasional.
- Tingkatkan visibilitas di seluruh data aplikasi SaaS untuk meningkatkan postur keamanan Anda.

Kasus penggunaan

Anda dapat menggunakan AppFabric untuk keamanan untuk:

- Hubungkan aplikasi SaaS Anda dengan cepat
  - AppFabric untuk keamanan secara native menghubungkan produktivitas SaaS teratas dan aplikasi keamanan satu sama lain, menyediakan solusi interoperabilitas SaaS yang dikelola sepenuhnya.
- Tingkatkan postur keamanan Anda
  - Data aplikasi dinormalisasi secara otomatis, memungkinkan administrator untuk menetapkan kebijakan umum, menstandarisasi peringatan keamanan, dan mengelola akses pengguna dengan mudah di beberapa aplikasi.

Mengakses AppFabric keamanan

AppFabric untuk keamanan tersedia di AS Timur (Virginia N.), Eropa (Irlandia), dan Asia Pasifik (Tokyo) Wilayah AWS. Untuk informasi selengkapnya Wilayah AWS, lihat AWS AppFabric titik akhir dan kuota di. Referensi Umum AWS

Di setiap Wilayah, Anda dapat mengakses AppFabric keamanan dengan salah satu cara berikut:

AWS Management Console

AWS Management Console Ini adalah antarmuka berbasis browser yang dapat Anda gunakan untuk membuat dan mengelola AWS sumber daya. AppFabric Konsol menyediakan akses ke AppFabric sumber daya Anda. Anda dapat menggunakan AppFabric konsol untuk membuat dan mengelola semua AppFabric sumber daya.

AppFabric API

Untuk mengakses AppFabric secara terprogram, gunakan AppFabric API, dan terbitkan permintaan HTTPS langsung ke layanan. Untuk informasi selengkapnya, lihat Referensi AWS AppFabric API.

AWS Command Line Interface (AWS CLI)

Dengan AWS CLI, Anda dapat mengeluarkan perintah di baris perintah sistem Anda untuk berinteraksi dengan AppFabric dan lainnya AWS layanan. Jika Anda ingin membangun skrip yang melakukan tugas, alat baris perintah juga berguna. Untuk informasi tentang menginstal dan menggunakan AWS CLI, lihat Panduan AWS Command Line Interface Pengguna untuk Versi 2. Untuk informasi tentang AWS CLI perintah AppFabric, lihat AppFabric bagian AWS CLI Referensi.

Layanan terkait

Anda dapat menggunakan yang berikut ini AWS layanan AppFabric untuk keamanan:

Amazon Data Firehose

Amazon Data Firehose adalah layanan ekstrak, transformasi, dan muat (ETL) yang andal menangkap, mengubah, dan mengirimkan data streaming ke danau data, penyimpanan data, dan layanan analitik. Saat menggunakan AppFabric, Anda dapat memilih untuk menampilkan log audit normal atau mentah Open Cybersecurity Schema Framework (OCSF) dalam format JSON ke aliran Firehose sebagai tujuan Anda. Untuk informasi selengkapnya, lihat Membuat lokasi keluaran di Firehose.

Danau Keamanan Amazon

Amazon Security Lake secara otomatis memusatkan data keamanan dari AWS lingkungan, penyedia SaaS, di tempat, dan sumber cloud ke dalam data lake yang dibuat khusus yang disimpan di akun Anda. Anda dapat mengintegrasikan data log AppFabric audit dengan Security Lake dengan memilih Amazon Data Firehose sebagai tujuan dan mengonfigurasi Firehose untuk mengirimkan data dalam format dan jalur yang benar di Security Lake. Untuk informasi selengkapnya, lihat Mengumpulkan data dari sumber khusus di Panduan Pengguna Amazon Security Lake.

Layanan Penyimpanan Sederhana Amazon

Amazon Simple Storage Service (Amazon S3) adalah layanan penyimpanan objek yang menawarkan skalabilitas, ketersediaan data, keamanan, dan kinerja terdepan di industri. Saat menggunakan AppFabric, Anda dapat memilih untuk menampilkan log audit OCSF yang dinormalisasi (JSON atauApache Parquet) atau mentah (JSON) ke bucket Amazon S3 baru atau yang sudah ada sebagai tujuan Anda. Untuk informasi selengkapnya, lihat Membuat lokasi keluaran di Amazon S3.

Amazon QuickSight

Amazon QuickSight memberdayakan organisasi berbasis data dengan intelijen bisnis terpadu (BI) di hyperscale. Dengan QuickSight, semua pengguna dapat memenuhi berbagai kebutuhan analitik dari sumber kebenaran yang sama melalui dasbor interaktif modern, laporan berhalaman, analitik tertanam, dan kueri bahasa alami. Anda dapat menganalisis data log AppFabric audit QuickSight, dengan memilih bucket Amazon S3 tempat AppFabric log Anda disimpan sebagai sumber Anda. Untuk informasi selengkapnya, lihat Membuat kumpulan data menggunakan file Amazon S3 di Panduan Pengguna QuickSight Amazon. Anda juga dapat mengimpor AppFabric data di Amazon S3 ke Amazon Athena dan memilih Amazon Athena sebagai sumber data di. QuickSight Untuk informasi selengkapnya, lihat Membuat kumpulan data menggunakan data Amazon Athena di Panduan Pengguna QuickSight Amazon.

AWS Key Management Service

Dengan AWS Key Management Service (AWS KMS), Anda dapat membuat, mengelola, dan mengontrol kunci kriptografi di seluruh aplikasi Anda dan AWS layanan. Saat membuat bundel aplikasi AppFabric, Anda menyiapkan kunci enkripsi untuk melindungi data aplikasi resmi Anda dengan aman. Kunci ini mengenkripsi data Anda dalam layanan. AppFabric AppFabric dapat menggunakan kunci yang Kunci milik AWS dibuat dan dikelola oleh AppFabric atas nama Anda, atau kunci yang dikelola pelanggan yang Anda buat dan kelola AWS KMS. Untuk informasi selengkapnya, lihat Membuat AWS KMS kunci.

Buka Kerangka Skema Keamanan Siber

Open Cybersecurity Schema Framework (OCSF) adalah upaya kolaboratif dan open-source oleh AWS dan mitra terkemuka di industri keamanan siber. OCSFmenyediakan skema standar untuk peristiwa keamanan umum, mendefinisikan kriteria pembuatan versi untuk memfasilitasi evolusi skema, dan mencakup proses tata kelola sendiri untuk produsen log keamanan dan konsumen. Kode sumber publik untuk OCSF di-host di GitHub.

OCSFskema berbasis di AppFabric

Skema berbasis AWS AppFabric for security OCSF1.1 dirancang khusus untuk memenuhi kebutuhan Anda akan observabilitas yang dinormalisasi, konsisten, dan berupaya rendah dari portofolio perangkat lunak mereka sebagai layanan (SaaS). AppFabric menentukan pemetaan yang tepat untuk setiap bidang dan acara. AppFabric, bekerja sama dengan komunitas OCSF open source, memperkenalkan kategori OCSF acara baru, kelas acara, kegiatan, dan objek sehingga OCSF

berlaku untuk acara aplikasi SaaS. AppFabric secara otomatis menormalkan peristiwa audit yang diterimanya dari aplikasi SaaS dan mengirimkan data ini ke Amazon Simple Storage Service (Amazon S3) atau layanan Amazon Data Firehose di layanan Anda. Akun AWS Untuk tujuan Amazon S3, Anda dapat memilih antara dua opsi normalisasi (OCSFatau Raw) dan dua opsi format data (JSONatau). Parquet Saat mengirim ke Firehose, Anda juga dapat memilih di antara dua opsi normalisasi (OCSFatau Raw) tetapi format data terbatas. JSON

Prasyarat dan rekomendasi

Jika Anda adalah AWS pelanggan baru, selesaikan prasyarat penyiapan yang tercantum di halaman ini sebelum Anda mulai menggunakan untuk keamanan. AWS AppFabric Untuk prosedur penyiapan ini, Anda menggunakan layanan AWS Identity and Access Management (IAM). Untuk informasi selengkapnya tentang IAM, lihat Panduan Pengguna IAM.

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 online.

   Bagian dari prosedur pendaftaran melibatkan tindakan menerima panggilan telepon dan memasukkan kode verifikasi di keypad telepon.

   Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWSdibuat. Pengguna root memiliki akses ke semua AWS layanan dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan tugas yang memerlukan akses pengguna root.

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

Buat pengguna dengan akses administratif

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

Amankan Anda Pengguna root akun AWS

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

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

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

Buat pengguna dengan akses administratif

1. Aktifkan Pusat Identitas IAM.

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

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

Masuk sebagai pengguna dengan akses administratif

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

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

Tetapkan akses ke pengguna tambahan

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

   Untuk petunjuknya, lihat Membuat set izin di Panduan AWS IAM Identity Center Pengguna.
2. Tetapkan pengguna ke grup, lalu tetapkan akses masuk tunggal ke grup.

   Untuk petunjuk, lihat Menambahkan grup di Panduan AWS IAM Identity Center Pengguna.

(Wajib) Prasyarat aplikasi lengkap

Untuk menggunakan keamanan AppFabric untuk menerima informasi pengguna dan log audit dari aplikasi, banyak aplikasi mengharuskan Anda memiliki peran dan jenis rencana tertentu. Pastikan Anda telah meninjau prasyarat untuk setiap aplikasi yang ingin Anda otorisasi AppFabric untuk keamanan, dan bahwa Anda memiliki rencana dan peran yang tepat. Untuk informasi selengkapnya tentang prasyarat khusus aplikasi, lihat Aplikasi yang Didukung, atau pilih salah satu topik khusus aplikasi berikut.

- 1Password
- Asana
- Azure Monitor
- Atlassian Confluence
- Atlassian Jira suite
- Box
- Cisco Duo
- Dropbox
- Genesys Cloud
- GitHub
- Google Analytics
- Google Workspace

- HubSpot
- IBM Security® Verify
- JumpCloud
- Microsoft365
- Miro
- Okta
- OneLogin by One Identity
- PagerDuty
- Ping Identity
- Salesforce
- ServiceNow
- Singularity Cloud
- Slack
- Smartsheet
- Terraform Cloud
- Webex by Cisco
- Zendesk
- Zoom

(Opsional) Buat lokasi keluaran

AppFabric untuk keamanan mendukung Amazon Simple Storage Service (Amazon S3) dan Amazon Data Firehose sebagai tujuan menelan log audit.

Amazon S3

Anda dapat membuat bucket Amazon S3 baru menggunakan AppFabric konsol saat membuat tujuan konsumsi. Anda juga dapat membuat ember menggunakan layanan Amazon S3. Jika Anda memilih untuk membuat bucket menggunakan layanan Amazon S3, Anda harus membuat bucket sebelum membuat tujuan AppFabric konsumsi, lalu pilih bucket saat Anda membuat tujuan konsumsi. Anda dapat memilih untuk menggunakan bucket Amazon S3 yang ada di bucket Anda Akun AWS, asalkan memenuhi persyaratan berikut untuk bucket yang ada:

- AppFabric demi keamanan mengharuskan bucket Amazon S3 Anda sama dengan sumber daya Amazon Wilayah AWS S3 Anda.
- Anda dapat mengenkripsi bucket menggunakan salah satu dari berikut ini:
  - Enkripsi di sisi server dengan kunci terkelola Amazon S3 (SSE-S3)
  - Enkripsi sisi server dengan kunci AWS Key Management Service (AWS KMS) (SSE-KMS) menggunakan default (). Kunci yang dikelola AWS `aws/s3`

Amazon Data Firehose

Anda dapat memilih untuk menggunakan Amazon Data Firehose sebagai tujuan konsumsi untuk AppFabric data keamanan. Untuk menggunakan Firehose, Anda dapat membuat aliran pengiriman Firehose Akun AWS sebelum membuat konsumsi atau saat Anda membuat tujuan konsumsi. AppFabric Anda dapat membuat aliran pengiriman Firehose menggunakan AWS Management Console, AWS CLI, atau AWS API atau SDK. Untuk petunjuk konfigurasi streaming, lihat topik berikut:

- AWS Management Console instruksi — Membuat Aliran Pengiriman Firehose Data Amazon di Panduan Pengembang Firehose Data Amazon
- AWS CLI instruksi — create-delivery-streamdalam Referensi AWS CLI Perintah
- AWS Petunjuk API dan SDK — CreateDeliveryStreamdi Referensi API Amazon Data Firehose

Persyaratan saat menggunakan Amazon Data Firehose sebagai tujuan output keamanan adalah sebagai berikut: AppFabric

- Anda harus membuat aliran Wilayah AWS sama dengan sumber daya keamanan Anda AppFabric .
- Anda harus memilih Direct PUT sebagai sumbernya.
- Lampirkan kebijakan AmazonKinesisFirehoseFullAccess AWS terkelola ke pengguna Anda, atau lampirkan izin berikut ke pengguna Anda:

```
{
    "Sid": "TagFirehoseDeliveryStream",
    "Effect": "Allow",
    "Action": ["firehose:TagDeliveryStream"],
    "Condition": {
        "ForAllValues:StringEquals": {"aws:TagKeys": "AWSAppFabricManaged"}
    },
    "Resource": "arn:aws:firehose:*:*:deliverystream/*"
```

```
}
```

Firehose mendukung integrasi dengan berbagai alat keamanan pihak ketiga, seperti Splunk dan. Logz.io Untuk informasi tentang cara mengonfigurasi Amazon Kinesis dengan benar sehingga menghasilkan data ke alat ini, lihat Pengaturan Tujuan di Panduan Pengembang Amazon Data Firehose.

(Opsional) Buat AWS KMS kunci

Dalam proses membuat paket aplikasi AppFabric untuk keamanan, Anda akan memilih atau menyiapkan kunci enkripsi untuk melindungi data Anda dengan aman dari semua aplikasi resmi. Kunci ini akan digunakan untuk mengenkripsi data Anda dalam AppFabric layanan.

AppFabric untuk keamanan mengenkripsi data secara default. AppFabric for security dapat menggunakan kunci yang Kunci milik AWS dibuat dan dikelola oleh AppFabric atas nama Anda atau kunci yang dikelola pelanggan yang Anda buat dan kelola di AWS Key Management Service (AWS KMS). Kunci milik AWS adalah kumpulan AWS KMS kunci yang AWS layanan dimiliki dan dikelola untuk digunakan dalam beberapa Akun AWS. Kunci yang dikelola pelanggan adalah AWS KMS kunci Akun AWS yang Anda buat, miliki, dan kelola. Untuk informasi selengkapnya tentang Kunci milik AWS dan kunci yang dikelola pelanggan, lihat Kunci dan AWS kunci pelanggan di Panduan AWS Key Management Service Pengembang.

Jika Anda ingin menggunakan kunci yang dikelola pelanggan untuk mengenkripsi data Anda, seperti token otorisasi, di dalam AppFabric untuk keamanan, Anda dapat membuatnya dengan. AWS KMS Untuk informasi selengkapnya tentang kebijakan izin yang memberikan akses ke kunci terkelola pelanggan Anda AWS KMS, lihat bagian Kebijakan kunci dalam panduan ini.

Memulai dengan AWS AppFabric untuk keamanan

Untuk memulai AWS AppFabric untuk keamanan, Anda harus terlebih dahulu membuat bundel aplikasi dan kemudian mengotorisasi dan menghubungkan aplikasi ke bundel aplikasi Anda. Setelah otorisasi aplikasi terhubung ke aplikasi, Anda dapat menggunakannya AppFabric untuk fitur keamanan seperti konsumsi log audit dan akses pengguna.

Bagian ini menjelaskan cara mulai menggunakan AppFabric di AWS Management Console.

Topik

- Langkah 1: Buat bundel aplikasi
- Langkah 2: Otorisasi aplikasi
- Langkah 3: Siapkan konsumsi log audit
- Langkah 4: Gunakan alat akses pengguna
- Langkah 5: Connect AppFabric untuk data keamanan di alat keamanan dan tujuan lainnya

Prasyarat

Sebelum memulai, Anda harus terlebih dahulu membuat Akun AWS dan pengguna administratif. Untuk informasi selengkapnya, lihat Mendaftar untuk Akun AWS dan Buat pengguna dengan akses administratif.

Langkah 1: Buat bundel aplikasi

Bundel aplikasi menyimpan semua otorisasi dan konsumsi aplikasi keamanan Anda AppFabric . Untuk membuat bundel aplikasi, siapkan kunci enkripsi untuk melindungi data aplikasi resmi Anda dengan aman.

1. Buka AppFabric konsol di https://console.aws.amazon.com/appfabric/.
2. Dalam Select a Region selector di sudut kanan atas halaman, pilih. Wilayah AWS AppFabric hanya tersedia di Wilayah AS Timur (Virginia N.), Eropa (Irlandia), dan Asia Pasifik (Tokyo).
3. Pilih Memulai.
4. Pada halaman Memulai, untuk Langkah 1. Buat bundel aplikasi, pilih Buat bundel aplikasi.
5. Di bagian Enkripsi, siapkan kunci enkripsi untuk melindungi data Anda dengan aman dari semua aplikasi resmi. Kunci ini digunakan untuk mengenkripsi data Anda dalam layanan keamanan AppFabric for.

   AppFabric untuk keamanan mengenkripsi data secara default. AppFabric dapat menggunakan kunci yang Kunci milik AWS dibuat dan dikelola oleh AppFabric atas nama Anda atau kunci yang dikelola pelanggan yang Anda buat dan kelola di AWS Key Management Service (AWS KMS).
6. Untuk AWS KMS Kunci, pilih Use Kunci milik AWS atau Customer managed key.

   Jika Anda memilih untuk menggunakan kunci yang dikelola pelanggan, masukkan Nama Sumber Daya Amazon (ARN) atau ID kunci kunci yang ada yang ingin Anda gunakan, atau pilih Buat AWS KMS kunci.

   Pertimbangkan hal berikut ketika memilih Kunci milik AWS atau kunci yang dikelola pelanggan:

- Kunci milik AWSadalah kumpulan kunci AWS Key Management Service (AWS KMS) yang AWS layanan dimiliki dan dikelola untuk digunakan dalam beberapa Akun AWS. Meskipun tidak Kunci milik AWS ada dalam Anda Akun AWS, an AWS layanan dapat menggunakan Kunci milik AWS untuk melindungi sumber daya di akun Anda. Kunci milik AWS jangan dihitung terhadap AWS KMS kuota untuk akun Anda. Anda tidak perlu membuat atau mempertahankan kunci atau kebijakan utamanya. Rotasi Kunci milik AWS bervariasi antar layanan. Untuk informasi tentang rotasi Kunci milik AWS for AppFabric, lihat Enkripsi saat istirahat.
- Kunci yang dikelola pelanggan adalah kunci KMS Akun AWS yang Anda buat, miliki, dan kelola. Anda memiliki kendali penuh atas AWS KMS kunci-kunci ini. Anda dapat menetapkan dan memelihara kebijakan utama mereka, kebijakan AWS Identity and Access Management (IAM), dan hibah. Anda dapat mengaktifkan dan menonaktifkannya, memutar materi kriptografi mereka, menambahkan tag, membuat alias yang merujuk ke AWS KMS kunci, dan menjadwalkan AWS KMS kunci untuk dihapus. Kunci terkelola pelanggan muncul di halaman kunci terkelola Pelanggan AWS Management Console untuk AWS KMS.

  Untuk mengidentifikasi kunci yang dikelola pelanggan secara definitif, gunakan operasi. `DescribeKey` Untuk kunci yang dikelola pelanggan, nilai `KeyManager` bidang `DescribeKey` respons adalah`CUSTOMER`. Anda dapat menggunakan kunci yang dikelola pelanggan Anda dalam operasi kriptografi dan penggunaan audit di AWS CloudTrail log. Dengan banyak AWS layanan yang terintegrasi AWS KMS, Anda dapat menentukan kunci yang dikelola pelanggan untuk melindungi data yang disimpan dan dikelola untuk Anda. Kunci yang dikelola pelanggan dikenakan biaya bulanan dan biaya untuk penggunaan melebihi Tingkat AWS Gratis. Kunci yang dikelola pelanggan dihitung terhadap AWS KMS kuota untuk akun Anda.

Untuk informasi selengkapnya tentang Kunci milik AWS dan kunci yang dikelola pelanggan, lihat Kunci dan AWS kunci pelanggan di Panduan AWS Key Management Service Pengembang.

> **Note**
>
> Saat bundel aplikasi dibuat, AppFabric untuk keamanan juga akan membuat peran IAM khusus yang Akun AWS disebut peran terkait layanan (SLR) untuk Anda. AppFabric Ini memungkinkan layanan untuk mengirim metrik ke Amazon CloudWatch. Setelah Anda menambahkan tujuan log audit, SLR memungkinkan akses layanan keamanan AppFabric untuk ke sumber daya AWS Anda (bucket Amazon S3, aliran pengiriman

Amazon Data Firehose). Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan untuk AppFabric.

7. (Opsional) Untuk Tag, Anda memiliki opsi untuk menambahkan tag ke bundel aplikasi Anda. Tag adalah pasangan nilai kunci yang menetapkan metadata ke sumber daya yang Anda buat. Untuk informasi selengkapnya, lihat Menandai AWS sumber daya Anda di Panduan Pengguna Editor AWS Tag.
8. Untuk membuat app bundle, pilih Create app bundle.

Langkah 2: Otorisasi aplikasi

Setelah bundel aplikasi berhasil dibuat, kini Anda dapat mengotorisasi keamanan AppFabric untuk terhubung dan berinteraksi dengan setiap aplikasi. Aplikasi resmi dienkripsi dan disimpan dalam bundel aplikasi Anda. Untuk menyiapkan beberapa otorisasi aplikasi per bundel aplikasi, ulangi langkah otorisasi aplikasi sesuai kebutuhan untuk setiap aplikasi.

Sebelum Anda memulai langkah-langkah untuk mengotorisasi aplikasi, tinjau dan verifikasi prasyarat untuk setiap aplikasi, seperti jenis paket yang diperlukan, di. Aplikasi-aplikasi yang didukung

1. Pada halaman Memulai, untuk Langkah 2. Otorisasi aplikasi, pilih Buat otorisasi aplikasi.
2. Di bagian Otorisasi aplikasi, pilih aplikasi yang ingin Anda berikan izin untuk keamanan AppFabric untuk terhubung dari dropdown Aplikasi. Aplikasi yang ditampilkan adalah aplikasi yang saat ini didukung oleh AppFabric untuk keamanan.
3. Saat Anda memilih aplikasi, bidang informasi yang diperlukan muncul. Bidang ini mencakup ID penyewa dan nama penyewa dan mungkin juga menyertakan ID klien, rahasia klien, atau token akses pribadi. Nilai input untuk bidang ini bervariasi menurut aplikasi. Untuk petunjuk spesifik aplikasi terperinci tentang cara menemukan nilai-nilai ini, lihat. Aplikasi-aplikasi yang didukung
4. (Opsional) Untuk Tag, Anda memiliki opsi untuk menambahkan tag ke otorisasi aplikasi Anda. Tag adalah pasangan nilai kunci yang menetapkan metadata ke sumber daya yang Anda buat. Untuk informasi selengkapnya, lihat Menandai AWS sumber daya Anda di Panduan Pengguna Editor AWS Tag.
5. Pilih Buat otorisasi aplikasi.
6. Jika jendela pop-up muncul (tergantung pada aplikasi yang sedang terhubung), pilih Izinkan untuk mengotorisasi keamanan AppFabric untuk terhubung dengan aplikasi Anda.

Jika otorisasi aplikasi berhasil, Anda akan melihat pesan sukses otorisasi Aplikasi yang terhubung di halaman Memulai.

7. Anda dapat memeriksa status otorisasi aplikasi kapan saja di halaman otorisasi Aplikasi yang tercantum di panel navigasi, di bawah status untuk setiap aplikasi. Status Terhubung berarti otorisasi aplikasi Anda telah diberikan AppFabric untuk keamanan untuk terhubung ke aplikasi dan selesai.
8. Status otorisasi aplikasi yang mungkin ditampilkan dalam tabel berikut, termasuk langkah-langkah pemecahan masalah yang dapat Anda ambil untuk memperbaiki kesalahan terkait.

Nama status	Deskripsi status	Langkah pemecahan masalah
Tertunda	Status Pending berarti otorisasi aplikasi untuk aplikasi dibuat, tetapi AppFabric untuk keamanan belum terhubung ke aplikasi.	Saat Anda melihat status ini, pilih Connect dari dropdown Tindakan pada halaman otorisasi App untuk memulai koneksi. Jika kesalahan ini berlanjut, periksa apakah pemblokir pop-up browser Anda dinonaktifkan. Jika ada pesan kesalahan, seperti 400 Permintaan Buruk di jendela pop-up, periksa apakah semua informasi, seperti ID penyewa, ID klien, dan rahasia klien, dimasukkan dengan benar. Mungkin juga otorisasi aplikasi aplikasi tidak dibuat dengan benar. Untuk informasi selengkapnya, lihat Aplikasi yang didukung.
Validasi koneksi gagal	Status validasi Sambungan gagal berarti bahwa AppFabric untuk keamanan	Periksa apakah semua informasi, seperti ID penyewa, ID klien, dan

Nama status	Deskripsi status	Langkah pemecahan masalah
	tidak dapat memvalidasi koneksi otorisasi aplikasi dengan aplikasi.	rahasia klien, dimasukkan dengan benar untuk otorisasi aplikasi.
Rotasi otomatis token gagal	Status rotasi otomatis token gagal berarti token penyegaran OAuth gagal setelah otorisasi aplikasi berhasil dihubungkan.	Jika kesalahan ini berlanjut , periksa aplikasi otentikas i aplikasi. Untuk informasi selengkapnya, lihat Aplikasi yang didukung.

9. Untuk mengotorisasi aplikasi tambahan, ulangi langkah 1 hingga 8 sesuai kebutuhan.

Langkah 3: Siapkan konsumsi log audit

Setelah Anda memiliki setidaknya satu otorisasi aplikasi yang dibuat di app bundle, kini Anda dapat menyiapkan proses log audit. Penyerapan log audit menggunakan log audit dari aplikasi resmi dan menormalkannya ke dalam Open Cybersecurity Schema Framework (OCSF). Kemudian mengantarkan mereka ke satu atau lebih tujuan di dalamnya AWS. Anda juga dapat memilih untuk mengirimkan file JSON mentah ke tujuan Anda.

1. Pada halaman Memulai, untuk Langkah 3. Siapkan bagian konsumsi log audit, pilih Pengaturan cepat konsumsi.

> **Note**
>
> Untuk penyiapan yang lebih cepat, gunakan halaman penyiapan cepat Ingestions, yang hanya dapat diakses dari halaman Memulai, untuk membuat konsumsi untuk beberapa otorisasi aplikasi sekaligus, dengan tujuan konsumsi yang sama. Misalnya, bucket Amazon S3 yang sama atau aliran data Amazon Data Firehose.
> Anda juga dapat membuat konsumsi dari halaman Ingestions, yang dapat diakses dari panel navigasi. Pada halaman Ingestions, Anda dapat mengatur satu konsumsi pada satu waktu ke tujuan yang berbeda. Pada halaman Ingestions, Anda juga dapat membuat tag untuk konsumsi. Petunjuk berikut adalah untuk halaman pengaturan cepat Ingestions.

2. Untuk Pilih otorisasi aplikasi, pilih otorisasi aplikasi yang ingin Anda buat untuk konsumsi log audit. Nama penyewa yang muncul di dropdown otorisasi Aplikasi adalah nama penyewa aplikasi yang sebelumnya telah Anda buat otorisasi aplikasi untuk keamanan. AppFabric
3. Untuk tujuan Tambah, pilih tujuan untuk konsumsi log audit dari aplikasi yang Anda pilih. Opsi tujuan termasuk Amazon S3 - Bucket yang Ada, Amazon S3 - Bucket Baru, atau Amazon Data Firehose. Jika Anda memilih beberapa nama penyewa, tujuan yang Anda pilih akan diterapkan pada setiap penggunaan otorisasi aplikasi.
4. Saat Anda memilih tujuan, kolom tambahan yang diperlukan akan muncul.

   a. Jika Anda memilih Amazon S3 — Bucket baru sebagai tujuan Anda, Anda harus memasukkan nama bucket S3 yang ingin Anda buat. Untuk petunjuk selengkapnya tentang cara membuat bucket Amazon S3, lihat Membuat tujuan keluaran.

   b. Jika Anda memilih Amazon S3 — Bucket yang ada sebagai tujuan Anda, pilih nama bucket Amazon S3 yang ingin Anda gunakan.

   c. Jika Anda memilih Amazon Data Firehose sebagai tujuan, pilih nama aliran pengiriman dari daftar tarik-turun nama aliran pengiriman Firehose. Untuk petunjuk selengkapnya tentang cara membuat aliran pengiriman Amazon Data Firehose, lihat Membuat tujuan keluaran, dan perhatikan kebijakan izin yang diperlukan untuk AppFabric keamanan.
5. Untuk Skema & Format, Anda dapat memilih untuk menyimpan log audit Anda di Raw - JSON, OCSF - JSON, OCSF - untuk bucket Amazon S3, atau Raw - JSON atau OCSF-JSON Parquet untuk Firehose.

   Format data mentah menyediakan data log audit Anda yang dikonversi ke JSON dari serangkaian data. Format data OCSF menormalkan data log audit Anda ke skema Open Cybersecurity Schema Framework (OCSF) AppFabric untuk keamanan. Untuk informasi selengkapnya tentang cara AppFabric menggunakan OCSF, lihat. Buka Kerangka Skema Keamanan Siber Anda dapat memilih hanya satu skema dan format tipe data pada satu waktu untuk konsumsi. Jika Anda ingin menambahkan skema tambahan dan format tipe data, Anda dapat mengatur tujuan konsumsi tambahan dengan mengulangi proses pembuatan konsumsi.
6. (Opsional) Jika Anda ingin menambahkan tag ke konsumsi, buka halaman Tertelan dari panel navigasi. Untuk pergi ke halaman detail konsumsi, pilih nama penyewa. Untuk Tag, Anda memiliki opsi untuk menambahkan tag ke konsumsi Anda. Tag adalah pasangan nilai kunci yang menetapkan metadata ke sumber daya yang Anda buat. Untuk informasi selengkapnya, lihat Menandai AWS sumber daya Anda di Panduan Pengguna Editor AWS Tag.
7. Pilih Mengatur konsumsi.

Ketika Anda berhasil mengatur konsumsi, Anda akan melihat pesan sukses dari Ingestion dibuat di halaman Memulai.

8. Anda juga dapat memeriksa status konsumsi dan status tujuan konsumsi Anda kapan saja di halaman Konsumsi dari panel navigasi. Di halaman ini, Anda dapat melihat nama penyewa yang dibuat saat membuat otorisasi aplikasi, tujuan, dan status konsumsi Anda. Status Diaktifkan untuk konsumsi Anda berarti konsumsi Anda diaktifkan. Jika Anda memilih nama penyewa otorisasi aplikasi di halaman ini, Anda dapat melihat halaman detail untuk otorisasi aplikasi tersebut, termasuk detail dan status tujuan. Status Aktif untuk tujuan konsumsi Anda berarti bahwa tujuan diatur dengan benar dan aktif. Jika otorisasi aplikasi memiliki status Terhubung dan status tujuan konsumsi adalah Aktif, maka log audit harus diproses dan dikirimkan. Jika status otorisasi aplikasi atau status tujuan konsumsi adalah salah satu status gagal, log audit tidak akan diproses atau dikirim meskipun status konsumsi diaktifkan. Untuk memperbaiki kegagalan otorisasi aplikasi, lihat Langkah 2. Otorisasi aplikasi.
9. Status tujuan konsumsi dan konsumsi yang mungkin ditampilkan dalam tabel berikut, dengan langkah-langkah pemecahan masalah yang dapat Anda ambil untuk memperbaiki status kesalahan apa pun.

Nama negara atau status	Deskripsi	Langkah pemecahan masalah
Dinonaktifkan	Status dinonaktifkan untuk konsumsi berarti konsumsi Anda dinonaktifkan.	Anda dapat mengaktifkan konsumsi dengan memilih Aktifkan dari dropdown Tindakan pada halaman Ingestions.
Failed	Status Gagal untuk tujuan konsumsi berarti bahwa tujuan konsumsi tidak menerima log audit. Misalnya, status ini mungkin terjadi karena lokasi penyimpanan penuh.	Untuk memperbaiki masalah ini, buka konsol Amazon S3 atau Firehose.

Langkah 4: Gunakan alat akses pengguna

Menggunakan alat akses pengguna AppFabric untuk keamanan, tim keamanan dan IT Admin dapat dengan cepat melihat siapa yang memiliki akses ke aplikasi tertentu dengan menjalankan pencarian sederhana menggunakan alamat email perusahaan karyawan. Pendekatan ini dapat membantu dalam mengurangi waktu yang dihabiskan untuk tugas-tugas seperti deprovisioning pengguna yang mungkin memerlukan pemeriksaan manual atau audit akses pengguna di seluruh aplikasi SaaS. Jika pengguna ditemukan, AppFabric untuk keamanan memberikan nama pengguna dalam aplikasi dan status pengguna dalam aplikasi mereka (misalnya, Aktif) jika disediakan oleh aplikasi. AppFabric untuk pencarian keamanan semua aplikasi resmi dalam bundel aplikasi untuk mengembalikan daftar aplikasi yang dapat diakses pengguna.

1. Pada halaman Memulai, untuk Langkah 4. Gunakan alat akses pengguna, pilih Cari pengguna.
2. Di bidang Alamat email, ketik alamat email pengguna, lalu pilih Cari.
3. Di bagian Hasil pencarian, Anda melihat daftar semua aplikasi resmi yang dapat diakses pengguna. Untuk menampilkan nama pengguna dalam aplikasi dan statusnya (jika tersedia), pilih hasil pencarian.
4. Pesan Pengguna yang ditemukan di kolom hasil penelusuran berarti pengguna dapat mengakses aplikasi yang terdaftar. Tabel berikut menunjukkan kemungkinan hasil pencarian, kesalahan, dan tindakan yang dapat Anda lakukan untuk mengatasi kesalahan.

Hasil pencarian	Deskripsi
Pengguna tidak ditemukan	Tidak ada pengguna yang ditemukan dengan alamat email yang digunakan.
Token otorisasi tidak ditemukan. Connect otorisasi aplikasi untuk aplikasi.	Periksa apakah semua informasi, seperti ID penyewa, ID klien, dan rahasia klien, dimasukkan dengan benar untuk otorisasi aplikasi.
Token otorisasi dicabut. Connect otorisasi aplikasi untuk aplikasi.	Periksa apakah semua informasi, seperti ID penyewa, ID klien, dan rahasia klien, dimasukkan dengan benar untuk otorisasi aplikasi.

Hasil pencarian	Deskripsi
Kami tidak dapat memutar token otorisasi. Connect otorisasi aplikasi untuk aplikasi.	Token penyegaran OAuth gagal setelah otorisasi aplikasi berhasil dihubungkan. Jika kesalahan ini berlanjut, periksa aplikasi otentikasi aplikasi. Untuk informasi selengkap nya, lihat Aplikasi yang didukung.
Izin yang diperlukan tidak ditemukan. Connect otorisasi aplikasi untuk aplikasi.	Periksa apakah semua informasi, seperti ID penyewa, ID klien, dan rahasia klien, dimasukkan dengan benar untuk otorisasi aplikasi.
Otorisasi aplikasi tidak valid.	Periksa apakah semua informasi, seperti ID penyewa, ID klien, dan rahasia klien, dimasukkan dengan benar untuk otorisasi aplikasi.
Kami tidak dapat memanggil API aplikasi karena izin yang tidak mencukupi.	Periksa apakah semua informasi, seperti ID penyewa, ID klien, dan rahasia klien, dimasukkan dengan benar untuk otorisasi aplikasi.
Batas permintaan aplikasi terlampaui.	Ini adalah pesan kesalahan yang diterima dari aplikasi. Anda dapat mencoba mencari alamat email nanti.
Aplikasi mengalami kesalahan server internal	Ini adalah pesan kesalahan yang diterima dari aplikasi. Anda dapat mencoba mencari alamat email nanti.
Aplikasi mengalami kesalahan gateway yang buruk	Ini adalah pesan kesalahan yang diterima dari aplikasi. Anda dapat mencoba mencari alamat email nanti.
Aplikasi belum siap untuk menangani permintaan	Ini adalah pesan kesalahan yang diterima dari aplikasi. Anda dapat mencoba mencari alamat email nanti.

Hasil pencarian	Deskripsi
Aplikasi mengalami kesalahan permintaan yang buruk.	Ini adalah pesan kesalahan yang kami terima dari aplikasi. Anda dapat mencoba mencari email lagi nanti.
Aplikasi mengalami kesalahan layanan tidak tersedia.	Ini adalah pesan kesalahan yang kami terima dari aplikasi. Anda dapat mencoba mencari email lagi nanti.

Langkah 5: Connect AppFabric untuk data keamanan di alat keamanan dan tujuan lainnya

Data aplikasi yang dinormalisasi (atau mentah) dari AppFabric kompatibel dengan alat apa pun yang mendukung konsumsi data dari Amazon S3 dan integrasi dengan Firehose, termasuk alat keamanan seperti,,,,,,, dan Barracuda XDR Dynatrace Logz.io Netskope NetWitness Rapid7Splunk, atau solusi keamanan milik Anda. Untuk mendapatkan data aplikasi yang dinormalisasi (atau mentah) AppFabric, ikuti langkah sebelumnya 1 hingga 3. Untuk detail selengkapnya tentang cara menyiapkan alat dan layanan keamanan tertentu, lihat Alat dan layanan keamanan yang kompatibel.

Aplikasi-aplikasi yang didukung

AWS AppFabric untuk keamanan mendukung integrasi dengan aplikasi berikut. Pilih nama aplikasi untuk informasi lebih lanjut tentang cara mengatur keamanan AppFabric agar tersambung dengannya.

Topik

- Genesys Cloud
- GitHub
- Google Analytics
- Google Workspace
- HubSpot
- IBM Security® Verify
- JumpCloud
- Microsoft365
- Miro
- Okta
- OneLogin by One Identity
- PagerDuty
- Ping Identity
- Salesforce
- ServiceNow
- Singularity Cloud
- Slack
- Smartsheet
- Terraform Cloud
- Webex by Cisco
- Zendesk
- Zoom

1Password

1Passwordadalah pengelola kata sandi yang membantu Anda membuat, menyimpan, dan menggunakan kata sandi yang kuat untuk semua akun online Anda. Ini juga melindungi data Anda dengan enkripsi, memberi tahu Anda tentang pelanggaran, dan memungkinkan Anda berbagi kata sandi.

Anda dapat menggunakan keamanan AWS AppFabric untuk menerima log audit dan data pengguna dari1Password, menormalkan data ke dalam format Open Cybersecurity Schema Framework

(OCSF), dan mengeluarkan data ke bucket Amazon Simple Storage Service (Amazon S3) atau aliran Amazon Data Firehose.

Topik

AppFabric dukungan untuk 1Password

AppFabric mendukung penerimaan informasi pengguna dan log audit dari1Password.

Prasyarat

Untuk digunakan AppFabric untuk mentransfer log audit dari 1Password tujuan yang didukung, Anda harus memenuhi persyaratan berikut:

- Anda harus memiliki paket berlangganan 1Password Bisnis atau Perusahaan berbayar aktif. Untuk informasi lebih lanjut, lihat 1PasswordPerusahaan di 1Password situs web.
- Anda harus memiliki peran administrator atau pemilik tim di 1Password akun. Untuk informasi selengkapnya, lihat Grup di situs web 1Password dukungan.

Pertimbangan batas tarif

API 1Password AuditLog Acara membatasi permintaan hingga 600 per menit dan hingga 30.000 per jam. Melebihi batas ini mengembalikan kesalahan. Untuk informasi selengkapnya, lihat batas Nilai 1Password API di referensi API 1Password Peristiwa.

Pertimbangan keterlambatan data

Anda mungkin melihat penundaan hingga 30 menit untuk acara audit yang akan dikirim ke tujuan Anda. Hal ini disebabkan keterlambatan dalam peristiwa audit yang disediakan oleh aplikasi serta karena tindakan pencegahan yang diambil untuk mengurangi kehilangan data. Namun, ini mungkin dapat disesuaikan di tingkat akun. Untuk bantuan, hubungi AWS Support.

Menghubungkan AppFabric ke 1Password akun Anda

Setelah Anda membuat app bundle dalam AppFabric layanan, Anda harus mengotorisasi AppFabric dengan1Password. Untuk menemukan informasi yang diperlukan untuk mengotorisasi 1Password AppFabric, gunakan langkah-langkah berikut.

Buat token 1Password akses pribadi

1Passwordmendukung token akses pribadi untuk klien publik. Selesaikan langkah-langkah berikut untuk menghasilkan token akses pribadi.

1. Masuk ke 1Password akun Anda.
2. Pilih Integrasi di panel navigasi.
3. Jika ada integrasi yang ada, pilih Direktori. Jika tidak, lanjutkan ke langkah berikutnya.
4. Pilih Lainnya di bawah Integrasi Pelaporan Acara.
5. Pada halaman Tambahkan integrasi, masukkan nama sistem informasi keamanan dan manajemen acara (SIEM) Anda (mis., AppFabric Aman)
6. Pilih Tambahkan Integrasi, lalu selesaikan langkah-langkah berikut di halaman Siapkan token.
   a. Berikan nama token yang akan digunakan di lingkungan yang AppFabric aman.
   b. Kami menyarankan Anda memilih Jangan Pernah di daftar drop-down Kedaluwarsa Setelah. Jika ada nilai lain yang dipilih maka 1Password cabut token setelah waktu kedaluwarsa berlalu.
   c. Di bagian Peristiwa yang Harus Dilaporkan, pilih Upaya masuk, Peristiwa penggunaan item, dan Acara audit.
7. Pilih Token Masalah untuk membuat token.
8. Pilih Simpan 1Password dan selesaikan langkah-langkah berikut.
   a. Judul akan diisi secara otomatis berdasarkan sistem dan nama token Anda.
   b. Pilih Pribadi di bawah Pilih Vault.
   c. Pilih Simpan.

Untuk informasi selengkapnya, lihat Memulai Pelaporan 1Password Acara di 1Password situs web.

Otorisasi aplikasi

ID Penyewa

AppFabric akan meminta ID penyewa Anda. ID penyewa AppFabric akan menjadi alamat 1Password masuk Anda. Lengkapi langkah-langkah berikut untuk menemukan ID penyewa Anda.

1. Masuk ke 1Password akun Anda.

2. Pilih Pengaturan di panel navigasi.
3. 1PasswordMasuk Anda tercantum di halaman. Misalnya, example-account.1password.com.

Nama penyewa

Masukkan nama yang mengidentifikasi 1Password organisasi unik ini. AppFabric menggunakan nama penyewa untuk memberi label pada otorisasi aplikasi dan konsumsi apa pun yang dibuat dari otorisasi aplikasi.

Token akun layanan

Anda harus memiliki token akun layanan dari akun 1Password layanan untuk masuk ke otorisasi AppFabric 1Password aplikasi. Jika Anda tidak memiliki token akun layanan, gunakan petunjuk berikut:

AppFabric akan meminta token akun layanan. Token akun layanan AppFabric adalah token akses pribadi yang Anda buat. Selesaikan langkah-langkah berikut di portal 1Password untuk menemukan token akses pribadi.

1. Pilih Dasbor.
2. Pilih Orang.
3. Pilih Nama Pemilik Akun.
4. Pilih Privat.
5. Pilih Lihat Vault.
6. Pilih Nama Token.

Otorisasi Klien

Buat otorisasi aplikasi dalam AppFabric menggunakan ID penyewa, nama penyewa, dan token akun layanan. Kemudian pilih Connect untuk mengaktifkan otorisasi.

Asana

Asanaadalah platform manajemen kerja yang membantu individu, tim, dan organisasi mengatur pekerjaan, dari tugas sehari-hari hingga inisiatif strategis lintas fungsi. Ini memberikan sistem kehidupan kejelasan di mana setiap orang dapat berkomunikasi, berkolaborasi, dan

mengoordinasikan pekerjaan. DenganAsana, tim mengintegrasikan alat bisnis penting ke dalam satu tempat sehingga pekerjaan bergerak maju di mana pun itu terjadi.

Anda dapat menggunakan keamanan AWS AppFabric untuk menerima log audit dan data pengguna dariAsana, menormalkan data ke dalam format Open Cybersecurity Schema Framework (OCSF), dan mengeluarkan data ke bucket Amazon Simple Storage Service (Amazon S3) atau aliran Amazon Data Firehose.

Topik

AppFabric dukungan untuk Asana

AppFabric mendukung penerimaan informasi pengguna dan log audit dariAsana.

Prasyarat

Untuk digunakan AppFabric untuk mentransfer log audit dari Asana tujuan yang didukung, Anda harus memenuhi persyaratan berikut:

- Anda harus memiliki akun Enterprise denganAsana. Untuk informasi selengkapnya tentang membuat atau meningkatkan ke akun Asana Enterprise, lihat AsanaPerusahaan di Asana situs web.
- Anda harus memiliki pengguna dengan peran Super Admin di Asana akun Anda. Untuk informasi selengkapnya tentang peran, lihat Peran admin dan admin super Asana di Asana situs web.

Pertimbangan batas tarif

Asanamemberlakukan batas tarif pada Asana API. Untuk informasi selengkapnya tentang batas tarif Asana API, lihat Batas tarif di situs web Panduan Asana Pengembang. Jika kombinasi AppFabric dan Asana aplikasi Anda yang ada melebihi batas, log audit yang muncul AppFabric mungkin tertunda.

Pertimbangan keterlambatan data

Anda mungkin melihat penundaan hingga 30 menit untuk acara audit yang akan dikirim ke tujuan Anda. Hal ini disebabkan keterlambatan dalam peristiwa audit yang disediakan oleh aplikasi serta karena tindakan pencegahan yang diambil untuk mengurangi kehilangan data. Namun, ini mungkin dapat disesuaikan di tingkat akun. Untuk bantuan, hubungi AWS Support.

Menghubungkan AppFabric ke Asana akun Anda

Setelah Anda membuat app bundle dalam AppFabric layanan, Anda harus mengotorisasi AppFabric denganAsana. Untuk menemukan informasi yang diperlukan untuk mengotorisasi Asana AppFabric, gunakan langkah-langkah berikut.

Otorisasi aplikasi

ID Penyewa

AppFabric akan meminta ID penyewa Anda. ID penyewa di AppFabric disebut ID domain diAsana. Untuk menemukan ID domain, gunakan petunjuk berikut dari Asana layar beranda:

1. Pilih gambar profil akun Anda dan pilih Konsol Admin.
2. Kemudian pilih Pengaturan.
3. Gulir ke Pengaturan Domain.
4. Masukkan ID domain dari bagian ini ke dalam konfigurasi ID AppFabric Penyewa.

Nama penyewa

Masukkan nama yang mengidentifikasi Asana organisasi unik ini. AppFabric menggunakan nama penyewa untuk memberi label pada otorisasi aplikasi dan konsumsi apa pun yang dibuat dari otorisasi aplikasi.

Token akun layanan

Anda harus memiliki token akun layanan dari akun Asana layanan untuk masuk ke otorisasi AppFabric Asana aplikasi. Jika Anda tidak memiliki token akun layanan, gunakan petunjuk berikut:

1. Untuk membuat akun layanan, ikuti petunjuk di Akun Layanan di situs web AsanaPanduan.
2. Salin dan simpan token dari bagian bawah halaman Tambah akun layanan saat pertama kali Anda melihat halaman Tambah akun layanan.
3. Jika Anda menutup halaman Tambah akun layanan sebelum menyimpan token, Anda harus mengedit akun layanan Anda, membuat token baru, dan menyimpannya.

Azure Monitor

Azure Monitoradalah solusi pemantauan komprehensif untuk mengumpulkan, menganalisis, dan menanggapi data pemantauan dari cloud dan lingkungan lokal Anda. Anda dapat menggunakan

Azure Monitor untuk memaksimalkan ketersediaan dan kinerja aplikasi dan layanan Anda. Ini membantu Anda memahami kinerja aplikasi Anda dan memungkinkan Anda merespons peristiwa sistem secara manual dan terprogram.

Azure Monitormengumpulkan dan mengumpulkan data dari setiap lapisan dan komponen sistem Anda di beberapa langganan dan penyewa Azure dan non-Azure. Ini menyimpannya dalam platform data umum untuk konsumsi oleh seperangkat alat umum yang dapat mengkorelasikan, menganalisis, memvisualisasikan, dan/atau menanggapi data. Anda juga dapat mengintegrasikan alat Microsoft dan non-Microsoft lainnya. Log Azure Monitor aktivitas adalah log platform yang memberikan wawasan tentang peristiwa tingkat langganan. Log aktivitas mencakup informasi seperti saat sumber daya dimodifikasi atau mesin virtual dimulai.

Anda dapat menggunakan keamanan AWS AppFabric untuk menerima log audit dan data pengguna dariAzure Monitor, menormalkan data ke dalam format Open Cybersecurity Schema Framework (OCSF), dan mengeluarkan data ke bucket Amazon Simple Storage Service (Amazon S3) atau aliran Amazon Data Firehose.

Topik

AppFabric dukungan untuk Azure Monitor

AppFabric mampu menerima informasi pengguna dan log audit dari Azure Monitor layanan berikut:

- Azure Monitor
- API Management
- Microsoft Sentinel
- Security Center

Prasyarat

Untuk digunakan AppFabric untuk mentransfer log audit dari Azure Monitor tujuan yang didukung, Anda harus memenuhi persyaratan berikut:

- Anda harus memiliki Microsoft Azure akun dengan uji coba gratis atau pay-as-you-go berlangganan.

- Setidaknya satu langganan diperlukan untuk mengambil acara dalam langganan itu.

Pertimbangan batas tarif

Azure Monitormemberlakukan batas tarif pada prinsipal keamanan (pengguna atau aplikasi) yang membuat permintaan dan ID berlangganan atau ID penyewa. Untuk informasi selengkapnya tentang batas tarif Azure Monitor API, lihat Memahami cara Azure Resource Manager membatasi permintaan di situs web Azure Monitor Pengembang.

Pertimbangan keterlambatan data

Anda mungkin melihat penundaan hingga 30 menit untuk acara audit yang akan dikirim ke tujuan Anda. Hal ini disebabkan keterlambatan dalam peristiwa audit yang disediakan oleh aplikasi serta karena tindakan pencegahan yang diambil untuk mengurangi kehilangan data. Namun, ini mungkin dapat disesuaikan di tingkat akun. Untuk bantuan, hubungi AWS Support.

Menghubungkan AppFabric ke Azure Monitor akun Anda

Setelah Anda membuat app bundle dalam AppFabric layanan, Anda harus mengotorisasi AppFabric denganAzure Monitor. Untuk menemukan informasi yang diperlukan untuk mengotorisasi Azure Monitor AppFabric, gunakan langkah-langkah berikut.

Buat aplikasi OAuth

AppFabric terintegrasi dengan Azure Monitor menggunakan OAuth2. Selesaikan langkah-langkah berikut untuk membuat aplikasi OAuth2 di: Azure Monitor

1. Arahkan ke Microsoft AzurePortal dan masuk.
2. Arahkan ke Microsoft EntraID.
3. Pilih Pendaftaran Aplikasi.
4. Pilih Pendaftaran Baru.
5. Masukkan nama untuk klien seperti Klien Azure Monitor OAuth. Ini akan menjadi nama aplikasi terdaftar.
6. Verifikasi jenis akun yang didukung disetel ke Penyewa Tunggal.
7. Untuk URI Redirect, pilih Web sebagai platform dan tambahkan URI pengalihan. Gunakan format berikut untuk URI pengalihan:

```
https://<region>.console.aws.amazon.com/appfabric/oauth2
```

Di alamat itu, `<region>` adalah kode Wilayah AWS tempat Anda mengonfigurasi bundel AppFabric aplikasi. Misalnya, kode untuk Wilayah AS Timur (Virginia N.) adalah`us-east-1`. Untuk Wilayah itu, URL pengalihan adalah`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

Respons otentikasi akan dikirim ke URI yang disediakan setelah berhasil mengautentikasi pengguna. Menyediakan ini sekarang adalah opsional dan dapat diubah nanti, tetapi nilai diperlukan untuk sebagian besar skenario otentikasi.

8. PilihPendaftaran.
9. Di aplikasi terdaftar, pilih Sertifikat & rahasia dan kemudian Rahasia klien baru.
10. Tambahkan deskripsi untuk rahasianya.
11. Pilih durasi kedaluwarsa rahasia. Anda dapat memilih durasi prasetel apa pun dari drop-down atau mengatur durasi khusus.
12. Pilih Tambahkan. Nilai rahasia klien hanya dapat dilihat segera setelah pembuatan. Pastikan untuk menyimpan rahasia di tempat yang aman sebelum meninggalkan halaman.

Izin yang diperlukan

Anda harus menambahkan izin berikut ke aplikasi OAuth Anda. Untuk menambahkan izin, ikuti petunjuk di bagian Tambahkan izin untuk mengakses API web Anda di Panduan Microsoft EntraPengembang.

- Microsoft GraphAPI Akses Pengguna > User.Read.All (Pilih Jenis Delegasi)
- Microsoft GraphAPI Akses Pengguna> offline_access (Pilih Jenis Delegasi)
- AzureAPI Log Audit Manajemen Layanan > user_impersonation (Pilih Jenis Delegasi)

Setelah Anda menambahkan izin, untuk memberikan persetujuan admin atas izin tersebut, ikuti petunjuk di bagian tombol persetujuan Admin pada Panduan Microsoft EntraPengembang.

Otorisasi aplikasi

AppFabric mendukung penerimaan informasi pengguna dan log audit dari Azure Monitor akun Anda. Untuk menerima log audit dan data pengguna dariAzure Monitor, Anda harus membuat dua otorisasi aplikasi, satu yang dinamai Azure Monitordalam daftar drop-down otorisasi aplikasi, dan satu lagi yang diberi nama Log Azure Monitor Audit dalam daftar drop-down otorisasi aplikasi. Anda dapat

menggunakan ID penyewa, ID klien, dan rahasia klien yang sama untuk kedua otorisasi aplikasi. Untuk menerima log audit dari Azure Monitor Anda memerlukan otorisasi aplikasi Log Azure Monitor Audit Azure Monitordan Audit. Untuk menggunakan alat akses pengguna saja, hanya otorisasi Azure Monitoraplikasi yang diperlukan.

ID Penyewa

AppFabric akan meminta ID penyewa Anda. Selesaikan langkah-langkah berikut untuk menemukan ID klien Anda di Azure Monitor:

1. Arahkan ke Microsoft AzurePortal.
2. Arahkan ke Azure Active Directory.
3. Di bagian Pendaftaran Aplikasi, pilih aplikasi yang sebelumnya dibuat.
4. Di bagian Ikhtisar, salin ID penyewa dari bidang ID Direktori (penyewa).

Nama penyewa

Masukkan nama yang mengidentifikasi Azure Monitor langganan unik ini. AppFabric menggunakan nama penyewa untuk memberi label pada otorisasi aplikasi dan konsumsi apa pun yang dibuat dari otorisasi aplikasi.

> **Note**
>
> Nama penyewa harus maksimal 2.048 karakter yang terdiri dari angka, huruf kecil/huruf besar, dan karakter khusus berikut: periode (.), garis bawah (_), tanda hubung (-) dan ruang kosong.

ID Klien

AppFabric akan meminta ID klien. Selesaikan prosedur berikut untuk menemukan ID klien Anda diAzure Monitor:

1. Arahkan ke Microsoft AzurePortal.
2. Arahkan ke Azure Active Directory.
3. Di bagian Pendaftaran Aplikasi, pilih aplikasi yang sebelumnya dibuat.
4. Di bagian Ikhtisar, salin ID klien dari bidang ID Aplikasi (klien).

Rahasia klien

AppFabric akan meminta rahasia klien. Rahasia klien untuk aplikasi OAuth terdaftar adalah apa yang Anda hasilkan di Langkah 11 dari bagian pembuatan Aplikasi OAuth. Jika Anda salah menempatkan rahasia klien yang dihasilkan selama pembuatan aplikasi OAuth, ulangi langkah 8-11 di bagian pembuatan Aplikasi OAuth untuk membuat ulang yang baru.

Otorisasi aplikasi

Setelah membuat otorisasi aplikasi di AppFabric, Anda akan menerima jendela pop-up dari Microsoft Azure untuk menyetujui otorisasi. Masuk ke akun Anda dari jendela dan setujui AppFabric otorisasi dengan memilih Izinkan.

Atlassian Confluence

Buat, berkolaborasi, dan atur semua pekerjaan Anda di satu tempat. Confluenceadalah ruang kerja tim tempat pengetahuan dan kolaborasi bertemu. Halaman dinamis memberi tim Anda tempat untuk membuat, menangkap, dan berkolaborasi dalam proyek atau ide apa pun. Ruang membantu tim Anda menyusun, mengatur, dan berbagi pekerjaan, sehingga setiap anggota tim memiliki visibilitas ke dalam pengetahuan kelembagaan dan akses ke informasi yang mereka butuhkan untuk melakukan pekerjaan terbaik mereka. Anda dapat menggunakan keamanan AWS AppFabric untuk menerima log audit dan data pengguna dariConfluence, menormalkan data ke dalam format Open Cybersecurity Schema Framework (OCSF), dan mengeluarkan data ke bucket Amazon Simple Storage Service (Amazon S3) atau aliran Amazon Data Firehose.

Topik

AppFabric dukungan untuk Atlassian Confluence

AppFabric mendukung penerimaan log audit dariAtlassian Confluence.

Prasyarat

Untuk digunakan AppFabric untuk mentransfer log audit dari Atlassian Confluence tujuan yang didukung, Anda harus memenuhi persyaratan berikut:

- Untuk mengakses log Audit, Anda harus memiliki akun standar, premium, atau perusahaan. Untuk informasi selengkapnya tentang membuat atau meningkatkan ke jenis Confluence paket yang berlaku, lihat ConfluenceHarga di Atlassian situs web.
- Untuk mengakses log Audit, Anda harus memiliki izin Administrator untuk akun Anda. Untuk informasi selengkapnya tentang peran, lihat Memberikan izin admin kepada pengguna di situs web Atlassian Support.

Pertimbangan batas tarif

Confluencememberlakukan batas tarif pada Atlassian Confluence API. Jika kombinasi AppFabric dan aplikasi Atlassian Confluence API Anda yang ada melebihi Atlassian Confluence batas, log audit yang muncul AppFabric mungkin tertunda.

Pertimbangan keterlambatan data

Anda mungkin melihat penundaan hingga 30 menit untuk acara audit yang akan dikirim ke tujuan Anda. Hal ini disebabkan keterlambatan dalam peristiwa audit yang disediakan oleh aplikasi serta karena tindakan pencegahan yang diambil untuk mengurangi kehilangan data. Namun, ini mungkin dapat disesuaikan di tingkat akun. Untuk bantuan, hubungi AWS Support.

Menghubungkan AppFabric ke Atlassian Confluence akun Anda

Setelah Anda membuat app bundle dalam AppFabric layanan, Anda harus mengotorisasi AppFabric denganAtlassian Confluence. Untuk menemukan informasi yang diperlukan untuk mengotorisasi Atlassian Confluence AppFabric, gunakan langkah-langkah berikut.

Buat aplikasi OAuth

AppFabric terintegrasi dengan Atlassian Confluence menggunakan OAuth. Untuk membuat aplikasi OAuth diAtlassian Confluence, gunakan langkah-langkah berikut.

1. Arahkan ke Konsol Atlassian Pengembang.
2. Pilih ikon profil Anda di kanan atas dan pilih Konsol pengembang.
3. Di samping Aplikasi saya, pilih Buat, integrasi OAuth 2.0.
4. Pilih Izin di panel navigasi kiri dan pilih Tambah di samping API. Confluence
5. Di bawah Lingkup klasik, pilih Baca pengguna (`read:confluence-user`).
6. Di bawah Cakupan granular, pilih Lihat catatan audit ()`read:audit-log:confluence`.
7. Pilih Otorisasi di panel navigasi kiri dan pilih Tambahkan di samping OAuth 2.0 (3LO).

8. Gunakan URL pengalihan dengan format berikut di kotak teks URL Callback dan pilih Simpan perubahan.

```
https://<region>.console.aws.amazon.com/appfabric/oauth2
```

Di URL ini, <region>adalah kode untuk paket AppFabric aplikasi yang telah Anda konfigurasi. Wilayah AWS Misalnya, kode untuk Wilayah AS Timur (Virginia N.) adalah`us-east-1`. Untuk Wilayah itu, URL pengalihan adalah`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

Lingkup yang dibutuhkan

Anda harus menambahkan salah satu cakupan berikut ke aplikasi Atlassian Confluence OAuth Anda. Untuk informasi selengkapnya tentang cakupan, lihat Cakupan untuk aplikasi OAuth 2.0 (3LO) dan Forge di situs web Pengembang. Atlassian Gunakan lingkup klasik jika tersedia.

- Lingkup Klasik:
  - `read:confluence-user`
- Lingkup Granular:
  - `read:audit-log:confluence`

Otorisasi aplikasi

ID Penyewa

AppFabric akan meminta ID penyewa Anda. ID penyewa di AppFabric adalah subdomain Atlassian Confluence instance Anda. Anda dapat menemukan subdomain Atlassian Confluence instance Anda di bilah alamat browser Anda antara https://dan. atlassian.net.

Nama penyewa

Masukkan nama yang mengidentifikasi Atlassian Confluence organisasi unik ini. AppFabric menggunakan nama penyewa untuk memberi label pada otorisasi aplikasi dan konsumsi apa pun yang dibuat dari otorisasi aplikasi.

ID Klien

AppFabric akan meminta ID klien. Untuk menemukan ID klien AndaAtlassian Confluence, gunakan langkah-langkah berikut:

1. Arahkan ke Konsol Atlassian Pengembang.
2. Pilih ikon profil Anda di kanan atas dan pilih Konsol pengembang, Aplikasi Saya.
3. Pilih aplikasi OAuth yang Anda gunakan untuk terhubung. AppFabric
4. Masukkan ID klien dari halaman Pengaturan ke bidang ID klien di AppFabric.

Rahasia klien

AppFabric akan meminta rahasia klien. Untuk menemukan rahasia klien AndaAtlassian Confluence, gunakan langkah-langkah berikut:

1. Arahkan ke Konsol Atlassian Pengembang.
2. Pilih ikon profil Anda di kanan atas dan pilih Konsol pengembang, Aplikasi Saya.
3. Pilih aplikasi OAuth yang Anda gunakan untuk terhubung. AppFabric
4. Masukkan rahasia dari halaman Pengaturan ke bidang Rahasia Klien di AppFabric.

Menyetujui otorisasi

Setelah membuat otorisasi aplikasi di AppFabric, Anda akan menerima jendela pop-up dari Atlassian Confluence untuk menyetujui otorisasi. Untuk menyetujui AppFabric otorisasi, pilih izinkan.

Atlassian Jira suite

AtlassianMemberikan potensi dari setiap tim. Perangkat lunak manajemen layanan dan DevOps manajemen kerja mereka yang gesit dan IT membantu tim mengatur, mendiskusikan, dan menyelesaikan pekerjaan bersama. Mayoritas Fortune 500 dan lebih dari 240.000 perusahaan dari semua ukuran di seluruh dunia - termasuk NASA,, KivaDeutsche Bank, dan Salesforce - mengandalkan Atlassian solusi untuk membantu tim mereka bekerja sama lebih baik dan memberikan hasil yang berkualitas tepat waktu. Pelajari lebih lanjut tentang Atlassian produk, termasukJira Software,Confluence,Jira Service Management,Trello,Bitbucket, dan Jira Align di Atlassian.

Anda dapat menggunakan keamanan AWS AppFabric untuk menerima log audit dan data pengguna dari Jira suite (selainJira Align), menormalkan data ke dalam format Open Cybersecurity Schema Framework (OCSF), dan mengeluarkan data ke bucket Amazon Simple Storage Service (Amazon S3) atau aliran Amazon Data Firehose.

Topik

- AppFabric dukungan untuk Jira suite
- Menghubungkan AppFabric ke Jira akun Anda

AppFabric dukungan untuk Jira suite

AppFabric mendukung penerimaan informasi pengguna dan log audit dariJira suite, dengan pengecualianJira Align.

Prasyarat

Untuk digunakan AppFabric untuk mentransfer log audit dari tujuan yang didukung Jira suite ke tujuan yang didukung, Anda harus memenuhi persyaratan berikut:

- Anda harus memiliki Paket Jira Standar atau lebih tinggi. Untuk informasi selengkapnya tentang kemampuan Jira paket, lihat halaman harga JiraPerangkat Lunak, Manajemen Jira Layanan, Manajemen Jira Kerja, dan Penemuan Jira Produk.
- Anda harus memiliki pengguna dengan peran admin Organisasi di Jira akun Anda. Untuk informasi selengkapnya tentang peran, lihat Memberikan izin admin kepada pengguna di situs web Atlassian Support.

Pertimbangan batas tarif

JiraSuite memberlakukan batas tarif pada Jira API. Untuk informasi selengkapnya tentang batas tarif Jira suite API, lihat Pembatasan tarif di situs web Panduan Atlassian Pengembang. Jika kombinasi AppFabric dan aplikasi Jira API Anda yang ada melebihi batas, log audit yang muncul AppFabric mungkin tertunda.

Pertimbangan keterlambatan data

Anda mungkin melihat penundaan hingga 30 menit untuk acara audit yang akan dikirim ke tujuan Anda. Hal ini disebabkan keterlambatan dalam peristiwa audit yang disediakan oleh aplikasi serta karena tindakan pencegahan yang diambil untuk mengurangi kehilangan data. Namun, ini mungkin dapat disesuaikan di tingkat akun. Untuk bantuan, hubungi AWS Support.

Menghubungkan AppFabric ke Jira akun Anda

Setelah Anda membuat app bundle dalam AppFabric layanan, Anda harus mengotorisasi AppFabric denganJira. Untuk menemukan informasi yang diperlukan untuk mengotorisasi Jira AppFabric, gunakan langkah-langkah berikut.

Buat aplikasi OAuth

AppFabric terintegrasi dengan Jira suite menggunakan OAuth. Untuk membuat aplikasi OAuth diJira, gunakan langkah-langkah berikut:

1. Arahkan ke Konsol Atlassian Pengembang.
2. Di samping Aplikasi saya, pilih Buat, integrasi OAuth 2.0.
3. Beri nama aplikasi Anda dan pilih Buat.
4. Arahkan ke bagian Otorisasi dan pilih Tambahkan di sebelah OAuth 2.0.
5. Gunakan URL dengan format berikut di bidang URL Callback dan pilih Simpan perubahan.

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   Di URL ini, <region>adalah kode Wilayah AWS tempat Anda mengonfigurasi bundel AppFabric aplikasi. Misalnya, kode untuk Wilayah AS Timur (Virginia N.) adalah`us-east-1`. Untuk Wilayah itu, URL pengalihan adalah`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.
6. Arahkan ke bagian Pengaturan, salin ID klien dan rahasia klien Anda, dan simpan untuk digunakan untuk otorisasi AppFabric aplikasi.

Lingkup yang dibutuhkan

Anda harus menambahkan cakupan berikut ke halaman Izin aplikasi Jira OAuth Anda:

- Di bawah Lingkup Klasik:
  - JiraAPI > `read:jira-user`
- Di bawah Lingkup Granular:
  - JiraAPI > `read:audit-log:jira`
  - JiraAPI > `read:user:jira`

Otorisasi aplikasi

ID Penyewa

AppFabric akan meminta ID penyewa Anda. ID penyewa di AppFabric adalah subdomain Jira instance Anda. Anda dapat menemukan subdomain Jira instance Anda di bilah alamat browser Anda antara https://dan. atlassian.net.

Nama penyewa

Masukkan nama yang mengidentifikasi Jira server unik ini. AppFabricmenggunakan nama penyewa untuk memberi label pada otorisasi aplikasi dan konsumsi apa pun yang dibuat dari otorisasi aplikasi.

ID Klien

AppFabric akan meminta ID klien Anda. Untuk menemukan ID klien Anda di Jira, gunakan langkah-langkah berikut:

1. Arahkan ke Konsol Atlassian Pengembang.
2. Pilih aplikasi OAuth yang Anda gunakan untuk terhubung. AppFabric
3. Masukkan ID klien dari halaman Pengaturan ke bidang ID klien di AppFabric.

Rahasia klien

AppFabric akan meminta rahasia klien Anda. Rahasia Klien AppFabric adalah Rahasia diJira. Untuk menemukan Rahasia AndaJira, gunakan langkah-langkah berikut:

1. Arahkan ke Konsol Atlassian Pengembang.
2. Pilih aplikasi OAuth yang Anda gunakan untuk terhubung. AppFabric
3. Masukkan rahasia dari halaman Pengaturan ke bidang Rahasia Klien di AppFabric.

Menyetujui otorisasi

Setelah membuat otorisasi aplikasi di AppFabric Anda akan menerima jendela pop-up dari Jira untuk menyetujui otorisasi. Untuk menyetujui AppFabric otorisasi, pilih Izinkan.

Box

Boxadalah Content Cloud terkemuka, platform tunggal yang memberdayakan organisasi untuk mengelola seluruh siklus hidup konten, bekerja dengan aman dari mana saja, dan berintegrasi di seluruh aplikasi. best-of-breed

Anda dapat menggunakannya AWS AppFabric untuk menerima log audit dan data pengguna dariBox, menormalkan data ke dalam format Open Cybersecurity Schema Framework (OCSF), dan menampilkan data ke bucket Amazon Simple Storage Service (Amazon S3) atau aliran Amazon Data Firehose.

Topik

- AppFabric dukungan untuk Box
- Menghubungkan AppFabric ke Box akun Anda

AppFabric dukungan untuk Box

AppFabric mendukung penerimaan informasi pengguna dan log audit dariBox.

Prasyarat

Untuk digunakan AppFabric untuk mentransfer log audit dari Box tujuan yang didukung, Anda harus memenuhi persyaratan berikut:

- Untuk mengakses log audit, Anda harus memiliki langganan berbayar aktif untuk paket Business, Business Plus, Enterprise, atau Enterprise Plus.
- Anda harus memiliki pengguna dengan Hak Istimewa Admin.
- Anda harus mengaktifkan otentikasi 2 faktor di Box akun Anda untuk melihat dan menyalin rahasia klien aplikasi dari tab konfigurasi.

Pertimbangan batas tarif

Boxmemberlakukan batas tarif pada Box API. Untuk informasi selengkapnya tentang batas tarif Box API, lihat Batas tarif di situs web Panduan Box Pengembang. Jika kombinasi AppFabric dan Box aplikasi Anda yang ada melebihi batas, log audit yang muncul AppFabric mungkin tertunda.

Pertimbangan keterlambatan data

Anda mungkin melihat penundaan hingga 30 menit dalam acara audit untuk dikirim ke tujuan Anda. Hal ini disebabkan keterlambatan dalam peristiwa audit yang disediakan oleh aplikasi serta karena tindakan pencegahan yang diambil untuk mengurangi kehilangan data. Namun, ini mungkin dapat disesuaikan pada tingkat akun. Untuk bantuan, hubungi AWS Support.

Menghubungkan AppFabric ke Box akun Anda

Setelah membuat bundel aplikasi dalam AppFabric layanan, Anda harus mengotorisasi AppFabric. Box Untuk menemukan informasi yang diperlukan untuk mengotorisasi Box AppFabric, gunakan langkah-langkah berikut.

Buat aplikasi OAuth

AppFabric terintegrasi dengan Box menggunakan OAuth. Gunakan langkah-langkah berikut untuk membuat aplikasi OAuth diBox, Untuk informasi selengkapnya, lihat Membuat Aplikasi OAuth di situs web. Box

1. Masuk ke Box dan pergi ke Konsol Pengembang.
2. Pilih Buat Aplikasi Baru.
3. Pilih Aplikasi Kustom dari daftar jenis aplikasi. Modal akan muncul untuk meminta seleksi untuk langkah berikutnya.
4. Masukkan nama dan deskripsi aplikasi.
5. Pilih Integrasi dari daftar dropdown Tujuan.
   a. Pilih Keamanan & Kepatuhan dari daftar dropdown Kategori.
   b. AWS AppFabric SecureMasukkan sistem eksternal mana yang Anda integrasikan? kotak teks.
6. Pilih Server Authentication (Client Credentials Grant) jika Anda ingin memverifikasi identitas aplikasi dengan ID klien dan rahasia klien.
7. Pilih Buat Aplikasi.
8. Pilih tab Konfigurasi.
9. Di bagian App Access Level pada halaman, pilih App + Enterprise Access.
10. Di bagian Lingkup Aplikasi pada halaman, Pilih Mengelola pengguna dan Mengelola properti perusahaan.
11. Pilih Simpan Perubahan.

    BoxAdmin perlu mengotorisasi aplikasi dalam Konsol Box Admin sebelum aplikasi dapat digunakan. Selesaikan langkah-langkah berikut untuk meminta otorisasi.

    a. Pilih tab Otorisasi untuk aplikasi Anda dalam Konsol Pengembang.
    b. Pilih Tinjau dan Kirim untuk mengirim email ke Admin Box perusahaan Anda untuk persetujuan. Untuk informasi selengkapnya, lihat Otorisasi dalam Boxpanduan.

    > **Note**
    >
    > Anda harus mengirimkan kembali aplikasi Anda jika ada perubahan yang dilakukan setelah pengiriman.

Cakupan yang dibutuhkan

Cakupan aplikasi berikut diperlukan. Untuk informasi selengkapnya tentang cakupan, lihat Cakupan di situs web dokumentasi Kotak.

- Mengelola properti perusahaan (`manage_enterprise_properties`)
- Kelola pengguna (`manage_managed_users`)

Otorisasi aplikasi

ID Penyewa

AppFabric akan meminta ID penyewa. ID penyewa di AppFabric adalah ID Box Perusahaan. ID Box Perusahaan dapat ditemukan di konsol admin di bawah Akun & Penagihan > Informasi Akun > ID Perusahaan. Untuk informasi selengkapnya, lihat ID Perusahaan di situs web dokumentasi Kotak.

Nama penyewa

Masukkan nama yang mengidentifikasi Box organisasi unik ini. AppFabric menggunakan nama penyewa untuk memberi label pada otorisasi aplikasi dan konsumsi apa pun yang dibuat dari otorisasi aplikasi.

ID klien dan rahasia klien

1. Masuk ke Box dan pergi ke Konsol Pengembang.
2. Pilih Aplikasi Saya di menu navigasi.
3. Pilih aplikasi OAuth yang Anda gunakan untuk terhubung. AppFabric
4. Pilih tab Konfigurasi.
5. Gulir ke bagian Oauth 2.0 Credentials pada halaman.
6. Masukkan ID klien dari OAuth Client Id Anda ke dalam kolom Client ID di. AppFabric
7. Pilih Ambil Rahasia Klien.
8. Masukkan rahasia klien dari Rahasia Klien OAuth Anda ke dalam bidang Rahasia Klien di. AppFabric

Cisco Duo

Cisco Duomelindungi terhadap pelanggaran dengan rangkaian manajemen akses terkemuka yang menyediakan pertahanan berlapis-lapis yang kuat dan kemampuan inovatif yang memungkinkan

pengguna yang sah masuk dan menjauhkan aktor jahat. Untuk setiap organisasi yang khawatir akan dilanggar dan membutuhkan solusi cepat, Cisco Duo dengan cepat memungkinkan keamanan yang kuat sekaligus meningkatkan produktivitas pengguna. Anda dapat menggunakan keamanan AWS AppFabric untuk menerima log audit dan data pengguna dariCisco Duo, menormalkan data ke dalam format Open Cybersecurity Schema Framework (OCSF), dan mengeluarkan data ke bucket Amazon Simple Storage Service (Amazon S3) atau aliran Amazon Data Firehose.

Topik

AppFabric dukungan untuk Cisco Duo

AppFabric mendukung penerimaan informasi pengguna dan log audit dariCisco Duo.

Prasyarat

Untuk digunakan AppFabric untuk mentransfer log audit dari Cisco Duo tujuan yang didukung, Anda harus memenuhi persyaratan berikut:

- Untuk mengakses log audit, Anda harus memiliki langganan aktif ke edisi Duo Essentials, Duo Advantage, atau Duo Premier. Atau, pelanggan baru dengan uji coba Advantage atau Premier juga dapat mengakses. Untuk informasi lebih lanjut tentang Cisco Duo edisi, lihat Edisi & Harga.
- Anda harus menjadi Administrator dengan peran Pemilik untuk membuat atau memodifikasi Admin API.
- Anda perlu menambahkan izin “Grant read log resource” untuk mengakses log audit di API admin.

Pertimbangan batas tarif

Cisco Duomemberlakukan batas tarif pada Cisco Duo API. Untuk informasi selengkapnya tentang batas tarif Cisco Duo API, lihat batas tarif di bawah Log Otentikasi. Jika kombinasi AppFabric dan aplikasi Cisco Duo API Anda yang ada melebihi Cisco Duo batas, log audit yang muncul AppFabric mungkin tertunda. Hubungi Cisco Duo jika Anda membutuhkan kenaikan batas tarif.

Pertimbangan keterlambatan data

Anda mungkin melihat penundaan hingga 30 menit untuk acara audit yang akan dikirim ke tujuan Anda. Hal ini disebabkan keterlambatan dalam peristiwa audit yang disediakan oleh aplikasi serta

karena tindakan pencegahan yang diambil untuk mengurangi kehilangan data. Namun, ini mungkin dapat disesuaikan di tingkat akun. Untuk bantuan, hubungi AWS Support.

Connect AppFabric ke Cisco Duo akun Anda

Setelah Anda membuat app bundle dalam AppFabric layanan, Anda harus mengotorisasi AppFabric denganCisco Duo. Untuk menemukan informasi yang diperlukan untuk mengotorisasi Cisco Duo AppFabric, gunakan langkah-langkah berikut.

Buat aplikasi Cisco Duo Admin API

AppFabric terintegrasi dengan Cisco Duo menggunakan token layanan API. Untuk membuat aplikasiCisco Duo, gunakan langkah-langkah berikut.

- Untuk membuat aplikasi Cisco Duo Admin API, ikuti petunjuk di Langkah pertama di Cisco DuoAdmin API.

Izin yang diperlukan

Anda harus menambahkan cakupan berikut ke Cisco Duo aplikasi Anda:

- Hibah log baca
- Hibah sumber daya baca

Otorisasi aplikasi

ID Penyewa

AppFabric akan meminta ID penyewa. Anda dapat menemukan ID penyewa di nama Cisco Duo host. Untuk menemukan nama host diCisco Duo, ikuti langkah-langkah ini.

1. Arahkan ke halaman Login Cisco Duo Admin dan masuk.
2. Arahkan ke Aplikasi dan kemudian pilih Protect an Application.
3. Temukan entri untuk Admin API di daftar aplikasi, lalu pilih Lindungi ke kanan untuk mengonfigurasi aplikasi Anda dan mendapatkan nama host API Anda.
4. Nama host API diformat sebagai`api-`*`<tenant-id>`*`.duosecurity.com`, di mana *`<tenant-id>`* adalah ID Penyewa.

Nama penyewa

Masukkan nama yang mengidentifikasi Cisco Duo organisasi unik ini. AppFabric menggunakan nama penyewa untuk memberi label pada otorisasi aplikasi dan konsumsi apa pun yang dibuat dari otorisasi aplikasi.

Token layanan

AppFabric akan meminta token layanan. Token layanan adalah kunci integrasi dan kunci rahasia yang dipisahkan titik dua dengan format berikut.

```
integrationkey:secretkey
```

Untuk menemukan kunci integrasi dan kunci rahasia AndaCisco Duo, gunakan langkah-langkah berikut.

1. Arahkan ke halaman Login Cisco Duo Admin dan masuk.
2. Arahkan ke Aplikasi dan kemudian pilih Protect an Application.
3. Klik Protect an Application dan temukan entri untuk Admin API dalam daftar aplikasi. Klik Lindungi di ujung kanan untuk mengkonfigurasi aplikasi. Gulir ke bawah ke bagian cakupan dan tambahkan **`Grant read log`** dan**`Grant read resource`**.

Dropbox

Dropboxmembantu organisasi Anda menyelesaikan pekerjaan yang lebih baik lebih cepat dengan menyatukan orang-orang Anda - tidak peduli apa yang mereka kerjakan, di mana mereka bekerja, atau jenis alat apa yang mereka gunakan. Ini memungkinkan pengguna untuk mempercepat inovasi dan efisiensi dengan menyediakan cara yang sederhana dan aman untuk berbagi konten. Dropboxadalah salah satu tempat untuk menjaga kehidupan tetap teratur dan membuat pekerjaan tetap bergerak. Dengan lebih dari 700 juta pengguna terdaftar di 180 negara, Dropbox sedang dalam misi untuk merancang cara kerja yang lebih tercerahkan.

Anda dapat menggunakan keamanan AWS AppFabric untuk menerima log audit dan data pengguna dariDropbox, menormalkan data ke dalam format Open Cybersecurity Schema Framework (OCSF), dan mengeluarkan data ke bucket Amazon Simple Storage Service (Amazon S3) atau aliran Amazon Data Firehose.

Topik

- AppFabric dukungan untuk Dropbox

- Menghubungkan AppFabric ke Dropbox akun Anda

AppFabric dukungan untuk Dropbox

AppFabric mendukung penerimaan informasi pengguna dan log audit dariDropbox.

Prasyarat

Untuk digunakan AppFabric untuk mentransfer log audit dari Dropbox tujuan yang didukung, Anda harus memenuhi persyaratan berikut:

- Anda harus memiliki akun Dropbox Bisnis. Untuk informasi selengkapnya tentang membuat atau meningkatkan ke akun Dropbox Bisnis, lihat DropboxBisnis di Dropbox situs web.
- Anda harus memiliki pengguna dengan peran Admin Tim di Dropbox akun Anda. Untuk informasi selengkapnya tentang peran, lihat Cara mengubah hak admin untuk Dropbox tim Anda di situs web Pusat Dropbox Bantuan.

Pertimbangan batas tarif

Dropboxmemberlakukan batas tarif pada Dropbox API. Untuk informasi selengkapnya tentang batas tarif Dropbox API, lihat Batas tarif di situs web Panduan Dropbox Kinerja. Jika kombinasi AppFabric dan aplikasi Dropbox API Anda yang ada melebihi batas, log audit yang muncul AppFabric mungkin tertunda.

Pertimbangan keterlambatan data

Anda mungkin melihat penundaan hingga 30 menit untuk acara audit yang akan dikirim ke tujuan Anda. Hal ini disebabkan keterlambatan dalam peristiwa audit yang disediakan oleh aplikasi serta karena tindakan pencegahan yang diambil untuk mengurangi kehilangan data. Namun, ini mungkin dapat disesuaikan di tingkat akun. Untuk bantuan, hubungi AWS Support.

Menghubungkan AppFabric ke Dropbox akun Anda

Setelah Anda membuat app bundle dalam AppFabric layanan, Anda harus mengotorisasi AppFabric denganDropbox. Untuk menemukan informasi yang diperlukan untuk mengotorisasi Dropbox AppFabric, gunakan langkah-langkah berikut.

Buat aplikasi OAuth

AppFabric terintegrasi dengan Dropbox menggunakan OAuth. Untuk membuat aplikasi OAuth diDropbox, gunakan langkah-langkah berikut:

1. Pilih Buat aplikasi di Konsol Dropbox Aplikasi di https://www.dropbox.com/developers/apps.
2. Pada halaman konfigurasi aplikasi baru, pilih akses Scoped untuk API.
3. Selanjutnya, pilih Penuh Dropbox untuk jenis akses.
4. Beri nama aplikasi OAuth Anda, lalu pilih Buat aplikasi untuk menyelesaikan pengaturan aplikasi OAuth awal.
5. Pada halaman info aplikasi, tambahkan URL pengalihan dengan format berikut di bidang URI pengalihan OAuth2.

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   Di URL ini, *<region>* adalah kode Wilayah AWS tempat Anda mengonfigurasi bundel AppFabric aplikasi. Misalnya, kode untuk Wilayah AS Timur (Virginia N.) adalah`us-east-1`. Untuk Wilayah itu, URL pengalihan adalah`https://`*us-east-1*`.console.aws.amazon.com/appfabric/oauth2`.
6. Pilih Tambahkan.
7. Salin dan simpan kunci aplikasi dan rahasia aplikasi Anda untuk digunakan dalam otorisasi AppFabric aplikasi.
8. Anda dapat meninggalkan semua bidang lain di tab Pengaturan dengan nilai defaultnya.

Lingkup yang dibutuhkan

Anda harus menambahkan cakupan berikut ke Dropbox aplikasi menggunakan tab Izin di layar info aplikasi:

- `account_info.read`
- `team_data.member`
- `events.read`
- `members.read`
- `team_info.read`

Pilih Kirim setelah Anda selesai.

Otorisasi aplikasi

ID Penyewa

AppFabric akan meminta ID penyewa Anda. Masukkan nilai apa pun yang secara unik mengidentifikasi Dropbox akun Anda, seperti nama tim.

Nama penyewa

Masukkan nama yang mengidentifikasi Dropbox akun unik ini. AppFabricmenggunakan nama penyewa untuk memberi label pada otorisasi aplikasi dan konsumsi apa pun yang dibuat dari otorisasi aplikasi.

ID Klien

AppFabric akan meminta ID klien. ID klien di AppFabric adalah kunci Dropbox aplikasi Anda. Untuk menemukan kunci aplikasi Dropbox Anda, gunakan langkah-langkah berikut:

1. Arahkan ke Dropbox App Console di https://www.dropbox.com/developers/apps.
2. Temukan aplikasi yang Anda gunakan untuk terhubung AppFabric.
3. Temukan kunci aplikasi di bagian Status pada halaman info aplikasi.
4. Masukkan kunci aplikasi untuk Dropbox aplikasi Anda ke kolom Client ID di AppFabric.

Rahasia klien

AppFabric akan meminta rahasia klien. Rahasia klien AppFabric adalah rahasia Dropbox aplikasi Anda. Untuk menemukan rahasia Dropbox aplikasi Anda, gunakan langkah-langkah berikut:

1. Arahkan ke Dropbox App Console di https://www.dropbox.com/developers/apps.
2. Temukan aplikasi yang Anda gunakan untuk terhubung AppFabric.
3. Temukan rahasia aplikasi di bagian Status pada halaman info aplikasi.
4. Masukkan rahasia aplikasi untuk Dropbox aplikasi Anda ke dalam bidang Rahasia Klien di AppFabric.

Menyetujui otorisasi

Setelah membuat otorisasi aplikasi di AppFabric, Anda akan menerima jendela pop-up dari Dropbox untuk menyetujui otorisasi. Untuk menyetujui AppFabric otorisasi, pilih Izinkan.

Genesys Cloud

Genesys Cloudmenciptakan percakapan lancar di seluruh saluran digital dan suara dalam all-in-one antarmuka yang mudah. Ini memposisikan perusahaan untuk memberikan pengalaman luar biasa bagi karyawan dan pelanggan dan menuai manfaat dari penyebaran yang cepat, mengurangi kompleksitas dan administrasi yang sederhana. Anda dapat menggunakan keamanan AWS AppFabric untuk menerima log audit dan data pengguna dariGenesys Cloud, menormalkan data ke dalam format Open Cybersecurity Schema Framework (OCSF), dan mengeluarkan data ke bucket Amazon Simple Storage Service (Amazon S3) atau aliran Amazon Data Firehose.

Topik

AppFabric dukungan untuk Genesys Cloud

AppFabric mendukung penerimaan informasi pengguna dan log audit dariGenesys Cloud.

Prasyarat

Untuk digunakan AppFabric untuk mentransfer log audit dari Genesys Cloud tujuan yang didukung, Anda harus memenuhi persyaratan berikut:

- Anda harus memiliki Genesys Cloud akun.
- Anda harus memiliki pengguna dengan peran Administrator di Genesys Cloud akun Anda.

Pertimbangan batas tarif

Genesys Cloudmemberlakukan batas tarif pada Genesys Cloud API. Untuk informasi selengkapnya tentang batas tarif Genesys Cloud API, lihat Batas tarif di Genesys Cloud Developer situs web.

Pertimbangan keterlambatan data

Anda mungkin melihat penundaan hingga 30 menit untuk acara audit yang akan dikirim ke tujuan Anda. Hal ini disebabkan keterlambatan dalam peristiwa audit yang disediakan oleh aplikasi serta karena tindakan pencegahan yang diambil untuk mengurangi kehilangan data. Namun, ini mungkin dapat disesuaikan di tingkat akun. Untuk bantuan, hubungi AWS Support.

Menghubungkan AppFabric ke Genesys Cloud akun Anda

Setelah Anda membuat app bundle dalam AppFabric layanan, Anda harus mengotorisasi AppFabric denganGenesys Cloud. Untuk menemukan informasi yang diperlukan untuk mengotorisasi Genesys Cloud AppFabric, gunakan langkah-langkah berikut.

Buat aplikasi OAuth

AppFabric terintegrasi dengan Genesys Cloud menggunakan OAuth. Untuk membuat aplikasi OAuth diGenesys Cloud, gunakan langkah-langkah berikut:

1. Ikuti petunjuk di Buat Klien OAuth di situs web Pusat Genesys Cloud Sumber Daya.

   Untuk jenis Hibah, pilih Otorisasi Kode.
2. Gunakan URL pengalihan dengan format berikut sebagai URI pengalihan Resmi.

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   Di URL ini, <region>adalah kode untuk paket AppFabric aplikasi yang telah Anda konfigurasi. Wilayah AWS Misalnya, kode untuk Wilayah AS Timur (Virginia N.) adalah`us-east-1`. Untuk Wilayah itu, URL pengalihan adalah`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.
3. Pilih kotak Lingkup untuk menampilkan daftar cakupan yang tersedia untuk aplikasi Anda. Pilih ruang lingkup `audits:readonly` dan`users:readonly`. Untuk informasi tentang cakupan, lihat Lingkup OAuth di Pusat Pengembang. Genesys Cloud
4. Pilih Simpan. Genesys Cloudmembuat ID Klien dan Rahasia Klien (token).

Lingkup yang dibutuhkan

Anda harus menambahkan cakupan berikut ke aplikasi Genesys Cloud OAuth Anda:

- `audits:readonly`
- `users:readonly`

Otorisasi aplikasi

ID Penyewa

AppFabric akan meminta ID penyewa Anda. ID penyewa di AppFabric adalah nama Genesys Cloud instance Anda. Anda dapat menemukan ID penyewa Anda di bilah alamat browser Anda. Misalnya, `usw2.pure.cloud` adalah ID penyewa di URL `https://login.usw2.pure.cloud` berikut.

Nama penyewa

Masukkan nama yang mengidentifikasi Genesys Cloud organisasi unik ini. AppFabric menggunakan nama penyewa untuk memberi label pada otorisasi aplikasi dan konsumsi apa pun yang dibuat dari otorisasi aplikasi.

ID Klien

AppFabric akan meminta ID klien. Untuk menemukan ID klien AndaGenesys Cloud, gunakan langkah-langkah berikut:

1. Pilih Admin.
2. Di bawah Integrasi, pilih OAuth.
3. Pilih klien OAuth untuk mendapatkan ID Klien.

Rahasia klien

AppFabric akan meminta rahasia klien. Untuk menemukan rahasia klien AndaGenesys Cloud, gunakan langkah-langkah berikut:

1. Pilih Admin.
2. Di bawah Integrasi, pilih OAuth.
3. Pilih klien OAuth untuk mendapatkan Rahasia Klien.

GitHub

GitHubadalah platform dan layanan berbasis cloud untuk pengembangan perangkat lunak dan kontrol versi menggunakan Git, memungkinkan pengembang untuk menyimpan dan mengelola kode mereka. Ini menyediakan kontrol versi terdistribusi dari Git plus kontrol akses, pelacakan bug, permintaan fitur perangkat lunak, manajemen tugas, integrasi berkelanjutan, dan wiki untuk setiap

proyek. Anda dapat menggunakan keamanan AWS AppFabric untuk menerima log audit dan data pengguna dariGitHub, menormalkan data ke dalam format Open Cybersecurity Schema Framework (OCSF), dan mengeluarkan data ke bucket Amazon Simple Storage Service (Amazon S3) atau aliran Amazon Data Firehose.

Topik

AppFabric dukungan untuk GitHub

AppFabric mendukung penerimaan informasi pengguna dan log audit dariGitHub.

Prasyarat

Untuk digunakan AppFabric untuk mentransfer log audit dari GitHub tujuan yang didukung, Anda harus memenuhi persyaratan berikut:

- Untuk mengakses log Audit, Anda harus memiliki akun perusahaan.
- Untuk mengakses log audit Enterprise, Anda harus memiliki peran Administrator untuk akun perusahaan Anda.
- Untuk mendapatkan log audit dari organisasi, Anda harus menjadi pemilik Organisasi.

Pertimbangan batas tarif

GitHubmemberlakukan batas tarif pada GitHub API. Untuk informasi selengkapnya tentang batas tarif GitHub API, lihat Batas dan Alokasi Permintaan API di GitHubsitus web. Jika kombinasi AppFabric dan aplikasi GitHub API Anda yang ada melebihi GitHub’s batas, log audit yang muncul AppFabric mungkin tertunda.

Pertimbangan keterlambatan data

Anda mungkin melihat penundaan hingga 30 menit untuk acara audit yang akan dikirim ke tujuan Anda. Hal ini disebabkan keterlambatan dalam peristiwa audit yang disediakan oleh aplikasi serta karena tindakan pencegahan yang diambil untuk mengurangi kehilangan data. Namun, ini mungkin dapat disesuaikan di tingkat akun. Untuk bantuan, hubungi AWS Support.

Menghubungkan AppFabric ke GitHub akun Anda

Setelah Anda membuat app bundle dalam AppFabric layanan, Anda harus mengotorisasi AppFabric denganGitHub. Untuk menemukan informasi yang diperlukan untuk mengotorisasi GitHub AppFabric, gunakan langkah-langkah berikut.

Buat aplikasi OAuth

AppFabric terintegrasi dengan GitHub menggunakan OAuth. Gunakan langkah-langkah berikut untuk membuat aplikasi OAuth di. GitHub Untuk informasi selengkapnya, lihat Membuat GitHubs Aplikasi di GitHubsitus web.

1. Pilih foto profil Anda yang terletak di sudut kanan atas halaman, lalu pilih Pengaturan.
2. Pilih Pengaturan pengembang di panel navigasi kiri.
3. Pilih aplikasi OAuth di panel navigasi kiri.
4. Pilih Aplikasi OAuth Baru.

   > **Note**
   >
   > Tombol ini akan diberi label Daftarkan aplikasi baru jika Anda belum pernah membuat aplikasi OAuth sebelumnya.

5. Masukkan nama aplikasi Anda di kotak teks Nama aplikasi.
6. Masukkan URL contoh aplikasi lengkap di kotak teks URL Beranda.
7. (Opsional) Masukkan deskripsi untuk aplikasi Anda di kotak teks Deskripsi aplikasi. Pengguna akan melihat deskripsi ini.
8. Masukkan URL dengan format berikut di kotak teks URL panggilan balik Otorisasi.

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   Di URL ini, <region>adalah kode Wilayah AWS tempat Anda mengonfigurasi bundel AppFabric aplikasi. Misalnya, kode untuk Wilayah AS Timur (Virginia N.) adalah`us-east-1`. Untuk Wilayah itu, URL pengalihan adalah`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.
9. Pilih Aktifkan Alur Perangkat jika aplikasi OAuth Anda akan menggunakan alur perangkat untuk mengidentifikasi dan mengotorisasi pengguna. Untuk informasi selengkapnya tentang alur perangkat, lihat Mengotorisasi aplikasi OAuth di situs web. GitHub

10. Pilih Daftar aplikasi.

Otorisasi aplikasi

ID Penyewa

AppFabric akan meminta ID penyewa Anda. ID penyewa harus disediakan dalam salah satu format berikut:

Log audit perusahaan:

Gunakan log audit perusahaan jika Anda ingin mengetahui tindakan gabungan dari semua organisasi yang dimiliki oleh akun perusahaan Anda.

Untuk menggunakan log audit perusahaan, ID penyewa adalah ID perusahaan akun Anda. Anda dapat menemukan ID perusahaan Anda di bilah alamat browser Anda. Misalnya, *`exampleenterprise`* adalah ID perusahaan di URL berikut`https://github.com/settings/enterprises/`*`examplenterprise`*.

Saat Anda menentukan ID penyewa untuk log audit perusahaan, Anda harus mengawalinya dengan. `enterprise:` Oleh karena itu, tentukan contoh sebelumnya sebagai`enterprise:examplenterprise`.

Log audit organisasi:

Gunakan log audit organisasi sebagai admin organisasi jika Anda ingin mengetahui tindakan yang dilakukan oleh anggota organisasi Anda. Ini mencakup rincian seperti siapa yang melakukan tindakan, apa tindakan itu, dan kapan itu dilakukan.

Untuk menggunakan log audit organisasi, ID penyewa adalah ID organisasi Anda. Anda dapat menemukan ID organisasi Anda di bilah alamat browser Anda. Misalnya, *`exampleorganization`* adalah ID organisasi di URL berikut`https://github.com/settings/organizations/`*`exampleorganization`*.

Saat Anda menentukan ID penyewa untuk log audit organisasi, Anda harus mengawalinya dengan. `organization:` Oleh karena itu, tentukan contoh sebelumnya sebagai`organization:exampleorganization`.

Nama penyewa

Masukkan nama yang mengidentifikasi GitHub perusahaan atau organisasi unik ini. AppFabric menggunakan nama penyewa untuk memberi label pada otorisasi aplikasi dan konsumsi apa pun yang dibuat dari otorisasi aplikasi.

ID Klien

AppFabric akan meminta ID klien. Gunakan langkah-langkah berikut untuk menemukan ID klien Anda diGitHub,

1. Pilih foto profil Anda yang terletak di sudut kanan atas halaman, lalu pilih Pengaturan.
2. Pilih Pengaturan pengembang di panel navigasi kiri.
3. Pilih aplikasi OAuth di panel navigasi kiri.
4. Pilih aplikasi OAuth tertentu, lalu cari nilai Client ID.

Rahasia klien

AppFabric akan meminta rahasia klien. Gunakan langkah-langkah berikut untuk menemukan rahasia klien AndaGitHub.

1. Pilih foto profil Anda yang terletak di sudut kanan atas halaman, lalu pilih Pengaturan.
2. Pilih Pengaturan pengembang di panel navigasi kiri.
3. Pilih aplikasi OAuth di panel navigasi kiri.
4. Pilih aplikasi OAuth tertentu, lalu cari nilai Rahasia Klien. Jika Anda tidak dapat menemukan rahasia klien yang ada, maka Anda mungkin perlu membuat yang baru.

Menyetujui otorisasi

Setelah membuat otorisasi aplikasi di AppFabric, Anda akan menerima jendela pop-up dari GitHub untuk menyetujui otorisasi. Untuk menyetujui AppFabric otorisasi, pilih Izinkan.

Pastikan organisasi Anda telah memberikan akses ke aplikasi OAuth, jika pembatasan akses Aplikasi OAuth diaktifkan.

Google Analytics

Google Analyticsadalah layanan analisis web yang menyediakan statistik dan alat analisis dasar untuk optimasi mesin pencari (SEO) dan tujuan pemasaran. Google Analyticsdigunakan untuk

melacak kinerja situs web dan mengumpulkan wawasan pengunjung. Ini dapat membantu organisasi menentukan sumber utama lalu lintas pengguna, mengukur keberhasilan kegiatan pemasaran dan kampanye mereka, melacak penyelesaian tujuan (seperti pembelian, menambahkan produk ke gerobak), menemukan pola dan tren dalam keterlibatan pengguna dan mendapatkan informasi pengunjung lainnya seperti demografi. Situs web ritel kecil dan menengah sering digunakan Google Analytics untuk memperoleh dan menganalisis berbagai analisis perilaku pelanggan, yang dapat digunakan untuk meningkatkan kampanye pemasaran, mengarahkan lalu lintas situs web, dan mempertahankan pengunjung dengan lebih baik.

Anda dapat menggunakan keamanan AWS AppFabric untuk menerima log audit dan data pengguna dariAzure Monitor, menormalkan data ke dalam format Open Cybersecurity Schema Framework (OCSF), dan mengeluarkan data ke bucket Amazon Simple Storage Service (Amazon S3) atau aliran Amazon Data Firehose.

Topik

AppFabric dukungan untuk Google Analytics

AppFabric mendukung penerimaan log audit dariGoogle Analytics.

Prasyarat

Untuk digunakan AppFabric untuk mentransfer log audit dari Google Analytics tujuan yang didukung, Anda harus memenuhi persyaratan berikut:

- Anda harus menjadi Administrator Google Analytics akun.
- AppFabric Untuk mengirimkan log, Anda harus mengaktifkan Google AnalyticsAdmin API pada Google Cloud proyek Anda. Pastikan untuk menggunakan proyek baru saat menyiapkan aplikasi Google Analytics OAuth.

Pertimbangan batas tarif

Google Analyticsmemberlakukan batas tarif pada Google Analytics API. Untuk informasi selengkapnya tentang batas tarif Google Analytics API, lihat Batas dan Kuota di situs web Google Analytics. Jika kombinasi AppFabric dan aplikasi Google Analytics API Anda yang ada melebihi batas, log audit yang muncul AppFabric mungkin tertunda.

Pertimbangan keterlambatan data

Anda mungkin melihat penundaan hingga 30 menit untuk acara audit yang akan dikirim ke tujuan Anda. Hal ini disebabkan keterlambatan dalam peristiwa audit yang disediakan oleh aplikasi serta karena tindakan pencegahan yang diambil untuk mengurangi kehilangan data. Namun, ini mungkin dapat disesuaikan di tingkat akun. Untuk bantuan, hubungi AWS Support.

Menghubungkan AppFabric ke Google Analytics akun Anda

Setelah Anda membuat app bundle dalam AppFabric layanan, Anda harus mengotorisasi AppFabric denganGoogle Analytics. Gunakan langkah-langkah berikut untuk menemukan informasi yang diperlukan untuk mengotorisasiGoogle Analytics. AppFabric

Buat aplikasi OAuth

AppFabric terintegrasi dengan Google Analytics menggunakan OAuth. Selesaikan langkah-langkah berikut untuk membuat aplikasi OAuth di: Google Analytics

1. Untuk mengonfigurasi layar persetujuan OAuth Anda, ikuti petunjuk di Konfigurasikan layar persetujuan OAuth di Panduan Pengembang Google di situs web Google.
2. Pilih Eksternal untuk tipe Pengguna
3. Untuk mengonfigurasi kredensi OAuth AppFabric, ikuti petunjuk di bagian kredensial ID klien OAuth di halaman Buat kredenal akses di Panduan Pengembang Google.
4. Gunakan URL pengalihan dengan format berikut.

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   Di alamat itu, `<region>` adalah kode Wilayah AWS tempat Anda mengonfigurasi bundel AppFabric aplikasi. Misalnya, kode untuk Wilayah AS Timur (Virginia N.) adalah`us-east-1`. Untuk Wilayah itu, URL pengalihan adalah`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

Cakupan yang dibutuhkan

Anda harus menambahkan cakupan berikut ke aplikasi Google Analytics OAuth Anda:

```
https://www.googleapis.com/auth/analytics.edit
```

Otorisasi aplikasi

ID Penyewa

AppFabric akan meminta ID penyewa. ID penyewa di AppFabric adalah ID Google Analytics akun Anda.

1. Pergi ke halaman Google Analytics beranda.
2. Pilih Admin di panel navigasi.
3. Anda akan menemukan ID akun Anda di bawah Account > Account Settings > Account details > Account ID.

Nama penyewa

Masukkan nama yang mengidentifikasi Google Analytics organisasi unik ini. AppFabric menggunakan nama penyewa untuk memberi label pada otorisasi aplikasi dan konsumsi apa pun yang dibuat dari otorisasi aplikasi.

ID Klien

AppFabric akan meminta ID klien. Gunakan langkah-langkah berikut untuk menemukan ID klien Anda diGoogle Analytics:

1. Pergi ke halaman Kredensial.
2. Di bagian ID Klien OAuth 2.0, pilih ID klien yang Anda buat.
3. ID klien tercantum di bagian Informasi tambahan pada halaman.

Rahasia klien

AppFabric akan meminta rahasia klien. Gunakan langkah-langkah berikut untuk menemukan rahasia klien Anda diGoogle Analytics:

1. Pergi ke halaman Kredensial.
2. Di bagian ID Klien OAuth 2.0, pilih nama klien.
3. Rahasia klien tercantum di bagian Rahasia klien di halaman.

Otorisasi aplikasi

Setelah membuat otorisasi aplikasi di AppFabric Anda akan menerima jendela pop-up dari Google Analytics untuk menyetujui otorisasi. Untuk menyetujui AppFabric otorisasi dengan memilih Izinkan.

Google Workspace

Google Workspaceadalah kumpulan komputasi awan, alat produktivitas dan kolaborasi, perangkat lunak dan produk yang dikembangkan dan dipasarkan oleh Google.

Anda dapat menggunakan keamanan AWS AppFabric untuk menerima log audit dan data pengguna dariGoogle Workspace, menormalkan data ke dalam format Open Cybersecurity Schema Framework (OCSF), dan mengeluarkan data ke bucket Amazon Simple Storage Service (Amazon S3) atau aliran Amazon Data Firehose.

Topik

AppFabric dukungan untuk Google Workspace

AppFabric mendukung penerimaan informasi pengguna dan log audit dariGoogle Workspace.

Prasyarat

Untuk digunakan AppFabric untuk mentransfer log audit dari Google Workspace tujuan yang didukung, Anda harus memenuhi persyaratan berikut:

- Anda harus berlangganan paket Google Workspace Enterprise Standard. Untuk informasi selengkapnya tentang membuat atau meningkatkan ke paket Standar Google Workspace Perusahaan, lihat situs web Google WorkspacePaket.
- Anda harus memiliki pengguna dengan peran Administrator di AndaGoogle Workspace.
- AppFabric Untuk mengirimkan log, Anda harus mengaktifkan Google Admin SDK API di project Google Cloud Anda. Untuk informasi selengkapnya, lihat Mengaktifkan Google Workspace API di Panduan Google Workspace Developer.

Pertimbangan batas tarif

Google Workspacememberlakukan batas tarif pada Google Workspace API. Untuk informasi selengkapnya tentang batas tarif Google Workspace API, lihat Batas dan Kuota di Panduan Google Workspace Admin di Google Workspace situs web. Jika kombinasi AppFabric dan aplikasi Google Workspace API Anda yang ada melebihi batas, log audit yang muncul AppFabric mungkin tertunda.

Pertimbangan keterlambatan data

Anda mungkin melihat penundaan hingga 30 menit untuk sebagian besar acara audit dan penundaan hingga 4 jam untuk acara audit tertentu yang akan dikirimkan ke tujuan Anda. Hal ini disebabkan keterlambatan dalam peristiwa audit yang disediakan oleh aplikasi serta karena tindakan pencegahan yang diambil untuk mengurangi kehilangan data. Untuk informasi selengkapnya, lihat Retensi data dan waktu jeda di situs web Bantuan WorkSpace Admin Google. Namun, ini mungkin dapat disesuaikan di tingkat akun. Untuk bantuan kontak AWS Support.

Menghubungkan AppFabric ke Google Workspace akun Anda

Setelah Anda membuat app bundle dalam AppFabric layanan, Anda harus mengotorisasi AppFabric denganGoogle Workspace. Untuk menemukan informasi yang diperlukan untuk mengotorisasi Google Workspace AppFabric, gunakan langkah-langkah berikut.

Buat aplikasi OAuth

AppFabric terintegrasi dengan Google Workspace menggunakan OAuth. Untuk membuat aplikasi OAuth diGoogle Workspace, gunakan langkah-langkah berikut:

1. Untuk mengonfigurasi layar persetujuan OAuth Anda, ikuti petunjuk di Konfigurasikan layar persetujuan OAuth di Panduan Google Workspace Pengembang di situs web. Google Workspace

   Pilih Internal untuk tipe Pengguna.
2. Untuk mengonfigurasi kredensi OAuth AppFabric, ikuti petunjuk di bagian kredensial ID klien OAuth di halaman Buat kredenal akses di Panduan Pengembang. Google Workspace
3. Gunakan URL pengalihan dengan format berikut.

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   Di URL ini, `<region>` adalah kode untuk paket AppFabric aplikasi yang telah Anda konfigurasi. Wilayah AWS Misalnya, kode untuk Wilayah AS Timur (Virginia N.) adalah`us-east-1`. Untuk

Wilayah itu, URL pengalihan adalah`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

Lingkup yang dibutuhkan

Anda harus menambahkan cakupan berikut ke aplikasi Google Workspace OAuth Anda:

- `https://www.googleapis.com/auth/admin.reports.audit.readonly`
- `https://www.googleapis.com/auth/admin.directory.user`

Jika Anda tidak melihat cakupan ini, tambahkan Admin SDK API ke library Google Cloud API Anda.

Otorisasi aplikasi

ID Penyewa

AppFabric akan meminta ID penyewa Anda. ID penyewa di AppFabric adalah ID Google Workspace proyek Anda. Untuk menemukan ID project Anda, lihat Menemukan ID proyek di situs web Bantuan Konsol Google API.

Nama penyewa

Masukkan nama yang mengidentifikasi unik Google Workspace ini. AppFabric menggunakan nama penyewa untuk memberi label pada otorisasi aplikasi dan konsumsi apa pun yang dibuat dari otorisasi aplikasi.

ID Klien

AppFabric akan meminta ID klien Anda. Untuk menemukan ID klien Anda, gunakan langkah-langkah berikut:

1. Temukan ID klien Anda menggunakan informasi di bagian Lihat Kredensial pada halaman Kelola Kredensial di Panduan Pengembang. Google Workspace
2. Masukkan ID klien untuk klien OAuth Anda ke dalam bidang ID Klien di. AppFabric

Rahasia klien

AppFabric akan meminta rahasia klien Anda. Untuk menemukan rahasia klien Anda, gunakan langkah-langkah berikut:

1. Temukan rahasia klien Anda menggunakan informasi di bagian Lihat Kredensial pada halaman Kelola Kredensial di Panduan Pengembang. Google Workspace
2. Jika Anda perlu mengatur ulang rahasia klien Anda, gunakan instruksi di bagian Reset Client Secret pada halaman Kelola Kredensial pada Panduan Google WorkspacePengembang.
3. Masukkan rahasia klien Anda ke dalam bidang rahasia Klien di AppFabric.

Menyetujui otorisasi

Setelah membuat otorisasi aplikasi di AppFabric Anda akan menerima jendela pop-up dari Google Workspace untuk menyetujui otorisasi. Untuk menyetujui AppFabric otorisasi, pilih izinkan.

HubSpot

HubSpotadalah platform pelanggan dengan semua perangkat lunak, integrasi, dan sumber daya yang Anda butuhkan untuk menghubungkan pemasaran, penjualan, manajemen konten, dan layanan pelanggan Anda. HubSpotPlatform terhubung memungkinkan Anda untuk mengembangkan bisnis Anda lebih cepat dengan berfokus pada apa yang paling penting: pelanggan Anda. Anda dapat menggunakan keamanan AWS AppFabric untuk menerima log audit dan data pengguna dariHubSpot, menormalkan data ke dalam format Open Cybersecurity Schema Framework (OCSF), dan mengeluarkan data ke bucket Amazon Simple Storage Service (Amazon S3) atau aliran Amazon Data Firehose.

Topik

AppFabric dukungan untuk HubSpot

AppFabric mendukung penerimaan informasi pengguna dan log audit dariHubSpot.

Prasyarat

Untuk digunakan AppFabric untuk mentransfer log audit dari HubSpot tujuan yang didukung, Anda harus memenuhi persyaratan berikut:

- Anda harus memiliki akun dengan langganan Enterprise HubSpot untuk mengakses log audit akses. Untuk informasi selengkapnya tentang HubSpot langganan, lihat Mengelola HubSpot langganan Anda di Pangkalan HubSpot Pengetahuan.

- Anda harus memiliki akun pengembang dan aplikasi yang terkait dengan akun tersebut.
- Anda harus menjadi admin super untuk menginstal aplikasi di HubSpot akun Anda atau memiliki izin Akses Marketplace App ditambah izin pengguna untuk menerima cakupan yang diminta aplikasi.

Pertimbangan batas tarif

HubSpotmemberlakukan batas tarif pada HubSpot API. Untuk informasi selengkapnya tentang batas tarif HubSpot API, termasuk batasan untuk aplikasi yang menggunakan OAuth, lihat Batas Nilai di situs web. HubSpot Jika kombinasi AppFabric dan aplikasi HubSpot API Anda yang ada melebihi HubSpot batas, log audit yang muncul AppFabric mungkin tertunda.

Pertimbangan keterlambatan data

Anda mungkin melihat penundaan hingga 30 menit untuk acara audit yang akan dikirim ke tujuan Anda. Hal ini disebabkan keterlambatan dalam peristiwa audit yang disediakan oleh aplikasi serta karena tindakan pencegahan yang diambil untuk mengurangi kehilangan data. Namun, ini mungkin dapat disesuaikan di tingkat akun. Untuk bantuan, hubungi AWS Support.

Menghubungkan AppFabric ke HubSpot akun Anda

Setelah Anda membuat app bundle dalam AppFabric layanan, Anda harus mengotorisasi AppFabric denganHubSpot. Untuk menemukan informasi yang diperlukan untuk mengotorisasi HubSpot AppFabric, gunakan langkah-langkah berikut.

Buat aplikasi OAuth

AppFabric terintegrasi dengan HubSpot menggunakan OAuth. Untuk membuat aplikasi OAuth diHubSpot, gunakan langkah-langkah berikut:

1. Ikuti petunjuk di bagian Buat aplikasi publik di HubSpot panduan di HubSpot situs web.
2. Dari tab Auth, tambahkan tiga cakupan yang tercantum di. Cakupan yang dibutuhkan
3. Gunakan URL pengalihan dengan format berikut di URL Pengalihan.

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   Di URL ini, <region>adalah kode untuk paket AppFabric aplikasi yang telah Anda konfigurasi. Wilayah AWS Misalnya, kode untuk Wilayah AS Timur (Virginia N.) adalah`us-east-1`. Untuk

Wilayah itu, URL pengalihan adalah`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

4. Pilih Buat aplikasi.

Cakupan yang dibutuhkan

Anda harus menambahkan cakupan berikut ke aplikasi HubSpot OAuth Anda:

- `settings.users.read`
- `crm.objects.owners.read`
- `account-info.security.read`

Otorisasi aplikasi

ID Penyewa

Masukkan ID yang mengidentifikasi HubSpot organisasi unik ini. Misalnya, masukkan ID HubSpot akun Anda.

Nama penyewa

Masukkan nama yang mengidentifikasi HubSpot organisasi unik ini. AppFabric menggunakan nama penyewa untuk memberi label pada otorisasi aplikasi dan konsumsi apa pun yang dibuat dari otorisasi aplikasi.

ID Klien

AppFabric akan meminta ID klien. Untuk menemukan ID klien AndaHubSpot, gunakan langkah-langkah berikut:

1. Arahkan ke halaman HubSpot login dan masuk menggunakan kredensi akun pengembang Anda.
2. Dari menu Apps, pilih aplikasi Anda.
3. Dari tab Auth, cari nilai ID Klien.

Rahasia klien

AppFabric akan meminta rahasia klien. Untuk menemukan rahasia klien AndaHubSpot, gunakan langkah-langkah berikut:

1. Arahkan ke halaman HubSpot login dan masuk menggunakan kredensi akun pengembang Anda.
2. Dari menu Apps, pilih aplikasi Anda.
3. Dari tab Auth, cari nilai rahasia Klien.

Menyetujui otorisasi

Setelah membuat otorisasi aplikasi di AppFabric, Anda akan menerima jendela pop-up dari HubSpot untuk menyetujui otorisasi. Masuk ke akun Anda menggunakan kredensi akun perusahaan Anda (bukan akun pengembang Anda) untuk menyetujui otorisasi. AppFabric Pilih izinkan.

IBM Security® Verify

IBM Security® VerifyKeluarga ini menyediakan kemampuan otomatis, berbasis cloud, dan lokal untuk mengelola tata kelola identitas, mengelola tenaga kerja dan identitas dan akses konsumen, serta mengendalikan akun istimewa. Baik Anda perlu menerapkan solusi cloud atau lokal, IBM Security® Verify membantu Anda membangun kepercayaan dan melindungi dari ancaman orang dalam terhadap tenaga kerja dan konsumen Anda.

Anda dapat menggunakan keamanan AWS AppFabric untuk menerima log audit dan data pengguna dariIBM Security® Verify, menormalkan data ke dalam format Open Cybersecurity Schema Framework (OCSF), dan mengeluarkan data ke bucket Amazon Simple Storage Service (Amazon S3) atau aliran Amazon Data Firehose.

Topik

- AppFabric dukungan untuk IBM Security® Verify
- Menghubungkan AppFabric ke IBM Security® Verify akun Anda

AppFabric dukungan untuk IBM Security® Verify

AppFabric mendukung penerimaan informasi pengguna dan log audit dariIBM Security® Verify.

Prasyarat

Untuk digunakan AppFabric untuk mentransfer log audit dari IBM Security® Verify tujuan yang didukung, Anda harus memenuhi persyaratan berikut:

- Untuk mengakses log audit, Anda harus memiliki akun IBM Security® VerifySaaS.

- Untuk mengakses log audit, Anda harus memiliki peran administrator di akun IBM Security® Verify SaaS Anda.

Pertimbangan batas tarif

IBM Security® Verifymemberlakukan batas tarif pada IBM Security® Verify API. Untuk informasi selengkapnya tentang batas tarif IBM Security® Verify API, lihat Ketentuan IBM. Jika kombinasi AppFabric dan aplikasi IBM Security® Verify API Anda yang ada melebihi IBM Security® Verify batas, log audit yang muncul AppFabric mungkin tertunda.

Pertimbangan keterlambatan data

Anda mungkin melihat penundaan hingga 30 menit dalam acara audit untuk dikirim ke tujuan Anda. Hal ini disebabkan keterlambatan dalam peristiwa audit yang disediakan oleh aplikasi serta karena tindakan pencegahan yang diambil untuk mengurangi kehilangan data. Namun, ini mungkin dapat disesuaikan pada tingkat akun. Untuk bantuan, hubungi AWS Support.

Menghubungkan AppFabric ke IBM Security® Verify akun Anda

Setelah Anda membuat app bundle dalam AppFabric layanan, Anda harus mengotorisasi AppFabric denganIBM Security® Verify. Untuk menemukan informasi yang diperlukan untuk mengotorisasi IBM Security® Verify AppFabric, gunakan langkah-langkah berikut.

Buat aplikasi OAuth

AppFabric terintegrasi dengan IBM Security® Verify menggunakan OAuth. Untuk membuat aplikasi OAuthIBM Security® Verify, lihat Membuat klien API di situs web dokumentasi IBM.

1. Untuk login pertama kali, gunakan URL login dan kredensional yang dikirim ke alamat email terdaftar Anda.
2. Akses konsol administrasi di`https://<hostname>.verify.ibm.com/ui/admin/`. Untuk informasi selengkapnya, lihat Mengakses. IBM Security® Verify
3. Di konsol administrasi, di bawah Security < API Access < API Client, pilih Tambah.
4. Pilih opsi berikut. Ini diperlukan untuk membaca log audit dan detail pengguna.
   - Baca laporan
   - Baca pengguna dan grup
5. Simpan opsi Default dalam metode Otentikasi Klien.

Jangan mengedit bidang Cakupan kustom.

6. Pilih Selanjutnya.
7. Jangan mengedit bidang filter IP.
8. Pilih Selanjutnya.
9. Jangan mengedit bidang Properti tambahan.
10. Pilih Selanjutnya.
11. Tentukan Nama dan Deskripsi. Deskripsi adalah opsional.
12. Pilih Buat klien API.

Otorisasi aplikasi

ID Penyewa

AppFabric akan meminta ID penyewa Anda. Anda dapat menemukan ID penyewa di URL IBM Security® Verify standar. Misalnya, di `https://hostname.verify.ibm.com/` URL, ID penyewa adalah *`nama host`* yang dapat ditemukan sebelumnya `.verify.ibm.com` (atau sebelumnya `ice.ibmcloud.com` jika Anda menggunakan nama host sebelumnya). Jika Anda menggunakan URL kesombongan, hubungi tim IBM Security® Verify dukungan Anda untuk mendapatkan URL standar Anda.

Nama penyewa

Masukkan nama yang mengidentifikasi IBM Security® Verify penyewa unik ini. AppFabric menggunakan nama penyewa untuk memberi label pada otorisasi aplikasi dan konsumsi apa pun yang dibuat dari otorisasi aplikasi.

ID Klien

AppFabric akan meminta ID klien. Untuk menemukan ID klien AndaIBM Security® Verify, gunakan langkah-langkah berikut:

1. Untuk login pertama kali, gunakan URL login dan kredensional yang dikirim ke alamat email terdaftar Anda.
2. Akses konsol administrasi dih`ttps://<hostname>.verify.ibm.com/ui/admin/`. Untuk informasi selengkapnya, lihat Mengakses. IBM Security® Verify

3. Di konsol administrasi, di bawah Security < API Access < API Client, pilih elipsis () di sebelah aplikasi OAuth tertentu.
4. Pilih Detail koneksi.
5. Temukan ID Klien di bawah kredensi API.

Rahasia klien

AppFabric akan meminta rahasia klien. Untuk menemukan rahasia klien AndaIBM Security® Verify, gunakan langkah-langkah berikut:

1. Untuk login pertama kali, gunakan URL login dan kredensional yang dikirim ke alamat email terdaftar Anda.
2. Akses konsol administrasi di`https://<hostname>.verify.ibm.com/ui/admin/`. Untuk informasi selengkapnya, lihat Mengakses. IBM Security® Verify
3. Di konsol administrasi, di bawah Security < API Access < API Client, pilih elipsis () di sebelah aplikasi OAuth tertentu.
4. Pilih Detail koneksi.
5. Temukan rahasia Klien di bawah kredensi API.

JumpCloud

JumpCloud Inc. adalah perusahaan perangkat lunak perusahaan Amerika yang menyediakan platform direktori berbasis cloud untuk manajemen identitas. Ini memusatkan dan menyederhanakan manajemen identitas, memungkinkan pengguna untuk mengakses sistem, aplikasi, jaringan, dan server file mereka dengan aman dengan satu set kredensi, terlepas dari platform, protokol, penyedia, atau lokasi.

Anda dapat menggunakan AWS AppFabric untuk menerima log audit dan data pengguna dari JumpCloud, menormalkan data ke dalam format Open Cybersecurity Schema Framework (OCSF), dan menampilkan data ke bucket Amazon Simple Storage Service (Amazon S3) atau aliran Amazon Kinesis Data Firehose.

Topik

- AppFabric dukungan untuk JumpCloud
- Menghubungkan AppFabric ke JumpCloud akun Anda

AppFabric dukungan untuk JumpCloud

AppFabric mendukung penerimaan informasi pengguna dan log audit dariJumpCloud.

Prasyarat

Untuk digunakan AppFabric untuk mentransfer log audit dari JumpCloud tujuan yang didukung, Anda harus memenuhi persyaratan berikut:

- Anda harus memiliki paket JumpCloud berlangganan berbayar aktif. Untuk informasi lebih lanjut, lihat Select a package that's right for youdi JumpCloud situs web.
- Anda harus memiliki peran “Admin dengan Penagihan”.

Pertimbangan batas tarif

JumpCloudtidak mempublikasikan batas tarif. Anda harus membuat kasus dukungan atau menghubungi tim JumpCloud Pelanggan Anda. Jika kombinasi AppFabric dan aplikasi JumpCloud API Anda yang ada melebihi JumpCloud's batas, log audit yang muncul AppFabric mungkin tertunda.

Pertimbangan keterlambatan data

Anda mungkin melihat penundaan hingga 30 menit untuk acara audit yang akan dikirim ke tujuan Anda. Hal ini disebabkan keterlambatan dalam peristiwa audit yang disediakan oleh aplikasi, dan karena tindakan pencegahan yang diambil untuk mengurangi kehilangan data. Namun, ini mungkin dapat disesuaikan di tingkat akun. Untuk bantuan, hubungi AWS Support.

Menghubungkan AppFabric ke JumpCloud akun Anda

Setelah Anda membuat app bundle dalam AppFabric layanan, Anda harus mengotorisasi AppFabric denganJumpCloud. Untuk menemukan informasi yang diperlukan untuk mengotorisasi JumpCloud AppFabric, ikuti langkah-langkah di bagian selanjutnya.

Buat token Organisasi dari JumpCloud akun

AppFabric menggunakan kunci API untuk diintegrasikan dengan JumpCloud Untuk membuat kunci API JumpCloud, ikuti langkah-langkah berikut:.

1. Masuk ke JumpCloud akun Anda sebagai administrator.
2. Di Portal Admin, pilih inisiasi akun Anda, terletak di kanan atas, dan pilih Kunci API Saya dari menu.
3. Pilih Generate New API Key, atau pilih kunci yang sudah ada.

> **Note**
>
> JumpCloudhanya mengizinkan satu kunci API aktif. Membuat kunci API baru akan mencabut akses ke kunci API saat ini. Ini akan membuat semua panggilan menggunakan kunci API sebelumnya tidak dapat diakses. Anda harus memperbarui integrasi yang ada yang menggunakan kunci API sebelumnya dengan nilai kunci baru.

Otorisasi aplikasi

ID Penyewa

AppFabric akan meminta ID penyewa Anda. Di sini “ID Organisasi” akan menjadi ID Penyewa. Untuk menemukan “ID Organisasi”, ikuti langkah-langkah ini.

1. Masuk ke JumpCloud akun Anda.
2. Di panel navigasi, pilih Pengaturan, lalu Profil Organisasi, lalu Umum.
3. Pilih ikon “mata” untuk menghapus tampilan yang dikaburkan.
4. Pilih ikon “halaman ganda” untuk menyalin ID.

Nama penyewa

Masukkan nama yang mengidentifikasi JumpCloud organisasi unik ini. AppFabric menggunakan nama penyewa untuk memberi label pada otorisasi aplikasi dan konsumsi apa pun yang dibuat dari otorisasi aplikasi.

Token akun layanan

AppFabric akan meminta token akun layanan Anda. Di AppFabric, ini adalah token API organisasi yang Anda buatBuat token Organisasi dari JumpCloud akun, sebelumnya dalam topik ini.

Microsoft365

Microsoft365 adalah keluarga produk perangkat lunak produktivitas, kolaborasi, dan layanan berbasis cloud yang dimiliki oleh. Microsoft

Anda dapat menggunakan keamanan AWS AppFabric untuk menerima log audit dan data pengguna dari Microsoft 365, menormalkan data ke dalam format Open Cybersecurity Schema Framework (OCSF), dan menampilkan data ke bucket Amazon Simple Storage Service (Amazon S3) atau aliran Amazon Data Firehose.

Topik

AppFabric dukungan untuk Microsoft 365

AppFabric mendukung penerimaan informasi pengguna dan log audit dari Microsoft 365.

Prasyarat

Untuk digunakan AppFabric untuk mentransfer log audit dari Microsoft 365 ke tujuan yang didukung, Anda harus memenuhi persyaratan berikut:

- Anda harus berlangganan paket Microsoft 365 Enterprise. Untuk informasi selengkapnya tentang membuat atau meningkatkan ke paket Microsoft 365 Enterprise, lihat Paket Microsoft365 Enterprise di Microsoft situs web.
- Anda harus memiliki pengguna dengan izin Administrator di akun Microsoft 365 Anda.
- Anda harus mengaktifkan pencatatan audit untuk organisasi Anda. Untuk informasi selengkapnya, lihat Mengaktifkan atau menonaktifkan audit di Microsoft situs web.

Pertimbangan batas tarif

Microsoft365 memberlakukan batas tarif pada API Microsoft 365. Untuk informasi selengkapnya tentang batas tarif API Microsoft 365, lihat Batas pembatasan khusus layanan Microsoft Grafik dalam dokumentasi Microsoft Grafik di situs web. Microsoft Jika kombinasi AppFabric dan Microsoft 365 aplikasi API Anda yang ada melebihi batas, log audit yang muncul AppFabric mungkin tertunda.

Pertimbangan keterlambatan data

Anda mungkin melihat penundaan hingga 30 menit untuk acara audit yang akan dikirim ke tujuan Anda. Hal ini disebabkan keterlambatan dalam peristiwa audit yang disediakan oleh aplikasi serta karena tindakan pencegahan yang diambil untuk mengurangi kehilangan data. Namun, ini mungkin dapat disesuaikan di tingkat akun. Untuk bantuan, hubungi AWS Support.

Menghubungkan AppFabric ke akun Microsoft 365 Anda

Setelah Anda membuat app bundle dalam AppFabric layanan, Anda harus mengotorisasi AppFabric dengan Microsoft 365. Untuk menemukan informasi yang diperlukan untuk mengotorisasi Microsoft 365 AppFabric, gunakan langkah-langkah berikut.

Buat aplikasi OAuth

AppFabric terintegrasi dengan Microsoft 365 menggunakan OAuth. Untuk membuat aplikasi OAuth di Microsoft 365, gunakan langkah-langkah berikut:

1. Ikuti petunjuk di bagian Daftarkan aplikasi di Panduan Pengembang Direktori Aktif Azure di Microsoft situs web.

   Pilih Akun di direktori organisasi ini hanya dalam konfigurasi Jenis Akun yang Didukung.
2. Ikuti petunjuk di bagian Tambahkan URI pengalihan di Azure Active Directory Developer Guide.

   Pilih platform Web.

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   Di URL ini, `<region>` adalah kode untuk paket AppFabric aplikasi yang telah Anda konfigurasi. Wilayah AWS Misalnya, kode untuk Wilayah AS Timur (Virginia N.) adalah`us-east-1`. Untuk Wilayah itu, URL pengalihan adalah`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

   Anda dapat melewati kolom input lainnya untuk platform Web.
3. Ikuti petunjuk di bagian Tambahkan rahasia klien dari Panduan Pengembang Direktori Aktif Azure.

Izin yang diperlukan

Anda harus menambahkan izin berikut ke aplikasi OAuth Anda. Untuk menambahkan izin, ikuti petunjuk di bagian Tambahkan izin untuk mengakses API web Anda pada Panduan Pengembang Direktori Aktif Azure.

- `Microsoft Graph API>` `User.Read` (ditambahkan secara otomatis)
- `Office 365 Management APIs>` `ActivityFeed.Read` (Pilih Jenis Delegasi)
- `Office 365 Management APIs>` `ActivityFeed.ReadDlp` (Pilih Jenis Delegasi)
- `Office 365 Management APIs>` `ServiceHealth.Read` (Pilih Jenis Delegasi)

Setelah Anda menambahkan izin, untuk memberikan izin admin untuk izin, ikuti petunjuk di bagian tombol persetujuan Admin pada Panduan Pengembang Direktori Aktif Azure.

Otorisasi aplikasi

AppFabric mendukung penerimaan informasi pengguna dan log audit dari akun Microsoft 365 Anda. Untuk menerima log audit dan data pengguna dari Microsoft 365, Anda harus membuat dua otorisasi aplikasi, satu yang diberi nama Microsoft365 dalam daftar drop-down otorisasi aplikasi, dan lainnya bernama Microsoft365 Audit Log dalam daftar drop-down otorisasi aplikasi. Anda dapat menggunakan ID penyewa, ID klien, dan rahasia klien yang sama untuk kedua otorisasi aplikasi. Untuk menerima log audit dari Microsoft 365, Anda memerlukan otorisasi aplikasi Log Audit MicrosoftMicrosoft365 dan 365. Untuk menggunakan alat akses pengguna saja, hanya otorisasi aplikasi Microsoft365 yang diperlukan.

ID Penyewa

AppFabric akan meminta ID penyewa Anda. ID penyewa di AppFabric adalah ID penyewa Azure Active Directory Anda. Untuk menemukan ID penyewa Azure Active Directory, lihat Cara menemukan ID penyewa Azure Active Directory di Dokumentasi Produk Azure di situs web. Microsoft

Nama penyewa

Masukkan nama yang mengidentifikasi akun Microsoft 365 unik ini. AppFabric menggunakan nama penyewa untuk memberi label pada otorisasi aplikasi dan konsumsi apa pun yang dibuat dari otorisasi aplikasi.

ID Klien

AppFabric akan meminta ID klien Anda. ID klien di AppFabric adalah ID aplikasi Microsoft 365 (klien). Untuk menemukan ID aplikasi (klien) Microsoft 365 Anda, gunakan langkah-langkah berikut:

1. Buka halaman ikhtisar untuk aplikasi OAuth yang Anda gunakan. AppFabric
2. ID aplikasi (klien) muncul di bawah Essentials.
3. Masukkan ID aplikasi (klien) untuk klien OAuth Anda ke dalam bidang ID Klien di. AppFabric

Rahasia klien

AppFabric akan meminta rahasia klien Anda. Microsoft365 memberikan nilai ini hanya ketika Anda awalnya membuat rahasia klien untuk aplikasi OAuth Anda. Untuk menghasilkan rahasia klien baru jika Anda tidak memilikinya, gunakan langkah-langkah berikut:

1. Untuk membuat rahasia klien, ikuti petunjuk di bagian Tambahkan rahasia klien dari Panduan Pengembang Direktori Aktif Azure.

2. Masukkan isi bidang Nilai ke dalam bidang rahasia Klien di AppFabric.

Menyetujui otorisasi

Setelah membuat otorisasi aplikasi di AppFabric, Anda akan menerima jendela pop-up dari Microsoft 365 untuk menyetujui otorisasi. Untuk menyetujui AppFabric otorisasi, pilih izinkan.

Miro

Miroadalah ruang kerja online untuk inovasi yang memungkinkan tim terdistribusi dari berbagai ukuran untuk membangun hal besar berikutnya. Kanvas tanpa batas platform memungkinkan tim untuk memimpin lokakarya dan pertemuan yang menarik, merancang produk, bertukar pikiran, dan banyak lagi. MiroBerkantor pusat di San Francisco dan Amsterdam, melayani lebih dari 50 juta pengguna di seluruh dunia, termasuk 99% dari Fortune 100. MiroDidirikan pada tahun 2011 dan saat ini memiliki lebih dari 1.500 karyawan di 12 hub di seluruh dunia. Untuk mempelajari lebih lanjut, kunjungi Miro.

Miromencakup rangkaian lengkap kemampuan kolaboratif yang dirancang untuk inovasi termasuk diagram, wireframing, visualisasi data real-time, fasilitasi lokakarya, dan dukungan bawaan untuk praktik tangkas, lokakarya, dan presentasi interaktif. Mirobaru-baru ini mengumumkan Miro AI yang memperluas Miro kemampuan, dengan pemetaan dan diagram berbasis AI, pengelompokan dan ringkasan, dan pembuatan konten. Miromemungkinkan organisasi untuk mengurangi jumlah alat mandiri, mengurangi fragmentasi informasi dan biaya.

Anda dapat menggunakan keamanan AWS AppFabric untuk menerima log audit dan data pengguna dariMiro, menormalkan data ke dalam format Open Cybersecurity Schema Framework (OCSF), dan menampilkan data ke bucket Amazon Simple Storage Service (Amazon S3) atau aliran Amazon Data Firehose.

Topik

- AppFabric dukungan untuk Miro
- Menghubungkan AppFabric ke Miro akun Anda

AppFabric dukungan untuk Miro

AppFabric mendukung penerimaan informasi pengguna dan log audit dariMiro.

Prasyarat

Untuk digunakan AppFabric untuk mentransfer log audit dari Miro tujuan yang didukung, Anda harus memenuhi persyaratan berikut:

- Anda harus memiliki Miro Enterprise Plan. Untuk informasi lebih lanjut tentang jenis paket Miro, lihat halaman Miroharga di Miro situs web.
- Anda harus memiliki pengguna dengan peran Admin Perusahaan di Miro akun Anda. Untuk informasi selengkapnya tentang peran, lihat bagian Tingkat Perusahaan Peran di Miro di situs web Pusat Bantuan Miro.
- Anda harus memiliki tim Pengembang Perusahaan di Miro akun Anda. Untuk informasi tentang membuat tim pengembang, lihat Tim Pengembang Perusahaan di situs web Pusat Bantuan Miro.

Pertimbangan batas tarif

Miromemberlakukan batas tarif pada Miro API. Untuk informasi selengkapnya tentang batas tarif Miro API, lihat Pembatasan Nilai dalam Panduan Miro Pengembang di Miro situs web. Jika kombinasi AppFabric dan aplikasi Miro API Anda yang ada melebihi batas, log audit yang muncul AppFabric mungkin tertunda.

Pertimbangan keterlambatan data

Anda mungkin melihat penundaan hingga 30 menit untuk acara audit yang akan dikirim ke tujuan Anda. Hal ini disebabkan keterlambatan dalam peristiwa audit yang disediakan oleh aplikasi serta karena tindakan pencegahan yang diambil untuk mengurangi kehilangan data. Namun, ini mungkin dapat disesuaikan di tingkat akun. Untuk bantuan, hubungi AWS Support.

Menghubungkan AppFabric ke Miro akun Anda

Setelah Anda membuat app bundle dalam AppFabric layanan, Anda harus mengotorisasi AppFabric denganMiro. Untuk menemukan informasi yang diperlukan untuk mengotorisasi Miro AppFabric, gunakan langkah-langkah berikut.

Buat aplikasi OAuth

AppFabric terintegrasi dengan Miro menggunakan OAuth. Untuk membuat aplikasi OAuth diMiro, gunakan langkah-langkah berikut:

1. Untuk membuat aplikasi OAuth, ikuti petunjuk di bagian Membuat dan menginstal aplikasi pada artikel tim Pengembang Perusahaan di situs web Pusat Bantuan Miro.

2. Pada dialog pembuatan aplikasi, pilih kotak centang token otorisasi pengguna kedaluwarsa setelah Anda memilih tim pengembang di organisasi perusahaan.

> **Note**
>
> Anda harus melakukan ini sebelum membuat aplikasi karena Anda tidak dapat mengubah opsi ini setelah Anda membuat aplikasi.

3. Pada halaman aplikasi, masukkan URL dengan format berikut di bagian Redirect URI untuk OAuth 2.0.

```
https://<region>.console.aws.amazon.com/appfabric/oauth2
```

   Di URL ini, <region>adalah kode untuk paket AppFabric aplikasi yang telah Anda konfigurasi. Wilayah AWS Misalnya, kode untuk Wilayah AS Timur (Virginia N.) adalah`us-east-1`. Untuk Wilayah itu, URL pengalihan adalah`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

4. Salin dan simpan ID klien dan rahasia klien Anda untuk digunakan dalam otorisasi AppFabric aplikasi.

Cakupan yang dibutuhkan

Anda harus menambahkan cakupan berikut di `Permissions` bagian halaman aplikasi Miro OAuth Anda:

- `auditlogs:read`
- `organizations:read`

Otorisasi aplikasi

ID Penyewa

AppFabric akan meminta ID penyewa Anda. ID penyewa di AppFabric adalah ID Miro Tim Anda. Untuk informasi tentang cara menemukan ID Tim Miro Anda, lihat bagian Pertanyaan yang Sering Diajukan di Saya adalah Miro Admin baru. Dimana untuk memulai? di situs web Pusat Miro Bantuan.

Nama penyewa

Masukkan nama yang mengidentifikasi Miro organisasi unik ini. AppFabric menggunakan nama penyewa untuk memberi label pada otorisasi aplikasi dan konsumsi apa pun yang dibuat dari otorisasi aplikasi.

ID Klien

AppFabric akan meminta ID klien Anda. Untuk menemukan ID klien Anda, gunakan langkah-langkah berikut:

1. Arahkan ke pengaturan Miro profil Anda.
2. Pilih tab Aplikasi Anda.
3. Pilih aplikasi yang Anda gunakan untuk terhubung AppFabric.
4. Masukkan ID klien dari bagian App Credentials ke dalam kolom Client ID di. AppFabric

Rahasia klien

AppFabric akan meminta rahasia klien Anda. Untuk menemukan rahasia klien Anda, gunakan langkah-langkah berikut:

1. Arahkan ke pengaturan Miro profil Anda.
2. Pilih tab Aplikasi Anda.
3. Pilih aplikasi yang Anda gunakan untuk terhubung AppFabric.
4. Masukkan rahasia klien dari bagian Kredensial Aplikasi ke dalam bidang rahasia Klien di. AppFabric

Menyetujui otorisasi

Setelah membuat otorisasi aplikasi di AppFabric, Anda akan menerima jendela pop-up dari Miro untuk menyetujui otorisasi. Untuk menyetujui AppFabric otorisasi, pilih Izinkan.

Okta

Oktaadalah Perusahaan Identitas Dunia. Sebagai mitra Identitas independen terkemuka, Okta membebaskan semua orang untuk menggunakan teknologi apa pun dengan aman — di mana saja, di perangkat atau aplikasi apa pun. Merek yang paling tepercaya percaya Okta untuk mengaktifkan akses, otentikasi, dan otomatisasi yang aman. Dengan fleksibilitas dan netralitas sebagai inti dari

Okta Workforce Identity and Customer Identity Clouds, para pemimpin bisnis dan pengembang dapat fokus pada inovasi dan mempercepat transformasi digital, berkat solusi yang dapat disesuaikan dan lebih dari 7.000 integrasi pra-bangun. Oktaadalah membangun dunia di mana Identitas adalah milik Anda. Pelajari lebih lanjut okta di.com.

Anda dapat menggunakan keamanan AWS AppFabric untuk menerima log audit dan data pengguna dariOkta, menormalkan data ke dalam format Open Cybersecurity Schema Framework (OCSF), dan mengeluarkan data ke bucket Amazon Simple Storage Service (Amazon S3) atau aliran Amazon Data Firehose.

Topik

AppFabric dukungan untuk Okta

AppFabric mendukung penerimaan informasi pengguna dan log audit dariOkta.

Prasyarat

Untuk digunakan AppFabric untuk mentransfer log audit dari Okta tujuan yang didukung, Anda harus memenuhi persyaratan berikut:

- Anda dapat menggunakan AppFabric dengan jenis Okta paket apa pun.
- Anda harus memiliki pengguna dengan peran Super Admin di Okta akun Anda.
- Pengguna yang menyetujui otorisasi aplikasi juga AppFabric harus memiliki peran Super Admin di akun AndaOkta.

Pertimbangan batas tarif

Oktamemberlakukan batas tarif pada Okta API. Untuk informasi selengkapnya tentang batas tarif Okta API, lihat Batas tarif di Panduan Okta Pengembang di Okta situs web. Jika kombinasi AppFabric dan aplikasi Okta API Anda yang ada melebihi Okta batas, log audit yang muncul AppFabric mungkin tertunda.

Pertimbangan keterlambatan data

Anda mungkin melihat penundaan hingga 30 menit untuk acara audit yang akan dikirim ke tujuan Anda. Hal ini disebabkan keterlambatan dalam peristiwa audit yang disediakan oleh aplikasi serta

karena tindakan pencegahan yang diambil untuk mengurangi kehilangan data. Namun, ini mungkin dapat disesuaikan di tingkat akun. Untuk bantuan, hubungi AWS Support.

Menghubungkan AppFabric ke Okta akun Anda

Setelah Anda membuat app bundle dalam AppFabric layanan, Anda harus mengotorisasi AppFabric denganOkta. Untuk menemukan informasi yang diperlukan untuk mengotorisasi Okta AppFabric, gunakan langkah-langkah berikut.

Buat aplikasi OAuth

AppFabric terintegrasi dengan Okta menggunakan OAuth. Untuk membuat aplikasi OAuth untuk terhubung AppFabric, ikuti petunjuk di Buat integrasi aplikasi OIDC di situs web Pusat Bantuan. Okta Berikut ini adalah pertimbangan konfigurasi untuk AppFabric:

1. Untuk Jenis Aplikasi, pilih Aplikasi Web.
2. Untuk jenis Grant, pilih Authorization Code dan Refresh Token.
3. Gunakan URL pengalihan dengan format berikut sebagai URI pengalihan Masuk dan URI pengalihan Keluar.

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   Di URL ini, <region>adalah kode untuk paket AppFabric aplikasi yang telah Anda konfigurasi. Wilayah AWS Misalnya, kode untuk Wilayah AS Timur (Virginia N.) adalah`us-east-1`. Untuk Wilayah itu, URL pengalihan adalah`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.
4. Anda dapat melewati konfigurasi Trusted Origins.
5. Berikan akses ke semua orang di Okta organisasi Anda dalam konfigurasi Akses Terkendali.

   > **Note**
   >
   > Jika Anda melewati langkah ini selama pembuatan aplikasi OAuth awal, Anda dapat menetapkan semua orang di organisasi Anda sebagai grup menggunakan tab Penugasan pada halaman konfigurasi aplikasi.
6. Anda dapat meninggalkan semua opsi lain dengan nilai defaultnya.

Cakupan yang dibutuhkan

Anda harus menambahkan cakupan berikut ke aplikasi Okta OAuth Anda:

- `okta.logs.read`
- `okta.users.read`

Otorisasi aplikasi

ID Penyewa

AppFabric akan meminta ID penyewa. ID penyewa di AppFabric adalah Okta domain Anda. Untuk informasi selengkapnya tentang menemukan Okta domain Anda, lihat Menemukan Oktadomain Anda di Panduan Okta Pengembang di Okta situs web.

Nama penyewa

Masukkan nama yang mengidentifikasi Okta organisasi unik ini. AppFabric menggunakan nama penyewa untuk memberi label pada otorisasi aplikasi dan konsumsi apa pun yang dibuat dari otorisasi aplikasi.

ID Klien

AppFabric akan meminta ID klien. Untuk menemukan ID klien AndaOkta, gunakan langkah-langkah berikut:

1. Arahkan ke konsol Okta pengembang.
2. Pilih tab Aplikasi.
3. Pilih aplikasi Anda dan kemudian pilih tab Umum.
4. Gulir ke bagian Client Client Client.
5. Masukkan ID klien dari klien OAuth Anda ke bidang ID Klien di. AppFabric

Rahasia klien

AppFabric akan meminta rahasia klien. Untuk menemukan rahasia klien AndaOkta, gunakan langkah-langkah berikut:

1. Arahkan ke konsol Okta pengembang.

2. Pilih tab Aplikasi.
3. Pilih aplikasi Anda dan kemudian pilih tab Umum.
4. Gulir ke bagian Client Client Client.
5. Masukkan rahasia klien dari aplikasi OAuth Anda ke bidang Rahasia Klien di. AppFabric

Menyetujui otorisasi

Setelah membuat otorisasi aplikasi di AppFabric, Anda akan menerima jendela pop-up dari Okta untuk menyetujui otorisasi. Untuk menyetujui AppFabric otorisasi, pilih izinkan. Pengguna yang menyetujui Okta otorisasi harus memiliki izin Super Admin. Okta

OneLogin by One Identity

OneLogin by One Identityadalah solusi manajemen akses berbasis cloud modern yang mengelola semua identitas digital dengan mulus untuk tenaga kerja, pelanggan, dan mitra Anda. OneLoginmenyediakan sistem masuk tunggal (SSO) yang aman, otentikasi multi-faktor (MFA), otentikasi adaptif, MFA tingkat desktop, integrasi direktori dengan AD, LDAP, G Suite dan direktori eksternal lainnya, manajemen siklus hidup identitas, dan banyak lagi. DenganOneLogin, Anda dapat melindungi organisasi Anda dari serangan yang paling umum, sehingga meningkatkan keamanan, pengalaman pengguna tanpa gesekan, dan kepatuhan terhadap persyaratan peraturan.Anda dapat menggunakan keamanan AWS AppFabric untuk menerima log audit dan data pengguna dariOneLogin, menormalkan data ke dalam format Open Cybersecurity Schema Framework (OCSF), dan menampilkan data ke Amazon Simple Storage Service (Amazon S3) bucket atau bucket Amazon Data Firehose Aliran Firehose.

Topik

- AppFabric dukungan untuk OneLogin by One Identity
- Menghubungkan AppFabric ke OneLogin by One Identity akun Anda

AppFabric dukungan untuk OneLogin by One Identity

AppFabric mendukung penerimaan informasi pengguna dan log audit dariOneLogin by One Identity.

Prasyarat

Untuk digunakan AppFabric untuk mentransfer log audit dari OneLogin by One Identity tujuan yang didukung, Anda harus memenuhi persyaratan berikut:

- Anda harus memiliki akun OneLogin Advanced atau Professional.
- Anda harus memiliki pengguna dengan Admin/Delegated Admin Privileges.

Pertimbangan batas tarif

OneLogin by One Identitymemberlakukan batas tarif pada OneLogin API. Untuk informasi selengkapnya tentang batas tarif OneLogin API, lihat Mendapatkan Batas Tingkat di Referensi OneLogin API. Jika kombinasi AppFabric dan aplikasi OneLogin API Anda yang ada melebihi OneLogin batas, log audit yang muncul AppFabric mungkin tertunda. Namun, batas OneLogin tarif dapat ditingkatkan. Untuk bantuan, hubungi Manajer OneLogin by One Identity Akun atau kontak Anda One Identity.

Pertimbangan keterlambatan data

Anda mungkin melihat penundaan hingga 30 menit untuk acara audit yang akan dikirim ke tujuan Anda. Hal ini disebabkan keterlambatan dalam peristiwa audit yang disediakan oleh aplikasi serta karena tindakan pencegahan yang diambil untuk mengurangi kehilangan data. Namun, ini mungkin dapat disesuaikan di tingkat akun. Untuk bantuan, hubungi AWS Support.

Menghubungkan AppFabric ke OneLogin by One Identity akun Anda

Setelah membuat bundel aplikasi dalam AppFabric layanan, Anda harus mengotorisasi AppFabric. OneLogin by One Identity Untuk menemukan informasi yang diperlukan untuk mengotorisasi OneLogin AppFabric, gunakan langkah-langkah berikut.

Buat aplikasi OAuth

AppFabric terintegrasi dengan OneLogin by One Identity menggunakan OAuth. Untuk membuat aplikasi OAuth diOneLogin, gunakan langkah-langkah berikut:

1. Arahkan ke halaman OneLogin login dan masuk.
2. Dari menu Developers, pilih API Credentials.
3. Pilih Kredensial Baru, masukkan nama untuk kredensi baru Anda, lalu pilih Baca semua.
4. Pilih Simpan. OneLoginmembuat ID klien dan rahasia klien.

Lingkup yang dibutuhkan

Anda harus menambahkan cakupan berikut ke aplikasi OneLogin by One Identity OAuth Anda:

- Baca semua. Untuk informasi selengkapnya tentang cakupan dan kredensional klien, lihat Bekerja dengan Kredensial API di Referensi API. OneLogin

Otorisasi aplikasi

ID Penyewa

AppFabric akan meminta ID penyewa. ID penyewa di AppFabric adalah subdomain instance Anda. Anda dapat menemukan ID penyewa Anda di bilah alamat browser Anda. Misalnya, `subdomain` adalah ID penyewa di URL `https://subdomain.onelogin.com` berikut.

Nama penyewa

Masukkan nama yang mengidentifikasi OneLogin by One Identity organisasi unik ini. AppFabric menggunakan nama penyewa untuk memberi label pada otorisasi aplikasi dan konsumsi apa pun yang dibuat dari otorisasi aplikasi.

ID Klien

AppFabric akan meminta ID klien. Untuk menemukan ID klien AndaOneLogin by One Identity, gunakan langkah-langkah berikut:

1. Arahkan ke halaman OneLogin login dan masuk.
2. Dari menu Developers, pilih API Credentials.
3. Pilih kredensi API untuk mendapatkan ID Klien.

Rahasia klien

AppFabric akan meminta rahasia klien. Untuk menemukan rahasia klien AndaOneLogin by One Identity, gunakan langkah-langkah berikut:

1. Arahkan ke halaman OneLogin login dan masuk.
2. Dari menu Developers, pilih API Credentials.
3. Pilih kredensi API untuk mendapatkan Rahasia Klien.

Otorisasi aplikasi klien

Di AppFabric, buat otorisasi aplikasi menggunakan ID dan nama penyewa, serta ID dan nama klien Anda. Pilih sambungkan untuk mengaktifkan otorisasi.

PagerDuty

PagerDutyadalah Platform Manajemen Operasi Digital yang membantu tim mengurangi masalah yang berdampak pada pelanggan dengan mengubah sinyal apa pun menjadi tindakan sehingga Anda dapat menyelesaikan masalah lebih cepat dan beroperasi lebih efisien. Terintegrasi denganCloudWatch,, GuardDutyCloudTrail, danPersonal Health Dashboard. Anda dapat menggunakan keamanan AWS AppFabric untuk menerima log audit dan data pengguna dariPagerDuty, menormalkan data ke dalam format Open Cybersecurity Schema Framework (OCSF), dan mengeluarkan data ke bucket Amazon Simple Storage Service (Amazon S3) atau aliran Amazon Data Firehose.

Topik

AppFabric dukungan untuk PagerDuty

AppFabric mendukung penerimaan informasi pengguna dan log audit dariPagerDuty.

Prasyarat

Untuk digunakan AppFabric untuk mentransfer log audit dari PagerDuty tujuan yang didukung, Anda harus memenuhi persyaratan berikut:

- Untuk mengakses log audit, Anda harus memiliki rencana PagerDuty Bisnis atau Operasi Digital.
- Anda harus menjadi Admin Global atau pemilik akun PagerDuty akun.

Pertimbangan batas tarif

PagerDutymemberlakukan batas tarif pada PagerDuty API. Untuk informasi selengkapnya tentang batas tarif PagerDuty API, lihat Batas Tingkat API REST di Platform PagerDuty Pengembang. Jika kombinasi AppFabric dan aplikasi PagerDuty API Anda yang ada melebihi PagerDuty batas, log audit yang muncul AppFabric mungkin tertunda.

Pertimbangan keterlambatan data

Anda mungkin melihat penundaan hingga 30 menit untuk acara audit yang akan dikirim ke tujuan Anda. Hal ini disebabkan keterlambatan dalam peristiwa audit yang disediakan oleh aplikasi serta

karena tindakan pencegahan yang diambil untuk mengurangi kehilangan data. Namun, ini mungkin dapat disesuaikan di tingkat akun. Untuk bantuan, hubungi AWS Support.

Menghubungkan AppFabric ke PagerDuty akun Anda

PagerDutyPlatform ini mendukung kunci akses API. Untuk membuat kunci akses API, gunakan langkah-langkah berikut.

Membuat Kunci Akses API

AppFabric terintegrasi dengan PagerDuty menggunakan kunci Akses API untuk klien publik. Untuk membuat kunci akses APIPagerDuty, gunakan langkah-langkah berikut:

1. Arahkan ke halaman PagerDuty login dan masuk.
2. Pilih Integrasi, Kunci Akses API.
3. Pilih Buat Kunci API Baru.
4. Masukkan deskripsi lalu pilih Kunci API hanya-baca.
5. Pilih Buat Kunci.
6. Salin dan simpan kunci API. Anda akan membutuhkan ini nanti AppFabric. Jika Anda menutup halaman sebelum menyimpan kunci API, Anda harus membuat kunci API baru dan menyimpannya. Kunci ini harus didedikasikan AppFabric untuk menghindari berbagi batas tarif PagerDuty API dengan integrasi Anda yang lain.

Otorisasi aplikasi

ID Penyewa

AppFabric akan meminta ID penyewa Anda. ID penyewa untuk PagerDuty akun Anda adalah URL dasar akun Anda. Anda dapat menemukannya dengan masuk PagerDuty dan menyalin dari bilah alamat browser web Anda. ID penyewa harus mengikuti salah satu format berikut:

- Untuk akun AS, `subdomain.pagerduty.com`
- Untuk akun UE, `subdomain.eu.pagerduty.com`

Nama penyewa

Masukkan nama yang mengidentifikasi PagerDuty organisasi unik ini. AppFabric menggunakan nama penyewa untuk memberi label pada otorisasi aplikasi dan konsumsi apa pun yang dibuat dari otorisasi aplikasi.

Token akun layanan

AppFabric akan meminta token akun layanan Anda. Token akun layanan di AppFabric adalah kunci akses API yang Anda buatMembuat Kunci Akses API.

Ping Identity

DiPing Identity, kami percaya dalam membuat pengalaman digital aman dan mulus untuk semua pengguna, tanpa kompromi. Itu sebabnya lebih dari setengah dari Fortune 100 memilih Ping Identity untuk melindungi interaksi digital bagi penggunanya sambil membuat pengalaman tanpa gesekan. Pada 23 Agustus 2023, Ping Identity dan ForgeRock bergabung bersama untuk memberikan lebih banyak pilihan, keahlian yang lebih dalam, dan solusi identitas yang lebih lengkap bagi pelanggan dan mitra. Anda dapat menggunakan keamanan AWS AppFabric untuk menerima log audit dan data pengguna dariPing Identity, menormalkan data ke dalam format Open Cybersecurity Schema Framework (OCSF), dan mengeluarkan data ke bucket Amazon Simple Storage Service (Amazon S3) atau aliran Amazon Data Firehose.

Topik

- AppFabric dukungan untuk Ping Identity
- Menghubungkan AppFabric ke Ping Identity akun Anda

AppFabric dukungan untuk Ping Identity

AppFabric mendukung penerimaan informasi pengguna dan log audit dariPing Identity.

Prasyarat

Untuk digunakan AppFabric untuk mentransfer log audit dari Ping Identity tujuan yang didukung, Anda harus memenuhi persyaratan berikut:

- Anda harus memiliki Ping Identity akun Essential, Plus, atau Premium. Untuk informasi selengkapnya tentang membuat atau meningkatkan ke jenis Ping Identity paket yang berlaku, lihat Ping Identityharga untuk semua fitur di Ping Identity situs web.
- Anda harus memiliki peran Hanya Baca Data Identitas di Ping Identity akun Anda. Anda dapat menambahkan peran ke akun Anda dengan memberikan peran untuk aplikasi Anda. Untuk informasi selengkapnya tentang peran, lihat Peran di situs web Ping Identity Support.

Pertimbangan batas tarif

Ping Identitytidak mempublikasikan batas tarif. Anda harus membuat kasus dukungan atau menjangkau tim Sukses Ping Identity Pelanggan Anda. Jika kombinasi AppFabric dan aplikasi Ping Identity API Anda yang ada melebihi Ping Identity batas, log audit yang muncul AppFabric mungkin tertunda.

Pertimbangan keterlambatan data

Anda mungkin melihat penundaan hingga 30 menit untuk acara audit yang akan dikirim ke tujuan Anda. Hal ini disebabkan keterlambatan dalam peristiwa audit yang disediakan oleh aplikasi serta karena tindakan pencegahan yang diambil untuk mengurangi kehilangan data. Namun, ini mungkin dapat disesuaikan di tingkat akun. Untuk bantuan, hubungi AWS Support.

Menghubungkan AppFabric ke Ping Identity akun Anda

Setelah Anda membuat app bundle dalam AppFabric layanan, Anda harus mengotorisasi AppFabric denganPing Identity. Untuk menemukan informasi yang diperlukan untuk mengotorisasi Ping Identity AppFabric, gunakan langkah-langkah berikut.

Buat aplikasi OAuth

AppFabric terintegrasi dengan Ping Identity menggunakan OAuth. Untuk membuat aplikasi OAuth diPing Identity, gunakan langkah-langkah berikut:

1. Ikuti petunjuk di bagian Buat koneksi aplikasi di panduan PingOneuntuk Pengembang di Ping Identity situs web.
2. Setelah Anda membuat aplikasi, sesuaikan jenis hibah.
   a. Saat masuk ke aplikasi, pilih tab Konfigurasi dan klik ikon pensil untuk membuat perubahan dalam konfigurasi yang ada.
   b. Di bawah Jenis Hibah, pilih Kode Otorisasi. Jaga Penegakan PKCE sebagai OPSIONAL.
   c. Pilih Refresh Token dan pilih durasi penyegaran Anda.
3. Gunakan URL pengalihan dengan format berikut di URL Redirect URL/Callback URL.

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   Di URL ini, <region>adalah kode untuk paket AppFabric aplikasi yang telah Anda konfigurasi. Wilayah AWS Misalnya, kode untuk Wilayah AS Timur (Virginia N.) adalah`us-east-1`. Untuk

Wilayah itu, URL pengalihan adalah`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

Otorisasi aplikasi

ID Penyewa

AppFabric akan meminta ID penyewa Anda. ID penyewa di AppFabric adalah nama Ping Identity instance Anda. Anda dapat menemukan ID penyewa Anda di bilah alamat browser Anda. Misalnya, `API_PATH/v1/environments/environmentID`. Dimana `API_PATH` mewakili domain regional untuk PingOne server, sepertiapi.pingone.com, dan `environmentID` mewakili ID lingkungan Anda yang ditunjukkan dalam properti lingkungan aplikasi Anda. Untuk informasi selengkapnya tentang properti lingkungan, lihat Properti Lingkungan di Ping Identity situs web.

Nama penyewa

Masukkan nama yang mengidentifikasi Ping Identity organisasi unik ini. AppFabric menggunakan nama penyewa untuk memberi label pada otorisasi aplikasi dan konsumsi apa pun yang dibuat dari otorisasi aplikasi.

ID Klien

AppFabric akan meminta ID klien. Untuk menemukan ID klien AndaPing Identity, gunakan langkah-langkah berikut:

1. Masuk ke konsol PingOne admin dan pilih Aplikasi.
2. Pilih aplikasi dari daftar.
3. Pilih tab Ikhtisar, lalu cari nilai ID Klien.

Rahasia klien

AppFabric akan meminta rahasia klien. Untuk menemukan rahasia klien AndaPing Identity, gunakan langkah-langkah berikut:

1. Masuk ke konsol PingOne admin dan pilih Aplikasi.
2. Pilih aplikasi dari daftar.
3. Pilih tab Ikhtisar, lalu cari nilai Rahasia Klien.

Menyetujui otorisasi

Setelah membuat otorisasi aplikasi di AppFabric, Anda akan menerima jendela pop-up dari Ping Identity untuk menyetujui otorisasi. Untuk menyetujui AppFabric otorisasi, pilih izinkan.

Salesforce

Salesforcemembuat perangkat lunak berbasis cloud yang dirancang untuk membantu bisnis menemukan lebih banyak prospek, menutup lebih banyak penawaran, dan memukau pelanggan dengan layanan luar biasa. Salesforce's Customer 360 menawarkan rangkaian lengkap produk, menyatukan tim penjualan, layanan, pemasaran, perdagangan, dan TI dengan satu pandangan bersama tentang informasi pelanggan, membantu organisasi menumbuhkan hubungan dengan pelanggan dan karyawan. Anda dapat menggunakannya AWS AppFabric untuk menerima log audit dan data pengguna dariSalesforce, menormalkan data ke dalam format Open Cybersecurity Schema Framework (OCSF), dan menampilkan data ke bucket Amazon Simple Storage Service (Amazon S3) atau aliran Amazon Data Firehose.

Topik

AppFabric dukungan untuk Salesforce

AppFabric mendukung penerimaan informasi pengguna dan log audit dariSalesforce.

Prasyarat

Untuk digunakan AppFabric untuk mentransfer log audit dari Salesforce tujuan yang didukung, Anda harus memenuhi persyaratan berikut:

- Anda harus memiliki edisi Kinerja, Perusahaan, atau Tidak TerbatasSalesforce. Hubungi Salesforce untuk meningkatkan ke salah satu edisi ini.
- Jika Anda ingin AppFabric mentransfer file log peristiwa per jam dengan set lengkap peristiwa log dariSalesforce, Anda harus berlangganan Event Monitoring sebagai bagian dari SalesforceFitur Shield. Jika tidak, AppFabric akan mentransfer peristiwa terbatas (yaitu Login, Logout, InsecureExternalAssets, Penggunaan API Total, CORS Pelanggaran, dan HostnameRedirects ELF Acara) dari file log harian Salesforce's standar. Anda dapat memeriksa apakah Salesforce akun Anda sudah berlangganan Fitur Shield dengan masuk ke Setup > Event Manager. Jika Anda melihat 19 acara atau lebih terdaftar, akun Anda akan berlangganan Pemantauan Acara.

Jika Anda tidak memiliki Pemantauan Acara, Anda dapat membeli langganan add-on ini dengan menghubungiSalesforce.

- Anda harus ikut serta untuk pembuatan File Log Peristiwa di Salesforce pengaturan.
- Anda harus menggunakan Profil Administrator Sistem untuk membuat OAuth aplikasi dan masuk dengan kredensi yang sama untuk. AppFabric

> **Note**
>
> APITotal Penggunaan, Catatan CORS Pelanggaran, Pengalihan Nama Host, Aset Eksternal Tidak Aman, Login, dan Logout tersedia tanpa biaya tambahan dalam edisi yang didukung. Salesforce Hubungi Salesforce untuk membeli jenis acara yang tersisa. Untuk informasi selengkapnya tentang jenis Salesforce acara, lihat Jenis Peristiwa yang EventLogFile Didukung di Salesforce situs web.
>
> AppFabric dapat mendukung hingga 100.000 peristiwa per jenis acara per instance file log (harian atau per jam, tergantung pada langganan add-on Pemantauan Acara). File log yang melebihi ambang batas dapat menyebabkan seluruh file log dikecualikan dari konsumsi.

Pertimbangan batas tarif

Salesforcememberlakukan batas tarif pada. Salesforce API Untuk informasi selengkapnya tentang batas Salesforce API tarif, lihat APIBatas Permintaan dan Alokasi di Salesforce situs web. Jika kombinasi AppFabric dan Salesforce API aplikasi Anda yang ada melebihi Salesforce’s batas, log audit yang muncul AppFabric mungkin tertunda.

Pertimbangan keterlambatan data

Anda mungkin melihat penundaan hingga 6 jam pada file log harian atau penundaan hingga 29 jam pada file log per jam untuk acara audit yang akan dikirim ke tujuan Anda. Hal ini disebabkan keterlambatan dalam peristiwa audit yang disediakan oleh aplikasi serta karena tindakan pencegahan yang diambil untuk mengurangi kehilangan data. Namun, ini mungkin dapat disesuaikan di tingkat akun. Untuk bantuan, hubungi AWS Support.

Menghubungkan AppFabric ke Salesforce akun Anda

Setelah membuat bundel aplikasi dalam AppFabric layanan, Anda harus mengotorisasi AppFabric. Salesforce Untuk menemukan informasi yang diperlukan untuk mengotorisasi Salesforce AppFabric, gunakan langkah-langkah berikut.

Buat OAuth aplikasi

AppFabric terintegrasi dengan Salesforce penggunaanOAuth. Untuk membuat OAuth aplikasiSalesforce, gunakan langkah-langkah berikut:

1. Masuk ke Salesforce akun Anda.
2. Buka halaman Setup seperti yang dijelaskan dalam Salesforcedokumentasi.
3. Cari Manajer Aplikasi di pencarian cepat.
4. Pilih Aplikasi Terhubung Baru.
5. Masukkan informasi yang diperlukan ke dalam kolom formulir.
6. Pilih Aktifkan OAuth pengaturan.
7. Pastikan untuk mematikan opsi berikut:
   - Memerlukan Kunci Bukti untuk Ekstensi Pertukaran Kode (PKCE) Untuk Alur Otorisasi yang Didukung
   - Memerlukan rahasia untuk Aliran Server Web
   - Memerlukan rahasia untuk Refresh Token Flow
8. Masukkan URL dengan format berikut di kotak URL teks Callback, dan pilih Simpan perubahan.

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   Dalam hal iniURL, `<region>` adalah kode tempat Wilayah AWS Anda mengonfigurasi bundel AppFabric aplikasi. Misalnya, kode untuk Wilayah AS Timur (Virginia N.) adalah`us-east-1`. Untuk Wilayah itu, pengalihannya URL adalah`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.
9. Isi cakupan sesuai kebutuhan (dijelaskan di Lingkup yang dibutuhkan bagian berikut). Semua bidang lainnya dapat dibiarkan dengan nilai defaultnya.
10. Pilih Simpan.
11. Selesaikan langkah-langkah berikut untuk memverifikasi kebijakan refresh token untuk OAuth aplikasi baru:
    a. Pada halaman Pengaturan, masukkan Aplikasi Terhubung ke dalam kotak teks Pencarian Cepat, lalu pilih Kelola Aplikasi Terhubung.
    b. Pilih Edit di samping aplikasi yang baru dibuat.
    c. Pastikan bahwa token Refresh valid hingga opsi yang dicabut dipilih.

   d. Simpan perubahan Anda.
12. Selesaikan langkah-langkah berikut untuk memverifikasi bahwa log audit sedang dibuat:
    a. Pada halaman Pengaturan, masukkan File Log Peristiwa ke dalam kotak teks Pencarian Cepat, lalu pilih Peramban File Log Peristiwa.
    b. Konfirmasikan bahwa log peristiwa tercantum di Browser File Log Peristiwa.
13. Arahkan ke aplikasi yang dibuat, dan pilih Lihat dari drop-down.
14. Pilih Kelola Detail Konsumen.

    Anda akan diarahkan ke tab baru di mana Anda perlu memverifikasi identitas Anda. Pada tab itu, catat nilai Consumer Key dan Consumer Secret. Anda akan membutuhkannya nanti untuk masuk.

Lingkup yang dibutuhkan

Anda harus menambahkan cakupan berikut ke Salesforce OAuth aplikasi Anda:

- Mengelola data pengguna melalui APIs (`API`).
- Lakukan permintaan kapan saja (`refresh_tokendanoffline_access`).

Otorisasi aplikasi

ID Penyewa

AppFabric akan meminta ID penyewa Anda. ID penyewa di AppFabric adalah subdomain Domain Salesforce Saya. Anda dapat menemukan subdomain Domain Saya di bilah alamat browser Anda antara `https://` dan`.my.salesforce.com`.

Untuk menemukan Domain Salesforce Saya, gunakan petunjuk berikut dari Salesforce layar beranda.

1. Buka halaman Setup seperti yang dijelaskan dalam Salesforcedokumentasi.
2. Cari Pengaturan Perusahaan di pencarian cepat, dan pilih Domain Saya di hasilnya.

Nama penyewa

Masukkan nama yang mengidentifikasi Salesforce organisasi unik ini. AppFabric menggunakan nama penyewa untuk memberi label pada otorisasi aplikasi dan konsumsi apa pun yang dibuat dari otorisasi aplikasi.

ID Klien

AppFabric akan meminta ID klien. Untuk menemukan ID klien AndaSalesforce, gunakan langkah-langkah berikut:

1. Arahkan ke halaman Pengaturan.
2. Pilih Pengaturan, lalu pilih Manajer Aplikasi.
3. Pilih aplikasi yang dibuat, dan pilih Lihat dari menu tarik-turun.
4. Pilih Kelola Detail Konsumen. Anda akan dialihkan ke tab baru.
5. Verifikasi identitas Anda, lalu cari nilai Consumer Key.
6. Masukkan Consumer Key ke dalam kolom ID klien di AppFabric.

Rahasia klien

AppFabric akan meminta rahasia klien Anda. Rahasia Klien AppFabric adalah Rahasia Konsumen diSalesforce. Untuk menemukan Rahasia AndaSalesforce, gunakan langkah-langkah berikut:

1. Arahkan ke halaman Pengaturan.
2. Pilih Pengaturan, lalu pilih Manajer Aplikasi.
3. Pilih aplikasi yang dibuat, dan pilih Lihat dari menu tarik-turun.
4. Pilih Kelola Detail Konsumen. Anda akan dialihkan ke tab baru.
5. Verifikasi identitas Anda, lalu cari nilai Rahasia Konsumen.
6. Masukkan Rahasia Konsumen ke dalam bidang rahasia klien di AppFabric.

Menyetujui otorisasi

Setelah membuat otorisasi aplikasi di AppFabric, Anda akan menerima jendela pop-up dari Salesforce untuk menyetujui otorisasi. Di halaman persetujuan, pastikan untuk menggunakan Peran Administrator Salesforce Sistem atau Salesforce pengguna yang memiliki Lihat File Log Peristiwa dan izin pengguna yang API diaktifkan saat mengotorisasi. Pilih Izinkan untuk menyetujui AppFabric otorisasi.

ServiceNow

ServiceNowadalah penyedia layanan berbasis cloud terkemuka yang mengotomatiskan operasi TI perusahaan. ServiceNowITOM memberi perusahaan visibilitas dan kontrol lengkap atas seluruh

lingkungan TI mereka - termasuk infrastruktur virtual dan cloud. Ini menyederhanakan pemetaan layanan, pengiriman dan jaminan, mengkonsolidasikan layanan TI dan data infrastruktur ke dalam satu sistem catatan. Ini juga mengotomatiskan dan merampingkan proses utama - termasuk peristiwa, insiden, masalah, konfigurasi, dan manajemen perubahan. Anda dapat menggunakan keamanan AWS AppFabric untuk menerima log audit dan data pengguna dariServiceNow, menormalkan data ke dalam format Open Cybersecurity Schema Framework (OCSF), dan mengeluarkan data ke bucket Amazon Simple Storage Service (Amazon S3) atau aliran Amazon Data Firehose.

Topik

AppFabric dukungan untuk ServiceNow

AppFabric mendukung penerimaan informasi pengguna dan log audit dariServiceNow.

Prasyarat

Untuk digunakan AppFabric untuk mentransfer log audit dari ServiceNow tujuan yang didukung, Anda harus memenuhi persyaratan berikut:

- Anda dapat menggunakan AppFabric dengan jenis ServiceNow paket apa pun.
- Anda harus memiliki pengguna dengan peran Administrator di ServiceNow akun Anda.
- Anda harus memiliki ServiceNow contoh.

Pertimbangan batas tarif

ServiceNowmemberlakukan batas tarif pada ServiceNow API. Untuk informasi selengkapnya tentang batas tarif ServiceNow API, lihat Pembatasan tarif API REST masuk di ServiceNow situs web. Jika kombinasi AppFabric dan aplikasi ServiceNow API Anda yang ada melebihi batas, log audit yang muncul AppFabric mungkin tertunda.

Pertimbangan keterlambatan data

Anda mungkin melihat penundaan hingga 30 menit untuk acara audit yang akan dikirim ke tujuan Anda. Hal ini disebabkan keterlambatan dalam peristiwa audit yang disediakan oleh aplikasi serta

karena tindakan pencegahan yang diambil untuk mengurangi kehilangan data. Namun, ini mungkin dapat disesuaikan di tingkat akun. Untuk bantuan, hubungi AWS Support.

Menghubungkan AppFabric ke ServiceNow akun Anda

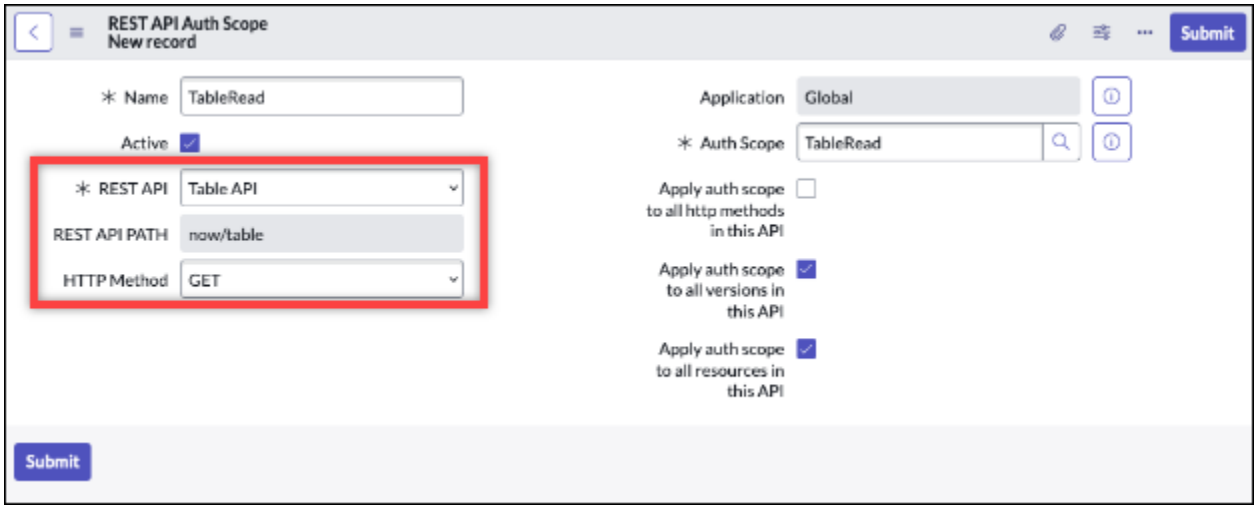
Setelah Anda membuat app bundle dalam AppFabric layanan, Anda harus mengotorisasi AppFabric denganServiceNow. Gunakan langkah-langkah berikut untuk menemukan informasi yang diperlukan untuk mengotorisasiServiceNow. AppFabric

Buat aplikasi OAuth

Now PlatformDukungan OAuth 2.0 - Jenis Hibah Otorisasi untuk klien publik untuk menghasilkan token akses.

1. Daftarkan aplikasi OAuth Anda. Ini membutuhkan tiga langkah berikut. Untuk informasi lebih lanjut tentang menyelesaikan langkah-langkah ini, lihat Daftarkan aplikasi Anda ServiceNow di ServiceNowsitus web.

   a. Daftarkan aplikasi dan pastikan Lingkup Auth memiliki akses ke API Tabel, dengan REST API PATH sekarang/tabel, dan Metode HTTP GET seperti yang ditunjukkan pada contoh berikut.



   b. Hasilkan kode otorisasi.

   c. Hasilkan token pembawa menggunakan kode otorisasi.

2. Gunakan URL pengalihan dengan format berikut.

```
https://<region>.console.aws.amazon.com/appfabric/oauth2
```

Di URL ini, <region>adalah kode Wilayah AWS tempat Anda mengonfigurasi bundel AppFabric aplikasi. Misalnya, kode untuk Wilayah AS Timur (Virginia N.) adalah`us-east-1`. Untuk Wilayah itu, URL pengalihan adalah`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

Otorisasi aplikasi

ID Penyewa

AppFabric akan meminta ID penyewa. ID penyewa di AppFabric adalah nama instance Anda. Anda dapat menemukan ID penyewa Anda di bilah alamat browser Anda. Misalnya, `example` adalah ID penyewa di URL `https://example.service-now.com` berikut.

Nama penyewa

Masukkan nama yang mengidentifikasi ServiceNow organisasi unik ini. AppFabric menggunakan nama penyewa untuk memberi label pada otorisasi aplikasi dan konsumsi apa pun yang dibuat dari otorisasi aplikasi.

ID Klien

AppFabric akan meminta ID klien. Gunakan langkah-langkah berikut untuk menemukan ID klien AndaServiceNow.

1. Arahkan ke ServiceNow konsol.
2. Pilih System OAuth, lalu pilih tab Application Registry.
3. Pilih aplikasi Anda.
4. Masukkan ID klien dari klien OAuth Anda ke bidang ID Klien di. AppFabric

Rahasia klien

AppFabric akan meminta rahasia klien. Gunakan langkah-langkah berikut untuk menemukan rahasia klien AndaServiceNow.

1. Arahkan ke ServiceNow konsol.
2. Pilih System OAuth, lalu pilih tab Application Registry.
3. Pilih aplikasi Anda.

4. Masukkan rahasia klien dari aplikasi OAuth Anda ke bidang Rahasia Klien di. AppFabric

Menyetujui otorisasi

Setelah membuat otorisasi aplikasi di AppFabric, Anda akan menerima jendela pop-up dari ServiceNow untuk menyetujui otorisasi. Pilih Izinkan untuk menyetujui AppFabric otorisasi.

Singularity Cloud

Singularity CloudPlatform ini melindungi perusahaan Anda dari ancaman semua kategori, di semua tahap. Kecerdasan buatannya yang dipatenkan memperluas keamanan dari tanda tangan dan pola yang diketahui hingga serangan paling canggih, seperti zero-day dan ransomware.

Anda dapat menggunakannya AWS AppFabric untuk menerima log audit dan data pengguna dariSingularity Cloud, menormalkan data ke dalam format Open Cybersecurity Schema Framework (OCSF), dan menampilkan data ke bucket Amazon Simple Storage Service (Amazon S3) atau aliran Amazon Data Firehose.

> **Note**
>
> Singularity Clouddokumentasi dapat diakses hanya setelah Anda masuk ke Singularity Cloud akun Anda. Oleh karena itu, kami tidak dapat menautkan langsung ke Singularity Cloud dokumentasi dari dokumen ini.

Topik

- AppFabric dukungan untuk Singularity Cloud
- Menghubungkan AppFabric ke Singularity Cloud akun Anda

AppFabric dukungan untuk Singularity Cloud

AppFabric mendukung penerimaan informasi pengguna dan log audit dariSingularity Cloud.

Prasyarat

Untuk digunakan AppFabric untuk mentransfer log audit dari Singularity Cloud tujuan yang didukung, Anda harus memiliki peran administrator di Singularity Cloud akun Anda. Untuk informasi

selengkapnya tentang batas tarif Singularity Cloud API, masuk ke akun Singularity Cloud Anda, telusuri bagian dokumentasi, dan cari peran.

Pertimbangan batas tarif

Singularity Cloudmemberlakukan batas tarif pada Singularity Cloud API. Untuk informasi selengkapnya tentang batas tarif Singularity Cloud API, masuk ke akun Singularity Cloud Anda, telusuri bagian dokumentasi, dan cari batas tarif API.

Pertimbangan keterlambatan data

Anda mungkin melihat penundaan hingga 30 menit acara audit untuk dikirim ke tujuan Anda. Hal ini disebabkan keterlambatan dalam peristiwa audit yang disediakan oleh aplikasi serta karena tindakan pencegahan yang diambil untuk mengurangi kehilangan data. Namun, ini mungkin dapat disesuaikan di tingkat akun. Untuk bantuan, hubungi AWS Support.

Menghubungkan AppFabric ke Singularity Cloud akun Anda

Setelah Anda membuat app bundle dalam AppFabric layanan, Anda harus mengotorisasi AppFabric denganSingularity Cloud. Untuk menemukan informasi yang diperlukan untuk mengotorisasi Singularity Cloud AppFabric, gunakan langkah-langkah berikut.

Buat token API untuk Singularity Cloud

Selesaikan prosedur berikut untuk membuat token API yang terkait dengan pengguna layanan. Token API tidak akan ditautkan ke pengguna konsol atau alamat email tertentu.

> **Note**
>
> Buat pengguna baru atau salin pengguna layanan untuk mendapatkan token API baru sebelum atau setelah token API pengguna layanan kedaluwarsa.

1. Masuk ke Singularity Cloud akun Anda.
2. Di bilah alat Pengaturan, pilih Pengguna, lalu pilih Pengguna Layanan.
3. Pilih Tindakan, lalu pilih Buat Pengguna Layanan Baru.
4. Di halaman Buat Pengguna Layanan Baru, masukkan nama, deskripsi, dan tanggal kedaluwarsa untuk pengguna layanan.

5. Pilih Selanjutnya.
6. Di bagian Select Scope of Access, pilih ruang lingkup.
   - Pilih Akun untuk tingkat akses.
   - Pilih akun yang ingin Anda dapatkan log audit.
7. Pilih Buat Pengguna.

   Token API dihasilkan. Sebuah jendela terbuka dan menampilkan string token dengan pesan yang menunjukkan ini adalah terakhir kalinya Anda dapat melihat token.
8. (Opsional) Pilih Salin Token API dan simpan di lokasi yang aman.
9. Pilih Tutup.

Otorisasi aplikasi

ID Penyewa

AppFabric akan meminta ID penyewa Anda. ID penyewa AppFabric akan menjadi subdomain dari alamat Sentinel One situs web tempat Anda masuk ke layanan. Misalnya, jika Anda masuk ke Singularity Cloud akun Anda di `example-company-1.sentinelone.net` alamat, ID penyewa Anda adalah`example-company-1`.

Nama penyewa

Masukkan nama yang mengidentifikasi Singularity Cloud organisasi unik ini. AppFabric menggunakan nama penyewa untuk memberi label pada otorisasi aplikasi dan konsumsi apa pun yang dibuat dari otorisasi aplikasi.

Token akun layanan

Gunakan token yang Anda buat menggunakan langkah-langkah di Buat token API untuk Singularity Cloud bagian panduan ini. Jika Anda salah tempat atau tidak dapat menemukan token, Anda dapat membuat yang baru dengan mengikuti langkah yang sama lagi.

> **Note**
>
> Jika token API baru dibuat di konsol Singularity Cloud saat AppFabric menelan log audit, konsumsi akan berhenti. Jika ini terjadi, Anda perlu memperbarui otorisasi aplikasi dengan token API baru untuk melanjutkan konsumsi log audit.

Slack

Slackadalah misi untuk membuat kehidupan kerja orang lebih sederhana, lebih menyenangkan, dan lebih produktif. Ini adalah platform produktivitas untuk perusahaan pelanggan yang meningkatkan kinerja dengan memberdayakan semua orang dengan otomatisasi tanpa kode, membuat pencarian dan berbagi pengetahuan mulus, dan menjaga tim tetap terhubung dan terlibat saat mereka bergerak maju bersama. Sebagai bagian dariSalesforce, terintegrasi Slack secara mendalam ke dalam Salesforce Customer 360, meningkatkan produktivitas di seluruh tim penjualan, layanan, dan pemasaran. Untuk mempelajari lebih lanjut dan memulai dengan Slack gratis, kunjungi slack.com.

Anda dapat menggunakan keamanan AWS AppFabric untuk menerima log audit dan data pengguna dariSlack, menormalkan data ke dalam format Open Cybersecurity Schema Framework (OCSF), dan mengeluarkan data ke bucket Amazon Simple Storage Service (Amazon S3) atau aliran Amazon Data Firehose.

Topik

AppFabric dukungan untuk Slack

AppFabric mendukung penerimaan informasi pengguna dan log audit dariSlack.

Prasyarat

Untuk digunakan AppFabric untuk mentransfer log audit dari Slack tujuan yang didukung, Anda harus memenuhi persyaratan berikut:

- Anda harus memiliki paket Enterprise Grid denganSlack. Untuk informasi selengkapnya, lihat Pengantar Slack Enterprise Grid di Slack situs web.
- Anda harus memiliki pengguna dengan peran Pemilik Org di Slack akun Anda. Untuk informasi selengkapnya tentang peran, lihat Jenis peran Slack di Pusat Slack Bantuan di Slack situs web.

Pertimbangan batas tarif

Slackmemberlakukan batas tarif pada Slack API. Untuk informasi selengkapnya tentang batas tarif Slack API, lihat Batas tarif di Panduan Penggunaan Slack API di Slack situs web. Jika kombinasi

AppFabric dan aplikasi Slack API Anda yang ada melebihi batas, log audit yang muncul AppFabric mungkin tertunda.

Pertimbangan keterlambatan data

Anda mungkin melihat penundaan hingga 30 menit untuk acara audit yang akan dikirim ke tujuan Anda. Hal ini disebabkan keterlambatan dalam peristiwa audit yang disediakan oleh aplikasi serta karena tindakan pencegahan yang diambil untuk mengurangi kehilangan data. Namun, ini mungkin dapat disesuaikan di tingkat akun. Untuk bantuan, hubungi AWS Support.

Menghubungkan AppFabric ke Slack akun Anda

Setelah Anda membuat app bundle dalam AppFabric layanan, Anda harus mengotorisasi AppFabric denganSlack. Untuk menemukan informasi yang diperlukan untuk mengotorisasi Slack AppFabric, gunakan langkah-langkah berikut.

Buat aplikasi OAuth

AppFabric terintegrasi dengan Slack menggunakan OAuth. Ada dua cara untuk membuat aplikasi OAuth: Menggunakan manifes aplikasi atau Dari awal. Untuk membuat aplikasi OAuth diSlack, gunakan langkah-langkah berikut.

Using an app manifest

1. Arahkan ke UI Manajemen Slack Aplikasi di browser Anda.
2. Pilih Buat Aplikasi Baru.
3. Pilih Dari manifes aplikasi.
4. Pilih ruang kerja yang ingin Anda otorisasi AppFabric.
5. Di kotak Masukkan manifes aplikasi di bawah ini, pilih JSON dan ganti JSON yang ada dengan yang berikut ini. Ganti <region>dengan yang sesuai Wilayah AWS (misalnya, *us-east-1*).

```
{
    "display_information": {
        "name": "AppFabric"
    },
    "oauth_config": {
        "redirect_urls": [
            "https://<region>.console.aws.amazon.com/appfabric/oauth2"
```

```
        ],
        "scopes": {
            "user": [
                "auditlogs:read",
                "users:read.email",
                "users:read"
            ]
        }
    },
    "settings": {
        "org_deploy_enabled": false,
        "socket_mode_enabled": false,
        "token_rotation_enabled": true
    }
}
```

6. Salin dan simpan ID klien dan rahasia klien dari halaman Informasi Dasar.
7. Untuk `auditLogs:read` cakupannya, Anda harus mengaktifkan distribusi publik aplikasi Anda. Untuk informasi selengkapnya, lihat Mengaktifkan distribusi publik di situs web Slack.

From scratch

1. Pilih Dari awal di layar Buat aplikasi.
2. Beri nama aplikasi Anda dan pilih ruang kerja.
3. Salin dan simpan ID klien dan rahasia klien dari halaman Informasi Dasar.
4. Pada halaman OAuth & Permissions, pilih opsi Advanced token security via token rotation.
5. Tambahkan URL dengan format berikut di bagian URL Pengalihan pada halaman OAuth & Izin.

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   Di URL ini, *<region>* adalah kode untuk paket AppFabric aplikasi yang telah Anda konfigurasi. Wilayah AWS Misalnya, kode untuk Wilayah AS Timur (Virginia N.) adalah`us-east-1`. Untuk Wilayah itu, URL pengalihan adalah`https://`*us-east-1*`.console.aws.amazon.com/appfabric/oauth2`.
6. Untuk `auditLogs:read` cakupannya, Anda harus mengaktifkan distribusi publik aplikasi Anda. Untuk informasi selengkapnya, lihat Mengaktifkan distribusi publik di situs web Slack.

Cakupan yang dibutuhkan

> **Note**
>
> Bagian ini hanya berlaku jika Anda memilih untuk membuat aplikasi OAuth dari awal. Lewati bagian ini jika Anda memilih untuk menggunakan manifes aplikasi untuk membuat otorisasi aplikasi.

Anda harus menambahkan cakupan token pengguna berikut di halaman OAuth & Izin aplikasi OAuth Anda: Slack

- `auditlogs:read`
- `users:read.email`
- `users:read`

Otorisasi aplikasi

ID Penyewa

AppFabric akan meminta ID penyewa Anda. ID penyewa di AppFabric adalah ID Slack ruang kerja Anda. Untuk mendapatkan ID penyewa Anda, ikuti petunjuk di Temukan Slack URL Anda di Pusat Slack Bantuan di Slack situs web. URL Slack ruang kerja Anda memiliki format yang mirip dengan `examplecorp.slack.com` atau`examplecorp.enterprise.slack.com`. ID penyewa yang Anda butuhkan adalah `examplecorp` tanpa `.slack.com` atau`.enterprise.slack.com`.

Nama penyewa

Masukkan nama yang mengidentifikasi ID Slack ruang kerja Anda. AppFabricmenggunakan nama penyewa untuk memberi label pada otorisasi aplikasi dan konsumsi apa pun yang dibuat dari otorisasi aplikasi

ID Klien

AppFabric akan meminta ID klien dari aplikasi Slack OAuth Anda. Untuk menemukan ID klien, gunakan langkah-langkah berikut:

1. Arahkan ke UI Manajemen Slack Aplikasi di browser Anda.

2. Pilih aplikasi OAuth yang Anda gunakan. AppFabric
3. Masukkan ID klien dari halaman Informasi Dasar ke bidang ID Klien di AppFabric.

Rahasia klien

AppFabric akan meminta rahasia klien dari aplikasi Slack OAuth Anda. Untuk menemukan rahasia klien, gunakan langkah-langkah berikut:

1. Arahkan ke UI Manajemen Slack Aplikasi di browser Anda.
2. Pilih aplikasi OAuth yang Anda gunakan. AppFabric
3. Masukkan rahasia klien dari halaman Informasi Dasar ke bidang rahasia Klien di AppFabric.

Menyetujui otorisasi

Setelah membuat otorisasi aplikasi di AppFabric, Anda akan menerima jendela pop-up dari Slack untuk menyetujui otorisasi. Untuk menyetujui AppFabric otorisasi, pilih izinkan.

Smartsheet

Smartsheetadalah platform manajemen kerja yang membantu Anda menyelaraskan pekerjaan, orang, dan teknologi di seluruh perusahaan Anda. Smartsheetmenawarkan serangkaian kemampuan tingkat perusahaan yang kuat untuk memberdayakan semua orang untuk mengelola proyek, mengotomatiskan alur kerja, dan dengan cepat membangun solusi dalam skala besar, menciptakan lingkungan untuk inovasi sambil menjaga keamanan dan kepatuhan.

Anda dapat menggunakan keamanan AWS AppFabric untuk menerima log audit dan data pengguna dariSmartsheet, menormalkan data ke dalam format Open Cybersecurity Schema Framework (OCSF), dan mengeluarkan data ke bucket Amazon Simple Storage Service (Amazon S3) atau aliran Amazon Data Firehose.

Topik

- AppFabric dukungan untuk Smartsheet
- Menghubungkan AppFabric ke Smartsheet akun Anda

AppFabric dukungan untuk Smartsheet

AppFabric mendukung penerimaan informasi pengguna dan log audit dariSmartsheet.

Prasyarat

Untuk digunakan AppFabric untuk mentransfer log audit dari Smartsheet tujuan yang didukung, Anda harus memenuhi persyaratan berikut:

- Anda harus memiliki akun Smartsheet Business, Enterprise, atau Advance. Untuk informasi selengkapnya tentang membuat atau meningkatkan Smartsheet akun Anda, lihat Smartsheetharga atau SmartsheetAdvance di Smartsheet situs web.
- Anda harus menyelesaikan proses pendaftaran Smartsheet pengembang.

Pertimbangan batas tarif

Smartsheetmemberlakukan batas tarif pada Smartsheet API. Untuk informasi selengkapnya tentang batas tarif Smartsheet API, lihat Pembatasan tarif di Referensi API Smartsheet di situs web Smartsheet.

Pertimbangan keterlambatan data

Anda mungkin melihat penundaan hingga 30 menit untuk acara audit yang akan dikirim ke tujuan Anda. Hal ini disebabkan keterlambatan dalam peristiwa audit yang disediakan oleh aplikasi serta karena tindakan pencegahan yang diambil untuk mengurangi kehilangan data. Namun, ini mungkin dapat disesuaikan di tingkat akun. Untuk bantuan, hubungi AWS Support.

Menghubungkan AppFabric ke Smartsheet akun Anda

Setelah Anda membuat app bundle dalam AppFabric layanan, Anda harus mengotorisasi AppFabric denganSmartsheet. Untuk menemukan informasi yang diperlukan untuk mengotorisasi Smartsheet AppFabric, gunakan langkah-langkah berikut.

Buat aplikasi OAuth

AppFabric terintegrasi dengan Smartsheet menggunakan OAuth. Untuk membuat aplikasi OAuth diSmartsheet, gunakan langkah-langkah berikut:

1. Arahkan ke alat pengembang di Smartsheet akun Anda.
2. Pilih Buat Aplikasi Baru dari layar alat pengembang.
3. Lengkapi semua kolom input di layar Create New App.
4. Gunakan nilai unik apa pun untuk URL Aplikasi dan Kontak/Dukungan Aplikasi.

5. Gunakan URL pengalihan dengan format berikut sebagai URL pengalihan Aplikasi.

```
https://<region>.console.aws.amazon.com/appfabric/oauth2
```

   Di URL ini, `<region>` adalah kode untuk paket AppFabric aplikasi yang telah Anda konfigurasi. Wilayah AWS Misalnya, kode untuk Wilayah AS Timur (Virginia N.) adalah`us-east-1`. Untuk Wilayah itu, URL pengalihan adalah`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

6. Pilih Simpan.
7. Salin dan simpan ID klien aplikasi dan rahasia aplikasi.

Lingkup yang dibutuhkan

Smartsheettidak mengharuskan Anda untuk secara eksplisit menambahkan cakupan ke konfigurasi OAuth Anda. AppFabric akan meminta cakupan berikut dalam permintaan otorisasi ke akun AndaSmartsheet:

- `READ_EVENTS`
- `READ_USERS`

Otorisasi aplikasi

ID Penyewa

AppFabric akan meminta ID penyewa Anda. ID penyewa di AppFabric adalah ID Smartsheet akun Anda.

Nama penyewa

AppFabric akan meminta ID penyewa Anda. Masukkan nilai apa pun yang secara unik mengidentifikasi akun Anda. Smartsheet

ID Klien

AppFabric akan meminta ID klien Anda. ID klien di AppFabric adalah ID klien Smartsheet aplikasi Anda. Untuk menemukan ID klien aplikasi AndaSmartsheet, gunakan langkah-langkah berikut:

1. Arahkan ke alat pengembang di Smartsheet akun Anda.

2. Pilih aplikasi OAuth yang Anda gunakan untuk terhubung. AppFabric
3. Masukkan ID klien aplikasi dari layar Profil Aplikasi ke bidang ID Klien di AppFabric.

Rahasia klien

AppFabric akan meminta rahasia klien Anda. Rahasia klien AppFabric adalah rahasia Smartsheet aplikasi Anda. Untuk menemukan rahasia aplikasi AndaSmartsheet, gunakan langkah-langkah berikut:

1. Arahkan ke alat pengembang di Smartsheet akun Anda.
2. Pilih aplikasi OAuth yang Anda gunakan untuk terhubung. AppFabric
3. Masukkan rahasia aplikasi dari layar Profil Aplikasi ke bidang Rahasia Klien di AppFabric.

Menyetujui otorisasi

Setelah membuat otorisasi aplikasi di AppFabric, Anda akan menerima jendela pop-up dari Smartsheet untuk menyetujui otorisasi. Untuk menyetujui AppFabric otorisasi, pilih Izinkan.

Terraform Cloud

HashiCorp Terraform Cloudadalah produk penyediaan multi-cloud yang paling banyak digunakan di dunia. TerraformEkosistem ini memiliki lebih dari 3.000 penyedia, 14.000 modul, dan 250 juta unduhan. Terraform Cloudadalah cara tercepat untuk mengadopsiTerraform, menyediakan segala yang dibutuhkan praktisi, tim, dan bisnis global untuk menciptakan dan berkolaborasi dalam infrastruktur dan mengelola risiko untuk keamanan, kepatuhan, dan kendala operasional. Anda dapat menggunakan keamanan AWS AppFabric untuk menerima log audit dan data pengguna dariTerraform Cloud, menormalkan data ke dalam format Open Cybersecurity Schema Framework (OCSF), dan mengeluarkan data ke bucket Amazon Simple Storage Service (Amazon S3) atau aliran Amazon Data Firehose.

Topik

AppFabric dukungan untuk Terraform Cloud

AppFabric mendukung penerimaan informasi pengguna dan log audit dariTerraform Cloud.

Prasyarat

Untuk digunakan AppFabric untuk mentransfer log audit dari Terraform Cloud tujuan yang didukung, Anda harus memenuhi persyaratan berikut:

- Untuk mengakses log audit, Anda harus memiliki rencana Edisi Terraform Cloud Plus dan menjadi pemilik organisasi. Untuk informasi selengkapnya tentang Terraform Cloud paket, lihat Terraformharga di HashiCorp Terraform situs web.
- Log Audit TBD tersedia untuk organisasi yang dapat dibuat dari Terraform Cloud akun.

Pertimbangan batas tarif

Terraform Cloudmemberlakukan batas tarif pada Terraform Cloud API. Untuk informasi selengkapnya tentang batas tarif Terraform Cloud API, lihat Pembatasan Tingkat API di setelan umum administrasi Terraform Cloud Developer di Terraform Cloud situs web. Jika kombinasi AppFabric dan aplikasi Terraform Cloud API Anda yang ada melebihi Terraform Cloud batas, log audit yang muncul AppFabric mungkin tertunda.

Pertimbangan keterlambatan data

Anda mungkin melihat penundaan hingga 30 menit untuk acara audit yang akan dikirim ke tujuan Anda. Hal ini disebabkan keterlambatan dalam peristiwa audit yang disediakan oleh aplikasi serta karena tindakan pencegahan yang diambil untuk mengurangi kehilangan data. Namun, ini mungkin dapat disesuaikan di tingkat akun. Untuk bantuan, hubungi AWS Support.

Menghubungkan AppFabric ke Terraform Cloud akun Anda

Setelah Anda membuat app bundle dalam AppFabric layanan, Anda harus mengotorisasi AppFabric denganTerraform Cloud. Untuk menemukan informasi yang diperlukan untuk mengotorisasi Terraform Cloud AppFabric, gunakan langkah-langkah berikut.

Buat token API organisasi

AppFabric terintegrasi dengan Terraform Cloud menggunakan token API organisasi. Untuk informasi selengkapnya tentang token API Terraform Cloud organisasi, lihat Token API Organisasi. Untuk membuat organisasi, ikuti instruksi di Creating Organizations. Untuk membuat token API organisasiTerraform Cloud, gunakan langkah-langkah berikut.

1. Arahkan ke halaman Terraform Cloudmasuk dan masuk.
2. Pilih Organisasi, Pengaturan di panel sisi kiri, lalu pilih token API.

3. Di bawah Token Organisasi, pilih Buat token organisasi, lalu pilih Hasilkan token.
4. (Opsional) Masukkan tanggal atau waktu kedaluwarsa token, atau buat token yang tidak pernah kedaluwarsa.
5. Salin dan simpan token. Anda akan membutuhkan ini nanti AppFabric. Jika Anda menutup halaman sebelum menyimpan token, Anda harus mencabut token lama dan membuat yang baru.

Otorisasi aplikasi

ID Penyewa

AppFabric akan meminta ID penyewa. ID penyewa untuk Terraform Cloud akun Anda adalah URL organisasi akun Anda saat ini. Anda dapat menemukannya dengan masuk ke Terraform Cloud organisasi Anda dan menyalin URL organisasi saat ini. ID penyewa harus mengikuti salah satu format berikut:

```
https://app.terraform.io/app/organization_URL
```

Nama penyewa

Masukkan nama yang mengidentifikasi Terraform Cloud organisasi unik ini. AppFabric menggunakan nama penyewa untuk memberi label pada otorisasi aplikasi dan konsumsi apa pun yang dibuat dari otorisasi aplikasi.

Token akun layanan

AppFabric akan meminta token akun layanan Anda. Token akun layanan di AppFabric adalah token API organisasi yang Anda buatBuat token API organisasi.

Webex by Cisco

Ciscoadalah pemimpin dunia dalam teknologi yang menggerakkan Internet. CiscoMenginspirasi kemungkinan baru dengan menata ulang aplikasi Anda, mengamankan data Anda, mengubah infrastruktur Anda, dan memberdayakan tim Anda untuk masa depan yang global dan inklusif.

Tentang Webex by Cisco

Webexadalah penyedia terkemuka solusi kolaborasi berbasis cloud yang mencakup rapat video, panggilan, pesan, acara, solusi pengalaman pelanggan seperti pusat kontak dan perangkat kolaborasi yang dibuat khusus. WebexFokus dalam memberikan pengalaman kolaborasi inklusif

mendorong inovasi, yang memanfaatkan AI dan Machine Learning, untuk menghilangkan hambatan geografi, bahasa, kepribadian, dan keakraban dengan teknologi. Solusinya didukung dengan keamanan dan privasi berdasarkan desain. Webexbekerja dengan aplikasi bisnis dan produktivitas terkemuka di dunia — disampaikan melalui satu aplikasi dan antarmuka. Pelajari lebih lanjut di webex.com.

Anda dapat menggunakan keamanan AWS AppFabric untuk menerima log audit dan data pengguna dariWebex, menormalkan data ke dalam format Open Cybersecurity Schema Framework (OCSF), dan mengeluarkan data ke bucket Amazon Simple Storage Service (Amazon S3) atau aliran Amazon Data Firehose.

Topik

AppFabric dukungan untuk Webex

AppFabric mendukung penerimaan informasi pengguna dan log audit dariWebex.

Prasyarat

Untuk digunakan AppFabric untuk mentransfer log audit dari Webex tujuan yang didukung, Anda harus memenuhi persyaratan berikut:

- Anda harus memiliki paket Collaboration Flex, Meet Plan, Call Plan, atau yang lebih tinggi. Untuk informasi selengkapnya tentang membuat atau meningkatkan ke jenis Webex paket yang berlaku, lihat Webexharga untuk semua fitur di Webex situs web.
- Akun Anda harus memiliki lisensi Pro Pack untuk mengakses Acara Audit Keamanan yang disediakan oleh salah satu AuditLog API Cisco.
- Anda harus memiliki pengguna dengan peran Administrator Organisasi > Administrator Lengkap.
- Konfigurasi Peran Administrator untuk Administrator Penuh Anda harus mengaktifkan opsi Petugas Kepatuhan.

Pertimbangan batas tarif

Webexmemberlakukan batas tarif pada Webex API. Untuk informasi selengkapnya tentang batas tarif Webex API, lihat Batas tarif di Panduan Webex Pengembang di Webex situs web. Jika kombinasi

AppFabric dan aplikasi Webex API Anda yang ada melebihi batas, log audit yang muncul AppFabric mungkin tertunda.

Pertimbangan keterlambatan data

Anda mungkin melihat penundaan hingga 30 menit untuk acara audit yang akan dikirim ke tujuan Anda. Hal ini disebabkan keterlambatan dalam peristiwa audit yang disediakan oleh aplikasi serta karena tindakan pencegahan yang diambil untuk mengurangi kehilangan data. Namun, ini mungkin dapat disesuaikan di tingkat akun. Untuk bantuan, hubungi AWS Support.

Menghubungkan AppFabric ke Webex akun Anda

Setelah membuat bundel aplikasi dalam AppFabric layanan, Anda harus mengotorisasi AppFabric. Webex Untuk menemukan informasi yang diperlukan untuk mengotorisasi Webex AppFabric, gunakan langkah-langkah berikut.

Buat aplikasi OAuth

AppFabric terintegrasi dengan Webex menggunakan OAuth. Untuk membuat aplikasi OAuth diWebex, gunakan langkah-langkah berikut:

1. Ikuti petunjuk di bagian Mendaftarkan Integrasi Anda di halaman Integrasi & Otorisasi Panduan WebexPengembang.
2. Gunakan URL pengalihan dengan format berikut.

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   Di URL ini, `<region>` adalah kode untuk paket AppFabric aplikasi yang telah Anda konfigurasi. Wilayah AWS Misalnya, kode untuk Wilayah AS Timur (Virginia N.) adalah`us-east-1`. Untuk Wilayah itu, URL pengalihan adalah`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

Lingkup yang dibutuhkan

Anda harus menambahkan cakupan berikut ke aplikasi Webex OAuth Anda:

- `spark-compliance:events_read`
- `audit:events_read`
- `spark-admin:people_read`

Otorisasi aplikasi

ID Penyewa

AppFabric akan meminta ID penyewa Anda. ID penyewa di AppFabric adalah ID Webex organisasi Anda. Untuk informasi tentang cara menemukan ID Webex organisasi, lihat Cari ID Organisasi Anda di CiscoWebex Control Hub di situs web Pusat Webex Bantuan.

Nama penyewa

Masukkan nama yang mengidentifikasi Webex instance unik ini. AppFabricmenggunakan nama penyewa untuk memberi label pada otorisasi aplikasi dan konsumsi apa pun yang dibuat dari otorisasi aplikasi.

ID Klien

AppFabric akan meminta ID Webex klien Anda. Untuk menemukan ID Webex klien Anda, gunakan langkah-langkah berikut:

1. Masuk ke Webex akun Anda di https://developer.webex.com.
2. Pilih avatar Anda di kanan atas.
3. Pilih Aplikasi Webex Saya.
4. Pilih aplikasi OAuth2 yang Anda gunakan untuk. AppFabric
5. Masukkan ID klien pada halaman ini ke dalam kolom ID Klien di AppFabric.

Rahasia klien

AppFabric akan meminta rahasia Webex klien Anda. Webexhanya menyajikan rahasia klien Anda sekali ketika Anda awalnya membuat aplikasi OAuth Anda. Untuk menghasilkan rahasia klien baru jika Anda tidak menyimpan rahasia klien awal, gunakan langkah-langkah berikut:

1. Masuk ke Webex akun Anda di https://developer.webex.com.
2. Pilih avatar Anda di kanan atas.
3. Pilih Aplikasi Webex Saya.
4. Pilih aplikasi OAuth2 yang Anda gunakan untuk. AppFabric
5. Di halaman ini, buat rahasia klien baru.
6. Masukkan rahasia klien baru ke dalam bidang rahasia Klien di AppFabric.

Menyetujui otorisasi

Setelah membuat otorisasi aplikasi di AppFabric Anda akan menerima jendela pop-up dari Webex untuk menyetujui otorisasi. Untuk menyetujui AppFabric otorisasi, pilih terima.

Zendesk

Zendeskmemulai revolusi pengalaman pelanggan pada tahun 2007 dengan memungkinkan bisnis apa pun di seluruh dunia untuk mengambil layanan pelanggan mereka secara online. Hari ini, Zendesk adalah juara layanan hebat di mana-mana untuk semua orang, dan menggerakkan miliaran percakapan, menghubungkan lebih dari 100.000 merek dengan ratusan juta pelanggan melalui telepon, obrolan, email, pesan, saluran sosial, komunitas, situs ulasan, dan pusat bantuan. Zendeskproduk dibangun dengan cinta untuk dicintai. Perusahaan ini didirikan di Kopenhagen, Denmark, dibangun dan tumbuh di California, dan saat ini mempekerjakan lebih dari 6.000 orang di seluruh dunia.

Anda dapat menggunakan keamanan AWS AppFabric untuk menerima log audit dan data pengguna dariZendesk, menormalkan data ke dalam format Open Cybersecurity Schema Framework (OCSF), dan mengeluarkan data ke bucket Amazon Simple Storage Service (Amazon S3) atau aliran Amazon Data Firehose.

Topik

AppFabric dukungan untuk Zendesk

AppFabric mendukung penerimaan informasi pengguna dan log audit dariZendesk.

Prasyarat

Untuk digunakan AppFabric untuk mentransfer log audit dari Zendesk tujuan yang didukung, Anda harus memenuhi persyaratan berikut:

- Anda harus memiliki akun Zendesk Suite Enterprise atau Enterprise Plus atau akun Zendesk Support Enterprise. Untuk informasi selengkapnya tentang membuat atau meningkatkan ke akun Zendesk Perusahaan, lihat Memeriksa jenis paket Anda Zendesk di Zendesk situs web.

- Anda harus memiliki pengguna dengan peran Administrator di Zendesk akun Anda. Untuk informasi selengkapnya tentang peran, lihat Memahami peran pengguna Zendesk Support di Zendesk situs web.

Pertimbangan batas tarif

Zendeskmemberlakukan batas tarif pada Zendesk API. Untuk informasi selengkapnya tentang batas tarif Zendesk API, lihat Batas tarif di Panduan Zendesk Pengembang di Zendesk situs web. Jika kombinasi AppFabric dan aplikasi Zendesk API Anda yang ada melebihi batas, log audit yang muncul AppFabric mungkin tertunda.

Pertimbangan keterlambatan data

Anda mungkin melihat penundaan hingga 30 menit untuk acara audit yang akan dikirim ke tujuan Anda. Hal ini disebabkan keterlambatan dalam peristiwa audit yang disediakan oleh aplikasi serta karena tindakan pencegahan yang diambil untuk mengurangi kehilangan data. Namun, ini mungkin dapat disesuaikan di tingkat akun. Untuk bantuan, hubungi AWS Support.

Menghubungkan AppFabric ke Zendesk akun Anda

Setelah Anda membuat app bundle dalam AppFabric layanan, Anda harus mengotorisasi AppFabric denganZendesk. Untuk menemukan informasi yang diperlukan untuk mengotorisasi Zendesk AppFabric, gunakan langkah-langkah berikut.

Buat aplikasi OAuth

AppFabric terintegrasi dengan Zendesk menggunakan OAuth. DiZendesk, Anda harus membuat aplikasi OAuth dengan pengaturan berikut:

1. Ikuti petunjuk di bagian Mendaftarkan aplikasi Anda dengan Zendesk pada artikel Menggunakan otentikasi OAuth dengan aplikasi Anda di situs web Support. Zendesk
2. Gunakan URL pengalihan dengan format berikut.

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   Di URL ini, `<region>` adalah kode untuk paket AppFabric aplikasi yang telah Anda konfigurasi. Wilayah AWS Misalnya, kode untuk Wilayah AS Timur (Virginia N.) adalah`us-east-1`. Untuk Wilayah itu, URL pengalihan adalah`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

Otorisasi aplikasi

ID Penyewa

AppFabric akan meminta ID Penyewa Anda. ID Penyewa di AppFabric adalah Zendesk subdomain Anda. Untuk informasi selengkapnya tentang menemukan Zendesk subdomain Anda, lihat Di mana saya dapat menemukan Zendesk subdomain saya di situs web Zendesk Support.

Nama penyewa

Masukkan nama yang mengidentifikasi Zendesk organisasi unik ini. AppFabric menggunakan nama penyewa untuk memberi label pada otorisasi aplikasi dan konsumsi apa pun yang dibuat dari otorisasi aplikasi.

ID Klien

AppFabric akan meminta ID klien. ID klien di AppFabric adalah pengidentifikasi unik Zendesk API Anda. Untuk menemukan pengenal unik Zendesk Anda, gunakan langkah-langkah berikut:

1. Arahkan ke Pusat Admin di Zendesk akun Anda.
2. Pilih Aplikasi dan integrasi.
3. Pilih API, ZendeskAPI.
4. Pilih tab Klien OAuth.
5. Pilih aplikasi OAuth yang Anda buat. AppFabric
6. Masukkan pengenal unik untuk klien OAuth Anda ke dalam bidang ID Klien di. AppFabric

Rahasia klien

AppFabric akan meminta rahasia klien. Rahasia klien AppFabric adalah token Zendesk rahasia Anda. Zendeskmenyajikan token rahasia Anda hanya sekali ketika Anda pertama kali membuat aplikasi Zendesk OAuth Anda. Untuk membuat token rahasia baru jika Anda tidak menyimpan token rahasia awal, gunakan langkah-langkah berikut:

1. Arahkan ke Pusat Admin di Zendesk akun Anda.
2. Pilih Aplikasi dan integrasi.
3. Pilih API, ZendeskAPI.
4. Pilih tab Klien OAuth.
5. Pilih aplikasi OAuth yang Anda buat. AppFabric

6. Pilih tombol Regenerasi di sebelah bidang token Rahasia.
7. Masukkan token rahasia baru ke dalam bidang rahasia Klien di AppFabric.

Menyetujui otorisasi

Setelah membuat otorisasi aplikasi di AppFabric, Anda akan menerima jendela pop-up dari Zendesk untuk menyetujui otorisasi. Untuk menyetujui AppFabric otorisasi, pilih Izinkan.

Zoom

Zoomadalah platform kolaborasi all-in-one cerdas yang membuat koneksi lebih mudah, lebih mendalam, dan lebih dinamis untuk bisnis dan individu. ZoomTeknologi menempatkan orang di pusat, memungkinkan koneksi yang bermakna, memfasilitasi kolaborasi modern, dan mendorong inovasi manusia melalui solusi seperti obrolan tim, telepon, rapat, pusat kontak cloud omnichannel, rekaman pintar, papan tulis, dan banyak lagi, dalam satu penawaran.

Anda dapat menggunakan keamanan AWS AppFabric untuk menerima log audit dan data pengguna dariZoom, menormalkan data ke dalam format Open Cybersecurity Schema Framework (OCSF), dan mengeluarkan data ke bucket Amazon Simple Storage Service (Amazon S3) atau aliran Amazon Data Firehose.

Topik

- AppFabric dukungan untuk Zoom
- Menghubungkan AppFabric ke Zoom akun Anda

AppFabric dukungan untuk Zoom

AppFabric mendukung penerimaan informasi pengguna dan log audit dariZoom.

Prasyarat

Untuk digunakan AppFabric untuk mentransfer log audit dari Zoom tujuan yang didukung, Anda harus memenuhi persyaratan berikut:

- Anda harus memiliki rencana Zoom Pro, Bisnis, Pendidikan, atau Perusahaan.
- Peran Zoom Admin Anda harus memiliki izin untuk membuat server-to-server OAuth aplikasi. Untuk informasi tentang mengaktifkan server-to-server OAuth aplikasi, lihat bagian Aktifkan izin pada OAuth halaman Server-ke-Server di Panduan ZoomPengembang di situs web. Zoom

- Peran Zoom Admin Anda harus memiliki izin untuk melihat log aktivitas admin dan masuk/keluar aktivitas audit. Untuk informasi selengkapnya tentang mengaktifkan izin untuk melihat aktivitas audit, lihat Menggunakan manajemen peran dan Menggunakan Log Aktivitas Admin di situs web Zoom Support.

Pertimbangan batas tarif

Zoommemberlakukan batas tarif pada. Zoom API Untuk informasi selengkapnya tentang batas Zoom API tarif, lihat Batas tarif di Panduan Zoom Pengembang. Jika kombinasi AppFabric dan Zoom aplikasi Anda yang ada melebihi batas, log audit yang muncul AppFabric mungkin tertunda.

Pertimbangan keterlambatan data

Anda mungkin melihat penundaan sekitar 24 jam untuk acara audit yang akan dikirim ke tujuan Anda. Hal ini disebabkan keterlambatan dalam peristiwa audit yang disediakan oleh aplikasi serta karena tindakan pencegahan yang diambil untuk mengurangi kehilangan data.

Menghubungkan AppFabric ke Zoom akun Anda

Setelah Anda membuat bundel aplikasi dalam AppFabric layanan, maka Anda harus mengotorisasi AppFabric denganZoom. Untuk menemukan informasi yang diperlukan untuk mengotorisasi Zoom AppFabric, gunakan langkah-langkah berikut.

Buat server-to-server OAuth aplikasi

AppFabric menggunakan server-to-server OAuth dengan kredensi aplikasi untuk diintegrasikan dengan. Zoom Untuk membuat server-to-server OAuth aplikasiZoom, ikuti petunjuk di Buat aplikasi Server-to-Server di Panduan OAuth PengembangZoom. AppFabric tidak mendukung Zoom webhook, dan Anda dapat melewati bagian untuk menambahkan langganan webhook.

Cakupan yang dibutuhkan

Zoommenawarkan dua jenis cakupan: cakupan granular (untuk aplikasi yang baru dibuat) dan cakupan klasik (untuk aplikasi yang dibuat sebelumnya).

Anda harus menambahkan cakupan granular berikut ke aplikasi Anda Zoom server-to-serverOAuth:

- `report:read:user_activities:admin`
- `report:read:operation_logs:admin`
- `user:read:email:admin`
- `user:read:user:admin`

Jika Anda menggunakan aplikasi yang dibuat sebelumnya, Anda perlu menambahkan cakupan klasik berikut:

- `report:read:admin`
- `user:read:admin`

Otorisasi aplikasi

ID Penyewa

AppFabric akan meminta ID penyewa Anda. ID penyewa di AppFabric adalah ID Zoom akun. Untuk menemukan ID Zoom akun Anda, gunakan langkah-langkah berikut:

1. Arahkan ke Zoom pasar.
2. Pilih Kelola.
3. Pilih server-to-server OAuth aplikasi yang Anda gunakan untuk AppFabric.
4. Masukkan ID akun dari halaman Kredensial Aplikasi ke bidang ID Penyewa di. AppFabric

Nama penyewa

Masukkan nama yang mengidentifikasi Zoom organisasi unik ini. AppFabric menggunakan nama penyewa untuk memberi label pada otorisasi aplikasi dan konsumsi apa pun yang dibuat dari otorisasi aplikasi.

ID Klien

AppFabric akan meminta ID klien Anda. Untuk menemukan ID Zoom klien Anda, gunakan langkah-langkah berikut:

1. Arahkan ke Zoom pasar.
2. Pilih Kelola.
3. Pilih server-to-server OAuth aplikasi yang Anda gunakan untuk AppFabric.
4. Masukkan ID klien dari halaman App Credentials ke dalam kolom Client ID di. AppFabric

Rahasia klien

AppFabric akan meminta rahasia klien Anda. Untuk menemukan rahasia Zoom klien Anda, gunakan langkah-langkah berikut:

1. Arahkan ke Zoom pasar.
2. Pilih Kelola.
3. Pilih server-to-server OAuth aplikasi yang Anda gunakan untuk AppFabric.
4. Masukkan rahasia klien dari halaman Kredensial Aplikasi ke bidang rahasia Klien di. AppFabric

Pengiriman log audit

Zoommembuat log audit tersedia dengan mengakses API setiap 24 jam. Saat melihat log audit dengan AppFabric, data yang Anda lihat Zoom adalah untuk aktivitas hari sebelumnya.

Alat dan layanan keamanan yang kompatibel

AWS AppFabric untuk keamanan mendukung integrasi dengan alat dan layanan keamanan berikut. Pilih nama layanan untuk informasi selengkapnya tentang cara mengatur keamanan AppFabric agar tersambung dengannya.

Topik

Barracuda XDR

Barracuda Networksadalah mitra tepercaya dan penyedia terkemuka solusi keamanan cloud-first, melindungi email, jaringan, data, dan aplikasi dengan solusi inovatif yang tumbuh dan beradaptasi dengan perjalanan bisnis. Barracuda XDRadalah solusi deteksi dan respons terbuka yang diperluas yang menggabungkan teknologi canggih dengan tim analis keamanan di pusat operasi keamanan (SOC) kami. Barracuda XDRPlatform ini menganalisis miliaran peristiwa mentah setiap hari dari 40+

sumber data terintegrasi, dan bersama dengan aturan deteksi ancaman ekstensif yang dipetakan ke kerangka kerja MITRE ATT&CK®, platform ini dapat mendeteksi ancaman lebih cepat dan mengurangi waktu respons.

AWS AppFabric pertimbangan konsumsi log audit

Bagian berikut menjelaskan skema AppFabric output, format output, dan tujuan output untuk digunakan. Barracuda XDR

Skema dan format

Barracuda XDRmendukung skema AppFabric output berikut dan format:

- OCSF - JSON: AppFabric menormalkan data menggunakan Open Cybersecurity Schema Framework (OCSF) dan mengeluarkan data dalam format JSON.

Lokasi keluaran

Barracuda XDRmendukung penerimaan Log Audit dari Amazon Security Lake. Untuk mengirim data dari AppFabric keBarracuda XDR, ikuti petunjuk di bawah ini:

1. Kirim data ke Amazon Security Lake: Konfigurasikan AppFabric untuk mengirim data ke Amazon Security Lake melalui Amazon Data Firehose. Untuk informasi selengkapnya, lihat Amazon Security Lake.
2. Kirim data keBarracuda XDR: Konfigurasikan Barracuda XDR untuk menerima log audit dari Amazon Security Lake. Untuk informasi selengkapnya, lihat Menyiapkan dan Menggunakan Amazon Security Lake.

Dynatrace

Dynatrace® PlatformIni menggabungkan observabilitas yang luas dan mendalam serta keamanan aplikasi runtime berkelanjutan dengan AIOps canggih untuk memberikan jawaban dan otomatisasi cerdas dari data. Hal ini memungkinkan inovator untuk memodernisasi dan mengotomatiskan operasi cloud, menghadirkan perangkat lunak lebih cepat dan lebih aman, dan memastikan pengalaman digital yang sempurna.

AWS AppFabric pertimbangan konsumsi log audit

Bagian berikut menjelaskan skema AppFabric output, format output, dan tujuan output untuk digunakan dengan. Dynatrace Platform

Skema dan format

Dynatrace PlatformMendukung skema AppFabric output berikut dan format:

- OCSF - JSON: AppFabric menormalkan data menggunakan Open Cybersecurity Schema Framework (OCSF) dan mengeluarkan data dalam format JSON.

Lokasi keluaran

Dynatrace PlatformMendukung penerimaan Log Audit dari lokasi AppFabric Output berikut.

- Amazon Simple Storage Service (Amazon S3)
  - Untuk mengonfigurasi Dynatrace Platform untuk menerima data dari bucket Amazon S3 yang berisi log audit Anda, ikuti petunjuk di project S3 Log Forwarder Dynatrace. GitHub

Logz.io

Logz.iomembantu bisnis cloud native memantau dan mengamankan lingkungan mereka melalui Platform Logz.ioOpen 360 — mengubah observabilitas dan keamanan dari beban berbiaya tinggi dan bernilai rendah menjadi enabler bernilai tinggi dan hemat biaya untuk hasil bisnis yang lebih baik.

Logz.ioCloud SIEM secara langsung mengatasi tantangan keamanan terkemuka saat ini - mulai dari kelebihan data hingga kesenjangan keterampilan cyber yang ada di mana-mana - melalui kueri cepat, deteksi multidimensi, dan konten keamanan yang dapat disesuaikan secara mendalam untuk membantu memantau dan menyelidiki seluruh lingkungan cloud Anda - tanpa penurunan kinerja, terlepas dari volume data.

Logz.ioSolusinya dibuat khusus untuk memberikan analisis dan investigasi ancaman tingkat lanjut dengan kompleksitas dan biaya yang lebih sedikit. Pelanggan didukung oleh analis keamanan khusus, konten ancaman sebagai layanan, dan kemampuan yang didukung AI yang dibuat khusus untuk membantu mengurangi data yang bising dan fokus pada informasi yang memungkinkan tim Anda memprioritaskan ancaman dunia nyata dengan cepat.

AWS AppFabric pertimbangan konsumsi log audit

Bagian berikut menjelaskan skema AppFabric output, format output, dan tujuan output untuk digunakan. Logz.io

Skema dan format

Logz.iomendukung skema AppFabric output berikut dan format:

- Mentah - JSON
  - AppFabric output data dalam skema asli yang digunakan oleh aplikasi sumber dalam format JSON.
- OCSF - JSON
  - AppFabric menormalkan data menggunakan Open Cybersecurity Schema Framework (OCSF) dan mengeluarkan data dalam format JSON.

Lokasi keluaran

Logz.iomendukung lokasi AppFabric output berikut:

- Amazon Data Firehose
  - Untuk mengonfigurasi aliran pengiriman Firehose agar mengirimkan dataLogz.io, ikuti petunjuk di Pilih Tujuan Anda di Logz.io Panduan Pengembang Amazon Data Firehose.
- Amazon Simple Storage Service (Amazon S3)
  - Logz.ioUntuk mengonfigurasi agar menerima data dari bucket Amazon S3 yang berisi log audit Anda, ikuti petunjuk di Mengonfigurasi bucket Amazon S3 di situs web. Logz.io

Netskope

Netskope, pemimpin keamanan siber global, mendefinisikan ulang keamanan cloud, data, dan jaringan untuk membantu organisasi menerapkan prinsip nol kepercayaan untuk melindungi data. Cepat dan mudah digunakan, Netskope platform ini menyediakan akses yang dioptimalkan dan keamanan tanpa kepercayaan untuk orang, perangkat, dan data ke mana pun mereka pergi. Netskopemembantu pelanggan mengurangi risiko, mempercepat kinerja, dan mendapatkan visibilitas yang tak tertandingi ke dalam aktivitas cloud, web, dan aplikasi pribadi apa pun. Ribuan pelanggan, termasuk lebih dari 25 dari Fortune 100, kepercayaan Netskope dan NewEdge jaringannya yang kuat untuk mengatasi ancaman yang berkembang, risiko baru, pergeseran teknologi, perubahan organisasi dan jaringan, dan persyaratan peraturan baru. Pelajari bagaimana Netskope membantu pelanggan siap untuk apa pun dalam perjalanan SASE mereka, kunjungi netskope.com.

AWS AppFabric pertimbangan konsumsi log audit

Bagian berikut menjelaskan skema AppFabric output, format output, dan tujuan output untuk digunakan. Netskope

Skema dan format

Netskopemendukung skema AppFabric output berikut dan format:

- Mentah - JSON
  - AppFabric output data dalam skema asli yang digunakan oleh aplikasi sumber dalam format JSON.
- OCSF - JSON
  - AppFabric menormalkan data menggunakan Open Cybersecurity Schema Framework (OCSF) dan mengeluarkan data dalam format JSON.

Lokasi keluaran

Netskopemendukung lokasi AppFabric output berikut:

- Amazon Simple Storage Service (Amazon S3)
  - NetskopeUntuk mengonfigurasi agar menerima data dari bucket Amazon S3 yang berisi log audit Anda, ikuti petunjuk di Perlindungan Data untuk Amazon Web Services S3 di situs web. Netskope

NetWitness

NetWitnessadalah pengembang terkemuka perangkat lunak deteksi dan respons yang diperluas (XDR). Basis global mereka dari pelanggan yang sangat sadar keamanan bergantung pada NetWitness XDR untuk bertahan melawan musuh yang canggih dan agresif. Dengan platform industri yang paling lengkap, terintegrasi, dan matang untuk mendeteksi, menyelidiki, dan menanggapi serangan digital, NetWitness XDR adalah fondasi pemersatu dari SOC modern dan efektif.

Karena arsitekturnya yang sangat modular, NetWitness XDR mendeteksi ancaman di mana pun mereka terjadi — di cloud, lokal, dengan pekerja seluler dan jarak jauh, atau di mana pun di antaranya. NetWitnessPlatform XDR memberikan visibilitas lengkap yang dikombinasikan dengan kecerdasan ancaman terapan dan analisis perilaku pengguna untuk mendeteksi ancaman, memprioritaskan aktivitas, menyelidiki, dan mengotomatiskan respons. Semua ini memberdayakan

analis keamanan dengan efisiensi yang lebih baik dan lebih cepat untuk menjaga operasi keamanan jauh di depan ancaman yang berdampak pada bisnis.

AWS AppFabric pertimbangan konsumsi log audit

Bagian berikut menjelaskan skema AppFabric output, format output, dan tujuan output untuk digunakan. NetWitness

Skema dan format

NetWitness mendukung skema AppFabric output berikut dan format:

- Mentah - JSON
  - AppFabric output data dalam skema asli yang digunakan oleh aplikasi sumber dalam format JSON.
- OCSF - JSON
  - AppFabric menormalkan data menggunakan Open Cybersecurity Schema Framework (OCSF) dan mengeluarkan data dalam format JSON.

Lokasi keluaran

NetWitnessmendukung lokasi AppFabric output berikut:

- Amazon Simple Storage Service (Amazon S3)
  - NetWitnessUntuk mengonfigurasi agar menerima data dari bucket Amazon S3 yang berisi log audit Anda, ikuti petunjuk di Panduan Konfigurasi Log Sumber Peristiwa Konektor Universal S3 di halaman Integrasi NetWitness Platform di situs web. NetWitness

Amazon QuickSight

Amazon QuickSight memberdayakan organisasi berbasis data dengan intelijen bisnis terpadu (BI) di hyperscale. Dengan QuickSight, semua pengguna dapat memenuhi berbagai kebutuhan analitik dari sumber kebenaran yang sama melalui dasbor interaktif modern, laporan berhalaman, analitik tertanam, dan kueri bahasa alami. Anda dapat menganalisis data log AWS AppFabric audit QuickSight, dengan memilih bucket Amazon Simple Storage Service (Amazon S3) tempat log keamanan disimpan sebagai sumber AppFabric Anda.

AppFabric pertimbangan konsumsi log audit

Bagian berikut menjelaskan skema AppFabric output, format output, dan tujuan output untuk digunakan dengan Amazon QuickSight.

Skema dan format

QuickSight mendukung skema AppFabric output berikut dan format:

- Mentah - JSON
  - AppFabric output data dalam skema asli yang digunakan oleh aplikasi sumber dalam format JSON.
- OCSF - JSON
  - AppFabric menormalkan data menggunakan Open Cybersecurity Schema Framework (OCSF) dan mengeluarkan data dalam format JSON.

Lokasi keluaran

QuickSight mendukung lokasi AppFabric output berikut:

- Amazon S3
  - Anda dapat menelan data dari Amazon S3 langsung QuickSight ke dalam dengan Membuat kumpulan data menggunakan file Amazon S3. Untuk memverifikasi bahwa kumpulan file target Anda tidak melebihi kuota sumber QuickSight data, lihat Kuota sumber data di QuickSight Panduan Pengguna Amazon.
  - Jika kumpulan file Anda melebihi QuickSight kuota untuk sumber data Amazon S3, Anda dapat menelan data Anda di Amazon S3 menggunakan Amazon Athena dan tabel. AWS Glue Menggunakan Athena dalam QuickSight kumpulan data Anda akan dikenakan biaya tambahan. Untuk informasi lebih lanjut tentang harga Athena, lihat halaman harga Athena.

    Untuk menggunakan Athena:

    1. Ikuti petunjuk di Menggunakan AWS Glue untuk menyambung ke sumber data di Amazon S3 di Panduan Pengguna Athena.
    2. Ikuti petunjuk dalam Membuat kumpulan data menggunakan data Athena di Panduan Pengguna QuickSight Amazon.

Rapid7

Rapid7Inc. memiliki misi untuk menciptakan dunia digital yang lebih aman dengan membuat keamanan siber lebih sederhana dan lebih mudah diakses. Rapid7Memberdayakan profesional keamanan untuk mengelola permukaan serangan modern melalui best-in-class teknologi, penelitian terdepan, dan keahlian strategis yang luas. Rapid7Solusi keamanan komprehensif membantu lebih dari 10.000 pelanggan global menyatukan manajemen risiko cloud dan deteksi ancaman untuk mengurangi permukaan serangan dan menghilangkan ancaman dengan kecepatan dan presisi.

AWS AppFabric pertimbangan konsumsi log audit

Bagian berikut menjelaskan skema AppFabric output, format output, dan tujuan output untuk digunakan denganRapid7.

Skema dan format

Rapid7mendukung skema AppFabric output berikut dan format:

- Mentah - JSON
  - AppFabric output data dalam skema asli yang digunakan oleh aplikasi sumber dalam format JSON.
- OCSF - JSON
  - AppFabric menormalkan data menggunakan Open Cybersecurity Schema Framework (OCSF) dan mengeluarkan data dalam format JSON.

Lokasi keluaran

Rapid7mendukung lokasi AppFabric output berikut:

- Amazon Simple Storage Service (Amazon S3)
  - Untuk mengonfigurasi Rapid7 agar menerima data dari bucket Amazon S3 yang berisi log audit Anda, ikuti petunjuk di postingan blog Cara Memantau Aktivitas Amazon S3 Anda dengan InsightIdR di situs web Blog. Rapid7

Amazon Security Lake

Amazon Security Lake secara otomatis memusatkan data keamanan dari AWS lingkungan, penyedia perangkat lunak sebagai layanan (SaaS), di tempat, dan sumber cloud ke dalam data

lake yang dibuat khusus yang disimpan di tempat Anda. Akun AWS Dengan Security Lake, Anda bisa mendapatkan pemahaman yang lebih lengkap tentang data keamanan Anda di seluruh organisasi Anda. Security Lake telah mengadopsi Open Cybersecurity Schema Framework (OCSF), skema acara keamanan open source. Dengan OCSF dukungan, layanan ini menormalkan dan menggabungkan data keamanan dari AWS dan berbagai sumber data keamanan perusahaan.

AppFabric pertimbangan konsumsi log audit

Anda bisa mendapatkan log audit SaaS Anda ke Amazon Security Lake di Anda Akun AWS dengan menambahkan sumber khusus ke Security Lake. Bagian berikut menjelaskan skema AppFabric output, format output, dan tujuan output untuk digunakan dengan Security Lake.

Skema dan format

Security Lake mendukung skema dan format AppFabric keluaran berikut:

- OCSF - JSON
  - AppFabric menormalkan data menggunakan Open Cybersecurity Schema Framework (OCSF) dan mengeluarkan data dalam format. JSON

Lokasi keluaran

Security Lake mendukung AppFabric sebagai sumber kustom menggunakan aliran pengiriman Amazon Data Firehose sebagai lokasi keluaran AppFabric konsumsi. Untuk mengonfigurasi AWS Glue tabel dan aliran pengiriman Firehose, dan untuk menyiapkan sumber kustom di Security Lake, gunakan prosedur berikut.

Buat AWS Glue tabel

1. Arahkan ke Amazon Simple Storage Service (Amazon S3) dan buat bucket dengan nama pilihan Anda.
2. Arahkan ke AWS Glue konsol.
3. Untuk Katalog Data, buka bagian Tabel, dan pilih Tambahkan Tabel.
4. Masukkan nama pilihan Anda untuk tabel ini.
5. Pilih bucket Amazon S3 yang Anda buat di langkah 1.
6. Untuk format data, pilih JSON, dan pilih Berikutnya.
7. Pada halaman Pilih atau tentukan skema, pilih Edit skema sebagai. JSON
8. Masukkan skema berikut, dan selesaikan proses pembuatan AWS Glue tabel.

```
[
    {
        "Name": "message",
        "Type": "string"
    },
    {
        "Name": "process",
        "Type":
 "struct<name:string,pid:int,user:struct<name:string,type:string,domain:string,uid:string,t
    },
    {
        "Name": "status",
        "Type": "string"
    },
    {
        "Name": "time",
        "Type": "bigint"
    },
    {
        "Name": "device",
        "Type":
 "struct<name:string,owner:struct<name:string,type:string,uid:string,type_id:int,risk_level
    },
    {
        "Name": "metadata",
        "Type":
 "struct<version:string,product:struct<name:string,version:string,uid:string,data_classific
    },
    {
        "Name": "severity",
        "Type": "string"
    },
    {
        "Name": "duration",
        "Type": "int"
    },
    {
        "Name": "type_name",
        "Type": "string"
    },
    {
        "Name": "activity_id",
        "Type": "int"
```

```
    },
    {
        "Name": "type_uid",
        "Type": "int"
    },
    {
        "Name": "observables",
        "Type": "array<struct<name:string,type:string,type_id:int,value:string>>"
    },
    {
        "Name": "category_name",
        "Type": "string"
    },
    {
        "Name": "class_uid",
        "Type": "int"
    },
    {
        "Name": "category_uid",
        "Type": "int"
    },
    {
        "Name": "class_name",
        "Type": "string"
    },
    {
        "Name": "timezone_offset",
        "Type": "int"
    },
    {
        "Name": "end_time",
        "Type": "bigint"
    },
    {
        "Name": "activity_name",
        "Type": "string"
    },
    {
        "Name": "cloud",
        "Type":
"struct<account:struct<name:string,type:string,uid:string,type_id:int>,project_uid:string,
    },
    {
        "Name": "query_info",
```

```
        "Type": "struct<name:string,uid:string,query_string:string>"
    },
    {
        "Name": "query_result",
        "Type": "string"
    },
    {
        "Name": "query_result_id",
        "Type": "int"
    },
    {
        "Name": "severity_id",
        "Type": "int"
    },
    {
        "Name": "status_code",
        "Type": "string"
    },
    {
        "Name": "status_detail",
        "Type": "string"
    },
    {
        "Name": "status_id",
        "Type": "int"
    },
    {
        "Name": "network_interfaces",
        "Type":
 "array<struct<name:string,type:string,hostname:string,mac:string,type_id:int,ip:string>>"
    },
    {
        "Name": "file",
        "Type":
 "struct<attributes:int,name:string,type:string,path:string,type_id:int,accessor:struct<nam
    },
    {
        "Name": "actor",
        "Type":
 "struct<process:struct<pid:int,file:struct<name:string,size:bigint,type:string,version:str
    },
    {
        "Name": "dst_endpoint",
```

```
        "Type":
"struct<owner:struct<name:string,type:string,uid:string,type_id:int,full_name:string,risk_
    },
    {
        "Name": "src_endpoint",
        "Type":
"struct<name:string,owner:struct<name:string,type:string,domain:string,uid:string,org:stru
    },
    {
        "Name": "user",
        "Type":
"struct<name:string,type:string,groups:array<struct<name:string,uid:string>>,type_id:int>"
    },
    {
        "Name": "resource",
        "Type":
"struct<version:string,uid:string,agent_list:array<struct<name:string,type:string,uid:stri
    },
    {
        "Name": "privileges",
        "Type": "array<string>"
    },
    {
        "Name": "action",
        "Type": "string"
    },
    {
        "Name": "action_id",
        "Type": "int"
    },
    {
        "Name": "protocol_ver",
        "Type": "string"
    },
    {
        "Name": "proxy",
        "Type":
"struct<name:string,port:int,type:string,ip:string,hostname:string,uid:string,type_id:int,
    },
    {
        "Name": "client_hassh",
        "Type":
"struct<algorithm:string,fingerprint:struct<value:string,algorithm:string,algorithm_id:int
    },
```

```
    {
        "Name": "authorizations",
        "Type": "array<string>"
    },
    {
        "Name": "proxy_tls",
        "Type":
"struct<version:string,certificate:struct<version:string,uid:string,subject:string,issuer:
    },
    {
        "Name": "load_balancer",
        "Type":
"struct<name:string,classification:string,dst_endpoint:struct<owner:struct<type:string,dom
    },
    {
        "Name": "disposition_id",
        "Type": "int"
    },
    {
        "Name": "disposition",
        "Type": "string"
    },
    {
        "Name": "proxy_traffic",
        "Type": "struct<bytes:bigint,packets:int>"
    },
    {
        "Name": "auth_type_id",
        "Type": "int"
    },
    {
        "Name": "proxy_http_response",
        "Type": "struct<code:int,message:string,status:string,length:int>"
    },
    {
        "Name": "server_hassh",
        "Type":
"struct<algorithm:string,fingerprint:struct<value:string,algorithm:string,algorithm_id:int
    },
    {
        "Name": "auth_type",
        "Type": "string"
    },
    {
```

```
        "Name": "firewall_rule",
        "Type": "struct<version:string,uid:string>"
    },
    {
        "Name": "proxy_connection_info",
        "Type":
"struct<direction:string,direction_id:int,protocol_num:int,protocol_ver:string>"
    },
    {
        "Name": "connection_info",
        "Type": "struct<direction:string,direction_id:int>"
    },
    {
        "Name": "api",
        "Type":
"struct<request:struct<data:string,uid:string>,response:struct<error:string,code:int,messa
    },
    {
        "Name": "attacks",
        "Type":
"array<struct<version:string,tactics:array<struct<name:string,uid:string>>,technique:struc
    },
    {
        "Name": "raw_data",
        "Type": "string"
    },
    {
        "Name": "email_uid",
        "Type": "string"
    },
    {
        "Name": "malware",
        "Type":
"array<struct<name:string,path:string,uid:string,classification_ids:array<int>,cves:array<
    },
    {
        "Name": "start_time_dt",
        "Type": "string"
    },
    {
        "Name": "direction",
        "Type": "string"
    },
    {
```

```
        "Name": "smtp_hello",
        "Type": "string"
    },
    {
        "Name": "unmapped",
        "Type": "string"
    },
    {
        "Name": "direction_id",
        "Type": "int"
    },
    {
        "Name": "email_auth",
        "Type":
"struct<spf:string,dkim:string,dkim_domain:string,dkim_signature:string,dmarc:string,dmarc
    },
    {
        "Name": "email",
        "Type":
"struct<uid:string,from:string,to:array<string>,data_classification:struct<category:string
    },
    {
        "Name": "impact_id",
        "Type": "int"
    },
    {
        "Name": "resources",
        "Type":
"array<struct<owner:struct<name:string,type:string,uid:string,type_id:int,full_name:string
    },
    {
        "Name": "finding_info",
        "Type":
"struct<title:string,uid:string,attacks:array<struct<version:string,tactics:array<struct<n
    },
    {
        "Name": "evidences",
        "Type":
"array<struct<process:struct<name:string,pid:int,file:struct<name:string,type:string,versi
    },
    {
        "Name": "impact",
        "Type": "string"
    },
```

```
    {
        "Name": "count",
        "Type": "int"
    },
    {
        "Name": "confidence_id",
        "Type": "int"
    },
    {
        "Name": "enrichments",
        "Type":
 "array<struct<data:string,name:string,type:string,value:string,provider:string>>"
    },
    {
        "Name": "rcode",
        "Type": "string"
    },
    {
        "Name": "app_name",
        "Type": "string"
    },
    {
        "Name": "rcode_id",
        "Type": "int"
    },
    {
        "Name": "query",
        "Type":
 "struct<type:string,hostname:string,class:string,opcode_id:int,packet_uid:int>"
    },
    {
        "Name": "proxy_endpoint",
        "Type":
 "struct<name:string,owner:struct<name:string,type:string,domain:string,uid:string,groups:a
    },
    {
        "Name": "response_time",
        "Type": "bigint"
    },
    {
        "Name": "delay",
        "Type": "int"
    },
    {
```

```
        "Name": "start_time",
        "Type": "bigint"
    },
    {
        "Name": "proxy_http_request",
        "Type":
 "struct<version:string,url:struct<port:int,scheme:string,path:string,hostname:string,query
    },
    {
        "Name": "version",
        "Type": "string"
    },
    {
        "Name": "stratum",
        "Type": "string"
    },
    {
        "Name": "stratum_id",
        "Type": "int"
    },
    {
        "Name": "dispersion",
        "Type": "int"
    },
    {
        "Name": "traffic",
        "Type":
 "struct<bytes_out:int,chunks:bigint,bytes:int,packets:int,packets_in:bigint>"
    },
    {
        "Name": "precision",
        "Type": "int"
    },
    {
        "Name": "size",
        "Type": "int"
    },
    {
        "Name": "actual_permissions",
        "Type": "int"
    },
    {
        "Name": "base_address",
        "Type": "string"
```

```
    },
    {
        "Name": "requested_permissions",
        "Type": "int"
    },
    {
        "Name": "end_time_dt",
        "Type": "string"
    },
    {
        "Name": "compliance",
        "Type":
"struct<control:string,status:string,standards:array<string>,status_id:int>"
    },
    {
        "Name": "remediation",
        "Type": "struct<desc:string>"
    },
    {
        "Name": "kb_article_list",
        "Type":
"array<struct<os:struct<name:string,type:string,type_id:int,cpe_name:string,edition:string
    },
    {
        "Name": "peripheral_device",
        "Type":
"struct<name:string,class:string,uid:string,model:string,serial_number:string,vendor_name:
    },
    {
        "Name": "time_dt",
        "Type": "string"
    },
    {
        "Name": "group",
        "Type": "struct<name:string,type:string,uid:string>"
    },
    {
        "Name": "users",
        "Type":
"array<struct<name:string,type:string,uid:string,type_id:int,risk_level:string,risk_level_
    },
    {
        "Name": "confidence_score",
        "Type": "int"
```

```
    },
    {
        "Name": "state",
        "Type": "string"
    },
    {
        "Name": "state_id",
        "Type": "int"
    },
    {
        "Name": "evidence",
        "Type": "string"
    },
    {
        "Name": "confidence",
        "Type": "string"
    },
    {
        "Name": "risk_level",
        "Type": "string"
    },
    {
        "Name": "risk_score",
        "Type": "int"
    },
    {
        "Name": "impact_score",
        "Type": "int"
    },
    {
        "Name": "risk_level_id",
        "Type": "int"
    },
    {
        "Name": "finding",
        "Type":
 "struct<title:string,uid:string,modified_time:bigint,modified_time_dt:string,first_seen_ti
    },
    {
        "Name": "user_result",
        "Type":
 "struct<name:string,type:string,uid:string,type_id:int,account:struct<name:string,uid:stri
    },
    {
```

```
        "Name": "codes",
        "Type": "array<int>"
    },
    {
        "Name": "command",
        "Type": "string"
    },
    {
        "Name": "type",
        "Type": "string"
    },
    {
        "Name": "kernel",
        "Type": "struct<name:string,type:string,type_id:int>"
    },
    {
        "Name": "http_response",
        "Type":
"struct<code:int,status:string,http_headers:array<struct<name:string,value:string>>>"
    },
    {
        "Name": "http_request",
        "Type":
"struct<url:struct<scheme:string,path:string,hostname:string,query_string:string,category_
    },
    {
        "Name": "tls",
        "Type":
"struct<version:string,certificate:struct<subject:string,issuer:string,fingerprints:array<
    },
    {
        "Name": "web_resources",
        "Type":
"array<struct<name:string,type:string,data_classification:struct<category:string,category_
    },
    {
        "Name": "http_cookies",
        "Type":
"array<struct<name:string,value:string,is_http_only:boolean,is_secure:boolean,samesite:str
    },
    {
        "Name": "type_id",
        "Type": "int"
    },
```

```
    {
        "Name": "databucket",
        "Type":
"struct<name:string,type:string,file:struct<attributes:int,name:string,owner:struct<name:s
    },
    {
        "Name": "table",
        "Type": "struct<uid:string,created_time_dt:string>"
    },
    {
        "Name": "session",
        "Type":
"struct<count:int,uid:string,uuid:string,issuer:string,created_time:bigint,is_remote:boole
    },
    {
        "Name": "certificate",
        "Type":
"struct<version:string,uid:string,subject:string,issuer:string,fingerprints:array<struct<v
    },
    {
        "Name": "is_mfa",
        "Type": "boolean"
    },
    {
        "Name": "logon_type_id",
        "Type": "int"
    },
    {
        "Name": "auth_protocol_id",
        "Type": "int"
    },
    {
        "Name": "logon_type",
        "Type": "string"
    },
    {
        "Name": "is_remote",
        "Type": "boolean"
    },
    {
        "Name": "is_cleartext",
        "Type": "boolean"
    },
    {
```

```
        "Name": "auth_protocol",
        "Type": "string"
    },
    {
        "Name": "is_renewal",
        "Type": "boolean"
    },
    {
        "Name": "lease_dur",
        "Type": "int"
    },
    {
        "Name": "relay",
        "Type":
 "struct<name:string,type:string,ip:string,mac:string,namespace:string,type_id:int>"
    },
    {
        "Name": "transaction_uid",
        "Type": "string"
    },
    {
        "Name": "file_result",
        "Type":
 "struct<name:string,size:int,type:string,path:string,desc:string,product:struct<name:strin
    },
    {
        "Name": "file_diff",
        "Type": "string"
    },
    {
        "Name": "create_mask",
        "Type": "string"
    },
    {
        "Name": "web_resources_result",
        "Type":
 "array<struct<type:string,data_classification:struct<category:string,category_id:int,confi
    },
    {
        "Name": "app",
        "Type":
 "struct<name:string,version:string,uid:string,data_classification:struct<category:string,c
    },
    {
```

```
        "Name": "src_url",
        "Type": "string"
    },
    {
        "Name": "priority_id",
        "Type": "int"
    },
    {
        "Name": "verdict",
        "Type": "string"
    },
    {
        "Name": "desc",
        "Type": "string"
    },
    {
        "Name": "verdict_id",
        "Type": "int"
    },
    {
        "Name": "priority",
        "Type": "string"
    },
    {
        "Name": "finding_info_list",
        "Type":
 "array<struct<title:string,uid:string,attacks:array<struct<version:string,tactics:array<st
    },
    {
        "Name": "expiration_time_dt",
        "Type": "string"
    },
    {
        "Name": "expiration_time",
        "Type": "bigint"
    },
    {
        "Name": "comment",
        "Type": "string"
    },
    {
        "Name": "entity",
        "Type": "struct<data:string,name:string,version:string,uid:string>"
    },
```

```
    {
        "Name": "entity_result",
        "Type":
"struct<data:string,name:string,type:string,version:string,uid:string>"
    },
    {
        "Name": "module",
        "Type":
"struct<type:string,file:struct<name:string,type:string,path:string,desc:string,type_id:in
    },
    {
        "Name": "exit_code",
        "Type": "int"
    },
    {
        "Name": "injection_type",
        "Type": "string"
    },
    {
        "Name": "injection_type_id",
        "Type": "int"
    },
    {
        "Name": "request",
        "Type": "struct<uid:string>"
    },
    {
        "Name": "response",
        "Type": "struct<error:string,code:int,message:string,error_message:string>"
    },
    {
        "Name": "driver",
        "Type":
"struct<file:struct<name:string,type:string,version:string,path:string,type_id:int,parent_
    },
    {
        "Name": "prev_security_states",
        "Type": "array<string>"
    },
    {
        "Name": "security_states",
        "Type": "array<string>"
    },
    {
```

```
        "Name": "folder",
        "Type":
"struct<name:string,type:string,path:string,desc:string,type_id:int,mime_type:string,paren
    },
    {
        "Name": "url",
        "Type":
"struct<port:int,scheme:string,path:string,hostname:string,query_string:string,resource_ty
    },
    {
        "Name": "tunnel_type_id",
        "Type": "int"
    },
    {
        "Name": "tunnel_type",
        "Type": "string"
    },
    {
        "Name": "protocol_name",
        "Type": "string"
    },
    {
        "Name": "job",
        "Type":
"struct<name:string,file:struct<name:string,type:string,path:string,signature:struct<certi
    },
    {
        "Name": "num_trusted_items",
        "Type": "int"
    },
    {
        "Name": "command_uid",
        "Type": "string"
    },
    {
        "Name": "num_registry_items",
        "Type": "int"
    },
    {
        "Name": "num_network_items",
        "Type": "int"
    },
    {
        "Name": "schedule_uid",
```

```
        "Type": "string"
    },
    {
        "Name": "num_resolutions",
        "Type": "int"
    },
    {
        "Name": "scan",
        "Type": "struct<name:string,type:string,type_id:int>"
    },
    {
        "Name": "num_detections",
        "Type": "int"
    },
    {
        "Name": "num_processes",
        "Type": "int"
    },
    {
        "Name": "num_files",
        "Type": "int"
    },
    {
        "Name": "total",
        "Type": "int"
    },
    {
        "Name": "num_folders",
        "Type": "int"
    },
    {
        "Name": "dce_rpc",
        "Type":
 "struct<command:string,flags:array<string>,command_response:string,opnum:int,rpc_interface
    },
    {
        "Name": "share",
        "Type": "string"
    },
    {
        "Name": "client_dialects",
        "Type": "array<string>"
    },
    {
```

```
        "Name": "open_type",
        "Type": "string"
    },
    {
        "Name": "tree_uid",
        "Type": "string"
    },
    {
        "Name": "share_type_id",
        "Type": "int"
    },
    {
        "Name": "share_type",
        "Type": "string"
    },
    {
        "Name": "dialect",
        "Type": "string"
    },
    {
        "Name": "cis_benchmark_result",
        "Type": "struct<name:string>"
    },
    {
        "Name": "vulnerabilities",
        "Type":
 "array<struct<references:array<string>,severity:string,affected_packages:array<struct<name
    },
    {
        "Name": "service",
        "Type": "struct<name:string,uid:string>"
    },
    {
        "Name": "data_security",
        "Type":
 "struct<category:string,pattern_match:string,category_id:int,confidentiality:string,confid
    },
    {
        "Name": "database",
        "Type":
 "struct<name:string,type:string,uid:string,type_id:int,data_classification:struct<category
    }
]
```

Buat sumber khusus di Security Lake

1. Arahkan ke konsol Amazon Security Lake.
2. Pilih Sumber khusus di panel navigasi.
3. Pilih Buat sumber khusus.
4. Masukkan nama untuk sumber kustom Anda dan pilih kelas OCSF acara yang berlaku.

> **Note**
>
> AppFabric menggunakan kelas peristiwa Perubahan Akun, Otentikasi, Manajemen Akses Pengguna, Manajemen Grup, Aktivitas Sumber Daya Web, dan Aktivitas Akses Sumber Daya Web.

5. Untuk Akun AWS ID dan ID Eksternal, masukkan Akun AWS ID Anda. Kemudian, pilih Buat.
6. Simpan lokasi Amazon S3 dari sumber kustom. Anda akan menggunakannya untuk mengatur aliran pengiriman Amazon Data Firehose.

Buat aliran pengiriman di Firehose

1. Arahkan ke konsol Amazon Data Firehose.
2. Pilih Buat aliran pengiriman.
3. Untuk Sumber, pilih Langsung PUT.
4. Untuk Tujuan, pilih S3.
5. Di bagian Transform and convert records, pilih Aktifkan konversi format rekaman dan pilih Apache Parquetsebagai format output.
6. Untuk AWS Glue tabel, pilih AWS Glue tabel yang Anda buat di prosedur sebelumnya, dan pilih versi terbaru.
7. Untuk pengaturan Tujuan, pilih bucket Amazon S3 yang Anda buat dengan sumber kustom Security Lake.
8. Untuk Partisi Dinamis, pilih Diaktifkan.
9. Untuk penguraian InlineJSON, pilih Diaktifkan.
   - Untuk Keyname, masukkan`eventDayValue`.
   - Untuk JQ Expression, masukkan`(.time/1000)|strftime("%Y%m%d")`.
10. Untuk awalan bucket S3, masukkan nilai berikut.

```
ext/<custom source name>/region=<region>/accountId=<account_id>/eventDay=!
{partitionKeyFromQuery:eventDayValue}/
```

Ganti *<custom source name>*, *<region>* and *<account_id>* dengan nama sumber kustom Security Lake Anda, Wilayah AWS dan Akun AWS ID.

11. Untuk awalan keluaran kesalahan bucket S3, masukkan nilai berikut.

```
ext/AppFabric/error/
```

12. Untuk durasi Coba lagi, pilih 300.
13. Untuk ukuran Buffer, pilih 128 MiB.
14. Untuk interval Buffer, pilih 60s.
15. Selesaikan proses pembuatan untuk aliran pengiriman Firehose.

Buat AppFabric konsumsi

Untuk mengirim data ke Amazon Security Lake, Anda harus membuat konsumsi di AppFabric konsol yang menggunakan aliran pengiriman Firehose yang Anda buat sebelumnya sebagai lokasi keluaran. Untuk informasi selengkapnya tentang mengonfigurasi AppFabric konsumsi untuk menggunakan Firehose sebagai lokasi keluaran, lihat Membuat lokasi keluaran.

Singularity Cloud

Singularity CloudPlatform ini melindungi perusahaan Anda dari ancaman semua kategori, di semua tahap. AI yang dipatenkan (Artificial Intelligence) memperluas keamanan dari tanda tangan dan pola yang diketahui hingga serangan paling canggih, seperti zero-day dan ransomware.

AWS AppFabric pertimbangan konsumsi log audit

Bagian berikut menjelaskan skema AppFabric output, format output, dan tujuan output untuk digunakan. Singularity Cloud

Skema dan format

Singularity Cloudmendukung skema AppFabric output berikut dan format:

OCSF - JSON: AppFabric menormalkan data menggunakan Open Cybersecurity Schema Framework (OCSF) dan mengeluarkan data dalam format JSON.

Lokasi keluaran

Singularity Cloudmendukung penerimaan Log Audit dari lokasi AppFabric Output berikut.

- Amazon Simple Storage Service (Amazon S3)
  - Singularity CloudUntuk mengonfigurasi agar menerima data dari bucket Amazon S3 yang berisi log audit Anda, ikuti petunjuk dalam Singularity Cloud's dokumentasi.

Splunk

Splunkmembantu membuat organisasi lebih tangguh. Organisasi Splunk terkemuka menggunakan platform keamanan dan observabilitas terpadu untuk menjaga sistem digital mereka tetap aman dan andal. Organizations percaya Splunk untuk mencegah masalah keamanan, infrastruktur, dan aplikasi menjadi insiden besar, menyerap guncangan dari gangguan digital dan mempercepat transformasi digital.

AWS AppFabric pertimbangan konsumsi log audit

Bagian berikut menjelaskan skema AppFabric output, format output, dan tujuan output untuk digunakan. Splunk

Skema dan format

Splunk mendukung skema dan AppFabric format keluaran berikut:

- Mentah - JSON
  - AppFabric output data dalam skema asli yang digunakan oleh aplikasi sumber dalam format JSON.
- OCSF - JSON
  - AppFabric menormalkan data menggunakan Open Cybersecurity Schema Framework (OCSF) dan mengeluarkan data dalam format JSON.
- OCSF - Parquet
  - AppFabric menormalkan data menggunakan Open Cybersecurity Schema Framework (OCSF) dan mengeluarkan data dalam format. Apache Parquet

Lokasi keluaran

Splunkmendukung lokasi AppFabric output berikut:

- Amazon Data Firehose
  - SplunkUntuk mengonfigurasi agar menerima log audit dari aliran Firehose yang berisi log audit Anda, ikuti petunjuk di SplunkAdd-on untuk Amazon Data Firehose di situs web. Splunk
- Amazon Simple Storage Service (Amazon S3)
  - SplunkUntuk mengonfigurasi agar menerima data dari bucket Amazon S3 yang berisi log audit Anda, ikuti petunjuk di Mengonfigurasi input S3 berbasis SQS untuk Add-on di situs web. Splunk AWSSplunk

Hapus AWS AppFabric untuk sumber daya keamanan

Jika Anda tidak ingin terus menggunakan AWS AppFabric untuk keamanan, pastikan untuk menghapus data di lokasi keluaran yang Anda buat selama penyiapan dan sumber daya keamanan Anda AppFabric untuk menghindari biaya tambahan. Untuk membersihkan AppFabric sumber daya Anda, Anda harus menghapus sumber daya dalam urutan terbalik di mana Anda membuatnya untuk setiap aplikasi perangkat lunak sebagai layanan (SaaS): Tujuan konsumsi > Konsumsi > Otorisasi aplikasi > Bundel aplikasi

Setelah menghapus otorisasi aplikasi akhir, Anda dapat menghapus bundel aplikasi.

Topik

Hapus tujuan konsumsi

Jika Anda memilih lokasi keluaran saat membuat konsumsi, AppFabric untuk keamanan akan membuat tujuan konsumsi atas nama Anda. Untuk menghapus tujuan konsumsi, gunakan langkah-langkah berikut:

1. Buka AppFabric konsol di https://console.aws.amazon.com/appfabric/.
2. Dari halaman Memulai, perluas menu di sebelah kiri.
3. Pilih Tertelan.
4. Pilih otorisasi aplikasi.

5. Pilih tombol opsi di sebelah tujuan yang ingin Anda hapus dan pilih Hapus.
6. Pilih Hapus pada kotak dialog tujuan hapus untuk mengonfirmasi.
7. Ulangi langkah-langkah di atas untuk semua tujuan Anda.

Hapus konsumsi

Untuk menghapus konsumsi, gunakan langkah-langkah berikut:

1. Dari halaman Memulai, perluas menu di sebelah kiri.
2. Pilih Tertelan.
3. Pilih tombol opsi yang ada di sebelah otorisasi aplikasi Anda.
4. Pilih menu dropdown Actions.
5. Pilih Hapus.
6. Pilih Hapus pada kotak dialog hapus konsumsi untuk mengonfirmasi.

Menghapus otorisasi aplikasi

Untuk menghapus otorisasi aplikasi, gunakan langkah-langkah berikut:

1. Dari halaman Memulai, perluas menu di sebelah kiri.
2. Pilih Otorisasi aplikasi.
3. Pilih tombol opsi di sebelah otorisasi aplikasi yang ingin Anda hapus.
4. Pilih menu dropdown Actions.
5. Pilih Hapus.
6. Pilih Hapus pada kotak dialog hapus konsumsi untuk mengonfirmasi.

Hapus bundel aplikasi

Untuk menghapus app bundle, gunakan langkah-langkah berikut:

1. Dari halaman Memulai, perluas menu di sebelah kiri.
2. Pilih Bundel aplikasi.
3. Pilih tombol Hapus.

4. Ketik `delete` untuk mengonfirmasi, lalu pilih Hapus.

Apa AWS AppFabric untuk produktivitas?

Fitur AWS AppFabric untuk produktivitas dalam pratinjau dan dapat berubah sewaktu-waktu.

> **Note**
>
> Didukung oleh Amazon Bedrock: AWS mengimplementasikan deteksi penyalahgunaan otomatis. Karena AWS AppFabric untuk produktivitas dibangun di Amazon Bedrock, pengguna mewarisi kontrol yang diterapkan di Amazon Bedrock untuk menegakkan keselamatan, keamanan, dan penggunaan AI yang bertanggung jawab.

AWS AppFabric untuk produktivitas (pratinjau) membantu menata kembali produktivitas pengguna akhir dalam aplikasi pihak ketiga dengan menghasilkan wawasan dan tindakan dengan konteks dari beberapa aplikasi. Pengembang aplikasi menyadari bahwa mengakses data pengguna dari aplikasi lain penting dalam menciptakan pengalaman aplikasi yang lebih produktif, tetapi mereka tidak ingin membangun dan mengelola integrasi dengan setiap aplikasi. Dengan AppFabric produktivitas, pengembang aplikasi mendapatkan akses ke API generatif yang didukung AI yang menghasilkan wawasan dan tindakan data lintas aplikasi sehingga mereka dapat memberikan pengalaman pengguna akhir yang lebih kaya melalui asisten AI generatif baru atau yang sudah ada. AppFabric untuk produktivitas mengintegrasikan data dari beberapa aplikasi menghilangkan kebutuhan pengembang untuk membangun atau memelihara point-to-point integrasi. Pengembang aplikasi dapat menyematkan AppFabric produktivitas langsung ke UI aplikasi mereka, mempertahankan pengalaman yang konsisten untuk pengguna akhir mereka sambil memunculkan konteks yang relevan dari aplikasi lain.

AppFabric untuk produktivitas menghubungkan data dari aplikasi yang umum digunakan sepertiAsana,,Atlassian Jira Suite,Google Workspace,Microsoft 365,Miro, SlackSmartsheet, dan banyak lagi. AppFabric Untuk produktivitas memberi pengembang aplikasi cara yang lebih mudah untuk membangun pengalaman aplikasi yang lebih personal yang meningkatkan adopsi, kepuasan, dan loyalitas pengguna. Sementara itu, pengguna akhir mendapat manfaat dari mengakses wawasan yang mereka butuhkan dari seluruh aplikasi mereka tanpa mengganggu alur kerja mereka.

Topik

Manfaat

Dengan AppFabric produktivitas, pengembang aplikasi mendapatkan akses ke API yang menghasilkan wawasan dan tindakan data lintas aplikasi sehingga mereka dapat memberikan pengalaman pengguna akhir yang lebih kaya melalui asisten AI generatif baru atau yang sudah ada.

- Sumber tunggal data pengguna lintas aplikasi: AppFabric untuk produktivitas mengintegrasikan data dari beberapa aplikasi yang menghilangkan kebutuhan pengembang untuk membangun atau memelihara point-to-point integrasi. Data aplikasi SaaS diproses untuk digunakan dalam aplikasi lain dengan secara otomatis menormalkan tipe data yang berbeda ke dalam format yang dapat dimengerti oleh aplikasi apa pun, memungkinkan pengembang aplikasi untuk memasukkan lebih banyak data yang benar-benar meningkatkan produktivitas pengguna akhir.
- Kontrol penuh atas pengalaman pengguna: Pengembang menyematkan AppFabric produktivitas langsung ke UI aplikasi mereka, mempertahankan kontrol penuh atas pengalaman pengguna sambil memberikan wawasan yang dipersonalisasi dan tindakan yang direkomendasikan kepada pengguna akhir dengan konteks dari seluruh aplikasi mereka. Ini membuat AppFabric produktivitas tersedia di aplikasi SaaS pilihan pengguna akhir dan dapat diakses di aplikasi yang mereka sukai untuk menyelesaikan tugas mereka. Pengguna akhir menghabiskan lebih sedikit waktu untuk beralih antar aplikasi, dan dapat tetap mengikuti alur pekerjaan mereka.
- Mempercepat waktu ke pasar: Dalam satu panggilan API, pengembang aplikasi dapat menerima wawasan tingkat pengguna di seluruh data pengguna yang dihasilkan tanpa harus menyempurnakan model, menulis prompt khusus, atau membangun integrasi di beberapa aplikasi. AppFabric mengabstraksi kompleksitas ini untuk memungkinkan pengembang aplikasi membangun, menyematkan, atau memperkaya kemampuan AI generatif lebih cepat. Hal ini memungkinkan pengembang aplikasi untuk fokus pada sumber daya mereka pada tugas-tugas yang paling penting.

- Referensi artifak untuk membangun kepercayaan pengguna: Sebagai bagian dari output, AppFabric untuk produktivitas akan memunculkan artefak yang relevan atau file sumber yang digunakan untuk menghasilkan wawasan guna membangun kepercayaan pengguna akhir pada output LLM.
- Izin pengguna yang disederhanakan: Artefak pengguna yang digunakan untuk menghasilkan wawasan didasarkan pada akses pengguna. AppFabric Untuk produktivitas menggunakan izin ISV dan kontrol akses sebagai sumber kebenaran.

Kasus penggunaan

Pengembang aplikasi dapat menggunakan produktivitas AppFabric untuk menata kembali produktivitas di dalam aplikasi mereka. AppFabric untuk produktivitas menawarkan dua API yang berfokus pada kasus penggunaan berikut untuk membantu pengguna akhir mereka menjadi lebih produktif:

- Prioritaskan hari Anda
  - API wawasan yang dapat ditindaklanjuti membantu pengguna mengelola hari mereka dengan memunculkan wawasan tepat waktu dari seluruh aplikasi mereka termasuk email, kalender, pesan, tugas, dan banyak lagi. Selain itu, pengguna dapat melakukan tindakan lintas aplikasi seperti membuat email, menjadwalkan rapat, dan membuat item tindakan dari aplikasi pilihan mereka. Misalnya, seorang karyawan yang mengalami eskalasi pelanggan dalam semalam tidak hanya akan melihat ringkasan percakapan semalam, tetapi juga akan dapat melihat tindakan yang disarankan untuk menjadwalkan pertemuan dengan Manajer Akun pelanggan. Tindakan diisi sebelumnya dengan bidang wajib (seperti nama tugas dan pemilik, atau pengirim/penerima email), dengan kemampuan untuk mengedit konten yang telah diisi sebelumnya sebelum menjalankan tindakan.
- Mempersiapkan pertemuan mendatang
  - API persiapan rapat membantu pengguna mempersiapkan rapat dengan merangkum tujuan pertemuan dan menampilkan artefak lintas aplikasi yang relevan seperti email, pesan, dan lainnya. Pengguna dapat dengan cepat mempersiapkan rapat sekarang dan tidak membuang waktu beralih antar aplikasi untuk menemukan konten.

Mengakses AppFabric produktivitas

AppFabric untuk produktivitas saat ini diluncurkan sebagai pratinjau dan tersedia di AS Timur (Virginia N.) Wilayah AWS. Untuk informasi selengkapnya Wilayah AWS, lihat AWS AppFabric titik akhir dan kuota di. Referensi Umum AWS

Di setiap Wilayah, Anda dapat mengakses AppFabric produktivitas dengan salah satu cara berikut:

- Sebagai pengembang aplikasi
  - Memulai AppFabric untuk produktivitas (pratinjau) untuk pengembang aplikasi
- Sebagai pengguna akhir
  - Memulai AppFabric untuk produktivitas (pratinjau) untuk pengguna akhir

Memulai AppFabric untuk produktivitas (pratinjau) untuk pengembang aplikasi

Fitur AWS AppFabric untuk produktivitas dalam pratinjau dan dapat berubah sewaktu-waktu.

Bagian ini membantu pengembang aplikasi mengintegrasikan AWS AppFabric produktivitas (pratinjau) ke dalam aplikasi mereka. AWS AppFabric Untuk produktivitas memungkinkan pengembang untuk membangun pengalaman aplikasi yang lebih kaya bagi penggunanya dengan menghasilkan wawasan dan tindakan yang didukung AI dari email, acara kalender, tugas, pesan, dan lainnya di beberapa aplikasi. Untuk daftar aplikasi yang didukung, lihat Aplikasi yang AWS AppFabric Didukung.

AppFabric Untuk produktivitas menawarkan pengembang aplikasi akses untuk membangun dan bereksperimen dalam lingkungan yang aman dan terkendali. Ketika Anda pertama kali mulai menggunakan AppFabric untuk produktivitas, Anda membuat AppClient dan mendaftarkan pengguna uji tunggal. Pendekatan ini dirancang untuk membantu Anda memahami dan menguji aliran otentikasi dan komunikasi antara aplikasi Anda dan AppFabric aplikasi. Setelah Anda menguji dengan satu pengguna, Anda dapat mengirimkan aplikasi Anda AppFabric untuk verifikasi sebelum memperluas akses ke pengguna tambahan (lihatLangkah 5. Permintaan AppFabric untuk memverifikasi aplikasi Anda). AppFabric akan memverifikasi informasi aplikasi sebelum memungkinkan adopsi yang tersebar luas untuk membantu melindungi pengembang aplikasi, pengguna akhir, dan data mereka — membuka jalan untuk memperluas adopsi pengguna dengan cara yang bertanggung jawab.

Topik

Prasyarat

Sebelum Anda memulai, Anda perlu membuat Akun AWS. Untuk informasi selengkapnya, lihat Mendaftar untuk Akun AWS. Anda juga perlu membuat setidaknya satu pengguna dengan akses ke kebijakan `"appfabric:CreateAppClient"` IAM yang tercantum di bawah ini, yang memungkinkan pengguna untuk mendaftarkan aplikasi Anda. AppFabric Untuk informasi selengkapnya tentang pemberian izin untuk fitur produktivitas, lihat. AppFabric AppFabric untuk contoh IAM kebijakan produktivitas Meskipun memiliki pengguna administratif bermanfaat, itu tidak wajib untuk pengaturan awal. Untuk informasi selengkapnya, lihat Buat pengguna dengan akses administratif.

AppFabric untuk produktivitas hanya di AS Timur (Virginia N.) selama pratinjau. Pastikan Anda berada di wilayah ini sebelum memulai langkah-langkah di bawah ini.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:CreateAppClient"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Langkah 1. Ciptakan AppFabric untuk produktivitas AppClient

Sebelum Anda dapat mulai AppFabric memunculkan wawasan produktivitas dalam aplikasi Anda, Anda perlu membuat file. AppFabric AppClient An pada dasarnya AppClient adalah gateway Anda AppFabric untuk produktivitas, berfungsi sebagai klien aplikasi OAuth aman yang memungkinkan komunikasi aman antara aplikasi Anda dan aplikasi. AppFabric Saat Anda membuat AppClient, Anda akan diberikan AppClient ID, pengenal unik yang penting untuk memastikan AppFabric bahwa itu berfungsi dengan aplikasi Anda dan Anda Akun AWS.

AppFabric Untuk produktivitas menawarkan pengembang aplikasi akses untuk membangun dan bereksperimen dalam lingkungan yang aman dan terkendali. Ketika Anda pertama kali mulai menggunakan AppFabric untuk produktivitas, Anda membuat AppClient dan mendaftarkan pengguna uji tunggal. Pendekatan ini dirancang untuk membantu Anda memahami dan menguji aliran otentikasi dan komunikasi antara aplikasi Anda dan AppFabric aplikasi. Setelah Anda menguji dengan satu pengguna, Anda dapat mengirimkan aplikasi Anda AppFabric untuk verifikasi sebelum memperluas akses ke pengguna tambahan (lihatLangkah 5. Permintaan AppFabric untuk memverifikasi aplikasi Anda). AppFabric akan memverifikasi informasi aplikasi sebelum memungkinkan adopsi yang tersebar luas untuk membantu melindungi pengembang aplikasi, pengguna akhir, dan data mereka — membuka jalan untuk memperluas adopsi pengguna dengan cara yang bertanggung jawab.

Untuk membuat AppClient, gunakan operasi AWS AppFabric `CreateAppClient` API. Jika Anda perlu memperbarui AppClient setelahnya, Anda dapat menggunakan operasi `UpdateAppClient` API untuk mengubah hanya redirecTurls. Jika Anda perlu mengubah salah satu parameter lain yang terkait dengan Anda AppClient seperti AppName atau deskripsi, Anda harus menghapus AppClient dan membuat yang baru. Untuk informasi selengkapnya, lihat CreateAppClient.

Anda dapat mendaftarkan aplikasi Anda dengan AWS layanan menggunakan `CreateAppClient` API menggunakan beberapa bahasa pemrograman, termasuk Python, Node.js, Java, C #, Go dan Rust. Untuk informasi selengkapnya, lihat Meminta contoh tanda tangan di Panduan Pengguna IAM. Anda perlu menggunakan kredensyal versi 4 tanda tangan akun Anda untuk melakukan operasi API ini. Untuk informasi selengkapnya tentang tanda tangan versi 4, lihat Menandatangani permintaan AWS API di Panduan Pengguna IAM.

Bidang Permintaan

- `appName`- Nama aplikasi yang akan ditampilkan kepada pengguna di halaman persetujuan portal AppFabric pengguna. Halaman persetujuan meminta izin pengguna akhir untuk menampilkan AppFabric wawasan di dalam aplikasi Anda. Untuk detail tentang halaman persetujuan, lihatLangkah 2. Memberikan persetujuan bagi aplikasi untuk menampilkan wawasan.

- `description`- Deskripsi untuk aplikasi.
- `redirectUrls`- URI untuk mengarahkan pengguna akhir setelah otorisasi. Anda dapat menambahkan hingga 5 RedirecTurls. Misalnya, `https://localhost:8080`.
- `starterUserEmails`- Alamat email pengguna yang akan diizinkan mengakses untuk menerima wawasan sampai aplikasi diverifikasi. Hanya satu alamat email yang diizinkan. Misalnya, `anyuser@example.com`
- `customerManagedKeyIdentifier`(opsional) - ARN kunci yang dikelola pelanggan (dihasilkan oleh KMS) untuk digunakan untuk mengenkripsi data. Jika tidak ditentukan, maka kunci yang AWS AppFabric dikelola akan digunakan. Untuk informasi selengkapnya tentang Kunci milik AWS dan kunci yang dikelola pelanggan, lihat Kunci dan AWS kunci pelanggan di Panduan AWS Key Management Service Pengembang.

Bidang Respons

- `appClientArn`- Nama Sumber Daya Amazon (ARN) yang menyertakan ID. AppClient Misalnya, AppClient ID adalah`a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`.
- `verificationStatus`- Status AppClient verifikasi.
  - `pending_verification`- Verifikasi AppClient masih dalam proses dengan AppFabric. Sampai AppClient diverifikasi, hanya satu pengguna (ditentukan dalam`starterUserEmails`) yang dapat menggunakan file AppClient. Pengguna akan melihat pemberitahuan di portal AppFabric pengguna, diperkenalkan diLangkah 3. Tambahkan URL portal AppFabric pengguna ke aplikasi Anda, yang menunjukkan bahwa aplikasi tidak diverifikasi.
  - `verified`- Proses verifikasi telah berhasil diselesaikan oleh AppFabric dan sekarang sepenuhnya diverifikasi. AppClient
  - `rejected`- Proses verifikasi untuk AppClient ditolak oleh AppFabric. AppClient Tidak dapat digunakan oleh pengguna tambahan sampai proses verifikasi dimulai kembali dan diselesaikan dengan sukses.

```
curl --request POST \
  --header "Content-Type: application/json" \
  --header "X-Amz-Content-Sha256: <sha256_payload>" \
  --header "X-Amz-Security-Token: <security_token>" \
  --header "X-Amz-Date: 20230922T172215Z" \
  --header "Authorization: AWS4-HMAC-SHA256 ..." \
  --url https://appfabric.<region>.amazonaws.com/appclients/ \
  --data '{
```

```
    "appName": "Test App",
    "description": "This is a test app",
    "redirectUrls": ["https://localhost:8080"],
    "starterUserEmails": ["anyuser@example.com"],
    "customerManagedKeyIdentifier": "arn:aws:kms:<region>:<account>:key/<key>"
}'
```

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

```
{
    "appClientConfigSummary": {
        "appClientArn": "arn:aws:appfabric:<region>:<account>:appclient/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "verificationStatus": "pending_verification"
    }
}
```

Langkah 2. Otentikasi dan otorisasi aplikasi Anda

Aktifkan aplikasi Anda untuk mengintegrasikan AppFabric wawasan dengan aman dengan membuat alur otorisasi OAuth 2.0. Pertama, Anda perlu membuat kode otorisasi, yang memverifikasi identitas aplikasi Anda. Untuk informasi selengkapnya, lihat Otorisasi. Kemudian Anda akan menukar kode otorisasi ini dengan token akses, yang memberikan izin kepada aplikasi Anda untuk mengambil dan menampilkan AppFabric wawasan dalam aplikasi Anda. Untuk informasi selengkapnya, lihat Token.

Untuk informasi selengkapnya tentang pemberian izin untuk mengotorisasi aplikasi, lihat. Izinkan akses untuk mengotorisasi aplikasi

1. Untuk membuat kode otorisasi, gunakan operasi AWS AppFabric `oauth2/authorize` API.

   Bidang Permintaan

   - `app_client_id`(wajib) - AppClient ID untuk yang Akun AWS dibuat di Langkah 1. Buat sebuah AppClient. Misalnya, `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`.
   - `redirect_uri`(wajib) - URI untuk mengarahkan pengguna akhir setelah otorisasi yang Anda gunakan pada Langkah 1. Buat sebuah AppClient. Misalnya, `https://localhost:8080`.
   - `state`(required) - Nilai unik untuk mempertahankan status antara permintaan dan callback. Misalnya, `a8904edc-890c-1005-1996-29a757272a44`.

```
GET https://productivity.appfabric.<region>.amazonaws.com/oauth2/authorize?
app_client_id=a1b2c3d4-5678-90ab-cdef-EXAMPLE11111\
redirect_uri=https://localhost:8080&state=a8904edc-890c-1005-1996-29a757272a44
```

2. Setelah otentikasi, Anda akan diarahkan ke URI yang ditentukan dengan kode otorisasi yang dikembalikan sebagai parameter kueri. Misalnya, di `manacode=mM0NyJ9.MEUCIHQQgV3ChXGs2LRwxLtpsgya3ybfPYXfX-sxTAdRF-gDAiEAxX7BYKlD9krG3J2VtprOjVXZ0FSUX9whdekqJ-oampc`.

```
https://localhost:8080/?code=mM0NyJ9.MEUCIHQQgV3ChXGs2LRwxLtpsgya3ybfPYXfX-
sxTAdRF-gDAiEAxX7BYKlD9krG3J2VtprOjVXZ0FSUX9whdekqJ-
oampc&state=a8904edc-890c-1005-1996-29a757272a44
```

3. Tukarkan kode otorisasi ini dengan token akses menggunakan operasi AppFabric `oauth2/token` API.

   Token ini digunakan untuk permintaan API dan awalnya valid untuk `starterUserEmails` sampai AppClient diverifikasi. Setelah AppClient diverifikasi, token ini dapat digunakan untuk setiap pengguna. Anda perlu menggunakan kredensyal versi 4 tanda tangan akun Anda untuk melakukan operasi API ini. Untuk informasi selengkapnya tentang tanda tangan versi 4, lihat Menandatangani permintaan AWS API di Panduan Pengguna IAM.

   Bidang Permintaan

   - `code`(wajib) - Kode otorisasi yang Anda terima setelah mengautentikasi pada langkah terakhir. Misalnya, `mM0NyJ9.MEUCIHQQgV3ChXGs2LRwxLtpsgya3ybfPYXfX-sxTAdRF-gDAiEAxX7BYKlD9krG3J2VtprOjVXZ0FSUX9whdekqJ-oampc`.
   - `app_client_id`(wajib) - AppClient ID untuk yang Akun AWS dibuat di Langkah 1. Buat sebuah AppClient. Misalnya, `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`.
   - `grant_type`(wajib) - Nilai harus`authorization_code`.
   - `redirect_uri`(wajib) - URI untuk mengarahkan pengguna setelah otorisasi yang Anda gunakan pada Langkah 1. Buat sebuah AppClient. Ini harus URI pengalihan yang sama yang digunakan untuk membuat kode otorisasi. Misalnya, `https://localhost:8080`.

   Bidang Respons

- `expires_in`- Seberapa cepat sebelum token kedaluwarsa. Waktu kedaluwarsa default adalah 12 jam.
- `refresh_token`- Token penyegaran yang diterima dari permintaan /token awal.
- `token`- Token yang diterima dari permintaan /token awal.
- `token_type`- Nilainya akan`Bearer`.
- `appfabric_user_id`- Id AppFabric pengguna. Ini dikembalikan hanya untuk permintaan yang menggunakan jenis `authorization_code` hibah.

```
curl --location \
"https://appfabric.<region>.amazonaws.com/oauth2/token" \
--header "Content-Type: application/json" \
--header "X-Amz-Content-Sha256: <sha256_payload>" \
--header "X-Amz-Security-Token: <security_token>" \
--header "X-Amz-Date: 20230922T172215Z" \
--header "Authorization: AWS4-HMAC-SHA256 ..." \
--data "{
    \"code\": \"mM0NyJ9.MEUCIHQQgV3ChXGs2LRwxLtpsgya3ybfPYXfX-sxTAdRF-
gDAiEAxX7BYKlD9krG3J2VtprOjVXZ0FSUX9whdekqJ-oampc",
    \"app_client_id\": \"a1b2c3d4-5678-90ab-cdef-EXAMPLE11111\",
    \"grant_type\": \"authorization_code\",
    \"redirect_uri\": \"https://localhost:8080\"
}"
```

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

```
{
    "expires_in": 43200,
    "refresh_token": "apkaeibaerjr2example",
    "token": "apkaeibaerjr2example",
    "token_type": "Bearer",
    "appfabric_user_id" : "<userId>"
}
```

Langkah 3. Tambahkan URL portal AppFabric pengguna ke aplikasi Anda

Pengguna akhir perlu mengotorisasi AppFabric untuk mengakses data dari aplikasi mereka yang digunakan untuk menghasilkan wawasan. AppFabric menghilangkan kerumitan bagi pengembang

aplikasi untuk memiliki proses ini dengan membangun portal pengguna khusus (layar pop-up) bagi pengguna akhir untuk mengotorisasi aplikasi mereka. Ketika pengguna siap AppFabric untuk mengaktifkan produktivitas, mereka akan dibawa ke portal pengguna yang memungkinkan mereka untuk menghubungkan dan mengelola aplikasi yang digunakan untuk menghasilkan wawasan dan tindakan lintas aplikasi. Saat masuk, pengguna dapat menghubungkan aplikasi AppFabric untuk produktivitas dan kemudian kembali ke aplikasi Anda untuk menjelajahi wawasan dan tindakan. Untuk mengintegrasikan aplikasi Anda dengan AppFabric produktivitas, Anda perlu menambahkan AppFabric URL tertentu ke aplikasi Anda. Langkah ini sangat penting untuk memungkinkan pengguna mengakses portal AppFabric pengguna langsung dari aplikasi Anda.

1. Arahkan ke pengaturan aplikasi Anda dan temukan bagian untuk menambahkan URL pengalihan.
2. Setelah Anda menemukan area yang sesuai, tambahkan AppFabric URL berikut sebagai URL pengalihan ke aplikasi Anda:

```
https://userportal.appfabric.<region>.amazonaws.com/eup_login
```

Setelah Anda menambahkan URL, aplikasi Anda akan diatur untuk mengarahkan pengguna ke portal AppFabric pengguna. Di sini, pengguna dapat masuk dan terhubung serta mengelola aplikasi mereka yang digunakan AppFabric untuk menghasilkan wawasan produktivitas.

Langkah 4. Gunakan AppFabric untuk memunculkan wawasan dan tindakan lintas aplikasi

Setelah pengguna menghubungkan aplikasi mereka, Anda dapat membawa wawasan pengguna Anda untuk meningkatkan produktivitas mereka dengan membantu mengurangi peralihan aplikasi dan konteks. AppFabric hanya menghasilkan wawasan untuk pengguna berdasarkan apa yang pengguna memiliki izin untuk mengakses. AppFabric menyimpan data pengguna yang Akun AWS dimiliki oleh AppFabric. Untuk informasi tentang cara AppFabric menggunakan data Anda, lihatPemrosesan data.

Anda dapat menggunakan API yang didukung AI berikut untuk menghasilkan dan menampilkan wawasan dan tindakan tingkat pengguna dalam aplikasi Anda:

- `ListActionableInsights`— Untuk informasi selengkapnya, lihat bagian Wawasan yang dapat ditindaklanjuti di bawah ini.

- `ListMeetingInsights`— Untuk informasi lebih lanjut, lihat bagian Persiapan Rapat nanti di panduan ini.

Wawasan yang dapat ditindaklanjuti () **`ListActionableInsights`**

`ListActionableInsights`API membantu pengguna mengelola wawasan yang dapat ditindaklanjuti dengan sebaik-baiknya berdasarkan aktivitas di seluruh aplikasi mereka, termasuk email, kalender, pesan, tugas, dan lainnya. Wawasan yang dikembalikan juga akan menampilkan tautan tertanam ke artefak yang digunakan untuk menghasilkan wawasan — membantu pengguna melihat data apa yang digunakan untuk menghasilkan wawasan dengan cepat. Selain itu, API dapat menampilkan tindakan yang disarankan berdasarkan wawasan dan memungkinkan pengguna untuk menjalankan tindakan lintas aplikasi dari dalam aplikasi Anda. Secara khusus, API terintegrasi dengan platform sepertiAsana,, Google WorkspaceMicrosoft 365, dan Smartsheet untuk memungkinkan pengguna mengirim email, membuat acara kalender, dan membuat tugas. Model bahasa besar (LLM) dapat mengisi detail sebelumnya dalam tindakan yang disarankan (seperti badan email atau nama tugas), yang dapat disesuaikan pengguna sebelum eksekusi — menyederhanakan pengambilan keputusan dan meningkatkan produktivitas. Mirip dengan pengalaman bagi pengguna akhir untuk mengotorisasi aplikasi, AppFabric menggunakan portal khusus yang sama bagi pengguna untuk melihat, mengedit, dan menjalankan tindakan lintas aplikasi. Untuk mengeksekusi tindakan, ISV harus mengarahkan ulang pengguna ke portal AppFabric pengguna di mana mereka dapat melihat detail tindakan dan AppFabric menjalankannya. Setiap tindakan yang dihasilkan oleh AppFabric memiliki URL yang unik. URL ini tersedia dalam respons respons `ListActionableInsights` API.

Di bawah ini adalah ringkasan tindakan lintas aplikasi yang didukung dan aplikasi mana:

- Kirim email (Google Workspace,Microsoft 365)
- Membuat kalender acara (Google Workspace,Microsoft 365)
- Buat tugas (Asana,Smartsheet)

Bidang Permintaan

- `nextToken`(opsional) - Token pagination untuk mengambil kumpulan wawasan berikutnya.
- `includeActionExecutionStatus`- Filter yang menerima daftar status eksekusi tindakan. Tindakan disaring berdasarkan nilai status yang diteruskan. Nilai yang mungkin: `NOT_EXECUTED` | `EXECUTED`

Permintaan Header

- Header otorisasi harus diteruskan dengan `Bearer Token` nilai.

Bidang Respons

- `insightId`- Id unik untuk wawasan yang dihasilkan.
- `insightContent`- Ini mengembalikan ringkasan wawasan dan tautan tertanam ke artefak yang digunakan untuk menghasilkan wawasan. Catatan: Ini akan menjadi konten HTML yang berisi tautan tertanam (<a>tag).
- `insightTitle`- Judul wawasan yang dihasilkan.
- `createdAt`- Saat wawasan dihasilkan.
- `actions`- Daftar tindakan yang direkomendasikan untuk wawasan yang dihasilkan. Objek aksi:
  - `actionId`- Id unik untuk tindakan yang dihasilkan.
  - `actionIconUrl`- URL ikon untuk aplikasi tempat tindakan disarankan untuk dijalankan.
  - `actionTitle`- Judul tindakan yang dihasilkan.
  - `actionUrl`- URL unik untuk pengguna akhir untuk melihat dan menjalankan tindakan di AppFabric portal pengguna. Catatan: untuk menjalankan tindakan, aplikasi ISV akan mengarahkan ulang pengguna ke portal AppFabric pengguna (layar pop up) menggunakan URL ini.
  - `actionExecutionStatus`- Enum yang menunjukkan status tindakan. Nilai yang mungkin adalah: `EXECUTED` | `NOT_EXECUTED`
- `nextToken`(opsional) - Token pagination untuk mengambil kumpulan wawasan berikutnya. Ini adalah bidang opsional yang jika dikembalikan null berarti tidak ada lagi wawasan untuk dimuat.

Untuk informasi selengkapnya, lihat ActionableInsights.

```
curl -v --location \
  "https://productivity.appfabric.<region>.amazonaws.com"\
"/actionableInsights" \
  --header "Authorization: Bearer <token>"
```

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

```
200 OK
```

```
{
    "insights": [
        {
            "insightId": "7tff3412-33b4-479a-8812-30EXAMPLE1111",
            "insightContent": "You received an email from James
            regarding providing feedback
            for upcoming performance reviews.",
            "insightTitle": "New feedback request",
            "createdAt": 2022-10-08T00:46:31.378493Z,
            "actions": [
                {
                    "actionId": "5b4f3412-33b4-479a-8812-3EXAMPLE2222",
                    "actionIconUrl": "https://d3gdwnnn63ow7w.cloudfront.net/
eup/123.svg",
                    "actionTitle": "Send feedback request email",
                    "actionUrl": "https://userportal.appfabric.us-east-1.amazonaws.com/
action/action_id_1"
                    "actionExecutionStatus": "NOT_EXECUTED"
                }
            ]
        },
        {
            "insightId": "2dff3412-33b4-479a-8812-30bEXAMPLE3333",
            "insightContent":"Steve sent you an email asking for details on project.
 Consider replying to the email.",
            "insightTitle": "New team launch discussion",
            "createdAt": 2022-10-08T00:46:31.378493Z,
            "actions": [
                {
                    "actionId": "74251e31-5962-49d2-9ca3-1EXAMPLE1111",
                    "actionIconUrl": "https://d3gdwnnn63ow7w.cloudfront.net/
eup/123.svg",
                    "actionTitle": "Reply to team launch email",
                    "actionUrl": "https://userportal.appfabric.us-east-1.amazonaws.com/
action/action_id_2"
                    "actionExecutionStatus": "NOT_EXECUTED"
                }
            ]
        }
    ],
    "nextToken": null
}
```

Persiapan rapat (**`ListMeetingInsights`**)

`ListMeetingInsights`API membantu pengguna mempersiapkan diri terbaik untuk pertemuan mendatang dengan meringkas tujuan pertemuan dan menampilkan artefak lintas aplikasi yang relevan seperti email, pesan, dan banyak lagi. Pengguna dapat dengan cepat mempersiapkan rapat sekarang dan tidak membuang waktu beralih antar aplikasi untuk menemukan konten.

Bidang Permintaan

- `nextToken`(opsional) - Token pagination untuk mengambil kumpulan wawasan berikutnya.

Permintaan Header

- Header otorisasi harus diteruskan dengan `Bearer Token` nilai.

Bidang Respons

- `insightId`- Id unik untuk wawasan yang dihasilkan.
- `insightContent`- Deskripsi wawasan yang menyoroti detail dalam format string. Seperti, mengapa wawasan ini penting.
- `insightTitle`- Judul wawasan yang dihasilkan.
- `createdAt`- Saat wawasan dihasilkan.
- `calendarEvent`- Acara atau rapat kalender penting yang harus difokuskan pengguna. Kalender objek Acara:
  - `startTime`- Waktu mulai acara.
  - `endTime`- Waktu akhir acara.
  - `eventUrl`- URL untuk acara kalender di aplikasi ISV.
- `resources`- Daftar yang berisi sumber daya lain yang terkait dengan menghasilkan wawasan. Objek sumber daya:
  - `appName`- Nama aplikasi tempat sumber daya berada.
  - `resourceTitle`- Judul sumber daya.
  - `resourceType`- Jenis sumber daya. Nilai yang mungkin adalah: `EMAIL` | `EVENT` | `MESSAGE` | `TASK`
  - `resourceUrl`- URL sumber daya di aplikasi.
  - `appIconUrl`- URL gambar aplikasi tempat sumber daya berada.

- `nextToken`(opsional) - Token pagination untuk mengambil kumpulan wawasan berikutnya. Ini adalah bidang opsional yang jika dikembalikan null berarti tidak ada lagi wawasan untuk dimuat.

Untuk informasi selengkapnya, lihat MeetingInsights.

```
curl --location \
  "https://productivity.appfabric.<region>.amazonaws.com"\
"/meetingContexts" \
  --header "Authorization: Bearer <token>"
```

Jika tindakan berhasil, layanan mengirimkan kembali respon HTTP 201.

```
200 OK

{
    "insights": [
        {
            "insightId": "74251e31-5962-49d2-9ca3-15EXAMPLE4444"
            "insightContent": "Project demo meeting coming up soon. Prepare
 accordingly",
            "insightTitle": "Demo meeting next week",
            "createdAt": 2022-10-08T00:46:31.378493Z,
            "calendarEvent": {
                    "startTime": {
                        "timeInUTC": 2023-10-08T10:00:00.000000Z,
                        "timeZone": "UTC"
                     },
                    "endTime": {
                        "timeInUTC": 2023-10-08T11:00:00.000000Z,
                        "timeZone": "UTC"
                     },
                    "eventUrl": "http://someapp.com/events/1234",
            }
            "resources": [
                {
                    "appName": "SOME_EMAIL_APP",
                    "resourceTitle": "Email for project demo",
                    "resourceType": "EMAIL",
                    "resourceUrl": "http://someapp.com/emails/1234",
                    "appIconUrl":"https://d3gdwnnn63ow7w.cloudfront.net/eup/123.svg"
                }
            ]
```

```
        },
        {
            "insightId": "98751e31-5962-49d2-9ca3-15EXAMPLE5555"
            "insightContent": "Important code complete task is now due. Consider
 updating the status.",
            "insightTitle": "Code complete task is due",
            "createdAt": 2022-10-08T00:46:31.378493Z,
            "calendarEvent":{
                    "startTime": {
                        "timeInUTC": 2023-10-08T10:00:00.000000Z,
                        "timeZone": "UTC"
                     },
                    "endTime": {
                        "timeInUTC": 2023-10-08T11:00:00.000000Z,
                        "timeZone": "UTC"
                     },
                    "eventUrl": "http://someapp.com/events/1234",
            },
            "resources": [
                {
                    "appName": "SOME_TASK_APPLICATION",
                    "resourceTitle": "Code Complete task is due",
                    "resourceType": "TASK",
                    "resourceUrl": "http://someapp.com/task/1234",
                    "appIconUrl": "https://d3gdwnnn63ow7w.cloudfront.net/eup/123.svg"
                }
            ]
        }
    ],
    "nextToken": null
}
```

Berikan umpan balik untuk wawasan atau tindakan Anda

Gunakan operasi AppFabric `PutFeedback` API untuk memberikan umpan balik untuk wawasan dan tindakan yang dihasilkan. Anda dapat menyematkan fitur ini di aplikasi Anda untuk memberikan cara untuk mengirimkan peringkat umpan balik (1 hingga 5, di mana peringkat yang lebih tinggi semakin baik) untuk yang diberikan InsightId atau ActionId.

Bidang permintaan

- `id`- Pengidentifikasi objek yang umpan baliknya dikirimkan. Ini bisa berupa InsightId atau ActionId.

- `feedbackFor`- Jenis sumber daya yang umpan balik dikirimkan. Nilai yang mungkin: `ACTIONABLE_INSIGHT` | `MEETING_INSIGHT` | `ACTION`
- `feedbackRating`- Peringkat umpan balik dari 1 ke5. Rating yang lebih tinggi semakin baik.

Bidang respons

- Tidak ada bidang respons.

Untuk informasi selengkapnya, lihat PutFeedback.

```
curl --request POST \
  --url "https://productivity.appfabric.<region>.amazonaws.com"\
"/feedback" \
  --header "Authorization: Bearer <token>" \
  --header "Content-Type: application/json" \
  --data '{
    "id": "1234-5678-9012",
    "feedbackFor": "ACTIONABLE_INSIGHT"
    "feedbackRating": 3
}'
```

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 201 dengan badan HTTP kosong.

Langkah 5. Permintaan AppFabric untuk memverifikasi aplikasi Anda

Untuk titik ini, Anda telah memperbarui UI aplikasi untuk menyematkan wawasan dan tindakan AppFabric lintas aplikasi, dan menerima wawasan untuk satu pengguna. Setelah puas dengan pengujian dan ingin memperluas pengalaman yang AppFabric diperkaya kepada pengguna tambahan, Anda dapat mengirimkan aplikasi Anda AppFabric untuk ditinjau dan diverifikasi. AppFabric akan memverifikasi informasi aplikasi sebelum memungkinkan adopsi yang tersebar luas untuk membantu melindungi pengembang aplikasi, pengguna akhir, dan data mereka — membuka jalan untuk memperluas adopsi pengguna dengan cara yang bertanggung jawab.

Memulai proses verifikasi

Mulailah proses verifikasi dengan mengirimkan email ke appfabric-appverification@amazon.com dan meminta agar aplikasi Anda diverifikasi.

Sertakan detail berikut di email Anda:

- Akun AWS ID Anda
- Nama aplikasi yang Anda cari verifikasi
- AppClient ID Anda
- Informasi kontak Anda

Selain itu, berikan informasi berikut, jika tersedia, untuk membantu kami menilai prioritas dan dampak:

- Perkiraan jumlah pengguna yang Anda rencanakan untuk memberikan akses
- Tanggal peluncuran target Anda

> **Note**
>
> Jika Anda memiliki Akun AWS manajer atau manajer pengembangan AWS mitra, silakan salin di email Anda. Menyertakan kontak ini dapat membantu mempercepat proses verifikasi.

Kriteria verifikasi

Sebelum memulai proses verifikasi, Anda harus memenuhi kriteria berikut:

- Anda harus menggunakan valid Akun AWS untuk digunakan AppFabric untuk produktivitas

Selain itu, Anda memenuhi setidaknya satu dari kriteria ini:

- Organisasi Anda adalah AWS mitra AWS Partner Network dengan setidaknya tingkat “AWS Pilih”. Untuk informasi selengkapnya, lihat AWS Tingkat Layanan Mitra.
- Organisasi Anda seharusnya menghabiskan setidaknya $10.000 untuk AppFabric layanan dalam tiga tahun terakhir.
- Aplikasi Anda harus terdaftar di AWS Marketplace. Untuk informasi selengkapnya, lihat AWS Marketplace.

Tunggu pembaruan status verifikasi

Setelah aplikasi Anda ditinjau, kami akan merespons melalui email dan status Anda AppClient akan berubah dari `pending_verification` menjadi`verified`. Jika aplikasi Anda ditolak, Anda harus memulai kembali proses verifikasi.

Mengelola AppFabric produktivitas AppClients

> Fitur AWS AppFabric untuk produktivitas dalam pratinjau dan dapat berubah sewaktu-waktu.

Anda dapat mengelola produktivitas Anda AppFabric AppClients untuk memastikan kelancaran operasi dan pemeliharaan proses otentikasi dan otorisasi.

Dapatkan detail dari AppClient

Gunakan operasi AppFabric `GetAppClient` API untuk melihat detail tentang Anda AppClient, termasuk memeriksa AppClient status. Untuk informasi selengkapnya, lihat GetAppClient.

Untuk mendapatkan detail AppClient, Anda harus memiliki, setidaknya, izin kebijakan `"appfabric:GetAppClient"` IAM. Untuk informasi selengkapnya, lihat Izinkan akses untuk mendapatkan detail AppClients.

Bidang Permintaan

- `appClientId`- AppClient Id.

Bidang Respons

- `appName`- Nama aplikasi yang akan ditampilkan kepada pengguna di halaman persetujuan portal AppFabric pengguna.
- `customerManagedKeyIdentifier`(opsional) - ARN dari Customer Managed Key (dihasilkan oleh KMS) untuk digunakan untuk mengenkripsi data. Jika tidak ditentukan, maka Kunci AWS AppFabric Terkelola akan digunakan.
- `description`- Deskripsi untuk aplikasi.
- `redirectUrls`- URI untuk mengarahkan pengguna akhir setelah otorisasi. Anda dapat menambahkan hingga 5 RedirecTurls. Misalnya, `https://localhost:8080`.
- `starterUserEmails`- Alamat email pengguna yang akan diizinkan mengakses untuk menerima wawasan sampai aplikasi diverifikasi. Hanya satu alamat email yang diizinkan. Misalnya, `anyuser@example.com`.

- `verificationStatus`- Status AppClient verifikasi.
  - `pending_verification`- Verifikasi AppClient masih dalam proses dengan AppFabric. Sampai AppClient diverifikasi, hanya satu pengguna (ditentukan dalam`starterUserEmails`) yang dapat menggunakan file AppClient.
  - `verified`- Proses verifikasi telah berhasil diselesaikan oleh AppFabric dan sekarang sepenuhnya diverifikasi. AppClient
  - `rejected`- Proses verifikasi untuk AppClient ditolak oleh AppFabric. AppClient Tidak dapat digunakan oleh pengguna tambahan sampai proses verifikasi dimulai kembali dan diselesaikan dengan sukses.

```
curl --request GET \
  --header "Content-Type: application/json" \
  --header "X-Amz-Content-Sha256: <sha256_payload>" \
  --header "X-Amz-Security-Token: <security_token>" \
  --header "X-Amz-Date: 20230922T172215Z" \
  --header "Authorization: AWS4-HMAC-SHA256 ..." \
  --url https://appfabric.<region>.amazonaws.com/appclients/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111
```

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

```
200 OK

{
    "appClient": {
        "appName": "Test App",
        "arn": "arn:aws:appfabric:<region>:111122223333:appclient/a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111",
        "customerManagedKeyArn": "arn:aws:kms:<region>:111122223333:key/<key>",
        "description": "This is a test app",
        "redirectUrls": [
            "https://localhost:8080"
        ],
        "starterUserEmails": [
            "anyuser@example.com"
        ],
        "verificationDetails": {
            "verificationStatus": "pending_verification"
        }
    }
```

```
}
```

Daftar AppClients

Gunakan operasi AppFabric `ListAppClients` API untuk melihat daftar Anda AppClients. AppFabric hanya memungkinkan satu AppClient per Akun AWS. Ini dapat berubah di masa depan. Untuk informasi selengkapnya, lihat ListAppClients.

Untuk mendaftar AppClients, Anda harus memiliki, setidaknya, izin kebijakan `"appfabric:ListAppClients"` IAM. Untuk informasi selengkapnya, lihat Izinkan akses ke daftar AppClients.

Bidang Permintaan

- Tidak ada bidang wajib.

Bidang Respons

- `appClientARN`- Nama Sumber Daya Amazon (ARN) yang menyertakan ID. AppClient Misalnya, AppClient ID adalah`a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`.
- `verificationStatus`- Status AppClient verifikasi.
  - `pending_verification`- Verifikasi AppClient masih dalam proses dengan AppFabric. Sampai AppClient diverifikasi, hanya satu pengguna (ditentukan dalam`starterUserEmails`) yang dapat menggunakan file AppClient.
  - `verified`- Proses verifikasi telah berhasil diselesaikan oleh AppFabric dan sekarang sepenuhnya diverifikasi. AppClient
  - `rejected`- Proses verifikasi untuk AppClient ditolak oleh AppFabric. AppClient Tidak dapat digunakan oleh pengguna tambahan sampai proses verifikasi dimulai kembali dan diselesaikan dengan sukses.

```
curl --request GET \
  --header "Content-Type: application/json" \
  --header "X-Amz-Content-Sha256: <sha256_payload>" \
  --header "X-Amz-Security-Token: <security_token>" \
  --header "X-Amz-Date: 20230922T172215Z" \
  --header "Authorization: AWS4-HMAC-SHA256 ..." \
  --url https://appfabric.<region>.amazonaws.com/appclients
```

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

```
200 OK

{
    "appClientList": [
        {
            "appClientArn": "arn:aws:appfabric:<region>:111122223333:appclient/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "verificationStatus": "pending_verification"
        }
    ]
}
```

Perbarui AppClient

Gunakan operasi AppFabric `UpdateAppClient` API untuk memperbarui redirectUrls yang dipetakan ke Anda. AppClient Jika Anda perlu mengubah parameter lain, seperti AppName, starterUserEmails, atau lainnya, Anda harus menghapus AppClient dan membuat yang baru. Untuk informasi selengkapnya, lihat UpdateAppClient.

Untuk memperbarui AppClient, Anda harus memiliki, setidaknya, izin kebijakan `"appfabric:UpdateAppClient"` IAM. Untuk informasi selengkapnya, lihat Izinkan akses untuk memperbarui AppClients.

Bidang Permintaan

- `appClientId`(required) - AppClient ID yang Anda perbarui redirectUrls.
- `redirectUrls`(wajib) - Daftar RedirecTurls yang diperbarui. Anda dapat menambahkan hingga 5 RedirecTurls.

Bidang Respons

- `appName`- Nama aplikasi yang akan ditampilkan kepada pengguna di halaman persetujuan portal AppFabric pengguna.
- `customerManagedKeyIdentifier`(opsional) - ARN dari Customer Managed Key (dihasilkan oleh KMS) untuk digunakan untuk mengenkripsi data. Jika tidak ditentukan, maka Kunci AWS AppFabric Terkelola akan digunakan.
- `description`- Deskripsi untuk aplikasi.

- `redirectUrls`- URI untuk mengarahkan pengguna akhir setelah otorisasi. Misalnya, `https://localhost:8080`.
- `starterUserEmails`- Alamat email pengguna yang akan diizinkan mengakses untuk menerima wawasan sampai aplikasi diverifikasi. Hanya satu alamat email yang diizinkan. Misalnya, `anyuser@example.com`.
- `verificationStatus`- Status AppClient verifikasi.
  - `pending_verification`- Verifikasi AppClient masih dalam proses dengan AppFabric. Sampai AppClient diverifikasi, hanya satu pengguna (ditentukan dalam`starterUserEmails`) yang dapat menggunakan file AppClient.
  - `verified`- Proses verifikasi telah berhasil diselesaikan oleh AppFabric dan sekarang sepenuhnya diverifikasi. AppClient
  - `rejected`- Proses verifikasi untuk AppClient ditolak oleh AppFabric. AppClient Tidak dapat digunakan oleh pengguna tambahan sampai proses verifikasi dimulai kembali dan diselesaikan dengan sukses.

```
curl --request PATCH \
  --header "Content-Type: application/json" \
  --header "X-Amz-Content-Sha256: <sha256_payload>" \
  --header "X-Amz-Security-Token: <security_token>" \
  --header "X-Amz-Date: 20230922T172215Z" \
  --header "Authorization: AWS4-HMAC-SHA256 ..." \
  --url https://appfabric.<region>.amazonaws.com/appclients/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111 \
  --data '{
    "redirectUrls": ["https://localhost:8081"]
}'
```

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

```
200 OK

{
    "appClient": {
        "appName": "Test App",
        "arn": "arn:aws:appfabric:<region>:111122223333:appclient/a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111",
        "customerManagedKeyArn": "arn:aws:kms:<region>:111122223333:key/<key>",
        "description": "This is a test app",
```

```
        "redirectUrls": [
            "https://localhost:8081"
        ],
        "starterUserEmails": [
            "anyuser@example.com"
        ],
        "verificationDetails": {
            "verificationStatus": "pending_verification"
        }
    }
}
```

Menghapus AppClient

Gunakan operasi AppFabric `DeleteAppClient` API untuk menghapus apa pun yang tidak lagi AppClients Anda perlukan. Untuk informasi selengkapnya, lihat DeleteAppClient.

Untuk menghapus AppClient, Anda harus memiliki, setidaknya, izin kebijakan `"appfabric:DeleteAppClient"` IAM. Untuk informasi selengkapnya, lihat Izinkan akses untuk menghapus AppClients.

Bidang permintaan

- `appClientId`- AppClient Id.

Bidang respons

- Tidak ada bidang respons.

```
curl --request DELETE \
  --header "Content-Type: application/json" \
  --header "X-Amz-Content-Sha256: <sha256_payload>" \
  --header "X-Amz-Security-Token: <security_token>" \
  --header "X-Amz-Date: 20230922T172215Z" \
  --header "Authorization: AWS4-HMAC-SHA256 ..." \
  --url https://appfabric.<region>.amazonaws.com/appclients/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111
```

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 204 dengan isi HTTP kosong.

Segarkan token untuk pengguna akhir

Token yang Anda AppClient peroleh untuk pengguna akhir dapat di-refresh pada saat kedaluwarsa. Ini dapat dilakukan dengan menggunakan Token API dengan `refresh_token` grant_type. Yang `refresh_token` akan digunakan dikembalikan sebagai bagian dari respons API token saat grant_type. `authorization_code` Kedaluwarsa default adalah 12 jam. Untuk memanggil refresh API, Anda harus memiliki izin kebijakan `"appfabric:Token"` IAM. Untuk informasi selengkapnya, lihat Token dan Izinkan akses untuk memperbarui AppClients.

Bidang Permintaan

- `refresh_token`(wajib) - Token penyegaran yang diterima dari `/token` permintaan awal.
- `app_client_id`(wajib) - ID AppClient sumber daya yang dibuat untuk file Akun AWS.
- `grant_type`(wajib) - Ini harus`refresh_token`.

Bidang Respons

- `expires_in`- Seberapa cepat sebelum token kedaluwarsa. Waktu kedaluwarsa default adalah 12 jam.
- `refresh_token`- Token penyegaran yang diterima dari permintaan /token awal.
- `token`- Token yang diterima dari permintaan /token awal.
- `token_type`- Nilainya akan`Bearer`.
- `appfabric_user_id`- Id AppFabric pengguna. Ini dikembalikan hanya untuk permintaan yang menggunakan jenis `authorization_code` hibah.

```
curl --location \
"https://appfabric.<region>.amazonaws.com/oauth2/token" \
--header "Content-Type: application/json" \
--header "X-Amz-Content-Sha256: <sha256_payload>" \
--header "X-Amz-Security-Token: <security_token>" \
--header "X-Amz-Date: 20230922T172215Z" \
--header "Authorization: AWS4-HMAC-SHA256 ..." \
--data "{
    \"refresh_token\": \"<refresh_token>",
    \"app_client_id\": \"a1b2c3d4-5678-90ab-cdef-EXAMPLE11111\",
    \"grant_type\": \"refresh_token\"
}"
```

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

```
200 OK

{
    "expires_in": 43200,
    "token": "apkaeibaerjr2example",
    "token_type": "Bearer",
    "appfabric_user_id" : "${UserID}"
}
```

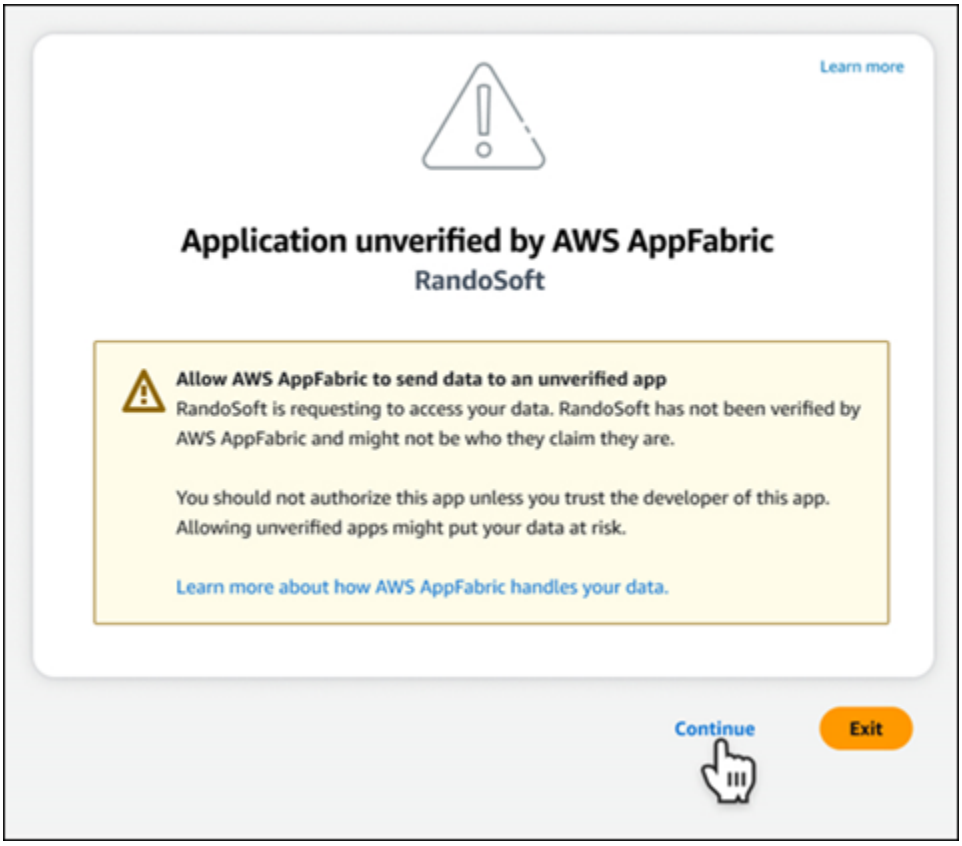
Pemecahan Masalah

Fitur AWS AppFabric untuk produktivitas dalam pratinjau dan dapat berubah sewaktu-waktu.

Bagian ini menjelaskan kesalahan umum dan pemecahan masalah AppFabric untuk produktivitas.

Aplikasi yang belum diverifikasi

Pengembang aplikasi yang menggunakan produktivitas AppFabric untuk memperkaya pengalaman aplikasi mereka akan melalui proses verifikasi sebelum meluncurkan fitur mereka ke pengguna akhir. Semua aplikasi dimulai sebagai tidak diverifikasi dan berubah menjadi diverifikasi hanya ketika proses verifikasi selesai. Ini berarti bahwa yang `starterUserEmails` Anda gunakan saat membuat AppClient akan melihat pesan ini.



Kesalahan **`CreateAppClient`**

ServiceQuotaExceededException

Jika Anda menerima pengecualian berikut saat membuat AppClient, Anda telah melebihi jumlah AppClients yang dapat dibuat per Akun AWS. Batasnya adalah 1. HTTPKode Status: 402

```
ServiceQuotaExceededException / SERVICE_QUOTA_EXCEEDED
You have exceeded the number of AppClients that can be created per AWS Account. The
 limit is 1.
HTTP Status Code: 402
```

Kesalahan **`GetAppClient`**

ResourceNotFoundException

Jika Anda menerima pengecualian berikut saat mendapatkan detail untuk sebuah AppClient, pastikan Anda telah memasukkan AppClient pengenal yang benar. Kesalahan ini menandakan bahwa yang ditentukan tidak AppClient ditemukan.

```
ResourceNotFoundException / APP_CLIENT_NOT_FOUND
```

```
The specified AppClient is not found. Ensure you've entered the correct AppClient
 identifier.
HTTP Status Code: 404
```

Kesalahan **DeleteAppClient**

ConflictException

Jika Anda menerima pengecualian berikut saat menghapus AppClient, permintaan penghapusan lainnya sedang berlangsung. Tunggu sampai selesai lalu coba lagi. HTTPKode Status: 409

```
ConflictException
Another delete request is in progress. Wait until it completes then try again.
HTTP Status Code: 409
```

ResourceNotFoundException

Jika Anda menerima pengecualian berikut saat menghapus AppClient, pastikan Anda telah memasukkan AppClient pengenal yang benar. Kesalahan ini menandakan bahwa yang ditentukan tidak AppClient ditemukan.

```
ResourceNotFoundException / APP_CLIENT_NOT_FOUND
The specified AppClient is not found. Ensure you've entered the correct AppClient
 identifier.
HTTP Status Code: 404
```

Kesalahan **UpdateAppClient**

ResourceNotFoundException

Jika Anda menerima pengecualian berikut saat memperbarui AppClient, pastikan Anda telah memasukkan AppClient pengenal yang benar. Kesalahan ini menandakan bahwa yang ditentukan tidak AppClient ditemukan.

```
ResourceNotFoundException / APP_CLIENT_NOT_FOUND
The specified AppClient is not found. Ensure you've entered the correct AppClient
 identifier.
HTTP Status Code: 404
```

Kesalahan **`Authorize`**

ValidationException

Anda mungkin menerima pengecualian berikut jika salah satu API parameter tidak memenuhi batasan yang ditentukan dalam spesifikasi. API

```
ValidationException
HTTP Status Code: 400
```

Alasan 1: Ketika AppClient ID tidak ditentukan

Yang `app_client_id` hilang dalam parameter permintaan. Buat AppClient jika belum dibuat atau gunakan yang sudah ada `app_client_id` dan coba lagi. Untuk menemukan AppClient ID, gunakan ListAppClientAPIoperasi.

Alasan 2: Kapan AppFabric tidak memiliki akses ke kunci yang dikelola pelanggan

```
Message: AppFabric couldn't access the customer managed key configured for AppClient.
```

AppFabric saat ini tidak dapat mengakses kunci yang dikelola pelanggan, kemungkinan karena perubahan terbaru dalam izinnya. Verifikasi kunci yang ditentukan ada dan pastikan AppFabric diberikan izin akses yang sesuai.

Alasan 3: Pengalihan URL yang ditentukan tidak valid

```
Message: Redirect url invalid
```

Pastikan pengalihan URL dalam permintaan Anda benar. Itu harus cocok dengan salah satu pengalihan URLs yang ditentukan saat Anda membuat atau memperbarui. AppClient Untuk melihat daftar pengalihan yang diizinkanURLs, gunakan GetAppClientAPIoperasi.

Kesalahan **`Token`**

TokenException

Anda mungkin menerima pengecualian berikut karena beberapa alasan.

```
TokenException
HTTP Status Code: 400
```

Alasan 1: Ketika email yang tidak valid ditentukan

```
Message: Invalid Email used
```

Pastikan alamat email yang Anda gunakan cocok dengan yang tercantum untuk `starterUserEmails` atribut saat Anda membuat AppClient. Jika email tidak cocok, ubah ke alamat email yang cocok dan coba lagi. Untuk melihat email yang digunakan, gunakan GetAppClientAPIoperasi.

Alasan 2: Untuk grant_type sebagai refresh_token saat token tidak ditentukan.

```
Message: refresh_token must be non-null for Refresh Token Grant-type
```

Token penyegaran yang ditentukan dalam permintaan adalah nol atau kosong. Tentukan aktif yang `refresh_token` diterima dalam respons API panggilan Token.

ThrottlingException

Anda mungkin menerima pengecualian berikut jika API dipanggil pada tingkat yang lebih dari kuota yang diizinkan.

```
ThrottlingException
HTTP Status Code: 429
```

`ListActionableInsights`,**`ListMeetingInsights`**, dan **`PutFeedback`** kesalahan

ValidationException

Anda mungkin menerima pengecualian berikut jika salah satu API parameter tidak memenuhi batasan yang ditentukan pada API spesifikasi.

```
ValidationException
HTTP Status Code: 400
```

ThrottlingException

Anda mungkin menerima pengecualian berikut jika API dipanggil pada tingkat yang lebih dari kuota yang diizinkan.

```
ThrottlingException
HTTP Status Code: 429
```

Memulai AppFabric untuk produktivitas (pratinjau) untuk pengguna akhir

Fitur AWS AppFabric untuk produktivitas ada dalam pratinjau dan dapat berubah sewaktu-waktu.

Bagian ini ditujukan untuk pengguna akhir aplikasi SaaS yang ingin mengaktifkan produktivitas (pratinjau) AWS AppFabric untuk meningkatkan manajemen tugas dan efisiensi alur kerja mereka. Ikuti langkah-langkah berikut untuk menghubungkan aplikasi Anda dan otorisasi AppFabric untuk memunculkan wawasan lintas aplikasi dan membantu Anda menyelesaikan tindakan (seperti mengirim email atau menjadwalkan rapat) dari aplikasi pilihan Anda. Anda dapat menghubungkan aplikasi sepertiAsana,,Atlassian Jira Suite,Google Workspace,Microsoft 365,Miro,Slack,Smartsheet, dan lainnya. Setelah Anda mengizinkan AppFabric untuk mengakses konten Anda, AppFabric bawalah wawasan dan tindakan lintas aplikasi secara langsung dalam aplikasi pilihan Anda — membantu Anda bekerja lebih efisien dan tetap berada dalam alur kerja Anda saat ini.

AppFabric untuk produktivitas menggunakan AI generatif yang didukung oleh Amazon Bedrock. AppFabric akan menghasilkan wawasan dan tindakan hanya setelah menerima izin eksplisit Anda. Anda mengizinkan setiap aplikasi individu untuk tetap memegang kendali penuh atas konten mana yang digunakan. AppFabric tidak akan menggunakan data Anda untuk melatih atau meningkatkan model bahasa besar yang mendasari yang digunakan untuk menghasilkan wawasan. Untuk informasi lebih lanjut, silakan lihat Amazon Bedrock FAQs.

Topik

Prasyarat

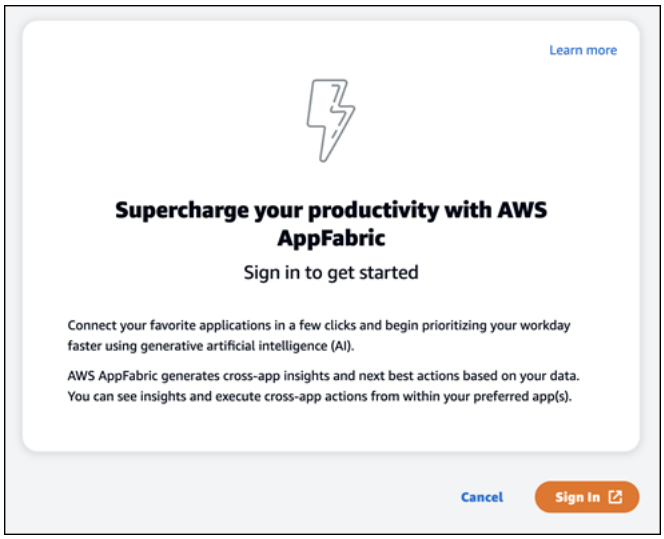
Sebelum memulai, pastikan Anda memiliki yang berikut:

- Kredensi untuk masuk AppFabric: Untuk mulai menggunakan AppFabric produktivitas, Anda memerlukan kredenal masuk gabungan (nama pengguna dan kata sandi) untuk salah satu penyedia berikut:,,, atau. Asana Google Workspace Microsoft 365 Slack Masuk untuk AppFabric membantu kami mengidentifikasi Anda sebagai pengguna di setiap aplikasi yang Anda aktifkan AppFabric untuk produktivitas. Setelah masuk, Anda dapat menghubungkan aplikasi Anda untuk mulai menghasilkan wawasan.
- Kredensi untuk menghubungkan aplikasi Anda: Wawasan dan tindakan lintas aplikasi hanya dibuat berdasarkan aplikasi yang Anda otorisasi. Anda akan memerlukan kredensi masuk (nama pengguna dan kata sandi) untuk setiap aplikasi yang ingin Anda otorisasi. Aplikasi yang didukung meliputi AsanaAtlassian Jira Suite,Google Workspace,,Microsoft 365,Miro,Slack, danSmartsheet.

Langkah 1. Masuk ke AppFabric

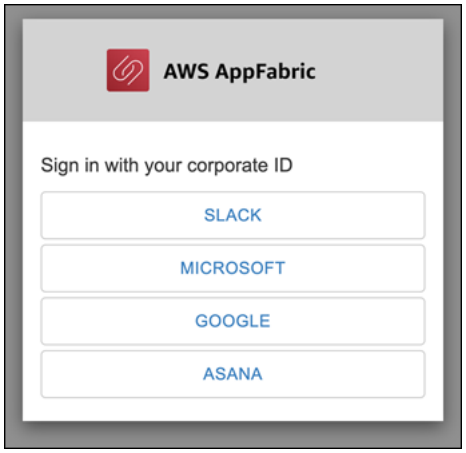
Connect aplikasi AppFabric untuk membawa konten dan wawasan Anda langsung ke dalam aplikasi pilihan Anda.

1. Setiap aplikasi akan digunakan AppFabric untuk produktivitas dengan berbagai cara untuk memberi Anda pengalaman aplikasi yang lebih kaya. Karena itu, setiap aplikasi akan memiliki titik masuk yang berbeda untuk mencapai halaman AppFabric beranda produktivitas di bawah ini. Halaman beranda menetapkan konteks tentang proses untuk mengaktifkan AppFabric dan pertama-tama meminta Anda untuk masuk. Setiap aplikasi yang ingin Anda aktifkan AppFabric akan mencapai layar ini.

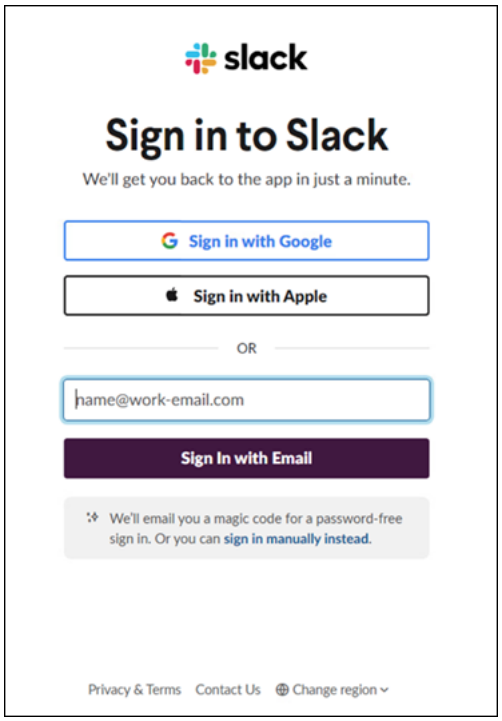


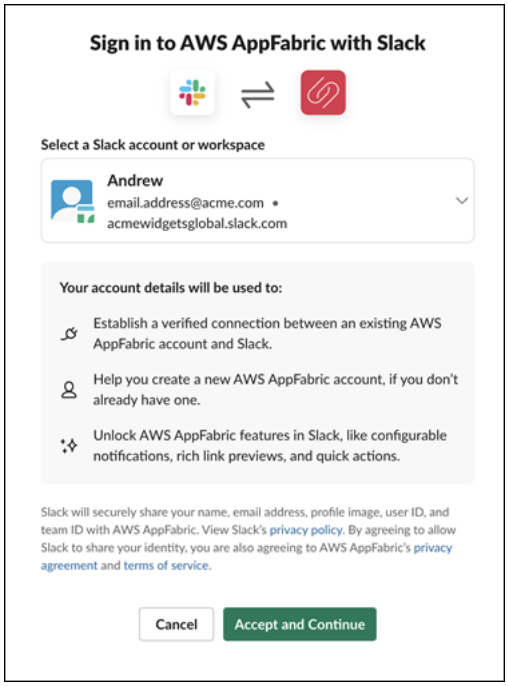
2. Masuk dengan kredensi Anda dari salah satu penyedia ini:Asana,, Google WorkspaceMicrosoft 365, atau. Slack Untuk pengalaman terbaik, kami sarankan masuk menggunakan penyedia yang sama untuk setiap aplikasi yang Anda aktifkan AppFabric . Misalnya, jika Anda memilih kredensi

Google Workspace di App1, sebaiknya pilih Google Workspace di App2, serta setiap kali Anda perlu masuk kembali. Jika Anda masuk dengan penyedia lain, Anda harus memulai ulang proses menghubungkan aplikasi.



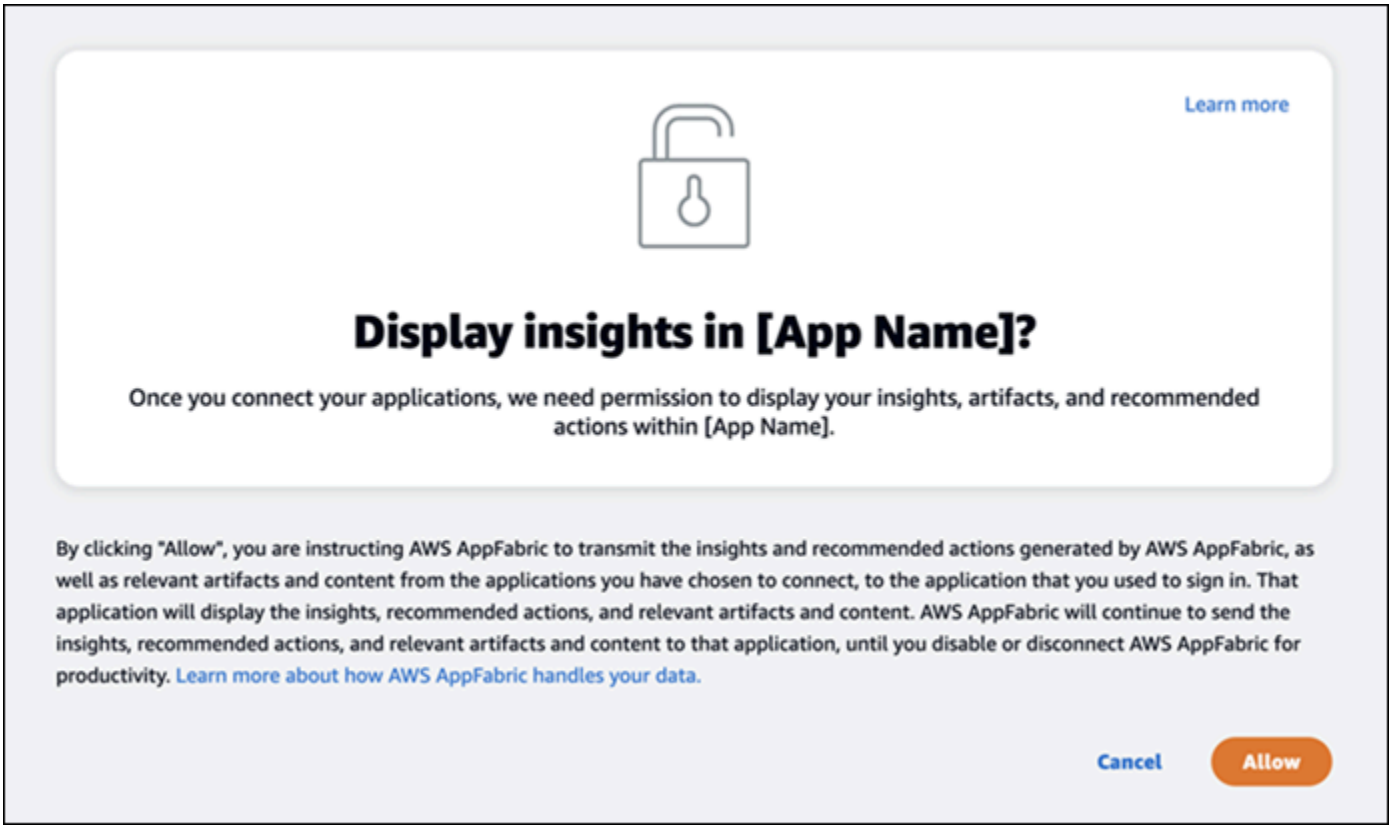
3. Jika diminta, masukkan kredenal masuk Anda dan terima masuk AppFabric dari penyedia ini.





Langkah 2. Memberikan persetujuan bagi aplikasi untuk menampilkan wawasan

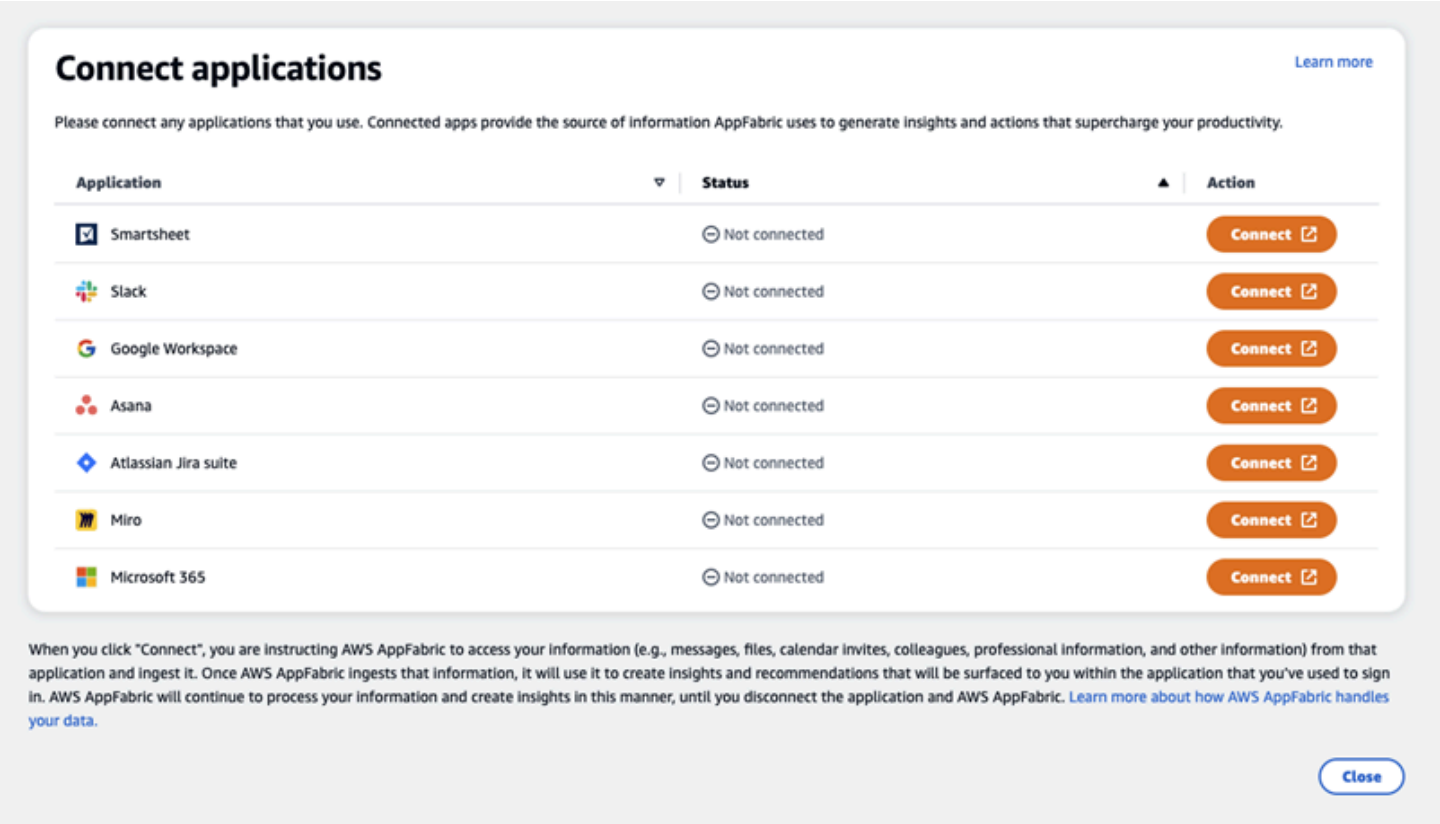
Setelah masuk, AppFabric akan menampilkan halaman persetujuan yang menanyakan apakah Anda mengizinkan AppFabric untuk menampilkan wawasan dan tindakan lintas aplikasi di dalam aplikasi yang Anda aktifkan AppFabric untuk produktivitas. Misalnya, apakah Anda mengizinkan AppFabric untuk mengambil Google Workspace email dan acara kalender Anda dan menampilkannyaAsana. Anda hanya perlu menyelesaikan langkah persetujuan ini satu kali per aplikasi yang Anda aktifkan AppFabric .



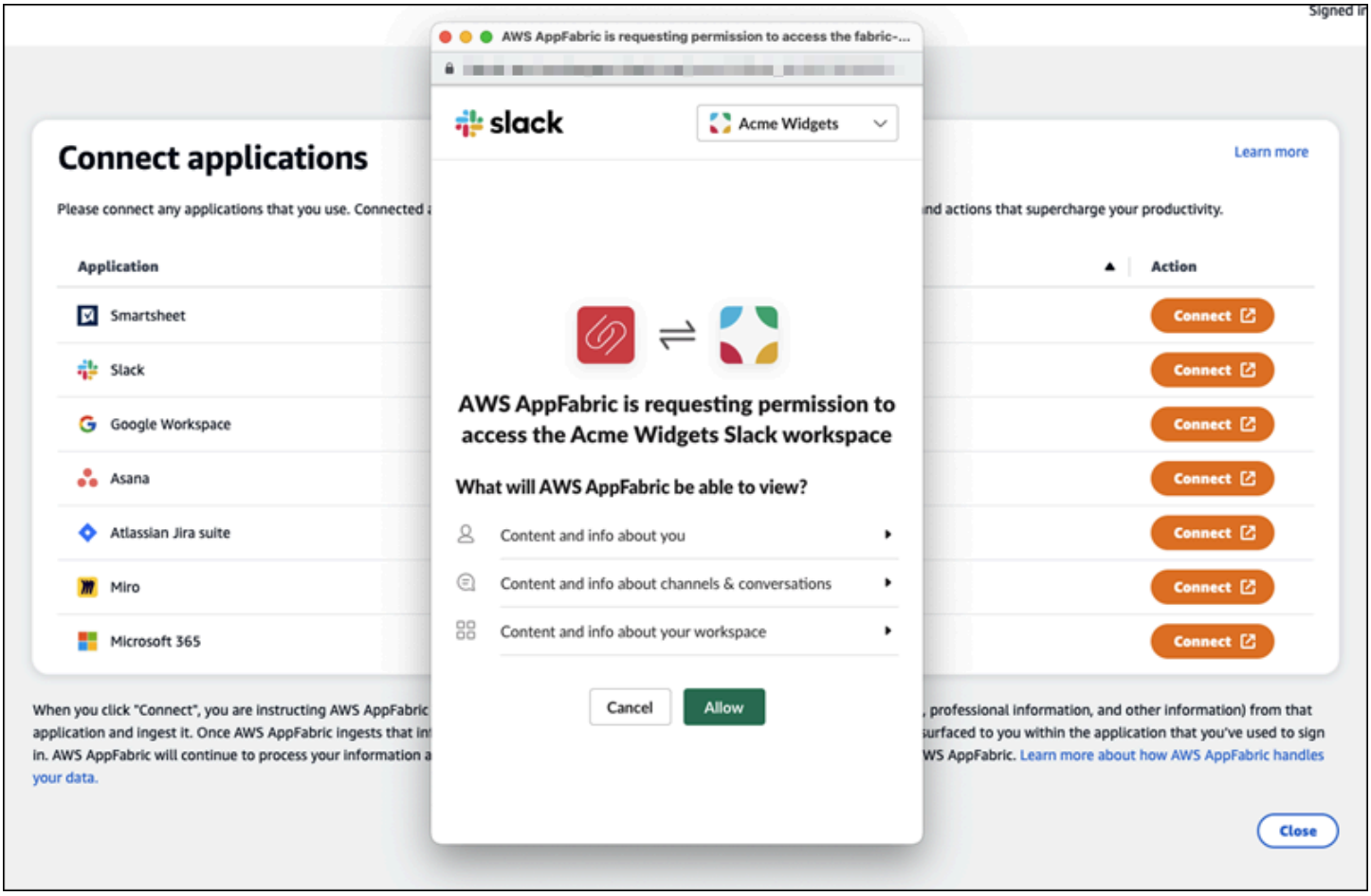
Langkah 3. Connect aplikasi Anda untuk menghasilkan wawasan dan tindakan

Setelah Anda menyelesaikan halaman persetujuan, Anda akan dibawa ke halaman Connect Applications di mana Anda dapat menghubungkan, memutuskan, atau menyambungkan kembali aplikasi individual yang pada akhirnya digunakan untuk menghasilkan wawasan dan tindakan lintas aplikasi Anda. Dalam kebanyakan kasus, setelah Anda masuk dan memberikan persetujuan, Anda akan terus menggunakan halaman ini untuk mengelola aplikasi yang terhubung.

Untuk menghubungkan aplikasi, pilih tombol Connect di sebelah aplikasi apa pun yang Anda gunakan.



Anda harus memberikan kredensi masuk Anda untuk aplikasi, dan mengizinkan AppFabric izin untuk mengakses data Anda untuk menghasilkan wawasan dan tindakan lengkap.

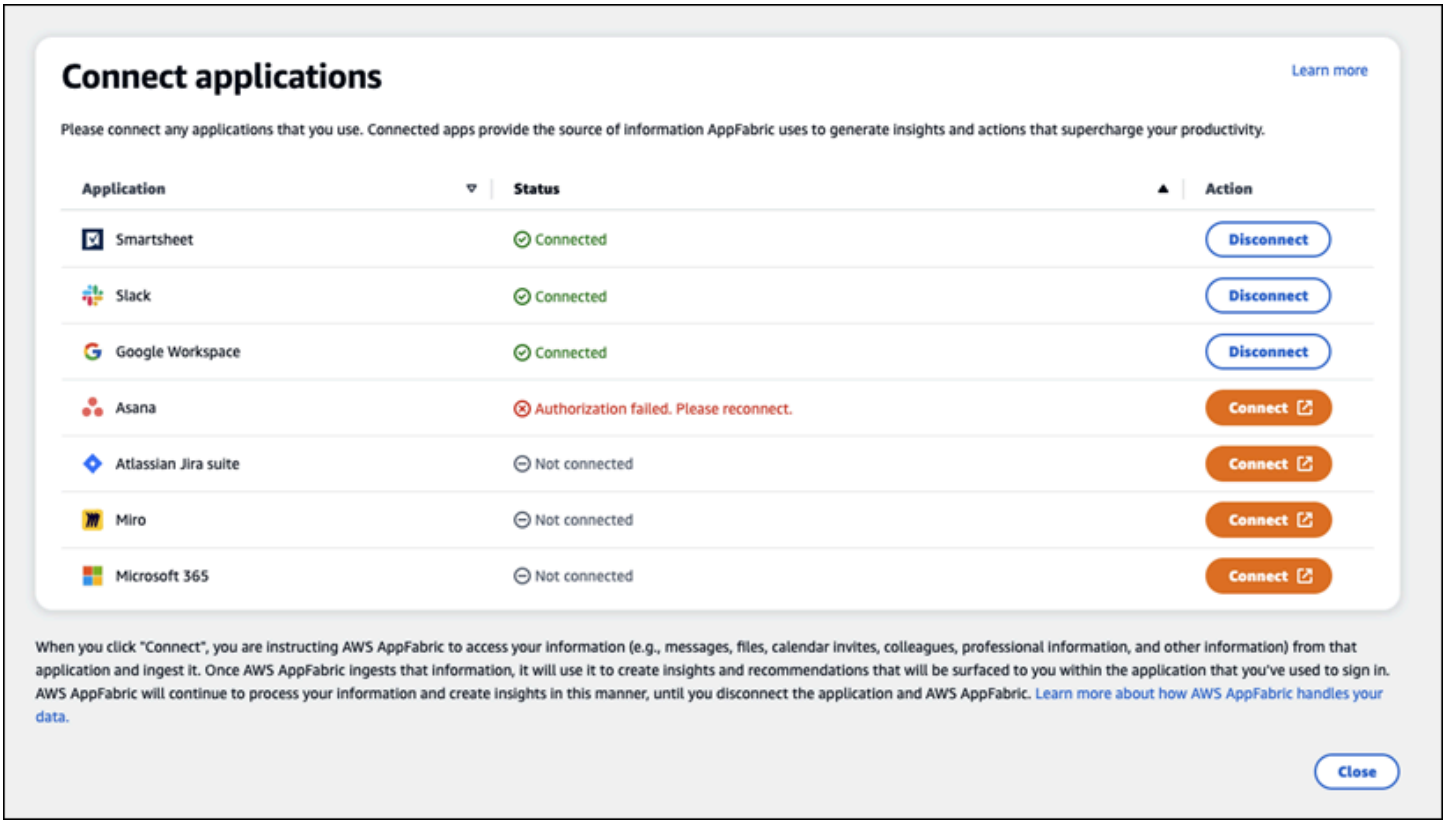


Setelah Anda berhasil menghubungkan aplikasi, Status untuk aplikasi itu akan berubah dari “Tidak Terhubung” menjadi “Terhubung”. Pengingat: Anda harus menyelesaikan langkah otorisasi ini untuk setiap aplikasi yang ingin Anda gunakan untuk menghasilkan wawasan dan tindakan.

Setelah Anda menghubungkan aplikasi, itu tidak terhubung selamanya. Anda harus menghubungkan kembali aplikasi secara berkala. Kami melakukan ini untuk memastikan kami masih memiliki izin Anda untuk menghasilkan wawasan.

Status aplikasi yang mungkin adalah:

- Terhubung - AppFabric diotorisasi dan menghasilkan wawasan menggunakan data Anda dari aplikasi ini.
- Tidak Terhubung - AppFabric tidak menghasilkan wawasan menggunakan data dari aplikasi ini. Anda dapat terhubung untuk mulai menghasilkan wawasan.
- Otorisasi gagal. Silakan sambungkan kembali. - Mungkin ada kegagalan otorisasi dengan aplikasi tertentu. Jika Anda melihat kesalahan ini, coba sambungkan kembali aplikasi Anda menggunakan tombol Connect.



Pengaturan selesai dan Anda dapat kembali ke aplikasi Anda. Diperlukan setidaknya beberapa jam untuk mulai melihat wawasan di dalam aplikasi Anda.

Jika diperlukan, Anda dapat menavigasi kembali ke halaman ini untuk mengelola aplikasi yang terhubung. Jika Anda memilih untuk Memutuskan sambungan aplikasi, AppFabric akan berhenti menggunakan data dari aplikasi tersebut atau mengumpulkan data baru untuk menghasilkan wawasan baru. Data dari aplikasi yang terputus akan secara otomatis dihapus dalam waktu 7 hari jika Anda memilih untuk tidak menghubungkan kembali aplikasi pada waktu itu.

Langkah 4. Mulai melihat wawasan dan jalankan tindakan lintas aplikasi di aplikasi Anda

Setelah menghubungkan aplikasi AppFabric, Anda akan memiliki akses ke wawasan berharga dan kemampuan untuk melakukan tindakan lintas aplikasi langsung dari aplikasi pilihan Anda. Catatan: fungsionalitas ini tidak dijamin di setiap aplikasi dan sepenuhnya bergantung pada fitur produktivitas mana AppFabric yang telah dipilih pengembang aplikasi untuk diaktifkan.

Wawasan lintas aplikasi

AppFabric untuk produktivitas menawarkan dua jenis wawasan:

- Wawasan yang dapat ditindaklanjuti: AppFabric menganalisis informasi dari email, acara kalender, tugas, dan pesan di seluruh aplikasi yang terhubung dan menghasilkan wawasan penting yang mungkin penting untuk Anda prioritaskan. Selain itu, AppFabric dapat menghasilkan tindakan yang disarankan (seperti mengirim email, menjadwalkan rapat, dan membuat tugas) yang dapat Anda edit dan jalankan saat tinggal di aplikasi pilihan Anda. Misalnya, Anda mungkin menerima wawasan yang mengatakan ada eskalasi pelanggan yang harus ditangani dan tindakan selanjutnya yang disarankan untuk menjadwalkan pertemuan dengan pelanggan Anda.
- Wawasan persiapan rapat: Fitur ini membantu Anda mempersiapkan diri terbaik untuk pertemuan mendatang. AppFabric akan menganalisis pertemuan Anda yang akan datang dan menghasilkan ringkasan singkat tentang tujuan pertemuan. Selain itu, ini akan memunculkan artefak yang relevan (seperti email, pesan, dan tugas) dari aplikasi Anda yang terhubung yang akan berguna untuk membantu Anda mempersiapkan rapat secara efisien tanpa beralih antar aplikasi untuk menemukan konten.

Tindakan lintas aplikasi

Untuk wawasan tertentu, AppFabric mungkin juga menghasilkan tindakan yang disarankan seperti mengirim email, menjadwalkan rapat, atau membuat tugas. Saat membuat tindakan, AppFabric dapat mengisi terlebih dahulu bidang tertentu berdasarkan konten dan konteks aplikasi Anda yang terhubung. Misalnya, AppFabric dapat menghasilkan respons email yang disarankan atau nama tugas berdasarkan wawasan. Ketika Anda mengklik tindakan yang disarankan, Anda akan dibawa ke antarmuka pengguna yang AppFabric dimiliki tempat Anda dapat mengedit konten yang telah diisi sebelumnya sebelum menjalankan tindakan. AppFabric tidak akan menjalankan tindakan tanpa tinjauan dan input pengguna terlebih dahulu sebagai AI generatif dan model bahasa besar yang mendasarinya (LLM) dapat berhalusinasi dari waktu ke waktu.

> **Note**
>
> Anda memiliki tanggung jawab untuk memvalidasi dan mengkonfirmasi AppFabric LLM output. AppFabric tidak menjamin keakuratan atau kualitas LLM outputnya. Untuk informasi selengkapnya, lihat Kebijakan AI yang Bertanggung AWS Jawab.

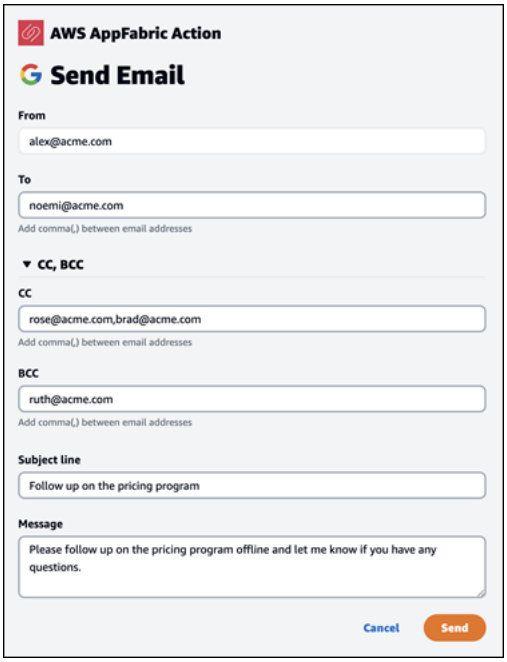
Buat email (Google Workspace,Microsoft 365)

AppFabric memungkinkan Anda untuk mengedit dan mengirim email dari dalam aplikasi pilihan Anda. Kami mendukung bidang email dasar termasuk From, To, Cc/Bcc, Email Subject Line, dan

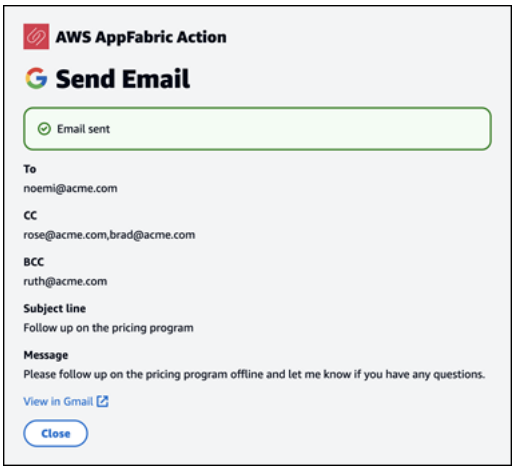
Email Body Message. AppFabric dapat menghasilkan konten di bidang ini untuk membantu Anda mengurangi waktu untuk menyelesaikan tugas. Setelah selesai mengedit email, pilih Kirim untuk mengirim email.

Bidang berikut diperlukan untuk mengirim email:

- Setidaknya satu email penerima (Kepada, CC danBCC) diperlukan, dan harus merupakan alamat email yang valid.
- Baris subjek dan bidang Pesan.



Setelah email dikirim, Anda akan melihat konfirmasi bahwa email telah dikirim. Selain itu, Anda akan melihat tautan untuk melihat email di aplikasi yang ditunjuk. Anda dapat menggunakan tautan ini untuk menavigasi ke aplikasi dengan cepat dan memverifikasi email telah dikirim.

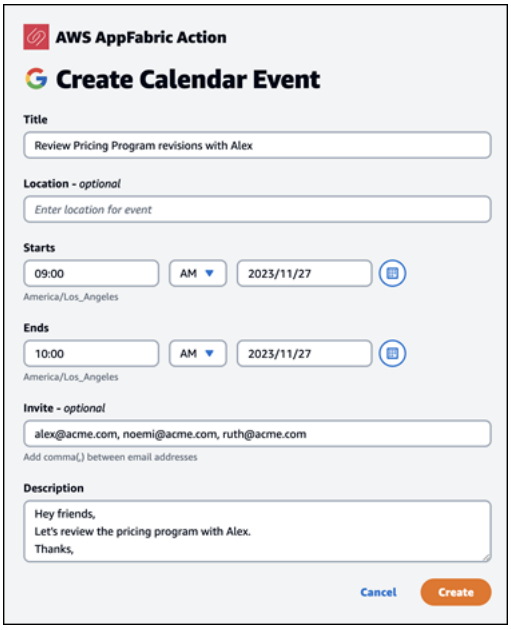


Buat acara kalender (Google Workspace,Microsoft 365)

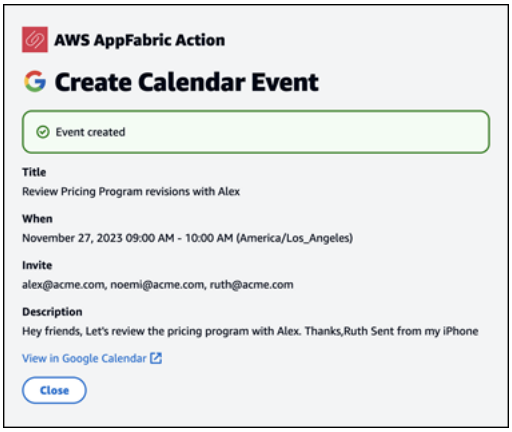
AppFabric memungkinkan Anda untuk mengedit dan membuat acara kalender dari dalam aplikasi pilihan Anda. Kami mendukung bidang acara kalender dasar termasuk Judul Acara, Lokasi, Waktu dan Tanggal Mulai/Berakhir, daftar Undangan, dan detail Acara. AppFabric dapat menghasilkan konten di bidang ini untuk membantu Anda mengurangi waktu untuk menyelesaikan tugas. Setelah selesai mengedit acara kalender, pilih Buat untuk membuat acara.

Bidang berikut diperlukan untuk membuat acara kalender:

- Bidang Judul, Mulai, Berakhir, dan Deskripsi.
- Waktu dan tanggal mulai tidak boleh lebih awal dari Waktu dan tanggal Berakhir.
- Bidang undangan bersifat opsional, tetapi memerlukan alamat email yang valid jika disediakan.



Setelah acara kalender dikirim, Anda akan melihat konfirmasi bahwa acara telah dibuat. Selain itu, Anda akan melihat tautan untuk melihat acara di aplikasi yang ditunjuk. Anda dapat menggunakan tautan ini untuk menavigasi ke aplikasi dengan cepat dan memverifikasi acara telah dibuat.

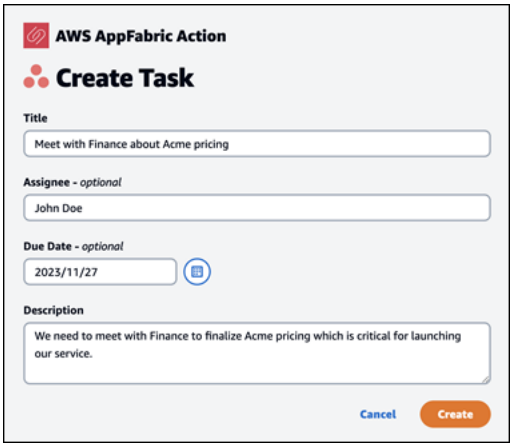


Buat tugas (Asana)

AppFabric memungkinkan Anda untuk mengedit dan membuat tugas Asana dari dalam aplikasi pilihan Anda. Kami mendukung bidang tugas dasar seperti Nama Tugas, Pemilik Tugas, Tanggal Jatuh Tempo, dan Deskripsi Tugas. AppFabric dapat menghasilkan konten di bidang ini untuk membantu Anda mengurangi waktu untuk membuat tugas. Setelah selesai mengedit tugas, pilih Buat untuk membuat tugas. Tugas dibuat di Asana ruang kerja atau proyek atau tugas yang berlaku, seperti yang disarankan oleh. LLM

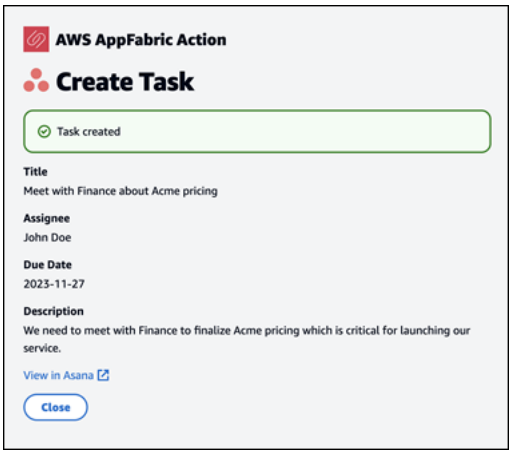
Bidang berikut diperlukan untuk membuat Asana tugas:

- Bidang Judul dan Deskripsi.
- Penerima tugas harus alamat email yang valid jika diubah.



Setelah tugas dibuat, Anda akan melihat konfirmasi bahwa tugas telah dibuatAsana. Selain itu, Anda akan melihat tautan untuk melihat tugas diAsana. Anda dapat menggunakan tautan ini untuk

menavigasi ke aplikasi dengan cepat untuk memverifikasi tugas telah dibuat, atau memindahkannya ke Asana ruang kerja atau proyek atau tugas yang sesuai.

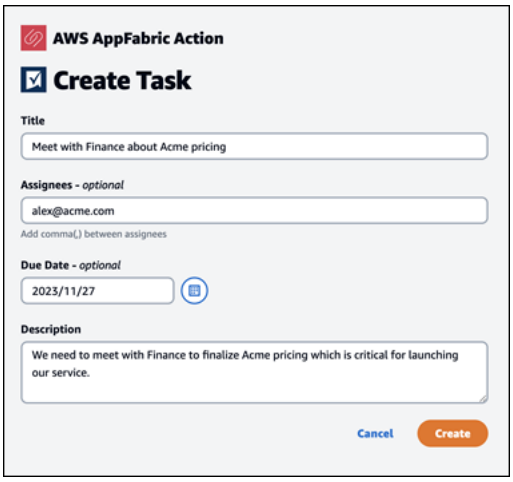


Buat tugas (Smartsheet)

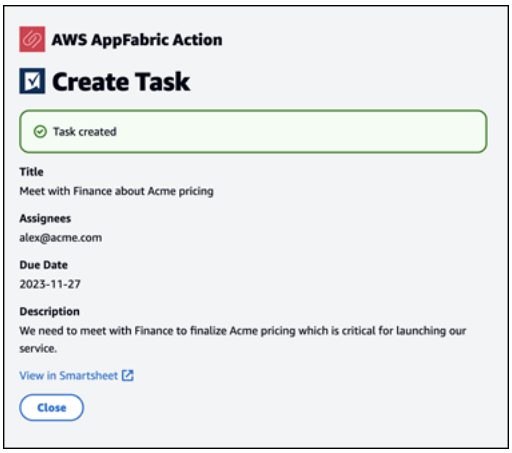
AppFabric memungkinkan Anda untuk mengedit dan membuat tugas Smartsheet dari dalam aplikasi pilihan Anda. Kami mendukung bidang tugas dasar seperti Nama Tugas, Pemilik Tugas, Tanggal Jatuh Tempo, dan Deskripsi Tugas. AppFabric dapat menghasilkan konten di bidang ini untuk membantu Anda mengurangi waktu untuk membuat tugas. Setelah selesai mengedit tugas, pilih Buat untuk membuat tugas. Untuk Smartsheet tugas, AppFabric akan membuat Smartsheet lembar pribadi baru dan mengisi tugas yang dibuat. Ini dilakukan untuk membantu memusatkan tindakan yang AppFabric dihasilkan di satu tempat secara terstruktur.

Bidang berikut diperlukan untuk membuat Smartsheet tugas:

- Bidang Judul dan Deskripsi.
- Penerima tugas harus alamat email yang valid jika disediakan.



Setelah tugas dibuat, Anda akan melihat konfirmasi bahwa tugas telah dibuatSmartsheet. Selain itu, Anda akan melihat tautan untuk melihat tugas diSmartsheet. Anda dapat menggunakan tautan ini untuk menavigasi dengan cepat ke aplikasi untuk melihat tugas di Smartsheet lembar yang dibuat. Semua Smartsheet tugas future akan diisi di lembar ini. Jika lembar dihapus, AppFabric akan membuat yang baru.



Perhatian Administrator TI dan Keamanan: Mengelola akses ke fitur AppFabric produktivitas (pratinjau)

Fitur AWS AppFabric untuk produktivitas dalam pratinjau dan dapat berubah sewaktu-waktu.

Portal pengguna AppFabric untuk produktivitas dapat diakses publik oleh semua pengguna aplikasi SaaS yang telah terintegrasi AppFabric dengan fitur produktivitas (pratinjau). Jika Anda seorang Administrator TI yang ingin mengelola akses ke fitur AI generatif ini dalam organisasi Anda, pertimbangkan opsi ini:

- Batasi Login Penyedia Identitas (IDP): Anda dapat memblokir akses masuk melalui Penyedia Identitas Anda untuk mengontrol akses pengguna ke fitur AI generatif.
- Nonaktifkan OAuth untuk Aplikasi Tertentu: Terapkan pembatasan hilir dengan menonaktifkan OAuth. Tindakan ini mencegah pengguna menghubungkan aplikasi yang memerlukan otentikasi OAuth ke ruang kerja perusahaan.

Pemecahan Masalah

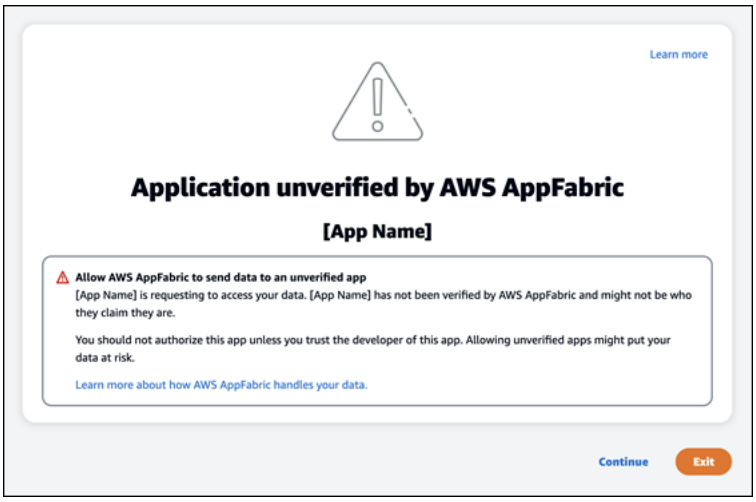
Fitur AWS AppFabric untuk produktivitas dalam pratinjau dan dapat berubah sewaktu-waktu.

Bagian ini menjelaskan kesalahan umum dan pemecahan masalah AppFabric untuk produktivitas.

Aplikasi yang belum diverifikasi

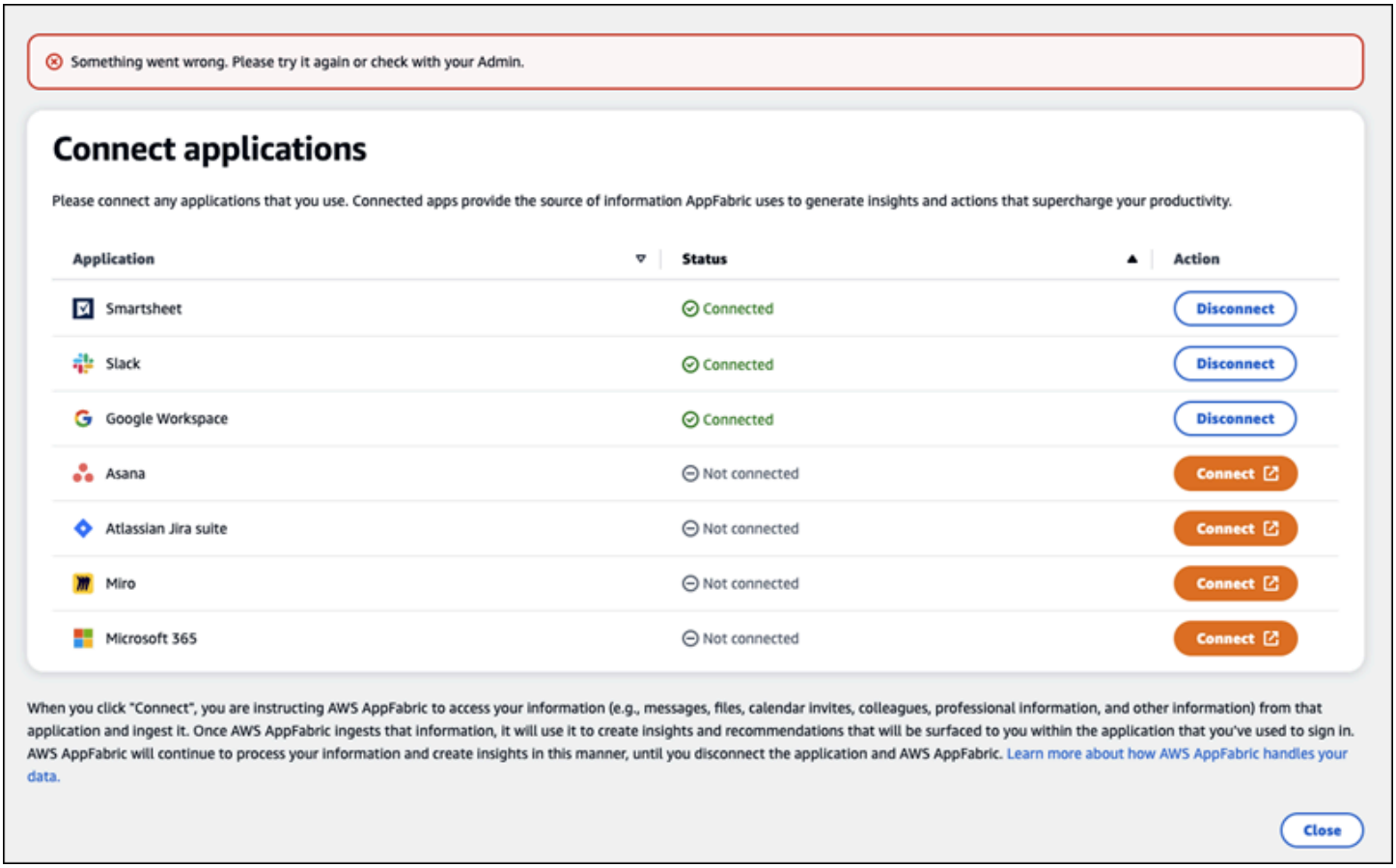
Aplikasi yang digunakan AppFabric untuk produktivitas untuk memperkaya pengalaman aplikasi mereka akan melalui proses verifikasi sebelum meluncurkan fitur mereka ke pengguna akhir. Jika Anda menemukan spanduk “tidak terverifikasi” saat mencoba masuk AppFabric, ini berarti aplikasi belum menjalani AppFabric proses verifikasi yang mengonfirmasi identitas pengembang aplikasi dan keakuratan informasi pendaftaran aplikasi. Semua aplikasi dimulai sebagai tidak diverifikasi dan berubah menjadi diverifikasi hanya ketika proses verifikasi selesai.

Berhati-hatilah saat menggunakan aplikasi yang belum diverifikasi. Jika Anda tidak yakin tentang pengembang aplikasi, Anda dapat menunggu hingga aplikasi mencapai status terverifikasi sebelum melanjutkan.



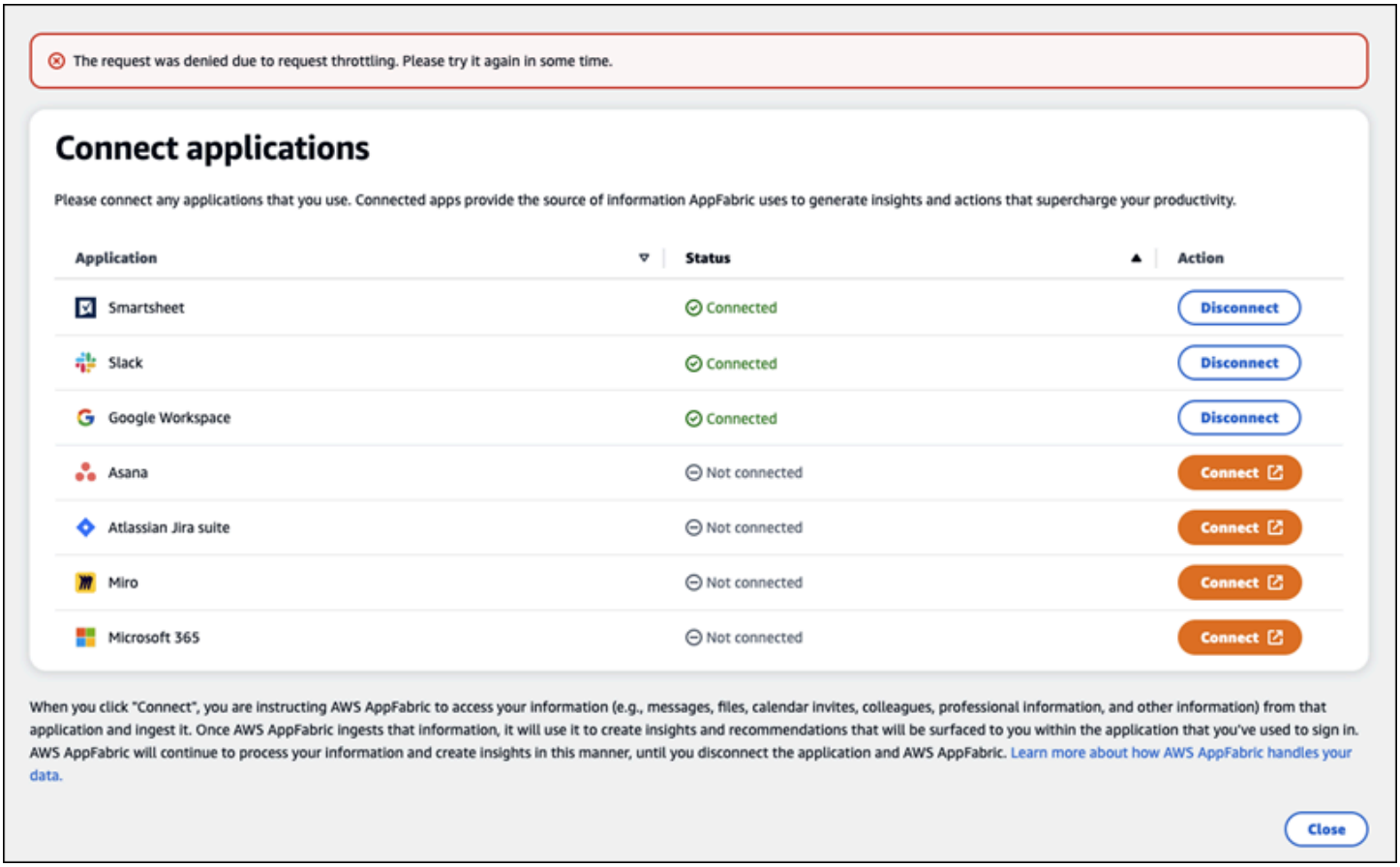
Ada yang tidak beres. Silakan coba lagi atau periksa dengan Admin Anda (`InternalServerException`)

Anda mungkin mendapatkan pesan ini ketika portal AppFabric pengguna gagal mencantumkan aplikasi atau memutuskan sambungan aplikasi karena kesalahan, pengecualian, atau kegagalan yang tidak diketahui. Coba lagi nanti.



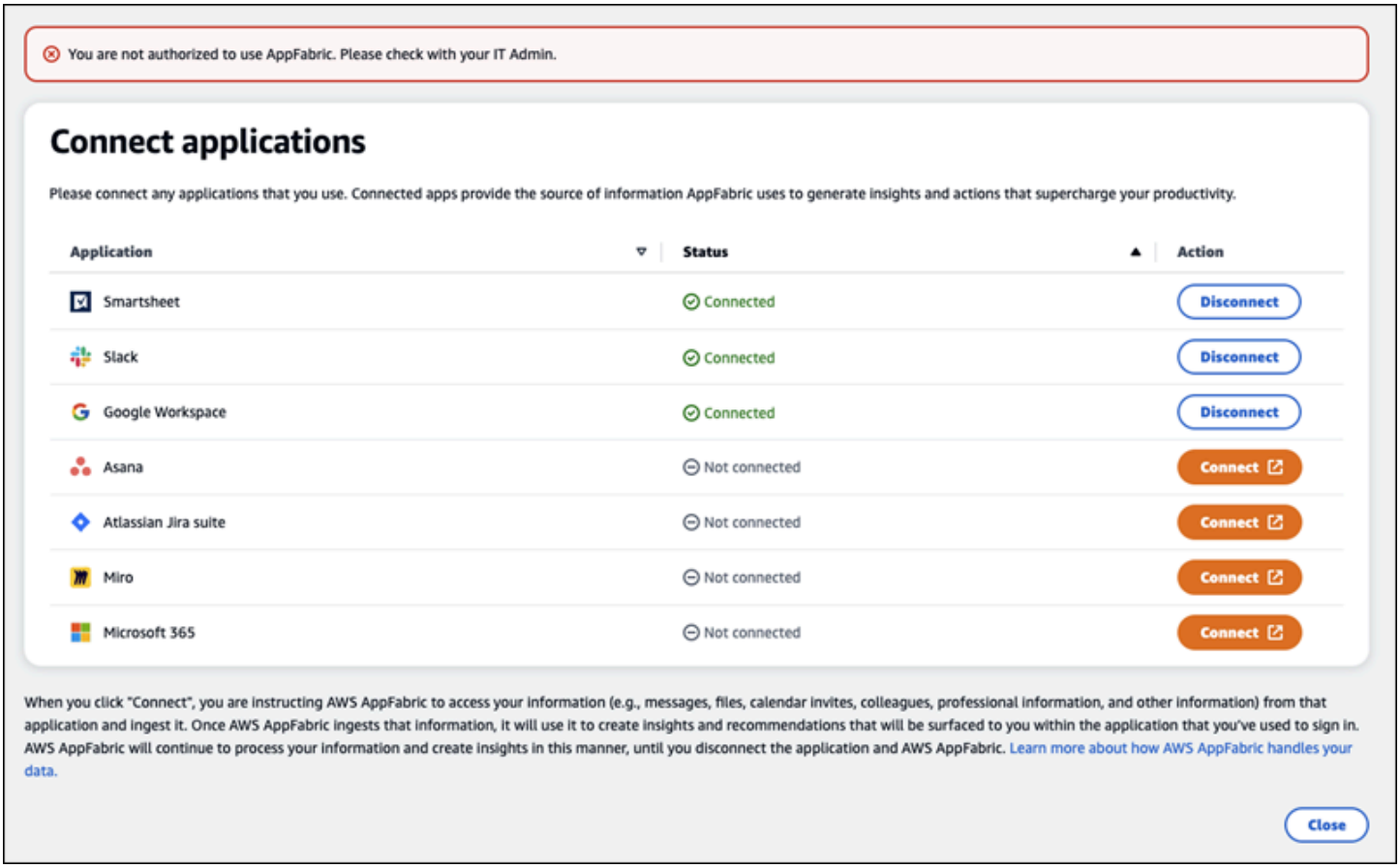
Permintaan ditolak karena throttling permintaan. Silakan coba lagi dalam beberapa waktu (**`ThrottlingException`**)

Anda mungkin mendapatkan pesan ini ketika portal AppFabric pengguna gagal mencantumkan aplikasi atau memutuskan sambungan aplikasi karena masalah pelambatan. Coba lagi nanti.



Anda tidak berwenang untuk menggunakan AppFabric. Silakan masuk AppFabric lagi (**`AccessDeniedException`**)

Anda mungkin mendapatkan pesan ini ketika portal AppFabric pengguna gagal untuk daftar aplikasi atau memutuskan sambungan aplikasi karena akses ditolak pengecualian. Masuk AppFabric lagi.



AppFabric API produktivitas

Fitur AWS AppFabric untuk produktivitas dalam pratinjau dan dapat berubah sewaktu-waktu.

Bagian ini menyediakan operasi API, tipe data, dan kesalahan umum untuk fitur AWS AppFabric produktivitas.

> **Note**
>
> Untuk semua AppFabric API lainnya, lihat Referensi AWS AppFabric API.

Topik

- Tindakan
- Jenis data
- Kesalahan umum

Tindakan

Fitur AWS AppFabric untuk produktivitas dalam pratinjau dan dapat berubah sewaktu-waktu.

Tindakan berikut didukung untuk fitur AppFabric produktivitas.

Untuk semua tindakan AppFabric API lainnya, lihat Tindakan AWS AppFabric API.

Topik

Otorisasi

Fitur AWS AppFabric untuk produktivitas dalam pratinjau dan dapat berubah sewaktu-waktu.

Mengotorisasi sebuah. AppClient

Topik

Isi permintaan

Permintaan menerima data berikut dalam format JSON.

Parameter	Deskripsi
app_client_id	ID AppClient untuk mengotorisasi.
redirect_uri	URI untuk mengarahkan pengguna akhir setelah otorisasi.
negara	Nilai unik untuk mempertahankan status antara permintaan dan callback.

CreateAppClient

Fitur AWS AppFabric untuk produktivitas dalam pratinjau dan dapat berubah sewaktu-waktu.

Menciptakan sebuah AppClient.

Topik

- Isi permintaan
- Elemen jawaban

Isi permintaan

Permintaan menerima data berikut dalam format JSON.

Parameter	Deskripsi
AppName	Nama aplikasi. Jenis: String Batasan Panjang: Panjang minimum 1. Panjang maksimum sebesar 255. Wajib: Ya
ClientToken	Menentukan pengidentifikasi unik dan peka huruf besar/kecil yang Anda berikan untuk memastikan idempotensi permintaan.

Parameter	Deskripsi
	Ini memungkinkan Anda mencoba kembali permintaan dengan aman tanpa sengaja melakukan operasi yang sama untuk kedua kalinya. Meneruskan nilai yang sama ke panggilan selanjutn ya ke operasi mengharuskan Anda juga meneruskan nilai yang sama untuk semua parameter lainnya. Kami menyarankan Anda menggunakan jenis nilai UUID. Jika Anda tidak memberikan nilai ini, maka AWS hasilkan nilai acak untuk Anda. Jika Anda mencoba lagi operasi dengan yang sama`ClientToken`, tetapi dengan parameter yang berbeda, percobaan ulang gagal dengan kesalahan`IdempotentParameterMismatch`. Jenis: String Pola: `[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Wajib: Tidak

Parameter	Deskripsi
customerManagedKey Pengenal	ARN yang kunci yang dikelola pelanggan dihasilkan oleh. AWS Key Management Service Kuncinya digunakan untuk mengenkripsi data. Jika tidak ada kunci yang ditentukan, maka an Kunci yang dikelola AWS digunakan. Peta pasangan kunci-nilai tag atau tag untuk ditetapkan ke sumber daya. Untuk informasi selengkapnya tentang Kunci milik AWS dan kunci yang dikelola pelanggan, lihat Kunci dan AWS kunci pelanggan di Panduan AWS Key Management Service Pengembang. Jenis: String Batasan Panjang: Panjang minimum 1. Panjang maksimum 1011. Pola: `arn:.+$|^[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Wajib: Tidak
deskripsi	Deskripsi untuk aplikasi. Tipe: String Diperlukan: Ya
IconURL	URL ke ikon atau logo untuk AppClient. Tipe: String Wajib: Tidak

Parameter	Deskripsi
RedirecTurls	URI untuk mengarahkan pengguna akhir setelah otorisasi. Anda dapat menambahkan hingga 5 RedirecTurls. Misalnya, `https://localhost:8080` . Tipe: Array string Anggota Array: Jumlah minimum 1 item. Jumlah maksimum 5 item. Batasan Panjang: Panjang minimum 1. Panjang maksimum 2048. Pola: `(http|https):\/\/[-a-zA-Z0-9_:.\/]+` Wajib: Ya
starterUserEmails	Alamat email pemula untuk pengguna yang diizinkan mengakses untuk menerima wawasan hingga AppClient diverifik asi. Tipe: Array string Anggota Array: Jumlah tetap 1 item. Batasan Panjang: Panjang minimum sebesar 0. Panjang maksimum 320. Pola: `[a-zA-Z0-9.!#$%&'*+/=?^_`{|}~-]+@[a-zA-Z0-9-]+(?:\.[a-zA-Z0-9-]+)*` Diperlukan: Ya

Parameter	Deskripsi
tag	Peta pasangan kunci-nilai tag atau tag untuk ditetapkan ke sumber daya. Jenis: Array objek Tag Anggota Array: Jumlah minimum 0 item. Jumlah maksimum 50 item. Wajib: Tidak

Elemen jawaban

Jika tindakan berhasil, layanan mengirimkan kembali respon HTTP 201.

Layanan mengembalikan data berikut dalam format JSON.

Parameter	Deskripsi
appClientSummary	Berisi ringkasan dari AppClient. Tipe: Objek AppClientSummary

DeleteAppClient

Fitur AWS AppFabric untuk produktivitas dalam pratinjau dan dapat berubah sewaktu-waktu.

Menghapus klien aplikasi.

Topik

- Isi permintaan
- Elemen jawaban

Isi permintaan

Permintaan menerima data berikut dalam format JSON.

Parameter	Deskripsi
appClientIdentifier	Nama Sumber Daya Amazon (ARN) atau Universal Unique Identifier (UUID) yang akan digunakan AppClient untuk permintaan tersebut. Batasan Panjang: Panjang minimum 1. Panjang maksimum 1011. Pola: `arn:.+$|^[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Diperlukan: Ya

Elemen jawaban

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 204 dengan isi HTTP kosong.

GetAppClient

> Fitur AWS AppFabric untuk produktivitas dalam pratinjau dan dapat berubah sewaktu-waktu.

Mengembalikan informasi tentang sebuah AppClient.

Topik

- Isi permintaan
- Elemen jawaban

Isi permintaan

Permintaan menerima data berikut dalam format JSON.

Parameter	Deskripsi
appClientIdentifier	Nama Sumber Daya Amazon (ARN) atau Universal Unique Identifier (UUID) yang akan digunakan AppClient untuk permintaan tersebut.

Parameter	Deskripsi
	Batasan Panjang: Panjang minimum 1. Panjang maksimum 1011. Pola: `arn:.+$|^[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Diperlukan: Ya

Elemen jawaban

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

Parameter	Deskripsi
AppClient	Berisi informasi tentang sebuah AppClient. Tipe: Objek AppClient

ListActionableInsights

Fitur AWS AppFabric untuk produktivitas dalam pratinjau dan dapat berubah sewaktu-waktu.

Daftar pesan email yang paling penting yang dapat ditindaklanjuti, tugas, dan pembaruan lainnya.

Topik

- Isi permintaan
- Elemen jawaban

Isi permintaan

Permintaan menerima data berikut dalam format JSON.

Parameter	Deskripsi
NextToken	Jika `nextToken` dikembalikan, ada lebih banyak hasil yang tersedia. Nilai `nextToken` adalah token pagination unik untuk setiap halaman. Lakukan panggilan lagi menggunakan token yang dikembalikan untuk mengambil halaman berikutny a. Jaga agar semua argumen lainnya tidak berubah. Setiap token pagination akan kedaluwarsa setelah 24 jam. Menggunak an token pagination yang kedaluwarsa akan mengembalikan kesalahan HTTP 400 InvalidToken .

Elemen jawaban

Jika tindakan berhasil, layanan mengirimkan kembali respon HTTP 201.

Layanan mengembalikan data berikut dalam format JSON.

Parameter	Deskripsi
ActionableInsightsList	Daftar wawasan yang dapat ditindaklanjuti, termasuk judul, deskripsi, tindakan, dan stempel waktu yang dibuat. Untuk informasi selengkapnya, lihat ActionableInsights.
NextToken	Jika `nextToken` dikembalikan, ada lebih banyak hasil yang tersedia. Nilai `nextToken` adalah token pagination unik untuk setiap halaman. Lakukan panggilan lagi menggunakan token yang dikembalikan untuk mengambil halaman berikutny a. Jaga agar semua argumen lainnya tidak berubah. Setiap token pagination akan kedaluwarsa setelah 24 jam. Menggunak an token pagination yang kedaluwarsa akan mengembalikan kesalahan HTTP 400 InvalidToken . Jenis: String

ListAppClients

Fitur AWS AppFabric untuk produktivitas dalam pratinjau dan dapat berubah sewaktu-waktu.

Mengembalikan daftar semua AppClients.

Topik

- Isi permintaan
- Elemen jawaban

Isi permintaan

Permintaan menerima data berikut dalam format JSON.

Parameter	Deskripsi
maxResults	Jumlah maksimum hasil yang dikembalikan per panggilan. Anda dapat menggunakan `nextToken` untuk mendapatkan halaman hasil lebih lanjut. Ini hanya batas atas. Jumlah aktual hasil yang dikembalikan per panggilan mungkin kurang dari maksimum yang ditentukan. Rentang yang Valid: Nilai minimum 1. Nilai maksimum 100.
NextToken	Jika `nextToken` dikembalikan, ada lebih banyak hasil yang tersedia. Nilai `nextToken` adalah token pagination unik untuk setiap halaman. Lakukan panggilan lagi menggunakan token yang dikembalikan untuk mengambil halaman berikutny a. Jaga agar semua argumen lainnya tidak berubah. Setiap token pagination akan kedaluwarsa setelah 24 jam. Menggunak an token pagination yang kedaluwarsa akan mengembalikan kesalahan HTTP 400 InvalidToken .

Elemen jawaban

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

Parameter	Deskripsi
appClientList	Berisi daftar AppClient hasil. Tipe: Array objek AppClientSummary
NextToken	Jika `nextToken` dikembalikan, ada lebih banyak hasil yang tersedia. Nilai `nextToken` adalah token pagination unik untuk setiap halaman. Lakukan panggilan lagi menggunakan token yang dikembalikan untuk mengambil halaman berikutny a. Jaga agar semua argumen lainnya tidak berubah. Setiap token pagination akan kedaluwarsa setelah 24 jam. Menggunak an token pagination yang kedaluwarsa akan mengembalikan kesalahan HTTP 400 InvalidToken . Jenis: String

ListMeetingInsights

Fitur AWS AppFabric untuk produktivitas dalam pratinjau dan dapat berubah sewaktu-waktu.

Daftar acara kalender yang paling penting yang dapat ditindaklanjuti.

Topik

- Isi permintaan
- Elemen jawaban

Isi permintaan

Permintaan menerima data berikut dalam format JSON.

Parameter	Deskripsi
NextToken	Jika `nextToken` dikembalikan, ada lebih banyak hasil yang tersedia. Nilai `nextToken` adalah token pagination unik untuk setiap halaman. Lakukan panggilan lagi menggunakan token yang dikembalikan untuk mengambil halaman berikutny a. Jaga agar semua argumen lainnya tidak berubah. Setiap token pagination akan kedaluwarsa setelah 24 jam. Menggunak an token pagination yang kedaluwarsa akan mengembalikan kesalahan HTTP 400 InvalidToken .

Elemen jawaban

Jika tindakan berhasil, layanan mengirimkan kembali respon HTTP 201.

Layanan mengembalikan data berikut dalam format JSON.

Parameter	Deskripsi
MeetingInsightList	Daftar wawasan pertemuan yang dapat ditindaklanjuti. Untuk informasi selengkapnya, lihat MeetingInsights.
NextToken	Jika `nextToken` dikembalikan, ada lebih banyak hasil yang tersedia. Nilai `nextToken` adalah token pagination unik untuk setiap halaman. Lakukan panggilan lagi menggunakan token yang dikembalikan untuk mengambil halaman berikutny a. Jaga agar semua argumen lainnya tidak berubah. Setiap token pagination akan kedaluwarsa setelah 24 jam. Menggunak an token pagination yang kedaluwarsa akan mengembalikan kesalahan HTTP 400 InvalidToken . Jenis: String

PutFeedback

Fitur AWS AppFabric untuk produktivitas dalam pratinjau dan dapat berubah sewaktu-waktu.

Memungkinkan pengguna mengirimkan umpan balik untuk wawasan atau tindakan tertentu.

Topik

- Isi permintaan
- Elemen jawaban

Isi permintaan

Permintaan menerima data berikut dalam format JSON.

Parameter	Deskripsi
id	ID objek yang umpan baliknya dikirimkan. Ini bisa berupa InsightId atau ActionId.
Umpan Balik	Jenis wawasan yang umpan baliknya dikirimkan. Nilai yang mungkin: `ACTIONABLE_INSIGHT | MEETING_INSIGHT | ACTION`
Umpan Balik Penilaian	Peringkat Umpan Balik dari 1 ke5. Rating yang lebih tinggi semakin baik.

Elemen jawaban

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 201 dengan badan HTTP kosong.

Token

Fitur AWS AppFabric untuk produktivitas dalam pratinjau dan dapat berubah sewaktu-waktu.

Berisi informasi yang memungkinkan AppClients untuk bertukar kode otorisasi untuk token akses.

Topik

- Isi permintaan

- Elemen jawaban

Isi permintaan

Permintaan menerima data berikut dalam format JSON.

Parameter	Deskripsi
kode	Kode otorisasi yang diterima dari titik akhir otorisasi. Jenis: String Batasan Panjang: Panjang minimum 1. Panjang maksimum 2048. Wajib: Tidak
grant_type	Jenis hibah untuk token. Harus `authorization_code` atau `refresh_token` . Tipe: String Diperlukan: Ya
app_client_id	ID dari AppClient. Jenis: String Pola: `[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Wajib: Ya
redirect_uri	URI pengalihan diteruskan ke titik akhir otorisasi. Tipe: String Wajib: Tidak
refresh_token	Token penyegaran diterima dari permintaan token awal. Jenis: String

Parameter	Deskripsi
	Batasan Panjang: Panjang minimum 1. Panjang maksimum 4096. Wajib: Tidak

Elemen jawaban

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

Parameter	Deskripsi
appfabric_user_id	ID pengguna untuk token. Ini dikembalikan hanya untuk permintaan yang menggunakan jenis `authorization_code` hibah. Jenis: String
kedaluwarsa_in	Jumlah detik hingga token kedaluwarsa. Tipe: Long
refresh_token	Token penyegaran yang akan digunakan untuk permintaan berikutnya. Jenis: String Batasan Panjang: Panjang minimum 1. Panjang maksimum 2048.
token	Token akses. Jenis: String Batasan Panjang: Panjang minimum 1. Panjang maksimum 2048.
token_type	Jenis token.

Parameter	Deskripsi
	Jenis: String

UpdateAppClient

Fitur AWS AppFabric untuk produktivitas dalam pratinjau dan dapat berubah sewaktu-waktu.

Pembaruan an AppClient.

Topik

- Isi permintaan
- Elemen jawaban

Isi permintaan

Permintaan menerima data berikut dalam format JSON.

Parameter	Deskripsi
appClientIdentifier	Nama Sumber Daya Amazon (ARN) atau Universal Unique Identifier (UUID) yang akan digunakan AppClient untuk permintaan tersebut. Batasan Panjang: Panjang minimum 1. Panjang maksimum 1011. Pola: `arn:.+$|^[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Wajib: Ya
RedirecTurls	URI untuk mengarahkan pengguna akhir setelah otorisasi. Anda dapat menambahkan hingga 5 RedirecTurls. Misalnya, `https://localhost:8080` . Tipe: Array string

Parameter	Deskripsi
	Anggota Array: Jumlah minimum 1 item. Jumlah maksimum 5 item. Batasan Panjang: Panjang minimum 1. Panjang maksimum 2048. Pola: `(http|https):\/\/[-a-zA-Z0-9_:.\/]+`

Elemen jawaban

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

Parameter	Deskripsi
AppClient	Berisi informasi tentang sebuah AppClient. Tipe: Objek AppClient

Jenis data

Fitur AWS AppFabric untuk produktivitas dalam pratinjau dan dapat berubah sewaktu-waktu.

AppFabric API berisi beberapa tipe data yang digunakan berbagai tindakan. Bagian ini menjelaskan tipe data untuk fitur AppFabric produktivitas secara rinci.

Untuk semua tipe data AppFabric API lainnya, lihat Jenis Data AWS AppFabric API.

> **Important**
>
> Urutan setiap elemen dalam struktur tipe data tidak dijamin. Aplikasi tidak harus mengambil urutan tertentu.

Topik

- ActionableInsights
- AppClient
- AppClientSummary
- MeetingInsights
- VerificationDetails

ActionableInsights

Fitur AWS AppFabric untuk produktivitas dalam pratinjau dan dapat berubah sewaktu-waktu.

Berisi ringkasan tindakan penting dan sesuai untuk pengguna berdasarkan email, undangan kalender, pesan, dan tugas dari portofolio aplikasi mereka. Pengguna dapat melihat wawasan proaktif dari seluruh aplikasi mereka untuk membantu mereka mengarahkan hari mereka dengan sebaik-baiknya. Wawasan ini memberikan pembenaran mengapa pengguna harus peduli dengan ringkasan wawasan bersama dengan referensi, seperti tautan yang disematkan, ke aplikasi individual dan artefak yang menghasilkan wawasan.

Parameter	Deskripsi
InsightID	Id unik untuk wawasan yang dihasilkan.
InsightContent	Ini mengembalikan ringkasan wawasan dan tautan tertanam ke artefak yang digunakan untuk menghasilkan wawasan. Ini akan menjadi konten HTML yang berisi tautan tertanam (<a>tag).
InsightTitle	Judul wawasan yang dihasilkan.
createDat	Ketika wawasan dihasilkan.
tindakan	Daftar tindakan yang direkomendasikan untuk wawasan yang dihasilkan. Objek tindakan berisi parameter berikut:

Parameter	Deskripsi
	• `actionId`— Id unik untuk tindakan yang dihasilkan. • `actionIconUrl` — URL ikon untuk aplikasi tempat tindakan disarankan untuk dijalankan. • `actionTitle` — Judul tindakan yang dihasilkan. • `actionUrl` — URL unik bagi pengguna akhir untuk melihat dan menjalankan tindakan di AppFabric portal pengguna. Untuk menjalankan tindakan, aplikasi ISV akan mengarahkan kembali pengguna ke portal AppFabric pengguna (layar pop up) menggunakan URL ini. • `actionExecutionStatus` — Enum yang menunjukkan status tindakan. Nilai yang mungkin adalah: `EXECUTED` | `NOT_EXECUTED`

AppClient

Fitur AWS AppFabric untuk produktivitas dalam pratinjau dan dapat berubah sewaktu-waktu.

Berisi informasi tentang sebuah AppClient.

Parameter	Deskripsi
AppName	Nama aplikasi. Tipe: String Diperlukan: Ya
arn	Nama Sumber Daya Amazon (ARN) dari. AppClient Jenis: String Batasan Panjang: Panjang minimum 1. Panjang maksimum 1011.

Parameter	Deskripsi
	Pola: `arn:.+` Wajib: Ya
deskripsi	Deskripsi untuk aplikasi. Tipe: String Diperlukan: Ya
IconURL	URL ke ikon atau logo untuk AppClient. Tipe: String Wajib: Tidak
RedirecTurls	URL pengalihan yang diizinkan untuk. AppClient Tipe: Array string Anggota Array: Jumlah minimum 1 item. Jumlah maksimum 5 item. Batasan Panjang: Panjang minimum 1. Panjang maksimum 2048. Pola: `(http|https):\/\/[-a-zA-Z0-9_:.\/]+` Wajib: Ya

Parameter	Deskripsi
starterUserEmails	Alamat email pemula untuk pengguna yang diizinkan mengakses untuk menerima wawasan hingga AppClient diverifikasi. Tipe: Array string Anggota Array: Jumlah tetap 1 item. Batasan Panjang: Panjang minimum sebesar 0. Panjang maksimum 320. Pola: `[a-zA-Z0-9.!#$%&'*+/=?^_`{|}~-]+@[a-zA-Z0-9-]+(?:\.[a-zA-Z0-9-]+)*` Wajib: Ya
VerifikasiDetail	Berisi status dan alasan AppClient verifikasi. Tipe: Objek VerificationDetails Wajib: Ya
customerManagedKeyArn	Nama Sumber Daya Amazon (ARN) dari yang kunci yang dikelola pelanggan dihasilkan oleh AWS Key Management Service for the. AppClient Jenis: String Batasan Panjang: Panjang minimum 1. Panjang maksimum 1011. Pola: `arn:.+` Wajib: Tidak

Parameter	Deskripsi
appClientId	ID dari AppClient. Dimaksudkan untuk digunakan dalam aliran o-auth untuk klien aplikasi. Jenis: String Pola: `[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Wajib: Tidak

AppClientSummary

Fitur AWS AppFabric untuk produktivitas dalam pratinjau dan dapat berubah sewaktu-waktu.

Berisi informasi tentang sebuah AppClient.

Parameter	Deskripsi
arn	Nama Sumber Daya Amazon (ARN) dari. AppClient Jenis: String Batasan Panjang: Panjang minimum 1. Panjang maksimum 1011. Pola: `arn:.+` Wajib: Ya
VerifikasiStatus	Status AppClient verifikasi. Jenis: String Nilai yang Valid: `pending_verification | verified | rejected`

Parameter	Deskripsi
	Wajib: Ya
appClientId	ID dari AppClient. Dimaksudkan untuk digunakan dalam aliran o-auth untuk klien aplikasi. Jenis: String Pola: `[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Wajib: Tidak

MeetingInsights

Fitur AWS AppFabric untuk produktivitas dalam pratinjau dan dapat berubah sewaktu-waktu.

Berisi ringkasan dari 3 pertemuan teratas bersama dengan tujuan pertemuan, artefak lintas aplikasi terkait, dan aktivitas dari tugas, email, pesan, dan acara kalender.

Parameter	Deskripsi
InsightID	Id unik untuk wawasan yang dihasilkan.
InsightContent	Deskripsi wawasan yang menyoroti detail dalam format string. Seperti, mengapa wawasan ini penting.
InsightTitle	Judul wawasan yang dihasilkan.
createDat	Ketika wawasan dihasilkan.
KalenderEvent	Acara atau rapat kalender penting yang harus difokuskan pengguna. Kalender objek Acara: • `startTime` — Waktu mulai acara.

Parameter	Deskripsi
	• `endTime`— Waktu akhir acara. • `eventUrl`— URL untuk acara kalender di aplikasi ISV.
sumber daya	Daftar yang berisi sumber daya lain yang terkait dengan menghasilkan wawasan. Objek sumber daya: • `appName`— Nama aplikasi tempat sumber daya tersebut berada. • `resourceTitle` — Judul sumber daya. • `resourceType` — Jenis sumber daya. Nilai yang mungkin adalah: `EMAIL | EVENT | MESSAGE | TASK` • `resourceUrl` — URL sumber daya di aplikasi. • `appIconUrl` — URL gambar aplikasi tempat sumber daya berada.
NextToken	Token pagination untuk mengambil kumpulan wawasan berikutnya. Ini adalah bidang opsional yang jika dikembalikan null berarti tidak ada lagi wawasan untuk dimuat.

VerificationDetails

Fitur AWS AppFabric untuk produktivitas dalam pratinjau dan dapat berubah sewaktu-waktu.

Berisi status dan alasan AppClient verifikasi.

Parameter	Deskripsi
VerifikasiStatus	Status AppClient verifikasi. Jenis: String

Parameter	Deskripsi
	Nilai yang Valid: `pending_verification | verified | rejected` Wajib: Ya
StatusReason	Alasan status AppClient verifikasi. Jenis: String Batasan Panjang: Panjang minimum 1. Panjang maksimum 1024. Wajib: Tidak

Kesalahan umum

Fitur AWS AppFabric untuk produktivitas dalam pratinjau dan dapat berubah sewaktu-waktu.

Bagian ini mencantumkan kesalahan yang umum terjadi pada tindakan API untuk fitur AWS AppFabric produktivitas.

Untuk semua kesalahan API AppFabric umum lainnya, lihat Pemecahan Masalah dan kesalahan umum AWS AppFabric API di Referensi AWS AppFabric API.

Nama pengecualian	Deskripsi
TokenException	Permintaan token tidak valid. Kode Status HTTP: 400

Pemrosesan data

Fitur AWS AppFabric untuk produktivitas dalam pratinjau dan dapat berubah sewaktu-waktu.

AppFabric mengambil langkah-langkah untuk menyimpan konten pengguna satu per satu, dalam bucket Amazon S3 yang dikelola oleh AppFabric, dan secara terpisah; yang membantu memastikan bahwa kami menghasilkan wawasan khusus pengguna. Kami menggunakan perlindungan yang wajar untuk melindungi konten Anda, yang dapat mencakup enkripsi saat istirahat dan dalam perjalanan. Kami telah mengonfigurasi sistem kami untuk menghapus konten pelanggan secara otomatis dalam waktu 30 hari sejak konsumsi. AppFabric tidak menghasilkan wawasan menggunakan artefak data yang tidak lagi dapat diakses oleh pengguna. Misalnya, ketika pengguna memutuskan sumber data (aplikasi), AppFabric berhenti mengumpulkan data dari aplikasi tersebut dan tidak menggunakan artefak yang tersisa dari aplikasi yang terputus untuk menghasilkan wawasan. AppFabricSistem dikonfigurasi untuk menghapus data tersebut dalam waktu 30 hari.

AppFabric tidak menggunakan konten pengguna untuk melatih atau meningkatkan model bahasa besar yang mendasari yang digunakan untuk menghasilkan wawasan. Untuk informasi selengkapnya AppFabric tentang fitur AI generatif, lihat FAQ Amazon Bedrock.

Enkripsi diam

AWS AppFabric mendukung enkripsi saat istirahat, fitur enkripsi sisi server di mana AppFabric secara transparan mengenkripsi semua data yang terkait dengan pengguna saat disimpan ke disk, dan mendekripsi mereka saat Anda mengakses data.

Enkripsi bergerak

AppFabric mengamankan semua konten dalam perjalanan menggunakan TLS 1.2 dan menandatangani permintaan API untuk AWS layanan dengan AWS Signature Version 4.

Terminologi dan konsep

Topik ini menjelaskan terminologi dan konsep utama AWS AppFabric untuk membantu Anda memulai.

Bundel aplikasi

Bundel AppFabric aplikasi menyimpan semua otorisasi dan konsumsi AppFabric aplikasi Anda (lihat definisi konsumsi berikut). Anda dapat membuat satu bundel aplikasi per Akun AWS per Wilayah AWS.

AppClient (juga klien aplikasi dan klien aplikasi)

OAuth AppClient untuk aplikasi penerima data. Setiap aplikasi penerima data harus mendaftarkan AppFabric data AppClient untuk mengakses. Pengguna pengembang membutuhkan AWS akun untuk mendaftar AppClient. Setiap AWS akun hanya dapat mendaftarkan satu AppClient. AppFabric akan menjual token akses berdasarkan AppClient. AppClient akan berisi informasi seputar aplikasi penerima data yang akan mengakses AppFabric data melalui ini AppClient.

Otorisasi aplikasi

Otorisasi aplikasi memberikan AppFabric izin untuk terhubung dan berinteraksi dengan aplikasi Anda. Ini memungkinkan konsumsi log audit dari aplikasi Anda, dengan OAuth (Otorisasi Terbuka - standar terbuka untuk delegasi akses untuk memberikan akses aplikasi) atau kredensi token akses pribadi (PAT). Anda dapat menyiapkan beberapa otorisasi aplikasi (hingga 50) per bundel aplikasi. Hal ini memungkinkan AppFabric untuk menelan log audit dari beberapa penyewa aplikasi, dengan mengulangi langkah pembuatan otorisasi aplikasi sesuai kebutuhan untuk setiap penyewa aplikasi. Kredensil yang dibagikan dienkripsi dengan Kunci milik AWS atau kunci yang dikelola pelanggan dari AWS Key Management Service (AWS KMS), dan disimpan di. AppFabric

Tertelan

AppFabric Penyerapan menggunakan otorisasi aplikasi untuk menarik log audit dari aplikasi melalui API publik aplikasi. Kemudian mengirimkan log audit ke satu atau lebih (hingga lima) tujuan.

ID Klien

Saat Anda membuat otorisasi aplikasi untuk terhubung dengan aplikasi yang menggunakan alur OAuth, AppFabric mungkin akan meminta ID klien dan rahasia klien. ID klien dan rahasia klien dapat

ditemukan di aplikasi otentikasi aplikasi Anda. Untuk petunjuk tentang tempat menemukan ID klien di aplikasi autentikasi tertentu, lihat Aplikasi yang didukung. ID klien dan rahasia klien yang dibagikan dienkripsi dengan kunci AWS KMS kunci yang Kunci milik AWS dikelola pelanggan dan disimpan di dalamnya. AppFabric

Rahasia klien

Saat Anda membuat otorisasi aplikasi untuk terhubung dengan aplikasi yang menggunakan alur OAuth, AppFabric mungkin akan meminta ID klien dan rahasia klien. ID klien dan rahasia klien dapat ditemukan di aplikasi otentikasi aplikasi Anda. Untuk petunjuk tentang tempat menemukan rahasia klien di aplikasi autentikasi tertentu, lihat Aplikasi yang didukung. ID klien dan rahasia klien yang dibagikan dienkripsi dengan kunci AWS KMS kunci yang Kunci milik AWS dikelola pelanggan dan disimpan di dalamnya. AppFabric

Tujuan konsumsi

Tujuan konsumsi menentukan di mana log audit yang ditarik dari konsumsi harus disimpan. Setiap konsumsi dapat mengirimkan log audit ke satu atau beberapa tujuan (hingga lima), yang merupakan bucket Amazon Simple Storage Service (Amazon S3) atau Amazon Data Firehose di perangkat Anda. Akun AWS Untuk setiap tujuan, Anda dapat menentukan apakah Anda ingin log dalam bentuk mentah atau dinormalisasi ke dalam skema Open Cybersecurity Schema Framework (OCSF). Ketika Anda memilih skema OCSF, Anda dapat menentukan format log (JSON atau). Apache Parquet ApacheParquetFormat hanya dapat digunakan jika Amazon S3 dipilih sebagai tujuan.

Aplikasi penerima data

Aplikasi yang akan menelepon AppFabric untuk mendapatkan wawasan yang dihasilkan dari AppFabric.

OAuth

OAuth adalah protokol terbuka untuk memungkinkan otorisasi aman dalam metode sederhana dan standar dari aplikasi web, seluler, dan desktop. AppFabric menggunakan OAuth untuk membuat beberapa otorisasi aplikasi.

Kerangka Kerja Skema Keamanan Siber Terbuka (OCSF)

Open Cybersecurity Schema Framework (OCSF) adalah proyek open-source yang memberikan kerangka kerja yang dapat diperluas untuk mengembangkan skema, bersama dengan skema keamanan inti vendor-agnostik. Vendor dan produsen data lainnya dapat mengadopsi dan

memperluas skema untuk domain spesifik mereka. Tujuannya adalah untuk memberikan standar terbuka, diadopsi dalam lingkungan, aplikasi, atau solusi apa pun, sambil melengkapi standar dan proses keamanan yang ada. AppFabric telah memperluas skema ini untuk membuat struktur peristiwa yang berpusat pada perangkat lunak sebagai layanan (SaaS) yang didukung oleh semua log audit aplikasi SaaS akan dinormalisasi. AppFabric Untuk informasi selengkapnya, lihat Buka Kerangka Skema Keamanan Siber.

Token akses pribadi (PAT)

Personal Access Token (PAT) adalah serangkaian karakter yang dapat digunakan untuk mengakses sistem komputer alih-alih kata sandi biasa. Saat Anda membuat otorisasi aplikasi untuk terhubung dengan aplikasi yang menggunakan alur PAT, AppFabric mungkin meminta PAT. PAT dapat ditemukan di aplikasi otentikasi aplikasi Anda. Untuk petunjuk tentang tempat menemukan PAT di aplikasi autentikasi tertentu, lihat Aplikasi yang didukung. Token akun layanan yang dibagikan dienkripsi dengan kunci AWS KMS kunci yang Kunci milik AWS dikelola pelanggan dan disimpan di dalamnya. AppFabric

Token akun layanan

Saat Anda membuat otorisasi AppFabric aplikasi untuk terhubung dengan aplikasi, beberapa aplikasi akan memerlukan akun layanan yang akan dibuat untuk otentikasi aplikasi. AppFabric mungkin meminta token akun layanan sebagai bagian dari proses otorisasi aplikasi. Untuk petunjuk tentang tempat menemukan token akun layanan di aplikasi autentikasi tertentu, lihat Aplikasi yang didukung. Token akun layanan yang dibagikan dienkripsi dengan kunci AWS KMS kunci yang Kunci milik AWS dikelola pelanggan dan disimpan di dalamnya. AppFabric

ID Penyewa

Saat Anda membuat otorisasi aplikasi, AppFabric mungkin akan meminta ID penyewa dan nama penyewa aplikasi Anda. ID penyewa adalah pengenal unik untuk penyewa aplikasi Anda. Setiap aplikasi mungkin memiliki istilah yang berbeda untuk penyewa seperti ID Ruang Kerja untuk Slack atau ID Domain untuk. Asana Untuk petunjuk tentang tempat menemukan ID penyewa dalam aplikasi tertentu, lihat Aplikasi yang didukung.

Nama penyewa

Saat Anda membuat otorisasi aplikasi, AppFabric mungkin akan meminta ID penyewa dan nama penyewa aplikasi Anda. Nama penyewa adalah nama unik yang Anda berikan ke ID penyewa, untuk digunakan dalam bundel aplikasi. Nilai ini digunakan untuk memberi label otorisasi aplikasi dan konsumsi terkait apa pun.

Keamanan di AWS AppFabric

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

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

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

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

Topik

Perlindungan data di AWS AppFabric

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di AWS AppFabric. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk AWS layanan yang Anda gunakan. Untuk informasi selengkapnya tentang privasi data, lihat Privasi Data FAQ. Untuk informasi tentang perlindungan data di Eropa, lihat Model Tanggung Jawab AWS Bersama dan posting GDPR blog di Blog AWS Keamanan.

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

- Gunakan otentikasi multi-faktor (MFA) dengan setiap akun.
- GunakanSSL/TLSuntuk berkomunikasi dengan AWS sumber daya. Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya AWS layanan.
- Gunakan layanan keamanan terkelola lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan FIPS 140-3 modul kriptografi yang divalidasi saat mengakses AWS melalui antarmuka baris perintah atau, gunakan titik akhir. API FIPS Untuk informasi selengkapnya tentang FIPS titik akhir yang tersedia, lihat Federal Information Processing Standard (FIPS) 140-3.

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

Anda tidak menyertakan informasi kredensil dalam URL untuk memvalidasi permintaan Anda ke server tersebut.

> **Note**
>
> Untuk informasi selengkapnya tentang perlindungan data yang berlaku AppFabric untuk keamanan, lihatPemrosesan data.

Enkripsi diam

AWS AppFabric mendukung enkripsi saat istirahat, fitur enkripsi sisi server yang AppFabric secara transparan mengenkripsi semua data yang terkait dengan bundel aplikasi Anda saat disimpan ke disk, dan mendekripsi saat Anda mengakses data. Secara default, AppFabric mengenkripsi data Anda menggunakan Kunci milik AWS from AWS Key Management Service ()AWS KMS. Anda juga dapat memilih untuk mengenkripsi data Anda menggunakan kunci yang dikelola pelanggan Anda sendiri. AWS KMS

Saat Anda menghapus bundel aplikasi, semua metadatanya akan dihapus secara permanen.

Enkripsi bergerak

Saat mengonfigurasi bundel aplikasi, Anda dapat memilih kunci yang dikelola pelanggan Kunci milik AWS atau yang dikelola. Saat mengumpulkan dan menormalkan data untuk konsumsi log audit, AppFabric menyimpan data sementara di bucket Amazon Simple Storage Service (Amazon S3) perantara dan mengenkripsinya menggunakan kunci ini. Bucket perantara ini dihapus setelah 30 hari, menggunakan kebijakan siklus hidup bucket.

AppFabric mengamankan semua data dalam perjalanan menggunakan TLS 1.2 dan menandatangani API permintaan AWS layanan dengan AWS Signature V4.

Manajemen kunci

AppFabric mendukung enkripsi data dengan Kunci milik AWS atau kunci yang dikelola pelanggan. Kami menyarankan Anda menggunakan kunci yang dikelola pelanggan karena menempatkan Anda dalam kendali penuh atas data terenkripsi Anda. Saat Anda memilih kunci yang dikelola pelanggan, AppFabric lampirkan kebijakan sumber daya ke kunci yang dikelola pelanggan yang memberinya akses ke kunci yang dikelola pelanggan.

Kunci yang dikelola pelanggan

Untuk membuat kunci terkelola pelanggan, ikuti langkah-langkah untuk Membuat KMS kunci enkripsi simetris di Panduan AWS KMS Pengembang.

Kebijakan kunci

Kebijakan utama mengontrol akses ke kunci yang dikelola pelanggan Anda. Setiap kunci yang dikelola pelanggan harus memiliki persis satu kebijakan utama, yang berisi pernyataan yang menentukan siapa yang dapat menggunakan kunci dan bagaimana mereka dapat menggunakannya. Saat membuat kunci terkelola pelanggan, Anda dapat menentukan kebijakan kunci. Untuk informasi tentang membuat kebijakan kunci, lihat Membuat kebijakan kunci di Panduan AWS KMS Pengembang.

Untuk menggunakan kunci yang dikelola pelanggan AppFabric, AWS Identity and Access Management (IAM) pengguna atau peran yang membuat AppFabric sumber daya Anda harus memiliki izin untuk menggunakan kunci terkelola pelanggan Anda. Kami menyarankan Anda membuat kunci yang Anda gunakan hanya dengan AppFabric dan menambahkan AppFabric pengguna Anda sebagai pengguna kunci. Pendekatan ini membatasi ruang lingkup akses ke data Anda. Izin yang dibutuhkan pengguna Anda adalah sebagai berikut:

- `kms:DescribeKey`
- `kms:CreateGrant`
- `kms:GenerateDataKey`
- `kms:Decrypt`

AWS KMS Konsol memandu Anda membuat kunci dengan kebijakan kunci yang sesuai. Untuk informasi selengkapnya tentang kebijakan utama, lihat Kebijakan utama AWS KMS di Panduan AWS KMS Pengembang.

Berikut ini adalah contoh kebijakan kunci yang mengizinkan:

- Kontrol Pengguna root akun AWS penuh dari kunci.
- Pengguna diizinkan AppFabric untuk menggunakan kunci yang dikelola pelanggan Anda dengan AppFabric.
- Kebijakan utama untuk penyiapan bundel aplikasi di`us-east-1`.

```
{
    "Id": "key-consolepolicy-3",
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow access for key administrators",
            "Effect": "Allow",
            "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
            "Action": ["kms:*"],
            "Resource": "arn:aws:kms:us-east-1:111122223333:key/key_ID"
        },
        {
            "Sid": "Allow read-only access to key metadata to the account",
            "Effect": "Allow",
            "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
            "Action": [
                "kms:Describe*",
                "kms:Get*",
                "kms:List*",
                "kms:RevokeGrant"
            ],
            "Resource": "*"
        },
        {
            "Sid": "Allow access to principals authorized to use AWS AppFabric",
            "Effect": "Allow",
            "Principal": {"AWS": "IAM-role/user-creating-appfabric-resources"},
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey",
                "kms:DescribeKey",
                "kms:CreateGrant",
                "kms:ListAliases"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "appfabric.us-east-1.amazonaws.com",
                    "kms:CallerAccount": "111122223333"
                }
            }
        }
    ]
```

```
}
```

Bagaimana AppFabric menggunakan hibah di AWS KMS

AppFabric membutuhkan hibah untuk menggunakan kunci yang dikelola pelanggan Anda. Untuk informasi selengkapnya, lihat Hibah AWS KMS di Panduan AWS KMS Pengembang.

Saat Anda membuat app bundle, AppFabric buat hibah atas nama Anda dengan mengirimkan `CreateGrant` permintaan ke AWS KMS. Hibah AWS KMS digunakan untuk memberikan AppFabric akses ke AWS KMS kunci di akun pelanggan. AppFabric mengharuskan hibah untuk menggunakan kunci yang dikelola pelanggan Anda untuk operasi internal berikut:

- Kirim `GenerateDataKey` permintaan AWS KMS untuk menghasilkan kunci data yang dienkripsi oleh kunci terkelola pelanggan Anda.
- Kirim `Decrypt` permintaan AWS KMS ke untuk mendekripsi kunci data terenkripsi sehingga mereka dapat digunakan untuk mengenkripsi data Anda dan untuk mendekripsi token akses aplikasi dalam perjalanan.
- Kirim `Encrypt` permintaan AWS KMS untuk mengenkripsi token akses aplikasi dalam perjalanan.

Berikut ini adalah contoh hibah.

```
{
  "KeyId": "arn:aws:kms:us-east-1:111122223333:key/ff000af-00eb-00ce-0e00-
ea000fb0fba0SAMPLE",
  "GrantId": "0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE",
  "Name": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
  "CreationDate": "2022-10-11T20:35:39+00:00",
  "GranteePrincipal": "appfabric.us-east-1.amazonaws.com",
  "RetiringPrincipal": "appfabric.us-east-1.amazonaws.com",
  "IssuingAccount": "arn:aws:iam::111122223333:root",
  "Operations": [
    "Decrypt",
    "Encrypt",
    "GenerateDataKey"
  ],
  "Constraints": {
    "EncryptionContextSubset": {
      "appBundleArn": "arn:aws:fabric:us-east-1:111122223333:appbundle/
ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE"
    }
```

```
  }
},
```

Saat Anda menghapus paket aplikasi, AppFabric menghentikan hibah yang dikeluarkan pada kunci yang dikelola pelanggan Anda.

Memantau kunci enkripsi Anda untuk AppFabric

Saat menggunakan kunci terkelola AWS KMS pelanggan AppFabric, Anda dapat menggunakan AWS CloudTrail log untuk melacak permintaan yang AppFabric dikirim AWS KMS.

Berikut ini adalah contoh CloudTrail peristiwa yang dicatat saat AppFabric digunakan `CreateGrant` untuk kunci yang dikelola pelanggan Anda.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:SampleUser",
        "arn": "arn:aws:sts::111122223333:assumed-role/AssumedRole/SampleUser",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/AssumedRole",
                "accountId": "111122223333",
                "userName": "SampleUser"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-04-28T14:01:33Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-04-28T14:05:48Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "appfabric.amazonaws.com",
    "userAgent": "appfabric.amazonaws.com",
```

```
    "requestParameters": {
        "granteePrincipal": "appfabric.us-east-1.amazonaws.com",
        "constraints": {
            "encryptionContextSubset": {
                "appBundleArn": "arn:aws:appfabric:us-east-1:111122223333:appbundle/
ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE"
            }
        },
        "keyId": "arn:aws:kms:us-east-1:111122223333:key/EXAMPLEID",
        "retiringPrincipal": "appfabric.us-east-1.amazonaws.com",
        "operations": [
            "Encrypt",
            "Decrypt",
            "GenerateDataKey"
        ]
    },
    "responseElements": {
        "grantId": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
        "keyId": "arn:aws:kms:us-east-1:111122223333:key/KEY_ID"
    },
    "additionalEventData": {
        "grantId":
 "0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE"
    },
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": false,
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-east-1:111122223333:key/key_ID"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "sharedEventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_256_GCM_SHA384",
        "clientProvidedHostHeader": "kms.us-east-1.amazonaws.com"
    }
```

```
}
```

Identitas dan manajemen akses untuk AWS AppFabric

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

Topik

Audiens

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

Pengguna layanan — Jika Anda menggunakan AppFabric layanan untuk melakukan pekerjaan Anda, maka administrator Anda memberi Anda kredensi dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak AppFabric 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 AppFabric, lihatMemecahkan masalah AWS AppFabric identitas dan akses.

Administrator layanan — Jika Anda bertanggung jawab atas AppFabric sumber daya di perusahaan Anda, Anda mungkin memiliki akses penuh ke AppFabric. Tugas Anda adalah menentukan AppFabric fitur dan sumber daya mana yang harus diakses pengguna layanan Anda. Anda kemudian

harus mengirimkan permintaan ke IAM administrator Anda untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep dasarIAM. Untuk mempelajari lebih lanjut tentang bagaimana perusahaan Anda dapat menggunakannya IAM AppFabric, lihatBagaimana AWS AppFabric bekerja dengan IAM.

IAMadministrator - Jika Anda seorang IAM administrator, Anda mungkin ingin mempelajari detail tentang cara menulis kebijakan untuk mengelola akses AppFabric. Untuk melihat contoh kebijakan AppFabric berbasis identitas yang dapat Anda gunakan, lihat. IAM Contoh kebijakan berbasis identitas untuk AWS AppFabric

Mengautentikasi dengan identitas

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

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

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

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

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

Akun AWS pengguna root

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

Identitas gabungan

Sebagai praktik terbaik, mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses AWS layanan dengan menggunakan kredensi sementara.

Identitas federasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, direktori Pusat Identitas AWS Directory Service, atau pengguna mana pun yang mengakses AWS layanan dengan menggunakan kredensil yang disediakan melalui sumber identitas. Ketika identitas federasi mengakses Akun AWS, mereka mengambil peran, dan peran memberikan kredensi sementara.

Untuk manajemen akses terpusat, kami sarankan Anda menggunakan AWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat IAM Identitas, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua aplikasi Akun AWS dan aplikasi Anda. Untuk informasi tentang Pusat IAM Identitas, lihat Apa itu Pusat IAM Identitas? dalam AWS IAM Identity Center User Guide.

Pengguna dan grup IAM

IAMPengguna adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, sebaiknya mengandalkan kredensi sementara alih-alih membuat IAM pengguna yang memiliki kredensi jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan khusus yang memerlukan kredensi jangka panjang dengan IAM pengguna, kami sarankan Anda memutar kunci akses. Untuk informasi selengkapnya, lihat Memutar kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensi jangka panjang di IAMPanduan Pengguna.

IAMGrup adalah identitas yang menentukan kumpulan IAM pengguna. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat memiliki grup bernama IAMAdminsdan memberikan izin grup tersebut untuk mengelola sumber dayaIAM.

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

IAMperan

IAMPeran adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Ini mirip dengan IAM pengguna, tetapi tidak terkait dengan orang tertentu. Anda dapat mengambil IAM peran sementara AWS Management Console dengan beralih peran. Anda dapat mengambil peran dengan memanggil AWS CLI atau AWS API operasi atau dengan menggunakan kustomURL. Untuk informasi selengkapnya tentang metode penggunaan peran, lihat Menggunakan IAM peran di Panduan IAM Pengguna.

IAMperan dengan kredensi sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat Membuat peran untuk Penyedia Identitas pihak ketiga di Panduan IAM Pengguna. Jika Anda menggunakan Pusat IAM Identitas, Anda mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah diautentikasi, Pusat IAM Identitas mengkorelasikan izin yang disetel ke peran. IAM Untuk informasi tentang set izin, lihat Set izin dalam Panduan Pengguna AWS IAM Identity Center .
- Izin IAM pengguna sementara — IAM Pengguna atau peran dapat mengambil IAM peran untuk sementara mengambil izin yang berbeda untuk tugas tertentu.
- Akses lintas akun — Anda dapat menggunakan IAM peran untuk memungkinkan seseorang (prinsipal tepercaya) di akun lain mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa AWS layanan, Anda dapat melampirkan kebijakan langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy).

Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM Panduan Pengguna. IAM

- Akses lintas layanan — Beberapa AWS layanan menggunakan fitur lain AWS layanan. Misalnya, saat Anda melakukan panggilan dalam suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.
  - Sesi akses teruskan (FAS) — Saat Anda menggunakan IAM pengguna atau peran untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FASmenggunakan izin dari pemanggilan utama AWS layanan, dikombinasikan dengan permintaan AWS layanan untuk membuat permintaan ke layanan hilir. FASPermintaan hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain AWS layanan atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan saat membuat FAS permintaan, lihat Meneruskan sesi akses.
  - Peran layanan — Peran layanan adalah IAMperan yang diasumsikan layanan untuk melakukan tindakan atas nama Anda. IAMAdministrator dapat membuat, memodifikasi, dan menghapus peran layanan dari dalamIAM. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke AWS layanan dalam IAMPanduan Pengguna.
  - Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. AWS layanan Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. IAMAdministrator dapat melihat, tetapi tidak mengedit izin untuk peran terkait layanan.
- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan IAM peran untuk mengelola kredenal sementara untuk aplikasi yang berjalan pada EC2 instance dan membuat AWS CLI atau AWS API meminta. Ini lebih baik untuk menyimpan kunci akses dalam EC2 instance. Untuk menetapkan AWS peran ke EC2 instance dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instance berisi peran dan memungkinkan program yang berjalan pada EC2 instance untuk mendapatkan kredensi sementara. Untuk informasi selengkapnya, lihat Menggunakan IAM peran untuk memberikan izin ke aplikasi yang berjalan di EC2 instans Amazon di IAMPanduan Pengguna.

Untuk mempelajari apakah akan menggunakan IAM peran atau IAM pengguna, lihat Kapan membuat IAM peran (bukan pengguna) di Panduan IAM Pengguna.

Mengelola akses menggunakan kebijakan

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

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

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

IAMkebijakan menentukan izin untuk tindakan terlepas dari metode yang Anda gunakan untuk melakukan operasi. Misalnya, anggaplah Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan itu bisa mendapatkan informasi peran dari AWS Management Console, AWS CLI, atau AWS API.

Kebijakan berbasis identitas

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

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

Kebijakan berbasis sumber daya

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

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

Daftar kontrol akses (ACLs)

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

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung. ACLs Untuk mempelajari selengkapnyaACLs, lihat Ikhtisar daftar kontrol akses (ACL) di Panduan Pengembang Layanan Penyimpanan Sederhana Amazon.

Jenis-jenis kebijakan lain

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

- Batas izin — Batas izin adalah fitur lanjutan tempat Anda menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas (pengguna atau peran). IAM IAM Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batas izin, lihat Batas izin untuk IAM entitas di IAMPanduan Pengguna.
- Kebijakan kontrol layanan (SCPs) — SCPs adalah JSON kebijakan yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di AWS Organizations. AWS Organizations

adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur dalam suatu organisasi, maka Anda dapat menerapkan kebijakan kontrol layanan (SCPs) ke salah satu atau semua akun Anda. SCPMembatasi izin untuk entitas di akun anggota, termasuk masing-masing Pengguna root akun AWS. Untuk informasi selengkapnya tentang Organizations danSCPs, lihat Kebijakan kontrol layanan di Panduan AWS Organizations Pengguna.

- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan secara tegas dalam salah satu kebijakan ini membatalkan izin. Untuk informasi selengkapnya, lihat Kebijakan sesi di Panduan IAM Pengguna.

Berbagai jenis kebijakan

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

Bagaimana AWS AppFabric bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses AppFabric, pelajari IAM fitur apa yang tersedia untuk digunakan AppFabric.

IAMfitur yang dapat Anda gunakan dengan AWS AppFabric

IAMfitur	AppFabric dukungan
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
Kunci kondisi kebijakan	Tidak

IAMfitur	AppFabric dukungan
ACLs	Tidak
ABAC(tag dalam kebijakan)	Ya
Kredensial sementara	Tidak
Izin prinsipal	Ya
Peran layanan	Tidak
Peran terkait layanan	Ya

Untuk mendapatkan tampilan tingkat tinggi tentang cara AppFabric dan AWS layanan pekerjaan lainnya dengan sebagian besar IAM fitur, lihat AWS layanan yang berfungsi IAM di Panduan IAM Pengguna.

Kebijakan berbasis identitas untuk AppFabric

Mendukung kebijakan berbasis identitas: Ya

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

Dengan kebijakan IAM berbasis identitas, Anda dapat menentukan tindakan dan sumber daya yang diizinkan atau ditolak serta kondisi di mana tindakan diizinkan atau ditolak. Anda tidak dapat menentukan secara spesifik prinsipal dalam sebuah kebijakan berbasis identitas karena prinsipal berlaku bagi pengguna atau peran yang melekat kepadanya. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam JSON kebijakan, lihat referensi elemen IAM JSON kebijakan di Panduan IAM Pengguna.

Contoh kebijakan berbasis identitas untuk AppFabric

Untuk melihat contoh kebijakan AppFabric berbasis identitas, lihat. Contoh kebijakan berbasis identitas untuk AWS AppFabric

Kebijakan berbasis sumber daya dalam AppFabric

Mendukung kebijakan berbasis sumber daya: Tidak

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

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan seluruh akun atau IAM entitas di akun lain sebagai prinsipal dalam kebijakan berbasis sumber daya. Menambahkan prinsipal akun silang ke kebijakan berbasis sumber daya hanya setengah dari membangun hubungan kepercayaan. Ketika prinsipal dan sumber daya berbeda Akun AWS, IAM administrator di akun tepercaya juga harus memberikan izin entitas utama (pengguna atau peran) untuk mengakses sumber daya. Mereka memberikan izin dengan melampirkan kebijakan berbasis identitas kepada entitas. Namun, jika kebijakan berbasis sumber daya memberikan akses ke prinsipal dalam akun yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun IAM di Panduan IAM Pengguna.

Tindakan kebijakan untuk AppFabric

Mendukung tindakan kebijakan: Ya

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

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

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

Untuk melihat daftar AppFabric tindakan, lihat Tindakan yang ditentukan oleh AWS AppFabric dalam Referensi Otorisasi Layanan.

Tindakan kebijakan AppFabric menggunakan awalan berikut sebelum tindakan:

```
appfabric
```

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

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

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

```
"Action": "appfabric:List*"
```

Untuk melihat contoh kebijakan AppFabric berbasis identitas, lihat. Contoh kebijakan berbasis identitas untuk AWS AppFabric

Sumber daya kebijakan untuk AppFabric

Mendukung sumber daya kebijakan: Ya

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

Elemen `Resource` JSON kebijakan menentukan objek atau objek yang tindakan tersebut berlaku. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Sebagai praktik terbaik, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

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

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

Untuk melihat daftar jenis AppFabric sumber daya dan jenis sumber dayaARNs, lihat Jenis sumber daya yang ditentukan oleh AWS AppFabric dalam Referensi Otorisasi Layanan. Untuk mempelajari tindakan yang dapat Anda tentukan ARN dari setiap sumber daya, lihat Tindakan yang ditentukan oleh. AWS AppFabric

Untuk melihat contoh kebijakan AppFabric berbasis identitas, lihat. Contoh kebijakan berbasis identitas untuk AWS AppFabric

Kunci kondisi kebijakan untuk AppFabric

Mendukung kunci kondisi kebijakan khusus layanan: Tidak

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

Elemen `Condition` (atau blok `Condition`) akan memungkinkan Anda menentukan kondisi yang menjadi dasar suatu pernyataan berlaku. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi bersyarat yang menggunakan operator kondisi, misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta.

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

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Misalnya, Anda dapat memberikan izin IAM pengguna untuk mengakses sumber daya hanya jika ditandai dengan nama IAM pengguna mereka. Untuk informasi selengkapnya, lihat elemen IAM kebijakan: variabel dan tag di Panduan IAM Pengguna.

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

Untuk melihat daftar kunci AppFabric kondisi, lihat Kunci kondisi untuk AWS AppFabric dalam Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat Tindakan yang ditentukan oleh AWS AppFabric.

Untuk melihat contoh kebijakan AppFabric berbasis identitas, lihat. Contoh kebijakan berbasis identitas untuk AWS AppFabric

ACLsdi AppFabric

MendukungACLs: Tidak

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

ABACdengan AppFabric

Mendukung ABAC (tag dalam kebijakan): Ya

Attribute-based access control (ABAC) adalah strategi otorisasi yang mendefinisikan izin berdasarkan atribut. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tag ke IAM entitas (pengguna atau peran) dan ke banyak AWS sumber daya. Menandai entitas dan sumber daya adalah langkah pertama dari. ABAC Kemudian Anda merancang ABAC kebijakan untuk mengizinkan operasi ketika tag prinsipal cocok dengan tag pada sumber daya yang mereka coba akses.

ABACmembantu dalam lingkungan yang berkembang pesat dan membantu dengan situasi di mana manajemen kebijakan menjadi rumit.

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

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

Untuk informasi lebih lanjut tentangABAC, lihat Apa ituABAC? dalam IAMUser Guide. Untuk melihat tutorial dengan langkah-langkah penyiapanABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) di IAMPanduan Pengguna.

Menggunakan kredensi sementara dengan AppFabric

Mendukung kredensi sementara: Tidak

Beberapa AWS layanan tidak berfungsi saat Anda masuk menggunakan kredensil sementara. Untuk informasi tambahan, termasuk yang AWS layanan bekerja dengan kredensil sementara, lihat AWS layanan yang berfungsi IAM di IAMPanduan Pengguna.

Anda menggunakan kredensi sementara jika Anda masuk AWS Management Console menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, ketika Anda mengakses AWS menggunakan link sign-on (SSO) tunggal perusahaan Anda, proses tersebut secara otomatis membuat kredensi sementara. Anda juga akan secara otomatis membuat kredensial sementara ketika Anda masuk ke konsol sebagai seorang pengguna lalu beralih peran. Untuk informasi selengkapnya tentang beralih peran, lihat Beralih ke peran (konsol) di Panduan IAM Pengguna.

Anda dapat secara manual membuat kredensil sementara menggunakan atau. AWS CLI AWS API Anda kemudian dapat menggunakan kredensil sementara tersebut untuk mengakses. AWS AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensi sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensi keamanan sementara di. IAM

Izin utama lintas layanan untuk AppFabric

Mendukung sesi akses maju (FAS): Ya

Saat Anda menggunakan IAM pengguna atau peran untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FASmenggunakan izin dari pemanggilan utama AWS layanan, dikombinasikan dengan permintaan AWS layanan untuk membuat permintaan ke layanan hilir. FASPermintaan hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain AWS layanan atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan saat membuat FAS permintaan, lihat Meneruskan sesi akses.

Peran layanan untuk AppFabric

Mendukung peran layanan: Tidak

Peran layanan adalah IAMperan yang diasumsikan layanan untuk melakukan tindakan atas nama Anda. IAMAdministrator dapat membuat, memodifikasi, dan menghapus peran layanan dari

dalamIAM. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke AWS layanan dalam IAMPanduan Pengguna.

> **Warning**
>
> Mengubah izin untuk peran layanan dapat merusak AppFabric fungsionalitas. Edit peran layanan hanya jika AppFabric memberikan panduan untuk melakukannya.

Peran terkait layanan untuk AppFabric

Mendukung peran terkait layanan: Ya

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. AWS layanan Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. IAMAdministrator dapat melihat, tetapi tidak mengedit izin untuk peran terkait layanan.

Untuk detail tentang membuat atau mengelola peran AppFabric terkait layanan, lihat. Menggunakan peran terkait layanan untuk AppFabric

Contoh kebijakan berbasis identitas untuk AWS AppFabric

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi AppFabric sumber daya. Mereka juga tidak dapat melakukan tugas dengan menggunakan AWS Management Console, AWS Command Line Interface (AWS CLI), atau AWS API. Untuk memberikan izin kepada pengguna untuk melakukan tindakan pada sumber daya yang mereka butuhkan, IAM administrator dapat membuat IAM kebijakan. Administrator kemudian dapat menambahkan IAM kebijakan ke peran, dan pengguna dapat mengambil peran.

Untuk mempelajari cara membuat kebijakan IAM berbasis identitas menggunakan contoh dokumen kebijakan ini, lihat Membuat JSON IAM kebijakan di Panduan Pengguna. IAM

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh AppFabric, termasuk format ARNs untuk setiap jenis sumber daya, lihat Kunci tindakan, sumber daya, dan kondisi untuk AWS AppFabric dalam Referensi Otorisasi Layanan.

Daftar Isi

Praktik terbaik kebijakan

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

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat kebijakan AWSAWS terkelola atau kebijakan terkelola untuk fungsi pekerjaan di Panduan IAM Pengguna.
- Menerapkan izin hak istimewa paling sedikit — Saat Anda menetapkan izin dengan IAM kebijakan, berikan hanya izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya

tentang penggunaan IAM untuk menerapkan izin, lihat Kebijakan dan izin IAM di IAM Panduan Pengguna.

- Gunakan ketentuan dalam IAM kebijakan untuk membatasi akses lebih lanjut — Anda dapat menambahkan kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Misalnya, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakanSSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik AWS layanan, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat elemen IAM JSON kebijakan: Kondisi dalam Panduan IAM Pengguna.
- Gunakan IAM Access Analyzer untuk memvalidasi IAM kebijakan Anda guna memastikan izin yang aman dan fungsional — IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan mematuhi bahasa IAM kebijakan () JSON dan praktik terbaik. IAM IAMAccess Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat Validasi kebijakan IAM Access Analyzer di IAMPanduan Pengguna.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan IAM pengguna atau pengguna root di Anda Akun AWS, aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA kapan API operasi dipanggil, tambahkan MFA kondisi ke kebijakan Anda. Untuk informasi selengkapnya, lihat Mengonfigurasi API akses MFA yang dilindungi di IAMPanduan Pengguna.

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

Menggunakan konsol AppFabric

Lampirkan kebijakan `AWSAppFabricReadOnlyAccess` AWS terkelola ke IAM identitas Anda untuk memberi mereka izin hanya-baca ke AppFabric layanan, termasuk AppFabric konsol di. AWS Management Console Atau, Anda dapat melampirkan kebijakan `AWSAppFabricFullAccess` AWS terkelola ke IAM identitas Anda untuk memberi mereka izin administratif penuh ke AppFabric layanan. Untuk informasi selengkapnya, lihat AWS kebijakan terkelola untuk AWS AppFabric.

AppFabric untuk contoh IAM kebijakan keamanan

Contoh kebijakan berikut berlaku untuk fitur AppFabric untuk keamanan.

Izinkan akses ke bundel aplikasi

Contoh kebijakan berikut memberikan akses ke bundel aplikasi dalam layanan. AppFabric

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:StartUserAccessTasks",
                "appfabric:BatchGetUserAccessTasks"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appbundle/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Batasi akses ke bundel aplikasi

Contoh kebijakan berikut membatasi akses ke bundel aplikasi dalam layanan. AppFabric

```
{
    "Statement": [
        {
            "Action": ["appfabric:*"],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "appfabric:StartUserAccessTasks",
                "appfabric:BatchGetUserAccessTasks"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appbundle/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Batasi menghapus atau menghentikan konsumsi

Contoh kebijakan berikut membatasi penghapusan atau penghentian konsumsi dalam layanan. AppFabric

```
{
    "Statement": [
        {
            "Action": ["appfabric:*"],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "appfabric:StopIngestion",
                "appfabric:DeleteIngestion",
                "appfabric:DeleteIngestionDestination"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appbundle/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

AppFabric untuk contoh IAM kebijakan produktivitas

Fitur AWS AppFabric untuk produktivitas dalam pratinjau dan dapat berubah sewaktu-waktu.

Contoh kebijakan berikut berlaku AppFabric untuk fitur produktivitas.

Izinkan akses akses hanya-baca ke fitur produktivitas

Contoh kebijakan berikut memberikan akses hanya-baca ke fitur AppFabric untuk produktivitas.

> **Important**
>
> Anda mungkin melihat kesalahan tindakan yang tidak valid saat menambahkan kebijakan ini di editor JSON kebijakan konsol. IAM Ini karena fitur AppFabric untuk produktivitas saat

ini dalam pratinjau. Anda harus mengabaikan kesalahan dan melanjutkan untuk membuat kebijakan.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:GetAppClient",
                "appfabric:ListActionableInsights",
                "appfabric:ListAppClients",
                "appfabric:ListMeetingInsights"
            ],
            "Resource": "*"
        }
    ],
    "Version": "2012-10-17"
}
```

Izinkan akses penuh ke fitur produktivitas

Contoh kebijakan berikut memberikan akses penuh ke fitur AppFabric untuk produktivitas.

Important

Anda mungkin melihat kesalahan tindakan yang tidak valid saat menambahkan kebijakan ini di editor JSON kebijakan konsol. IAM Ini karena fitur AppFabric untuk produktivitas saat ini dalam pratinjau. Anda harus mengabaikan kesalahan dan melanjutkan untuk membuat kebijakan.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:CreateAppClient",
                "appfabric:DeleteAppClient",
                "appfabric:GetAppClient",
```

```
                "appfabric:ListActionableInsights",
                "appfabric:ListAppClients",
                "appfabric:ListMeetingInsights",
                "appfabric:PutFeedback",
                "appfabric:Token"
                "appfabric:UpdateAppClient"
            ],
            "Resource": "*"
        }
    ],
    "Version": "2012-10-17"
}
```

Izinkan akses untuk membuat AppClients

Contoh kebijakan berikut memberikan akses untuk membuat AppClients. Untuk informasi selengkapnya, lihat Membuat AppFabric untuk produktivitas AppClient.

> **Important**
>
> Anda mungkin melihat kesalahan tindakan yang tidak valid saat menambahkan kebijakan ini di editor JSON kebijakan konsol. IAM Ini karena fitur AppFabric untuk produktivitas saat ini dalam pratinjau. Anda harus mengabaikan kesalahan dan melanjutkan untuk membuat kebijakan.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:CreateAppClient"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Izinkan akses untuk mendapatkan detail AppClients

Contoh kebijakan berikut memberikan akses untuk mendapatkan detailnya. AppClients Untuk informasi selengkapnya, lihat Mendapatkan detail dari file AppClient.

> **Important**
>
> Anda mungkin melihat kesalahan tindakan yang tidak valid saat menambahkan kebijakan ini di editor JSON kebijakan konsol. IAM Ini karena fitur AppFabric untuk produktivitas saat ini dalam pratinjau. Anda harus mengabaikan kesalahan dan melanjutkan untuk membuat kebijakan.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:GetAppClient",
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Izinkan akses ke daftar AppClients

Contoh kebijakan berikut memberikan akses ke daftar AppClients. Untuk informasi selengkapnya, lihat Mendapatkan detail dari file AppClient.

> **Important**
>
> Anda mungkin melihat kesalahan tindakan yang tidak valid saat menambahkan kebijakan ini di editor JSON kebijakan konsol. IAM Ini karena fitur AppFabric untuk produktivitas saat ini dalam pratinjau. Anda harus mengabaikan kesalahan dan melanjutkan untuk membuat kebijakan.

```
{
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:ListAppClients"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Izinkan akses untuk memperbarui AppClients

Contoh kebijakan berikut memberikan akses ke pembaruan AppClients. Untuk informasi selengkapnya, lihat Memperbarui file AppClient.

> **Important**
>
> Anda mungkin melihat kesalahan tindakan yang tidak valid saat menambahkan kebijakan ini di editor JSON kebijakan konsol. IAM Ini karena fitur AppFabric untuk produktivitas saat ini dalam pratinjau. Anda harus mengabaikan kesalahan dan melanjutkan untuk membuat kebijakan.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:UpdateAppClient"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Izinkan akses untuk menghapus AppClients

Contoh kebijakan berikut memberikan akses untuk menghapus AppClients. Untuk informasi selengkapnya, lihat Memperbarui file AppClient.

> **Important**
>
> Anda mungkin melihat kesalahan tindakan yang tidak valid saat menambahkan kebijakan ini di editor JSON kebijakan konsol. IAM Ini karena fitur AppFabric untuk produktivitas saat ini dalam pratinjau. Anda harus mengabaikan kesalahan dan melanjutkan untuk membuat kebijakan.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:DeleteAppClient"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Izinkan akses untuk mengotorisasi aplikasi

Contoh kebijakan berikut memberikan akses untuk mengotorisasi aplikasi menggunakan Token. API Untuk informasi selengkapnya, lihat Mengautentikasi dan mengotorisasi aplikasi Anda.

> **Important**
>
> Anda mungkin melihat kesalahan tindakan yang tidak valid saat menambahkan kebijakan ini di editor JSON kebijakan konsol. IAM Ini karena fitur AppFabric untuk produktivitas saat ini dalam pratinjau. Anda harus mengabaikan kesalahan dan melanjutkan untuk membuat kebijakan.

```
{
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:Token"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Contoh IAM kebijakan lainnya

Mengizinkan pengguna melihat izin mereka sendiri

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

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

```
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Menggunakan peran terkait layanan untuk AppFabric

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

Peran terkait layanan membuat pengaturan AppFabric lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. AppFabric mendefinisikan izin peran terkait layanan, dan kecuali ditentukan lain, hanya AppFabric dapat mengambil perannya. Izin yang ditetapkan mencakup kebijakan kepercayaan dan kebijakan izin, dan kebijakan izin tersebut tidak dapat dilampirkan ke entitas lain. IAM

Anda dapat menghapus peran tertaut layanan hanya setelah menghapus sumber daya terkait terlebih dahulu. Ini melindungi AppFabric sumber daya Anda karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat AWS layanan yang bekerja dengan IAM dan cari layanan yang memiliki Ya di kolom Peran terkait layanan. Pilih Ya bersama tautan untuk melihat dokumentasi peran tertaut layanan untuk layanan tersebut.

Izin peran terkait layanan untuk AppFabric

AppFabric menggunakan peran terkait layanan bernama `AWSServiceRoleForAppFabric` — Memungkinkan AppFabric untuk menempatkan data di sumber daya tujuan konsumsi, seperti bucket Amazon S3 atau aliran pengiriman Amazon Data Firehose. Ini juga memungkinkan AppFabric untuk menempatkan data CloudWatch metrik di `AWS/AppFabric` namespace..

`AWSServiceRoleForAppFabric` peran terkait layanan memercayakan layanan berikut untuk menjalankan peran tersebut:

- `appfabric.amazonaws.com`

Kebijakan izin peran bernama `AWSAppFabricServiceRolePolicy` memungkinkan AppFabric untuk menyelesaikan tindakan berikut pada sumber daya yang ditentukan:

- Tindakan: `cloudwatch:PutMetricData` di `AWS/AppFabric` namespace. Tindakan ini memberikan izin untuk AppFabric memasukkan data metrik ke dalam CloudWatch `AWS/AppFabric` namespace Amazon. Untuk informasi selengkapnya tentang AppFabric metrik yang tersedia CloudWatch, lihatPemantauan AWS AppFabric dengan Amazon CloudWatch.
- Tindakan: `s3:PutObject` dalam ember Amazon S3. Tindakan ini memberikan izin untuk AppFabric memasukkan data tertelan ke dalam bucket Amazon S3 yang Anda tentukan.
- Tindakan: `firehose:PutRecordBatch` dalam aliran pengiriman Amazon Data Firehose. Tindakan ini memberikan izin AppFabric untuk memasukkan data yang tertelan ke dalam aliran pengiriman Amazon Data Firehose yang Anda tentukan.

Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AppFabric.

Anda harus mengonfigurasi izin agar pengguna, grup, atau peran Anda membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat Izin peran terkait layanan di Panduan Pengguna. IAM

Membuat peran terkait layanan untuk AppFabric

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda membuat bundel AppFabric aplikasi di AWS Management Console, AWS CLI, atau, akan AWS API AppFabric membuat peran terkait layanan untuk Anda.

Mengedit peran terkait layanan untuk AppFabric

AppFabric tidak memungkinkan Anda untuk mengedit peran `AWSServiceRoleForAppFabric` terkait layanan. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat mengedit deskripsi peran menggunakanIAM. Untuk informasi selengkapnya, lihat Mengedit peran terkait layanan di IAMPanduan Pengguna.

Menghapus peran terkait layanan untuk AppFabric

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran terkait layanan, kami merekomendasikan Anda menghapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan yang tidak dipantau atau dipelihara secara aktif. Namun, Anda harus menghapus semua paket AppFabric aplikasi sebelum dapat menghapus peran terkait layanan.

Membersihkan peran terkait layanan

Sebelum dapat digunakan IAM untuk menghapus peran terkait layanan, Anda harus terlebih dahulu menghapus sumber daya apa pun yang digunakan oleh peran tersebut. Bundel aplikasi yang Anda buat AppFabric digunakan oleh peran. Untuk informasi selengkapnya, lihat Hapus AWS AppFabric untuk sumber daya keamanan.

> **Note**
>
> Jika AppFabric layanan menggunakan peran saat Anda mencoba menghapus sumber daya, maka penghapusan mungkin gagal. Jika hal itu terjadi, tunggu beberapa menit dan coba mengoperasikannya lagi.

Untuk menghapus peran terkait layanan secara manual

Gunakan IAM konsol, AWS CLI, atau AWS API untuk menghapus peran `AWSServiceRoleForAppFabric` terkait layanan. Untuk informasi selengkapnya, lihat Menghapus peran terkait layanan di Panduan Pengguna. IAM

Wilayah yang Didukung untuk AppFabric peran terkait layanan

AppFabric mendukung penggunaan peran terkait layanan di semua Wilayah AWS tempat layanan tersedia. Untuk informasi lebih lanjut, lihat AppFabric titik akhir dan kuota di. Referensi Umum AWS

AWS kebijakan terkelola untuk AWS AppFabric

Untuk menambahkan izin ke pengguna, grup, dan peran, lebih mudah menggunakan kebijakan AWS terkelola daripada menulis kebijakan sendiri. Butuh waktu dan keahlian untuk membuat kebijakan terkelola IAM pelanggan yang hanya memberi tim Anda izin yang mereka butuhkan. Untuk memulai dengan cepat, Anda dapat menggunakan kebijakan AWS terkelola kami. Kebijakan ini mencakup

kasus penggunaan umum dan tersedia di Akun AWS Anda. Untuk informasi selengkapnya tentang kebijakan AWS AWS terkelola, lihat kebijakan terkelola di Panduan IAM Pengguna.

AWS layanan memelihara dan memperbarui kebijakan AWS terkelola. Anda tidak dapat mengubah izin dalam kebijakan AWS terkelola. Layanan terkadang menambahkan izin tambahan ke kebijakan yang dikelola AWS untuk mendukung fitur-fitur baru. Jenis pembaruan ini akan memengaruhi semua identitas (pengguna, grup, dan peran) di mana kebijakan tersebut dilampirkan. Layanan kemungkinan besar akan memperbarui kebijakan yang dikelola AWS saat ada fitur baru yang diluncurkan atau saat ada operasi baru yang tersedia. Layanan tidak menghapus izin dari kebijakan AWS terkelola, sehingga pembaruan kebijakan tidak akan merusak izin yang ada.

Selain itu, AWS mendukung kebijakan terkelola untuk fungsi pekerjaan yang mencakup beberapa layanan. Misalnya, kebijakan ReadOnlyAccess AWS terkelola menyediakan akses hanya-baca ke semua AWS layanan dan sumber daya. Saat layanan meluncurkan fitur baru, AWS tambahkan izin hanya-baca untuk operasi dan sumber daya baru. Untuk daftar dan deskripsi kebijakan fungsi pekerjaan, lihat kebijakan AWS terkelola untuk fungsi pekerjaan di Panduan IAM Pengguna.

AWS kebijakan terkelola: AWSAppFabricReadOnlyAccess

Anda dapat melampirkan `AWSAppFabricReadOnlyAccess` kebijakan ke IAM identitas Anda. Kebijakan ini memberikan izin hanya-baca ke layanan. AppFabric

> **Note**
>
> `AWSAppFabricReadOnlyAccess`Kebijakan ini tidak memberikan akses hanya-baca ke fitur AppFabric untuk produktivitas.

Detail izin

Kebijakan ini mencakup izin berikut:

- `appfabric`— Memberikan izin untuk mendapatkan bundel aplikasi, daftar bundel aplikasi, mendapatkan otorisasi aplikasi, daftar otorisasi aplikasi, mendapatkan konsumsi, mencantumkan konsumsi, mendapatkan tujuan konsumsi, daftar tujuan konsumsi, dan daftar tag sumber daya.

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

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:GetAppAuthorization",
                "appfabric:GetAppBundle",
                "appfabric:GetIngestion",
                "appfabric:GetIngestionDestination",
                "appfabric:ListAppAuthorizations",
                "appfabric:ListAppBundles",
                "appfabric:ListIngestionDestinations",
                "appfabric:ListIngestions",
                "appfabric:ListTagsForResource"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS kebijakan terkelola: AWSAppFabricFullAccess

Anda dapat melampirkan `AWSAppFabricFullAccess` kebijakan ke IAM identitas Anda. Kebijakan ini memberikan izin administratif ke layanan. AppFabric

> **Important**
>
> `AWSAppFabricFullAccess`Kebijakan ini tidak memberikan akses ke fitur AppFabric untuk produktivitas karena fitur tersebut saat ini dalam pratinjau. Untuk informasi selengkapnya tentang mengomel akses ke fitur AppFabric untuk produktivitas, lihat[AppFabric untuk contoh IAM kebijakan produktivitas](#).

Detail izin

Kebijakan ini mencakup izin berikut:

- `appfabric`— Memberikan izin administratif penuh untuk AppFabric.
- `kms`— Memberikan izin untuk membuat daftar alias.
- `s3`— Memberikan izin untuk membuat daftar semua bucket Amazon S3 Anda, dan dapatkan lokasi bucket.

- `firehose`— Memberikan izin untuk mencantumkan aliran pengiriman Amazon Data Firehose, dan menjelaskan aliran pengiriman.
- `iam`— Memberikan izin untuk membuat peran `AWSServiceRoleForAppFabric` terkait layanan untuk. AppFabric Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan untuk AppFabric.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["appfabric:*"],
            "Resource": "*"
        },
        {
            "Sid": "KMSListAccess",
            "Effect": "Allow",
            "Action": ["kms:ListAliases"],
            "Resource": "*"
        },
        {
            "Sid": "S3ReadAccess",
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "FirehoseReadAccess",
            "Effect": "Allow",
            "Action": [
                "firehose:DescribeDeliveryStream",
                "firehose:ListDeliveryStreams"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowUseOfServiceLinkedRole",
            "Effect": "Allow",
```

```
            "Action": ["iam:CreateServiceLinkedRole"],
            "Condition": {
                "StringEquals": {"iam:AWSServiceName": "appfabric.amazonaws.com"}
            },
            "Resource": "arn:aws:iam::*:role/aws-service-role/appfabric.amazonaws.com/
AWSServiceRoleForAppFabric"
        }
    ]
}
```

AWS kebijakan terkelola: AWSAppFabricServiceRolePolicy

Anda tidak dapat melampirkan `AWSAppFabricServiceRolePolicy` kebijakan ke IAM entitas Anda. Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan AppFabric untuk melakukan tindakan atas nama Anda. Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan untuk AppFabric.

Detail izin

Kebijakan ini mencakup izin berikut:

- `cloudwatch`— Memberikan izin untuk AppFabric memasukkan data metrik ke dalam CloudWatch `AWS/AppFabric` namespace Amazon. Untuk informasi selengkapnya tentang AppFabric metrik yang tersedia CloudWatch, lihatPemantauan AWS AppFabric dengan Amazon CloudWatch.
- `s3`— Memberikan izin AppFabric untuk memasukkan data yang tertelan ke dalam bucket Amazon S3 yang Anda tentukan.
- `firehose`— Memberikan izin AppFabric untuk memasukkan data yang tertelan ke dalam aliran pengiriman Amazon Data Firehose yang Anda tentukan.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CloudWatchEmitMetric",
            "Effect": "Allow",
            "Action": ["cloudwatch:PutMetricData"],
            "Resource": "*",
            "Condition": {
                "StringEquals": {"cloudwatch:namespace": "AWS/AppFabric"}
            }
```

```
        },
        {
            "Sid": "S3PutObject",
            "Effect": "Allow",
            "Action": ["s3:PutObject"],
            "Resource": "arn:aws:s3:::*/AWSAppFabric/*",
            "Condition": {
                "StringEquals": {"s3:ResourceAccount": "${aws:PrincipalAccount}"}
            }
        },
        {
            "Sid": "FirehosePutRecord",
            "Effect": "Allow",
            "Action": ["firehose:PutRecordBatch"],
            "Resource": "arn:aws:firehose:*:*:deliverystream/*",
            "Condition": {
                "StringEqualsIgnoreCase": {"aws:ResourceTag/AWSAppFabricManaged":
 "true"}
            }
        }
    ]
}
```

AppFabric pembaruan kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola AppFabric sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan RSS feed di halaman Riwayat AppFabric dokumen.

Perubahan	Deskripsi	Tanggal
AWSAppFabricReadOnlyAccess – Kebijakan baru	AppFabric menambahkan kebijakan baru untuk memberikan izin hanya-baca ke layanan. AppFabric	Juni 27, 2023
AWSAppFabricFullAccess – Kebijakan baru	AppFabric menambahkan kebijakan baru untuk memberikan izin administratif ke AppFabric layanan.	Juni 27, 2023

Perubahan	Deskripsi	Tanggal
AWSAppFabricServiceRolePolicy – Kebijakan baru	AppFabric menambahkan kebijakan baru untuk peran `AWSServiceRoleForAppFabric` terkait layanan.	Juni 27, 2023
AppFabric mulai melacak perubahan	AppFabric mulai melacak perubahan untuk kebijakan yang AWS dikelola.	Juni 27, 2023

Memecahkan masalah AWS AppFabric identitas dan akses

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan AppFabric danIAM.

Topik

- Saya tidak berwenang untuk melakukan tindakan di AppFabric
- Saya tidak berwenang untuk melakukan iam:PassRole
- Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses AppFabric sumber daya saya

Saya tidak berwenang untuk melakukan tindakan di AppFabric

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 `mateojackson` IAM pengguna mencoba menggunakan konsol untuk melihat detail tentang *`my-example-widget`* sumber daya fiksi tetapi tidak memiliki izin `appfabric:`*`GetWidget`* fiksi.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 appfabric: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 `appfabric:`*`GetWidget`*.

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

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 AppFabric.

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

Contoh kesalahan berikut terjadi ketika IAM pengguna bernama `marymajor` mencoba menggunakan konsol untuk melakukan tindakan di AppFabric. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

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

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

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

Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses AppFabric sumber daya saya

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

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mempelajari apakah AppFabric mendukung fitur-fitur ini, lihatBagaimana AWS AppFabric bekerja dengan IAM.

- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat Menyediakan akses ke IAM pengguna lain Akun AWS yang Anda miliki di Panduan IAM Pengguna.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga dalam Panduan IAM Pengguna.
- Untuk mempelajari cara menyediakan akses melalui federasi identitas, lihat Menyediakan akses ke pengguna yang diautentikasi secara eksternal (federasi identitas) di Panduan Pengguna. IAM
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM Panduan Pengguna. IAM

Validasi kepatuhan untuk AWS AppFabric

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

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

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

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

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

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

Praktik terbaik keamanan untuk AWS AppFabric

AWS AppFabric menyediakan beberapa 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 cukup untuk lingkungan Anda, anggap sebagai pertimbangan yang membantu dan bukan sebagai resep.

Memantau aplikasi tanpa akses admin

Dengan izin read-only AWS Identity and Access Management (IAM), siapa pun dapat berintegrasi dengan AppFabric Amazon QuickSight dan informasi keamanan lainnya dan alat manajemen

peristiwa (SIEM), seperti. Splunk Untuk memantau keamanan aplikasi, data dikirimkan ke bucket Amazon Simple Storage Service (Amazon S3) atau aliran pengiriman Amazon Data Firehose.

Memantau AppFabric acara

Anda dapat memantau AppFabric menggunakan CloudWatch metrik Amazon. CloudWatch mengumpulkan data dari AppFabric setiap menit dan memprosesnya menjadi metrik. Anda dapat menyetel alarm yang menonaktifkan notifikasi saat metrik cocok dengan ambang batas yang ditentukan. Untuk informasi selengkapnya, lihat Pemantauan AWS AppFabric dengan Amazon CloudWatch.

Ketahanan di AWS AppFabric

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

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

Keamanan infrastruktur di AWS AppFabric

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

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

Selain itu, permintaan harus ditandatangani dengan menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan IAM prinsipal. Atau, untuk menghasilkan kredensil keamanan sementara

untuk menandatangani permintaan, Anda dapat menggunakan AWS Security Token Service()AWS STS.

Konfigurasi dan analisis kerentanan di AWS AppFabric

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

Pemantauan AWS AppFabric

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

- Amazon CloudWatch memantau AWS sumber daya Anda dan aplikasi yang Anda jalankan AWS secara real time. Anda dapat mengumpulkan dan melacak metrik, membuat dasbor yang disesuaikan, dan mengatur alarm yang memberi tahu Anda atau mengambil tindakan saat metrik tertentu mencapai ambang batas yang ditentukan. Misalnya, Anda dapat CloudWatch melacak penggunaan CPU atau metrik lain dari instans Amazon EC2 Anda dan secara otomatis meluncurkan instans baru bila diperlukan. Untuk informasi selengkapnya, lihat Panduan CloudWatch Pengguna Amazon.
- Amazon CloudWatch Logs memungkinkan Anda memantau, menyimpan, dan mengakses file log Anda dari instans Amazon EC2, AWS CloudTrail, dan sumber lainnya. CloudWatch Log dapat memantau informasi dalam file log dan memberi tahu Anda ketika ambang batas tertentu terpenuhi. Anda juga dapat mengarsipkan data log dalam penyimpanan yang sangat durabel. Untuk informasi selengkapnya, lihat Panduan Pengguna Amazon CloudWatch Logs.
- AWS CloudTrailmenangkap panggilan API dan peristiwa terkait yang dibuat oleh atau atas nama Anda Akun AWS dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. Untuk informasi selengkapnya, silakan lihat Panduan Pengguna AWS CloudTrail.

Pemantauan AWS AppFabric dengan Amazon CloudWatch

Anda dapat memantau AWS AppFabric penggunaan CloudWatch, yang mengumpulkan data mentah dan memprosesnya menjadi metrik yang dapat dibaca, mendekati waktu nyata. Statistik ini disimpan untuk jangka waktu 15 bulan, sehingga Anda dapat mengakses informasi historis dan mendapatkan perspektif yang lebih baik tentang performa aplikasi atau layanan web Anda. Anda juga dapat mengatur alarm yang memperhatikan ambang batas tertentu dan mengirim notifikasi atau mengambil tindakan saat ambang batas tersebut terpenuhi. Untuk informasi selengkapnya, lihat Panduan CloudWatch Pengguna Amazon.

AppFabric Layanan melaporkan metrik berikut di `AWS/AppFabric` namespace.

Metrik	Deskripsi
AppFabric Status Otorisasi Aplikasi	Status otorisasi aplikasi (1untuk terhubung; `0` untuk yang lain).
AppFabric Latensi Pengiriman Data	Waktu yang dibutuhkan (dalam hitungan detik) AppFabric untuk mengumpulkan log audit dari aplikasi SaaS dan mengirimkannya ke tujuan yang dikonfigurasi (Amazon S3 atau Amazon Data Firehose).
Status Tujuan Tertelan	Status tujuan konsumsi (1untuk aktif; `0` untuk yang lain).
Keterlambatan Data Keseluruhan	Perbedaan waktu (dalam detik) antara saat peristiwa terjadi pada aplikasi SaaS dan ketika log audit terkait dikirim ke tujuan yang dikonfigurasi (Amazon S3 atau Amazon Data Firehose) oleh. AppFabric
Volume Data yang Tertelan	Ukuran data yang dikirimkan ke Amazon Simple Storage Service (Amazon S3) atau Amazon Data Firehose.

Dimensi berikut didukung untuk AppFabric metrik.

Dimensi	Deskripsi
Tujuan Tertelan Arn	Nama Sumber Daya Amazon (ARN) dari tujuan konsumsi.

Logging panggilan AWS AppFabric API menggunakan AWS CloudTrail

AWS AppFabric terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan dalam AppFabric. CloudTrail menangkap

semua panggilan API untuk AppFabric sebagai peristiwa. Panggilan yang diambil termasuk panggilan dari AppFabric konsol dan panggilan kode ke operasi AppFabric API. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara berkelanjutan ke bucket Amazon S3, termasuk acara untuk. AppFabric Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat AppFabric, alamat IP dari mana permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Untuk informasi selengkapnya CloudTrail, lihat Panduan AWS CloudTrail Pengguna.

AppFabric informasi di CloudTrail

CloudTrail diaktifkan pada Akun AWS saat Anda membuat akun. Ketika aktivitas terjadi AppFabric, aktivitas tersebut dicatat dalam suatu CloudTrail peristiwa bersama dengan AWS layanan peristiwa lain dalam sejarah Peristiwa. Anda dapat melihat, mencari, dan mengunduh peristiwa terbaru di Akun AWS Anda. Untuk informasi selengkapnya, lihat Melihat CloudTrail peristiwa dengan riwayat peristiwa di Panduan AWS CloudTrail Pengguna.

Untuk catatan acara yang sedang berlangsung di Anda Akun AWS, termasuk acara untuk AppFabric, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di konsol, jejak tersebut berlaku untuk semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di AWS partisi dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi lainnya AWS layanan untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat topik berikut di Panduan Pengguna AWS CloudTrail :

- Ikhtisar untuk membuat jejak
- CloudTrail layanan dan integrasi yang didukung
- Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail
- Menerima file CloudTrail log dari beberapa Wilayah dan Menerima file CloudTrail log dari beberapa akun

Semua AppFabric tindakan dicatat oleh CloudTrail dan didokumentasikan dalam Referensi AWS AppFabric API. Misalnya, panggilan ke`CreateAppBundle`,`UpdateAppBundle`, dan `GetAppBundle` tindakan menghasilkan entri dalam file CloudTrail log.

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

- Apakah permintaan itu dibuat dengan kredenal pengguna root atau AWS Identity and Access Management (IAM).
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna terfederasi.
- Apakah permintaan tersebut dibuat oleh AWS layanan lain.

Untuk informasi selengkapnya, lihat CloudTrail userIdentityelemen dalam Panduan AWS CloudTrail Pengguna.

Memahami entri file AppFabric log

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

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan `CreateAppBundle` tindakan.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:SampleUser",
        "arn": "arn:aws:sts::111122223333:assumed-role/AssumedRole/SampleUser",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAXUFER33B4FVC2GCYR",
                "arn": "arn:aws:iam::111122223333:role/AssumedRole",
                "accountId": "111122223333",
                "userName": "SampleUser"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-05-31T21:11:15Z",
                "mfaAuthenticated": "false"
```

```
            }
        }
    },
    "eventTime": "2023-05-31T21:22:16Z",
    "eventSource": "appfabric.amazonaws.com",
    "eventName": "CreateAppBundle",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "3.90.81.91",
    "userAgent": "Coral/Apache-HttpClient5",
    "requestParameters": {
        "clientToken": "64d9069f-e565-49a4-9374-6dc8631142e2"
    },
    "responseElements": {
        "appBundle": {
            "arn": "arn:aws:appfabric:us-
east-1:111122223333:appbundle/6aa92da0-5eeb-4ff4-aabf-4db7fd022ad1",
            "idpClientConfiguration": {
                "samlAudience": "urn:amazon:cognito:sp:us-east-1_GEdGiavzr",
                "samlRedirect": "https://6aa92da0-5eeb-4ff4-aabf-4db7fd022ad1.auth.us-
east-1.amazoncognito.com/saml2/idpresponse",
                "oidcRedirect": "https://6aa92da0-5eeb-4ff4-aabf-4db7fd022ad1.auth.us-
east-1.amazoncognito.com/oauth2/idpresponse"
            }
        }
    },
    "requestID": "17e15a5d-8c66-46c7-ad5b-f521004fa9c2",
    "eventID": "ba1dd847-86f6-4386-85be-0398e844a358",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
    "tlsDetails": {
        "clientProvidedHostHeader": "frontend.fabric.us-east-1.amazonaws.com"
    }
}
```

Kuota untuk AWS AppFabric

Anda Akun AWS memiliki kuota default, sebelumnya disebut sebagai batas, untuk masing-masing. AWS layanan Kecuali dinyatakan lain, setiap kuota bersifat khusus per Wilayah. Anda dapat meminta peningkatan untuk beberapa kuota dan kuota lainnya tidak dapat ditingkatkan.

Untuk melihat kuota AppFabric, buka konsol Service Quotas. Di panel navigasi, pilih AWS layanan dan pilih AppFabric.

Untuk meminta penambahan kuota, lihat Meminta penambahan kuota di Panduan Pengguna Service Quotas. Jika kuota belum tersedia dalam Service Quotas, gunakan formulir penambahan batas.

Kuota AppFabric yang terkait dengan yang ada di Anda Akun AWS ditunjukkan pada tabel berikut.

Nama	Default	Dapat disesu an	Deskripsi
Bundel aplikasi	Setiap Wilayah yang didukung: 1	Tidak	Jumlah maksimum bundel aplikasi yang dapat Anda buat di akun di AWS Wilayah saat ini.
Otorisasi aplikasi	Setiap Wilayah yang didukung: 50	Tidak	Jumlah maksimum otorisasi aplikasi yang dapat Anda buat di akun di AWS Wilayah saat ini.
Tertelan	Setiap Wilayah yang didukung: 50	Tidak	Jumlah maksimum konsumsi yang dapat Anda buat di akun di Wilayah saat ini AWS .
Tujuan konsumsi	Setiap Wilayah yang didukung: 5	Tidak	Jumlah maksimum tujuan konsumsi yang dapat Anda buat per konsumsi di akun di Wilayah saat ini. AWS

Nama	Default	Dapat disesu an	Deskripsi
AppClient	Setiap Wilayah yang didukung: 1	Tidak	Jumlah maksimum AppClients yang dapat Anda buat di akun di AWS Wilayah saat ini. Fitur AWS AppFabric untuk produktivitas ada dalam pratinjau dan dapat berubah sewaktu-waktu.

Riwayat dokumen untuk Panduan AppFabric Administrasi

Tabel berikut menjelaskan rilis dokumentasi untuk AWS AppFabric.

Perubahan	Deskripsi	Tanggal
Aplikasi baru yang didukung	Ditambahkan JumpCloud sebagai aplikasi yang didukung. Untuk informasi selengkapnya, lihat Aplikasi yang didukung di AWS AppFabric.	Juni 5, 2024
Aplikasi dan alat keamanan baru yang didukung	Ditambahkan Azure Monitor dan Google Analytics sebagai aplikasi yang didukung. Untuk informasi selengkapnya, lihat Aplikasi yang didukung di AWS AppFabric. Ditambahk an Singularity Cloud sebagai alat keamanan yang didukung. Untuk informasi selengkap nya lihat Alat keamanan yang kompatibel.	April 30, 2024
Aplikasi baru yang didukung	Ditambahkan SentinelO ne sebagai aplikasi yang didukung. Untuk informasi selengkapnya, lihat Aplikasi yang didukung di AWS AppFabric.	April 25, 2024
Aplikasi baru yang didukung	Ditambahkan 1Password sebagai aplikasi yang didukung. Untuk informasi selengkapnya, lihat Aplikasi	April 23, 2024

	yang didukung di AWS AppFabric.	
Alat keamanan baru yang didukung	Ditambahkan Dynatrace sebagai alat keamanan yang kompatibel. Untuk informasi selengkapnya lihat Alat keamanan yang kompatibel.	Maret 26, 2024
Metrik baru	Menambahkan metrik Status Otorisasi AppFabric Aplikasi. Untuk informasi selengkap nya, lihat Memantau AWS AppFabric dengan CloudWatc h Log Amazon.	8 Maret 2024
Aplikasi baru yang didukung	Ditambahkan IBM Security® Verify sebagai aplikasi yang didukung. Untuk informasi selengkapnya, lihat Aplikasi yang didukung di AWS AppFabric.	6 Maret 2024
Aplikasi baru yang didukung	Ditambahkan Box sebagai aplikasi yang didukung. Untuk informasi selengkapnya, lihat Aplikasi yang didukung di AWS AppFabric.	Februari 28, 2024

Aplikasi dan metrik baru yang didukung	DitambahkanCisco Duo,Sales force, dan Terraform Cloud sebagai aplikasi yang didukung. Untuk informasi selengkapnya tentang mereka, lihat Aplikasi yang didukung di AWS AppFabric. Menambahkan metrik Latensi Pengiriman AppFabric Data dan Keterlambatan Data Keseluruhan. Untuk informasi selengkapnya, lihat Memantau AWS AppFabric dengan CloudWatch Log Amazon.	Februari 1, 2024
Ditambahkan Atlassian ConfluenceGenesys Cloud,HubSpot,,OneLogin by One Identity,PagerDuty, dan Ping Identity sebagai aplikasi yang didukung dan Barracuda XDR sebagai alat keamanan yang kompatibel	Untuk informasi selengkapnya tentang aplikasi baru yang didukung, lihat Aplikasi yang didukung di AWS AppFabric dan Alat keamanan yang kompatibel.	15 Desember 2023
Ditambahkan Atlassian ConfluenceGenesys Cloud,HubSpot,,OneLogin by One Identity,PagerDuty, dan Ping Identity sebagai aplikasi yang didukung dan Barracuda XDR sebagai alat keamanan yang kompatibel	Untuk informasi selengkapnya tentang aplikasi baru yang didukung, lihat Aplikasi yang didukung di AWS AppFabric dan Alat keamanan yang kompatibel.	15 Desember 2023

Ditambahkan AWS AppFabric untuk dokumentasi pratinjau produktivitas	Untuk informasi selengkapnya tentang AppFabric produktiv itas, lihat Apa yang dimaksud AWS AppFabric dengan produktivitas?	27 November 2023
Ditambahkan GitHub dan ServiceNow sebagai aplikasi yang didukung	Untuk informasi selengkap nya tentang aplikasi baru yang didukung, lihat Aplikasi yang didukung.	31 Oktober 2023
Mulai melacak kebijakan AWS terkelola untuk AWS AppFabric	Untuk informasi selengkap nya tentang kebijakan AWS terkelola AppFabric, lihat kebijakan AWS terkelola untuk AWS AppFabric.	Juni 27, 2023
Rilis awal	Rilis awal Panduan AWS AppFabric Administrasi.	Juni 27, 2023

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