aws

Panduan Administrator

Rantai Pasokan AWS

Rantai Pasokan AWS: Panduan Administrator

Table of Contents

Apa itu Rantai Pasokan AWS?

Rantai Pasokan AWS adalah aplikasi manajemen rantai pasokan berbasis cloud yang menyatukan data dan menyediakan metode peramalan bertenaga ML untuk meningkatkan peramalan permintaan dan visibilitas inventaris, wawasan yang dapat ditindaklanjuti, kolaborasi kontekstual bawaan, perencanaan permintaan, perencanaan pasokan, visibilitas pemasok n-tier, dan manajemen informasi keberlanjutan. Rantai Pasokan AWS dapat terhubung ke perencanaan sumber daya perusahaan (ERP) dan sistem manajemen rantai pasokan yang ada dan menggunakan AI dan AI generatif untuk mengubah dan mengintegrasikan data yang berbeda ke dalam danau data rantai pasokan (SCDL). AWS Supply Chain dapat meningkatkan manajemen risiko rantai pasokan tanpa melakukan replatforming, biaya lisensi di muka, atau komitmen jangka panjang.

Topik

Browser yang didukung oleh Rantai Pasokan AWS

Sebelum Anda bekerja dengan AWS Supply Chain, verifikasi bahwa browser Anda didukung menggunakan tabel berikut.

Peramban	Versi yang Didukung
Google Chrome	Tiga versi terbaru.
Mozilla Firefox ESR	Versi didukung hingga end-of-lifetanggal Firefox mereka. Untuk detailnya, lihat kalender rilis ESR Firefox.
Mozilla Firefox	Tiga versi terbaru.
Microsoft Edge dan Edge Chromium	Versi 84 dan yang lebih baru.
Safari	Safari 10 atau lebih baru di macOS.

Bahasa yang didukung oleh Rantai Pasokan AWS

Rantai Pasokan AWS mendukung bahasa-bahasa berikut:

- Inggris (US)
- Inggris (UK)
- Bahasa Jerman
- Bahasa Spanyol
- Prancis
- Bahasa Italia
- Bahasa Portugis
- Mandarin (Sederhana)
- Mandarin (Tradisional)
- Bahasa Jepang
- Bahasa Korea

Menyiapkan AWS akun

Gunakan bagian ini untuk membuat AWS akun dan membuat pengguna IAM. Untuk informasi tentang praktik terbaik untuk membuat AWS akun, lihat Menetapkan AWS lingkungan praktik terbaik Anda.

Topik

- Mendaftar untuk Akun AWS
- Buat pengguna dengan akses administratif

Mendaftar untuk Akun AWS

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

Untuk mendaftar untuk Akun AWS

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

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

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

AWS mengirimi Anda email konfirmasi setelah proses pendaftaran selesai. Kapan saja, Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan masuk https://aws.amazon.comke/ 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.

Prasyarat untuk digunakan Rantai Pasokan AWS

Sebelum Anda membuat Rantai Pasokan AWS instance, pastikan Anda menyelesaikan langkah-langkah berikut:

- Anda memiliki sebuah Akun AWS. Untuk membuat Akun AWS, lihatMenyiapkan AWS akun.
- Pastikan IAM Identity Center diaktifkan. Untuk mengaktifkan Pusat Identitas IAM, lihat Mengaktifkan Pusat Identitas IAM.
- Anda memiliki izin administratif yang diperlukan. Untuk informasi selengkapnya mengenai izin, lihat Konfigurasi lanjutan.
- Instance IAM Identity Center harus diaktifkan di wilayah yang sama di mana Anda ingin membuat Rantai Pasokan AWS instance Anda. Rantai Pasokan AWS hanya didukung di AS Timur (Virginia N.), AS Barat (Oregon), Eropa (Frankfurt), Asia Pasifik (Sydney), dan Wilayah Eropa (Irlandia).

  Jika Rantai Pasokan AWS instans tidak berada di wilayah yang sama dengan wilayah Pusat Identitas IAM, hubungi kami untuk bantuan lebih lanjut.

- Anda harus memiliki setidaknya satu pengguna di instans Pusat Identitas IAM untuk ditetapkan sebagai administrator. Rantai Pasokan AWS Anda dapat menghubungkan direktori aktif Anda ke IAM Identity Center. Untuk informasi selengkapnya, lihat Connect ke direktori Microsoft AD.
- Tambahkan pengguna tambahan yang membutuhkan akses Rantai Pasokan AWS ke Pusat Identitas IAM.
- Anda perlu AWS Key Management Service (AWS KMS) untuk membuat sebuah instance. Rantai Pasokan AWS menggunakan ini AWS KMS key untuk mengenkripsi semua data yang masuk Rantai Pasokan AWS. Untuk informasi tentang AWS KMS Kunci, lihat Membuat kunci.

Memulai dengan Rantai Pasokan AWS

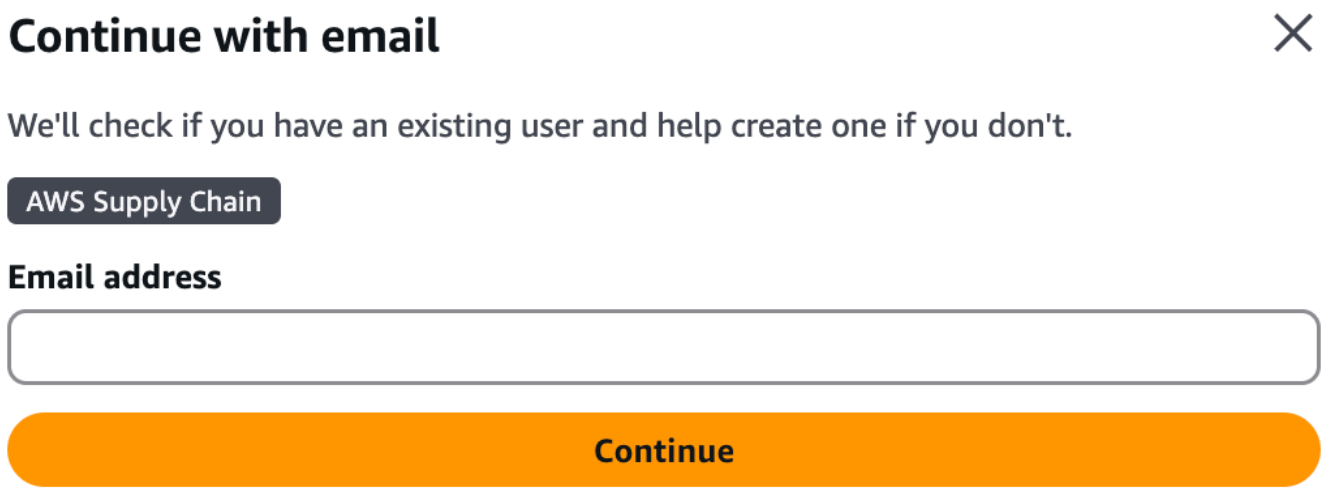
Di bagian ini, Anda dapat belajar membuat Rantai Pasokan AWS instance, memberikan peran izin pengguna, masuk ke aplikasi Rantai Pasokan AWS web, dan membuat peran izin pengguna khusus. An Akun AWS dapat memiliki hingga 10 Rantai Pasokan AWS instance dalam keadaan aktif atau inisialisasi.

Topik

Langkah 1: Tetapkan profil Pengguna Pusat Identitas IAM

Untuk membuat instance dan menggunakan Rantai Pasokan AWS layanan, Anda perlu menghubungkan profil pengguna IAM Identity Center yang ada atau membuat yang baru.

1. Buka konsol Rantai Pasokan AWS. Anda juga dapat mencari "Rantai Pasokan AWS" dari utama AWS Management Console.
2. Jika perlu, ubah AWS Wilayah dengan memilih Pilih Wilayah yang terletak di bagian atas konsol. Pilih Wilayah Anda dari daftar drop-down.
3. Pilih Buat Rantai Pasokan AWS instance. Notifikasi akan muncul.



4. Masukkan alamat email Anda dan pilih Lanjutkan. IDC akan memverifikasi apakah email tersebut cocok dengan pengguna yang ada.
5. Lakukan salah satu tindakan berikut:

   - Jika IDC mencocokkan alamat email dengan pengguna — Pilih Connect your identity source dan onboard tim Anda.

     > **Note**
     >
     > Ini dapat digunakan jika organisasi Anda memiliki instans IDC mapan yang ingin Anda gunakan. Rantai Pasokan AWS

   - Jika IDC tidak menemukan kecocokan dengan pengguna yang ada — Pemberitahuan Buat Pengguna Baru akan muncul. Lanjutkan ke langkah berikutnya.
6. Dalam notifikasi, masukkan yang berikut ini lalu pilih Lanjutkan:

   - Alamat Email
   - Nama depan
   - Nama belakang

   IDC membuat pengguna secara otomatis dan menambahkannya sebagai Rantai Pasokan AWS administrator.
7. Lakukan salah satu tindakan berikut:

   - Untuk membuat instance menggunakan konfigurasi standar — Pilih Buat. Lihat the section called “Gunakan konfigurasi standar”.
   - Untuk membuat instance menggunakan konfigurasi kustom — Pilih Edit dalam pengaturan lanjutan. Lihat the section called “Gunakan konfigurasi lanjutan”.

Langkah 2: Buat sebuah instance

Membuat instance dalam Rantai Pasokan AWS menetapkan lingkungan khusus untuk manajemen rantai pasokan dan analitik. Untuk menyiapkan instance, Anda mengonfigurasi detail dasar, menetapkan pengaturan, dan menentukan izin akses pengguna awal.

> **Note**
>
> Hanya AWS Management Console administrator yang dapat membuat instance. AWS Management Console Administrator yang membuat Rantai Pasokan AWS instance harus memiliki semua izin yang tercantum di bawahMenggunakan Rantai Pasokan AWS. Administrator ini harus mengundang pengguna IAM sebagai Rantai Pasokan AWS administrator untuk mengelola Rantai Pasokan AWS.

Anda membuat instance menggunakan salah satu dari dua metode, Konfigurasi standar atau konfigurasi lanjutan. Konfigurasi standar menggunakan proses otomatis yang membuat instance Anda dengan cepat menggunakan parameter preset. Konfigurasi lanjutan memungkinkan Anda untuk menyesuaikan instance Anda dengan mengatur parameter Anda sendiri.

Topik

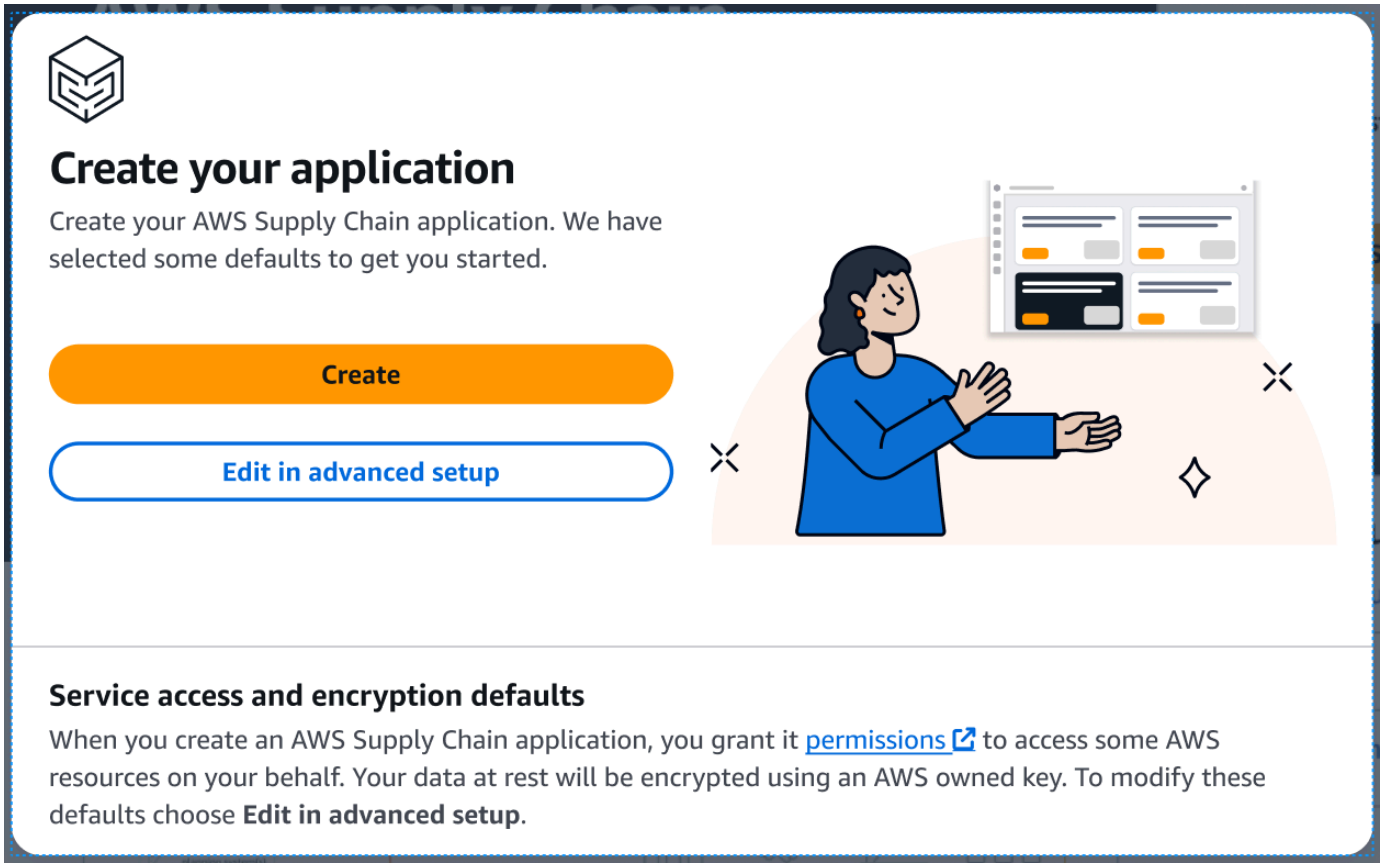
- Gunakan konfigurasi standar
- Gunakan konfigurasi lanjutan

Gunakan konfigurasi standar

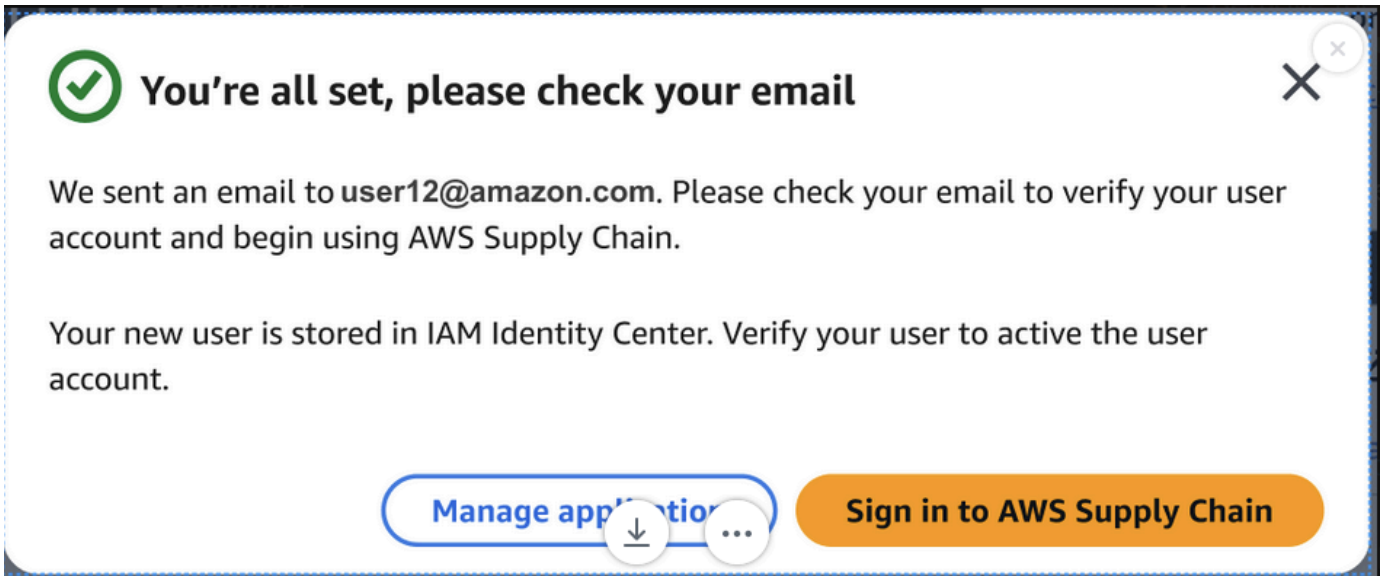
Konfigurasi standar membuat Rantai Pasokan AWS instance Anda menggunakan pengaturan keamanan dan enkripsi default. Instans beroperasi di AWS wilayah geografis. Untuk informasi selengkapnya tentang wilayah, lihat Wilayah dan titik akhir di Panduan Pengguna IAM dan titik akhir Regional di. Referensi Umum AWS

Untuk membuat Rantai Pasokan AWS instance menggunakan konfigurasi standar parameter preset, ikuti langkah-langkah ini.

1. Pilih Buat.

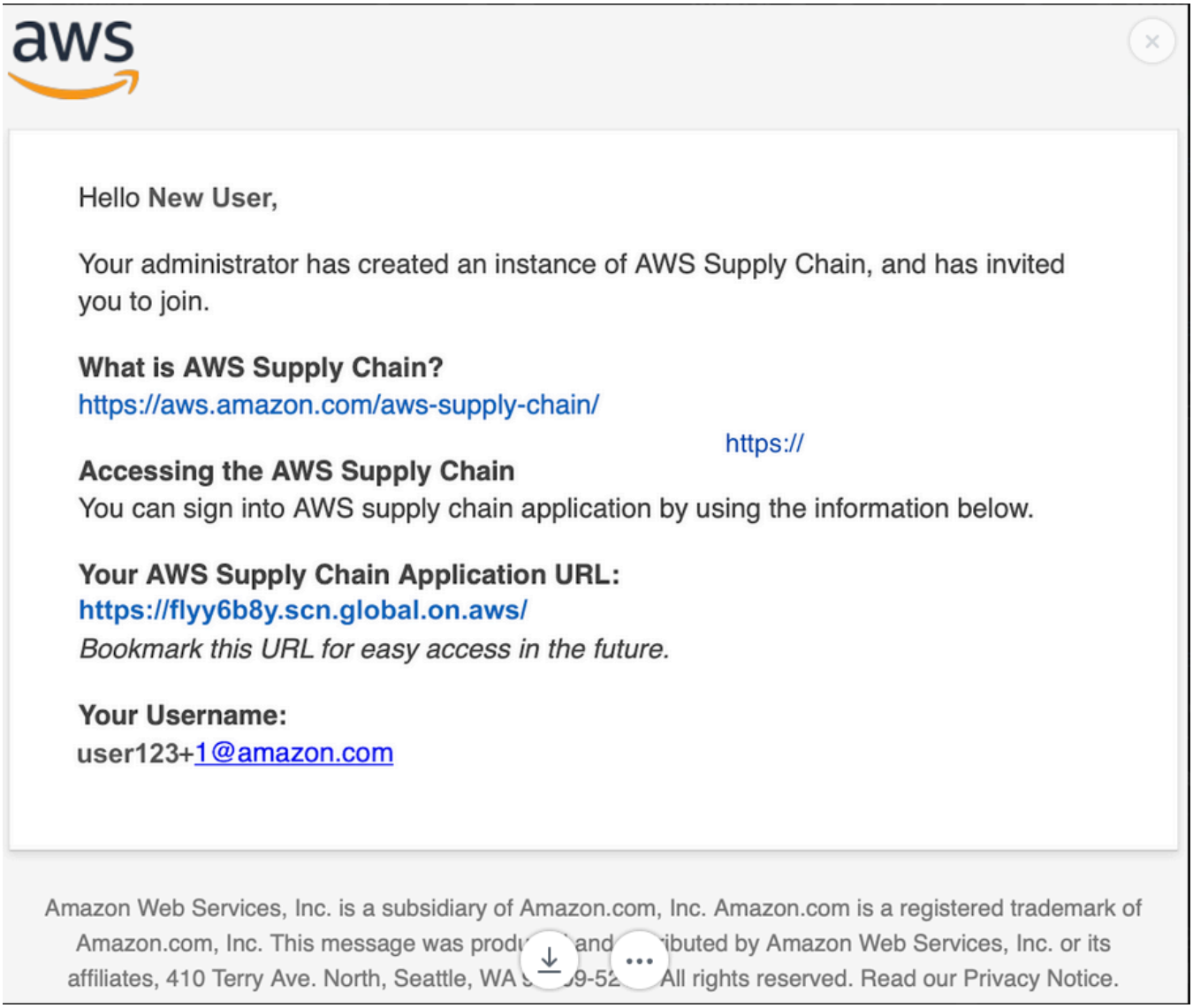


Konfirmasi akan muncul.



2. Periksa email Anda untuk hal-hal berikut:

   - Email dari tim IDC.
   - Email dari tim Manajemen Identitas.

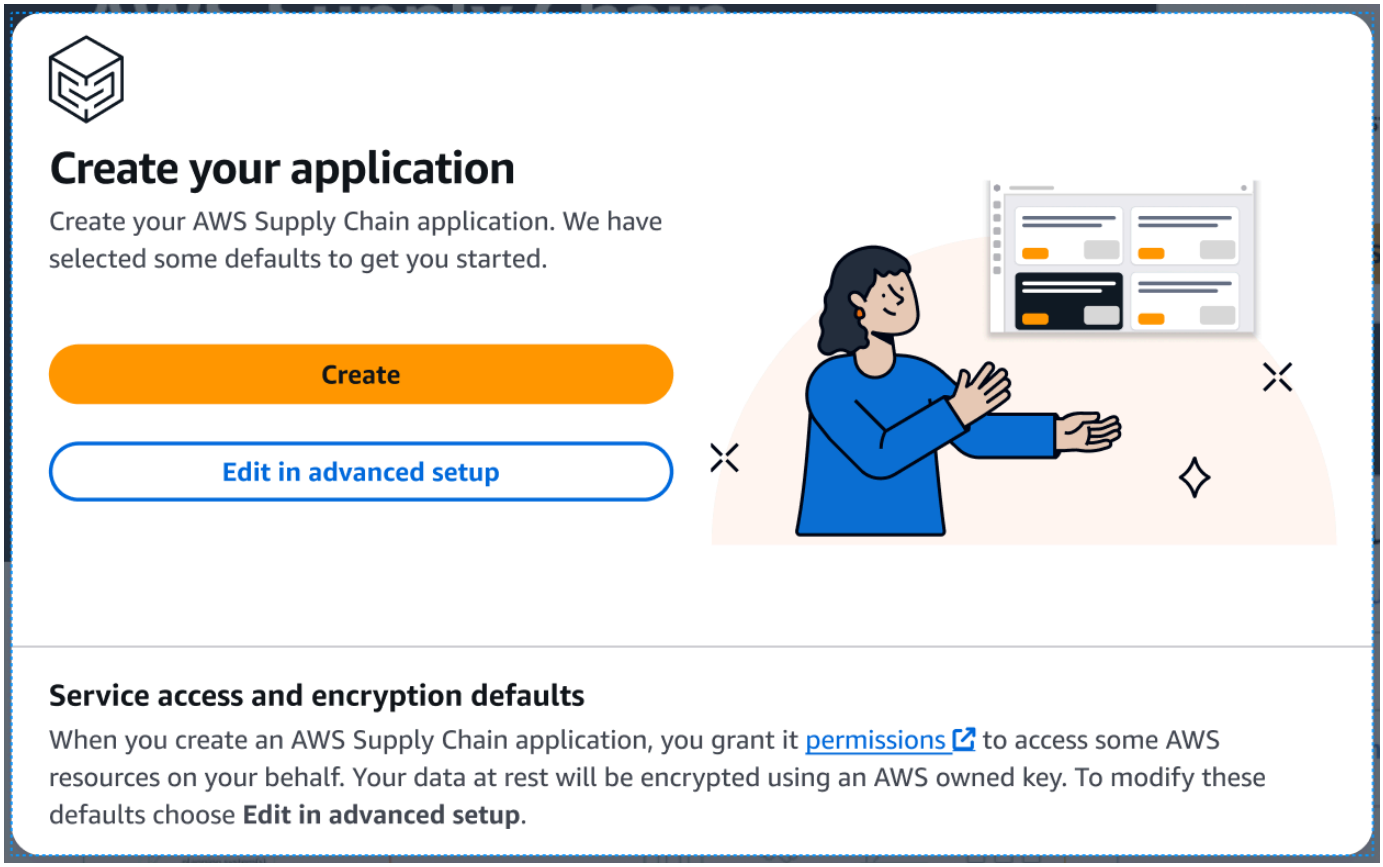


3. Setelah Anda menerima email undangan, masuk ke Rantai Pasokan AWS. Lihatthe section called “Masuk ke aplikasi Rantai Pasokan AWS web”.

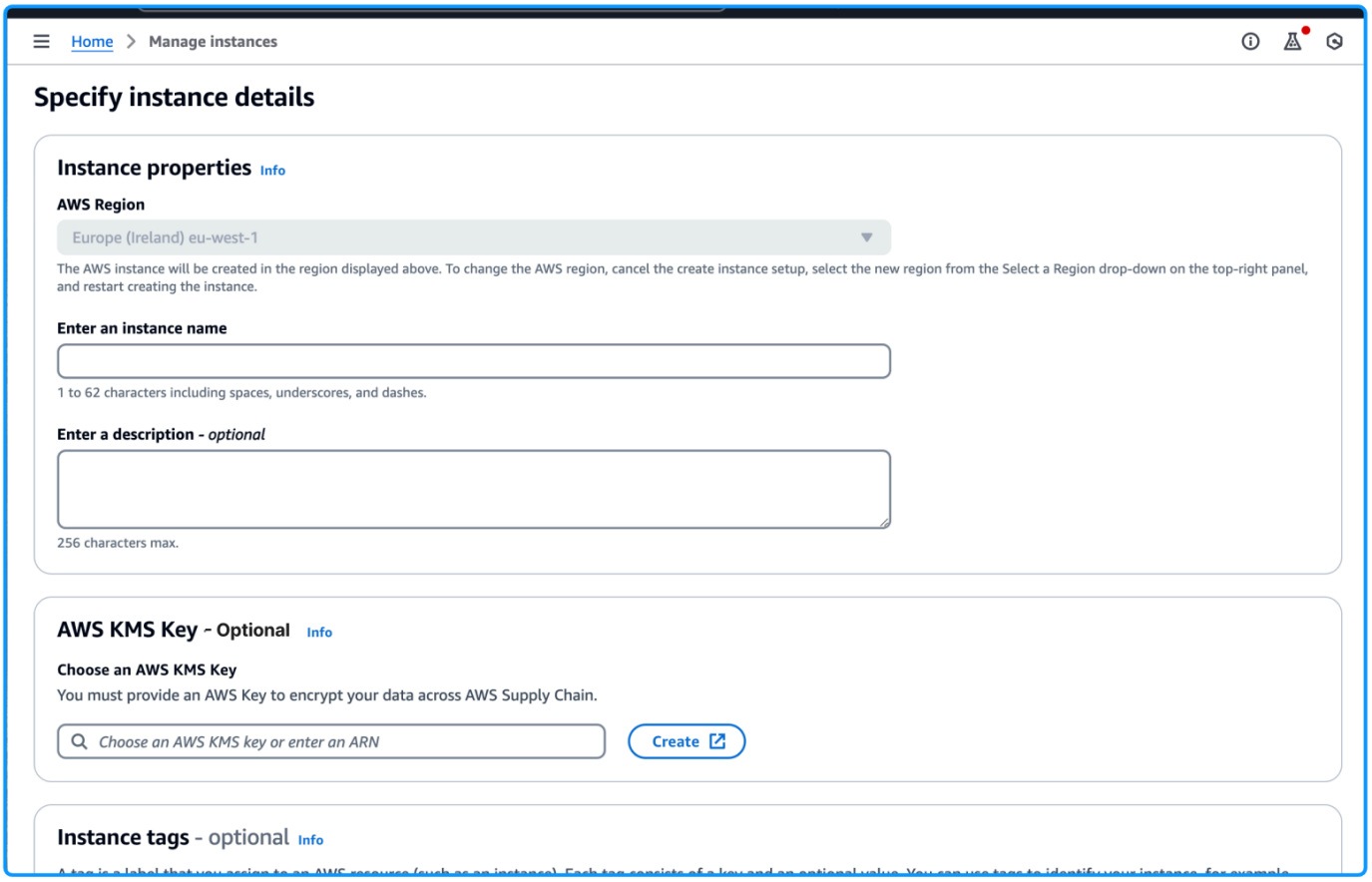
Gunakan konfigurasi lanjutan

Konfigurasi lanjutan memungkinkan Anda untuk menyesuaikan instance Anda dengan mengatur parameter Anda sendiri. Untuk membuat Rantai Pasokan AWS instance menggunakan konfigurasi lanjutan parameter preset, ikuti langkah-langkah ini.

1. Pilih Edit dalam pengaturan lanjutan.



Halaman properti Instance akan muncul.



2. Masukkan yang berikut ini pada halaman properti Instance:

   - Nama - Masukkan nama instance.
   - Deskripsi — Masukkan deskripsi Rantai Pasokan AWS instance Anda (misalnya, instance produksi, contoh pengujian, dll.).
   - Kunci AWS KMS (Opsional) — Anda dapat memilih untuk menggunakan AWS KMS Kunci default (disarankan) atau memberikan Kunci Anda sendiri AWS KMS . Untuk informasi selengkapnya, lihat the section called “Menggunakan AWS KMS kunci khusus”.
   - Tag instans — Anda dapat menambahkan tag ke instance Anda yang dapat digunakan untuk identifikasi. Misalnya, Anda dapat menambahkan tag untuk menentukan jenis instance yang Anda buat (misalnya, produksi, pengujian, UAT, dll.).

   > **Note**
   >
   > Jika Anda berencana untuk menggunakan koneksi data S/4 Hana, pastikan bahwa AWS KMS kunci yang Anda berikan memiliki `aws-supply-chain-access` tag dengan Nilai terkait. `true`

3. Pilih Buat instance.
4. (Opsional) Setelah Rantai Pasokan AWS instans Anda dibuat dan jika Anda memilih untuk menggunakan Kunci Anda sendiri di bawah AWS KMS AWS KMS Kunci, perbarui kebijakan KMS Anda Rantai Pasokan AWS untuk mengizinkan mengakses AWS KMS kunci Anda.

> **Note**
>
> Ganti *YourAccountNumber* dan *YourInstanceID* dengan ID Rantai Pasokan AWS Instance Akun AWS dan Anda.

```
 {

    "Sid": "Allow AWS Supply Chain to access the AWS KMS Key",
    "Effect": "Allow",
    "Principal":  {
        "AWS": "arn:aws:iam::YourAccountNumber:role/service-role/scn-instance-
role-YourInstanceID"
    },
    "Action":  [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKey"
    ],
    "Resource": "*"
}
```

Menggunakan AWS KMS kunci khusus

Anda dapat menggunakan AWS KMS kunci Anda sendiri saat membuat instance. Jika Anda ingin mengelola kunci Anda sendiri, tetapi tidak ingin menggunakan kunci yang ada, Anda dapat membuat kunci baru.

> **Note**
>
> Menggunakan kunci yang AWS dimiliki adalah pengaturan default yang disarankan untuk Rantai Pasokan AWS instance.

Menggunakan AWS KMS kunci yang ada

1. Pilih Sesuaikan pengaturan enkripsi.
2. Pergi ke Pilih AWS KMS Kunci.
3. Masukkan kunci Anda di bidang yang disediakan.
4. Pilih Perbarui.

Membuat AWS KMS kunci

1. Pilih Buat.
2. Ikuti langkah-langkah di Buat kunci KMS.
3. Perbarui kunci baru dengan izin berikut.

   - Tentukan izin administratif utama: Biarkan tidak dicentang
   - Tentukan izin penggunaan kunci: Biarkan tidak dicentang
   - Perbarui kebijakan kunci: Edit kebijakan kunci dan ganti dengan:

```
{

    "Version": "2012-10-17",
    "Statement":  [
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal":  {
                "AWS": "arn:aws:iam::YourAccountNumber:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow access through SecretManager for all principals in the
 account that are authorized to use SecretManager",
```

```
            "Effect": "Allow",
            "Principal":  {
                "AWS": "*"
            },
            "Action":  [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:CreateGrant",
                "kms:DescribeKey",
                "kms:GenerateDataKeyWithoutPlaintext",
                "kms:ReEncryptFrom",
                "kms:ReEncryptTo"
            ],
            "Resource": "*",
            "Condition":  {
                "StringEquals":  {
                    "kms:ViaService": "secretsmanager.Region.amazonaws.com",
                    "kms:CallerAccount": "YourAccountNumber"
                }
            }
        },
        {
            "Sid": "Allow AWS Supply Chain to access the AWS KMS Key",
            "Effect": "Allow",
            "Principal":  {
                "Service": "scn.Region.amazonaws.com"
            },
            "Action":  [
                "kms:Encrypt",
                "kms:GenerateDataKeyWithoutPlaintext",
                "kms:ReEncryptFrom",
                "kms:ReEncryptTo",
                "kms:Decrypt",
                "kms:GenerateDataKey",
                "kms:DescribeKey",
                "kms:CreateGrant",
                "kms:RetireGrant"
            ],
            "Resource":"*"
        }
    ]
```

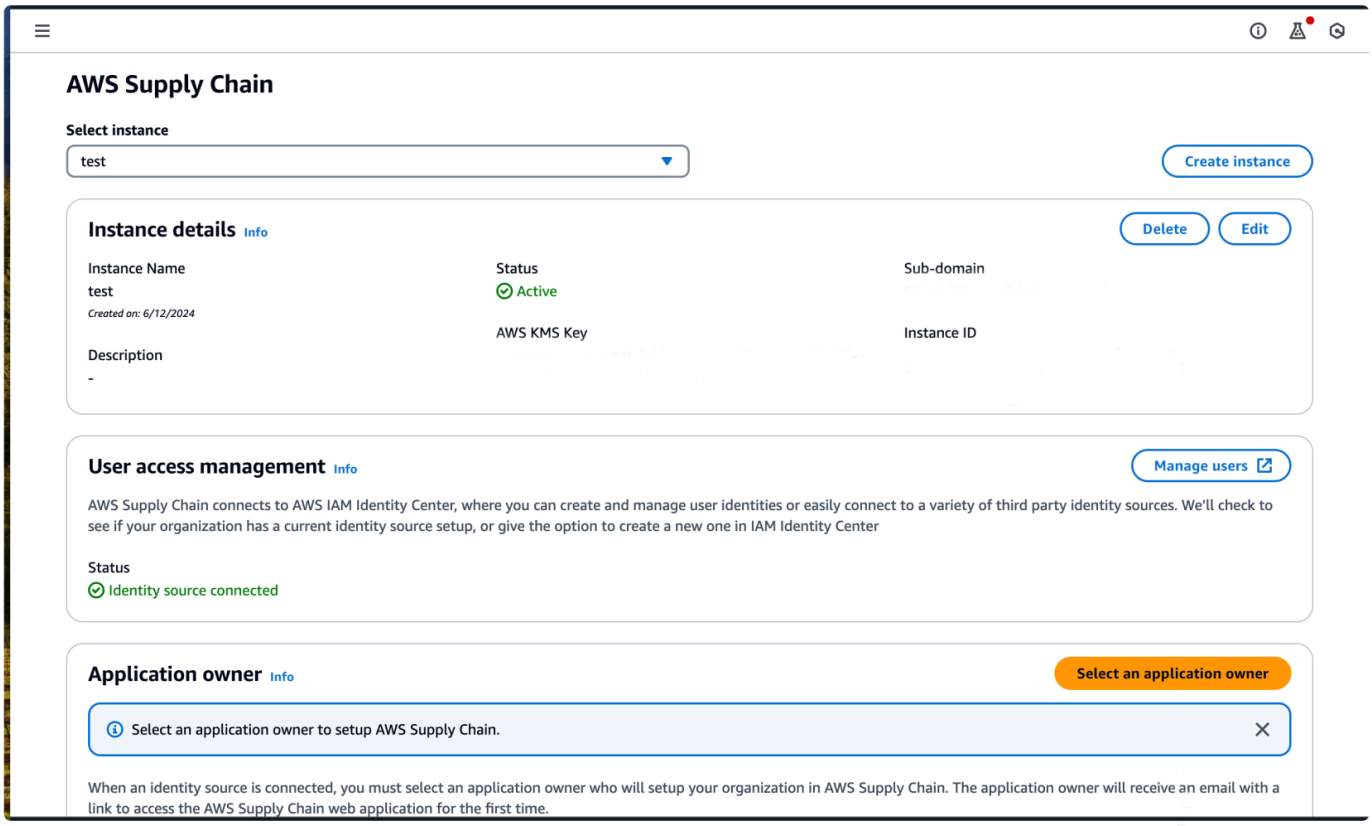
```
}
```

Langkah 3: Pilih pemilik Rantai Pasokan AWS aplikasi

Sebagai administrator AWS konsol, Anda memilih pemilik Rantai Pasokan AWS aplikasi untuk mengelola akses aplikasi Rantai Pasokan AWS web. Pemilik Rantai Pasokan AWS aplikasi dapat menambah atau menghapus peran izin pengguna ke aplikasi Rantai Pasokan AWS web.

Setelah instance dibuat dan sumber identitas terhubung, ikuti langkah-langkah ini untuk memilih pemilik Rantai Pasokan AWS aplikasi.

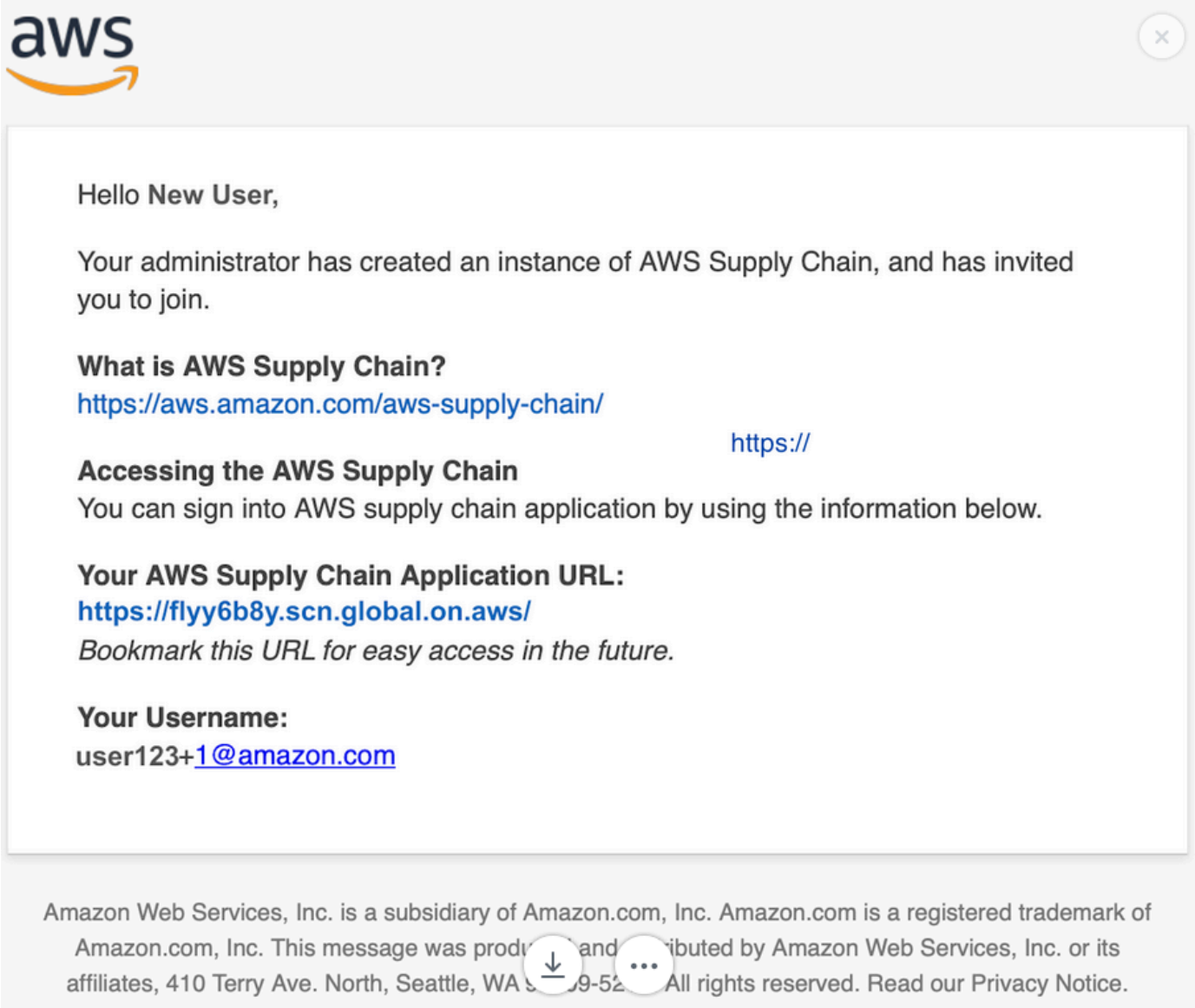
1. Buka dasbor Rantai Pasokan AWS konsol.
2. Pergi ke Pilih pemilik aplikasi dan pilih pengguna untuk menjadi pemilik Rantai Pasokan AWS aplikasi. Hasil penelusuran hanya menampilkan pengguna yang cocok dengan kriteria pencarian.



3. (Opsional) Pilih Buka Pusat Identitas IAM untuk menambahkan lebih banyak pengguna. Untuk informasi selengkapnya tentang menambahkan pengguna, lihat Mengelola sumber identitas Anda di Panduan Pengguna AWS IAM Identity Center dan untuk informasi selengkapnya tentang peran izin pengguna, lihat Peran izin pengguna.

> **Note**
>
> Anda hanya dapat menambahkan satu pengguna pada satu waktu dari Rantai Pasokan AWS Konsol. Anda tidak dapat menambahkan grup sebagai pemilik aplikasi di Rantai Pasokan AWS.

4. Pilih Kirim Undangan. Email dikirim ke administrator aplikasi web. Setelah administrator aplikasi web menerima email undangan, mereka akan dapat memilih URL aplikasi dan masuk ke file Rantai Pasokan AWS.



Di dasbor Rantai Pasokan AWS konsol, Anda akan melihat pengguna terdaftar di bawah Pemilik aplikasi.

Pilih Kelola di AWS Supply Chain untuk menambah dan menghapus pengguna di aplikasi Rantai Pasokan AWS web

Masuk ke aplikasi Rantai Pasokan AWS web

Sebagai Rantai Pasokan AWS administrator, Anda seharusnya telah menerima undangan email ke aplikasi Rantai Pasokan AWS web.

1. Anda dapat memilih tautan di email atau di dasbor Rantai Pasokan AWS konsol, di bawah Sub-domain, pilih URL web.

   Halaman login aplikasi Rantai Pasokan AWSweb muncul.
2. Masukkan kredensi pengguna AWS IAM Identity Center dan pilih Masuk.

   > **Note**
   >
   > Anda hanya akan diminta untuk melengkapi profil untuk akun dan organisasi Anda saat Anda masuk untuk pertama kalinya.
3. Pada halaman Lengkapi profil Anda, masukkan Job Title dan zona Waktu Anda. Pilih Berikutnya.
4. Pada halaman Mari tambahkan informasi organisasi Anda, masukkan nama Organisasi dan pilih Lokasi kantor pusat. Secara opsional, Anda dapat menambahkan logo perusahaan. Pilih Berikutnya.
5. Pada halaman Siapkan rekan tim Anda di Rantai Pasokan AWS halaman, pilih pengguna yang ingin Anda akses ke aplikasi Rantai Pasokan AWS web. Pilih Undang Pengguna. Untuk informasi tentang peran izin Rantai Pasokan AWS pengguna, lihatMengelola peran izin pengguna.
6. Jika Anda ingin menambahkan pengguna nanti, Anda dapat memilih Lewati untuk sekarang.

   Halaman lengkap Orientasi muncul.
7. Setiap pengguna yang Anda tambahkan menerima pesan email dengan tautan yang masuk Rantai Pasokan AWS, atau Anda dapat memilih Salin tautan dan mengirim tautan ke pengguna.
8. Pilih Lanjutkan ke beranda untuk melihat Rantai Pasokan AWS dasbor.

Menggunakan Rantai Pasokan AWS

Rantai Pasokan AWS adalah aplikasi berbasis cloud yang membantu Anda mendapatkan visibilitas ke jaringan rantai pasokan Anda, membuat keputusan dengan cepat, dan meningkatkan ketahanan rantai pasokan. Dengan menggunakan Rantai Pasokan AWS, Anda dapat menghubungkan sumber data yang berbeda, menghasilkan wawasan menggunakan pembelajaran mesin, dan berkolaborasi dengan tim internal dan mitra eksternal. Bagian ini akan memandu Anda melalui beberapa fungsi Rantai Pasokan AWS dasar.

Topik

Menggunakan Rantai Pasokan AWS konsol

Menggunakan konsol adalah cara termudah untuk mengelola sumber daya dan konfigurasi layanan Anda. Konsol menyediakan antarmuka berbasis web yang intuitif tempat Anda dapat melihat, membuat, memodifikasi, dan memantau sumber daya Anda. Bagian ini menunjukkan cara mengakses dan menavigasi konsol untuk melakukan tugas manajemen umum.

> **Note**
>
> Jika AWS akun Anda adalah akun anggota AWS organisasi dan menyertakan Kebijakan Kontrol Layanan (SCP), pastikan SCP organisasi memberikan izin berikut ke akun anggota. Jika izin berikut tidak disertakan dalam kebijakan SCP organisasi, pembuatan Rantai Pasokan AWS instance akan gagal.

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

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

Izin berikut diperlukan oleh Admin Konsol untuk membuat dan memperbarui Rantai Pasokan AWS instance dengan sukses.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Action": "scn:*",
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": [
    "s3:GetObject",
    "s3:PutObject",
    "s3:ListBucket",
    "s3:CreateBucket",
    "s3:PutBucketVersioning",
    "s3:PutBucketObjectLockConfiguration",
    "s3:PutEncryptionConfiguration",
    "s3:PutBucketPolicy",
    "s3:PutLifecycleConfiguration",
    "s3:PutBucketPublicAccessBlock",
    "s3:DeleteObject",
    "s3:ListAllMyBuckets",
    "s3:PutBucketOwnershipControls",
    "s3:PutBucketNotification",
    "s3:PutAccountPublicAccessBlock",
    "s3:PutBucketLogging",
    "s3:PutBucketTagging"
   ],
   "Resource": "arn:aws:s3:::aws-supply-chain-*",
   "Effect": "Allow"
  },
  {
   "Action": [
    "cloudtrail:CreateTrail",
    "cloudtrail:PutEventSelectors",
    "cloudtrail:GetEventSelectors",
```

```
    "cloudtrail:StartLogging"
   ],
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": [
    "events:DescribeRule",
    "events:PutRule",
    "events:PutTargets"
   ],
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": [
    "chime:CreateAppInstance",
    "chime:DeleteAppInstance",
    "chime:PutAppInstanceRetentionSettings",
    "chime:TagResource"
   ],
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": [
    "cloudwatch:PutMetricData",
    "cloudwatch:Describe*",
    "cloudwatch:Get*",
    "cloudwatch:List*"
   ],
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": [
    "organizations:CreateOrganization",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:EnableAWSServiceAccess",
    "organizations:ListDelegatedAdministrators"
   ],
   "Resource": "*",
   "Effect": "Allow"
```

```
  },
  {
   "Action": [
    "kms:CreateGrant",
    "kms:RetireGrant",
    "kms:DescribeKey"
   ],
   "Resource": key_arn,
   "Effect": "Allow"
  },
  {
   "Action": [
    "kms:ListAliases"
   ],
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": [
    "iam:CreateRole",
    "iam:CreatePolicy",
    "iam:GetRole",
    "iam:PutRolePolicy",
    "iam:AttachRolePolicy",
    "iam:CreateServiceLinkedRole"
   ],
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": [
    "sso:AssociateDirectory",
    "sso:AssociateProfile",
    "sso:CreateApplication",
    "sso:CreateApplicationAssignment",
    "sso:CreateInstance",
    "sso:CreateManagedApplicationInstance",
    "sso:DeleteApplication",
    "sso:DeleteApplicationAssignment",
    "sso:DeleteManagedApplicationInstance",
    "sso:DescribeApplication",
    "sso:DescribeDirectories",
    "sso:DescribeInstance",
    "sso:DescribeRegisteredRegions",
```

```
    "sso:DescribeTrusts",
    "sso:DisassociateProfile",
    "sso:GetManagedApplicationInstance",
    "sso:GetPeregrineStatus",
    "sso:GetProfile",
    "sso:GetSharedSsoConfiguration",
    "sso:GetSsoConfiguration",
    "sso:GetSSOStatus",
    "sso:ListApplicationAssignments",
    "sso:ListApplicationTemplates",
    "sso:ListDirectoryAssociations",
    "sso:ListInstances",
    "sso:ListProfileAssociations",
    "sso:ListProfiles",
    "sso:PutApplicationAuthenticationMethod",
    "sso:PutApplicationGrant",
    "sso:RegisterRegion",
    "sso:SearchDirectoryGroups",
    "sso:SearchDirectoryUsers",
    "sso:SearchGroups",
    "sso:SearchUsers",
    "sso:StartPeregrine",
    "sso:StartSSO",
    "sso:UpdateSsoConfiguration",
    "sso-directory:SearchUsers"
   ],
   "Resource": "*",
   "Effect": "Allow"
  }
 ]
}
```

*key_arn*menentukan kunci yang ingin Anda gunakan untuk Rantai Pasokan AWS contoh. Untuk praktik terbaik dan membatasi akses hanya ke kunci yang ingin Anda gunakan Rantai Pasokan AWS, lihat Menentukan kunci KMS dalam pernyataan kebijakan IAM. Untuk mewakili semua kunci KMS, gunakan karakter wildcard saja (“*”).

Memperbarui profil Anda

Anda dapat memperbarui akun dan profil organisasi Anda kapan saja di aplikasi Rantai Pasokan AWS web.

Memperbarui profil akun Anda

Untuk memperbarui profil akun Anda, ikuti langkah-langkah ini.

1. Di dasbor aplikasi Rantai Pasokan AWS web, dari panel navigasi kiri, pilih ikon Pengaturan.
2. Pilih Profil Akun.

   Halaman Profil Akun muncul.
3. Perbarui informasi akun, dan pilih Simpan.

Memperbarui profil organisasi Anda

Untuk memperbarui profil organisasi, ikuti langkah-langkah ini.

1. Di dasbor aplikasi Rantai Pasokan AWS web, dari panel navigasi kiri, pilih ikon Pengaturan.
2. Pilih Organisasi, lalu pilih Profil Organisasi.

   Halaman Profil Organisasi muncul.
3. Perbarui Logo organisasi atau lokasi Kantor Pusat, lalu pilih Simpan.

Mengelola peran izin pengguna

Sebagai Rantai Pasokan AWS administrator, Anda dapat menggunakan peran izin pengguna default atau membuat peran izin khusus. Rantai Pasokan AWS memiliki peran izin pengguna default berikut:

- Administrator — Akses untuk membuat, melihat, dan mengelola semua data dan izin pengguna.
- Data Analyst — Akses untuk membuat, melihat, dan mengelola semua koneksi data.
- Manajer Inventaris — Akses untuk membuat, melihat, dan mengelola Wawasan.
- Perencana Permintaan — Akses untuk membuat, melihat, dan mengelola perkiraan, mengesampingkan, dan mempublikasikan rencana permintaan.
- Manajer Data Mitra — Akses untuk mengelola dan melihat mitra, mengelola dan melihat permintaan data, dan melihat data keberlanjutan.
- Perencana Pasokan — Akses untuk mengelola dan melihat rencana pasokan.

> **Note**
>
> Sebagai Rantai Pasokan AWS administrator, sebelum Anda menambahkan pengguna, perhatikan hal berikut:
>
> - Setiap peran izin pengguna default ditentukan dengan serangkaian izin. Anda dapat menambahkan pengguna ke peran izin pengguna default atau membuat peran izin khusus.
> - Pengguna hanya dapat ditugaskan ke satu peran izin pengguna.
> - Anda tidak dapat mengedit atau menghapus peran izin pengguna default.
> - Saat Anda mengedit peran izin khusus yang Anda buat, izin untuk semua pengguna di bawah peran izin khusus akan diperbarui.
> - Saat Anda menghapus peran izin khusus yang Anda buat, semua pengguna di bawah peran izin khusus akan kehilangan akses Rantai Pasokan AWS.
> - Menambahkan grup tidak didukung di Rantai Pasokan AWS.

Topik

Menambahkan pengguna

Sebagai Rantai Pasokan AWS administrator, Anda dapat menambahkan pengguna untuk mengakses aplikasi Rantai Pasokan AWS web. Pengguna pertama harus ditambahkan ke IAM Identity Center (IDC), dan kemudian mereka dapat ditambahkan ke. Rantai Pasokan AWS Untuk informasi selengkapnya tentang menambahkan pengguna ke IDC, lihat Menetapkan akses pengguna.

Setelah pengguna ditambahkan ke IDC, ikuti langkah-langkah ini untuk menambahkan pengguna.

1. Pilih ikon Pengaturan di Rantai Pasokan AWS dasbor.
2. Pilih Pengguna dan Izin.
3. Pilih Pengguna, Pengguna. Halaman Kelola Pengguna akan muncul.

4. Pilih Tambahkan Pengguna Baru. Halaman Tambah Pengguna muncul.
5. Pilih pengguna dari menu tarik-turun Tambahkan pengguna.
6. Pilih peran untuk pengguna dari menu drop-down Pilih peran di bawah.
7. Pilih Tambahkan.

Memperbarui izin pengguna

Untuk memperbarui peran izin pengguna bagi Rantai Pasokan AWS pengguna saat ini, ikuti langkah-langkah ini.

1. Di Rantai Pasokan AWS dasbor, dari panel navigasi kiri, pilih ikon Pengaturan.
2. Pilih Izin, lalu pilih Pengguna.

   Halaman Kelola Pengguna akan muncul.
3. Pada halaman Kelola Pengguna, pilih pengguna atau grup yang ingin Anda perbarui peran izin pengguna, dan dari menu tarik-turun Peran Izin, pilih salah satu peran izin.

   > **Note**
   >
   > Bergantung pada izin peran yang Anda tetapkan, Rantai Pasokan AWS dasbor disesuaikan. Untuk informasi selengkapnya, lihat Membuat peran izin pengguna khusus.
4. Pilih Simpan.

Menghapus pengguna

Sebagai Rantai Pasokan AWS administrator, Anda dapat menghapus pengguna dari aplikasi Rantai Pasokan AWS web. Ikuti langkah-langkah ini untuk menghapus pengguna.

1. Di Rantai Pasokan AWS dasbor, dari panel navigasi kiri, pilih ikon Pengaturan.
2. Pilih Izin, lalu pilih Pengguna.

   Halaman Kelola Pengguna akan muncul.
3. Pada halaman Kelola Pengguna, pilih pengguna yang ingin Anda hapus dan pilih ikon Hapus.

Membuat peran izin pengguna khusus

Selain peran izin pengguna default, Anda dapat membuat peran izin pengguna khusus untuk menyertakan beberapa peran izin dan menambahkan lokasi dan produk tertentu. Ikuti langkah-langkah ini untuk membuat peran izin baru.

1. Di Rantai Pasokan AWS dasbor, dari panel navigasi kiri, pilih ikon Pengaturan. Pilih Izin, lalu pilih Peran Izin.

   Halaman Peran Izin muncul.
2. Pilih Buat Peran Baru.
3. Pada halaman Kelola Peran Izin, di bawah Nama Peran, masukkan nama.
4. Pindahkan slider untuk memilih peran izin pengguna.

   - Mengelola — Menugaskan pengguna dengan izin kelola dapat menambah, mengedit, dan mengelola informasi.
   - Lihat - Menetapkan pengguna dengan izin tampilan hanya dapat melihat informasi saat ini.
5.

   > **Note**
   >
   > Anda hanya dapat memilih produk dan lokasi di bawah Akses Lokasi dan Akses Produk jika instans Anda terhubung ke sumber data. Misalnya, Anda dapat membuat pengguna Admin khusus hanya untuk mengelola alpukat di lokasi Seattle, atau pengguna Insight hanya untuk mengelola wawasan alpukat di lokasi Seattle.

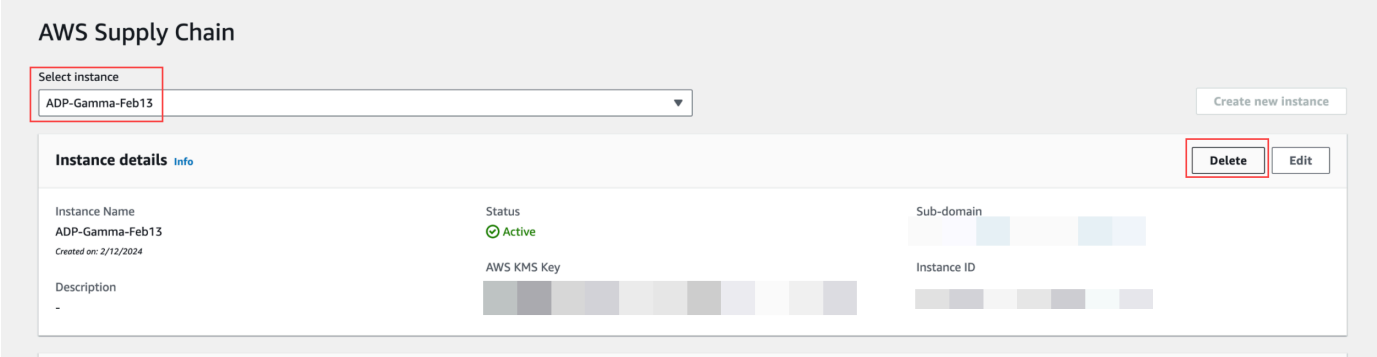
   Di bawah Akses Lokasi, cari Wilayah saat Anda mengetik di bilah pencarian dan pilih Wilayah.
6. Di bawah Akses Produk, cari produk saat Anda mengetik di bilah pencarian dan pilih produk.
7. Pilih Simpan.

Menghapus sebuah instans

Untuk menghapus instance, ikuti langkah-langkah ini.

> **Note**
>
> Saat Anda menghapus instans, informasi dari bucket Amazon S3 tidak akan dihapus secara otomatis.

1. Buka Rantai Pasokan AWS konsol dihttps://console.aws.amazon.com/scn/home.
2. Di dasbor Rantai Pasokan AWS konsol, dari dropdown, pilih instance yang ingin Anda hapus.



3. Pilih Hapus.
4. Pada halaman Hapus Rantai Pasokan AWS Instans, di bawah Konfirmasi, ketik **`delete`** untuk mengonfirmasi bahwa Anda ingin menghapus instance.
5. Pilih Hapus. Penghapusan instance dimulai dan setelah instance dihapus, Anda akan melihat pesan konfirmasi.

> **Note**
>
> Setelah instance dihapus, informasi yang terkait dengan Amazon Q in dihapus Rantai Pasokan AWS secara otomatis.

Keamanan di Rantai Pasokan AWS

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang AWS dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara Anda dan AWS. Model tanggung jawab bersama menggambarkan ini sebagai keamanan cloud dan keamanan di cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang berjalan Layanan AWS di dalamnya AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara teratur menguji dan memverifikasi keefektifan keamanan kami sebagai bagian dari program kepatuhan AWS. Untuk mempelajari tentang program kepatuhan yang berlaku Rantai Pasokan AWS, lihat AWS Layanan dalam Lingkup oleh AWS Layanan Program Kepatuhan .
- Keamanan di cloud — Layanan AWS Yang Anda gunakan menentukan tanggung jawab Anda. Anda juga bertanggung jawab atas faktor-faktor lain. termasuk sensitivitas data Anda, persyaratan Anda, dan hukum dan peraturan yang berlaku.

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

Topik

Perlindungan data di Rantai Pasokan AWS

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di Rantai Pasokan AWS. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Lihat informasi yang lebih lengkap tentang privasi data dalam Pertanyaan Umum Privasi Data. Lihat informasi tentang perlindungan data di Eropa di pos blog Model Tanggung Jawab Bersama dan GDPR AWS di Blog Keamanan AWS .

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensyal dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan sumber daya. AWS Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan logging aktivitas pengguna dengan AWS CloudTrail. Untuk informasi tentang penggunaan CloudTrail jejak untuk menangkap AWS aktivitas, lihat Bekerja dengan CloudTrail jejak di AWS CloudTrail Panduan Pengguna.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola tingkat lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-3 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi selengkapnya tentang titik akhir FIPS yang tersedia di Standar Pemrosesan Informasi Federal (FIPS) 140-3.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan Rantai Pasokan AWS atau lainnya Layanan AWS menggunakan konsol, API AWS CLI, atau AWS SDKs. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log

penagihan atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

Data ditangani oleh Rantai Pasokan AWS

Untuk membatasi data yang dapat diakses oleh pengguna resmi dari instans Rantai AWS Pasokan tertentu, data yang disimpan dalam Rantai AWS Pasokan dipisahkan oleh ID AWS akun Anda dan ID instans Rantai AWS Pasokan Anda.

AWS Supply Chain menangani berbagai data rantai pasokan seperti, informasi pengguna, informasi yang diekstrak dari konektor data, dan detail inventaris.

Preferensi memilih keluar

Kami dapat menggunakan dan menyimpan Konten Anda yang diproses oleh Rantai Pasokan AWS, sebagaimana tercantum dalam Ketentuan Layanan AWS. Jika ingin memilih untuk tidak menggunakan atau menyimpan konten, Anda dapat membuat kebijakan opt-out di AWS Organizations. Rantai Pasokan AWS Untuk informasi selengkapnya tentang membuat kebijakan opt-out, lihat sintaks dan contoh kebijakan opt-out layanan AI.

Enkripsi diam

Data kontak yang diklasifikasikan sebagai PII, atau data yang mewakili konten pelanggan termasuk konten yang digunakan di Amazon Q dalam Rantai Pasokan AWS disimpan oleh Rantai Pasokan AWS, dienkripsi saat istirahat (yaitu, sebelum dimasukkan, disimpan, atau disimpan ke disk) dengan kunci yang terbatas waktu dan spesifik untuk instance. Rantai Pasokan AWS

Enkripsi sisi server Amazon S3 digunakan untuk mengenkripsi semua data konsol dan aplikasi web dengan kunci AWS Key Management Service data yang unik untuk setiap akun pelanggan. Untuk informasi tentang AWS KMS keys, lihat Apa itu AWS Key Management Service? di Panduan AWS Key Management Service Pengembang.

> **Note**
>
> Rantai Pasokan AWS fitur Perencanaan Pasokan dan Visibilitas N-Tier tidak mendukung enkripsi data-at-rest dengan KMS-CMK yang disediakan.

Enkripsi bergerak

Data termasuk konten yang digunakan di Amazon Q yang Rantai Pasokan AWS dipertukarkan dengan Rantai AWS Pasokan dilindungi saat transit antara browser web pengguna dan Rantai AWS Pasokan menggunakan enkripsi TLS standar industri.

Manajemen kunci

Rantai Pasokan AWS sebagian mendukung KMS-CMK.

Untuk informasi tentang memperbarui kunci AWS KMS Rantai Pasokan AWS, lihat. Langkah 2: Buat sebuah instance

Privasi lalu lintas antar jaringan

> **Note**
>
> Rantai Pasokan AWS tidak mendukung PrivateLink.

Titik akhir virtual private cloud (VPC) untuk Rantai Pasokan AWS adalah entitas logis dalam VPC yang memungkinkan konektivitas hanya untuk. Rantai Pasokan AWS Rutekan VPC meminta Rantai Pasokan AWS dan merutekan respons kembali ke VPC. Untuk informasi selengkapnya, lihat Titik Akhir VPC di Panduan Pengguna VPC.

Bagaimana Rantai Pasokan AWS menggunakan hibah di AWS KMS

Rantai Pasokan AWS membutuhkan hibah untuk menggunakan kunci yang dikelola pelanggan Anda.

Rantai Pasokan AWS membuat beberapa hibah menggunakan AWS KMS kunci yang dilewatkan selama CreateInstanceoperasi. Rantai Pasokan AWS membuat hibah atas nama Anda dengan mengirimkan CreateGrantpermintaan ke AWS KMS. Hibah AWS KMS digunakan untuk memberikan Rantai Pasokan AWS akses ke AWS KMS kunci di akun pelanggan.

> **Note**
>
> Rantai Pasokan AWS menggunakan mekanisme otorisasi itu sendiri. Setelah pengguna ditambahkan Rantai Pasokan AWS, Anda tidak dapat menolak daftar pengguna yang sama menggunakan AWS KMS kebijakan.

Rantai Pasokan AWS menggunakan hibah untuk hal-hal berikut:

- Untuk mengirim GenerateDataKeypermintaan AWS KMS untuk mengenkripsi data yang disimpan dalam instance Anda.
- Untuk mengirim permintaan Dekripsi untuk AWS KMS membaca data terenkripsi yang terkait dengan instance.
- Untuk menambahkan DescribeKey, CreateGrant, dan RetireGrantizin agar data Anda tetap aman saat mengirimnya ke AWS layanan lain seperti Amazon Forecast.

Anda dapat mencabut akses ke hibah, atau menghapus akses layanan ke kunci yang dikelola pelanggan kapan saja. Jika Anda melakukannya, Rantai Pasokan AWS tidak akan dapat mengakses data apa pun yang dienkripsi oleh kunci yang dikelola pelanggan, yang memengaruhi operasi yang bergantung pada data tersebut.

Memantau enkripsi Anda untuk Rantai Pasokan AWS

Contoh berikut adalah AWS CloudTrail peristiwa untuk`Encrypt`,`GenerateDataKey`, dan `Decrypt` untuk memantau operasi KMS yang dipanggil oleh Rantai Pasokan AWS untuk mengakses data yang dienkripsi oleh kunci yang dikelola pelanggan Anda:

Encrypt

```
            {
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "scn.amazonaws.com"
    },
    "eventTime": "2024-03-06T22:39:32Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Encrypt",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "172.12.34.56"
    "userAgent": "Example/Desktop/1.0 (V1; OS)",
    "requestParameters": {
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "keyId": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample"
    },
```

```
    "responseElements": null,
    "requestID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
    "eventID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
    "readOnly": true,
    "resources": [
        {
            "accountId": account ID,
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "112233445566",
    "sharedEventID": "fdf9ee0f-e43f-4e43-beac-df69067edb8b",
    "eventCategory": "Management"
}
```

GenerateDataKey

```
            {
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "scn.amazonaws.com"
    },
     "eventTime": "2024-03-06T22:39:32Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "172.12.34.56"
    "userAgent": "Example/Desktop/1.0 (V1; OS)",
    "requestParameters": {
        "encryptionContext": {
            "aws:s3:arn": "arn:aws:s3:::test/rawEvent/bf6666c1-111-48aaca-b6b0-
dsadsadsa3432423/noFlowName/scn.data.inboundorder/20240306_223934_536"
        },
        "keyId": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample",
        "keySpec": "AES_222"
```

```
    },
    "responseElements": null,
    "requestID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
    "eventID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
    "readOnly": true,
    "resources": [
        {
            "accountId": account ID,
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "112233445566",
    "sharedEventID": "fdf9ee0f-e43f-4e43-beac-df69067edb8b",
    "eventCategory": "Management"
}
```

Decrypt

```
            {
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "scn.amazonaws.com"
    },
     "eventTime": "2024-03-06T22:39:32Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "172.12.34.56"
    "userAgent": "Example/Desktop/1.0 (V1; OS)",
    "requestParameters": {
        "keyId": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample",
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
    },
    "responseElements": null,
    "requestID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
```

```
    "eventID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
    "readOnly": true,
    "resources": [
        {
            "accountId": account ID,
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "112233445566",
    "sharedEventID": "fdf9ee0f-e43f-4e43-beac-df69067edb8b",
    "eventCategory": "Management"
}
```

Akses Rantai Pasokan AWS menggunakan endpoint antarmuka ()AWS PrivateLink

Anda dapat menggunakan AWS PrivateLink untuk membuat koneksi pribadi antara VPC Anda dan. Rantai Pasokan AWS Anda dapat mengakses Rantai Pasokan AWS seolah-olah itu ada di VPC Anda, tanpa menggunakan gateway internet, perangkat NAT, koneksi VPN, atau koneksi. AWS Direct Connect Instans di VPC Anda tidak memerlukan alamat IP publik untuk mengakses. Rantai Pasokan AWS

Anda membuat koneksi pribadi ini dengan membuat titik akhir antarmuka, yang didukung oleh AWS PrivateLink. Kami membuat antarmuka jaringan endpoint di setiap subnet yang Anda aktifkan untuk titik akhir antarmuka. Ini adalah antarmuka jaringan yang dikelola pemohon yang berfungsi sebagai titik masuk untuk lalu lintas yang ditakdirkan. Rantai Pasokan AWS

Untuk informasi selengkapnya, lihat Akses Layanan AWS melalui AWS PrivateLink di AWS PrivateLink Panduan.

Pertimbangan untuk Rantai Pasokan AWS

Sebelum Anda menyiapkan titik akhir antarmuka Rantai Pasokan AWS, tinjau Pertimbangan dalam Panduan.AWS PrivateLink

Rantai Pasokan AWS mendukung panggilan ke semua tindakan API-nya melalui titik akhir antarmuka.

Buat titik akhir antarmuka untuk Rantai Pasokan AWS

Anda dapat membuat titik akhir antarmuka untuk Rantai Pasokan AWS menggunakan konsol VPC Amazon atau () AWS Command Line Interface .AWS CLI Untuk informasi selengkapnya, lihat Membuat titik akhir antarmuka di AWS PrivateLink Panduan.

Buat titik akhir antarmuka untuk Rantai Pasokan AWS menggunakan nama layanan berikut:

```
com.amazonaws.region.scn
```

Jika Anda mengaktifkan DNS pribadi untuk titik akhir antarmuka, Anda dapat membuat permintaan API untuk Rantai Pasokan AWS menggunakan nama DNS Regional default. Misalnya, *scn*.*region*.amazonaws.com.

Buat kebijakan titik akhir untuk titik akhir antarmuka Anda

Kebijakan endpoint adalah sumber daya IAM yang dapat Anda lampirkan ke titik akhir antarmuka. Kebijakan endpoint default memungkinkan akses penuh Rantai Pasokan AWS melalui titik akhir antarmuka. Untuk mengontrol akses yang diizinkan Rantai Pasokan AWS dari VPC Anda, lampirkan kebijakan titik akhir kustom ke titik akhir antarmuka.

kebijakan titik akhir mencantumkan informasi berikut:

- Prinsipal yang dapat melakukan tindakan (Akun AWS, pengguna IAM, dan peran IAM)
- Tindakan-tindakan yang dapat dilakukan
- Sumber daya di mana tindakan dapat dilakukan

Untuk informasi selengkapnya, lihat Mengontrol akses ke layanan menggunakan kebijakan titik akhir di Panduan AWS PrivateLink .

Contoh: Kebijakan titik akhir VPC untuk tindakan Rantai Pasokan AWS

Berikut ini adalah contoh kebijakan endpoint kustom. Saat Anda melampirkan kebijakan ini ke titik akhir antarmuka Anda, kebijakan ini akan memberikan akses ke Rantai Pasokan AWS tindakan yang tercantum untuk semua prinsip di semua sumber daya.

```
{
```

```
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [

            "scn:action-1",
            "scn:action-2",
            "scn:action-3"

         ],
         "Resource":"*"
      }
   ]
}
```

IAM untuk Rantai Pasokan AWS

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

Topik

- Audiens
- Mengautentikasi dengan identitas
- Mengelola akses menggunakan kebijakan
- Bagaimana Rantai Pasokan AWS bekerja dengan IAM
- Contoh kebijakan berbasis identitas untuk Rantai Pasokan AWS
- Memecahkan masalah Rantai Pasokan AWS identitas dan akses

Audiens

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

Pengguna layanan — Jika Anda menggunakan Rantai Pasokan AWS layanan untuk melakukan pekerjaan Anda, administrator Anda memberi Anda kredensi dan izin yang Anda butuhkan. Saat

Anda menggunakan lebih banyak Rantai Pasokan AWS fitur untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara mengelola akses dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di Rantai Pasokan AWS, lihat Memecahkan masalah Rantai Pasokan AWS identitas dan akses.

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

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

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 pengguna IAM, atau dengan mengasumsikan peran IAM.

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

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

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensil Anda. Jika Anda tidak menggunakan AWS alat, Anda

harus menandatangani permintaan sendiri. Guna mengetahui informasi selengkapnya tentang penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, lihat AWS Signature Version 4 untuk permintaan API dalam Panduan Pengguna IAM.

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

Akun AWS pengguna root

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

Identitas gabungan

Sebagai praktik terbaik, mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS 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 Layanan AWS 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 Identitas IAM, 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 Identitas IAM, lihat Apakah itu Pusat Identitas IAM? dalam Panduan Pengguna AWS IAM Identity Center .

Pengguna dan grup IAM

Pengguna IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, kami merekomendasikan untuk mengandalkan kredensial sementara, bukan membuat pengguna IAM yang memiliki kredensial jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan tertentu yang memerlukan kredensial jangka panjang dengan pengguna IAM, kami merekomendasikan Anda merotasi kunci akses. Untuk informasi selengkapnya, lihat Merotasi kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang dalam Panduan Pengguna IAM.

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

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

Peran IAM

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

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat Buat peran untuk penyedia identitas pihak ketiga dalam Panduan Pengguna IAM. Jika menggunakan Pusat Identitas IAM, Anda harus mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas

tersebut diautentikasi, Pusat Identitas IAM akan mengorelasikan set izin ke peran dalam IAM. Untuk informasi tentang set izin, lihat Set izin dalam Panduan Pengguna AWS IAM Identity Center .

- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM guna mendapatkan berbagai izin secara sementara untuk tugas tertentu.
- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (prinsipal tepercaya) di akun lain untuk mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa Layanan AWS, Anda dapat melampirkan kebijakan 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 dalam Panduan Pengguna IAM.
- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. 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 pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses maju.
  - Peran layanan – Peran layanan adalah peran IAM yang dijalankan oleh layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Buat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.
  - Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.
- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan peran IAM untuk mengelola kredensi sementara untuk aplikasi yang berjalan pada EC2 instance dan membuat AWS CLI atau AWS permintaan API. 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 peran IAM untuk memberikan izin ke aplikasi yang berjalan di EC2 instans Amazon di Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

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

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. 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 di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

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

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Tentukan izin IAM kustom dengan kebijakan terkelola pelanggan dalam Panduan Pengguna IAM.

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan yang dikelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat 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 yang dikelola atau kebijakan inline, lihat Pilih antara kebijakan yang dikelola dan kebijakan inline dalam Panduan Pengguna IAM.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

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

Daftar kontrol akses (ACLs)

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

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

Jenis-jenis kebijakan lain

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

- Batasan izin – Batasan izin adalah fitur lanjutan tempat Anda mengatur izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas ke entitas IAM (pengguna IAM atau peran IAM). Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan

antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batasan izin, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.

- Kebijakan kontrol layanan (SCPs) — SCPs adalah kebijakan JSON yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di. AWS Organizations AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur dalam organisasi, Anda dapat menerapkan kebijakan kontrol layanan (SCPs) ke salah satu atau semua akun Anda. SCP membatasi izin untuk entitas di akun anggota, termasuk masing-masing. Pengguna root akun AWS Untuk informasi selengkapnya tentang Organizations dan SCPs, lihat Kebijakan kontrol layanan di Panduan AWS Organizations Pengguna.
- Kebijakan kontrol sumber daya (RCPs) — RCPs adalah kebijakan JSON yang dapat Anda gunakan untuk menetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda tanpa memperbarui kebijakan IAM yang dilampirkan ke setiap sumber daya yang Anda miliki. RCP membatasi izin untuk sumber daya di akun anggota dan dapat memengaruhi izin efektif untuk identitas, termasuk Pengguna root akun AWS, terlepas dari apakah itu milik organisasi Anda. Untuk informasi selengkapnya tentang Organizations dan RCPs, termasuk daftar dukungan Layanan AWS tersebut RCPs, lihat Kebijakan kontrol sumber daya (RCPs) 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 eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya, lihat Kebijakan sesi dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat Logika evaluasi kebijakan di Panduan Pengguna IAM.

Bagaimana Rantai Pasokan AWS bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses Rantai Pasokan AWS, pelajari fitur IAM yang tersedia untuk digunakan. Rantai Pasokan AWS

Fitur IAM yang dapat Anda gunakan Rantai Pasokan AWS

Fitur IAM	Rantai Pasokan AWS dukungan
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
Kunci kondisi kebijakan	Ya
Kredensial sementara	Ya
Sesi akses teruskan (FAS)	Ya
Peran layanan	Ya
Peran terkait layanan	Tidak

Untuk mendapatkan tampilan tingkat tinggi tentang cara Rantai Pasokan AWS dan AWS layanan lain bekerja dengan sebagian besar fitur IAM, lihat AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM.

Kebijakan berbasis identitas untuk Rantai Pasokan AWS

Mendukung kebijakan berbasis identitas: Ya

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas,

lihat Tentukan izin IAM kustom dengan kebijakan terkelola pelanggan dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. 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 kebijakan JSON, lihat Referensi elemen kebijakan JSON IAM dalam Panduan Pengguna IAM.

Contoh kebijakan berbasis identitas untuk Rantai Pasokan AWS

Untuk melihat contoh kebijakan Rantai Pasokan AWS berbasis identitas, lihat. Contoh kebijakan berbasis identitas untuk Rantai Pasokan AWS

Kebijakan berbasis sumber daya dalam Rantai Pasokan AWS

Mendukung kebijakan berbasis sumber daya: Tidak

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan secara spesifik seluruh akun atau entitas IAM 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, administrator IAM 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 principal dalam akun yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun di IAM dalam Panduan Pengguna IAM.

Tindakan kebijakan untuk Rantai Pasokan AWS

Mendukung tindakan kebijakan: Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

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

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

Tindakan kebijakan Rantai Pasokan AWS menggunakan awalan berikut sebelum tindakan:

```
scn
```

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan tersebut dengan koma.

```
"Action": [
      "scn:action1",
      "scn:action2"
         ]
```

Untuk melihat contoh kebijakan Rantai Pasokan AWS berbasis identitas, lihat. Contoh kebijakan berbasis identitas untuk Rantai Pasokan AWS

Sumber daya kebijakan untuk Rantai Pasokan AWS

Mendukung sumber daya kebijakan: Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

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

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

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

Untuk melihat contoh kebijakan Rantai Pasokan AWS berbasis identitas, lihat. Contoh kebijakan berbasis identitas untuk Rantai Pasokan AWS

Kunci kondisi kebijakan untuk Rantai Pasokan AWS

Mendukung kunci kondisi kebijakan khusus layanan: Yes

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen `Condition` (atau blok `Condition`) akan memungkinkan Anda menentukan kondisi yang menjadi dasar suatu pernyataan berlaku. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi bersyarat yang menggunakan operator kondisi, misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta.

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

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

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

Untuk melihat contoh kebijakan Rantai Pasokan AWS berbasis identitas, lihat. Contoh kebijakan berbasis identitas untuk Rantai Pasokan AWS

Menggunakan kredensi sementara dengan Rantai Pasokan AWS

Mendukung kredensial sementara: Ya

Beberapa Layanan AWS tidak berfungsi saat Anda masuk menggunakan kredensi sementara. Untuk informasi tambahan, termasuk yang Layanan AWS bekerja dengan kredensi sementara, lihat Layanan AWS yang bekerja dengan IAM di Panduan Pengguna IAM.

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 tautan masuk tunggal (SSO) perusahaan Anda, proses tersebut secara otomatis membuat kredensil sementara. Anda juga akan secara otomatis membuat kredensial sementara ketika Anda masuk ke konsol sebagai seorang pengguna lalu beralih peran. Untuk informasi selengkapnya tentang peralihan peran, lihat Beralih dari pengguna ke peran IAM (konsol) dalam Panduan Pengguna IAM.

Anda dapat membuat kredenal sementara secara manual menggunakan API AWS CLI atau AWS . Anda kemudian dapat menggunakan kredensi 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 Kredensial keamanan sementara di IAM.

Teruskan sesi akses untuk Rantai Pasokan AWS

Mendukung sesi akses maju (FAS): Ya

Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses maju.

Peran layanan untuk Rantai Pasokan AWS

Mendukung peran layanan: Ya

Peran layanan adalah peran IAM yang diambil oleh sebuah layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Buat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.

> **Warning**
>
> Mengubah izin untuk peran layanan dapat merusak Rantai Pasokan AWS fungsionalitas. Edit peran layanan hanya jika Rantai Pasokan AWS memberikan panduan untuk melakukannya.

Peran terkait layanan untuk Rantai Pasokan AWS

Mendukung peran terkait layanan: Tidak

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Untuk detail tentang membuat atau mengelola peran terkait layanan, lihat Layanan AWS bahwa bekerja dengan IAM. Cari layanan dalam tabel yang memiliki `Yes` di kolom Peran terkait layanan. Pilih tautan Ya untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Contoh kebijakan berbasis identitas untuk Rantai Pasokan AWS

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi Rantai Pasokan AWS 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 di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian akan dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM dengan menggunakan contoh dokumen kebijakan JSON ini, lihat Membuat kebijakan IAM di Panduan Pengguna IAM.

Topik

- Praktik terbaik kebijakan

Praktik terbaik kebijakan

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

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat Kebijakan yang dikelola AWS atau Kebijakan yang dikelola AWS untuk fungsi tugas dalam Panduan Pengguna IAM.
- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat Kebijakan dan izin dalam IAM dalam Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Kondisi dalam Panduan Pengguna IAM.
- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk

informasi selengkapnya, lihat Validasi kebijakan dengan IAM Access Analyzer dalam Panduan Pengguna IAM.

- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Anda, Akun AWS aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Amankan akses API dengan MFA dalam Panduan Pengguna IAM.

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

Memecahkan masalah Rantai Pasokan AWS identitas dan akses

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

Topik

- Saya tidak berwenang untuk melakukan tindakan di Rantai Pasokan AWS
- Saya tidak berwenang untuk melakukan iam: PassRole
- Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses Rantai Pasokan AWS sumber daya saya

Saya tidak berwenang untuk melakukan tindakan di Rantai Pasokan AWS

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

Contoh kesalahan berikut terjadi ketika pengguna IAM `mateojackson` mencoba menggunakan konsol untuk melihat detail tentang suatu sumber daya *`my-example-widget`* rekaan, tetapi tidak memiliki izin `scn:`*`GetWidget`* rekaan.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 scn:GetWidget on resource: my-example-widget
```

Dalam hal ini, Mateo meminta administratornya untuk memperbarui kebijakannya untuk mengizinkan dia mengakses sumber daya *my-example-widget* menggunakan tindakan `scn:GetWidget`.

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 Rantai Pasokan AWS.

Beberapa Layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika pengguna IAM bernama `marymajor` mencoba menggunakan konsol tersebut untuk melakukan tindakan di Rantai Pasokan AWS. 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 Rantai Pasokan AWS 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 Rantai Pasokan AWS mendukung fitur-fitur ini, lihatBagaimana Rantai Pasokan AWS bekerja dengan IAM.

- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat Menyediakan akses ke pengguna IAM di pengguna lain Akun AWS yang Anda miliki di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat Menyediakan akses ke pengguna terautentikasi eksternal (federasi identitas) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM.

AWS kebijakan terkelola untuk Rantai Pasokan AWS

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

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

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

Untuk informasi selengkapnya, lihat Kebijakan terkelola AWS dalam Panduan Pengguna IAM.

AWS kebijakan terkelola: AWSSupply ChainFederationAdminAccess

AWSSupplyChainFederationAdminAccess menyediakan akses pengguna Rantai Pasokan AWS federasi ke Rantai Pasokan AWS aplikasi, termasuk izin yang diperlukan untuk melakukan tindakan

dalam aplikasi. Rantai Pasokan AWS Kebijakan ini memberikan izin administratif atas pengguna dan grup Pusat Identitas IAM dan dilampirkan ke peran yang dibuat oleh Rantai Pasokan AWS untuk Anda. Anda tidak boleh melampirkan AWSSupply ChainFederationAdminAccess kebijakan ke entitas IAM lainnya.

Meskipun kebijakan ini menyediakan semua akses Rantai Pasokan AWS melalui izin scn: *, Rantai Pasokan AWS peran tersebut menentukan izin Anda. Rantai Pasokan AWS Peran hanya menyertakan izin yang diperlukan, dan tidak memiliki izin ke admin. APIs

Detail izin

Kebijakan ini mencakup izin berikut:

- `Chime`— Menyediakan akses untuk membuat atau menghapus pengguna di bawah Amazon Chime AppInstance; Menyediakan akses untuk mengelola saluran, anggota saluran, dan moderator; Menyediakan akses untuk mengirim pesan ke saluran. Operasi Chime dicakup ke instance aplikasi yang ditandai dengan "Id”. SCNInstance
- `AWS IAM Identity Center (AWS SSO)`— Memberikan izin yang diperlukan untuk mengaitkan dan memisahkan profil pengguna, asosiasi daftar profil, daftar tugas aplikasi, menjelaskan aplikasi, menjelaskan contoh, dan mendapatkan konfigurasi penugasan aplikasi di IAM Identity Center.
- `AppFlow`— Menyediakan akses untuk membuat, memperbarui, dan menghapus profil koneksi; Menyediakan akses untuk membuat, memperbarui, menghapus, memulai, dan menghentikan aliran; Menyediakan akses ke aliran tag dan untag dan menjelaskan catatan aliran.
- `Amazon S3`— Menyediakan akses untuk daftar semua ember. Menyediakan GetBucketLocation, GetBucketPolicy,, PutObject, GetObject, dan ListBucket akses ke bucket dengan resource arn arn:aws:s3::: -*. aws-supply-chain-data
- `SecretsManager`— Menyediakan akses untuk membuat rahasia dan memperbarui kebijakan rahasia.
- `KMS`— Menyediakan AppFlow layanan Amazon akses ke daftar kunci dan alias kunci. Menyediakan DescribeKey, CreateGrant dan ListGrants izin untuk kunci KMS ditandai dengan key-value aws-suply-chain-access: true; Menyediakan akses untuk membuat rahasia dan memperbarui kebijakan rahasia.

  Izin (kms:ListKeys, kms:, kms: ListAliases GenerateDataKey, dan kms:Decrypt) tidak dibatasi untuk AppFlow Amazon dan izin ini dapat diberikan ke Kunci apa pun di akun Anda. AWS KMS

Untuk melihat izin kebijakan ini, lihat AWSSupplyChainFederationAdminAccessdi. AWS Management Console

Rantai Pasokan AWS pembaruan kebijakan AWS terkelola

Tabel berikut mencantumkan detail tentang pembaruan kebijakan AWS terkelola Rantai Pasokan AWS sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman Riwayat Rantai Pasokan AWS dokumen.

Perubahan	Deskripsi	Tanggal
AWSSupplyChainFederationAdminAccess— Kebijakan yang diperbarui	Rantai Pasokan AWS memperbarui kebijakan terkelola untuk memungkinkan pengguna federasi mengakses ListApplicationAssignments,, DescribeApplication DescribeInstance, dan GetApplicationAssignmentConfiguration operasi di Pusat Identitas IAM.	Desember 10, 2024
AWSSupplyChainFederationAdminAccess— Kebijakan yang diperbarui	Rantai Pasokan AWS memperbarui kebijakan terkelola untuk memungkinkan pengguna federasi mengakses ListProfileAssociations operasi di Pusat Identitas IAM.	November 01, 2023
AWSSupplyChainFederationAdminAccess— Kebijakan yang diperbarui	Rantai Pasokan AWS memperbarui kebijakan terkelola untuk memungkinkan pengguna federasi mengakses PutObject dan GetObject operasi pada bucket S3 khusus dengan resource arn	21 September 2023

Perubahan	Deskripsi	Tanggal
	arn:aws:s3: ::aws-supply-chain-data-*.	
AWSSupplyChainFederationAdminAccess – Kebijakan baru	Rantai Pasokan AWS menambahkan kebijakan baru untuk memungkinkan pengguna federasi mengakses Rantai Pasokan AWS aplikasi. Ini termasuk izin yang diperlukan untuk melakukan tindakan dalam Rantai Pasokan AWS aplikasi.	01 Maret, 2023
Rantai Pasokan AWS mulai melacak perubahan	Rantai Pasokan AWS mulai melacak perubahan untuk kebijakan AWS terkelolanya.	01 Maret, 2023

Validasi kepatuhan untuk Rantai Pasokan AWS

Auditor pihak ketiga menilai keamanan dan kepatuhan Rantai Pasokan AWS sebagai bagian dari beberapa program AWS kepatuhan. Program ini mencakup SOC, PCI, FedRAMP, HIPAA, dan lainnya.

Untuk daftar Layanan AWS yang termasuk dalam lingkup program kepatuhan tertentu, lihat AWS Layanan dalam Lingkup oleh AWS Layanan Program Kepatuhan . Untuk informasi umum, lihat Program AWS Kepatuhan Program AWS .

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

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

- Panduan Memulai Cepat Keamanan dan Kepatuhan Panduan Memulai penerapan ini membahas pertimbangan arsitektur dan memberikan langkah-langkah yang harus diambil saat Anda menerapkan lingkungan dasar yang berfokus pada keamanan dan berfokus pada kepatuhan. AWS
- Arsitektur untuk Whitepaper Keamanan dan Kepatuhan HIPAA — Whitepaper ini menjelaskan bagaimana perusahaan dapat menggunakan untuk membuat aplikasi yang sesuai dengan HIPAA. AWS
- AWS Sumber Daya AWS — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- Mengevaluasi Sumber Daya dengan Aturan dalam Panduan AWS Config Pengembang — Panduan ini menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub— Ini Layanan AWS memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalam AWS untuk membantu Anda memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik.

Ketahanan di Rantai Pasokan AWS

Infrastruktur AWS global dibangun di sekitar Wilayah AWS dan Availability Zones. Wilayah AWS menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi. Ini 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.

Selain infrastruktur AWS global, Rantai Pasokan AWS menawarkan beberapa fitur untuk membantu mendukung ketahanan data dan kebutuhan cadangan Anda.

Penebangan dan Pemantauan Rantai Pasokan AWS

Logging dan Monitoring adalah bagian penting untuk menjaga keandalan, ketersediaan, dan kinerja Rantai AWS Pasokan dan AWS solusi Anda yang lain. AWS menyediakan alat AWS CloudTrail

pemantauan untuk mengawasi Rantai AWS Pasokan, melaporkan ketika ada sesuatu yang salah, dan mengambil tindakan otomatis bila perlu.

> **Note**
>
> APIs dipanggil hanya dari Rantai Pasokan AWS konsol ditangkap AWS CloudTrail.

AWS CloudTrail merekam panggilan API dan kejadian terkait yang dilakukan oleh atau atas Akun AWS Anda dan mengirimkan berkas log ke bucket Amazon S3 yang Anda tentukan. Anda dapat mengidentifikasi pengguna dan akun yang memanggil AWS, alamat IP asal panggilan dilakukan, dan waktu panggilan terjadi. Anda dapat melihat peristiwa Rantai AWS Pasokan di scn.amazonaws.com. Untuk informasi selengkapnya, lihat Panduan Pengguna AWS CloudTrail.

> **Note**
>
> Perhatikan hal berikut dengan Rantai Pasokan AWS:
>
> - Ketika Anda mengundang pengguna yang tidak memiliki akses ke Rantai Pasokan AWS, pengguna ini tidak menerima informasi dalam pemberitahuan yang mereka terima dari aplikasi web. Pengguna yang diundang menerima pemberitahuan email dengan tautan ke aplikasi web. Mereka hanya dapat masuk dan melihat konten dalam pemberitahuan jika mereka memiliki izin pengguna yang diperlukan.
> - Semua pengguna dengan atau tanpa izin pengguna untuk Insight tertentu dapat melihat pesan obrolan Wawasan.
> - Sebagai admin aplikasi, ketika Anda menambahkan pengguna ke Rantai Pasokan AWS instance, mereka memiliki akses ke file AWS KMS key. Anda dapat mengelola izin pengguna untuk menambah atau menghapus pengguna. Untuk informasi selengkapnya tentang izin pengguna, lihatMengelola peran izin pengguna.

Rantai Pasokan AWS peristiwa data di CloudTrail

> **Note**
>
> Aplikasi web APIs yang tercantum di bawah Rantai Pasokan AWS aplikasi web APIs tercantum dalam peristiwa data di CloudTrail.

Peristiwa data memberikan informasi tentang operasi sumber daya yang dilakukan pada atau di sumber daya (misalnya, membaca atau menulis ke objek Amazon S3). Ini juga dikenal sebagai operasi bidang data. Peristiwa data seringkali merupakan aktivitas volume tinggi. Secara default, CloudTrail tidak mencatat peristiwa data. Riwayat CloudTrail peristiwa tidak merekam peristiwa data.

Biaya tambahan berlaku untuk peristiwa data. Untuk informasi selengkapnya tentang CloudTrail harga, lihat AWS CloudTrail Harga.

Anda dapat mencatat peristiwa data untuk jenis Rantai Pasokan AWS sumber daya menggunakan CloudTrail konsol AWS CLI, atau operasi CloudTrail API.

- Untuk mencatat peristiwa data menggunakan CloudTrail konsol, buat penyimpanan data jejak atau peristiwa untuk mencatat peristiwa data, atau perbarui penyimpanan data jejak atau peristiwa yang ada untuk mencatat peristiwa data.

  1. Pilih Peristiwa data untuk mencatat peristiwa data.
  2. Dari daftar tipe peristiwa Data, pilih jenis sumber daya yang ingin Anda log peristiwa data.
  3. Pilih template pemilih log yang ingin Anda gunakan. Anda dapat mencatat semua peristiwa data untuk jenis sumber daya, mencatat semua `readOnly` peristiwa, mencatat semua `writeOnly` peristiwa, atau membuat templat pemilih log khusus untuk memfilter pada `readOnly`eventName, dan `resources.ARN` bidang.

- Untuk mencatat peristiwa data menggunakan AWS CLI, konfigurasikan `--advanced-event-selectors` parameter untuk mengatur `eventCategory` bidang sama dengan `Data` dan `resources.type` bidang sama dengan nilai tipe sumber daya. Anda dapat menambahkan kondisi untuk memfilter nilai`readOnly`,`eventName`, dan `resources.ARN` bidang.
  - Untuk mengonfigurasi jejak untuk mencatat peristiwa data, jalankan put-event-selectorsperintah. Untuk informasi selengkapnya, lihat Mencatat peristiwa data untuk jejak dengan. AWS CLI
  - Untuk mengonfigurasi penyimpanan data peristiwa untuk mencatat peristiwa data, jalankan create-event-data-storeperintah untuk membuat penyimpanan data acara baru untuk mencatat peristiwa data, atau menjalankan update-event-data-storeperintah untuk memperbarui penyimpanan data acara yang ada. Untuk informasi selengkapnya, lihat Mencatat peristiwa data untuk menyimpan data peristiwa dengan AWS CLI.

* Anda dapat mengonfigurasi pemilih acara lanjutan untuk memfilter pada`eventName`,`readOnly`, dan `resources.ARN` bidang untuk mencatat hanya peristiwa yang penting bagi Anda. Untuk informasi selengkapnya tentang bidang ini, lihat AdvancedFieldSelector.

Rantai Pasokan AWS acara manajemen di CloudTrail

Acara manajemen memberikan informasi tentang operasi manajemen yang dilakukan pada sumber daya di AWS akun Anda. Ini juga dikenal sebagai operasi pesawat kontrol. Secara default, CloudTrail mencatat peristiwa manajemen.

AWS Supply Chain mencatat semua operasi bidang kontrol ke CloudTrail sebagai peristiwa manajemen.

Rantai Pasokan AWS aplikasi web APIs

Yang APIs tercantum dalam bagian ini dipanggil oleh Rantai Pasokan AWS aplikasi atas nama pengguna federasi. Ini APIs tidak terlihat di CloudTrail log dan tidak ditangkap dalam dokumen Referensi Otorisasi Layanan, lihat Rantai Pasokan AWS. Akses ke ini APIs dikendalikan oleh Rantai Pasokan AWS aplikasi berdasarkan izin peran pengguna federasi. Anda tidak boleh mencoba mengontrol akses ke ini APIs untuk mencegah ketidaksuburan aplikasi. Rantai Pasokan AWS

Peran pengguna

APIs Berikut ini digunakan untuk mengelola pengguna, peran pengguna, pemberitahuan pengguna, dan pesan obrolan di Rantai Pasokan AWS.

```
scn:AddMembersToResourceBasedChat
scn:AssignGalaxyRoleToUser
scn:AssociateUser
scn:BatchGetUsers
scn:BatchMarkNotificationAsDelivered
scn:CreateRole
scn:DeleteRole
scn:DescribeChatForUser
scn:GetAccessDetailConfig
scn:GetChatPreferencesForUser
scn:GetMessagingSessionConnectionDetails
scn:GetNotificationsPreference
scn:GetOrCreateChimeUser
scn:GetOrCreateResourceBasedChat
scn:GetOrCreateUserBasedChat
scn:GetOrganizationInfo
scn:GetResourceBasedChatArn
scn:GetUserDetails
```

```
scn:ListChatMembers
scn:ListChatMessages
scn:ListChatModerators
scn:ListChats
scn:ListRoles
scn:ListUserNotifications
scn:ListUsersWithRole
scn:MarkNotificationAsDelivered
scn:MarkNotificationAsRead
scn:RemoveMemberFromResourceBasedChat
scn:RemoveUser
scn:SearchChimeUsers
scn:SearchUsers
scn:SendChatMessage
scn:SetNotificationsPreference
scn:UpdateChatPreferencesForUser
scn:UpdateChatReadMarker
scn:UpdateOrganizationInfo
scn:UpdateRole
scn:UpdateUser
```

Danau data

APIs Berikut ini digunakan untuk membuat dan mengelola aliran data dan koneksi di danau data.

```
scn:CreateConnection
scn:CreateDataflow
scn:CreateDeleteDataByPartitionJob
scn:CreateExtractFlows
scn:CreatePresignedUrl
scn:CreateSampleParsingJob
scn:CreateSapODataConnection
scn:CreateUpdateDatasetSchemaJob
scn:DeleteConnection
scn:DeleteDataflow
scn:DeleteExtractFlows
scn:DeleteSapODataConnection
scn:describeDatasetGroup
scn:DescribeDataset
```

```
scn:DescribeJob
scn:GetConnection
scn:GetCreateExtractFlowsStatus
scn:GetDataflow
scn:ListConnections
scn:ListCustomerFiles
scn:ListDataflows
scn:ListDataflowStats
scn:ListDatasets
scn:UpdateConnection
scn:UpdateDataflow
scn:UpdateExtractFlow
```

Wawasan

APIs Berikut ini digunakan oleh aplikasi Insights untuk mengelola filter, daftar pantauan, dan melihat perubahan inventaris.

```
scn:AddModeratorToResourceBasedChat
scn:ComputePostRebalancedQuantities
scn:ComputePostRebalancedQuantitiesV1
scn:CreateInsightFilter
scn:CreateInsightSubscription
scn:DeleteInsightFilter
scn:DeleteInsightSubscription
scn:GetInsightLineItem
scn:GetInsightSubscription
scn:GetInstanceAttribute
scn:GetInstanceRequiredDatasetAvailabilityStatus
scn:GetKpiData
scn:GetModelEndpointStatus
scn:GetPIVForProduct
scn:GetPIVForSite
scn:GetPIVForSiteAndProduct
scn:GetPIVForSitesAndProducts
scn:GetProducts
scn:GetProductSummaryAggregates
scn:GetSites
scn:GetSiteSummaryAggregates
```

```
scn:IsUserAuthorizedForInsightLineItem
scn:ListCustomAttributeValues
scn:ListGeographiesAsGalaxyAdmin
scn:ListInsightFilters
scn:ListInsightLineItems
scn:ListInsightSubscriptions
scn:ListInventoryQuantityAggregates
scn:ListInventoryRisksBySiteAndProduct
scn:ListInventorySummariesBySite
scn:ListPIVProductsBySite
scn:ListProductHierarchiesAsGalaxyAdmin
scn:ListProducts
scn:ListProductsAsGalaxyAdmin
scn:ListSites
scn:ListUsers
scn:PotentiallyComputeThenListRebalancingOptionsForInsightLineItem
scn:RegisterInstanceAttribute
scn:UpdateInsightFilter
scn:UpdateInsightLineItemStatus
scn:UpdateInsightSubscription
scn:UpdateRebalancingOptionStatus
scn:UpdateRebalancingOptionStatusV1
```

Perencanaan Permintaan

APIs Berikut ini digunakan Rantai Pasokan AWS untuk membuat dan mengelola prakiraan, rencana permintaan, atau buku kerja.

```
scn:AssociateDatasetWithWorkbook
scn:CreateBaselineForecast
scn:CreateDemandPlan
scn:CreateDemandPlanningCycle
scn:CreateDemandPlanningDatasetExportJob
scn:CreateDerivedForecast
scn:CreateWorkbook
scn:DeleteDemandForecastConfig
scn:DeleteDemandPlanningCycle
scn:DeleteDerivedForecast
scn:DeleteWorkbook
```

```
scn:DescribeBaselineForecast
scn:DescribeDemandPlanningCycleAccuracyJob
scn:DescribeDerivedForecast
scn:DescribePlanningCycle
scn:DescribeWorkbook
scn:DisassociatePlanningCycle
scn:GetDemandForecastConfig
scn:GetDemandPlan
scn:GetDemandPlanningCycle
scn:GetDemandPlanningCycleAccuracy
scn:GetDemandPlanningDatasetJob
scn:ListDemandPlans
scn:ListDerivedForecasts
scn:ListForecastingJobs
scn:ListPlanningCycles
scn:ListWorkbooks
scn:PublishDemandPlan
scn:PutDemandForecastConfig
scn:StartDemandPlanningCycleAccuracyJob
scn:StartForecastingJob
scn:UpdateDemandPlan
scn:UpdateDemandPlanningCycleMetadata
scn:UpdateWorkbook
```

Perencanaan Pasokan

APIs Berikut ini digunakan Rantai Pasokan AWS untuk membuat dan mengelola rencana pasokan.

```
scn:CreateReplenishmentPipeline
scn:GetReplenishmentPipeline
scn:UpdateReplenishmentPipeline
scn:ListReplenishmentPipelinesByInstance
scn:GetInstanceReplenishmentConfig
scn:CreateBacktest
scn:CreateReplenishmentReviewInstanceConfig
scn:GetReplenishmentReviewInstanceConfig
scn:ListReplenishmentVendors
scn:GetExceptionsSupplyInsightsStatistics
scn:GetPorSupplyInsightsStatistics
```

```
scn:GetPlanToPOConversionAnalytics
scn:GetPurchasePlanStatistics
scn:ListPlanExceptions
scn:ListPurchaseOrderRequestLines
scn:UpdatePurchaseOrderRequestLines
scn:ListBomPurchasePlans
scn:ListBomProductionPlans
scn:ListBomTransferPlans
scn:ListBomInsights
scn:ListBomProcesses
scn:ExportBomPlans
scn:GetBomPlanSummary
scn:GetDashboardAnalytics
scn:GetPurchaseOrderRequestExplanation
scn:ListBomSupplyPlan
scn:GetBomPlanRecordDetails
scn:GetBomPlanSummaryAnalytics
scn:ListBomPurchaseOrders
scn:ListBomTransferOrders
scn:ListBomProductionOrders
scn:ExportAllExplodedBoms
scn:ExportBillOfMaterials
scn:ExportInventoryPolicy
scn:ExportProductionProcess
scn:ExportSourcingRule
scn:ExportTransportationLane
scn:ExportVendorLeadTime
scn:ImportBillOfMaterials
scn:ImportInventoryPolicy
scn:ImportProductionProcess
scn:ImportSourcingRule
scn:ImportTransportationLane
scn:ImportVendorLeadTime
```

Amazon Q di Rantai Pasokan AWS

Berikut ini APIs digunakan di Amazon Q in Rantai Pasokan AWS.

```
scn:GetQMessage
```

```
scn:ListQMessages
scn:PutQMessageFeedback
scn:SendQMessage
scn:GetQEnablementStatus
scn:UpdateQEnablementStatus
```

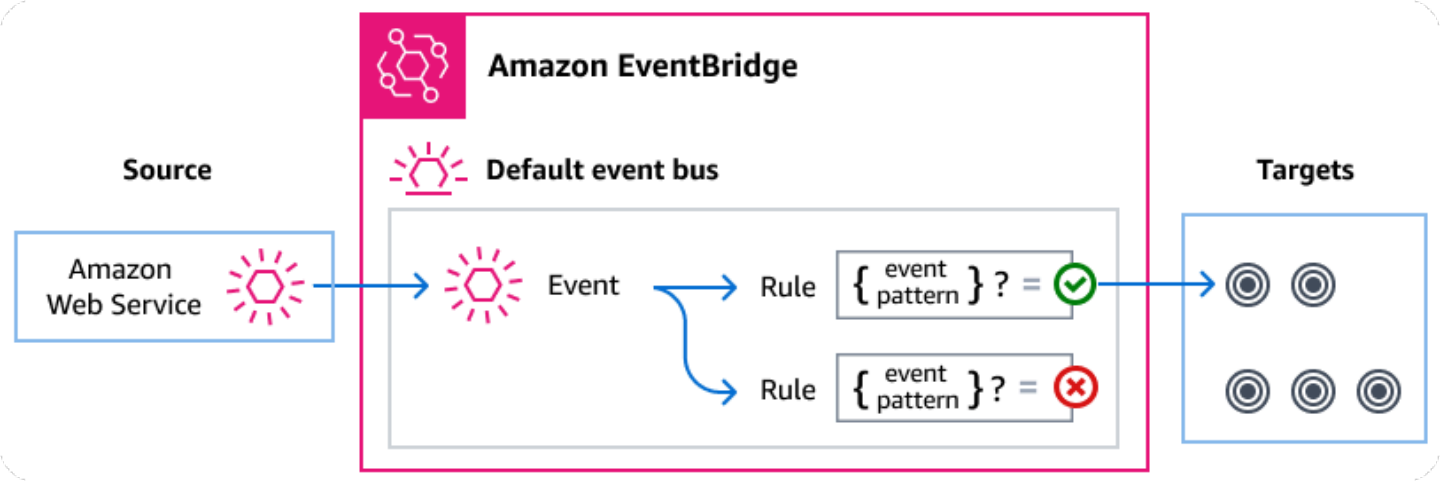
Mengelola Rantai Pasokan AWS acara menggunakan Amazon EventBridge

Dengan menggunakan EventBridge, Anda dapat mengotomatiskan layanan lain untuk merespons perubahan status eksekusi Alur Kerja Step Functions Standar.

Amazon EventBridge adalah layanan tanpa server yang menggunakan peristiwa untuk menghubungkan komponen aplikasi bersama-sama, sehingga memudahkan Anda untuk membangun aplikasi berbasis peristiwa yang dapat diskalakan. Arsitektur berbasis peristiwa adalah gaya membangun sistem perangkat lunak yang digabungkan secara longgar yang bekerja sama dengan memancarkan dan menanggapi peristiwa. Peristiwa mewakili perubahan dalam sumber daya atau lingkungan.

Begini cara kerjanya:

Seperti banyak AWS layanan, Rantai Pasokan AWS menghasilkan dan mengirim acara ke bus acara EventBridge default. (Bus acara default secara otomatis disediakan di setiap AWS akun.) Bus acara adalah router yang menerima acara dan mengirimkannya ke nol atau lebih tujuan, atau target. Aturan yang Anda tentukan untuk bus acara mengevaluasi peristiwa saat mereka tiba. Setiap aturan memeriksa apakah suatu peristiwa cocok dengan pola acara aturan. Jika acara tidak cocok, bus acara mengirimkan acara ke target yang ditentukan.



Topik

Rantai Pasokan AWS acara

Rantai Pasokan AWS mengirimkan peristiwa berikut ke bus EventBridge acara default secara otomatis. Peristiwa yang cocok dengan pola acara aturan dikirimkan ke target yang ditentukan berdasarkan. Acara mungkin dikirim rusak.

Untuk informasi selengkapnya, lihat EventBridge peristiwa di Panduan Amazon EventBridge Pengguna.

Jenis detail acara	Deskripsi
Perubahan Status Integrasi Data Rantai Pasokan AWS	Menampilkan status untuk setiap file yang dicerna ke dalam Rantai Pasokan AWS.

Menyampaikan Rantai Pasokan AWS acara menggunakan EventBridge aturan

Agar bus acara EventBridge default mengirim Rantai Pasokan AWS acara ke target, Anda harus membuat aturan. Setiap aturan berisi pola acara, yang EventBridge cocok dengan setiap acara yang diterima di bus acara. Jika data peristiwa cocok dengan pola peristiwa yang ditentukan, EventBridge mengirimkan peristiwa itu ke target aturan.

Untuk petunjuk komprehensif tentang cara membuat aturan bus acara, lihat Membuat aturan yang bereaksi terhadap peristiwa di Panduan EventBridge Pengguna.

Membuat pola acara yang cocok dengan Rantai Pasokan AWS acara

Setiap pola acara adalah objek JSON yang berisi:

- `source`Atribut yang mengidentifikasi layanan yang mengirim acara. Untuk Rantai Pasokan AWS acara, sumbernya adalah`aws.supplychain`.

- (Opsional): `detail-type` Atribut yang berisi array jenis acara yang cocok.
- (Opsional): `detail` Atribut yang berisi data acara lain yang cocok.

Misalnya, pola acara berikut cocok dengan semua `AWS Supply Chain Data Integration Status Change` peristiwa dari Rantai Pasokan AWS:

```
{
  "source": ["aws.supplychain"],
  "detail-type": ["AWS Supply Chain Data Integration Status Change"]
}
```

Untuk informasi selengkapnya tentang penulisan pola acara, lihat Pola acara di Panduan EventBridge Pengguna.

Rantai Pasokan AWS referensi detail acara

Semua peristiwa dari AWS layanan memiliki seperangkat bidang umum yang berisi metadata tentang acara tersebut, seperti AWS layanan yang merupakan sumber acara, waktu acara dibuat, akun dan wilayah tempat acara berlangsung, dan lainnya. Untuk definisi bidang umum ini, lihat Referensi struktur acara di Panduan Amazon EventBridge Pengguna.

Selain itu, setiap acara memiliki `detail` bidang yang berisi data khusus untuk peristiwa tertentu. Referensi di bawah ini mendefinisikan bidang detail untuk berbagai Rantai Pasokan AWS acara.

Saat menggunakan EventBridge untuk memilih dan mengelola Rantai Pasokan AWS acara, penting untuk mengingat hal berikut:

- `source`Bidang untuk semua acara dari Rantai Pasokan AWS diatur ke`aws.supplychain`.
- `detail-type`Bidang menentukan jenis acara.

  Misalnya, `AWS Supply Chain Data Integration Status Change`.
- `detail`Bidang berisi data yang spesifik untuk peristiwa tertentu.

Untuk informasi tentang membuat pola peristiwa yang memungkinkan aturan untuk mencocokkan Rantai Pasokan AWS peristiwa, lihat Pola acara di Panduan Amazon EventBridge Pengguna.

Untuk informasi selengkapnya tentang peristiwa dan cara EventBridge memprosesnya, lihat Amazon EventBridge peristiwa di Panduan Amazon EventBridge Pengguna.

Perubahan Status Integrasi Data Rantai Pasokan AWS

Di bawah ini adalah contoh untuk `AWS Supply Chain Data Integration Status Change event` acara tersebut.

```
{
    "version": "0",
    "id": "instanceID",
    "detail-type": "AWS Supply Chain Data Integration Status Change",
    "source": "aws.supplychain",
    "account": "acccountID",
    "time": "2024-03-30T12:26:13Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "version": "1.0",
        "instanceId": "instanceID",
        "flowArn": "arn:aws:scn:region:acccountID:instance/instanceID/data-integration-
flows/flowname",
        "flowExecutionId": "flowExecutionId",
        "status": "IN_PROGRESS",
        "startTime": "2024-03-30T12:26:13Z",
        "endTime": "",
        "message": "",
        "sourceType": "S3",
        "sourceInfo": {
            "s3Source": {
                "bucketName": "aws-supply-chain-data-instanceID",
                "key": "flowname"
            }
        }
    }
}
```

`endTime`hanya tersedia jika statusnya gagal atau sukses.

Kuota untuk Rantai Pasokan AWS

Anda Akun AWS memiliki kuota default, sebelumnya disebut sebagai batas, untuk masing-masing. Layanan AWS Kecuali dinyatakan lain, setiap kuota bersifat khusus per Wilayah. Anda dapat meminta untuk meningkatkan kuota untuk sumber daya yang diatur ke tingkat akun Anda. Untuk informasi lebih lanjut tentang kuota tingkat akun, lihat tabel di bawah ini.

Untuk melihat kuota Rantai Pasokan AWS, buka konsol Service Quotas. Pada panel navigasi, pilih Layanan AWS dan pilih Rantai Pasokan AWS.

Untuk meminta peningkatan kuota, lihat Meminta Peningkatan Kuota dalam Panduan Pengguna Service Quotas. Jika kuota belum tersedia di Service Quotas, gunakan formulir kenaikan batas.

Anda Akun AWS memiliki kuota berikut yang terkait Rantai Pasokan AWS dengan.

Sumber Daya	Default	Dapat disesuaikan
Jumlah instans **Note** Anda dapat membuat hingga 10 instance dalam AWS akun.	10	Tidak
Jumlah ember Amazon S3	100	Tidak
Undangan aktif dan tertunda dalam akun AWS	30	Ya
Permintaan data dalam AWS akun	4.000	Ya
Item baris wawasan per daftar pantauan	1.000	Tidak
Daftar pantauan wawasan per instans dalam akun AWS	1.000	Ya

Sumber Daya	Default	Dapat disesuaikan
Daftar pantauan wawasan per pengguna dalam akun AWS	100	Ya
Aliran integrasi data per instance dalam AWS akun	100	Tidak
Ruang nama set data khusus per instance dalam akun AWS	20	Ya
Kumpulan data per namespace set data khusus per instance dalam akun AWS	250	Ya
Kumpulan data dalam namespace set data default per instance dalam akun AWS	1.000	Tidak

Pertanyaan yang sering diajukan (FAQs)

Informasi berikut dapat membantu Anda memecahkan masalah umum dalam mengaktifkan Pusat Identitas IAM.

Pertanyaan	Jawaban
Mengapa integrasi IAM Identity Center diperlukan?	IAM Identity Center adalah fitur dalam IAM yang mengelola sinkronisasi sumber identitas . IAM Identity Center adalah sumber identitas untuk Rantai Pasokan AWS contoh tersebut. Anda perlu mengkonfigurasi IAM Identity Center untuk setup AWS Console dan aplikasi Rantai Pasokan AWS web. Untuk informasi selengkapnya tentang Pusat Identitas IAM, lihat Mengaktifkan Pusat AWS Identitas IAM di Panduan Pengguna.AWS IAM Identity Center
Mengapa menggunakan instans organisas i Pusat Identitas IAM untuk Rantai Pasokan AWS?	Dengan membuat instance organisasi, Anda dapat mengaktifkan akses Pusat Identitas IAM di seluruh AWS akun. Misalnya, jika Pusat Identitas IAM Anda tidak diaktifkan di akun yang sama dengan AWS akun Rantai Pasokan AWS instans. Untuk informasi selengkapnya tentang manfaat dalam membuat instans Pusat Identitas IAM organisasi, lihat Instans organisas i Pusat Identitas IAM di Panduan Pengguna. AWS IAM Identity Center
Mengapa hak administrator yang didelegasikan diperlukan untuk? Rantai Pasokan AWS	Tidak perlu memiliki administrator yang didelegasikan untuk digunakan Rantai Pasokan AWS tetapi ini adalah praktik terbaik untuk pengaturan AWS Organisasi untuk membatasi akses ke akun manajemen untuk organisas i dan mengelola Pusat Identitas IAM. Untuk informasi selengkapnya, lihat Delegated adminsitrotor for Organizations. AWS .

Pertanyaan	Jawaban
	Saat membuat instance organisasi, pastikan akun yang akan digunakan untuk membuat Rantai Pasokan AWS instance adalah bagian dari organisasi yang sama dengan akun IAM Identity Center. Pastikan izin yang diperlukan diaktifkan untuk membuat instance dan Anda dapat membuat Rantai Pasokan AWS instance di wilayah yang sama dengan akun IAM Identity Center. Untuk informasi tentang izin yang diperlukan untuk membuat Rantai Pasokan AWS instance, lihatMemulai dengan Rantai Pasokan AWS.

AWS dukungan

Jika Anda seorang administrator dan perlu menghubungi dukungan untuk Rantai Pasokan AWS, pilih salah satu opsi berikut:

- Jika Anda memiliki Dukungan akun, buka Support Center dan kirimkan tiket.
- Buka AWS Management Consoledan pilih AWS Supply Chain, Support, Create case.

Sangat membantu untuk memberikan informasi berikut:

- ID Instance Rantai AWS Pasokan Anda/ARN.
- AWS Wilayah Anda.
- Penjelasan rinci tentang masalah Anda.

Riwayat dokumen untuk Panduan Rantai Pasokan AWS Administrator

Tabel berikut menjelaskan rilis dokumentasi untuk Rantai Pasokan AWS.

Perubahan	Deskripsi	Tanggal
Rantai Pasokan AWS Kuota yang diperbarui	Memperbarui kuota untuk AWS akun Anda yang terkait Rantai Pasokan AWS dengan.	12 Mei 2025
Kebijakan AWS terkelola yang diperbarui	Rantai Pasokan AWS memperbarui kebijakan terkelola untuk memungkinkan pengguna federasi mengakses ListApplicationAssignments,, DescribeApplication DescribeI nstance, dan GetApplic ationAssignmentConfiguration operasi di Pusat Identitas IAM.	Desember 10, 2024
Pembaruan kebijakan KMS	Memperbarui kebijakan KMS agar dapat Rantai Pasokan AWS mengakses AWS KMS kunci Anda.	Maret 18, 2024
PrivateLink dukungan	Anda dapat mengakses Rantai Pasokan AWS menggunak an titik akhir antarmuka (AWS PrivateLink).	Februari 26, 2024
Menambahkan Grup	Pengguna harus menjadi bagian dari grup Pusat Identitas IAM untuk mengakses Rantai Pasokan AWS.	14 November 2023

Kebijakan AWS terkelola yang diperbarui	Rantai Pasokan AWS memperbarui kebijakan terkelola untuk memungkinkan pengguna federasi mengakses ListProfileAssociations operasi di Pusat Identitas IAM.	1 November 2023
Kebijakan AWS terkelola yang diperbarui	Rantai Pasokan AWS memperbarui kebijakan terkelola untuk mengizinkan pengguna federasi mengakses PutObject dan GetObject operasi pada bucket Amazon S3 khusus dengan resource arn arn:aws:s3: ::aws-supply-chain-data-*.	21 September 2023
Informasi terbaru tentang dukungan wilayah	Rantai Pasokan AWS Perencanaan Permintaan sekarang juga didukung di Wilayah Asia Pasifik (Sydney).	12 September 2023
Menggunakan AWS Konsol untuk ikut serta dan memilih keluar Rantai Pasokan AWS	Rantai Pasokan AWS pengguna kini dapat menggunakan AWS Konsol untuk ikut serta dan memilih Rantai Pasokan AWS untuk tidak menggunakan atau menyimpan Konten Anda di AWS Organizations.	7 September 2023
Informasi terbaru tentang dukungan wilayah	Rantai Pasokan AWS sekarang juga didukung di Wilayah Asia Pasifik (Sydney), dan Wilayah Eropa (Irlandia).	Juli 19, 2023

Informasi terbaru tentang cara menghubungi AWS Support dan membuat instance	Rantai Pasokan AWS pengguna sekarang dapat menghubungi AWS Support untuk mendapatkan bantuan dan memperbarui konten tentang cara membuat instance.	3 April 2023
Ditambahkan kebijakan AWS terkelola	AWS Supply Chain menambahkan kebijakan baru untuk memungkinkan pengguna federasi mengakses aplikasi AWS Supply Chain, termasuk izin yang diperlukan untuk melakukan tindakan dalam aplikasi AWS Supply Chain.	1 Maret 2023
Rilis awal	Rilis awal Panduan Rantai Pasokan AWS Administrator.	29 November 2022

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