



Panduan Administrator

# Rantai Pasokan AWS



# Rantai Pasokan AWS: Panduan Administrator

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

---

# Table of Contents

Apakah Rantai Pasokan AWS itu? .....	1
Peramban yang didukung .....	1
Bahasa didukung .....	1
.....	1
Menyiapkan AWS akun .....	3
Mendaftar untuk Akun AWS .....	3
Buat pengguna dengan akses administratif .....	4
Menutup AWS akun .....	5
Memulai dengan Rantai Pasokan AWS .....	6
Prasyarat .....	6
Menggunakan konsol tersebut .....	8
Membuat sebuah instance .....	11
Mengaktifkan Pusat Identitas IAM .....	16
Menambahkan pengguna di Pusat Identitas IAM .....	16
Memilih pemilik Rantai Pasokan AWS aplikasi .....	16
Tetapkan grup .....	17
Masuk ke aplikasi web AWS Supply Chain .....	18
Masuk Rantai Pasokan AWS untuk pertama kalinya .....	18
Memperbarui profil akun Anda .....	19
Memperbarui profil organisasi Anda .....	19
Peran izin pengguna .....	19
Menambahkan pengguna .....	20
Memperbarui izin pengguna .....	21
Menghapus pengguna .....	22
Membuat peran izin pengguna khusus .....	22
Menghapus sebuah instans .....	23
Keamanan .....	24
Perlindungan data .....	25
Data yang ditangani oleh Rantai Pasokan AWS .....	26
Preferensi memilih keluar .....	26
Enkripsi diam .....	26
Enkripsi dalam bergerak .....	27
Manajemen kunci .....	27
Privasi lalu lintas antar jaringan .....	27

Bagaimana Rantai Pasokan AWS menggunakan hibah di AWS KMS .....	27
AWS PrivateLink .....	31
Pertimbangan .....	31
Membuat sebuah titik akhir antarmuka .....	32
Membuat kebijakan titik akhir .....	32
IAM .....	33
Audiens .....	33
Mengautentikasi dengan identitas .....	34
Mengelola akses menggunakan kebijakan .....	38
Bagaimana Rantai Pasokan AWS bekerja dengan IAM .....	40
Contoh kebijakan berbasis identitas .....	46
Pemecahan Masalah .....	48
Kebijakan yang dikelola oleh AWS .....	50
AWSSupplyChainFederationAdminAccess .....	51
Pembaruan kebijakan .....	52
Validasi Kepatuhan .....	53
Ketahanan .....	54
Penebangan dan Pemantauan Rantai AWS Pasokan .....	54
Rantai Pasokan AWS peristiwa data di CloudTrail .....	55
Rantai Pasokan AWS acara manajemen di CloudTrail .....	56
API aplikasi web .....	57
Kuota .....	63
Dukungan administratif .....	65
Riwayat dokumen .....	66
.....	lxi

# Apakah Rantai Pasokan AWS itu?

Rantai Pasokan AWS adalah aplikasi manajemen rantai pasokan berbasis cloud yang bekerja dengan solusi yang ada seperti perencanaan sumber daya perusahaan (ERP) dan sistem manajemen rantai pasokan. Dengan menggunakan Rantai Pasokan AWS, Anda dapat menghubungkan dan mengekstrak data terkait inventaris, penawaran, dan permintaan Anda dari ERP yang ada atau sistem rantai pasokan ke dalam satu model Rantai Pasokan AWS data terpadu.

## Topik

- [Browser yang didukung oleh Rantai Pasokan AWS](#)
- [Bahasa yang didukung oleh Rantai Pasokan AWS](#)

## 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 terakhir terakhir terakhir terakhir.
Mozilla Firefox ESR	Versi didukung hingga <a href="#">end-of-lifetanggal</a> Firefox mereka. Untuk detailnya, lihat <a href="#">kalender rilis Firefox ESR</a> .
Mozilla Firefox	Tiga versi terakhir terakhir terakhir terakhir.
Microsoft Edge dan Edge Chromium	Versi 84 dan yang lebih baru.
Safari	Safari 10 atau versi lebih baru di macOS.

## Bahasa yang didukung oleh Rantai Pasokan AWS

Rantai Pasokan AWS mendukung bahasa berikut:

- Bahasa Inggris (AS)
- Bahasa Inggris (UK)
- Bahasa Jerman
- Bahasa Spanyol
- Bahasa Perancis
- Bahasa Italia
- Portugese
- Bahasa Mandarin Disederhanakan)
- Mandarin (Tradisional)
- Bahasa Jepang
- Bahasa Korea
- orang Indonesia

# 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](#)
- [Menutup AWS akun](#)

## Mendaftar untuk Akun AWS

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

Untuk mendaftar untuk Akun AWS

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

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

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

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

## Buat pengguna dengan akses administratif

Setelah Anda mendaftarkan 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 Console](#) sebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.

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

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

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

Buat pengguna dengan akses administratif

1. Aktifkan Pusat Identitas IAM.

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

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

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

Masuk sebagai pengguna dengan akses administratif

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

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



## Tetapkan akses ke pengguna tambahan

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

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

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

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

## Menutup AWS akun

Untuk informasi tentang cara menutup AWS akun, lihat [Menutup akun](#).

# 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

- [Prasyarat](#)
- [Menggunakan konsol Rantai Pasokan AWS](#)
- [Membuat sebuah instance](#)
- [Mengaktifkan Pusat Identitas IAM](#)
- [Memilih pemilik Rantai Pasokan AWS aplikasi](#)
- [Tetapkan grup](#)
- [Masuk ke aplikasi web AWS Supply Chain](#)
- [Memperbarui profil akun Anda](#)
- [Memperbarui profil organisasi Anda](#)
- [Peran izin pengguna](#)
- [Membuat peran izin pengguna khusus](#)
- [Menghapus sebuah instans](#)

## Prasyarat

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

- Anda telah membuat sebuah Akun AWS. Untuk informasi selengkapnya, lihat [Menyiapkan AWS akun](#).

**Note**

Jika Anda belum mengaktifkan AWS IAM Identity Center, buat AWS organisasi dan aktifkan IAM Identity Center. Untuk informasi selengkapnya tentang membuat AWS organisasi, lihat [Membuat organisasi](#).

- Aktifkan IAM Identity Center di Wilayah AWS tempat 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), dan Wilayah Eropa (Irlandia). Untuk informasi selengkapnya, lihat [Mengaktifkan Pusat Identitas IAM](#).

**Note**

Rantai Pasokan AWS Perencanaan Permintaan dan Perencanaan Pasokan tidak didukung di Wilayah Eropa (Irlandia).

**Note**

Jika Anda belum mengaktifkan Pusat Identitas IAM di Wilayah selain yang tercantum di sini, Anda tidak dapat membuat Rantai Pasokan AWS instance.

- Anda dapat membuat pengguna IAM dari konsol AWS Identity and Access Management (IAM). Untuk informasi selengkapnya, lihat [Menyiapkan AWS akun](#).
- Tambahkan pengguna yang membutuhkan akses Rantai Pasokan AWS ke Pusat Identitas IAM. Untuk informasi selengkapnya, lihat [Menambahkan pengguna di Pusat Identitas IAM](#). Anda juga dapat menghubungkan direktori aktif Anda ke IAM Identity Center. Untuk informasi selengkapnya, lihat [Connect ke direktori Microsoft AD](#) di Panduan AWS IAM Identity Center Pengguna.
- Saat menggunakan direktori aktif Microsoft, pastikan sinkronisasi direktori aktif diaktifkan.
- 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.

# Menggunakan konsol Rantai Pasokan AWS

## 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.

Untuk memastikan bahwa pengguna dan peran masih dapat menggunakan Rantai Pasokan AWS konsol, lampirkan juga kebijakan Rantai Pasokan AWS ConsoleAccess atau ReadOnly AWS terkelola ke entitas. Untuk informasi selengkapnya, lihat [Menambah izin untuk pengguna](#) dalam Panduan Pengguna IAM.

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:DescribeOrganization",
        "organizations:CreateOrganization",
        "organizations:EnableAWSServiceAccess"
    ],
    "Resource": "*",
    "Effect": "Allow"
},
{
    "Action": [
        "kms:CreateGrant",
        "kms:RetireGrant",
        "kms:DescribeKey",
        "kms:ListAliases"
    ],
    "Resource": "*",
    "Effect": "Allow"
},
{
    "Action": [
        "iam:CreateRole",
        "iam:CreatePolicy",
        "iam:GetRole",
        "iam:PutRolePolicy",
        "iam:AttachRolePolicy",
        "iam:CreateServiceLinkedRole"
    ],
    "Resource": "*",
```


```
    "Effect": "Allow"
  },
  {
    "Action": [
      "sso:StartPeregrine",
      "sso:DescribeRegisteredRegions",
      "sso:ListDirectoryAssociations",
      "sso:GetPeregrineStatus",
      "sso:GetSSOStatus",
      "sso:ListProfiles",
      "sso:GetProfile",
      "sso:AssociateProfile",
      "sso:AssociateDirectory",
      "sso:RegisterRegion",
      "sso:StartSSO",
      "sso:CreateManagedApplicationInstance",
      "sso>DeleteManagedApplicationInstance",
      "sso:GetManagedApplicationInstance",
      "sso-directory:SearchUsers"
    ],
    "Resource": "*",
    "Effect": "Allow"
  }
]
```

## Membuat sebuah instance

### Note


Anda dapat membuat hingga 10 instance Akun AWS dalam file. 10 instance termasuk instance aktif dan inisialisasi. Jika Anda telah mengaktifkan IAM Identity Center (penerus AWS Single Sign-On), Anda harus membuat Rantai Pasokan AWS instance Anda di tempat yang sama di Wilayah AWS mana Anda telah mengaktifkan IAM Identity Center. Rantai Pasokan AWS tidak mendukung panggilan Pusat Identitas IAM di seluruh Wilayah.

Untuk membuat Rantai Pasokan AWS instance, ikuti langkah-langkah ini.

 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 bawah [Menggunakan konsol Rantai Pasokan AWS](#). Administrator ini harus mengundang pengguna IAM sebagai Rantai Pasokan AWS administrator untuk mengelola Rantai Pasokan AWS.

1. Buka Rantai Pasokan AWS konsol di <https://console.aws.amazon.com/scn/home>.
2. Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya tentang Wilayah, lihat [Wilayah dan titik akhir](#) di Panduan Pengguna IAM. Juga, lihat Wilayah dan titik akhir di. Referensi Umum Amazon Web

 Note

Rantai Pasokan AWS hanya didukung di AS Timur (Virginia N.), AS Barat (Oregon), Eropa (Frankfurt) Asia Pasifik (Sydney), dan Wilayah Eropa (Irlandia). Rantai Pasokan AWS Perencanaan Permintaan dan Perencanaan Pasokan tidak didukung di Wilayah Eropa (Irlandia).

3. Di Rantai Pasokan AWS dasbor, pilih Buat instance.
4. Pada halaman properti Instance, masukkan informasi berikut:
  - AWS Wilayah — Pilih Wilayah tempat Anda mengaktifkan Pusat Identitas IAM. Untuk mengubah Wilayah, pilih Pilih Wilayah dari menu tarik-turun di kanan atas. Anda tidak dapat mengubah Wilayah setelah membuat instance.
  - Nama - Masukkan nama instance.
  - (Opsional) Deskripsi - Masukkan deskripsi untuk contoh.
5. Di bawah Kunci AWS KMS, masukkan kunci KMS Anda dan perbarui kebijakan kunci KMS Anda dengan yang berikut:



**Note**

Sebagai administrator 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, lihat [Peran izin pengguna](#).

**Note**

Ganti *YourAccountNumber*, *Wilayah*, *YourInstanceID*, dan *YourKmsKeyArn* dengan Akun AWS, AWS Wilayah, ID Rantai Pasokan AWS Instance, dan AWS KMS Kunci Anda.

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

Jika Anda tidak memiliki kunci KMS, pilih Buat untuk pergi ke AWS KMS konsol, di mana Anda dapat membuat kunci ini. Gunakan kebijakan kunci KMS sebelumnya. Untuk informasi rinci tentang cara membuat kunci KMS, lihat [Membuat kunci](#) di Panduan AWS Key Management Service Pengembang.

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

6. (Opsional) Di bawah tag Instance, pilih Tambahkan tag baru untuk menetapkan tag untuk instance Anda. Anda dapat menggunakan tag ini untuk mengidentifikasi instance Anda. Untuk informasi tentang tag, lihat [Membuat tag](#).
7. Pilih Buat instans.

Dibutuhkan sekitar 2 hingga 3 menit untuk membuat Rantai Pasokan AWS instance. Setelah instance dibuat, bidang Status di Rantai Pasokan AWS dasbor ditampilkan sebagai Aktif.

8. Setelah Rantai Pasokan AWS instans Anda dibuat, perbarui kebijakan KMS Anda Rantai Pasokan AWS untuk mengizinkan mengakses AWS KMS kunci Anda.

**Note**

Ganti *YourInstanceID* dengan ID Rantai Pasokan AWS instans Anda. Anda dapat menemukan ID instans Anda di dasbor Rantai Pasokan AWS konsol.

```

    {
      "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": "*"
    },
    {
      "Sid": "Enable ASC to backfill KMS permissions",
      "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": "YourKmsKeyArn"
    }
  }

```

## Mengaktifkan Pusat Identitas IAM

Sebelum Anda mulai menggunakan Rantai Pasokan AWS, Anda harus terhubung ke sumber identitas. Untuk informasi selengkapnya, lihat [Memulai IAM](#) di Panduan Pengguna IAM.

## Menambahkan pengguna di Pusat Identitas IAM

Anda dapat mengelola pengguna untuk Rantai Pasokan AWS menggunakan layanan Pusat Identitas IAM. IAM Identity Center adalah layanan IAM Identity Center berbasis cloud yang memudahkan untuk mengelola akses Pusat Identitas IAM ke semua aplikasi Anda Akun AWS dan cloud secara terpusat. Untuk menambahkan pengguna IAM, lihat [Membuat pengguna IAM di akun AWS Anda di Panduan Pengguna IAM](#).

Untuk informasi selengkapnya tentang membuat grup pengguna IAM, lihat [Membuat grup pengguna IAM](#) di Panduan Pengguna IAM.

### Note

Untuk menambahkan pengguna Rantai Pasokan AWS, pengguna harus menjadi bagian dari grup Pusat Identitas IAM.

## Memilih pemilik Rantai Pasokan AWS aplikasi

### Note

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. Di dasbor Rantai Pasokan AWS konsol, di bawah Pemilik aplikasi, pilih Tetapkan pemilik aplikasi.
2. Di bawah Pilih pemilik aplikasi, pilih pengguna yang akan bertindak sebagai pemilik Rantai Pasokan AWS aplikasi. Anda hanya dapat mencari nama pengguna dan pengguna yang cocok dengan kriteria pencarian muncul.

Untuk menambahkan lebih banyak pengguna, pilih Buka Pusat Identitas IAM. Untuk informasi selengkapnya tentang menambahkan pengguna, lihat [Menambahkan pengguna di Pusat Identitas IAM](#) 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.

3. pilih Kirim Undangan.

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

4. Pilih Kelola Rantai Pasokan AWS untuk menambah dan menghapus pengguna di aplikasi Rantai Pasokan AWS web.

## Tetapkan grup

Sebagai pemilik aplikasi atau Rantai Pasokan AWS administrator, Anda hanya dapat menambahkan pengguna yang merupakan bagian dari grup Pusat Identitas IAM ke Rantai Pasokan AWS.

1. Di dasbor Rantai Pasokan AWS konsol, di bawah Grup, pilih Tetapkan Grup.

Halaman Grup muncul.

2. Di bawah Nama grup pilih grup dengan pengguna yang dapat mengakses Rantai Pasokan AWS dan pilih Tetapkan.

Anda akan melihat grup yang Anda cantumkan di bawah Grup di Rantai Pasokan AWS dasbor.

3. Anda dapat memilih Kelola grup untuk menambahkan grup baru di Pusat Identitas IAM. Setelah grup ditambahkan di Pusat Identitas IAM, grup akan terdaftar di bawah Nama grup di Rantai Pasokan AWS.

## Masuk ke aplikasi web AWS Supply Chain

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 AWS web muncul.

2. Masukkan kredensi pengguna AWS IAM Identity Center dan pilih Masuk.

## Masuk Rantai Pasokan AWS untuk pertama kalinya

### Note

Anda hanya akan diminta untuk melengkapi profil untuk akun dan organisasi Anda saat Anda masuk untuk pertama kalinya.

Setelah Anda masuk ke aplikasi Rantai Pasokan AWS web sebagai Rantai Pasokan AWS administrator, ikuti langkah-langkah ini untuk menyelesaikan pengaturan.

1. Pada halaman Lengkapi profil Anda, masukkan Job Title dan zona Waktu Anda. Pilih Selanjutnya.
2. Pada halaman Mari tambahkan informasi organisasi Anda, masukkan nama Organisasi dan pilih Lokasi kantor pusat. Secara opsional, Anda dapat menambahkan logo perusahaan. Pilih Selanjutnya.
3. 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 cara menambahkan pengguna ke Pusat Identitas IAM, lihat [Menambahkan pengguna di Pusat Identitas IAM](#). Untuk informasi tentang peran izin Rantai Pasokan AWS pengguna, lihat [Peran izin pengguna](#).

4. Jika Anda ingin menambahkan pengguna nanti, Anda dapat memilih Lewati untuk sekarang.  
Halaman lengkap Onboarding muncul.
5. 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.
6. Pilih Lanjutkan ke beranda untuk melihat Rantai Pasokan AWS dasbor.

## Memperbarui profil akun Anda

Anda dapat memperbarui profil akun Anda kapan saja di aplikasi Rantai Pasokan AWS web. Ikuti langkah-langkah ini untuk memperbarui akun.

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

Anda dapat memperbarui profil Organisasi kapan saja di aplikasi Rantai Pasokan AWS web. Ikuti langkah-langkah ini untuk memperbarui profil organisasi.

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.

## 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 — Akses untuk membuat, melihat, dan mengelola perkiraan, mengganti, 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](#)
- [Memperbarui izin pengguna](#)
- [Menghapus pengguna](#)

## Menambahkan pengguna

#### Note

Sebelum Anda menambahkan pengguna, pastikan pengguna adalah bagian dari grup Pusat Identitas IAM dan grup ditetapkan. Rantai Pasokan AWS



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

1. Di Rantai Pasokan AWS dasbor, dari panel navigasi kiri, pilih ikon Pengaturan.

2. Pilih Izin, lalu pilih Pengguna.

Halaman Kelola Pengguna muncul.

3. Pilih Tambahkan Pengguna Baru.

Halaman Tambah Pengguna muncul.

4. Pada menu tarik-turun Tambahkan pengguna, pilih pengguna, dan di bawah Pilih peran, pilih peran untuk pengguna.

5. Pilih Tambahkan.

## Memperbarui izin pengguna

Anda dapat memperbarui peran izin pengguna untuk Rantai Pasokan AWS pengguna saat ini. Ikuti langkah-langkah ini untuk memperbarui peran izin pengguna.

1. Di Rantai Pasokan AWS dasbor, dari panel navigasi kiri, pilih ikon Pengaturan.

2. Pilih Izin, lalu pilih Pengguna.

Halaman Kelola Pengguna 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 di bawah ini:

### Note

Bergantung pada izin peran yang Anda tetapkan, Rantai Pasokan AWS dasbor disesuaikan. Untuk informasi selengkapnya, lihat [Membuat peran izin pengguna khusus](#).

- 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.

- **Planner** — Akses untuk membuat, melihat, dan mengelola prakiraan, mengesampingkan, dan mempublikasikan rencana permintaan.
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 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.

### 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.

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. 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.

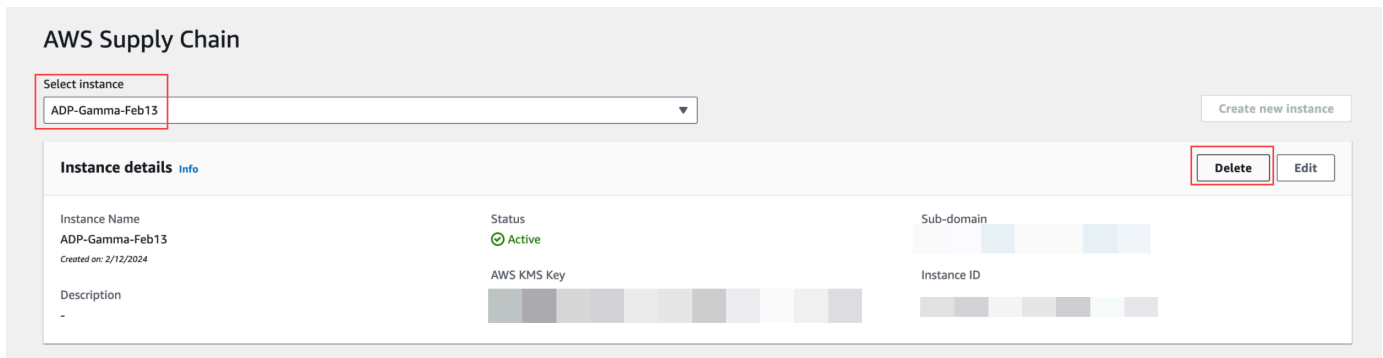
## Menghapus sebuah instans

Untuk menghapus instance, gunakan langkah-langkah berikut.

### Note

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

1. Buka Rantai Pasokan AWS konsol di <https://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.

# 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](#)
- [Akses Rantai Pasokan AWS menggunakan endpoint antarmuka \(\) AWS PrivateLink](#)
- [IAM untuk Rantai Pasokan AWS](#)
- [Kebijakan terkelola AWS untuk Rantai Pasokan AWS](#)
- [Validasi kepatuhan untuk Rantai Pasokan AWS](#)
- [Ketahanan di Rantai Pasokan AWS](#)
- [Penebangan dan Pemantauan Rantai Pasokan AWS](#)

# 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 kredensial 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 pencatatan aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi yang lebih lengkap tentang titik akhir FIPS yang tersedia di [Standar Pemrosesan Informasi Federal \(FIPS\) 140-2](#).

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 SDK. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat

menganjurkan supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

## Data yang 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 Anda ingin memilih untuk tidak menggunakan atau menyimpan konten Anda, 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 yang 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 dalam bergerak

Data yang dipertukarkan dengan AWS Supply Chain dilindungi dalam perjalanan antara browser web pengguna dan AWS Supply Chain 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 [Membuat 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 `CreateInstance` operasi. Rantai Pasokan AWS membuat hibah atas nama Anda dengan mengirimkan [CreateGrant](#) permintaan 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 GenerateDataKey permintaan AWS KMS untuk [mengenkrupsi](#) data yang disimpan dalam instance Anda.
- Untuk mengirim permintaan Dekripsi ke AWS KMS agar dapat membaca data terenkripsi yang terkait dengan instance.
- Untuk menambahkan DescribeKey, CreateGrant, dan RetireGrant izin 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, maka 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 Basic IAM. Untuk mempelajari lebih lanjut tentang bagaimana perusahaan Anda dapat menggunakan IAM Rantai Pasokan AWS, lihat [Bagaimana 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 kredensial 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 kredensial yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (IAM Identity Center), autentikasi masuk tunggal perusahaan Anda, dan kredensial 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 kredensial Anda. Jika Anda tidak menggunakan AWS alat, Anda

harus menandatangani permintaan sendiri. Untuk informasi selengkapnya tentang penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, lihat [Menandatangani permintaan AWS API](#) di 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 [Menggunakan autentikasi multi-faktor \(MFA\) dalam AWS](#) 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 kredensial 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 memiliki grup yang bernama IAMAdmins dan memberikan izin ke 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 [Kapan harus membuat pengguna IAM \(bukan peran\)](#) 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. Anda dapat mengambil peran IAM untuk sementara AWS Management Console dengan [beralih peran](#). 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 [Menggunakan peran IAM](#) 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 [Membuat 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 secara 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 di Panduan Pengguna IAM](#).
- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Sebagai contoh, ketika Anda memanggil 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 [Membuat 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 peran layanan. 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 instans EC2 dan membuat atau permintaan

API. AWS CLI AWS Cara ini lebih dianjurkan daripada menyimpan kunci akses dalam instans EC2. Untuk menetapkan AWS peran ke instans EC2 dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instans berisi peran dan memungkinkan program yang berjalan di instans EC2 mendapatkan kredensial sementara. Untuk informasi selengkapnya, lihat [Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan dalam instans Amazon EC2](#) dalam Panduan Pengguna IAM.

Untuk mempelajari apakah kita harus menggunakan peran IAM atau pengguna IAM, lihat [Kapan harus membuat peran IAM \(bukan pengguna\)](#) dalam Panduan Pengguna IAM.

## Mengelola akses menggunakan kebijakan

Anda 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. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

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 [Membuat kebijakan IAM](#) 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 Anda lampirkan 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 [Memilih 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 (ACL)

Daftar kontrol akses (ACL) mengendalikan prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis sumber daya, meskipun kebijakan tersebut tidak menggunakan format dokumen kebijakan JSON.

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung ACL. Untuk mempelajari ACL selengkapnya, lihat [Gambaran umum daftar kontrol akses \(ACL\)](#) dalam Panduan Developer Amazon Simple Storage Service.

## 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 (SCP) — SCP 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 di organisasi, Anda dapat menerapkan kebijakan kontrol layanan (SCP) 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 Organisasi dan SCP, lihat [Cara kerja SCP](#) dalam Panduan Pengguna AWS Organizations .
- 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
<a href="#">Kebijakan berbasis identitas</a>	Ya
<a href="#">Kebijakan berbasis sumber daya</a>	Tidak
<a href="#">Tindakan kebijakan</a>	Ya
<a href="#">Sumber daya kebijakan</a>	Ya
<a href="#">Kunci kondisi kebijakan</a>	Ya
<a href="#">Kredensial sementara</a>	Ya
<a href="#">Sesi akses teruskan (FAS)</a>	Ya
<a href="#">Peran layanan</a>	Ya
<a href="#">Peran terkait layanan</a>	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 [Membuat kebijakan IAM](#) 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 prinsipal dalam akun yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi selengkapnya, lihat [Akses sumber daya lintas akun di IAM](#) di 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. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan 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.

Menyertakan 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. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan 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	Ya
--	----

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan 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 tag yang sesuai dengan nama pengguna IAM mereka. Untuk informasi selengkapnya, lihat [Elemen kebijakan IAM: variabel dan tag](#) 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 kredensial sementara dengan Rantai Pasokan AWS

Mendukung penggunaan kredensial sementara      Ya

Beberapa Layanan AWS tidak berfungsi saat Anda masuk menggunakan kredensial 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 kredensial 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 [Peralihan peran \(konsol\)](#) dalam Panduan Pengguna IAM.

Anda dapat membuat kredensial sementara secara manual menggunakan API AWS CLI atau AWS . Anda kemudian dapat menggunakan kredensial sementara tersebut untuk mengakses. AWS AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensial 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 [Membuat 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 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 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 [Mengonfigurasi akses API yang dilindungi MFA](#) dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat [Praktik terbaik keamanan dalam 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 (ACL), 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, lihat [Bagaimana 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](#).

## Kebijakan terkelola AWS untuk Rantai Pasokan AWS

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

Perlu diingat bahwa kebijakan terkelola AWS mungkin tidak memberikan izin hak akses paling rendah untuk kasus penggunaan khusus 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 ada dalam kebijakan-kebijakan terkelola AWS. Jika AWS memperbarui izin yang ditentukan dalam sebuah kebijakan terkelola AWS, maka pembaruan itu akan mempengaruhi semua identitas pengguna utama (pengguna, grup, dan peran) yang terkait dengan kebijakan tersebut. AWS kemungkinan besar akan memperbarui kebijakan terkelola AWS saat sebuah Layanan AWS baru diluncurkan atau operasi API baru tersedia untuk layanan yang sudah ada.

Untuk informasi selengkapnya, silakan lihat [kebijakan terkelola AWS](#) di Panduan Pengguna IAM.

## AWSkebijakan terkelola: AWSSupplyChainFederationAdminAccess

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 AWSSupplyChainFederationAdminAccess 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 AWSPeran hanya menyertakan izin yang diperlukan, dan tidak memiliki izin ke API admin.

### 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 "SCN". InstanceId
- **AWS IAM Identity Center (AWS SSO)**— Memberikan izin yang diperlukan untuk mengaitkan dan memisahkan profil pengguna dan daftar profil yang terkait dengan contoh aplikasi 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-supply-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 [AWSSupplyChainFederationAdminAccess](#) di AWS Management Console

## Rantai Pasokan AWS memperbarui pada kebijakan terkelola AWS

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 dokumen Rantai Pasokan AWS.

Perubahan	Deskripsi	Tanggal
<a href="#">AWSSupplyChainFederationAdminAccess</a> — Kebijakan yang diperbarui	Rantai Pasokan AWS memperbarui kebijakan terkelola untuk memungkinkan pengguna federasi mengakses ListProfileAssociations operasi di Pusat Identitas IAM.	November 01, 2023
<a href="#">AWSSupplyChainFederationAdminAccess</a> — Kebijakan yang diperbarui	Rantai Pasokan AWS memperbarui kebijakan terkelola untuk mengizinkan pengguna federasi mengakses PutObject dan GetObject operasi pada bucket S3 khusus dengan	21 September 2023



Perubahan	Deskripsi	Tanggal
	resource arn arn:aws:s3: ::aws-supply- chain-data-*	
<a href="#">AWSSupplyChainFederationAdminAccess</a> – Kebijakan baru	Rantai Pasokan AWSmenambahkan 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 terkelola AWS	01 Maret, 2023

## Validasi kepatuhan untuk Rantai Pasokan AWS

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

Untuk daftar Layanan AWS yang termasuk dalam cakupan program kepatuhan spesifik, lihat [AWS Layanan dalam Cakupan program Kepatuhan](#) tertentu, lihat . Untuk informasi umum, lihat [Program Kepatuhan AWS](#).

Anda bisa mengunduh laporan audit pihak ketiga 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, serta undang-undang dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- [Panduan Mulai Cepat Keamanan dan Kepatuhan Panduan](#) Kepatuhan — Panduan penerapan ini membahas pertimbangan arsitektur dan memberikan langkah yang harus dilakukan saat

menerapkan AWS lingkungan dasar yang berfokus pada keamanan dan berfokus pada kepatuhan di.

- [Merancang Laporan Resmi Keamanan dan Kepatuhan HIPAA](#) – Laporan resmi ini menjelaskan cara perusahaan dapat menggunakan AWS untuk membuat aplikasi yang patuh-HIPAA.
- [Sumber Daya Kepatuhan AWS](#) – Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- [Mengevaluasi Sumber Daya dengan Aturan](#) dalam Panduan AWS Config Developer — Panduan ini menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- [AWS Security Hub](#)— Ini Layanan AWS memberikan tampilan komprehensif tentang status keamanan Anda dalam AWS untuk membantu Anda memeriksa kepatuhan Anda terhadap standar dan praktik terbaik industri yang terkait dengan keamanan.

## Ketahanan di Rantai Pasokan AWS

Infrastruktur AWS global dibangun di sekitar Wilayah AWS dan Availability Zone. Wilayah AWS menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi. Ini terhubung dengan jaringan yang memiliki latensi rendah, throughput tinggi, dan sangat berlebihan. Dengan Zona Ketersediaan, Anda dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis melakukan fail over di antara zona tanpa gangguan. Availability Zone memiliki ketersediaan yang lebih baik, toleran terhadap kegagalan, dan dapat diukur skalanya jika dibandingkan dengan satu atau beberapa infrastruktur pusat data tradisional.

Untuk informasi selengkapnya tentang Wilayah AWS dan Availability Zone, lihat [Infrastruktur Global AWS](#).

Selain infrastruktur global AWS, Rantai Pasokan AWS menawarkan beberapa fitur untuk membantu mendukung ketahanan data dan kebutuhan backup 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**

API yang 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](https://scn.amazonaws.com). Untuk informasi selengkapnya, silakan 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, lihat [Peran izin pengguna](#).

## Rantai Pasokan AWS 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 `readOnlyeventName`, dan `resources.ARN` bidang.
- Untuk mencatat peristiwa data menggunakan AWS CLI, konfigurasi `--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-selectors](#) perintah. 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-store](#) perintah untuk membuat penyimpanan data peristiwa baru untuk mencatat peristiwa data, atau jalankan [update-event-data-store](#) perintah untuk memperbarui penyimpanan data peristiwa 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 lebih lanjut 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 API aplikasi web

API yang tercantum dalam bagian ini dipanggil oleh Rantai Pasokan AWS aplikasi atas nama pengguna federasi. API ini tidak terlihat di CloudTrail log dan tidak ditangkap dalam dokumen Referensi Otorisasi Layanan, lihat [Rantai Pasokan AWS](#). Akses ke API ini dikendalikan oleh Rantai Pasokan AWS aplikasi berdasarkan izin peran pengguna federasi. Anda tidak boleh mencoba mengontrol akses ke API ini untuk mencegah ketidaksihonestan aplikasi. Rantai Pasokan AWS

### Peran pengguna

API berikut 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

API berikut digunakan untuk membuat dan mengelola aliran data dan koneksi di data lake.

```
scn:CreateConnection
scn:CreateDataflow
scn:CreateDeleteDataByPartitionJob
scn:CreateExtractFlows
scn:CreatePresignedUrl
scn:CreateSampleParsingJob
scn:CreateSap0DataConnection
scn:CreateUpdateDatasetSchemaJob
scn>DeleteConnection
scn>DeleteDataflow
scn>DeleteExtractFlows
scn>DeleteSap0DataConnection
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

API berikut 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

API berikut 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

API berikut 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
```


## Kuota untuk Rantai Pasokan AWS

Anda Akun AWS memiliki kuota default, sebelumnya disebut sebagai batas, untuk masing-masing Layanan AWS Kecuali dinyatakan sebaliknya, setiap kuota unik untuk suatu 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 penambahan kuota, lihat [Meminta Penambahan Kuota](#) dalam Panduan Pengguna Kuota Layanan. 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	10	Tidak
<div style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; background-color: #e6f2ff;"> <p> <b>Note</b> Anda dapat membuat hingga 10 instans dalam sebuah AWS akun.</p> </div>		
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

Sumber daya	Default	Dapat disesuaikan
Daftar pantauan wawasan per instans dalam akun AWS	1.000	Ya
Wawasan daftar pantauan per pengguna dalam akun AWS	100	Ya



# Riwayat dokumen untuk Panduan Rantai Pasokan AWS Administrator

Tabel berikut menjelaskan rilis dokumentasi untuk Rantai Pasokan AWS.

Perubahan	Deskripsi	Tanggal
<a href="#">Pembaruan kebijakan KMS</a>	Memperbarui kebijakan KMS agar dapat Rantai Pasokan AWS mengakses AWS KMS kunci Anda.	Maret 18, 2024
<a href="#">PrivateLink dukungan</a>	Anda dapat mengakses Rantai Pasokan AWS menggunakan titik akhir antarmuka (AWS PrivateLink).	Februari 26, 2024
<a href="#">Menambahkan Grup</a>	Pengguna harus menjadi bagian dari grup Pusat Identitas IAM untuk mengakses Rantai Pasokan AWS.	14 November 2023
<a href="#">Kebijakan AWS terkelola yang diperbarui</a>	Rantai Pasokan AWS memperbarui kebijakan terkelola untuk memungkinkan pengguna federasi mengakses ListProfileAssociations operasi di Pusat Identitas IAM.	1 November 2023
<a href="#">Kebijakan AWS terkelola yang diperbarui</a>	Rantai Pasokan AWS memperbarui kebijakan terkelola untuk mengizinkan pengguna federasi mengakses PutObject dan GetObject operasi pada bucket Amazon S3 khusus dengan resource	21 September 2023

arn:aws:s3::aws-supply-chain-data-\*

[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 bantuan dan memperbaiki 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.