Panduan Pengguna

AWS Ground Station

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

AWS Ground Station: Panduan Pengguna

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

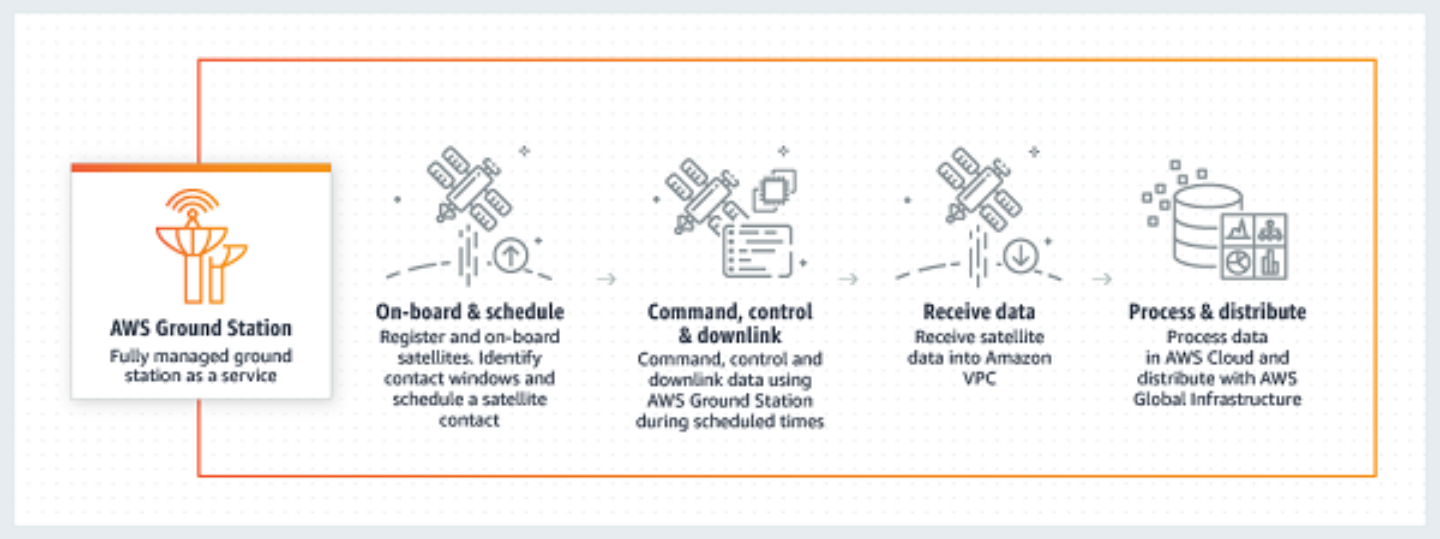
Merek dagang dan tampilan dagang Amazon tidak boleh digunakan sehubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan di antara pelanggan, atau dengan cara apa pun yang menghina atau mendiskreditkan Amazon. Semua merek dagang lain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

Table of Contents

Apa Itu AWS Ground Station?

AWS Ground Stationadalah layanan yang dikelola sepenuhnya yang memungkinkan Anda mengontrol komunikasi satelit, memproses data satelit, dan menskalakan operasi satelit Anda. Ini berarti bahwa Anda tidak lagi harus membangun atau mengelola infrastruktur stasiun tanah Anda sendiri.

AWS Ground Stationmemungkinkan Anda untuk fokus pada inovasi dan bereksperimen dengan cepat dengan aplikasi baru yang menelan data satelit dan secara dinamis meningkatkan server dan penggunaan penyimpanan Anda, daripada menghabiskan sumber daya untuk mengoperasikan dan memelihara stasiun darat Anda sendiri.



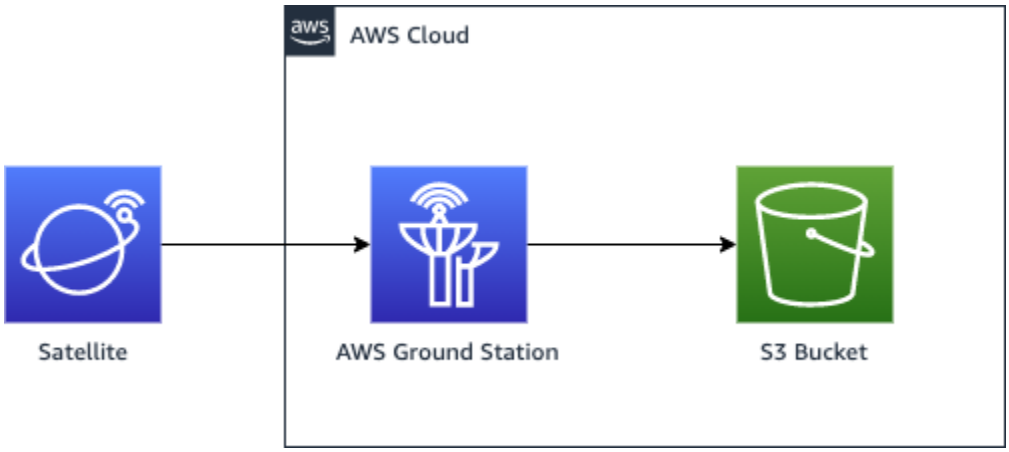
Cara Kerja AWS Ground Station

Reservasi satelit juga dikenal sebagai kontak. Satelit Anda berkomunikasi dengan AWS Ground Station antena selama kontak. Anda dapat memesan kontak melalui API atau melalui AWS konsol dengan menentukan lokasi, waktu, dan informasi misi. Data kontak Anda dapat dialirkan ke dan dari instans Amazon Elastic Compute Cloud (Amazon EC2) atau dikirimkan secara asinkron ke bucket Amazon Simple Storage Service (Amazon S3) di akun Anda.

Anda dapat membuat sumber daya konfigurasi yang dapat diperluas dan dapat digunakan kembali sehingga Anda memiliki kendali atas bagaimana AWS Ground Station antena dikonfigurasi selama kontak Anda. Dengan menggunakan profil misi, Anda dapat menentukan dari mana data berasal, format apa yang seharusnya, dan ke mana mengirimnya.

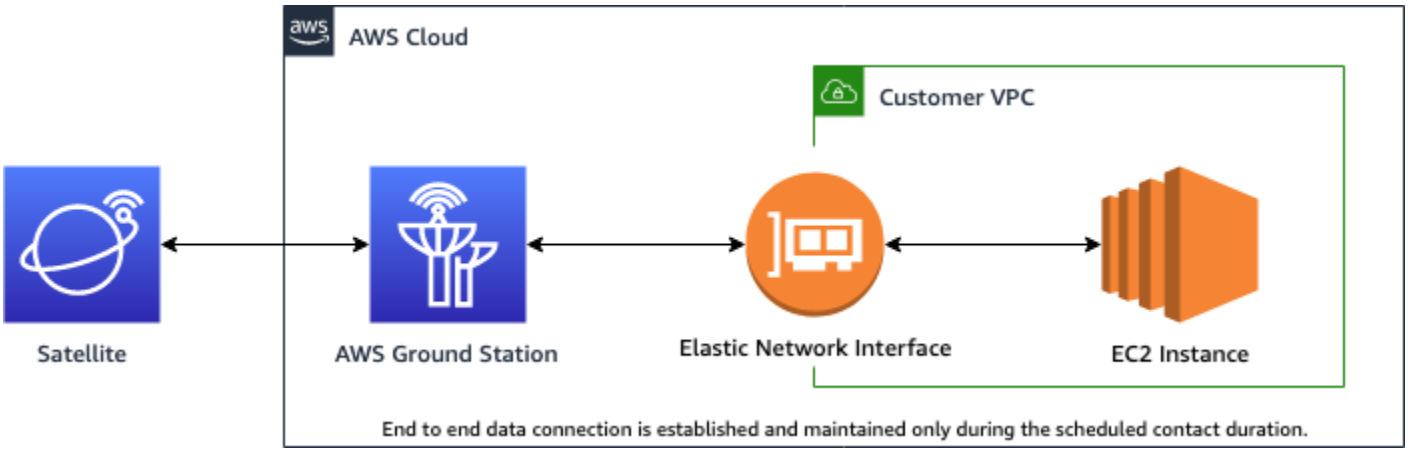
Pengiriman Data ke Amazon S3

Dengan pengiriman data ke Amazon S3, data kontak Anda dikirimkan secara asinkron ke bucket Amazon S3 di akun Anda. Data kontak Anda dikirimkan sebagai file packet capture (pcap) untuk memungkinkan pemutaran ulang data kontak ke Software Defined Radio (SDR) atau untuk mengekstrak data payload dari file pcap untuk diproses. File PCAP dikirim ke bucket Amazon S3 Anda setiap 30 detik karena data kontak diterima oleh perangkat keras antena untuk memungkinkan pemrosesan data kontak selama kontak jika diinginkan. Setelah diterima, Anda dapat memproses data menggunakan perangkat lunak pasca-pemrosesan Anda sendiri atau menggunakan layanan AWS lainnya seperti Amazon SageMaker atau Amazon Rekognition. Pengiriman data ke Amazon S3 hanya tersedia untuk downlink data dari satelit Anda; tidak mungkin untuk menautkan data ke satelit Anda dari Amazon S3.



Pengiriman Data ke Amazon EC2

Dengan pengiriman data ke Amazon EC2, data kontak Anda dialirkan ke dan dari instans Amazon EC2 Anda. Anda dapat memproses data secara real-time di instans Amazon EC2 atau meneruskan data untuk pasca-pemrosesan.



Informasi Selengkapnya

Dengan AWS Ground Station Anda dapat mengakses lebih dari 125 layanan melalui komunikasi satelit. Perhatikan hal berikut:

- Anda dapat menerima data RF pita sempit dalam S-band (2200 hingga 2300 MHz) atau X-band (7750 hingga 8400 MHz) pada bandwidth hingga 54 MHz.
  - Data S-Band RF didigitalkan dan disediakan sebagai aliran digital dalam format VITA-49 Signal Data/IP.
  - Data frekuensi menengah X-Band (IF) didigitalkan dan disediakan sebagai aliran digital dalam format Data Sinyal/IP VITA-49.
- Anda dapat menerima data yang didemodulasi/diterjemahkan pita lebar dalam X-band (7750 hingga 8400 MHz) pada bandwidth hingga 500 MHz
  - Data frekuensi menengah X-Band (IF) didemodulasi, diterjemahkan, dan disediakan sebagai aliran digital dalam format Data Ekstensi/IP VITA-49.
- Anda dapat menerima data wideband Digital Intermediate Frequency (DiGIF) dari 40 MHz hingga 400 MHz bandwidth melalui AWS Ground Station Agen.
  - Lihat AWS Ground Station Panduan Pengguna Agen untuk informasi selengkapnya tentang Pengiriman Data DiGIF AWS Ground Station Agen dan Pita Lebar.

- Anda dapat mengirimkan data RF dalam S-Band (2025 hingga 2120 MHz) pada bandwidth hingga 54 MHz.
  - Data RF disediakan AWS Ground Station sebagai aliran digital dalam format Data Sinyal/IP VITA-49.
- Anda harus lari AWS Ground Station dari AWS Wilayah yang mendukung AWS Ground Station. Untuk melihat daftar wilayah yang didukung, lihat Tabel Wilayah infrastruktur global.
- Anda dapat mengirimkan data ke instans Amazon EC2 yang berjalan di wilayah yang sama dengan antena, atau Anda dapat menggunakan pengiriman data lintas wilayah untuk mengirim data dari antena ke instans Amazon EC2 di Wilayah AWS pilihan Anda. antenna-to-destination Wilayah berikut saat ini tersedia:
  - Wilayah Timur AS (Ohio) (us-timur-2) ke Wilayah AS Barat (Oregon) (us-barat-2)
  - Wilayah AS Barat (Oregon) (us-barat-2) ke Wilayah Timur AS (Ohio) (us-timur-2)

Persyaratan Layanan

Anda hanya dapat menggunakan Layanan untuk menyimpan, mengambil, menanyakan, melayani, dan mengeksekusi Konten Anda yang dimiliki, dilisensikan, atau diperoleh secara sah oleh Anda. Sebagaimana digunakan dalam Ketentuan Layanan ini, (a) “Konten Anda” mencakup “Konten Perusahaan” dan “Konten Pelanggan” apa pun dan (b) “Konten AWS” mencakup “Properti Amazon.” Sebagai bagian dari Layanan, Anda dapat diizinkan untuk menggunakan perangkat lunak tertentu (termasuk dokumentasi terkait) yang disediakan oleh kami atau pemberi lisensi pihak ketiga.

> **Important**
>
> Perangkat lunak ini tidak dijual atau didistribusikan kepada Anda dan Anda dapat menggunakannya semata-mata sebagai bagian dari Layanan. Anda tidak boleh mentransfernya ke luar Layanan tanpa otorisasi khusus untuk melakukannya.

Komponen Inti

Grup titik akhir aliran data, konfigurasi, dan profil misi adalah komponen inti dari. AWS Ground Station Komponen ini menentukan bagaimana Anda menjadwalkan kontak Anda, bagaimana antena berkomunikasi dengan satelit Anda, dan di mana data Anda dikirim. Sebelum memulai AWS Ground Station, kami sarankan Anda mempelajari komponen-komponen ini. Contoh diberikan di bagian masing-masing.

Topik

Grup Titik Akhir Dataflow

Titik akhir Dataflow menentukan lokasi tempat Anda ingin data dialirkan ke atau dari selama kontak. Titik akhir diidentifikasi dengan nama yang Anda pilih saat mengeksekusi kontak. Nama-nama ini tidak harus unik. Hal ini memungkinkan beberapa kontak untuk dieksekusi pada saat yang sama menggunakan profil misi yang sama.

Alamat daftar titik akhir terdiri dari yang berikut:

- `name`- Alamat IP titik akhir aliran data ini.
- `port`- Port untuk terhubung ke.

Detail keamanan titik akhir terdiri dari yang berikut:

- `roleArn`- Nama Sumber Daya Amazon (ARN) dari peran yang AWS Ground Station akan diasumsikan untuk membuat Antarmuka Jaringan Elastis (ENI) di VPC Anda. ENI ini berfungsi sebagai titik masuk dan keluar dari data yang dialirkan selama kontak.
- `securityGroupIds`- Grup keamanan untuk dilampirkan ke antarmuka jaringan elastis.
- `subnetIds`- Daftar subnet AWS Ground Station tempat menempatkan antarmuka jaringan elastis untuk mengirim aliran ke instance Anda.

Peran IAM yang diteruskan `roleArn` harus memiliki kebijakan kepercayaan yang memungkinkan kepala `groundstation.amazonaws.com` layanan untuk mengambil peran tersebut. Lihat bagian Contoh Kebijakan Kepercayaan di bawah ini untuk contoh. Selama pembuatan titik akhir, id sumber daya titik akhir tidak ada, jadi kebijakan kepercayaan harus menggunakan tanda bintang (`*`) sebagai pengganti. *`your-endpoint-id`* Ini dapat diperbarui setelah pembuatan untuk menggunakan id sumber daya titik akhir untuk cakupan kebijakan kepercayaan ke grup titik akhir aliran data tertentu.

Peran IAM harus memiliki kebijakan IAM yang memungkinkan AWS Ground Station untuk mengatur ENI. Lihat bagian Kebijakan Peran Contoh di bawah ini untuk contoh.

Contoh Kebijakan Kepercayaan

Untuk informasi selengkapnya tentang cara memperbarui kebijakan kepercayaan peran, lihat Mengelola peran IAM di Panduan Pengguna IAM.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "groundstation.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "your-account-id"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:groundstation:dataflow-endpoint-region:your-account-id:dataflow-endpoint-group/your-endpoint-id"
        }
      }
    }
  ]
}
```

Contoh Kebijakan Peran

Untuk informasi selengkapnya tentang cara memperbarui atau melampirkan kebijakan peran, lihat Mengelola kebijakan IAM di Panduan Pengguna IAM.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
```

```
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups"
      ]
    }
  ]
}
```

Titik akhir aliran data selalu dibuat sebagai bagian dari grup endpoint aliran data. Dengan menyertakan beberapa titik akhir aliran data dalam grup, Anda menegaskan bahwa titik akhir yang ditentukan semuanya dapat digunakan bersama selama satu kontak. Misalnya, jika kontak perlu mengirim data ke tiga titik akhir aliran data terpisah, Anda harus memiliki tiga titik akhir dalam satu grup titik akhir aliran data yang cocok dengan konfigurasi titik akhir aliran data di profil misi Anda.

Ketika satu atau beberapa sumber daya dalam grup titik akhir aliran data digunakan untuk kontak, seluruh grup dicadangkan selama durasi kontak tersebut. Anda dapat mengeksekusi beberapa kontak secara bersamaan, tetapi kontak tersebut harus dieksekusi pada grup endpoint aliran data yang berbeda.

Grup titik akhir aliran data harus dalam `HEALTHY` keadaan untuk menjadwalkan kontak yang menggunakannya. Di bawah ini adalah alasan grup titik akhir aliran data Anda mungkin tidak dalam `HEALTHY` keadaan serta tindakan korektif yang tepat untuk diambil.

- `NO_REGISTERED_AGENT`- Mulai instans EC2 Anda, yang akan mendaftarkan agen. Perhatikan bahwa Anda harus memiliki file konfigurasi pengontrol yang valid agar panggilan ini berhasil. Lihat AWS Ground Station Panduan Pengguna Agen untuk detail tentang mengonfigurasi file itu.
- `INVALID_IP_OWNERSHIP`- Gunakan DeleteDataflowEndpointGroup API untuk menghapus Dataflow Endpoint Group, lalu gunakan CreateDataflowEndpointGroup API untuk membuat ulang Dataflow Endpoint Group menggunakan alamat IP dan port yang terkait dengan instans EC2.
- `UNVERIFIED_IP_OWNERSHIP`- Alamat IP belum divalidasi. Validasi terjadi secara berkala sehingga ini harus diselesaikan sendiri.
- `NOT_AUTHORIZED_TO_CREATE_SLR`- Akun tidak berwenang untuk membuat Peran Tertaut Layanan yang diperlukan. Periksa langkah-langkah pemecahan masalah di Menggunakan peran terkait layanan untuk Ground Station

Lihat dokumentasi berikut untuk informasi selengkapnya tentang cara melakukan operasi pada grup endpoint aliran data yang menggunakan AWS CloudFormation, API AWS Command Line Interface, atau API. AWS Ground Station

- AWS::GroundStation::DataflowEndpointJenis CloudFormation sumber daya grup
- Referensi Grup Titik Akhir Dataflow AWS CLI
- Referensi API Grup Titik Akhir Dataflow

Konfigurasi

Konfigurasi adalah sumber daya yang AWS Ground Station digunakan untuk menentukan parameter untuk setiap aspek kontak Anda. Tambahkan konfigurasi yang Anda inginkan ke profil misi, dan kemudian profil misi itu akan digunakan saat menjalankan kontak. Anda dapat menentukan beberapa jenis konfigurasi yang berbeda.

Lihat dokumentasi berikut untuk informasi selengkapnya tentang cara melakukan operasi pada konfigurasi menggunakan AWS CloudFormation, API AWS Command Line Interface, atau AWS Ground Station API. Tautan ke dokumentasi untuk jenis konfigurasi tertentu juga disediakan di bawah ini.

- AWS::GroundStation::Config CloudFormation jenis sumber daya
- Referensi Config AWS CLI
- Referensi API Config

Konfigurasi Titik Akhir Dataflow

> **Note**
>
> Konfigurasi titik akhir aliran data hanya digunakan untuk pengiriman data ke Amazon EC2 dan tidak digunakan untuk pengiriman data ke Amazon S3.

Anda dapat menggunakan konfigurasi titik akhir aliran data untuk menentukan titik akhir aliran data mana dalam grup titik akhir aliran data dari mana atau ke mana Anda ingin data mengalir selama kontak. Dua parameter konfigurasi titik akhir aliran data menentukan nama dan wilayah titik akhir aliran data. Saat memesan kontak, AWS Ground Station analisis profil misi yang Anda tentukan dan

coba temukan grup titik akhir aliran data yang berisi semua titik akhir aliran data yang ditentukan oleh konfigurasi titik akhir aliran data yang terdapat dalam profil misi Anda.

`dataflowEndpointName`Properti konfigurasi titik akhir aliran data menentukan titik akhir aliran data mana dalam grup titik akhir aliran data ke mana atau dari mana data akan mengalir selama kontak.

`dataflowEndpointRegion`Properti menentukan wilayah mana titik akhir aliran data berada. Jika wilayah ditentukan dalam konfigurasi titik akhir aliran data Anda, AWS Ground Station cari titik akhir aliran data di wilayah yang ditentukan. Jika tidak ada wilayah yang ditentukan, AWS Ground Station akan default ke wilayah stasiun bumi kontak. Kontak dianggap sebagai kontak pengiriman data lintas wilayah jika wilayah titik akhir aliran data Anda tidak sama dengan wilayah stasiun darat kontak.

Lihat dokumentasi berikut untuk informasi selengkapnya tentang cara melakukan operasi pada konfigurasi titik akhir aliran data menggunakan AWS CloudFormation,, atau API AWS Command Line Interface. AWS Ground Station

- AWS::GroundStation::Config DataflowEndpointConfig CloudFormation properti
- AWS CLI Referensi Config (lihat bagian`dataflowEndpointConfig -> (structure)`)
- DataflowEndpointConfig Referensi API

Config Perekaman S3

> **Note**
>
> Konfigurasi perekaman S3 hanya digunakan untuk pengiriman data ke Amazon S3 dan tidak digunakan untuk pengiriman data ke Amazon EC2.

Anda dapat menggunakan konfigurasi perekaman S3 untuk menentukan bucket Amazon S3 yang ingin dikirimkan data yang ditautkan ke bawah. Dua parameter konfigurasi perekaman S3 menentukan bucket Amazon S3 dan peran IAM AWS Ground Station untuk diasumsikan saat mengirimkan data ke bucket Amazon S3 Anda. Peran IAM dan bucket Amazon S3 yang ditentukan harus memenuhi kriteria berikut:

- Nama bucket Amazon S3 harus dimulai dengan. `aws-groundstation`
- Peran IAM harus memiliki kebijakan kepercayaan yang memungkinkan kepala `groundstation.amazonaws.com` layanan untuk mengambil peran tersebut. Lihat bagian Contoh Kebijakan Kepercayaan di bawah ini untuk contoh. Selama pembuatan konfigurasi, id

sumber daya konfigurasi tidak ada, kebijakan kepercayaan harus menggunakan tanda bintang (*) sebagai pengganti *your-config-id*dan dapat diperbarui setelah dibuat dengan id sumber daya konfigurasi.

- Peran IAM harus memiliki kebijakan IAM yang memungkinkan peran untuk melakukan `s3:GetBucketLocation` tindakan pada bucket dan `s3:PutObject` tindakan pada objek bucket. Jika bucket Amazon S3 memiliki kebijakan bucket, kebijakan bucket juga harus mengizinkan peran IAM untuk melakukan tindakan ini. Lihat bagian Kebijakan Peran Contoh di bawah ini untuk contoh.

Contoh Kebijakan Kepercayaan

Untuk informasi selengkapnya tentang cara memperbarui kebijakan kepercayaan peran, lihat Mengelola peran IAM di Panduan Pengguna IAM.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "groundstation.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "your-account-id"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:groundstation:config-region:your-account-id:config/
s3-recording/your-config-id"
        }
      }
    }
  ]
}
```

Contoh Kebijakan Peran

Untuk informasi selengkapnya tentang cara memperbarui atau melampirkan kebijakan peran, lihat Mengelola kebijakan IAM di Panduan Pengguna IAM.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation"
      ],
      "Resource": [
        "arn:aws:s3:::your-bucket-name"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3:::your-bucket-name/*"
      ]
    }
  ]
}
```

Lihat dokumentasi berikut untuk informasi selengkapnya tentang cara melakukan operasi pada konfigurasi perekaman S3 menggunakan AWS CloudFormation, API AWS Command Line Interface, atau API. AWS Ground Station

- AWS::GroundStation::Config Properti S3 RecordingConfig CloudFormation
- AWS CLI Referensi Config (lihat bagian`s3RecordingConfig -> (structure)`)
- Referensi RecordingConfig API S3

Melacak Config

Anda dapat menggunakan konfigurasi pelacakan di profil misi untuk menentukan apakah autotrack harus diaktifkan selama kontak Anda. Konfigurasi ini memiliki satu parameter:`autotrack`. `autotrack`Parameter dapat memiliki nilai-nilai berikut:

- `REQUIRED`- Autotrack diperlukan untuk kontak Anda.
- `PREFERRED`- Autotrack lebih disukai untuk kontak, tetapi kontak masih dapat dieksekusi tanpa autotrack.
- `REMOVED`- Tidak ada autotrack yang harus digunakan untuk kontak Anda.

Lihat dokumentasi berikut untuk informasi selengkapnya tentang cara melakukan operasi pada konfigurasi pelacakan menggunakan AWS CloudFormation, API AWS Command Line Interface, atau AWS Ground Station API.

- AWS::GroundStation::Config TrackingConfig CloudFormation properti
- AWS CLI Referensi Config (lihat bagian`trackingConfig -> (structure)`)
- TrackingConfig Referensi API

Konfigurasi Downlink Antena

Anda dapat menggunakan konfigurasi downlink antena untuk mengonfigurasi antena untuk downlink selama kontak Anda. Mereka terdiri dari konfigurasi spektrum yang menentukan frekuensi, bandwidth, dan polarisasi yang harus digunakan selama kontak downlink Anda. Jika kasus penggunaan downlink Anda memerlukan demodulasi atau decoding, lihat. Antena Downlink Demod Decode Config

Lihat dokumentasi berikut untuk informasi selengkapnya tentang cara melakukan operasi pada konfigurasi downlink antena menggunakan AWS CloudFormation, API AWS Command Line Interface, atau API. AWS Ground Station

- AWS::GroundStation::Config AntennaDownlinkConfig CloudFormation properti
- AWS CLI Referensi Config (lihat bagian`antennaDownlinkConfig -> (structure)`)
- AntennaDownlinkConfig Referensi API

Antena Downlink Demod Decode Config

Konfigurasi decode demod downlink antena adalah jenis konfigurasi yang lebih kompleks dan dapat disesuaikan yang dapat Anda gunakan untuk menjalankan kontak downlink dengan demod atau decode. Jika Anda tertarik untuk mengeksekusi jenis kontak ini, hubungi AWS Ground Station tim. Kami akan membantu Anda menentukan konfigurasi dan profil misi yang tepat untuk kasus penggunaan Anda.

Lihat dokumentasi berikut untuk informasi selengkapnya tentang cara melakukan operasi pada konfigurasi decode demod downlink antena menggunakan AWS CloudFormation, the AWS Command Line Interface, atau API. AWS Ground Station

- AWS::GroundStation::Config AntennaDownlinkDemodDecodeConfig CloudFormation properti
- AWS CLI Referensi Config (lihat bagian`antennaDownlinkDemodDecodeConfig -> (structure)`)
- AntennaDownlinkDemodDecodeConfig Referensi API

Konfigurasi Uplink Antena

Anda dapat menggunakan konfigurasi uplink antena untuk mengonfigurasi antena untuk uplink selama kontak Anda. Mereka terdiri dari konfigurasi spektrum dengan frekuensi, polarisasi, dan target daya radiasi isotropik efektif (EIRP). Untuk informasi tentang cara mengonfigurasi kontak untuk uplink loopback, lihat. Konfigurasi Gema Uplink

Lihat dokumentasi berikut untuk informasi selengkapnya tentang cara melakukan operasi pada konfigurasi uplink antena menggunakan AWS CloudFormation, the AWS Command Line Interface, atau API. AWS Ground Station

- AWS::GroundStation::Config AntennaUplinkConfig CloudFormation properti
- AWS CLI Referensi Config (lihat bagian`antennaUplinkConfig -> (structure)`)
- AntennaUplinkConfig Referensi API

Konfigurasi Gema Uplink

Konfigurasi gema uplink memberi tahu antena cara menjalankan gema uplink. Ini menggemakan sinyal yang dikirim oleh antena kembali ke titik akhir aliran data Anda. Konfigurasi gema uplink berisi ARN dari konfigurasi uplink. Antena menggunakan parameter dari konfigurasi uplink yang ditunjuk oleh ARN saat menjalankan gema uplink.

Lihat dokumentasi berikut untuk informasi selengkapnya tentang cara melakukan operasi pada konfigurasi echo uplink menggunakan AWS CloudFormation, the AWS Command Line Interface, atau API. AWS Ground Station

- AWS::GroundStation::Config UplinkEchoConfig CloudFormation properti
- AWS CLI Referensi Config (lihat bagian`uplinkEchoConfig -> (structure)`)

- UplinkEchoConfig Referensi API

Profil Misi

Profil misi berisi konfigurasi dan parameter untuk bagaimana kontak dijalankan. Ketika Anda memesan kontak atau mencari kontak yang tersedia, Anda menyediakan profil misi yang ingin Anda gunakan. Profil misi menyatukan semua konfigurasi Anda dan menentukan bagaimana antena akan dikonfigurasi dan ke mana data akan pergi selama kontak Anda.

Selain melacak konfigurasi, semua konfigurasi terkandung di `dataflowEdges` bidang profil misi. Tepi aliran data tunggal adalah daftar dua ARN—yang pertama adalah konfigurasi from dan yang kedua adalah konfigurasi to. Dengan menentukan tepi aliran data antara dua konfigurasi, Anda memberi tahu AWS Ground Station dari mana dan ke mana data harus mengalir selama kontak. Konfigurasi pelacakan tidak digunakan sebagai bagian dari tepi aliran data, tetapi ditentukan sebagai bidang terpisah.

`name`Bidang profil misi membantu membedakan antara profil misi yang Anda buat.

Lihat dokumentasi berikut untuk informasi selengkapnya tentang cara melakukan operasi pada profil misi menggunakan AWS CloudFormation, API AWS Command Line Interface, atau AWS Ground Station API.

- AWS::GroundStation::MissionProfile CloudFormation jenis sumber daya
- AWS CLI Referensi Profil Misi
- Referensi API Profil Misi

AWS Ground StationLokasi

Pelanggan dapat mengirimkan dan menerima data menggunakan antena AWS Ground Station di lokasi berikut: AS (Oregon), AS (Ohio), AS (Alaska), Timur Tengah (Bahrain), Eropa (Stockholm), Asia Pasifik (Dubbo), Eropa (Irlandia), Afrika (Cape Town), AS (Hawaii), Asia Pasifik (Seoul), Asia Pasifik (Singapura), dan Amerika Selatan (Punta Ara).

Pelanggan dapat mengirimkan data dan mengonfigurasi kontak mereka dengan konsol AWS Ground Station di wilayah berikut: AS Barat (Oregon), AS Timur (Ohio), Timur Tengah (Bahrain), Eropa (Stockholm), Asia Pasifik (Dubbo), Eropa (Irlandia), Afrika (Cape Town), AS Timur (Virginia N.), Eropa (Frankfurt), Asia Pasifik (Seoul), Asia Pasifik (Singapura), dan Amerika Selatan (São Paulo).

Catatan: Anda hanya dapat membuat sumber daya AWS Ground Station di wilayah yang menjadi tuan rumah konsol AWS Ground Station yang disebutkan dalam paragraf sebelumnya.

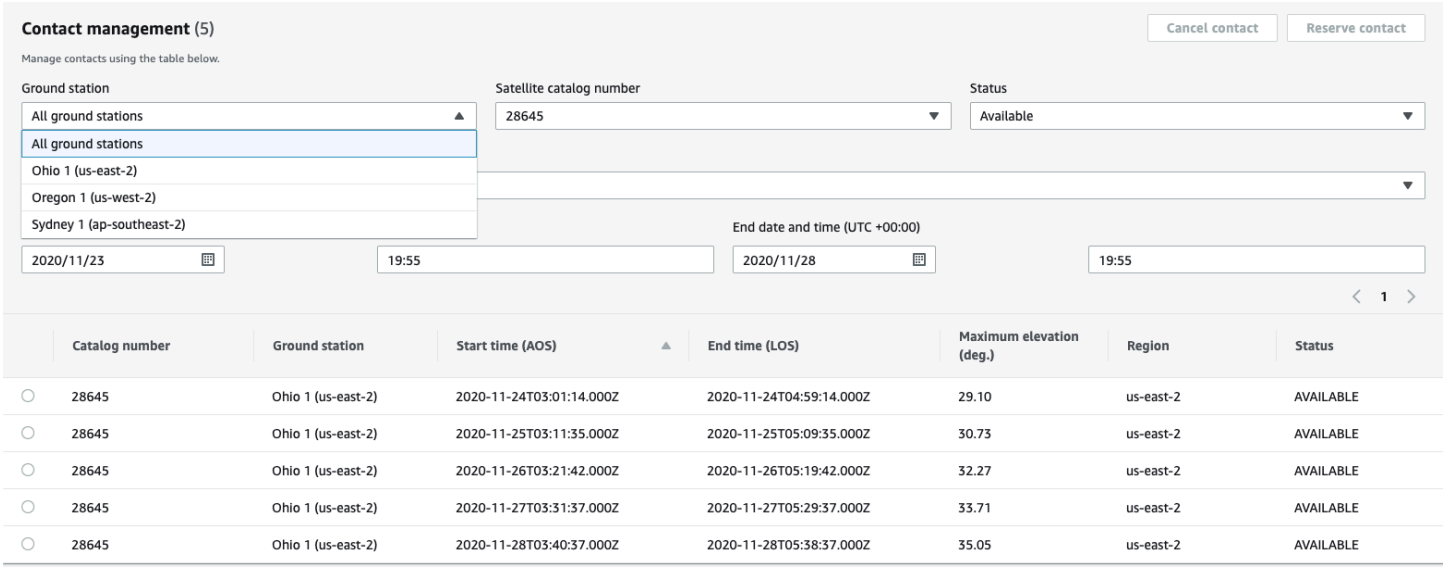
Topik

- Menemukan Wilayah AWS untuk Ground Station

Menemukan Wilayah AWS untuk Ground Station

AWS Global Network mencakup lokasi Ground Station yang tidak secara fisik terletak di Wilayah AWS tempat mereka terhubung. Pencatatan dan pemesanan kontak di salah satu lokasi Ground Station ini harus dilakukan menggunakan Wilayah AWS yang terhubung dengan Ground Station.

Ada beberapa metode untuk menentukan Wilayah AWS Ground Station. Halaman AWS Ground Station konsol menampilkan Wilayah AWS Stasiun Ground saat menampilkannya di filter dan tabel kontak seperti yang ditunjukkan pada gambar di bawah ini. AWS SDK berisi Wilayah AWS Ground Station ListGroundStationsebagai respons. Terakhir, AWS CLI berisi Wilayah AWS Ground Station sebagai respons. list-ground-stations



Topik

- Contoh Ground Station Terletak di Luar Wilayah AWS

Contoh Ground Station Terletak di Luar Wilayah AWS

Hawaii 1 adalah contoh lokasi Ground Station yang tidak secara fisik terletak di Wilayah AWS yang terhubung. Hawaii 1 Ground Station terletak di Hawaii, AS tetapi terhubung ke Wilayah AWS us-barat-2 (Oregon). Untuk membuat daftar dan mencadangkan kontak menggunakan Hawaii 1, Anda harus memiliki profil misi yang dikonfigurasi di Wilayah AWS us-barat-2 (Oregon) dan menggunakan Wilayah AWS us-barat-2 (Oregon) di konsol, AWS CLI, atau AWS Ground Station AWS SDK.

- Untuk membuat daftar dan memesan kontak untuk Hawaii 1 di konsol, Anda harus menggunakan AWS Ground Station AWS Ground Station konsol di wilayah us-barat-2 (Oregon).
- Untuk membuat daftar dan mencadangkan kontak untuk Hawaii 1 menggunakan AWS CLI, Anda harus menentukan wilayah sebagai us-west-2 menggunakan argumen CLI. `--region`
- Untuk membuat daftar dan mencadangkan kontak untuk Hawaii 1 menggunakan AWS SDK, Anda harus menyetel wilayah klien Anda ke us-west-2. Cara Anda mengatur ini tergantung pada bahasa pemrograman yang Anda gunakan. Contoh cara menyetel penggunaan JavaScript ini dijelaskan di AWS SDK untuk JavaScript dokumentasi. Untuk informasi selengkapnya, lihat dokumentasi SDK khusus bahasa.

Menyiapkan AWS Ground Station

Sebelum Anda mulai menggunakan AWS Ground Station, Anda perlu tahu izin apa AWS Identity and Access Management (IAM) yang Anda butuhkan, dan kredenal kendaraan luar angkasa apa yang harus disediakan. Gunakan langkah-langkah berikut untuk mengatur akun Anda.

Topik

Mendaftar untuk Akun AWS

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

Untuk mendaftar untuk Akun AWS

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

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

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

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

Buat pengguna dengan akses administratif

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

Amankan Anda Pengguna root akun AWS

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

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

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

Buat pengguna dengan akses administratif

1. Aktifkan Pusat Identitas IAM.

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

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

Masuk sebagai pengguna dengan akses administratif

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

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

Tetapkan akses ke pengguna tambahan

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

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

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

Tambahkan Izin Ground Station ke Akun Anda AWS

Untuk menggunakan AWS Ground Station tanpa memerlukan pengguna administratif, Anda perlu membuat kebijakan baru dan melampirkannya ke AWS akun Anda.

1. Masuk ke AWS Management Console dan buka konsol IAM.
2. Membuat kebijakan baru. Gunakan langkah-langkah berikut:
   a. Di panel navigasi, pilih Kebijakan, lalu pilih Buat Kebijakan.
   b. Di tab JSON, edit JSON dengan salah satu nilai berikut. Gunakan JSON yang paling sesuai untuk aplikasi Anda.
      - Untuk hak administratif Ground Station, atur Action ke groundstation: * sebagai berikut:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "groundstation:*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

- Untuk hak akses hanya-baca, setel Action ke GroundStation:get*, GroundStation:list*, dan groundStation:Describe* sebagai berikut:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "groundstation:Get*",
        "groundstation:List*",
        "groundstation:Describe*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

- Untuk keamanan tambahan melalui otentikasi multifaktor, atur Action ke groundstation: *, dan Condition/Bool ke aws ::true sebagai berikut: MultiFactorAuthPresent

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "groundstation:*",
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "aws:MultiFactorAuthPresent": true
                }
            }
        }
    ]
}
```

3. Di konsol IAM, lampirkan kebijakan yang Anda buat ke pengguna yang diinginkan.

Untuk informasi selengkapnya tentang pengguna IAM dan melampirkan kebijakan, lihat Panduan Pengguna IAM.

Orientasi Pelanggan

Untuk menyelesaikan pendaftaran AWS Ground Station akun Anda, lihat bagian Satelit dan Sumber Daya di halaman AWS Ground Station konsol untuk detail orientasi. AWS Ground Station Tim akan bekerja dengan Anda untuk membawa satelit Anda ke layanan. Setelah Anda menaiki satelit Anda, satelit akan tersedia untuk digunakan saat mengelola kontak. Petunjuk untuk mengelola kontak disediakan di Daftar dan Pemesanan Kontak.

Orientasi satelit Anda akan memberi Anda akses untuk mengirim dan menerima data ke dan dari satelit. Selain melakukan onboarding satelit Anda sendiri, pelanggan juga dapat menggunakan satelit berikut untuk menurunkan data siaran langsung menggunakan AWS Ground Station:

- Aqua
- SNPP
- JPSS-1/NOAA-20
- Terra

Setelah onboard, satelit ini dapat diakses untuk segera digunakan. AWS Ground Station memelihara sejumlah AWS CloudFormation template yang telah dikonfigurasi untuk membuat memulai dengan layanan lebih mudah. Petunjuk dan detail untuk mengakses dan menggunakan template ini disediakan di bagian Create Your Resources Using a AWS CloudFormation Template pada panduan pengguna.

Untuk informasi lebih lanjut tentang satelit ini dan jenis data yang mereka kirimkan, lihat Aqua, JPSS-1/NOAA-20 dan SNPP, dan Terra.

Langkah Berikutnya

AWS Ground Station Akun Anda sekarang disiapkan dan siap untuk konfigurasi. Lanjutkan Memulai untuk mengkonfigurasi sumber daya Anda untuk digunakan AWS Ground Station.

Memulai dengan AWS Ground Station

AWS Ground Station memungkinkan Anda untuk memerintahkan, mengontrol, dan menurunkan data dari satelit Anda.

Dengan AWS Ground Station, Anda dapat menjadwalkan akses ke antena stasiun bumi per menit dan hanya membayar untuk waktu antena yang digunakan. AWS Ground Station mengirimkan data kontak Anda secara asinkron ke bucket Amazon Simple Storage Service (Amazon S3) di akun Anda atau secara sinkron dengan streaming ke dan dari instans Amazon Elastic Compute Cloud (Amazon EC2) di akun Anda. Langkah-langkah berikut menjelaskan cara mengonfigurasi sumber daya yang diperlukan untuk menerima data kontak secara asinkron di bucket Amazon S3. Lihat Pengiriman Data ke Amazon EC2 panduan untuk informasi tentang cara menggunakan pengiriman data ke Amazon EC2.

Topik

Konsep Basic

Sebelum Anda mulai, Anda harus membiasakan diri dengan konsep dasar di AWS Ground Station. Untuk informasi selengkapnya, lihat Komponen Inti.

Kemudian, lanjutkan Prasyarat untuk belajar tentang prasyarat untuk memulai. AWS Ground Station

Prasyarat

Sebelum memulai AWS Ground Station, pastikan Anda memiliki AWS akun dengan kredensi yang tepat. Ikuti langkah-langkahnya di Menyiapkan AWS Ground Station.

> **Note**
>
> Jika Anda akan menggunakan Wideband DiGIF Data Delivery, lihat instruksi AWS Ground Station Panduan Pengguna Agen untuk.

Jika tidak, lanjutkan keLangkah 1: Pilih AWS CloudFormation Template.

Langkah 1: Pilih AWS CloudFormation Template

Setelah Anda onboard satelit Anda, Anda perlu menentukan profil misi untuk menentukan konfigurasi AWS Ground Station antena untuk menurunkan data dari satelit Anda. Untuk membantu Anda dalam proses ini, kami menyediakan AWS CloudFormation template yang telah dikonfigurasi sebelumnya untuk Narrowband dan Wideband DigiF Data Delivery yang menggunakan satelit siaran publik. Template ini memudahkan Anda untuk mulai menggunakan AWS Ground Station. Untuk informasi selengkapnya AWS CloudFormation, lihat Apa itu AWS CloudFormation?

Bergantung pada jenis kontak yang ingin Anda ambil, pilih jenis templat CFN yang sesuai dari daftar di bawah ini:

- Templat Pengiriman Data Narrowband S3 AWS CloudFormation.
- Template Pengiriman Data Wideband DigIf S3 AWS CloudFormation.

Jika Anda tidak ingin menggunakan salah satu AWS CloudFormation template premade, Anda dapat melihat instruksi diMembangun template Anda sendiri.

Templat Pengiriman Data Narrowband S3 AWS CloudFormation

Template yang telah dikonfigurasi

Hari ini, Anda dapat mengonfigurasi beberapa aliran data per kontak untuk mengalir ke bucket S3. Aliran data ini tersedia dalam dua format berbeda. Aliran data yang berisi data Sinyal/IP VITA-49 dapat dikonfigurasi untuk sinyal S-Band dan X-Band hingga 54 MHz dalam bandwidth. VITA-49 Extension Data/IP dapat dikonfigurasi untuk sinyal X-Band yang didemodulasi dan/atau diterjemahkan hingga 500 MHz dalam bandwidth.

AWS Ground Station menyediakan template untuk kedua format aliran data yang menunjukkan cara menggunakan layanan. Gunakan panduan ini untuk menemukan template yang tepat untuk Anda.

Template yang tersedia

Anda dapat menggunakan template yang telah dikonfigurasi untuk menerima data siaran langsung dari satelit Aqua, SNPP, JPSS-1/NOAA-20, dan Terra. AWS CloudFormationTemplate ini berisi sumber daya Amazon S3 yang diperlukan AWS Ground Station untuk menjadwalkan dan

mengeksekusi kontak dan menerima data dalam bucket Amazon S3 di akun Anda. Jika Aqua, SNPP, JPSS-1/NOAA-20, dan Terra tidak terhubung ke akun Anda, lihat Orientasi Pelanggan.

Templat Pengiriman Data Narrowband

Jika Anda menggunakan pengiriman data narrowband untuk kontak Anda, gunakan AWS CloudFormation templat di bawah ini.

- AWS CloudFormation Template bernama `AquaSnppJpss-1DemodDecodeS3DataDelivery.yml` berisi bucket Amazon S3 dan AWS Ground Station sumber daya yang diperlukan untuk menjadwalkan kontak dan menerima data siaran langsung yang didemodulasi dan diterjemahkan. Template ini adalah titik awal yang baik jika Anda berencana untuk memproses data menggunakan perangkat lunak NASA Direct Readout Labs (RT-STPS dan IPOPP).

  Untuk mengunduh templat menggunakan AWS CLI, gunakan perintah berikut:

  ```
  aws s3 cp s3://groundstation-cloudformation-templates-us-west-2/
  AquaSnppJpss-1DemodDecodeS3DataDelivery.yml .
  ```

  Anda dapat melihat dan mengunduh templat di konsol dengan menavigasi ke URL berikut di browser Anda:

  ```
  https://s3.console.aws.amazon.com/s3/object/groundstation-cloudformation-templates-
  us-west-2/AquaSnppJpss-1DemodDecodeS3DataDelivery.yml
  ```

  Anda dapat menentukan template secara langsung AWS CloudFormation menggunakan link berikut:

  ```
  https://groundstation-cloudformation-templates-us-west-2.s3.us-west-2.amazonaws.com/
  AquaSnppJpss-1DemodDecodeS3DataDelivery.yml
  ```

- AWS CloudFormation Template bernama `AquaSnppJpss-1TerraDigIfS3DataDelivery.yml` berisi bucket Amazon S3 dan AWS Ground Station sumber daya yang diperlukan untuk menjadwalkan kontak dan menerima data siaran langsung Sinyal/IP VITA-49. Template ini adalah titik awal yang baik jika Anda berencana untuk memproses data menggunakan radio yang ditentukan perangkat lunak (SDR) untuk mendemodulasi dan memecahkan kode data sebelum pasca-pemrosesan.

Untuk mengunduh templat menggunakan AWS CLI, gunakan perintah berikut:

```
aws s3 cp s3://groundstation-cloudformation-templates-us-west-2/
AquaSnppJpss-1TerraDigIfS3DataDelivery.yml .
```

Anda dapat melihat dan mengunduh templat di konsol dengan menavigasi ke URL berikut di browser Anda:

```
https://s3.console.aws.amazon.com/s3/object/groundstation-cloudformation-templates-
us-west-2/AquaSnppJpss-1TerraDigIfS3DataDelivery.yml
```

Anda dapat menentukan template secara langsung AWS CloudFormation menggunakan link berikut:

```
https://groundstation-cloudformation-templates-us-west-2.s3.us-west-2.amazonaws.com/
AquaSnppJpss-1TerraDigIfS3DataDelivery.yml
```

Sumber daya apa yang didefinisikan oleh template ini?

Kedua template berisi sumber daya yang sama, dengan satu-satunya perbedaan adalah konfigurasi antena. Lihat deskripsi Antenna Config di bawah ini untuk informasi lebih lanjut.

- Amazon S3 Bucket - Bucket tempat data downlink akan dikirimkan. Nama bucket ini dimulai dengan `aws-groundstation` memenuhi kriteria yang dijelaskan dalam S3 Recording Config.
- Peran IAM - Peran yang dapat diasumsikan oleh prinsipal `groundstation.amazonaws.com` layanan yang AWS Ground Station diasumsikan saat menulis data downlink ke bucket Amazon S3 Anda.
- Kebijakan Bucket Amazon S3 - Kebijakan yang memungkinkan Peran IAM melakukan tindakan berikut pada bucket Amazon S3 dan objeknya:
  - `s3:GetBucketLocation`
  - `s3:PutObject`
- Tracking Config - Konfigurasi AWS Ground Station pelacakan yang menentukan bagaimana sistem antena melacak satelit Anda saat bergerak melintasi langit.

- S3 Recording Config - Konfigurasi perekaman S3 AWS Ground Station yang mereferensikan bucket Amazon S3 dan peran AWS Ground Station IAM untuk digunakan saat mengirimkan data Anda.
- Antenna Config - Konfigurasi AWS Ground Station antena yang menentukan cara mengkonfigurasi AWS Ground Station antena selama kontak. `AquaSnppJpss-1DemodDecodeS3DataDelivery.yml`Template berisi konfigurasi decode demod downlink antena yang mengonfigurasi AWS Ground Station antena untuk mendemodulasi dan memecahkan kode data downlink sebelum mengirimkannya ke bucket Amazon S3 Anda. `AquaSnppJpss-1TerraDigIfS3DataDelivery.yml`Sebagai gantinya berisi konfigurasi downlink antena yang mengonfigurasi AWS Ground Station antena untuk mengirimkan data ke Amazon S3 Anda sebagai paket sinyal/IP VITA-49.
- Profil Misi - Profil AWS Ground Station misi yang mengelompokkan semua AWS Ground Station konfigurasi bersama-sama untuk memungkinkan Anda menjadwalkan dan menjalankan kontak menggunakan konfigurasi yang direferensikan.

Template Pengiriman Data Wideband DigIf S3 AWS CloudFormation

Template Pengiriman Data DiGIF Wideband

Jika Anda menggunakan pengiriman data Wideband Digital Intermediate Frequency (DiGIF) untuk kontak Anda, gunakan templat AWS CloudFormation di bawah ini.

- AWS CloudFormation Template bernama `DirectBroadcastSatelliteWbDigIfS3DataDelivery.yml` berisi bucket Amazon S3 dan AWS Ground Station sumber daya yang diperlukan untuk menjadwalkan kontak dan menerima data siaran langsung Sinyal/IP VITA-49 melalui Agen. AWS Ground Station Template ini adalah titik awal yang baik jika Anda berencana untuk memproses data menggunakan radio yang ditentukan perangkat lunak (SDR) untuk mendemodulasi dan memecahkan kode data sebelum pasca-pemrosesan. Untuk informasi lebih lanjut tentang AWS Ground Station Agen, lihatAWS Ground Station Panduan Pengguna Agen.

  Untuk mengunduh templat menggunakan AWS CLI, gunakan perintah berikut:

```
aws s3 cp s3://groundstation-cloudformation-templates-us-west-2/agent/s3_recording/
DirectBroadcastSatelliteWbDigIfS3DataDelivery.yml .
```

Anda dapat melihat dan mengunduh templat di konsol dengan menavigasi ke URL berikut di browser Anda:

```
https://s3.console.aws.amazon.com/s3/object/groundstation-cloudformation-templates-us-west-2/agent/s3_recording/DirectBroadcastSatelliteWbDigIfS3DataDelivery.yml
```

Anda dapat menentukan template secara langsung AWS CloudFormation menggunakan link berikut:

```
https://groundstation-cloudformation-templates-us-west-2.s3.us-west-2.amazonaws.com/agent/s3_recording/DirectBroadcastSatelliteWbDigIfS3DataDelivery.yml
```

Sumber daya apa yang didefinisikan oleh template ini?

- Amazon S3 Bucket - Bucket tempat data downlink akan dikirimkan. Nama bucket ini dimulai dengan `aws-groundstation` memenuhi kriteria yang dijelaskan dalam S3 Recording Config.
- Peran IAM - Peran yang dapat diasumsikan oleh prinsipal `groundstation.amazonaws.com` layanan yang AWS Ground Station diasumsikan saat menulis data downlink ke bucket Amazon S3 Anda.
- Kebijakan Bucket Amazon S3 - Kebijakan yang memungkinkan Peran IAM melakukan tindakan berikut pada bucket Amazon S3 dan objeknya:
  - `s3:GetBucketLocation`
  - `s3:PutObject`
- AWS KMS Key - AWS KMS Kunci yang digunakan untuk mengenkripsi aliran data.
- Peran Kunci Ground Station - Peran IAM yang AWS Ground Station akan mengasumsikan untuk mengakses dan menggunakan AWS KMS Kunci untuk mendekripsi aliran data
- Kebijakan Akses Kunci Ground Station - Kebijakan IAM yang menentukan tindakan AWS Ground Station dapat dilakukan pada Kunci Pengiriman Data
- Tracking Config - Konfigurasi AWS Ground Station pelacakan yang menentukan bagaimana sistem antena melacak satelit Anda saat bergerak melintasi langit.
- S3 Recording Config - Konfigurasi perekaman S3 AWS Ground Station yang mereferensikan bucket Amazon S3 dan peran AWS Ground Station IAM untuk digunakan saat mengirimkan data Anda.

- Konfigurasi Antena untuk Aqua, SNPP, JPSS-1/NOAA-20, dan Terra - Tiga konfigurasi AWS Ground Station antena terpisah yang menentukan cara mengkonfigurasi antena selama kontak dengan Aqua, SNPP, JPSS-1/NOAA-20, dan Terra. AWS Ground Station Template berisi konfigurasi downlink antena yang mengonfigurasi AWS Ground Station antena untuk mengirimkan data ke Amazon S3 Anda sebagai paket sinyal/IP VITA-49.
- Profil Misi untuk Aqua, SNPP, JPSS-1/NOAA-20, dan Terra - Tiga profil AWS Ground Station misi terpisah yang mengelompokkan semua konfigurasi bersama untuk memungkinkan Anda menjadwalkan dan menjalankan kontak menggunakan AWS Ground Station konfigurasi yang direferensikan dengan Aqua, SNPP, JPSS-1/NOAA-20, dan Terra.

Membangun template Anda sendiri

Mengkonfigurasi sumber daya untuk menjadwalkan dan mengeksekusi kontak untuk satelit Anda sendiri mengharuskan Anda mengonfigurasi AWS Ground Station sumber daya di akun agar sesuai dengan pengaturan satelit Anda. Ini sulit dilakukan sendiri. AWS Ground Station Tim ini tersedia untuk membantu Anda mengonfigurasi AWS Ground Station sumber daya di akun Anda untuk downlink dari dan uplink ke satelit Anda. Untuk mengonfigurasi satelit Anda sendiri untuk digunakan AWS Ground Station, hubungi AWS Support.

Langkah 2: Konfigurasikan AWS CloudFormation Stack

Setelah memilih template yang paling sesuai untuk kasus penggunaan Anda, konfigurasikan AWS CloudFormation tumpukan. Sumber daya yang dibuat dalam prosedur ini dikonfigurasi ke wilayah tempat Anda berada saat Anda membuatnya.

1. Di bagian AWS Management Console, pilih Layanan > CloudFormation.
2. Di panel navigasi, pilih Stacks (Tumpukan). Kemudian, pilih Buat tumpukan> Dengan sumber daya baru (standar).
3. Di halaman Create Stack, tentukan template yang Anda pilih the section called “Langkah 1: Pilih AWS CloudFormation Template” dengan melakukan salah satu hal berikut.

    a. Pilih URL Amazon S3 sebagai sumber templat Anda, lalu salin dan tempel URL templat yang ingin Anda gunakan di URL Amazon S3. Lalu, pilih Selanjutnya.

    b. Pilih Unggah file templat sebagai sumber templat Anda dan pilih Pilih File. Unggah template yang Anda unduhthe section called “Langkah 1: Pilih AWS CloudFormation Template”. Lalu, pilih Selanjutnya.

4. Lakukan langkah-langkah berikut di halaman Tentukan detail tumpukan:

    a. Masukkan nama di kotak Nama Tumpukan. Sebaiknya gunakan nama sederhana untuk mengurangi kemungkinan kesalahan di masa depan.

    b. Pilih Berikutnya.

5. Konfigurasikan opsi tumpukan dan opsi lanjutan untuk instans Amazon EC2 Anda.

    a. Tambahkan tag dan izin apa pun di bagian Tag dan Izin.

    b. Buat perubahan apa pun untuk kebijakan Stack, konfigurasi Rollback, opsi Pemberitahuan, dan opsi pembuatan Stack.

    c. Pilih Berikutnya.

6. Setelah meninjau detail tumpukan Anda, pilih pengakuan Kemampuan, dan pilih Buat tumpukan.

AWS Ground Station Panduan Pengguna Agen

Topik

Gambaran Umum

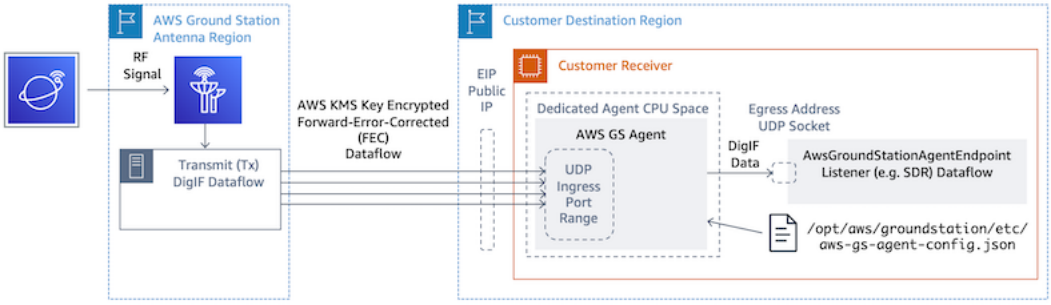
Apa AWS Ground Station agennya?

Agen AWS Ground Station, tersedia sebagai RPM, memungkinkan AWS Ground Station pelanggan menerima aliran data Wideband Digital Intermediate Frequency (DiGIF) sinkron (downlink) selama kontak AWS Ground Station. Pelanggan dapat memilih dua opsi untuk pengiriman data:

1. Pengiriman data ke instans EC2 - Pengiriman data ke instans EC2 milik pelanggan. AWS Ground Station Pelanggan mengelola AWS Ground Station Agen. Opsi ini mungkin paling cocok untuk Anda jika Anda membutuhkan pemrosesan data mendekati waktu nyata. Lihat Pengiriman Data ke Amazon EC2 panduan untuk informasi tentang pengiriman data EC2.
2. Pengiriman data ke bucket S3 - Pengiriman data ke bucket AWS S3 milik pelanggan melalui layanan terkelola Ground Station. Lihat Memulai dengan AWS Ground Station panduan untuk informasi tentang pengiriman data S3.

Kedua mode pengiriman data mengharuskan pelanggan untuk membuat satu set sumber daya AWS. Penggunaan CloudFormation template untuk membuat sumber daya AWS Anda sangat disarankan untuk memastikan keandalan, akurasi, dan dukungan. Setiap kontak hanya dapat mengirimkan data ke EC2 atau S3 tetapi tidak ke keduanya secara bersamaan.

> **Note**
>
> Karena pengiriman data S3 adalah layanan terkelola Ground Station, panduan ini berfokus pada pengiriman data ke instans EC2 Anda.



Aliran data DiGIF dari Wilayah AWS Ground Station Antena ke instans EC2 Anda dengan Software-Defined Radio (SDR) atau pendengar serupa.

Fitur AWS Ground Station Agen

AWS Ground Station Agen menerima data downlink Digital Intermediate Frequency (DiGIF) dan mengeluarkan data yang didekripsi yang memungkinkan hal-hal berikut:

- Kemampuan downlink DiGIF dari 40 MHz hingga 400 MHz bandwidth.
- Pengiriman data DigiF dengan tingkat tinggi dan jitter rendah ke IP publik (AWS Elastic IP) apa pun di jaringan AWS.
- Pengiriman data yang andal menggunakan Forward Error Correction (FEC).
- Mengamankan pengiriman data menggunakan AWS KMS kunci terkelola pelanggan untuk enkripsi.

Persyaratan Agen

> **Note**
>
> Panduan AWS Ground Station Agen ini mengasumsikan bahwa Anda telah onboard ke Ground Station menggunakan panduan ini. Menyiapkan AWS Ground Station

Instans EC2 penerima AWS Ground Station Agen memerlukan satu set sumber daya AWS yang bergantung untuk mengirimkan data DiGIF secara andal dan aman ke titik akhir Anda.

1. VPC untuk meluncurkan penerima EC2.
2. Kunci AWS KMS untuk enkripsi/dekripsi data.
3. Kunci SSH atau Profil Instans EC2 yang dikonfigurasi untuk SSM Session Manager.
4. Aturan Grup Jaringan/Keamanan untuk mengizinkan hal berikut:
    1. Lalu lintas UDP dari AWS Ground Station port yang ditentukan dalam grup endpoint aliran data Anda. Agen mencadangkan berbagai port bersebelahan yang digunakan untuk mengirimkan data ke titik akhir aliran data ingress.
    2. Akses SSH ke instans Anda (Catatan: Anda dapat menggunakan AWS Session Manager untuk mengakses instans EC2 Anda).
    3. Baca akses ke bucket S3 yang dapat diakses publik untuk manajemen agen.
    4. Lalu lintas SSL pada port 443 memungkinkan agen untuk berkomunikasi dengan layanan. AWS Ground Station
    5. Lalu lintas dari daftar `com.amazonaws.global.groundstation` awalan AWS Ground Station terkelola.

Selain itu, konfigurasi VPC termasuk subnet publik diperlukan. Lihat Panduan Pengguna VPC untuk latar belakang konfigurasi subnet.

Konfigurasi yang kompatibel:

1. IP Elastis yang terkait dengan instans EC2 Anda di subnet publik.
2. IP Elastis yang terkait dengan ENI di subnet publik, dilampirkan ke instans EC2 Anda (di subnet apa pun).

Anda dapat menggunakan grup keamanan yang sama dengan instans EC2 Anda atau menentukannya dengan setidaknya seperangkat aturan minimum yang terdiri dari:

- Lalu lintas UDP dari AWS Ground Station port yang ditentukan dalam grup endpoint aliran data Anda.

Lihat bagian Memilih Templat “Template Pengiriman Data DigiF Pita Lebar” AWS CloudFormation misalnya templat Pengiriman Data EC2 dengan sumber daya ini yang telah dikonfigurasi sebelumnya.

Diagram VPC

Diagram: IP Elastis yang terkait dengan instans EC2 Anda di subnet publik

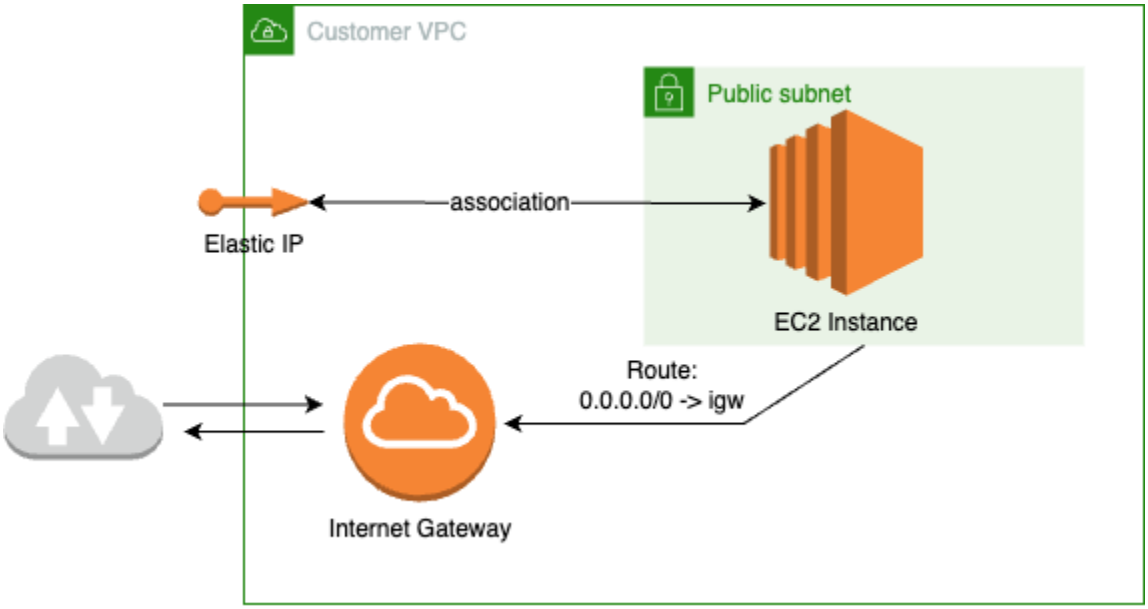
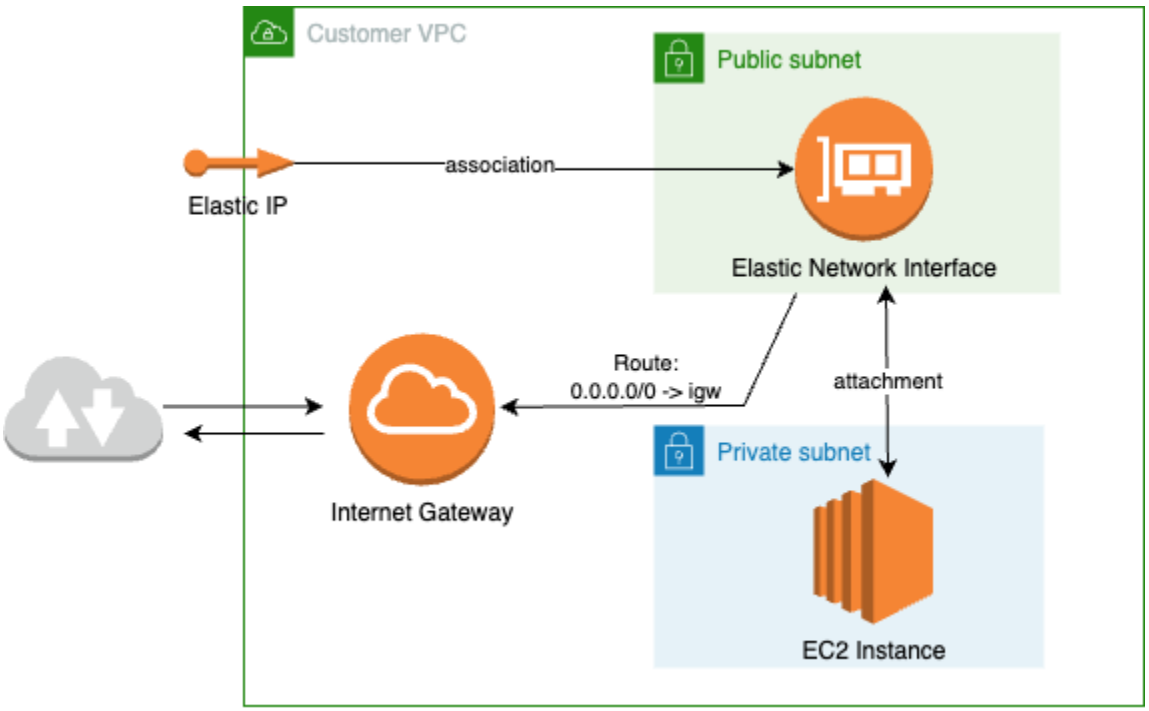


Diagram: IP Elastis yang terkait dengan ENI di subnet publik, dilampirkan ke instans EC2 Anda di subnet pribadi



Sistem operasi yang didukung

Amazon Linux 2 dengan 5.10+ kernel.

Jenis instans yang didukung tercantum dalam Pemilihan Instans EC2 dan Perencanaan CPU

Pengiriman Data melalui AWS Ground Station Agen

Diagram di bawah ini memberikan gambaran umum tentang bagaimana data mengalir AWS Ground Station selama kontak Wideband Digital Intermediate Frequency (DiGIF).

AWS Ground Station Agen akan menangani orkestrasi komponen dataplane untuk kontak. Sebelum menjadwalkan kontak agen harus dikonfigurasi dengan benar, dimulai, dan harus terdaftar (pendaftaran otomatis pada saat agen startup) dengan AWS Ground Station. Selain itu, perangkat lunak penerima data (seperti radio yang ditentukan perangkat lunak) harus berjalan dan dikonfigurasi untuk menerima data di AwsGroundStationAgentEndpointeGressAddress.

Di belakang layar, AWS Ground Station Agen akan menerima tugas dari AWS Ground Station dan membatalkan AWS KMS enkripsi yang diterapkan dalam perjalanan, sebelum meneruskannya ke titik akhir tujuan eGressAddress tempat Software Defined Radio (SDR) Anda mendengarkan. AWS Ground Station Agen dan komponen dasarnya akan menghormati batas CPU yang ditetapkan dalam

file konfigurasi untuk memastikannya tidak memengaruhi kinerja aplikasi lain yang berjalan pada instance.

Pelanggan harus memiliki AWS Ground Station Agen yang berjalan pada instance penerima yang terlibat dalam kontak. AWS Ground Station Agen tunggal dapat mengatur beberapa aliran data, seperti yang terlihat di bawah ini, jika pelanggan lebih suka menerima semua aliran data pada satu instance penerima.

Beberapa Dataflow, Penerima Tunggal

Contoh Skenario:

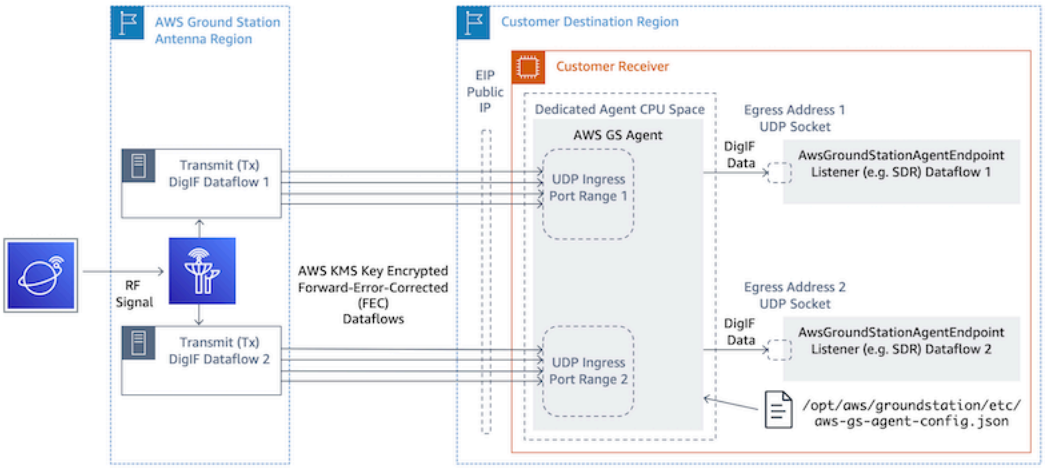
Pelanggan ingin menerima dua downlink antena sebagai aliran data DiGIF pada instance penerima EC2 yang sama. Dua downlink akan menjadi 200MHz dan 100MHz.

AwsGroundStationAgentEndpoints:

Akan ada dua `AwsGroundStationAgentEndpoint` sumber daya, satu untuk setiap aliran data. Kedua titik akhir akan memiliki alamat IP publik yang sama (`ingressAddress.socketAddress.name`). Ingress `portRange` tidak boleh tumpang tindih, karena aliran data diterima pada instance EC2 yang sama. `egressAddress.socketAddress.port`Keduanya harus unik.

Perencanaan CPU:

- 1 core (2 vCPU) untuk menjalankan AWS Ground Station Agen tunggal pada instance.
- 6 core (12 vCPU) untuk menerima DiGIF Dataflow 1 (pencarian 200MHz dalam tabel). Perencanaan Inti CPU
- 4 core (8 vCPU) untuk menerima DiGIF Dataflow 2 (pencarian 100MHz dalam tabel). Perencanaan Inti CPU
- Total Ruang CPU Agen Khusus = 11 core (22 vCPU) pada soket yang sama.



Beberapa Dataflow, Beberapa Penerima

Contoh Skenario:

Pelanggan ingin menerima dua downlink antena sebagai aliran data DiGIF pada instans penerima EC2 yang berbeda. Kedua downlink akan menjadi 400MHz.

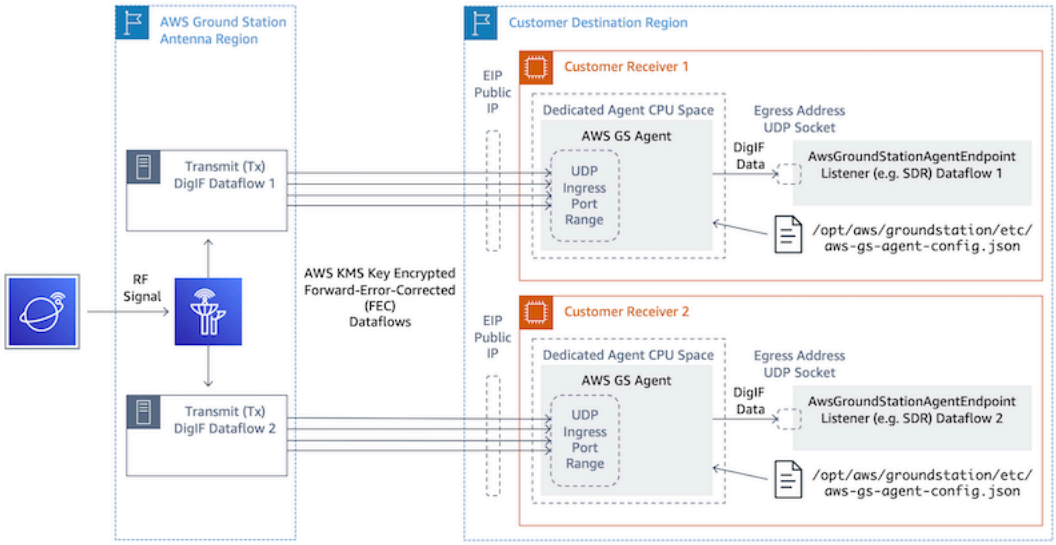
AwsGroundStationAgentEndpoints:

Akan ada dua `AwsGroundStationAgentEndpoint` sumber daya, satu untuk setiap aliran data. Endpoint akan memiliki alamat IP publik yang berbeda (`ingressAddress.socketAddress.name`). Tidak ada batasan pada nilai port untuk salah satu `ingressAddress` atau `egressAddress` karena aliran data diterima pada infrastruktur terpisah dan tidak akan bertentangan satu sama lain.

Perencanaan CPU:

- Instance Penerima 1
  - 1 core (2 vCPU) untuk menjalankan AWS Ground Station Agen tunggal pada instance.
  - 9 core (18 vCPU) untuk menerima DiGIF Dataflow 1 (pencarian 400MHz dalam tabel). Perencanaan Inti CPU
  - Total Dedicated Agent CPU Space = 10 core (20 vCPU) pada soket yang sama.
- Instance Penerima 2
  - 1 core (2 vCPU) untuk menjalankan AWS Ground Station Agen tunggal pada instance.
  - 9 core (18 vCPU) untuk menerima DiGIF Dataflow 2 (pencarian 400MHz dalam tabel). Perencanaan Inti CPU

- Total Dedicated Agent CPU Space = 10 core (20 vCPU) pada soket yang sama.



Pemilihan Instans EC2 dan Perencanaan CPU

Jenis Instans EC2 yang Didukung

AWS Ground Station Agen memerlukan inti CPU khusus untuk beroperasi karena alur kerja pengiriman data intensif komputasi. Kami mendukung jenis contoh berikut. Lihat Perencanaan Inti CPU untuk memutuskan jenis instance mana yang paling sesuai dengan kasus penggunaan Anda.

Jenis instans	vCPU default	Inti CPU default
c5.12xlarge	48	24
c5.18xlarge	72	36
c5.24xlarge	96	48
c5n.18xlarge	72	36
c5n.metal	72	36
c6i.32xlarge	128	64
g4dn.12xlarge	48	24

Jenis instans	vCPU default	Inti CPU default
g4dn.16xlarge	64	32
g4dn.metal	96	48
m4.16xlarge	64	32
m5.12xlarge	48	24
m5.24xlarge	96	48
m6i.32xlarge	128	64
p3dn.24xlarge	96	48
p4d.24xlarge	96	48
r5.24xlarge	96	48
r5.metal	96	48
r5n.24xlarge	96	48
r5n.metal	96	48
r6i.32xlarge	128	64

Perencanaan Inti CPU

AWS Ground Station Agen memerlukan inti prosesor khusus yang berbagi cache L3 untuk setiap aliran data. Agen ini dirancang untuk memanfaatkan pasangan CPU Hyper-threaded (HT) dan mengharuskan pasangan HT dicadangkan untuk penggunaannya. Pasangan hyper-threaded adalah sepasang CPU virtual (vCPU) yang terkandung dalam satu inti. Tabel berikut menyediakan pemetaan laju data aliran data ke jumlah inti yang diperlukan yang disediakan untuk agen untuk aliran data tunggal. Tabel ini mengasumsikan Cascade Lake atau CPU yang lebih baru dan berlaku untuk semua jenis instans yang didukung. Jika bandwidth Anda berada di antara entri dalam tabel, pilih yang tertinggi berikutnya.

Agen membutuhkan inti cadangan tambahan untuk manajemen dan koordinasi, sehingga total inti yang diperlukan adalah jumlah inti yang dibutuhkan (dari bagan di bawah) untuk setiap aliran data ditambah satu inti tambahan (2 vCPU).

AntennaDownlink Bandwidth (MHz)	Kecepatan Data DigiF VITA-49,2 yang diharapkan (MB/s)	Jumlah Core (HT CPU Pairs)	Jumlah vCPU
50	1000	3	6
100	2000	4	8
150	3000	5	10
200	4000	6	12
250	5000	6	12
300	6000	7	14
350	7000	8	16
400	8000	9	18

Mengumpulkan Informasi Arsitektur

`lscpu`memberikan informasi tentang arsitektur sistem Anda. Output dasar menunjukkan vCPU mana (diberi label sebagai “CPU”) milik node NUMA mana (dan setiap node NUMA berbagi cache L3). Di bawah ini kami memeriksa `c5.24xlarge` contoh untuk mengumpulkan informasi yang diperlukan untuk mengkonfigurasi AWS Ground Station Agen. Ini termasuk informasi yang berguna seperti jumlah vCPU, core, dan asosiasi VCPU-ke-Node.

```
> lscpu
Architecture: x86_64
CPU op-mode(s): 32-bit, 64-bit
Byte Order: Little Endian
CPU(s): 96
On-line CPU(s) list: 0-95
Thread(s) per core: 2             <------
```

```
Core(s) per socket: 24
Socket(s): 2
NUMA node(s): 2
Vendor ID: GenuineIntel
CPU family: 6
Model: 85
Model name: Intel(R) Xeon(R) Platinum 8275CL CPU @ 3.00GHz
Stepping: 7
CPU MHz: 3601.704
BogoMIPS: 6000.01
Hypervisor vendor: KVM
Virtualization type: full
L1d cache: 32K
L1i cache: 32K
L2 cache: 1024K
L3 cache: 36608K
NUMA node0 CPU(s): 0-23,48-71     <------
NUMA node1 CPU(s): 24-47,72-95    <------
```

Cores yang didedikasikan untuk AWS Ground Station Agen harus menyertakan kedua vCPU untuk setiap inti yang ditetapkan. Semua core untuk aliran data harus ada pada node NUMA yang sama. `-p`Opsi untuk `lscpu` perintah memberi kita inti ke asosiasi CPU yang diperlukan untuk mengkonfigurasi agen. Bidang yang relevan adalah CPU (yang kami sebut sebagai vCPU), Core, dan L3 (yang menunjukkan cache L3 mana yang dibagikan oleh inti itu). Perhatikan bahwa pada sebagian besar prosesor Intel Node NUMA sama dengan cache L3.

Pertimbangkan subset `lscpu -p` output berikut untuk a `c5.24xlarge` (disingkat dan diformat untuk kejelasan).

```
CPU,Core,Socket,Node,,L1d,L1i,L2,L3
0   0    0      0     0   0   0  0
1   1    0      0     1   1   1  0
2   2    0      0     2   2   2  0
3   3    0      0     3   3   3  0
...
16  0    0      0     0   0   0  0
17  1    0      0     1   1   1  0
18  2    0      0     2   2   2  0
19  3    0      0     3   3   3  0
```

Dari output kita dapat melihat bahwa Core 0 termasuk vCPU 0 dan 16, Core 1 termasuk vCPU 1 dan 17, Core 2 termasuk vCPUs 2 dan 18. Dengan kata lain pasangan hyper-threaded adalah: 0 dan 16, 1 dan 17, 2 dan 18.

Contoh Penugasan CPU

Sebagai contoh, kita akan menggunakan `c5.24xlarge` instance untuk downlink Dual Polarity Wideband pada 350MHz. Dari tabel di Perencanaan Inti CPU kita tahu bahwa downlink 350 MHz membutuhkan 8 core (16 vCPU) untuk aliran data tunggal. Ini berarti bahwa pengaturan polaritas ganda ini menggunakan dua aliran data membutuhkan total 16 core (32 vCPU) ditambah satu inti (2 vCPU) untuk Agen.

Kami tahu `lscpu` output untuk `c5.24xlarge` include `NUMA node0 CPU(s): 0-23,48-71` dan`NUMA node1 CPU(s): 24-47,72-95`. Karena NUMA node0 memiliki lebih dari yang kita butuhkan, kita hanya akan menetapkan dari core: 0-23 dan 48-71.

Pertama, kita akan memilih 8 core untuk setiap aliran data yang berbagi cache L3 atau NUMA Node. Kemudian kita akan mencari vCPU yang sesuai (berlabel “CPU”) di output di. `lscpu -p` Lampiran: `lscpu -p` output (penuh) untuk c5.24xlarge Contoh proses pemilihan inti mungkin terlihat seperti berikut:

- Cadangan core 0-1 untuk OS.
- Aliran 1: pilih core 2-9 yang dipetakan ke vCPU 2-9 dan 50-57.
- Aliran 2: pilih core 10-17 yang dipetakan ke vCPU 10-17 dan 58-65.
- Inti agen: pilih inti 18 yang memetakan ke vCPU 18 dan 66.

Ini menghasilkan vCPU 2-18 dan 51-66 sehingga daftar untuk menyediakan agen adalah. `[2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66]` Anda harus memastikan proses Anda sendiri tidak berjalan pada CPU ini seperti yang dijelaskan dalamMenjalankan Layanan dan Proses Bersama AWS Ground Station Agen.

Perhatikan bahwa inti spesifik yang dipilih dalam contoh ini agak sewenang-wenang. Kumpulan inti lainnya akan berfungsi selama memenuhi persyaratan semua berbagi cache L3 untuk setiap aliran data.

Lampiran: **`lscpu -p`** output (penuh) untuk c5.24xlarge

```
> lscpu -p
# The following is the parsable format, which can be fed to other
# programs. Each different item in every column has an unique ID
# starting from zero.
# CPU,Core,Socket,Node,,L1d,L1i,L2,L3
0,0,0,0,,0,0,0,0
1,1,0,0,,1,1,1,0
2,2,0,0,,2,2,2,0
3,3,0,0,,3,3,3,0
4,4,0,0,,4,4,4,0
5,5,0,0,,5,5,5,0
6,6,0,0,,6,6,6,0
7,7,0,0,,7,7,7,0
8,8,0,0,,8,8,8,0
9,9,0,0,,9,9,9,0
10,10,0,0,,10,10,10,0
11,11,0,0,,11,11,11,0
12,12,0,0,,12,12,12,0
13,13,0,0,,13,13,13,0
14,14,0,0,,14,14,14,0
15,15,0,0,,15,15,15,0
16,16,0,0,,16,16,16,0
17,17,0,0,,17,17,17,0
18,18,0,0,,18,18,18,0
19,19,0,0,,19,19,19,0
20,20,0,0,,20,20,20,0
21,21,0,0,,21,21,21,0
22,22,0,0,,22,22,22,0
23,23,0,0,,23,23,23,0
24,24,1,1,,24,24,24,1
25,25,1,1,,25,25,25,1
26,26,1,1,,26,26,26,1
27,27,1,1,,27,27,27,1
28,28,1,1,,28,28,28,1
29,29,1,1,,29,29,29,1
30,30,1,1,,30,30,30,1
31,31,1,1,,31,31,31,1
32,32,1,1,,32,32,32,1
33,33,1,1,,33,33,33,1
34,34,1,1,,34,34,34,1
```

```
35,35,1,1,,35,35,35,1
36,36,1,1,,36,36,36,1
37,37,1,1,,37,37,37,1
38,38,1,1,,38,38,38,1
39,39,1,1,,39,39,39,1
40,40,1,1,,40,40,40,1
41,41,1,1,,41,41,41,1
42,42,1,1,,42,42,42,1
43,43,1,1,,43,43,43,1
44,44,1,1,,44,44,44,1
45,45,1,1,,45,45,45,1
46,46,1,1,,46,46,46,1
47,47,1,1,,47,47,47,1
48,0,0,0,,0,0,0,0
49,1,0,0,,1,1,1,0
50,2,0,0,,2,2,2,0
51,3,0,0,,3,3,3,0
52,4,0,0,,4,4,4,0
53,5,0,0,,5,5,5,0
54,6,0,0,,6,6,6,0
55,7,0,0,,7,7,7,0
56,8,0,0,,8,8,8,0
57,9,0,0,,9,9,9,0
58,10,0,0,,10,10,10,0
59,11,0,0,,11,11,11,0
60,12,0,0,,12,12,12,0
61,13,0,0,,13,13,13,0
62,14,0,0,,14,14,14,0
63,15,0,0,,15,15,15,0
64,16,0,0,,16,16,16,0
65,17,0,0,,17,17,17,0
66,18,0,0,,18,18,18,0
67,19,0,0,,19,19,19,0
68,20,0,0,,20,20,20,0
69,21,0,0,,21,21,21,0
70,22,0,0,,22,22,22,0
71,23,0,0,,23,23,23,0
72,24,1,1,,24,24,24,1
73,25,1,1,,25,25,25,1
74,26,1,1,,26,26,26,1
75,27,1,1,,27,27,27,1
76,28,1,1,,28,28,28,1
77,29,1,1,,29,29,29,1
78,30,1,1,,30,30,30,1
```

```
79,31,1,1,,31,31,31,1
80,32,1,1,,32,32,32,1
81,33,1,1,,33,33,33,1
82,34,1,1,,34,34,34,1
83,35,1,1,,35,35,35,1
84,36,1,1,,36,36,36,1
85,37,1,1,,37,37,37,1
86,38,1,1,,38,38,38,1
87,39,1,1,,39,39,39,1
88,40,1,1,,40,40,40,1
89,41,1,1,,41,41,41,1
90,42,1,1,,42,42,42,1
91,43,1,1,,43,43,43,1
92,44,1,1,,44,44,44,1
93,45,1,1,,45,45,45,1
94,46,1,1,,46,46,46,1
95,47,1,1,,47,47,47,1
```

Memasang agen

AWS Ground Station Agen dapat diinstal dengan cara-cara berikut:

1. AWS CloudFormation template (disarankan).
2. Instalasi manual di Amazon EC2.

Menggunakan CloudFormation template

CloudFormation Template pengiriman data EC2 membuat sumber daya AWS yang diperlukan untuk mengirimkan data ke instans EC2 Anda. AWS CloudFormation Template ini menggunakan AMI AWS Ground Station terkelola yang memiliki AWS Ground Station Agen yang sudah diinstal sebelumnya. Skrip boot instans EC2 yang dibuat kemudian mengisi file konfigurasi agen dan menerapkan tuning kinerja yang diperlukan (). Penyetelan Kinerja Instans EC2

Langkah 1: Buat AWS Resources

Buat tumpukan sumber daya AWS Anda menggunakan templateTemplat DiGIF Wideband Satelit Siaran Langsung (Pita Lebar).

Langkah 2: Periksa Status Agen

Secara default agen dikonfigurasi dan aktif (dimulai). Untuk memeriksa status agen, Anda dapat terhubung ke instans EC2 (SSH atau SSM Session Manager) dan lihat. AWS Ground Station Status Agen

Instalasi manual pada EC2

Meskipun Ground Station merekomendasikan penggunaan CloudFormation templat untuk menyediakan Sumber Daya AWS Anda, mungkin ada kasus penggunaan di mana templat standar mungkin tidak cukup. Untuk kasus seperti itu kami sarankan Anda menyesuaikan template sesuai dengan kebutuhan Anda. Jika itu masih tidak memenuhi persyaratan Anda, Anda dapat membuat sumber daya AWS secara manual dan menginstal agen.

Langkah 1: Buat AWS Resources

Lihat petunjuk Membuat dan Mengkonfigurasi Sumber Daya Secara Manual untuk menyiapkan sumber daya AWS yang diperlukan untuk kontak secara manual.

AwsGroundStationAgentEndpointSumber daya mendefinisikan titik akhir untuk menerima aliran data DiGIF melalui AWS Ground Station Agen dan sangat penting untuk mengambil kontak yang berhasil. Meskipun dokumentasi API terletak di Referensi API, bagian ini akan membahas secara singkat konsep yang relevan dengan AWS Ground Station Agen.

Titik akhir `ingressAddress` adalah tempat AWS Ground Station Agen akan menerima lalu lintas UDP AWS KMS terenkripsi dari Antena. `socketAddressname`Ini adalah IP publik dari instans EC2 (dari EIP terlampir). `portRange`Harus setidaknya 300 port bersebelahan dalam kisaran yang telah dicadangkan dari penggunaan lain. Lihat Reserve Ingress Ports - Jaringan Dampak untuk instruksi. Port ini harus dikonfigurasi untuk memungkinkan lalu lintas masuknya UDP pada grup keamanan untuk VPC tempat instance penerima berjalan.

Titik akhir `egressAddress` adalah tempat Agen akan menyerahkan aliran data DiGIF kepada pelanggan. Pelanggan harus memiliki aplikasi (misalnya SDR) yang menerima data melalui soket UDP di lokasi ini.

Langkah 2: Buat instans EC2

AMI berikut didukung:

1. AWS Ground Station AMI - `groundstation-al2-gs-agent-ami-*` di mana* adalah tanggal AMI dibangun - dilengkapi dengan agen yang diinstal (disarankan).

2. `amzn2-ami-kernel-5.10-hvm-x86_64-gp2`.

Langkah 3: Unduh dan instal agen

> **Note**
>
> Langkah-langkah di bagian ini harus diselesaikan jika Anda tidak memilih AWS Ground Station Agen AMI pada langkah sebelumnya.

Agen unduhan

AWS Ground Station Agen tersedia dari bucket S3 khusus wilayah dan dapat diunduh ke instans dukungan EC2 menggunakan baris perintah AWS (CLI) dari `s3://groundstation-wb-digif-software-${AWS::Region}/aws-groundstation-agent/latest/amazon_linux_2_x86_64/aws-groundstation-agent.rpm` mana $ {AWS::Region} merujuk ke salah satu AWS Ground Station Console dan Wilayah Pengiriman Data yang didukung.

Contoh: Unduh versi rpm terbaru dari AWS region us-east-2 secara lokal ke folder/tmp.

```
aws s3 --region us-east-2 cp s3://groundstation-wb-digif-software-us-east-2/aws-groundstation-agent/latest/amazon_linux_2_x86_64/aws-groundstation-agent.rpm /tmp
```

Jika Anda perlu mengunduh versi AWS Ground Station Agen tertentu, Anda dapat mengunduhnya dari folder versi tertentu di bucket S3.

Contoh: Unduh versi 1.0.2716.0 rpm dari AWS region us-east-2 secara lokal ke folder /tmp.

```
aws s3 --region us-east-2 cp s3://groundstation-wb-digif-software-us-east-2/aws-groundstation-agent/1.0.2716.0/amazon_linux_2_x86_64/aws-groundstation-agent.rpm /tmp
```

> **Note**
>
> Jika Anda ingin mengonfirmasi bahwa RPM yang Anda unduh telah dijual AWS Ground Station, ikuti instruksi untukValidasi Instalasi RPM.

Instal agen

```
sudo yum install ${MY_RPM_FILE_PATH}

Example: Assumes agent is in the "/tmp" directory
sudo yum install /tmp/aws-groundstation-agent.rpm
```

Langkah 4: Konfigurasikan agen

Setelah menginstal agen, Anda harus memperbarui file konfigurasi agen. Lihat Mengkonfigurasi agen.

Langkah 5: Terapkan Tuning Kinerja

AWS Ground Station Agen AMI: Jika Anda memilih AWS Ground Station Agen AMI pada langkah sebelumnya maka terapkan penyetelan kinerja berikut.

- Tune Hardware Menginterupsi dan Menerima Antrian - Mempengaruhi CPU dan Jaringan
- Reserve Ingress Ports - Jaringan Dampak
- Mulai ulang

AMI lainnya: Jika Anda memilih AMI lain di langkah sebelumnya, terapkan semua penyetelan yang tercantum di bawah Penyetelan Kinerja Instans EC2 dan Reboot instance.

Langkah 6: Kelola agen

Untuk memulai, berhenti dan periksa status agen lihatMengelola agen.

Mengelola agen

AWS Ground Station Agen menyediakan kemampuan berikut untuk mengonfigurasi, memulai, menghentikan, meningkatkan, menurunkan versi, dan menghapus instalan agen menggunakan perkakas perintah Linux bawaan.

Topik

- AWS Ground Station Konfigurasi Agen
- AWS Ground Station Agen Mulai

- AWS Ground Station Agen Berhenti
- AWS Ground Station Peningkatan Agen
- AWS Ground Station Agen Downgrade
- AWS Ground Station Agen Uninstall
- AWS Ground Station Status Agen
- AWS Ground Station Info Agen RPM

AWS Ground Station Konfigurasi Agen

Arahkan ke`/opt/aws/groundstation/etc`, yang harus berisi satu file bernama aws-gs-agent-config .json. Lihat File Konfigurasi Agen

AWS Ground Station Agen Mulai

```
#start
sudo systemctl start aws-groundstation-agent

#check status
systemctl status aws-groundstation-agent
```

Harus menghasilkan output yang menunjukkan agen aktif.

```
aws-groundstation-agent.service - aws-groundstation-agent
Loaded: loaded (/usr/lib/systemd/system/aws-groundstation-agent.service; enabled;
 vendor preset: disabled)
Active: active (running) since Tue 2023-03-14 00:39:08 UTC; 1 day 13h ago
Docs: https://aws.amazon.com/ground-station/
Main PID: 8811 (aws-gs-agent)
CGroup: /system.slice/aws-groundstation-agent.service
##8811 /opt/aws/groundstation/bin/aws-gs-agent production
```

AWS Ground Station Agen Berhenti

```
#stop
sudo systemctl stop aws-groundstation-agent

#check status
systemctl status aws-groundstation-agent
```

Harus menghasilkan output yang menunjukkan agen tidak aktif (berhenti).

```
aws-groundstation-agent.service - aws-groundstation-agent
Loaded: loaded (/usr/lib/systemd/system/aws-groundstation-agent.service; enabled;
 vendor preset: disabled)
Active: inactive (dead) since Thu 2023-03-09 15:35:08 UTC; 6min ago
Docs: https://aws.amazon.com/ground-station/
Process: 84182 ExecStart=/opt/aws/groundstation/bin/launch-aws-gs-agent (code=exited,
 status=0/SUCCESS)
Main PID: 84182 (code=exited, status=0/SUCCESS)
```

AWS Ground Station Peningkatan Agen

1. Unduh versi terbaru agen. Lihat Agen unduhan.
2. Hentikan agennya.

   ```
   #stop
   sudo systemctl stop aws-groundstation-agent

   #confirm inactive (stopped) state
   systemctl status aws-groundstation-agent
   ```

3. Perbarui agen.

   ```
   sudo yum update ${MY_RPM_FILE_PATH}

   # check the new version has been installed correctly by comparing the agent version
    with the starting agent version
   yum info aws-groundstation-agent
   ```

```
# reload the systemd configuration
sudo systemctl daemon-reload

# restart the agent
sudo systemctl restart aws-groundstation-agent

# check agent status
systemctl status aws-groundstation-agent
```

AWS Ground Station Agen Downgrade

1. Unduh versi agen yang Anda butuhkan. Lihat Agen unduhan.
2. Downgrade agen.

```
# get the starting agent version
yum info aws-groundstation-agent

# stop the agent service
sudo systemctl stop aws-groundstation-agent

# downgrade the rpm
sudo yum downgrade ${MY_RPM_FILE_PATH}

# check the new version has been installed correctly by comparing the agent version
 with the starting agent version
yum info aws-groundstation-agent

# reload the systemd configuration
sudo systemctl daemon-reload

# restart the agent
sudo systemctl restart aws-groundstation-agent

# check agent status
systemctl status aws-groundstation-agent
```

AWS Ground Station Agen Uninstall

Menghapus instalan agen akan mengganti nama /opt/aws/groundstation/etc/ .json menjadi aws-gs-agent-config /opt/aws/groundstation/etc/ .json.rpmsave. aws-gs-agent-config Menginstal agen lagi pada instance yang sama lagi akan menulis nilai default aws-gs-agent-config untuk.json dan perlu diperbarui dengan nilai yang benar yang sesuai dengan sumber daya AWS Anda. Lihat File Konfigurasi Agen.

```
sudo yum remove aws-groundstation-agent
```

AWS Ground Station Status Agen

Status agen aktif (agen sedang berjalan) atau tidak aktif (agen dihentikan).

```
systemctl status aws-groundstation-agent
```

Contoh output menunjukkan bahwa agen diinstal, status tidak aktif (berhenti) dan diaktifkan (mulai layanan saat boot).

```
aws-groundstation-agent.service - aws-groundstation-agent
Loaded: loaded (/usr/lib/systemd/system/aws-groundstation-agent.service; enabled;
 vendor preset: disabled)
Active: inactive (dead) since Thu 2023-03-09 15:35:08 UTC; 6min ago
Docs: https://aws.amazon.com/ground-station/
Process: 84182 ExecStart=/opt/aws/groundstation/bin/launch-aws-gs-agent (code=exited,
 status=0/SUCCESS)
Main PID: 84182 (code=exited, status=0/SUCCESS)
```

AWS Ground Station Info Agen RPM

```
yum info aws-groundstation-agent
```

Output adalah sebagai berikut:

> **Note**
>
> “Versi” mungkin berbeda berdasarkan versi terbaru yang diterbitkan agen.

```
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
Installed Packages
Name        : aws-groundstation-agent
Arch        : x86_64
Version     : 1.0.2677.0
Release     : 1
Size        : 51 M
Repo        : installed
Summary     : Client software for AWS Ground Station
URL         : https://aws.amazon.com/ground-station/
License     : Proprietary
Description : This package provides client applications for use with AWS Ground Station
```

Mengkonfigurasi agen

Setelah menginstal agen, Anda harus memperbarui file konfigurasi agen di`/opt/aws/groundstation/etc/aws-gs-agent-config.json`.

File Konfigurasi Agen

Contoh

```
{
  "capabilities": [
    "arn:aws:groundstation:eu-central-1:123456789012:dataflow-endpoint-group/
bb6c19ea-1517-47d3-99fa-3760f078f100"
  ],
  "device": {
  "privateIps": [
    "127.0.0.1"
```

```
  ],
  "publicIps": [
    "1.2.3.4"
  ],
  "agentCpuCores":
 [ 24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,72,73,74,75,76,77,78,79,80,81
}
```

Rincian Lapangan

kemampuan

Kemampuan ditentukan sebagai Nama Sumber Daya Amazon Grup Titik Akhir Dataflow.

Diperlukan: Benar

Format: Array String

- Nilai: kemampuan ARN → String

Contoh:

```
"capabilities": [
    "arn:aws:groundstation:${AWS::Region}:${AWS::AccountId}:dataflow-endpoint-group/
${DataflowEndpointGroupId}"
]
```

pesawat

Bidang ini berisi bidang tambahan yang diperlukan untuk menghitung “perangkat” EC2 saat ini.

Diperlukan: Benar

Format: Objek

Anggota:

- PrivateIP

- PublicIP
- agentCpuCores
- NetworkAdapters

PrivateIP

Bidang ini saat ini tidak digunakan, tetapi disertakan untuk kasus penggunaan di masa mendatang. Jika tidak ada nilai yang disertakan, itu akan default ke [“127.0.0.1”]

Diperlukan: Salah

Format: Array String

- Nilai: Alamat IP → String

Contoh:

```
"privateIps": [
    "127.0.0.1"
],
```

PublicIP

IP elastis (EIP) per kelompok titik akhir aliran data.

Diperlukan: Benar

Format: Array String

- Nilai: Alamat IP → String

Contoh:

```
"publicIps": [
    "9.8.7.6"
],
```

AgentCPUCores

Ini menentukan inti virtual mana yang dicadangkan untuk aws-gs-agent proses tersebut. Lihat persyaratan Perencanaan Inti CPU untuk menetapkan nilai ini dengan tepat.

Diperlukan: Benar

Format: Array Int

- Nilai: Nomor Inti → int

Contoh:

```
"agentCpuCores": [

 24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,72,73,74,75,76,77,78,79,80,81,8
]
```

NetworkAdapters

Ini sesuai dengan adaptor ethernet, atau antarmuka yang terpasang ke ENI, yang akan menerima data.

Diperlukan: Salah

Format: Array String

- Nilai: nama adaptor ethernet (dapat menemukannya dengan menjalankan`ifconfig`)

Contoh:

```
"networkAdapters": [
    "eth0"
]
```

Penyetelan Kinerja Instans EC2

> **Note**
>
> Jika Anda menyediakan sumber daya AWS menggunakan CloudFormation templat, penyetelan ini akan diterapkan secara otomatis. Jika Anda menggunakan AMI atau membuat instans EC2 secara manual, maka penyetelan kinerja ini harus diterapkan untuk mencapai kinerja yang paling andal.

Ingatlah untuk me-reboot instance Anda setelah menerapkan penyetelan apa pun.

Topik

- Tune Hardware Menginterupsi dan Menerima Antrian - Mempengaruhi CPU dan Jaringan
- Penyatuan Interupsi Tune Rx - Jaringan Dampak
- Tune Rx Ring Buffer - Jaringan Dampak
- Tune CPU C-State - Dampak CPU
- Reserve Ingress Ports - Jaringan Dampak
- Mulai ulang

Tune Hardware Menginterupsi dan Menerima Antrian - Mempengaruhi CPU dan Jaringan

Bagian ini mengonfigurasi penggunaan inti CPU systemd, SMP IRQ, Receive Packet Steering (RPS) dan Receive Flow Steering (RFS). Lihat Lampiran: Parameter yang Direkomendasikan untuk Interup/RPS Tune sekumpulan pengaturan yang direkomendasikan berdasarkan jenis instans yang Anda gunakan.

1. Pin systemd memproses jauh dari inti CPU agen.
2. Permintaan interupsi perangkat keras rute jauh dari inti CPU agen.
3. Konfigurasikan RPS untuk mencegah antrian perangkat keras dari kartu antarmuka jaringan tunggal menjadi hambatan dalam lalu lintas jaringan.
4. Konfigurasikan RFS untuk meningkatkan hit rate cache CPU dan dengan demikian mengurangi latensi jaringan.

`set_irq_affinity.sh`Skrip yang disediakan oleh RPM mengkonfigurasi semua hal di atas untuk Anda. Tambahkan ke crontab sehingga diterapkan pada setiap boot:

```
echo "@reboot sudo /opt/aws/groundstation/bin/set_irq_affinity.sh
 '${interrupt_core_list}' '${rps_core_mask}' >> /var/log/user-data.log 2>&1" >>/var/
spool/cron/root
```

- Ganti `interrupt_core_list` dengan core yang dicadangkan untuk kernel dan OS - biasanya yang pertama dan kedua bersama dengan pasangan inti hyper-threaded. Ini seharusnya tidak tumpang tindih dengan inti yang dipilih di atas. (Contoh: '0,1,48,49' untuk instance 96-CPU hyper-threaded).
- `rps_core_mask`adalah bit mask heksadesimal yang menentukan CPU mana yang harus memproses paket masuk, dengan setiap digit mewakili 4 CPU. Itu juga harus dipisahkan koma setiap 8 karakter mulai dari kanan. Disarankan untuk mengizinkan semua CPU dan membiarkan caching menangani penyeimbangan.
  - Untuk melihat daftar parameter yang direkomendasikan untuk setiap jenis instans, lihatLampiran: Parameter yang Direkomendasikan untuk Interup/RPS Tune.
- Contoh untuk instance 96-CPU:

```
echo "@reboot sudo /opt/aws/groundstation/bin/set_irq_affinity.sh '0,1,48,49'
 'ffffffff,ffffffff,ffffffff' >> /var/log/user-data.log 2>&1" >>/var/spool/cron/root
```

Penyatuan Interupsi Tune Rx - Jaringan Dampak

Penggabungan interupsi membantu mencegah banjir sistem host dengan terlalu banyak interupsi dan membantu meningkatkan throughput jaringan. Dengan konfigurasi ini, paket dikumpulkan dan satu interupsi tunggal dihasilkan setiap 128 mikrodetik. Tambahkan ke crontab sehingga diterapkan pada setiap boot:

```
echo "@reboot sudo ethtool -C ${interface} rx-usecs 128 tx-usecs 128 >>/var/log/user-
data.log 2>&1" >>/var/spool/cron/root
```

- Ganti `interface` dengan antarmuka jaringan (adaptor ethernet) yang dikonfigurasi untuk menerima data. Biasanya ini adalah `eth0` antarmuka jaringan default yang ditetapkan untuk instance EC2.

Tune Rx Ring Buffer - Jaringan Dampak

Tingkatkan jumlah entri dering untuk buffer cincin Rx untuk mencegah penurunan paket atau overrun selama koneksi pecah. Tambahkan ke crontab sehingga diatur dengan benar pada setiap boot:

```
echo "@reboot sudo ethtool -G ${interface} rx 16384 >>/var/log/user-data.log 2>&1" >>/
var/spool/cron/root
```

- Ganti `interface` dengan antarmuka jaringan (adaptor ethernet) yang dikonfigurasi untuk menerima data. Biasanya ini adalah `eth0` antarmuka jaringan default yang ditetapkan untuk instance EC2.
- Jika menyiapkan instance c6i.32xlarge, perintah perlu dimodifikasi untuk menyetel buffer ring ke, bukan. `8192` `16384`

Tune CPU C-State - Dampak CPU

Atur CPU C-state untuk mencegah idle yang dapat menyebabkan paket hilang selama dimulainya kontak. Membutuhkan contoh reboot.

```
echo "GRUB_CMDLINE_LINUX_DEFAULT=\"console=tty0 console=ttyS0,115200n8
 net.ifnames=0 biosdevname=0 nvme_core.io_timeout=4294967295 intel_idle.max_cstate=1
 processor.max_cstate=1 max_cstate=1\"" >/etc/default/grub
echo "GRUB_TIMEOUT=0" >>/etc/default/grub
grub2-mkconfig -o /boot/grub2/grub.cfg
```

Reserve Ingress Ports - Jaringan Dampak

Cadangan semua port dalam rentang port alamat ingress Anda `AwsGroundStationAgentEndpoint` untuk mencegah konflik dengan penggunaan kernel. Konflik penggunaan port akan menyebabkan kegagalan kontak dan pengiriman data.

```
echo "net.ipv4.ip_local_reserved_ports=${port_range_min}-${port_range_max}" >> /etc/
sysctl.conf
```

- Contoh:`echo "net.ipv4.ip_local_reserved_ports=42000-43500" >> /etc/sysctl.conf`.

Mulai ulang

Setelah semua penyetelan berhasil diterapkan, reboot instance agar penyetelan diterapkan.

```
sudo reboot
```

Lampiran: Parameter yang Direkomendasikan untuk Interup/RPS Tune

Bagian ini menentukan nilai parameter yang disarankan untuk digunakan di bagian tuning Tune Hardware Interrupts and Receive Queues - Dampak CPU dan Jaringan.

Rangkaian	Tipe Instans	${interrupt_core_list}	${rps_core_mask}
c6i	• c6i.32xlarge	• 0,1,64,65	• ffffffff, ffffffff, ffffffff, ffffffff
c5	• c5.24xlarge • c5.18xlarge • c5.12xlarge	• 0,1,48,49 • 0,1,36,37 • 0,1,24,25	• ffffffff, ffffffff, ffffffff • ff, ffffffff, ffffffff • ffff, ffffffff

Rangkaian	Tipe Instans	${interrupt_core_list}	${rps_core_mask}
c5n	• c5n.metal • c5n.18xlarge	• 0,1,36,37 • 0,1,36,37	• ff, ffffffff, ffffffff • ff, ffffffff, ffffffff
m5	• m5.24xlarge • m5.12xlarge	• 0,1,48,49 • 0,1,24,25	• ffffffff, ffffffff, ffffffff • ffff, ffffffff
r5	• r5.metal • r5.24xlarge	• 0,1,48,49 • 0,1,48,49	• ffffffff, ffffffff, ffffffff • ffffffff, ffffffff, ffffffff
r5n	• r5n.metal • r5n.24xlarge	• 0,1,48,49 • 0,1,48,49	• ffffffff, ffffffff, ffffffff • ffffffff, ffffffff, ffffffff
g4dn	• g4dn.metal • g4dn.16xlarge • g4dn.12xlarge	• 0,1,48,49 • 0,1,32,33 • 0,1,24,25	• ffffffff, ffffffff, ffffffff • ffffffff, ffffffff • ffff, ffffffff

Rangkaian	Tipe Instans	${interrupt_core_list}	${rps_core_mask}
p4d	• p4d.24xlarge	• 0,1,48,49	• ffffffff, ffffffff, ffffffff
p3dn	• p3dn.24xlarge	• 0,1,48,49	• ffffffff, ffffffff, ffffffff

Bersiaplah untuk mengambil kontak DiGIF

1. Tinjau Perencanaan Inti CPU untuk aliran data yang diinginkan, dan berikan daftar inti yang dapat digunakan agen. Lihat Perencanaan Inti CPU.
2. Tinjau file konfigurasi AWS Ground Station Agen. Lihat AWS Ground Station Konfigurasi Agen.
3. Konfirmasikan bahwa penyetelan kinerja yang diperlukan diterapkan. Lihat Penyetelan Kinerja Instans EC2.
4. Konfirmasikan bahwa Anda mengikuti semua praktik terbaik yang disebut. Lihat Praktik terbaik.
5. Konfirmasikan bahwa AWS Ground Station Agen dimulai sebelum waktu mulai kontak yang dijadwalkan melalui:

   ```
   systemctl status aws-groundstation-agent
   ```

6. Konfirmasikan bahwa AWS Ground Station Agen sehat sebelum waktu mulai kontak yang dijadwalkan melalui:

   ```
   aws groundstation get-dataflow-endpoint-group --dataflow-endpoint-group-id
    ${DATAFLOW-ENDPOINT-GROUP-ID} --region ${REGION}
   ```

   Verifikasi `awsGroundStationAgentEndpoint` bahwa Anda AKTIF dan SEHAT. `agentStatus` `auditResults`

Praktik terbaik

Praktik EC2 terbaik

Ikuti praktik terbaik EC2 saat ini dan pastikan ketersediaan penyimpanan data yang memadai.

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-best-practices.html

Penjadwal Linux

Penjadwal Linux dapat memesan ulang paket pada soket UDP jika proses yang sesuai tidak disematkan ke inti tertentu. Setiap thread yang mengirim atau menerima data UDP harus menyematkan dirinya ke inti tertentu selama durasi transmisi data.

AWS Ground Station Daftar Awalan Terkelola

Disarankan untuk menggunakan daftar awalan yang `com.amazonaws.global.groundstation` dikelola AWS saat menentukan aturan jaringan untuk memungkinkan komunikasi dari Antena. Lihat Bekerja dengan Daftar Awalan Terkelola AWS untuk informasi selengkapnya tentang Daftar Awalan Terkelola AWS.

Batasan kontak tunggal

Agen AWS Ground Station mendukung beberapa aliran per kontak, tetapi hanya mendukung satu kontak pada satu waktu. Untuk mencegah masalah penjadwalan, jangan bagikan instance di beberapa grup titik akhir aliran data. Jika konfigurasi agen tunggal dikaitkan dengan beberapa ARN DFEG yang berbeda, itu akan gagal untuk mendaftar.

Menjalankan Layanan dan Proses Bersama AWS Ground Station Agen

Saat meluncurkan layanan dan proses pada Instans EC2 yang sama dengan AWS Ground Station Agen, penting untuk mengikatnya ke vCPU yang tidak digunakan oleh kernel AWS Ground Station Agen dan Linux karena ini dapat menyebabkan kemacetan dan bahkan kehilangan data selama kontak. Konsep pengikatan ke vCPU tertentu ini dikenal sebagai afinitas.

Inti yang harus dihindari:

- `agentCpuCores`dari File Konfigurasi Agen

- `interrupt_core_list`dari[Tune Hardware Menginterupsi dan Menerima Antrian - Mempengaruhi CPU dan Jaringan](#).
  - Nilai default dapat ditemukan dari [Lampiran: Parameter yang Direkomendasikan untuk Interup/RPS Tune](#)

Sebagai contoh menggunakan **`c5.24xlarge`** instance

Jika Anda menentukan

```
"agentCpuCores": [24,25,26,27,72,73,74,75]"
```

dan berlari

```
echo "@reboot sudo /opt/aws/groundstation/bin/set_irq_affinity.sh
'0,1,48,49' 'ffffffff,ffffffff,ffffffff' >> /var/log/user-data.log 2>&1"
>>/var/spool/cron/root
```

kemudian hindari core berikut:

```
0,1,24,25,26,27,48,49,72,73,74,75
```

Layanan Afinitizing (systemd)

Layanan yang baru diluncurkan akan secara otomatis berhubungan dengan yang `interrupt_core_list` disebutkan sebelumnya. Jika kasus penggunaan layanan yang Anda luncurkan memerlukan inti tambahan, atau membutuhkan inti yang kurang padat, ikuti bagian ini.

Periksa afinitas layanan Anda saat ini dikonfigurasi dengan perintah:

```
systemctl show --property CPUAffinity <service name>
```

Jika Anda melihat nilai kosong seperti`CPUAffinity=`, itu berarti kemungkinan akan menggunakan inti default dari perintah di atas `...bin/set_irq_affinity.sh <using the cores here> ...`

Untuk mengganti dan menyetel afinitas tertentu, temukan lokasi file layanan dengan menjalankan:

```
systemctl show -p FragmentPath <service name>
```

Buka dan modifikasi file (menggunakan`vi`,`nano`, dll.) Dan letakkan `CPUAffinity=<core list>` di `[Service]` bagian seperti:

```
[Unit]
...

[Service]
...
CPUAffinity=2,3

[Install]
...
```

Simpan file dan mulai ulang layanan untuk menerapkan afinitas dengan:

```
systemctl daemon-reload
systemctl restart <service name>

# Additionally confirm by re-running
systemctl show --property CPUAffinity <service name>
```

Untuk informasi lebih lanjut kunjungi: Red Hat Enterprise Linux 8 - Mengelola, memantau, dan memperbarui kernel - Bab 27. Mengkonfigurasi kebijakan Afinitas CPU dan NUMA menggunakan systemd.

Proses Affinisiasi (skrip)

Sangat disarankan untuk skrip dan proses yang baru diluncurkan untuk dikaitkan secara manual karena perilaku Linux default akan memungkinkan mereka untuk menggunakan inti apa pun pada mesin.

Untuk menghindari konflik inti untuk setiap proses yang berjalan (seperti python, skrip bash, dll.), Luncurkan proses dengan:

```
taskset -c <core list> <command>
# Example: taskset -c 8 ./bashScript.sh
```

Jika proses sudah berjalan, gunakan perintah sepertipidof,top, atau ps untuk menemukan ID Proses (PID) dari proses tertentu. Dengan PID Anda dapat melihat afinitas saat ini dengan:

```
taskset -p <pid>
```

dan dapat memodifikasinya dengan:

```
taskset -p <core mask> <pid>
# Example: taskset -p c 32392 (which sets it to cores 0xc -> 0b1100 -> cores 2,3)
```

Untuk informasi lebih lanjut tentang taskset lihat taskset - Halaman manual Linux

Pemecahan Masalah

Agen gagal memulai

AWS Ground Station Agen mungkin gagal memulai karena beberapa alasan, tetapi skenario yang paling umum mungkin adalah file konfigurasi agen yang salah konfigurasi. Setelah memulai agen (lihatAWS Ground Station Agen Mulai) Anda mungkin mendapatkan status seperti:

```
#agent is automatically retrying a restart
aws-groundstation-agent.service - aws-groundstation-agent
Loaded: loaded (/usr/lib/systemd/system/aws-groundstation-agent.service; enabled;
 vendor preset: disabled)
Active: activating (auto-restart) (Result: exit-code) since Fri 2023-03-10 01:48:14
 UTC; 23s ago
Docs: https://aws.amazon.com/ground-station/
Process: 43038 ExecStart=/opt/aws/groundstation/bin/launch-aws-gs-agent (code=exited,
 status=101)
Main PID: 43038 (code=exited, status=101)
```

```
#agent has failed to start
aws-groundstation-agent.service - aws-groundstation-agent
Loaded: loaded (/usr/lib/systemd/system/aws-groundstation-agent.service; enabled;
 vendor preset: disabled)
Active: failed (Result: start-limit) since Fri 2023-03-10 01:50:15 UTC; 13s ago
Docs: https://aws.amazon.com/ground-station/
Process: 43095 ExecStart=/opt/aws/groundstation/bin/launch-aws-gs-agent (code=exited,
 status=101)
Main PID: 43095 (code=exited, status=101)
```

Pemecahan Masalah

```
sudo journalctl -u aws-groundstation-agent | grep -i -B 3 -A 3 'Loading Config' | tail
 -6
```

dapat menghasilkan output dari:

```
launch-aws-gs-agent[43095]: Running with options Production(ProductionOptions
 { endpoint: None, region: None })
launch-aws-gs-agent[43095]: Loading Config
launch-aws-gs-agent[43095]: System has 96 logical cores
systemd[1]: aws-groundstation-agent.service: main process exited, code=exited,
 status=101/n/a
systemd[1]: Unit aws-groundstation-agent.service entered failed state.
```

Kegagalan untuk memulai agen setelah “Memuat Config” menunjukkan masalah dengan konfigurasi agen. Lihat File Konfigurasi Agen untuk memverifikasi konfigurasi agen Anda.

AWS Ground Station Log Agen

AWS Ground Station Agen menulis informasi tentang eksekusi kontak, kesalahan, dan status kesehatan untuk mencatat file pada instance yang menjalankan agen. Anda dapat melihat file log dengan menghubungkan secara manual ke sebuah instance.

Anda dapat melihat log agen di lokasi berikut.

```
/var/log/aws/groundstation
```

Tidak Ada Kontak Tersedia

Penjadwalan kontak membutuhkan AWS Ground Station Agen yang sehat. Harap konfirmasikan bahwa AWS Ground Station Agen Anda telah memulai dan bahwa itu sehat dengan menanyakan AWS Ground Station API melalui get-dataflow-endpoint-group:

```
aws groundstation get-dataflow-endpoint-group --dataflow-endpoint-group-id ${DATAFLOW-
ENDPOINT-GROUP-ID} --region ${REGION}
```

Verifikasi `awsGroundStationAgentEndpoint` bahwa Anda AKTIF dan SEHAT. `agentStatus` `auditResults`

Mendapatkan Dukungan

Hubungi tim Ground Station melalui AWS Support.

1. Sediakan `contact_id` untuk setiap kontak yang terkena dampak. AWS Ground Station Tim tidak dapat menyelidiki kontak tertentu tanpa informasi ini.
2. Berikan detail seputar semua langkah pemecahan masalah yang telah diambil.
3. Berikan pesan kesalahan apa pun yang ditemukan saat menjalankan perintah dalam panduan pemecahan masalah kami.

Catatan Rilis Agen

Versi Agen Terbaru

Versi 1.0.3555.0

Tanggal Rilis: 03/27/2024

Tanggal Akhir Support: 08/31/2024

Checksum RPM:

- SHA256: `108f3aceb00e5af549839cd766c56149397e448a6e1e1429c89a9eebb6bc0fc1`
- MD5: `65b72fa507fb0af32651adbb18d2e30f`

Perubahan:

- Tambahkan metrik Agen untuk versi eksekusi yang dipilih selama startup tugas.
- Tambahkan dukungan file konfigurasi untuk menghindari versi yang dapat dieksekusi tertentu saat versi lain tersedia.
- Tambahkan diagnostik jaringan dan perutean.
- Fitur keamanan tambahan.
- Perbaiki masalah di mana beberapa kesalahan pelaporan metrik ditulis ke stdout/journal alih-alih file log.
- Dengan anggun menangani kesalahan soket jaringan yang tidak dapat dijangkau.
- Ukur kehilangan paket dan latensi antara agen sumber dan tujuan.
- Rilis aws-gs-datapipe versi 2.0 untuk mendukung fitur protokol baru dan kemampuan untuk secara transparan meningkatkan kontak ke protokol baru.

Versi Agen Usang

Versi 1.0.2942.0

Tanggal Rilis: 06/26/2023

Tanggal Akhir Support: 31/05/2024

Checksum RPM:

- SHA256: `7d94b642577504308a58bab28f938507f2591d4e1b2c7ea170b77bea97b5a9b6`
- MD5: `661ff2b8f11aba5d657a6586b56e0d8f`

Perubahan:

- Menambahkan log kesalahan saat Agen RPM diperbarui pada disk dan membutuhkan Agen restart agar perubahan diterapkan.

- Menambahkan validasi penyetelan jaringan untuk memastikan langkah-langkah penyetelan panduan pengguna Agen diikuti dan diterapkan dengan benar.
- Perbaiki bug yang menyebabkan peringatan yang salah di log Agen tentang arsip log.
- Peningkatan deteksi kehilangan paket.
- Instalasi Agen yang Diperbarui untuk mencegah penginstalan atau peningkatan RPM jika Agen sudah berjalan.

Versi 1.0.2716.0

Tanggal Rilis: 03/15/2023

Tanggal Akhir Support: 31/05/2024

Checksum RPM:

- SHA256: `cb05b6a77dfcd5c66d81c0072ac550affbcefefc372cc5562ee52fb220844929`
- MD5: `65266490c4013b433ec39ee50008116c`

Perubahan:

- Aktifkan pengunggahan log saat Agen mengalami kegagalan selama penugasan.
- Perbaiki bug kompatibilitas linux dalam skrip penyetelan jaringan yang disediakan.

Versi 1.0.2677.0

Tanggal Rilis: 02/15/2023

Tanggal Akhir Support: 31/05/2024

Checksum RPM:

- SHA256: `77cfe94acb00af7ca637264b17c9b21bd7afdc85b99dffdd627aec9e99397489`
- MD5: `b8533be7644bb4d12ab84de21341adac`

Perubahan:

- Rilis Agen pertama yang tersedia secara umum.

Validasi Instalasi RPM

Versi RPM terbaru, hash MD5 divalidasi dari RPM, dan SHA256 hash menggunakan sha256sum ditunjukkan di bawah ini. Nilai-nilai ini, digabungkan, dapat digunakan untuk memvalidasi versi RPM yang digunakan untuk agen stasiun bumi.

Versi Agen Terbaru

Versi 1.0.3555.0

Tanggal Rilis: 03/27/2024

Tanggal Akhir Support: 08/31/2024

Checksum RPM:

- SHA256: `108f3aceb00e5af549839cd766c56149397e448a6e1e1429c89a9eebb6bc0fc1`
- MD5: `65b72fa507fb0af32651adbb18d2e30f`

Perubahan:

- Tambahkan metrik Agen untuk versi eksekusi yang dipilih selama startup tugas.
- Tambahkan dukungan file konfigurasi untuk menghindari versi yang dapat dieksekusi tertentu saat versi lain tersedia.
- Tambahkan diagnostik jaringan dan perutean.
- Fitur keamanan tambahan.
- Perbaiki masalah di mana beberapa kesalahan pelaporan metrik ditulis ke stdout/journal alih-alih file log.
- Dengan anggun menangani kesalahan soket jaringan yang tidak dapat dijangkau.
- Ukur kehilangan paket dan latensi antara agen sumber dan tujuan.
- Rilis aws-gs-datapipe versi 2.0 untuk mendukung fitur protokol baru dan kemampuan untuk secara transparan meningkatkan kontak ke protokol baru.

Verifikasi RPM

Alat yang Anda perlukan untuk dapat memverifikasi instalasi RPM ini adalah:

- sha256jumlah
- rpm

Kedua alat datang secara default di Amazon Linux 2. Alat-alat ini akan membantu memvalidasi bahwa RPM yang Anda gunakan adalah versi yang benar. Pertama unduh RPM terbaru dari bucket S3 (lihat Agen unduhan petunjuk tentang mengunduh RPM). Setelah file ini diunduh, akan ada beberapa hal yang perlu diperiksa:

- Hitung sha256sum dari file RPM. Lakukan tindakan berikut dari baris perintah instance komputasi yang Anda gunakan:

  ```
  sha256sum aws-groundstation-agent.rpm
  ```

  Ambil nilai ini dan bandingkan dengan tabel di atas. Ini menunjukkan bahwa file RPM yang diunduh adalah file yang valid untuk digunakan yang AWS Ground Station telah dijual kepada pelanggan. Jika hash tidak cocok, jangan instal RPM, dan hapus dari instance komputasi.
- Periksa hash MD5 file juga, untuk memastikan bahwa RPM belum dikompromikan. Untuk melakukan ini, gunakan alat baris perintah RPM dengan menjalankan perintah berikut:

  ```
  rpm -Kv ./aws-groundstation-agent.rpm
  ```

  Validasi bahwa hash MD5 yang tercantum di sini sama dengan hash MD5 dari versi yang ada pada tabel di atas. Setelah kedua hash ini divalidasi terhadap tabel ini yang tercantum dalam AWS Docs, pelanggan dapat dipastikan bahwa RPM yang diunduh dan diinstal adalah versi RPM yang aman dan tanpa kompromi.

Daftar dan Pemesanan Kontak

Anda dapat memasukkan data satelit, mengidentifikasi lokasi antena, berkomunikasi, dan menjadwalkan waktu antena untuk satelit yang dipilih dengan menggunakan konsol atau. AWS Ground Station AWS CLI Anda dapat meninjau, membatalkan, dan menjadwal ulang reservasi kontak hingga delapan hari sebelum waktu yang dijadwalkan. Selain itu, Anda dapat melihat detail paket harga menit cadangan Anda jika Anda menggunakan model harga menit yang AWS Ground Station dipesan.

AWS Ground Station mendukung pengiriman data lintas wilayah. Konfigurasi titik akhir aliran data yang merupakan bagian dari profil misi yang Anda pilih menentukan wilayah mana data dikirimkan. Untuk informasi selengkapnya tentang penggunaan pengiriman data lintas wilayah, lihat Menggunakan Layanan Pengiriman Data Lintas Wilayah.

Untuk menjadwalkan kontak, sumber daya Anda harus dikonfigurasi. Jika Anda belum mengonfigurasi sumber daya, lihat Memulai.

Topik

- Menggunakan Ground Station Console
- Memesan dan Mengelola Kontak dengan AWS CLI

Menggunakan Ground Station Console

Anda dapat menggunakan AWS Ground Station konsol untuk memesan, melihat, dan membatalkan reservasi kontak. Untuk menggunakan AWS Ground Station konsol, buka AWS Ground Station konsol dan pilih Pesan kontak sekarang.

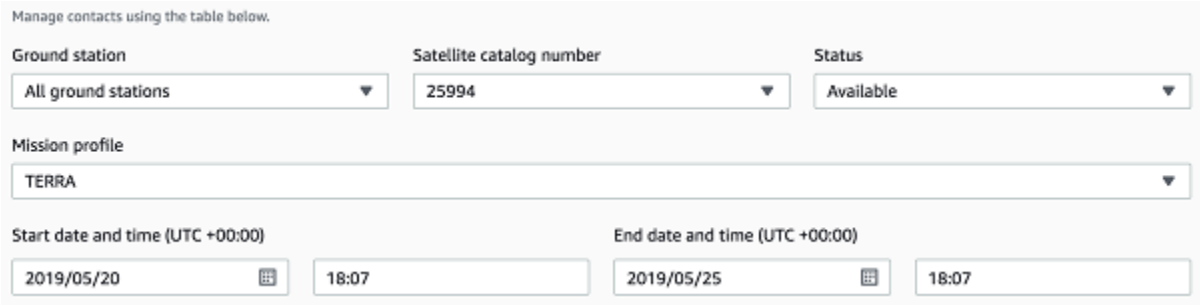
Gunakan topik berikut untuk menggunakan AWS Ground Station konsol untuk memesan, melihat, dan membatalkan kontak.

Topik

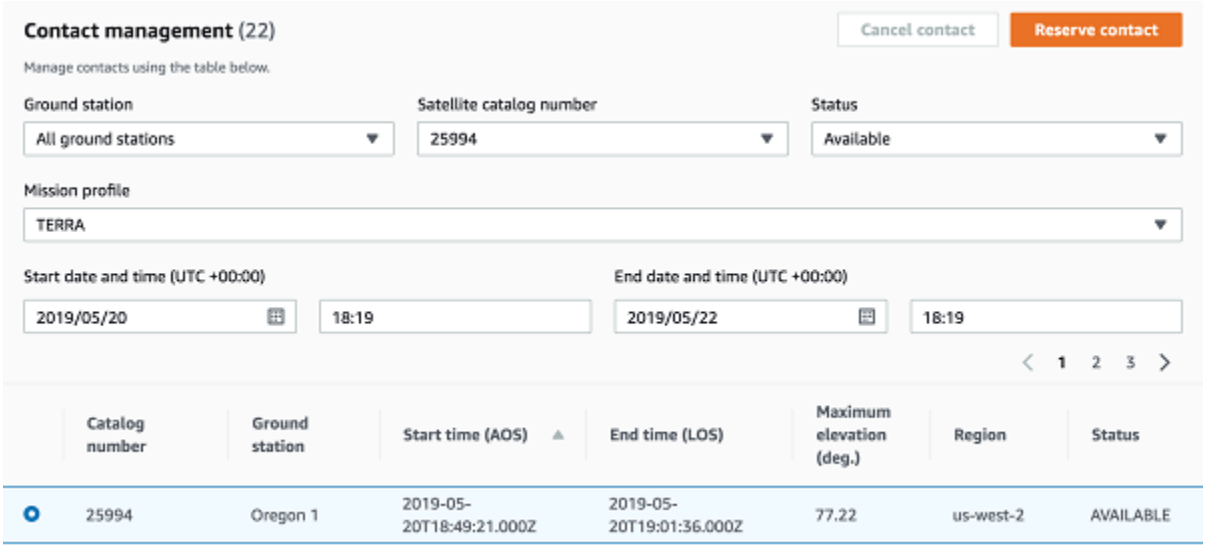
Pesan Kontak

Setelah mengakses AWS Ground Station konsol, gunakan sumber daya yang dikonfigurasi untuk memesan kontak di tabel Manajemen kontak.

1. Dalam tabel Manajemen kontak, pilih parameter yang ingin Anda gunakan untuk mencari kontak yang tersedia. Pastikan Anda melihat kontak yang tersedia dengan menggunakan filter Status.



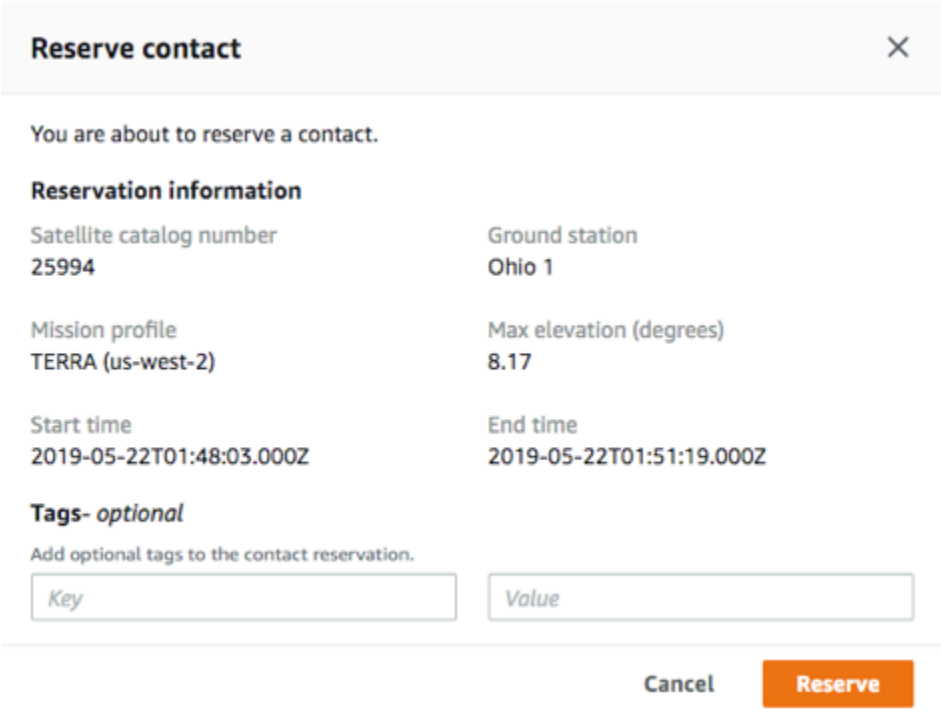
2. Pilih kontak yang memenuhi persyaratan Anda dan kemudian pilih Pesan kontak.



3. Di kotak dialog Kontak Cadangan, tinjau informasi reservasi kontak Anda.

   a. (opsional) Di bawah Tag, masukkan kunci dan nilai untuk setiap tag yang ingin Anda tambahkan.

   b. Pilih Reserve.

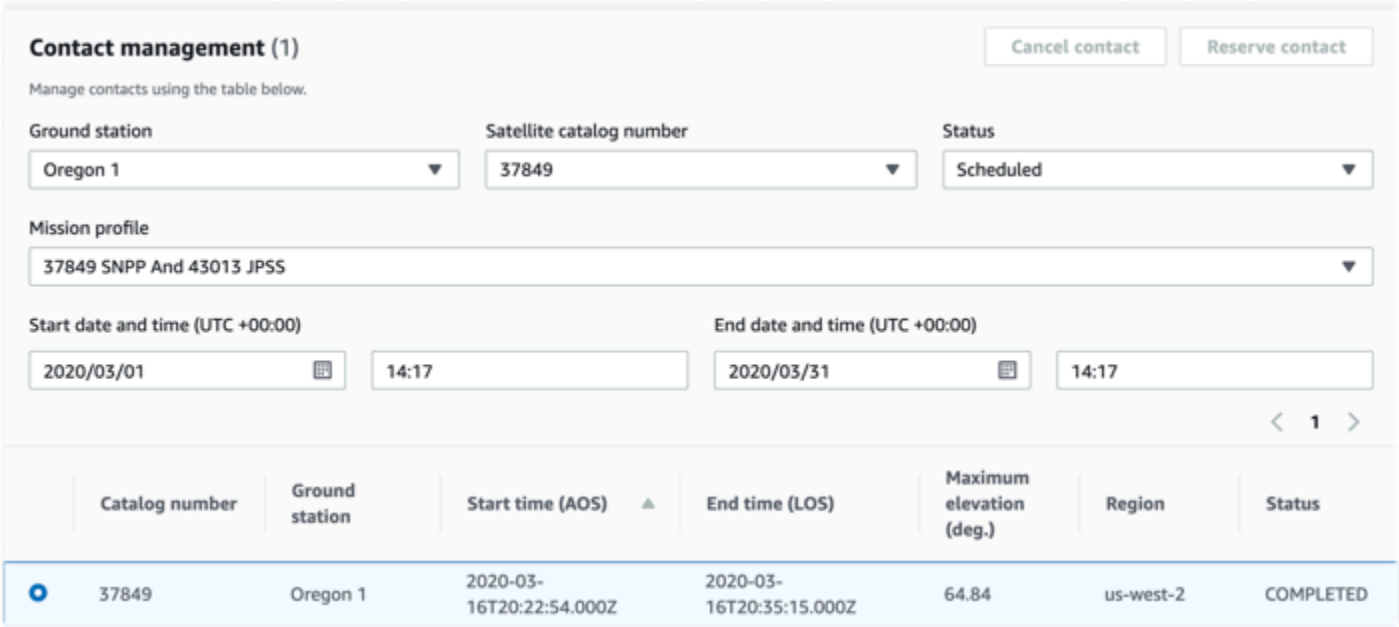


AWS Ground Station akan menggunakan data konfigurasi dari profil misi Anda untuk mengeksekusi kontak di stasiun bumi yang ditentukan.

Lihat Kontak Terjadwal dan Selesai

Setelah menjadwalkan kontak, Anda dapat menggunakan AWS Ground Station konsol untuk melihat detail kontak terjadwal dan selesai.

Dalam tabel Manajemen kontak, pilih parameter yang ingin Anda gunakan untuk mencari kontak terjadwal dan selesai. Pastikan Anda melihat kontak Terjadwal atau Selesai dengan menggunakan filter Status.

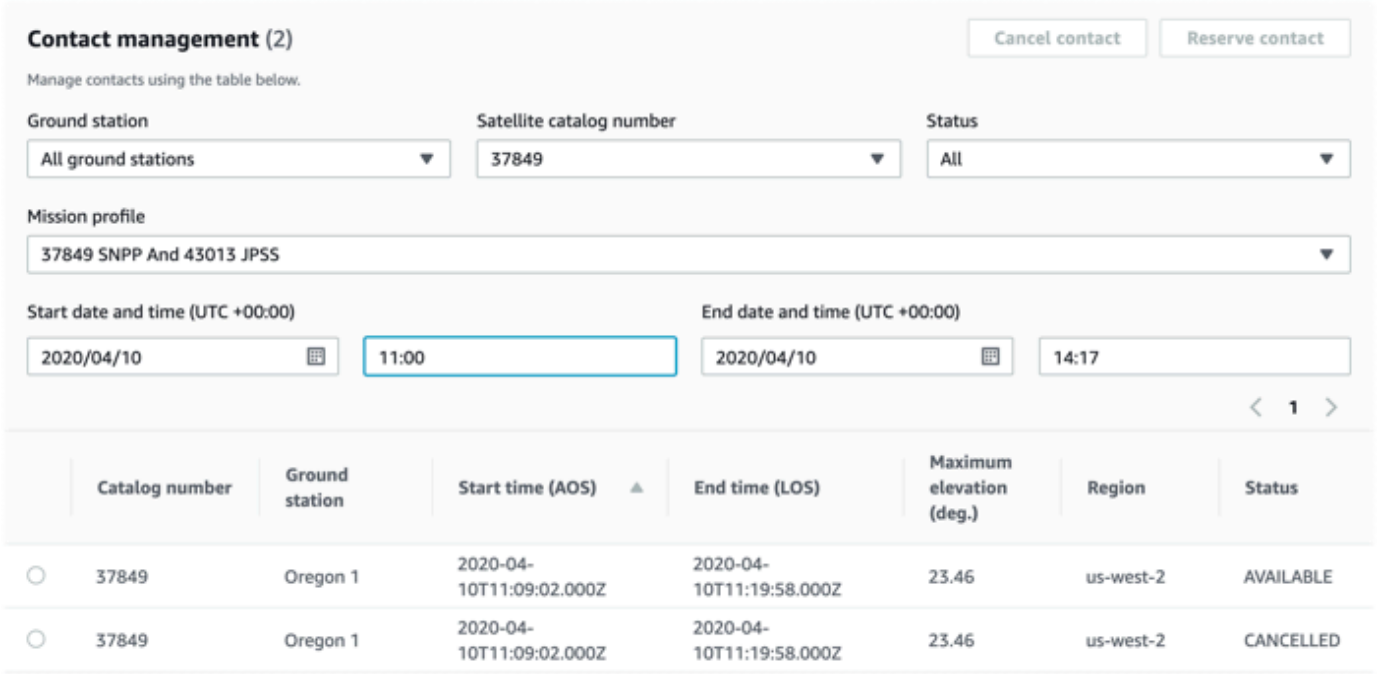


Kontak terjadwal atau selesai Anda akan terdaftar jika kontak cocok dengan parameter.

Membatalkan Kontak

Anda dapat menggunakan AWS Ground Station konsol untuk membatalkan kontak terjadwal

1. Dalam tabel Manajemen kontak, pilih parameter yang ingin Anda gunakan untuk mencari kontak terjadwal dan selesai. Pastikan Anda melihat kontak Terjadwal dengan menggunakan filter Status.
2. Pilih kontak yang ingin Anda batalkan dalam daftar kontak terjadwal. Kemudian, pilih Batalkan Kontak.
3. Dalam kotak dialog Batalkan kontak, pilih Ok.



Status kontak akan DIBATALKAN.

Satelit Penamaan

AWS Ground Station Konsol memiliki kemampuan untuk menampilkan nama yang ditentukan pengguna untuk satelit bersama dengan ID Norad saat menggunakan halaman Kontak. Menampilkan nama satelit membuatnya lebih mudah untuk memilih satelit yang benar saat menjadwalkan. Untuk melakukan ini, tag dapat digunakan.

Menandai AWS Ground Station Satellites dapat dilakukan melalui API tag-resource dengan AWS CLI atau salah satu AWS SDK. Panduan ini akan mencakup penggunaan AWS Ground Station CLI untuk menandai satelit siaran publik Aqua (Norad ID 27424) di. `us-west-2`

AWS Ground Station CLI

Hal ini AWS CLI dapat digunakan untuk berinteraksi dengan AWS Ground Station Sebelum menggunakan AWS CLI untuk menandai satelit Anda, AWS CLI prasyarat berikut harus dipenuhi:

- Pastikan AWS CLI sudah terpasang. Untuk informasi tentang penginstalan AWS CLI, lihat Menginstal AWS CLI versi 2.
- Pastikan itu AWS CLI dikonfigurasi. Untuk informasi tentang mengonfigurasi AWS CLI, lihat Mengonfigurasi AWS CLI versi 2.

- Simpan pengaturan konfigurasi dan kredenal yang sering Anda gunakan dalam file yang dikelola oleh file. AWS CLI Anda memerlukan pengaturan dan kredensional ini untuk memesan dan mengelola AWS Ground Station kontak Anda. AWS CLI Untuk informasi selengkapnya tentang menyimpan konfigurasi dan setelan kredensialnya, lihat Pengaturan File Konfigurasi dan Kredenal.

Setelah AWS CLI dikonfigurasi dan siap digunakan, tinjau halaman AWS Ground Station CLI Command Reference untuk membiasakan diri dengan perintah yang tersedia. Ikuti struktur AWS CLI perintah saat menggunakan layanan ini dan awali perintah Anda `groundstation` untuk menentukan AWS Ground Station sebagai layanan yang ingin Anda gunakan. Untuk informasi selengkapnya tentang struktur AWS CLI perintah, lihat Struktur Perintah di halaman AWS CLI. Contoh struktur perintah disediakan di bawah ini.

```
aws groundstation <command> <subcommand> [options and parameters]
```

Nama Satelit

Pertama, Anda perlu mendapatkan ARN untuk satelit yang ingin Anda tag. Ini dapat dilakukan melalui API daftar-satelit di AWS CLI:

```
aws groundstation list-satellites --region us-west-2
```

Menjalankan perintah CLI di atas akan mengembalikan output yang mirip dengan ini:

```
{
    "satellites": [
        {
            "groundStations": [
                "Ohio 1",
                "Oregon 1"
            ],
            "noradSatelliteID": 27424,
            "satelliteArn":
 "arn:aws:groundstation::111111111111:satellite/11111111-2222-3333-4444-555555555555",
            "satelliteId": "11111111-2222-3333-4444-555555555555"
        }
    ]
}
```

Temukan satelit yang ingin Anda tandai dan catat`satelliteArn`. Satu peringatan penting untuk penandaan adalah bahwa API tag-resource memerlukan ARN regional, dan ARN yang dikembalikan oleh daftar-satelit bersifat global. Untuk langkah selanjutnya, Anda harus menambah ARN dengan wilayah tempat Anda ingin melihat tag (kemungkinan wilayah yang Anda jadwalkan). Untuk contoh ini, kami menggunakan`us-west-2`. Dengan perubahan ini, ARN akan berubah dari:

```
arn:aws:groundstation::111111111111:satellite/11111111-2222-3333-4444-555555555555
```

ke:

```
arn:aws:groundstation:us-
west-2:111111111111:satellite/11111111-2222-3333-4444-555555555555
```

Untuk menunjukkan nama satelit di konsol, satelit harus memiliki tag "`Name`" dengan kunci. Selain itu, karena kita menggunakan AWS CLI, tanda kutip harus lolos dengan garis miring terbalik. Tag akan terlihat seperti:

```
{\"Name\":\"AQUA\"}
```

Selanjutnya, Anda akan memanggil API tag-resource untuk menandai satelit. Hal ini dapat dilakukan dengan AWS CLI sejenisnya:

```
aws groundstation tag-resource --region us-west-2 --resource-arn
 arn:aws:groundstation:us-
west-2:111111111111:satellite/11111111-2222-3333-4444-555555555555 --tags {\"Name\":
\"AQUA\"}
```

Setelah melakukan ini, Anda akan dapat melihat nama yang Anda tetapkan untuk satelit di AWS Ground Station konsol.

Ubah Nama Untuk Satelit

Jika Anda ingin mengubah nama untuk satelit, Anda cukup memanggil tag-resource dengan ARN satelit lagi dengan "`Name`" kunci yang sama, tetapi dengan nilai yang berbeda dalam tag. Ini akan memperbarui tag yang ada dan menampilkan nama baru di konsol. Contoh panggilan untuk ini terlihat seperti:

```
aws groundstation tag-resource --region us-west-2 --resource-arn
 arn:aws:groundstation:us-
```

```
west-2:111111111111:satellite/11111111-2222-3333-4444-555555555555 --tags {\"Name\":
\"NewName\"}
```

Hapus Nama Untuk Satelit

Nama yang ditetapkan untuk satelit dapat dihapus dengan API untag-resource. API ini membutuhkan ARN satelit dengan wilayah tempat tag berada, dan daftar kunci tag. Untuk nama, kunci tag adalah“Name”. Contoh panggilan ke API ini menggunakan AWS CLI terlihat seperti:

```
aws groundstation untag-resource --region us-west-2 --resource-arn
 arn:aws:groundstation:us-
west-2:111111111111:satellite/11111111-2222-3333-4444-555555555555 --tag-keys Name
```

Memesan dan Mengelola Kontak dengan AWS CLI

Anda dapat menggunakan AWS CLI untuk memesan dan mengelola kontak Anda di AWS Ground Station. Sebelum menggunakan AWS CLI untuk memesan dan mengelola kontak, AWS CLI prasyarat berikut harus dipenuhi:

- Pastikan AWS CLI sudah terpasang. Untuk informasi tentang penginstalan AWS CLI, lihat Menginstal AWS CLI versi 2.
- Pastikan itu AWS CLI dikonfigurasi. Untuk informasi tentang mengonfigurasi AWS CLI, lihat Mengonfigurasi AWS CLI versi 2.
- Simpan pengaturan konfigurasi dan kredenal yang sering Anda gunakan dalam file yang dikelola oleh file. AWS CLI Anda memerlukan pengaturan dan kredensional ini untuk memesan dan mengelola AWS Ground Station kontak Anda. AWS CLI Untuk informasi selengkapnya tentang menyimpan konfigurasi dan setelan kredensialnya, lihat Pengaturan File Konfigurasi dan Kredenal.

Setelah AWS CLI dikonfigurasi dan siap digunakan, tinjau halaman AWS Ground Station CLI Command Reference untuk membiasakan diri dengan perintah yang tersedia. Ikuti struktur AWS CLI perintah saat menggunakan layanan ini dan awali perintah Anda `groundstation` untuk menentukan AWS Ground Station sebagai layanan yang ingin Anda gunakan. Untuk informasi selengkapnya tentang struktur AWS CLI perintah, lihat Struktur Perintah di halaman AWS CLI. Contoh struktur perintah disediakan di bawah ini.

```
aws groundstation <command> <subcommand> [options and parameters]
```

Gunakan topik berikut untuk memesan, melihat, dan membatalkan kontak dengan AWS CLI.

Topik

Lihat dan Daftar Kontak dengan AWS CLI

Untuk membuat daftar dan melihat `CANCELLEDCOMPLETED`,, atau `SCHEDULED` kontak dengan AWS CLI, jalankan `aws groundstation list-contacts` dengan parameter berikut.

- Waktu Mulai - Tentukan waktu mulai kontak Anda dengan`--start-time <value>`. Berikut ini adalah format nilai waktu yang dapat diterima: `YYYY-MM-DDTHH:MM:SSZ`
- Waktu Akhir - Tentukan waktu akhir kontak Anda dengan`--end-time <value>`. Berikut ini adalah format nilai waktu yang dapat diterima: `YYYY-MM-DDTHH:MM:SSZ`
- Daftar Status - Tentukan status kontak Anda dengan`--status-list <value>`. Nilai yang dapat diterima termasuk `AVAILABLECANCELLED`,`COMPLETED`,, atau`SCHEDULED`. Untuk melihat daftar lengkap nilai yang valid, lihat daftar-kontak.

Untuk daftar dan melihat `AVAILABLE` kontak dengan AWS CLI parameter berikut diperlukan selain yang tercantum di atas.

- Ground Station ID - Tentukan ID stasiun bumi Anda dengan`--ground-station <value>`.
- Profil Misi ARN - Tentukan ARN profil misi Anda dengan. `--mission-profile-arn <value>`
- ARN satelit - Tentukan ARN satelit Anda dengan. `--satellite-arn <value>`

Anda dapat menggunakan `list` perintah untuk mencari sumber daya Anda. Untuk informasi selengkapnya tentang menentukan parameter Anda, lihat daftar-kontak

Contoh perintah untuk daftar kontak yang tersedia disediakan di bawah ini.

```
aws groundstation --region us-east-2 list-contacts --ground-station 'Ohio 1'
 --mission-profile-arn 'arn:aws:groundstation:us-east-2:123456789012:mission-
```

```
profile/11111111-2222-3333-4444-555555555555' --satellite-arn
 'arn:aws:groundstation::123456789012:satellite/11111111-2222-3333-4444-555555555555'
 --start-time '2020-04-10T00:09:22Z' --end-time '2020-04-10T00:11:22' --status-list
 'AVAILABLE'
```

Contoh daftar kontak yang tersedia disediakan di bawah ini.

```
{
  "contactList": [
    {
      "contactStatus": "AVAILABLE",
      "endTime": "2020-04-15T03:16:35-06:00",
      "groundStation": "Oregon 1",
      "maximumElevation": {
        "unit": "DEGREE_ANGLE",
        "value": 11.22
      },
      "missionProfileArn": "arn:aws:groundstation:us-west-2:111111111111:mission-
profile/11111111-2222-3333-4444-555555555555",
      "region": "us-west-2",
      "satelliteArn":
 "arn:aws:groundstation::111111111111:satellite/11111111-2222-3333-4444-555555555555",
      "startTime": "2020-04-15T03:06:08-06:00"
    }
  ]
}
```

Reservasi Kontak dengan AWS CLI

AWS CLI memberi Anda opsi untuk memesan kontak per menit. Fitur ini unik untuk AWS CLI dan tidak dapat dilakukan di AWS Ground Station konsol.

Untuk memesan kontak dengan AWS CLI, jalankan `aws groundstation reserve-contact` dengan parameter berikut.

- Ground Station ID - Tentukan ID stasiun bumi Anda dengan`--ground-station <value>`.
- Profil Misi ARN - Tentukan ARN profil misi Anda dengan. `--mission-profile-arn <value>`
- ARN satelit - Tentukan ARN satelit Anda dengan. `--satellite-arn <value>`
- Waktu Mulai - Tentukan waktu mulai kontak Anda dengan`--start-time <value>`. Berikut ini adalah format nilai waktu yang dapat diterima: `YYYY-MM-DDTHH:MM:SSZ`

- Waktu Akhir - Tentukan waktu akhir kontak Anda dengan`--end-time <value>`. Berikut ini adalah format nilai waktu yang dapat diterima: `YYYY-MM-DDTHH:MM:SSZ`

Reservasi kontak adalah proses asinkron. Respons terhadap `reserve-contact` perintah menyediakan pengenal kontak. Untuk menentukan hasil dari proses reservasi asinkron, gunakan. `describe-contact` Untuk informasi lebih lanjut tentang ini, lihat bagian di bawah ini berjudulJelaskan Kontak dengan AWS CLI.

Anda dapat menggunakan `list` perintah untuk mencari sumber daya Anda. Untuk informasi selengkapnya tentang menentukan parameter, lihat reserve-contact.

Contoh perintah pemesanan kontak disediakan di bawah ini.

```
aws groundstation reserve-contact --ground-station 'Ohio 1' --mission-
profile-arn 'arn:aws:groundstation:us-east-2:123456789012:mission-
profile/11111111-2222-3333-4444-555555555555' --satellite-arn
 'arn:aws:groundstation::123456789012:satellite/11111111-2222-3333-4444-555555555555'
 --start-time '2020-04-10T00:09:22Z' --end-time '2020-04-10T00:11:22'
```

Contoh kontak yang berhasil dipesan disediakan di bawah ini.

```
{
  "contactId": "11111111-2222-3333-4444-555555555555"
}
```

Jelaskan Kontak dengan AWS CLI

Untuk melihat status kontak/reservasi dengan AWS CLI, gunakan perintah CLI`describe-contact`. Ini berguna untuk memverifikasi hasil dari proses reservasi kontak asinkron, memantau status kontak yang sedang berlangsung, dan menentukan status kontak yang sudah selesai.

Untuk menggambarkan kontak dengan AWS CLI, jalankan `aws groundstation describe-contact` dengan parameter berikut.

- ID Kontak - Tentukan ID kontak Anda dengan`--contact-id <value>`.

Anda dapat menggunakan `list` perintah untuk mencari sumber daya Anda. Untuk informasi selengkapnya tentang menentukan parameter Anda, lihat deskripsi-kontak.

Contoh perintah untuk menggambarkan kontak disediakan di bawah ini.

```
aws groundstation describe-contact --contact-id 11111111-2222-3333-4444-555555555555
```

Contoh kontak yang berhasil dijadwalkan disediakan di bawah ini.

```
{
  "groundStation": "Ireland 1",
  "tags": {},
  "missionProfileArn": "arn:aws:groundstation:us-west-2:111111111111:mission-
profile/11111111-2222-3333-4444-555555555555",
  "region": "us-west-2",
  "contactId": "11111111-2222-3333-4444-555555555555",
  "prePassStartTime": 1645850471.0,
  "postPassEndTime": 1645851172.0,
  "startTime": 1645850591.0,
  "maximumElevation": {
      "value": 12.66,
      "unit": "DEGREE_ANGLE"
  },
  "satelliteArn":
 "arn:aws:groundstation::111111111111:satellite/11111111-2222-3333-4444-555555555555",
  "endTime": 1645851052.0,
  "contactStatus": "SCHEDULED"
}
```

Batalkan Kontak dengan AWS CLI

Untuk membatalkan kontak dengan AWS CLI, jalankan `aws groundstation cancel-contact` dengan parameter berikut.

- Wilayah - Tentukan wilayah stasiun bumi Anda dengan`--region <value>`.
- ID Kontak - Tentukan ID kontak dengan`--contact-id <value>`.

Anda dapat menggunakan `list` perintah untuk mencari sumber daya Anda. Untuk informasi selengkapnya tentang menentukan parameter, lihat membatalkan kontak

Contoh perintah pemesanan kontak disediakan di bawah ini.

```
aws groundstation --region us-east-2 cancel-contact --contact-id
 '11111111-2222-3333-4444-555555555555'
```

Contoh kontak yang berhasil dibatalkan disediakan di bawah ini.

```
{
  "contactId": "11111111-2222-3333-4444-555555555555"
}
```

Pengiriman Data ke Amazon EC2

AWS Ground Station mengirimkan data kontak Anda secara asinkron ke bucket Amazon Simple Storage Service (Amazon S3) di akun Anda atau secara sinkron dengan streaming ke dan dari instans Amazon Elastic Compute Cloud (Amazon EC2) di akun Anda. Langkah-langkah berikut menjelaskan cara mengonfigurasi sumber daya yang diperlukan untuk mengalirkan data kontak ke dan dari instans Amazon EC2. Lihat Memulai dengan AWS Ground Station panduan untuk informasi tentang pengiriman data ke Amazon S3.

Topik

Langkah 1: Buat Pasangan Kunci SSH EC2

Jika Anda belum memilikinya, buat key pair baru di konsol Amazon EC2 untuk setiap AWS Wilayah tempat Anda berencana menerima data. Gunakan langkah-langkah di bawah ini.

1. Di tempat Anda AWS Management Console, pilih AWS Wilayah tempat Anda berencana untuk memesan kontak. Anda perlu membuat key pair untuk setiap AWS Region yang Anda pilih.

   > **Note**
   >
   > AWS Ground Station belum tersedia untuk semua wilayah. Pastikan itu AWS Ground Station didukung oleh AWS Wilayah yang Anda inginkan. Untuk informasi selengkapnya tentang lokasi AWS Ground Station antena, lihat FAQ AWS Ground Station.

2. Ikuti panduan Buat Pasangan Kunci di Panduan Pengguna Amazon EC2 untuk membuat pasangan kunci.
3. Ulangi untuk AWS Wilayah lain jika diperlukan.

Langkah 2: Siapkan VPC Anda

Pengaturan lengkap VPC berada di luar cakupan panduan ini. Jika Anda tidak memiliki VPC yang sudah dikustomisasi, Anda dapat menggunakan VPC default yang dibuat di akun Anda. AWS Sebaiknya tambahkan benteng Linux ke VPC Anda sehingga Anda dapat SSH ke instans Amazon EC2 Anda tanpa melampirkan alamat IP publik. Untuk informasi selengkapnya tentang mengonfigurasi benteng Linux di VPC Anda, lihat Linux Bastion Host di AWS.

Untuk kenyamanan Anda, petunjuk untuk menambahkan host bastion dengan cepat ke lingkungan Linux Anda AWS ada di bawah ini. Meskipun ini tidak diperlukan, disarankan praktik terbaik.

1. Masuk ke AWS akun Anda.
2. Di Linux Bastion Host di AWS Cloud: halaman Penerapan Referensi Mulai Cepat, pilih Luncurkan Mulai Cepat (untuk VPC baru).
3. Di halaman Create Stack, pilih Next. Template sudah diisi sebelumnya.
4. Di halaman Tentukan detail tumpukan, lakukan pengeditan dan perubahan di kotak berikut:
   a. Masukkan nama tumpukan untuk host Anda di kotak Nama Tumpukan.
   b. Untuk Availability Zones, pilih Availability Zones yang ingin Anda gunakan untuk subnet di VPC. Setidaknya dua Availability Zone harus dipilih.
   c. Untuk akses eksternal benteng yang diizinkan CIDR, masukkan blok CIDR tempat Anda ingin mengaktifkan akses SSH. Jika Anda tidak yakin, Anda dapat menggunakan nilai 0.0.0.0/0 untuk mengaktifkan akses SSH dari host mana pun yang memiliki kunci SSH.
   d. Untuk nama Key pair, pilih nama key pair yang Anda buatthe section called “Langkah 1: Buat Pasangan Kunci SSH EC2”.
   e. Untuk jenis instans Bastion, pilih t2.micro.

      > **Important**
      >
      > Jenis instans t2.micro tidak tersedia untuk Wilayah Eropa (Stockholm) (eu-north-1). Jika Anda menggunakan AWS Ground Station di Wilayah Eropa (Stockholm) (eu-north-1), pilih t3.micro.

   f. Untuk penerusan TCP, pilih true.
   g. (Opsional) Lakukan pengeditan dan perubahan lain seperlunya. Untuk menyesuaikan penerapan, Anda dapat mengubah konfigurasi VPC, memilih nomor dan jenis instans host

bastion, mengaktifkan penerusan TCP atau X11, dan mengaktifkan spanduk default atau kustom untuk host bastion Anda.

h. Pilih Berikutnya.

5. Di halaman Configure stack options, buat perubahan atau pengeditan apa pun yang diperlukan.
6. Pilih Berikutnya.
7. Tinjau detail host benteng Anda dan pilih dua pengakuan Kemampuan. Kemudian, pilih Buat tumpukan.

Langkah 3: Pilih dan Sesuaikan AWS CloudFormation Template

Hari ini, Anda dapat mengonfigurasi beberapa aliran data per kontak untuk mengalir ke VPC Anda. Aliran data ini tersedia dalam dua format berbeda. Aliran data yang berisi data Sinyal/IP VITA-49 dapat dikonfigurasi untuk sinyal S-Band dan X-Band hingga 54 MHz dalam bandwidth. VITA-49 Extension Data/IP dapat dikonfigurasi untuk sinyal X-Band yang didemodulasi dan/atau diterjemahkan hingga 500 MHz dalam bandwidth.

Setelah Anda onboard satelit Anda, Anda perlu menentukan profil misi dan membuat instance untuk memproses atau mendorong aliran data dari atau ke satelit Anda. Untuk membantu Anda dalam proses ini, kami menyediakan AWS CloudFormation templat yang telah dikonfigurasi sebelumnya yang menggunakan satelit siaran publik. Template ini memudahkan Anda untuk mulai menggunakan AWS Ground Station. Untuk informasi selengkapnya AWS CloudFormation, lihat Apa itu AWS CloudFormation?

Penting untuk dicatat bahwa Anda perlu memiliki perangkat lunak pengolah data atau perangkat lunak penyimpanan data yang mendengarkan sisi localhost Data Defender dari instans Amazon EC2. Perangkat lunak ini adalah apa yang akan Anda gunakan untuk menyimpan dan/atau memproses data yang dikirimkan ke instans Amazon EC2 selama kontak.

Mengonfigurasi Pengaturan Instans Amazon EC2 Anda

AWS CloudFormation Template yang disediakan di bagian ini dikonfigurasi untuk menggunakan jenis instans Amazon EC2 m5.4xlarge secara default. Namun, kami mendorong Anda untuk menyesuaikan dan memilih pengaturan instans Amazon EC2 yang tepat untuk kasus penggunaan Anda. Persyaratan seperti penyimpanan I/O dan kinerja CPU harus dipertimbangkan ketika memilih pengaturan instans Anda. Misalnya, menjalankan modem perangkat lunak pada instance penerima mungkin memerlukan instance yang dioptimalkan komputasi dengan lebih banyak core dan kecepatan clock yang lebih tinggi. Cara terbaik untuk menentukan pengaturan instans yang

tepat untuk kasus penggunaan Anda adalah dengan menguji setelan instans dengan beban kerja Anda, dan Amazon EC2 memudahkan untuk beralih di antara setelan instans. Gunakan templat dan sesuaikan pengaturan instans untuk kebutuhan Anda.

Sebagai rekomendasi umum, AWS Ground Station dorong penggunaan instance yang mendukung peningkatan jaringan untuk uplink dan downlink Anda, seperti AWS Nitro System. Untuk informasi selengkapnya tentang jaringan yang disempurnakan, lihat Mengaktifkan jaringan yang disempurnakan dengan Adaptor Jaringan Elastis (ENA) di instans Linux.

Selain mengonfigurasi jenis instans Amazon EC2, AWS CloudFormation templat mengonfigurasi Gambar Mesin Amazon (AMI) dasar yang akan digunakan untuk instans. AWS Ground Station Basis berisi perangkat lunak yang diperlukan untuk menerima data dari layanan yang sudah diinstal sebelumnya pada instans EC2 Anda. Untuk informasi selengkapnya tentang AMI, lihat Gambar Mesin Amazon (AMI).

Membuat dan Mengkonfigurasi Sumber Daya Secara Manual

AWS CloudFormation Templat sampel di bagian ini mengonfigurasi semua sumber daya yang diperlukan untuk mulai mengeksekusi kontak satelit. Jika Anda lebih suka membuat dan mengonfigurasi sumber daya yang diperlukan secara manual untuk mulai mengeksekusi kontak satelit, Anda perlu melakukan hal berikut:

- Buat AWS Ground Station konfigurasi. Untuk informasi selengkapnya tentang membuat AWS Ground Station konfigurasi secara manual, lihat Create Config AWS CLI Command Reference atau Create Config API Reference.
- Buat profil AWS Ground Station misi. Untuk informasi selengkapnya tentang membuat profil AWS Ground Station misi secara manual, lihat Membuat Profil Misi AWS CLI Command Reference atau Membuat Referensi API Profil Misi.
- Buat grup AWS Ground Station endpoint aliran data. Untuk informasi selengkapnya tentang membuat grup titik akhir aliran AWS Ground Station data secara manual, lihat Membuat Referensi Perintah AWS CLI Grup Titik Akhir Dataflow atau Membuat Referensi API Grup Titik Akhir Dataflow.
- Buat instance EC2. Untuk informasi selengkapnya tentang membuat instans EC2 secara manual untuk digunakan dengan AWS Ground Station, lihatMembuat Instans Amazon EC2.
- Konfigurasikan pengaturan grup keamanan instans EC2 Anda AWS Ground Station untuk memungkinkan pengiriman data ke/dari instans EC2 Anda. Untuk informasi selengkapnya tentang mengonfigurasi setelan grup keamanan instans EC2 Anda secara manual, lihat Membuat Referensi Perintah AWS CLI Grup Keamanan atau Buat Referensi API Grup Keamanan.

Memilih Templat

AWS Ground Station menyediakan template yang menunjukkan cara menggunakan layanan dan dapat diakses dengan cara yang berbeda. Gunakan panduan ini untuk menemukan template yang tepat untuk Anda.

Menggunakan template yang telah dikonfigurasi sebelumnya

Anda dapat menggunakan template yang telah dikonfigurasi untuk menerima data siaran langsung dari satelit Aqua, SNPP, JPSS-1/NOAA-20, dan Terra. Template ini berisi AWS CloudFormation sumber daya yang diperlukan untuk menjadwalkan dan mengeksekusi kontak. `AquaSnppJpss`Template terdiri dari AWS CloudFormation sumber daya yang diperlukan untuk menerima data siaran langsung yang didemodulasi dan diterjemahkan. Gunakan template ini sebagai titik awal jika Anda berencana untuk memproses data menggunakan perangkat lunak NASA Direct Readout Labs (RT-STPS dan IPOPP). `AquaSnppJpssTerraDigIF`Template terdiri dari AWS CloudFormation sumber daya yang diperlukan untuk menerima data siaran langsung frekuensi menengah digital (DigIf) mentah. Gunakan template ini sebagai titik awal untuk memproses data menggunakan software defined radio (SDR). `DirectBroadcastSatelliteWbDigIfEc2DataDelivery`Template terdiri dari AWS CloudFormation sumber daya yang diperlukan untuk menerima data siaran langsung Wideband digital frekuensi menengah (DiGIF) mentah melalui Agen. AWS Ground Station

Templat Pengiriman Data Narrowband:

- the section called “AquaSnppJpss Templat (Pita sempit)”
- the section called “AquaSnppJpssTerraDigTemplat IF (Narrowband)”

Templat Pengiriman Data DiGIF Wideband:

- the section called “Templat DiGIF Wideband Satelit Siaran Langsung (Pita Lebar)”

> **Important**
>
> Satelit harus onboard ke layanan untuk mengakses AMI dengan template. AWS CloudFormation

Menggunakan satelit Anda sendiri

Mengkonfigurasi satelit Anda sendiri memerlukan serangkaian parameter dan sumber daya yang berbeda. Ini sulit dilakukan sendiri. AWS Ground Station Tim ini tersedia untuk membantu Anda mengonfigurasi satelit Anda sendiri untuk digunakan dan dapat membantu Anda mengonfigurasi sumber daya untuk aliran gema downlink, uplink, dan uplink. Untuk mengonfigurasi satelit Anda sendiri untuk digunakan AWS Ground Station, hubungi AWS Support.

Mengakses Template

Anda dapat mengakses template di bucket Amazon S3 regional di bawah ini. Perhatikan bahwa tautan berikut menggunakan titik akhir S3 regional. Ubah `<us-west-2>` ke wilayah tempat Anda membuat AWS CloudFormation tumpukan.

```
s3://groundstation-cloudformation-templates-us-west-2/
```

Anda juga dapat mengunduh templat menggunakan file AWS CLI. Untuk informasi tentang mengonfigurasi AWS CLI, lihat Mengonfigurasi. AWS CLI

AquaSnppJpss Templat (Pita sempit)

AWS CloudFormation Template bernama `AquaSnppJpss.yml` dirancang untuk memberi Anda akses cepat untuk mulai menerima data untuk satelit Aqua, SNPP, dan JPSS-1/NOAA-20. Ini berisi instans Amazon EC2 dan AWS Ground Station sumber daya yang diperlukan untuk menjadwalkan kontak dan menerima data siaran langsung yang didemodulasi dan diterjemahkan. Template ini adalah titik awal yang baik jika Anda berencana untuk memproses data menggunakan perangkat lunak NASA Direct Readout Labs (RT-STPS dan IPOPP).

Jika Aqua, SNPP, dan JPSS-1/NOAA-20 tidak terhubung ke akun Anda, lihat Orientasi Pelanggan.

> **Important**
>
> Instans Amazon EC2 harus dihentikan sebelum menerapkan template. Periksa untuk memastikan bahwa instance dihentikan sampai Anda siap menggunakannya.

Anda dapat mengakses template dengan mengakses bucket S3 orientasi pelanggan. Perhatikan bahwa tautan di bawah ini menggunakan bucket S3 regional. Ubah `<us-west-2>` ke wilayah tempat Anda membuat AWS CloudFormation tumpukan.

> **Note**
>
> Instruksi berikut menggunakan YAMAL. Namun, template tersedia dalam format YAMAL dan JSON. Untuk menggunakan JSON, ganti <.yml> dengan<.json>.

Untuk mengunduh templat menggunakan AWS CLI, gunakan perintah berikut:

```
aws s3 cp s3://groundstation-cloudformation-templates-us-west-2/AquaSnppJpss.yml .
```

Anda dapat melihat dan mengunduh templat di konsol dengan menavigasi ke URL berikut di browser Anda:

```
https://s3.console.aws.amazon.com/s3/object/groundstation-cloudformation-templates-us-west-2/AquaSnppJpss.yml
```

Anda dapat menentukan template secara langsung AWS CloudFormation menggunakan link berikut:

```
https://groundstation-cloudformation-templates-us-west-2.s3.us-west-2.amazonaws.com/AquaSnppJpss.yml
```

Sumber daya apa yang didefinisikan oleh template?

`AquaSnppJpss`Template mencakup sumber daya berikut:

- Peran Layanan Pengiriman Data - AWS Ground Station mengasumsikan peran ini untuk membuat/menghapus ENI di akun Anda untuk mengalirkan data.
- (Opsional) Instans Penerima - Instans Amazon EC2 yang akan mengirim/menerima data ke/dari satelit Anda menggunakan. AWS Ground Station
  - Grup Keamanan Instance - Grup keamanan untuk instans Amazon EC2 Anda.
  - Peran Instance - Peran untuk instans Amazon EC2 Anda.
  - Profil Instance - Profil instans untuk instans Amazon EC2 Anda.
  - Grup Penempatan Cluster - Grup penempatan tempat instans Amazon EC2 Anda diluncurkan.
- Dataflow Endpoint Security Group - Grup keamanan yang dimiliki oleh AWS Ground Station elastic network interface. Secara default, grup keamanan ini memungkinkan AWS Ground Station untuk mengalirkan lalu lintas ke alamat IP apa pun di VPC Anda. Anda dapat memodifikasi ini dengan cara yang membatasi lalu lintas ke kumpulan alamat IP tertentu.

- Receiver Instance Network Interface - Sebuah elastic network interface yang menyediakan alamat IP tetap AWS Ground Station untuk terhubung. Ini melekat pada instance penerima aktif. `eth1`
- Receiver Instance Interface Attachment - Sebuah elastic network interface yang melekat pada instans Amazon EC2 Anda.
- (Opsional) CloudWatch Event Triggers - AWS Lambda Fungsi yang dipicu menggunakan CloudWatch Peristiwa yang dikirim oleh AWS Ground Station sebelum dan sesudah kontak. AWS Lambda Fungsi akan memulai dan secara opsional menghentikan Instance Penerima Anda.
- (Opsional) Verifikasi EC2 untuk Kontak - Opsi untuk menggunakan Lambda untuk menyiapkan sistem verifikasi instans Amazon EC2 Anda untuk kontak dengan pemberitahuan SNS. Penting untuk dicatat bahwa ini mungkin dikenakan biaya tergantung pada penggunaan Anda saat ini.
- Dataflow Endpoint Group - Grup titik akhir aliran AWS Ground Station data yang mendefinisikan titik akhir yang digunakan untuk mengirim/menerima data ke/dari satelit Anda. Sebagai bagian dari pembuatan grup endpoint dataflow, AWS Ground Station buat elastic network interface di akun Anda untuk mengalirkan data.
- Tracking Config - Konfigurasi AWS Ground Station pelacakan menentukan bagaimana sistem antena melacak satelit Anda saat bergerak melalui langit.
- Ground Station Amazon Machine Image Retrieval Lambda - Opsi untuk memilih perangkat lunak apa yang diinstal dalam instans Anda dan AMI pilihan Anda. Opsi perangkat lunak termasuk `DDX 2.6.2 Only` dan`DDX 2.6.2 with qRadio 3.6.0`. Jika Anda ingin menggunakan Pengiriman Data DiGIF Wideband dan AWS Ground Station Agen, silakan gunakan. AquaSnppJpssTerraDigTemplat IF (Narrowband) Opsi ini akan terus berkembang saat pembaruan dan fitur perangkat lunak tambahan dirilis.

Selain itu, template menyediakan sumber daya berikut untuk satelit Aqua, SNPP, JPSS-1/NOAA-20:

- Konfigurasi demod/decode downlink untuk JPSS-1/NOAA-20 dan SNPP, dan konfigurasi demod/decode downlink untuk Aqua.
- Profil misi untuk JPSS-1/NOAA-20 dan SNPP, dan profil misi untuk Aqua.

Nilai dan parameter untuk satelit dalam template ini sudah terisi. Parameter ini memudahkan Anda untuk AWS Ground Station segera menggunakannya dengan satelit ini. Anda tidak perlu mengkonfigurasi nilai Anda sendiri untuk digunakan AWS Ground Station saat menggunakan template ini. Namun, Anda dapat menyesuaikan nilai untuk membuat template berfungsi untuk kasus penggunaan Anda.

Di mana saya menerima data saya?

Grup titik akhir aliran data diatur untuk menggunakan antarmuka jaringan instance penerima yang dibuat oleh bagian dari template. Instance penerima menggunakan Data Defender untuk menerima aliran data dari AWS Ground Station port yang ditentukan oleh titik akhir aliran data. Setelah diterima, data tersedia untuk konsumsi melalui port UDP 50000 pada adaptor loopback dari instance penerima. Untuk informasi selengkapnya tentang menyiapkan grup titik akhir aliran data, lihat Grup. AWS::GroundStation::DataflowEndpoint

AquaSnppJpssTerraDigTemplat IF (Narrowband)

AWS CloudFormation Template bernama `AquaSnppJpssTerraDigIF.yml` dirancang untuk memberi Anda akses cepat untuk mulai menerima data frekuensi menengah digital (DiGIF) untuk satelit Aqua, SNPP, JPSS-1/NOAA-20, dan Terra. Ini berisi instans Amazon EC2 dan AWS CloudFormation sumber daya yang diperlukan untuk menerima data siaran langsung DiGIF mentah. Template ini adalah titik awal yang baik untuk memproses data menggunakan software defined radio (SDR).

Jika Aqua, SNPP, JPSS-1/NOAA-20, dan Terra tidak terhubung ke akun Anda, lihat Orientasi Pelanggan.

> **Important**
>
> Instans Amazon EC2 harus dihentikan sebelum menerapkan template. Periksa untuk memastikan bahwa instance dihentikan sampai Anda siap menggunakannya.

Anda dapat mengakses template dengan mengakses bucket S3 orientasi pelanggan. Perhatikan bahwa tautan di bawah ini menggunakan bucket S3 regional. Ubah `<us-west-2>` ke wilayah tempat Anda membuat AWS CloudFormation tumpukan.

> **Note**
>
> Instruksi berikut menggunakan YAMAL. Namun, template tersedia dalam format YAMAL dan JSON. Untuk menggunakan JSON, ganti `<.yml>` dengan`<.json>`.

Untuk mengunduh templat menggunakan AWS CLI, gunakan perintah berikut:

```
aws s3 cp s3://groundstation-cloudformation-templates-us-west-2/
AquaSnppJpssTerraDigIF.yml .
```

Anda dapat melihat dan mengunduh templat di konsol dengan menavigasi ke URL berikut di browser Anda:

```
https://s3.console.aws.amazon.com/s3/object/groundstation-cloudformation-templates-us-
west-2/AquaSnppJpssTerraDigIF.yml
```

Anda dapat menentukan template secara langsung AWS CloudFormation menggunakan link berikut:

```
https://groundstation-cloudformation-templates-us-west-2.s3.us-west-2.amazonaws.com/
AquaSnppJpssTerraDigIF.yml
```

Sumber daya apa yang didefinisikan oleh template?

`AquaSnppJpssTerraDigIF`Template mencakup sumber daya berikut:

- Peran Layanan Pengiriman Data - AWS Ground Station mengasumsikan peran ini untuk membuat/menghapus ENI di akun Anda untuk mengalirkan data.
- (Opsional) Instans Penerima - Instans Amazon EC2 yang akan mengirim/menerima data ke/dari satelit Anda menggunakan. AWS Ground Station
  - Grup Keamanan Instance - Grup keamanan untuk instans Amazon EC2 Anda.
  - Peran Instance - Peran untuk instans Amazon EC2 Anda.
  - Profil Instance - Profil instans untuk instans Amazon EC2 Anda.
  - Grup Penempatan Cluster - Grup penempatan tempat instans Amazon EC2 Anda diluncurkan.
- Dataflow Endpoint Security Group - Grup keamanan yang dimiliki oleh AWS Ground Station elastic network interface. Secara default, grup keamanan ini memungkinkan AWS Ground Station untuk mengalirkan lalu lintas ke alamat IP apa pun di VPC Anda. Anda dapat memodifikasi ini dengan cara yang membatasi lalu lintas ke kumpulan alamat IP tertentu.
- Receiver Instance Network Interface - Sebuah elastic network interface yang menyediakan alamat IP tetap AWS Ground Station untuk terhubung. Ini melekat pada instance penerima aktif. `eth1`
- Receiver Instance Interface Attachment - Sebuah elastic network interface yang melekat pada instans Amazon EC2 Anda.

- (Opsional) CloudWatch Event Triggers - AWS Lambda Fungsi yang dipicu menggunakan CloudWatch Peristiwa yang dikirim oleh AWS Ground Station sebelum dan sesudah kontak. AWS Lambda Fungsi akan memulai dan secara opsional menghentikan Instance Penerima Anda.
- (Opsional) Verifikasi EC2 untuk Kontak - Opsi untuk menggunakan Lambda untuk menyiapkan sistem verifikasi instans Amazon EC2 Anda untuk kontak dengan pemberitahuan SNS. Penting untuk dicatat bahwa ini mungkin dikenakan biaya tergantung pada penggunaan Anda saat ini.
- Dataflow Endpoint Group - Grup titik akhir aliran AWS Ground Station data yang mendefinisikan titik akhir yang digunakan untuk mengirim/menerima data ke/dari satelit Anda. Sebagai bagian dari pembuatan grup endpoint dataflow, AWS Ground Station buat elastic network interface di akun Anda untuk mengalirkan data.
- Tracking Config - Konfigurasi AWS Ground Station pelacakan menentukan bagaimana sistem antena melacak satelit Anda saat bergerak melalui langit.
- Downlink Dig IF Endpoint Config - Titik akhir yang ditentukan yang digunakan untuk downlink data dari satelit Anda.
- Ground Station Amazon Machine Image Retrieval Lambda - Opsi untuk memilih perangkat lunak apa yang diinstal dalam instans Anda dan AMI pilihan Anda. Opsi perangkat lunak termasuk `DDX 2.6.2 Only` dan`DDX 2.6.2 with qRadio 3.6.0`. Opsi ini akan terus berkembang saat pembaruan dan fitur perangkat lunak tambahan dirilis.

Selain itu, template menyediakan sumber daya berikut untuk satelit Aqua, SNPP, JPSS-1/NOAA-20, dan Terra:

- Konfigurasi antena DiGIF downlink untuk Aqua, SNPP, JPSS-1/NOAA-20, dan Terra.
- Profil misi untuk JPSS-1/NOAA-20 dan SNPP, profil misi untuk Aqua, dan profil misi untuk Terra.

Nilai dan parameter untuk satelit dalam template ini sudah terisi. Parameter ini memudahkan Anda untuk AWS Ground Station segera menggunakannya dengan satelit ini. Anda tidak perlu mengkonfigurasi nilai Anda sendiri untuk digunakan AWS Ground Station saat menggunakan template ini. Namun, Anda dapat menyesuaikan nilai untuk membuat template berfungsi untuk kasus penggunaan Anda.

Di mana saya menerima data saya?

Grup titik akhir aliran data diatur untuk menggunakan antarmuka jaringan instance penerima yang dibuat oleh bagian dari template. Instance penerima menggunakan Data Defender untuk menerima aliran data dari AWS Ground Station port yang ditentukan oleh titik akhir aliran data. Setelah

diterima, data tersedia untuk konsumsi melalui port UDP 50000 pada adaptor loopback dari instance penerima. Untuk informasi selengkapnya tentang menyiapkan grup titik akhir aliran data, lihat Grup. AWS::GroundStation::DataflowEndpoint

Templat DiGIF Wideband Satelit Siaran Langsung (Pita Lebar)

AWS CloudFormation Template bernama `DirectBroadcastSatelliteWbDigIfEc2DataDelivery.yml` dirancang untuk memberi Anda akses cepat untuk mulai menerima data frekuensi menengah digital (DiGIF) untuk satelit Aqua, SNPP, JPSS-1/NOAA-20, dan Terra. Ini berisi instans Amazon EC2 dan AWS CloudFormation sumber daya yang diperlukan untuk menerima data siaran langsung DiGIF mentah. Template ini adalah titik awal yang baik untuk memproses data menggunakan software defined radio (SDR).

Jika Aqua, SNPP, JPSS-1/NOAA-20, dan Terra tidak terhubung ke akun Anda, lihat Orientasi Pelanggan.

> **Important**
>
> Instans Amazon EC2 harus dihentikan sebelum menerapkan template. Periksa untuk memastikan bahwa instance dihentikan sampai Anda siap menggunakannya.

Anda dapat mengakses template dengan mengakses bucket S3 orientasi pelanggan. Perhatikan bahwa tautan di bawah ini menggunakan bucket S3 regional. Ubah `<us-west-2>` ke wilayah tempat Anda membuat AWS CloudFormation tumpukan.

> **Note**
>
> Instruksi berikut menggunakan YAMAL. Namun, template tersedia dalam format YAMAL dan JSON. Untuk menggunakan JSON, ganti `<.yml>` dengan`<.json>`.

Untuk mengunduh templat menggunakan AWS CLI, gunakan perintah berikut:

```
aws s3 cp s3://groundstation-cloudformation-templates-us-west-2/agent/ec2_delivery/
DirectBroadcastSatelliteWbDigIfEc2DataDelivery.yml .
```

Anda dapat melihat dan mengunduh templat di konsol dengan menavigasi ke URL berikut di browser Anda:

```
https://s3.console.aws.amazon.com/s3/object/groundstation-cloudformation-templates-us-
west-2/agent/ec2_delivery/DirectBroadcastSatelliteWbDigIfEc2DataDelivery.yml
```

Anda dapat menentukan template secara langsung AWS CloudFormation menggunakan link berikut:

```
https://groundstation-cloudformation-templates-us-west-2.s3.us-west-2.amazonaws.com/
agent/ec2_delivery/DirectBroadcastSatelliteWbDigIfEc2DataDelivery.yml
```

Sumber daya apa yang didefinisikan oleh template?

`DirectBroadcastSatelliteWbDigIfEc2DataDelivery`Template mencakup sumber daya berikut:

- (Opsional) Instans Penerima - Instans Amazon EC2 yang akan mengirim/menerima data ke/dari satelit Anda menggunakan. AWS Ground Station
  - Grup Keamanan Instance - Grup keamanan untuk instans Amazon EC2 Anda.
  - Peran Instance - Peran untuk instans Amazon EC2 Anda.
  - Profil Instance - Profil instans untuk instans Amazon EC2 Anda.
  - Grup Penempatan Cluster - Grup penempatan tempat instans Amazon EC2 Anda diluncurkan.
- Kunci Pengiriman Data - AWS KMS Kunci yang digunakan untuk mengenkripsi aliran data.
- Peran Kunci Ground Station - Peran IAM yang AWS Ground Station akan mengasumsikan untuk mengakses dan menggunakan AWS KMS Kunci untuk mendekripsi aliran data
- Kebijakan Akses Kunci Ground Station - Kebijakan IAM yang menentukan tindakan AWS Ground Station dapat dilakukan pada Kunci Pengiriman Data
- Receiver Instance Elastic Network Interface - (Bersyarat) Sebuah elastic network interface dibuat dalam subnet yang ditentukan oleh PublicSubnetIdjika disediakan. Ini diperlukan jika instance penerima berada di subnet pribadi. Elastic network interface akan dikaitkan dengan EIP dan dilampirkan ke instance receiver.
- Receiver Instance Elastic IP - IP elastis yang AWS Ground Station akan terhubung ke. Ini melekat pada instance receiver atau elastic network interface.
- Salah satu asosiasi IP Elastis berikut:
  - Instance Penerima ke Asosiasi IP Elastis - Asosiasi IP Elastis ke instance penerima Anda, jika tidak PublicSubnetIdditentukan. Ini membutuhkan SubnetIdreferensi subnet publik.
  - Receiver Instance Elastic Network Interface to Elastic IP Association - Asosiasi IP elastis ke instance receiver elastic network interface, jika PublicSubnetIdditentukan.

- (Opsional) CloudWatch Event Triggers - AWS Lambda Fungsi yang dipicu menggunakan CloudWatch Peristiwa yang dikirim oleh AWS Ground Station sebelum dan sesudah kontak. AWS Lambda Fungsi akan memulai dan secara opsional menghentikan Instance Penerima Anda.
- (Opsional) Verifikasi EC2 untuk Kontak - Opsi untuk menggunakan Lambda untuk menyiapkan sistem verifikasi instans Amazon EC2 Anda untuk kontak dengan pemberitahuan SNS. Penting untuk dicatat bahwa ini mungkin dikenakan biaya tergantung pada penggunaan Anda saat ini.
- Dataflow Endpoint Group - Grup titik akhir aliran AWS Ground Station data yang mendefinisikan titik akhir yang digunakan untuk mengirim/menerima data ke/dari satelit Anda.
- Tracking Config - Konfigurasi AWS Ground Station pelacakan menentukan bagaimana sistem antena melacak satelit Anda saat bergerak melalui langit.

Selain itu, template menyediakan sumber daya berikut untuk satelit Aqua, SNPP, JPSS-1/NOAA-20, dan Terra:

- Konfigurasi downlink untuk JPSS-1/NOAA-20 dan SNPP, konfigurasi downlink untuk Aqua, dan konfigurasi downlink untuk Terra.
- Profil misi untuk JPSS-1/NOAA-20 dan SNPP, profil misi untuk Aqua, dan profil misi untuk Terra.

Nilai dan parameter untuk satelit dalam template ini sudah terisi. Parameter ini memudahkan Anda untuk AWS Ground Station segera menggunakannya dengan satelit ini. Anda tidak perlu mengkonfigurasi nilai Anda sendiri untuk digunakan AWS Ground Station saat menggunakan template ini. Namun, Anda dapat menyesuaikan nilai untuk membuat template berfungsi untuk kasus penggunaan Anda.

Di mana saya menerima data saya?

Grup titik akhir aliran data diatur untuk menggunakan antarmuka jaringan instance penerima yang dibuat oleh bagian dari template. Instance penerima menggunakan AWS Ground Station Agen untuk menerima aliran data dari AWS Ground Station port yang ditentukan oleh titik akhir aliran data. Untuk informasi selengkapnya tentang menyiapkan grup titik akhir aliran data, lihat Grup. AWS::GroundStation::DataflowEndpoint Untuk informasi lebih lanjut tentang AWS Ground Station Agen, lihatAWS Ground Station Panduan Pengguna Agen.

Membuat Instans Amazon EC2

> **Note**
>
> Tidak perlu atau disarankan untuk membuat sumber daya Anda AWS Ground Station (termasuk instans Amazon EC2) secara manual karena AWS Ground Station menyediakan AWS CloudFormation templat premade untuk ini (Lihat Langkah 3: Pilih dan Sesuaikan AWS CloudFormation Template untuk informasi lebih lanjut). Jika menggunakan AWS CloudFormation template tidak akan berfungsi untuk kasus penggunaan Anda, silakan lanjutkan membaca.

AWS Ground Station menyediakan AMI Amazon EC2 yang sudah dimuat sebelumnya dengan perangkat lunak yang diperlukan untuk mengambil pengiriman data pada instans Amazon EC2 baik untuk Narrowband atau Pengiriman Data Pita Lebar. DigIf

> **Important**
>
> Satelit harus onboard ke layanan untuk mengakses AMI. AWS Ground Station

Amazon EC2 AMI dengan DataDefender

AMI ini sudah diinstal sebelumnya dengan DataDefender perangkat lunak dan digunakan untuk kontak downlink pengiriman data Narrowband.

Skema penamaan untuk AMI ini adalah`groundstation-al2-ddx$DDX_VERSION-ami-$DATE_PUBLISHED`. AMI DDX baru diterbitkan tak lama setelah AL2 Amazon EC2 AMI baru diterbitkan. Jika AWS Ground Station memutuskan untuk mendukung versi baru DataDefender perangkat lunak, AMI baru akan diterbitkan menggunakan versi yang diperbarui.

Memilih AWS Ground Station AMI dengan DataDefender

Anda dapat mengakses AWS Ground Station AMI melalui tab AMI di konsol Amazon EC2. Setelah berada di halaman itu, AMI dapat diakses di bawah filter Gambar Pribadi.

Kami merekomendasikan untuk menyortir AMI berdasarkan tanggal yang diterbitkan dan menggunakan nama AMI yang paling baru diterbitkan`groundstation-al2-ddx$DDX_VERSION-ami-$DATE_PUBLISHED`.

Amazon EC2 AMI dengan Agen AWS Ground Station

AMI ini sudah diinstal sebelumnya dengan AWS Ground Station Agen dan digunakan untuk kontak downlink Wideband DiGIF.

Skema penamaan untuk AMI ini adalah `groundstation-al2-gs-agent-ami-*` di mana * adalah tanggal AMI dibangun. AWS Ground Station Agen AMI baru diterbitkan tak lama setelah AL2 Amazon EC2 AMI baru diterbitkan atau ketika versi baru AWS Ground Station dari Agen RPM dirilis.

Untuk informasi lebih lanjut tentang AWS Ground Station Agen, lihatAWS Ground Station Panduan Pengguna Agen.

Memilih AWS Ground Station Agen AMI

Anda dapat mengakses AWS Ground Station Agen AMI melalui tab AMI di konsol Amazon EC2. Setelah berada di halaman itu, AMI dapat diakses di bawah filter Gambar Publik.

Kami merekomendasikan untuk menyortir AMI berdasarkan tanggal yang diterbitkan dan menggunakan nama AMI yang paling baru diterbitkan`groundstation-al2-gs-agent-ami-$DATE_PUBLISHED`.

Langkah 4: Konfigurasikan AWS CloudFormation Stack

Setelah memilih template yang paling sesuai untuk kasus penggunaan Anda, konfigurasikan AWS CloudFormation tumpukan. Sumber daya yang dibuat dalam prosedur ini dikonfigurasi ke wilayah tempat Anda berada saat Anda membuatnya. Ini termasuk profil misi dan propertinya yang menentukan ke wilayah mana data Anda dikirimkan.

1. Di bagian AWS Management Console, pilih Layanan > CloudFormation.
2. Di panel navigasi, pilih Stacks (Tumpukan). Kemudian, pilih Buat tumpukan> Dengan sumber daya baru (standar).
3. Di halaman Create Stack, tentukan template yang Anda pilih the section called “Memilih Templat” dengan melakukan salah satu hal berikut.

    a. Pilih URL Amazon S3 sebagai sumber templat Anda, lalu salin dan tempel URL templat yang ingin Anda gunakan di URL Amazon S3. Lalu, pilih Selanjutnya.

    b. Pilih Unggah file templat sebagai sumber templat Anda dan pilih Pilih File. Unggah template yang Anda unduhthe section called “Memilih Templat”. Lalu, pilih Selanjutnya.
4. Di halaman Tentukan detail tumpukan, buat perubahan berikut:

a. Masukkan nama di kotak Nama Tumpukan. Sebaiknya gunakan nama sederhana untuk mengurangi kemungkinan kesalahan di masa depan.

b. Untuk CloudWatchEventActions, pilih tindakan mana yang akan dilakukan untuk pemicu CloudWatch peristiwa sebelum dan sesudah kontak.

c. Untuk createEC2 VerificationForContacts, pilih apakah Anda ingin menyiapkan sistem verifikasi (menggunakan Lambda) instans EC2 Anda atau tidak untuk kontak dengan notifikasi SNS. Penting untuk dicatat bahwa ini mungkin dikenakan biaya tergantung pada penggunaan Anda saat ini.

d. Untuk CreateReceiverInstance, pilih apakah Anda ingin membuat instans penerima Amazon EC2 atau tidak.

e. Pilih SSH Key yang Anda buat. the section called “Langkah 1: Buat Pasangan Kunci SSH EC2”

f. Pilih SubnetIddi mana Anda ingin membuat instans Amazon EC2 Anda.

   Jika menggunakan AWS Ground Station Agen diperlukan subnet publik, baik untuk penempatan instance atau elastic network interface; Jika Anda menentukan subnet pribadi untuk menempatkan instance Anda, Anda juga harus menentukan subnet publik di PublicSubnetId(lihat di bawah) untuk digunakan dengan Agen. SubnetId AWS Ground Station

   Untuk kasus penggunaan non-agen, kami sarankan menempatkan instans Amazon EC2 Anda di subnet pribadi sebagai praktik terbaik, meskipun tidak diperlukan. Anda dapat menggunakan Linux Bastion Host di AWS Cloud: Quick Start Reference Deployment untuk secara otomatis membuat subnet pribadi jika Anda belum mengonfigurasi akun Anda dengan one in. the section called “Langkah 2: Siapkan VPC Anda”

   > **Note**
   >
   > Organisasi Anda mungkin memiliki subnet lain yang didedikasikan untuk instans Amazon EC2 Anda.

g. (Opsional) Pilih PublicSubnetIduntuk digunakan hanya jika menggunakan AWS Ground Station Agen dengan instance di subnet pribadi. Ini diperlukan jika Anda menentukan subnet pribadi di SubnetId.

Subnet ini harus berada di akun Anda di zona ketersediaan yang sama dengan yang ditentukan oleh SubnetId. Menyediakan PublicSubnetIdwasiat menghasilkan pembuatan elastic network interface di subnet publik yang disediakan, yang melekat pada instans Anda. Antarmuka ini digunakan untuk akses jaringan AWS Ground Station Agen dari instans Anda yang ditempatkan di subnet pribadi yang ditentukan dalam SubnetId.

h. Pilih VPC Stack yang Anda buat. the section called “Langkah 2: Siapkan VPC Anda”

i. Pilih Berikutnya.

5. Konfigurasikan opsi tumpukan dan opsi lanjutan untuk instans Amazon EC2 Anda.

   a. Tambahkan tag dan izin apa pun di bagian Tag dan Izin.

   b. Buat perubahan apa pun untuk kebijakan Stack, konfigurasi Rollback, opsi Pemberitahuan, dan opsi pembuatan Stack.

   c. Pilih Berikutnya.

6. Setelah meninjau detail tumpukan Anda, pilih pengakuan Kemampuan, dan pilih Buat tumpukan.

Langkah 5: Instal dan Konfigurasikan Prosesor/Radio FE

Instans Amazon EC2 yang ditentukan dalam AWS CloudFormation template tidak memiliki prosesor Front End (FE) atau radio yang ditentukan perangkat lunak (SDR) yang diinstal secara default. Anda perlu menginstal prosesor FE atau SDR untuk memproses paket VITA-49 yang dialirkan ke/dari sistem antena. AWS Ground Station

Cara Anda menginstal dan mengonfigurasi prosesor FE atau SDR Anda tergantung pada prosesor FE atau SDR yang Anda gunakan. Pemasangan prosesor FE atau SDR berada di luar cakupan panduan pengguna ini.

Untuk menginstal dan mengonfigurasi prosesor/radio FE, hubungi AWS Support.

> **Important**
>
> Merupakan praktik terbaik untuk menjalankan prosesor FE atau SDR Anda pada instance yang dibuat oleh AWS CloudFormation template untuk memastikan manfaat aliran data DTLS ke/dari Data Defender.

Langkah Berikutnya

AWS Ground Station Akun dan sumber daya Anda sekarang dikonfigurasi dan siap digunakan. Sumber daya ini tersedia untuk digunakan di AWS Ground Station konsol tempat Anda dapat memasukkan data satelit, mengidentifikasi lokasi antena, berkomunikasi, dan menjadwalkan waktu antena untuk satelit yang dipilih. Anda juga dapat mulai menggunakan alat yang berbeda untuk memantau aktivitas dan mengonfigurasi alarm.

Gunakan topik berikut untuk informasi lebih lanjut:

- Daftar dan Pemesanan Kontak
- Pemantauan AWS Ground Station

Menggunakan Layanan Pengiriman Data Lintas Wilayah

Fitur pengiriman data AWS Ground Station lintas wilayah memberi Anda fleksibilitas untuk mengirim data dari antena ke instans Amazon EC2 di Wilayah AWS Anda. Pengiriman data lintas wilayah saat ini tersedia di semua wilayah yang AWS Ground Station didukung saat menerima data kontak Anda di Bucket Amazon S3. Ini hanya tersedia di antenna-to-destination wilayah berikut saat menggunakan pengiriman data ke Amazon EC2:

- Wilayah Timur AS (Ohio) (us-timur-2) ke Wilayah AS Barat (Oregon) (us-barat-2)
- Wilayah AS Barat (Oregon) (us-barat-2) ke Wilayah Timur AS (Ohio) (us-timur-2)

Untuk menggunakan pengiriman data lintas wilayah, Anda harus memiliki AWS CloudFormation templat yang dikonfigurasi. Untuk informasi selengkapnya tentang memilih dan menyesuaikan AWS CloudFormation templat, lihatLangkah 3: Pilih dan Sesuaikan AWS CloudFormation Template.

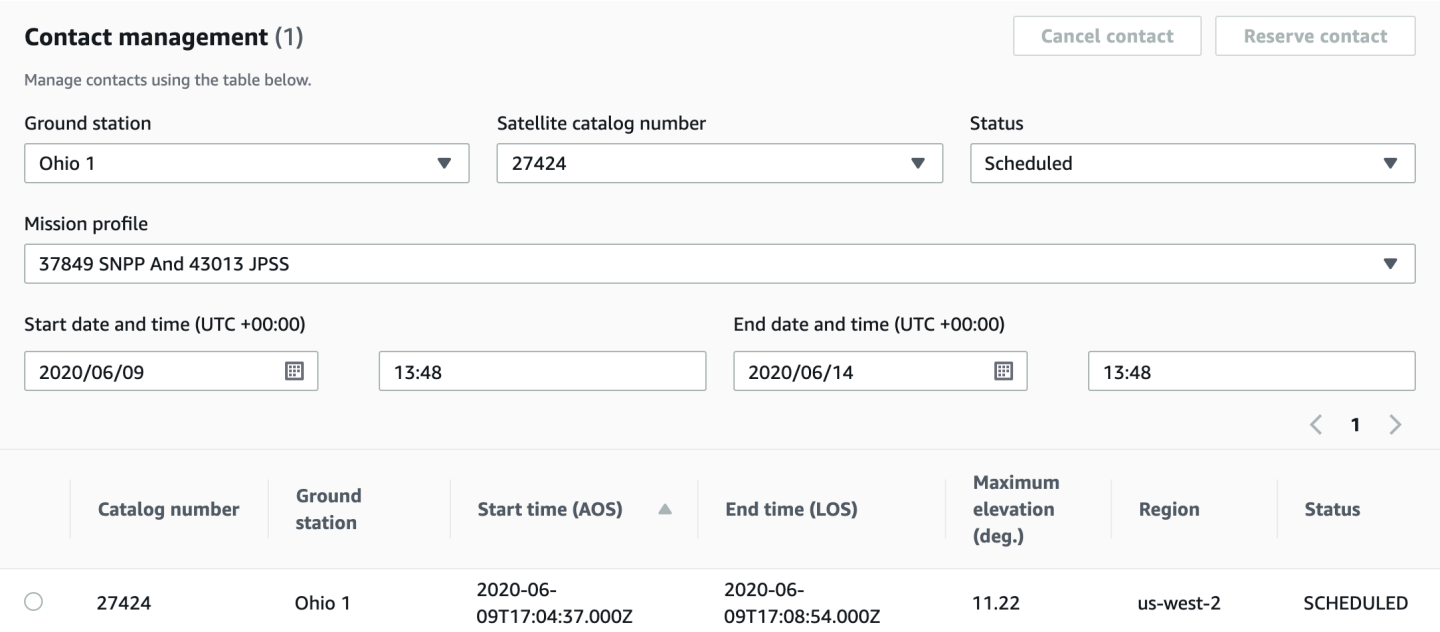
Gunakan topik berikut untuk menggunakan pengiriman data lintas wilayah di AWS Ground Station.

Topik

Untuk menggunakan pengiriman data lintas wilayah di konsol

Saat Anda memesan kontak di AWS Ground Station konsol, pilih profil misi yang dikonfigurasi untuk mengirimkan data kontak ke wilayah yang Anda inginkan. Pastikan semua parameter Anda sudah benar dan pilih Reserve contact. Jika Anda tidak melihat profil misi yang diinginkan di konsol, periksa untuk memastikan Anda membuat profil misi di wilayah tempat Anda melihat konsol.

Setelah memesan kontak Anda, Anda dapat melihat kontak terjadwal untuk memverifikasi bahwa Anda telah menjadwalkan pengiriman data lintas wilayah dengan melihat lokasi antena stasiun bumi dan wilayah tujuan. Gambar berikut menunjukkan kontak yang dijadwalkan untuk pengiriman data lintas wilayah. Kontak dikonfigurasi untuk menggunakan antena stasiun bumi Ohio dan mengirimkan data ke Oregon.



Untuk menggunakan pengiriman data lintas wilayah dengan AWS CLI

Saat Anda memesan kontak AWS CLI, pilih profil misi yang dikonfigurasi untuk mengirimkan data kontak ke wilayah yang Anda inginkan. Tentukan ARN profil misi yang diinginkan dengan. `--mission-profile-arn <value>` Pastikan semua parameter Anda benar dan jalankan perintah. Jika Anda tidak melihat profil misi ARN yang diinginkan saat melihat dan mencantumkan kontak, periksa untuk memastikan Anda membuat profil misi di wilayah tempat Anda menjalankan. AWS CLI

Setelah memesan kontak Anda, Anda dapat melihat kontak terjadwal untuk memverifikasi bahwa Anda telah menjadwalkan pengiriman data lintas wilayah dengan melihat lokasi antena stasiun bumi dan wilayah tujuan. Output berikut menunjukkan kontak yang dijadwalkan untuk pengiriman data lintas wilayah. Kontak dikonfigurasi untuk menggunakan antena stasiun bumi Ohio dan mengirimkan data ke Oregon.

```
{
  "contactList": [
    {
      "contactId": "11111111-2222-3333-4444-555555555555",
      "contactStatus": "SCHEDULED",
      "endTime": "2020-05-05T03:16:35-06:00",
      "groundStation": "Ohio 1",
      "maximumElevation": {
```

```
        "unit": "DEGREE_ANGLE",
        "value": 26.74
      },
      "missionProfileArn": "arn:aws:groundstation:us-west-2:123456789012:mission-
profile/11111111-2222-3333-4444-555555555555",
      "postPassEndTime": "2020-05-05T03:17:35-06:00",
      "prePassStartTime": "2020-05-05T03:04:08-06:00",
      "region": "us-west-2",
      "satelliteArn":
 "arn:aws:groundstation::123456789012:satellite/11111111-2222-3333-4444-555555555555",
      "startTime": "2020-05-05T03:06:08-06:00"
    }
  ]
}
```

Pemantauan AWS Ground Station

Pemantauan merupakan bagian penting dari menjaga keandalan, ketersediaan, dan kinerja AWS Ground Station. AWS menyediakan alat pemantauan berikut untuk menonton AWS Ground Station, melaporkan ketika ada sesuatu yang salah, dan mengambil tindakan otomatis bila perlu.

- Amazon CloudWatch Events memberikan aliran peristiwa sistem yang mendekati waktu nyata yang menjelaskan perubahan AWS sumber daya. CloudWatch Peristiwa memungkinkan komputasi berbasis peristiwa otomatis, karena Anda dapat menulis aturan yang mengawasi peristiwa tertentu dan memicu tindakan otomatis di AWS layanan lain saat peristiwa ini terjadi. Untuk informasi selengkapnya tentang CloudWatch Acara Amazon, lihat Panduan Pengguna CloudWatch Acara Amazon.
- AWS EventBridge Events menghadirkan aliran peristiwa sistem yang mendekati real-time yang menjelaskan perubahan AWS sumber daya. EventBridge Peristiwa memungkinkan komputasi berbasis peristiwa otomatis, karena Anda dapat menulis aturan yang mengawasi peristiwa tertentu dan memicu tindakan otomatis di AWS layanan lain saat peristiwa ini terjadi. Untuk informasi selengkapnya tentang EventBridge Acara, lihat Panduan Pengguna EventBridge Acara Amazon.
- AWS CloudTrailmenangkap panggilan API dan peristiwa terkait yang dibuat oleh atau atas nama AWS akun Anda dan mengirimkan file 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. Untuk informasi selengkapnya AWS CloudTrail, lihat Panduan AWS CloudTrail Pengguna.
- Amazon CloudWatch Metrics menangkap metrik untuk kontak terjadwal Anda saat menggunakan. AWS Ground Station CloudWatch Metrik memungkinkan Anda menganalisis data berdasarkan saluran, polarisasi, dan ID satelit untuk mengidentifikasi kekuatan dan kesalahan sinyal dalam kontak Anda. Untuk informasi selengkapnya, lihat Menggunakan CloudWatch Metrik Amazon.
- AWS Notifikasi Pengguna dapat digunakan untuk menyiapkan saluran pengiriman agar mendapat pemberitahuan tentang AWS Ground Station peristiwa. Anda akan menerima notifikasi saat ada sebuah peristiwa yang cocok dengan sebuah aturan yang Anda tentukan. Anda dapat menerima notifikasi untuk peristiwa melalui beberapa saluran, termasuk email, notifikasi obrolan AWS Chatbot, atau notifikasi push AWS Console Mobile Application. Anda juga dapat melihat notifikasi di Pusat Pemberitahuan Konsol. Notifikasi Pengguna mendukung agregasi, yang dapat mengurangi jumlah pemberitahuan yang Anda terima selama acara tertentu.

Gunakan topik berikut untuk memantau AWS Ground Station.

Topik

Mengotomatisasi AWS Ground Station dengan Acara

> **Note**
>
> Dokumen ini menggunakan istilah “acara” di seluruh. CloudWatch Peristiwa dan EventBridge merupakan layanan dan API dasar yang sama. Aturan untuk mencocokkan peristiwa yang masuk dan meruteknya ke target untuk diproses dapat dibuat menggunakan salah satu layanan.

Acara memungkinkan Anda untuk mengotomatiskan AWS layanan Anda dan merespons secara otomatis peristiwa sistem seperti masalah ketersediaan aplikasi atau perubahan sumber daya. Acara dari AWS layanan disampaikan dalam waktu dekat. Anda dapat menulis aturan sederhana untuk menunjukkan kejadian mana yang sesuai kepentingan Anda, dan tindakan otomatis apa yang diambil ketika suatu kejadian sesuai dengan suatu aturan. Tindakan yang dapat dipicu secara otomatis meliputi hal-hal berikut:

- Memanggil fungsi AWS Lambda
- Meminta Perintah Amazon EC2 Run
- Mengirim peristiwa ke Amazon Kinesis Data Streams
- Mengaktifkan mesin AWS Step Functions negara
- Memberi tahu topik Amazon SNS atau antrian AWS SMS

Beberapa contoh penggunaan acara dengan AWS Ground Station meliputi:

- Memanggil fungsi Lambda untuk mengotomatiskan awal dan penghentian instans Amazon EC2 berdasarkan status peristiwa.
- Menerbitkan ke topik Amazon SNS setiap kali kontak berubah status. Topik-topik ini dapat diatur untuk mengirimkan pemberitahuan email di awal atau akhir kontak.

Untuk informasi selengkapnya, lihat Panduan Pengguna CloudWatch Acara Amazon atau Panduan Pengguna EventBridge Acara Amazon.

Contoh Acara

> **Note**
>
> Semua peristiwa yang dihasilkan oleh AWS Ground Station memiliki “aws.groundstation” sebagai nilai untuk “sumber”.

Perubahan Status Kontak Ground Station

Jika Anda ingin melakukan tindakan tertentu saat kontak yang akan datang mengubah status, Anda dapat mengatur aturan untuk mengotomatiskan tindakan ini. Ini berguna ketika Anda ingin menerima pemberitahuan tentang perubahan status kontak Anda. Jika Anda ingin mengubah saat menerima acara ini, Anda dapat memodifikasi profil misi Anda contactPrePassDurationSecondsdan contactPostPassDurationSeconds. Acara dikirim ke wilayah tempat kontak dijadwalkan.

Contoh diberikan di bawah ini.

```
{
    "version": "0",
    "id": "01234567-0123-0123",
    "account": "123456789012",
    "time": "2019-05-30T17:40:30Z",
    "region": "us-west-2",
    "source": "aws.groundstation",
    "resources": [
        "arn:aws:groundstation:us-
west-2:123456789012:contact/11111111-1111-1111-1111-111111111111"
    ],
    "detailType": "Ground Station Contact State Change",
    "detail": {
        "contactId": "11111111-1111-1111-1111-111111111111",
        "groundstationId": "Ground Station 1",
        "missionProfileArn": "arn:aws:groundstation:us-west-2:123456789012:mission-
profile/11111111-1111-1111-1111-111111111111",
        "satelliteArn":
 "arn:aws:groundstation::123456789012:satellite/11111111-1111-1111-1111-111111111111",
        "contactStatus": "PASS"
```

```
    },
    "account": "123456789012"
}
```

Nilai yang mungkin untuk `contactStatus` didefinisikan dalamthe section called “Status Kontak Ground Station”.

Perubahan Status Grup Ground Station Dataflow Endpoint

Jika Anda ingin melakukan tindakan saat grup titik akhir aliran data Anda digunakan untuk menerima data, Anda dapat menyiapkan aturan untuk mengotomatiskan tindakan ini. Ini akan memungkinkan Anda untuk melakukan tindakan yang berbeda dalam menanggapi status perubahan status grup titik akhir dataflow. Jika Anda ingin mengubah saat menerima peristiwa ini, gunakan grup titik akhir aliran data dengan dan. contactPrePassDurationSecondscontactPostPassDurationSeconds Acara ini akan dikirim ke wilayah grup endpoint aliran data.

Contoh diberikan di bawah ini.

```
{
    "version": "0",
    "id": "01234567-0123-0123",
    "account": "123456789012",
    "time": "2019-05-30T17:40:30Z",
    "region": "us-west-2",
    "source": "aws.groundstation",
    "resources": [
        "arn:aws:groundstation:us-west-2:123456789012:dataflow-endpoint-
group/bad957a8-1d60-4c45-a92a-39febd98921d, arn:aws:groundstation:us-
west-2:123456789012:contact/98ddd10f-f2bc-479c-bf7d-55644737fb09,
 arn:aws:groundstation:us-west-2:123456789012:mission-profile/c513c84c-eb40-4473-88a2-
d482648c9234"
    ],
    "detailType": "Ground Station Dataflow Endpoint Group State Change",
    "detail": {
        "dataflowEndpointGroupId": "bad957a8-1d60-4c45-a92a-39febd98921d",
        "groundstationId": "Ground Station 1",
        "contactId": "98ddd10f-f2bc-479c-bf7d-55644737fb09",
        "dataflowEndpointGroupArn": "arn:aws:groundstation:us-
west-2:680367718957:dataflow-endpoint-group/bad957a8-1d60-4c45-a92a-39febd98921d",
        "missionProfileArn": "arn:aws:groundstation:us-west-2:123456789012:mission-
profile/c513c84c-eb40-4473-88a2-d482648c9234",
```

```
        "dataflowEndpointGroupState": "PREPASS"
    },
    "account": "123456789012"
}
```

Kemungkinan negara untuk `dataflowEndpointGroupState` memasukkan`PREPASS`,`PASS`,`POSTPASS`, dan`COMPLETED`.

Ground Station Perubahan Negara Ephemeris

Jika Anda ingin melakukan tindakan saat ephemeris mengubah status, Anda dapat mengatur aturan untuk mengotomatiskan tindakan ini. Ini memungkinkan Anda untuk melakukan tindakan yang berbeda sebagai respons terhadap keadaan perubahan ephemeris. Misalnya, Anda dapat melakukan tindakan ketika ephemeris telah menyelesaikan validasi, dan sekarang. `ENABLED` Pemberitahuan untuk acara ini akan dikirim ke wilayah jika ephemeris diunggah.

Contoh diberikan di bawah ini.

```
    {
    "id": "7bf73129-1428-4cd3-a780-95db273d1602",
    "detail-type": "Ground Station Ephemeris State Change",
    "source": "aws.groundstation",
    "account": "123456789012",
    "time": "2019-12-03T21:29:54Z",
    "region": "us-west-2",
    "resources": [
    "arn:aws:groundstation::123456789012:satellite/10313191-c9d9-4ecb-a5f2-
bc55cab050ec",
    "arn:aws:groundstation::123456789012:ephemeris/111111-cccc-bbbb-a555-bcccca005000",
    ],
    "detail": {
    "ephemerisStatus": "ENABLED",
    "ephemerisId": "111111-cccc-bbbb-a555-bcccca005000",
    "satelliteId": "10313191-c9d9-4ecb-a5f2-bc55cab050ec"
    }
    }
```

Kemungkinan negara untuk `ephemerisStatus` memasukkan`ENABLED`,`VALIDATING`,`INVALID`,`ERROR`,`DISABLED`, `EXPIRED`

Pencatatan Panggilan AWS Ground Station API dengan AWS CloudTrail

AWS Ground Station terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di AWS Ground Station. CloudTrail menangkap semua panggilan API untuk AWS Ground Station sebagai peristiwa. Panggilan yang diambil termasuk panggilan dari AWS Ground Station konsol dan panggilan kode ke operasi AWS Ground Station API. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara berkelanjutan ke bucket Amazon S3, termasuk acara untuk. AWS Ground Station Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat AWS Ground Station, alamat IP dari mana permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Untuk mempelajari selengkapnya CloudTrail, lihat Panduan AWS CloudTrail Pengguna.

AWS Ground Station Informasi di CloudTrail

CloudTrail diaktifkan di AWS akun Anda saat Anda membuat akun. Ketika aktivitas terjadi di AWS Ground Station, aktivitas tersebut dicatat dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh acara terbaru di AWS akun Anda. Untuk informasi selengkapnya, lihat Melihat Acara dengan Riwayat CloudTrail Acara.

Untuk catatan peristiwa yang sedang berlangsung di AWS akun Anda, termasuk acara untuk AWS Ground Station, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Secara default, ketika Anda membuat jejak di konsol tersebut, jejak tersebut diterapkan ke semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di AWS partisi dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat berikut:

- Gambaran umum untuk Membuat Jejak
- CloudTrail Layanan dan Integrasi yang Didukung
- Mengonfigurasi Notifikasi Amazon SNS untuk CloudTrail
- Menerima File CloudTrail Log dari Beberapa Wilayah dan Menerima File CloudTrail Log dari Beberapa Akun

Semua AWS Ground Station tindakan dicatat oleh CloudTrail dan didokumentasikan dalam Referensi AWS Ground Station API. Misalnya, panggilan ke`ReserveContact`, `CancelContact` dan `ListConfigs` tindakan menghasilkan entri dalam file CloudTrail log.

Setiap peristiwa atau entri log berisi informasi tentang siapa yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan berikut:

- Apakah permintaan itu dibuat dengan kredensyal pengguna root atau AWS Identity and Access Management (IAM).
- Apakah permintaan dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna gabungan.
- Apakah permintaan itu dibuat oleh AWS layanan lain.

Untuk informasi selengkapnya, lihat Elemen CloudTrail UserIdentity.

Memahami Entri File AWS Ground Station Log

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Peristiwa mewakili permintaan tunggal dari sumber manapun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, jadi file tersebut tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan `ReserveContact` tindakan.

Contoh: ReserveContact

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINICIPLE_ID",
        "arn": "arn:aws:sts::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
```

```
                "creationDate": "2019-05-15T21:11:59Z"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EX_PRINICIPLE_ID",
                "arn": "arn:aws:iam::123456789012:role/Alice",
                "accountId": "123456789012",
                "userName": "Alice"
            }
        }
    },
    "eventTime": "2019-05-15T21:14:37Z",
    "eventSource": "groundstation.amazonaws.com",
    "eventName": "ReserveContact",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "127.0.0.1",
    "userAgent": "Coral/Jakarta",
    "requestParameters": {
        "satelliteArn":
 "arn:aws:groundstation::123456789012:satellite/11111111-2222-3333-4444-555555555555",
        "groundStation": "Ohio 1",
        "startTime": 1558356107,
        "missionProfileArn": "arn:aws:groundstation:us-east-2:123456789012:mission-
profile/11111111-2222-3333-4444-555555555555",
        "endTime": 1558356886
    },
    "responseElements": {
        "contactId": "11111111-2222-3333-4444-555555555555"
    },
    "requestID": "11111111-2222-3333-4444-555555555555",
    "eventID": "11111111-2222-3333-4444-555555555555",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "11111111-2222-3333-4444-555555555555"
}
```


Metrik dengan Amazon CloudWatch

Selama kontak, AWS Ground Station secara otomatis menangkap dan mengirim data CloudWatch untuk analisis. Data Anda dapat dilihat pada grafik atau sebagai kode sumber di CloudWatch konsol Amazon. Untuk informasi selengkapnya tentang mengakses dan CloudWatch Metrik, lihat Menggunakan Metrik Amazon CloudWatch .

AWS Ground Station Metrik dan Dimensi

Metrik apa yang tersedia?

Metrik berikut tersedia dari AWS Ground Station.

Metrik	Deskripsi
`AzimuthAngle`	Sudut azimuth antena. Utara sejati adalah 0 derajat dan timur 90 derajat. Unit: derajat
`BitErrorRate`	Tingkat kesalahan pada bit dalam jumlah transmisi bit tertentu. Kesalahan bit disebabkan oleh kebisinga n, distorsi, atau gangguan Unit: Kesalahan bit per satuan waktu
`BlockErrorRate`	Tingkat kesalahan blok dalam jumlah tertentu dari blok yang diterima. Kesalahan blok disebabkan oleh interferensi. Unit: Blok yang salah/Jumlah total blok
`CarrierFrequencyRecovery_Cn0`	Rasio kepadatan pembawa terhadap kebisingan per unit bandwidth. Satuan: Desibel-Hertz (dB-Hz)
`CarrierFrequencyRecovery_Lo cked`	Atur ke 1 saat loop pemulihan frekuensi pembawa demodulator terkunci dan 0 saat dibuka kuncinya. Unit: tanpa unit
`CarrierFrequencyRecovery_Of fsetFrequency_Hz`	Offset antara pusat sinyal yang diperkirakan dan frekuensi pusat ideal. Hal ini disebabkan oleh pergeseran Doppler dan offset osilator lokal antara pesawat ruang angkasa dan sistem antena.

Metrik	Deskripsi
	Satuan: hertz (Hz)
`ElevationAngle`	Sudut elevasi antena. Cakrawala adalah 0 derajat dan zenith adalah 90 derajat. Unit: derajat
`Es/N0`	Rasio energi per simbol terhadap kerapatan spektral daya kebisingan. Unit: desibel (dB)
`ReceivedPower`	Kekuatan sinyal yang diukur dalam demodulator/decoder. Satuan: desibel relatif terhadap miliwatt (dBm)
`SymbolTimingRecovery_ErrorVectorMagnitude`	Besarnya vektor kesalahan antara simbol yang diterima dan titik konstelasi ideal. Unit: persen
`SymbolTimingRecovery_Locked`	Setel ke 1 saat loop pemulihan waktu simbol demodulator terkunci dan 0 saat dibuka Unit: tanpa unit
`SymbolTimingRecovery_OffsetSymbolRate`	Offset antara perkiraan tingkat simbol dan tingkat simbol sinyal ideal. Hal ini disebabkan oleh pergeseran Doppler dan offset osilator lokal antara pesawat ruang angkasa dan sistem antena. Unit: simbol/detik

Dimensi apa yang digunakan AWS Ground Station?

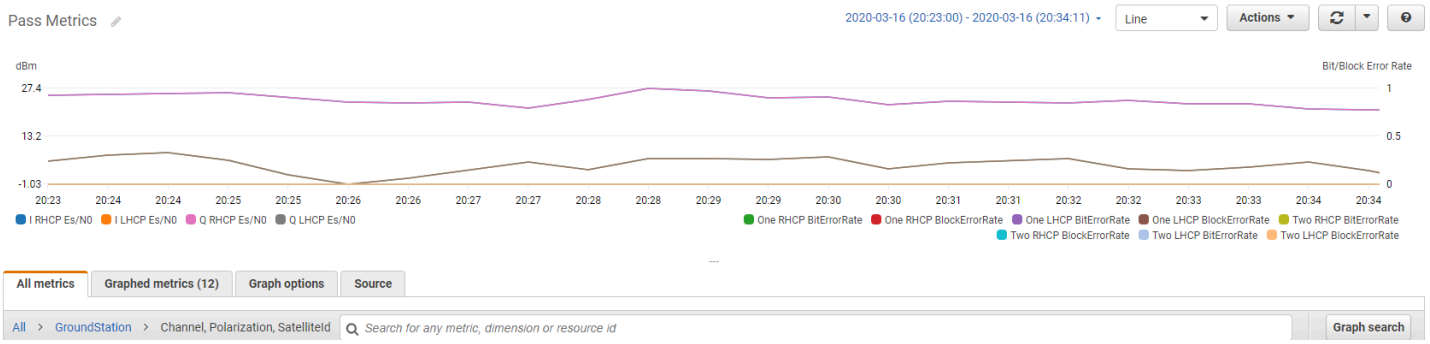
Anda dapat memfilter AWS Ground Station data menggunakan dimensi berikut.

Dimensi	Deskripsi
`Channel`	Saluran untuk setiap kontak termasuk Satu, Dua, I (dalam fase), dan Q (kuadratur).
`Polarization`	Polarisasi untuk setiap kontak termasuk LHCP (Left Hand Circular Polarized) atau RHCP (Tangan Kanan Circular Polarized).
`SatelliteId`	ID satelit berisi ARN satelit untuk kontak Anda.

Melihat metrik

Saat melihat metrik grafik, penting untuk dicatat bahwa jendela agregasi menentukan bagaimana metrik Anda akan ditampilkan. Setiap metrik dalam kontak dapat ditampilkan sebagai data per detik selama 3 jam setelah data diterima. Data Anda akan dikumpulkan oleh CloudWatch Metrik sebagai data per menit setelah periode 3 jam berlalu. Jika Anda perlu melihat metrik pada pengukuran data per detik, disarankan untuk melihat data Anda dalam periode 3 jam setelah data diterima atau disimpan di luar Metrik. CloudWatch

Selain itu, data apa pun yang diambil dalam 60 detik pertama tidak akan berisi informasi yang cukup untuk menghasilkan metrik yang berarti, dan kemungkinan tidak akan ditampilkan. Untuk melihat metrik yang bermakna, disarankan untuk melihat data Anda setelah 60 detik berlalu.

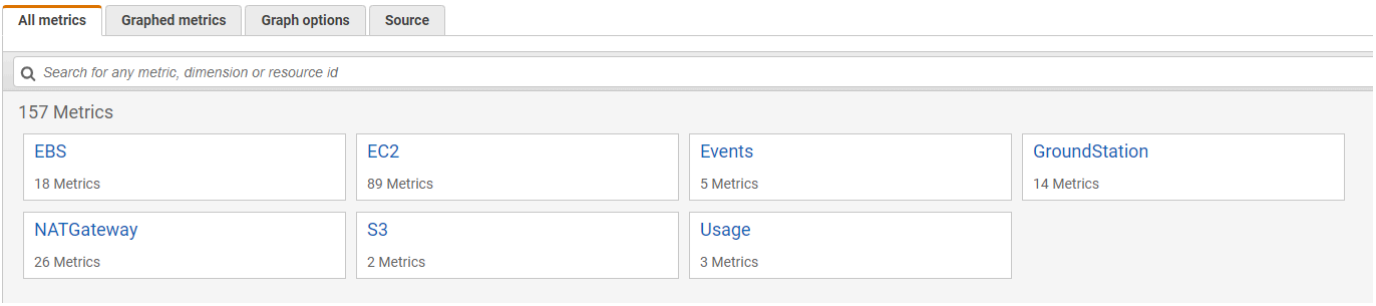


Untuk informasi selengkapnya tentang AWS Ground Station metrik grafik CloudWatch, lihat Metrik Grafik.

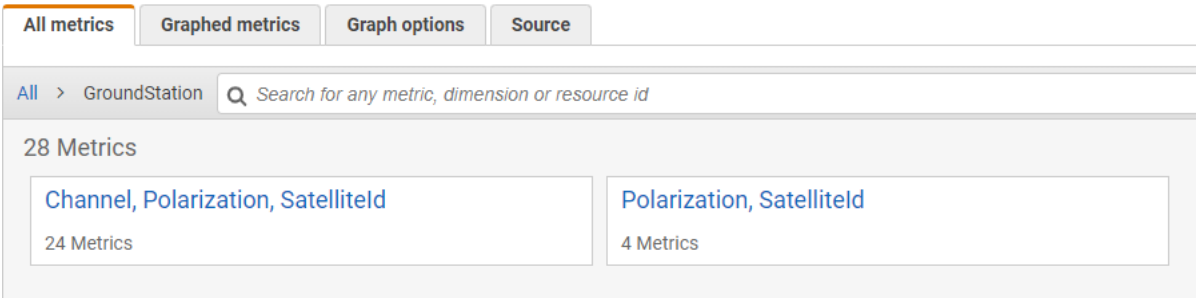
Untuk melihat metrik menggunakan konsol

1. Buka konsol CloudWatch .

2. Pada panel navigasi, silakan pilih Metrik.
3. Pilih GroundStationnamespace.



4. Pilih dimensi metrik yang Anda inginkan (misalnya, Saluran, Polarisasi,. SatelliteId



5. Tab Semua metrik menampilkan semua metrik dimensi tersebut di namespace. Anda dapat melakukan hal berikut:

   a. Untuk menyortir tabel, gunakan judul kolomnya.

   b. Untuk membuat grafik metrik, pilih kotak centang yang terkait dengan metrik. Untuk memilih semua metrik, pilih kotak centang di baris judul tabel.

   c. Untuk menyaring berdasarkan sumber daya, pilih ID sumber daya, kemudian pilih Tambahkan ke pencarian.

   d. Untuk menyaring berdasarkan metrik, pilih nama metrik, kemudian pilih Tambahkan ke pencarian.

Untuk melihat metrik menggunakan AWS CLI

1. Pastikan AWS CLI sudah terpasang. Untuk informasi tentang penginstalan AWS CLI, lihat Menginstal AWS CLI.
2. Buat file JSON konfigurasi CloudWatch agen. Untuk petunjuk cara membuat file konfigurasi CloudWatch agen, lihat Membuat File Konfigurasi CloudWatch Agen.

3. Buat daftar CloudWatch metrik yang tersedia dengan menjalankan`aws cloudwatch list-metrics`.
4. Ubah file JSON yang Anda buat di langkah 2 agar sesuai dengan metrik `SatellitID` dari Anda.

> **Note**
>
> Jangan mengurangi `Period` bidang ke nilai di bawah 60. AWS Ground Station menerbitkan metrik setiap 60 detik dan tidak ada metrik yang akan dikembalikan jika nilainya dikurangi.

5. Jalankan `aws cloudwatch get-metric-data` dengan periode waktu pass Anda dan file JSON konfigurasi CloudWatch agen Anda. Contoh diberikan di bawah ini.

```
aws cloudwatch get-metrics-data –start-time 2020-02-26T19:12:00Z –end-time
 2020-02-26T19:24:00Z –metric-data-queries file://metricdata.json
```

Metrik akan diberikan stempel waktu dari kontak Anda. Contoh keluaran AWS Ground Station metrik disediakan di bawah ini.

```
{
      “MetricDataResults”: [
          {
              “Id”: “myQuery”,
              “Label”: “Es/N0”,
              “Timestamps”: [
                  “2020-02-18T19:44:00Z”,
                  “2020-02-18T19:43:00Z”,
                  “2020-02-18T19:42:00Z”,
                  “2020-02-18T19:41:00Z”,
                  “2020-02-18T19:40:00Z”,
                  “2020-02-18T19:39:00Z”,
                  “2020-02-18T19:38:00Z”,
                  “2020-02-18T19:37:00Z”,
              ],
              “Values”: [
                  24.58344556958329,
                  24.251638725562216,
                  22.919391450230158,
                  22.83838908204037,
                  23.303086848486842,
```

```
                    22.845261784583364,
                    21.34531397048953,
                    19.171561698261222
                ],
                “StatusCode”: “Complete”
            }
        ]
        “Messages”: []
}
```

Pemecahan Masalah

Dokumentasi berikut dapat membantu Anda memecahkan masalah yang dapat mencegah AWS Ground Station kontak berhasil diselesaikan.

Topik

Memecahkan Masalah Kontak yang Mengirimkan Data ke Amazon EC2

Jika Anda tidak berhasil menyelesaikan AWS Ground Station kontak, Anda perlu memverifikasi bahwa instans Amazon EC2 Anda berjalan, memverifikasi bahwa Pembela Data sedang berjalan, dan memverifikasi bahwa aliran Pembela Data Anda dikonfigurasi dengan benar.

Prasyarat

Prosedur berikut mengasumsikan bahwa instans Amazon EC2 sudah disiapkan. Untuk menyiapkan instans Amazon EC2 di AWS Ground Station, lihat Memulai.

Langkah 1: Verifikasi bahwa Instans EC2 Anda Berjalan

1. Temukan instans Amazon EC2 yang digunakan untuk kontak yang sedang Anda atasi masalah. Gunakan langkah-langkah berikut:

   a. Di CloudFormationdasbor Anda, pilih tumpukan yang berisi instans Amazon EC2 Anda.

   b. Pilih tab Sumber Daya dan temukan instans Amazon EC2 Anda di kolom Logical ID. Verifikasi bahwa instance dibuat di kolom Status.

   c. Di kolom ID Fisik, pilih tautan untuk instans Amazon EC2 Anda. Ini akan membawa Anda ke konsol manajemen Amazon EC2.

2. Di konsol manajemen Amazon EC2, pastikan Status Instans Amazon EC2 Anda berjalan.

3. Jika instans Anda berjalan, lanjutkan ke langkah berikutnya. Jika instans Anda tidak berjalan, mulai instance dengan menggunakan langkah berikut:

   - Dengan memilih instans Amazon EC2, pilih Tindakan > Status Instans > Mulai.

Langkah 2: Tentukan Jenis Aplikasi Dataflow yang Digunakan

Jika Anda menggunakan AWS Ground Station Agen untuk pengiriman data, silakan alihkan ke bagian Agen Pemecahan Masalah AWS Ground Station.

Jika tidak, jika Anda menggunakan aplikasi Data Defender (DDX) terus. the section called “Langkah 3: Verifikasi bahwa Pembela Data Berjalan”

Langkah 3: Verifikasi bahwa Pembela Data Berjalan

Memverifikasi status Pembela Data mengharuskan Anda untuk terhubung ke instans di Amazon EC2. Untuk detail selengkapnya tentang menghubungkan ke instans Anda, lihat Connect to Your Linux Instance.

Prosedur berikut menyediakan langkah-langkah pemecahan masalah menggunakan perintah dalam klien SSH.

1. Buka terminal atau prompt perintah dan sambungkan ke instans Amazon EC2 Anda menggunakan SSH. Teruskan port 80 dari host jarak jauh untuk melihat UI web Pembela Data. Perintah berikut menunjukkan cara menggunakan SSH untuk terhubung ke instans Amazon EC2 melalui benteng dengan port forwarding diaktifkan.

   > **Note**
   >
   > Anda harus mengganti<SSH KEY>,<BASTION HOST>, dan <HOST>dengan kunci ssh spesifik, nama host bastion, dan nama host instans Amazon EC2.

   Untuk Windows

   ```
   ssh -L 8080:localhost:80 -o ProxyCommand="C:\Windows\System32\OpenSSH\ssh.exe -o
    \"ForwardAgent yes\" -W %h:%p -i \"<SSH KEY>\" ec2-user@<BASTION HOST>" -i "<SSH
    KEY>" ec2-user@<HOST>
   ```

Untuk Mac

```
ssh -L 8080:localhost:80 -o ProxyCommand="ssh -A -o 'ForwardAgent yes' -W %h:%p -i
 <SSH KEY> ec2-user@<BASTION HOST>" -i <SSH  KEY> ec2-user@<HOST>
```

2. Verifikasi bahwa Data Defender (juga disebut DDX) berjalan dengan mengambil (memeriksa) untuk proses yang berjalan bernama ddx dalam output. Perintah untuk grepping (memeriksa) untuk proses yang berjalan dan output contoh yang berhasil disediakan di bawah ini.

```
[ec2-user@Receiver-Instance ~]$ ps -ef | grep ddx
Rtlogic   4977      1 10 Oct16 ?        2-00:22:14 /opt/rtlogic/ddx/bin/ddx -m/
opt/rtlogic/ddx/modules -p/opt/rtlogic/ddx/plugins -c/opt/rtlogic/ddx/bin/ddx.xml -
umask=077 -daemon -f installed=true -f security=true -f enable HttpsForwarding=true
Ec2-user 18787 18657  0 16:51 pts/0      00:00:00 grep -color=auto ddx
```

Jika Pembela Data sedang berjalan, lewati ke the section called “Langkah 4: Verifikasi bahwa Aliran Pembela Data Anda Dikonfigurasi” Jika tidak, lanjutkan ke langkah berikutnya.

3. Mulai Data Defender menggunakan perintah tampilkan di bawah ini.

```
sudo service rtlogic-ddx start
```

Jika Data Defender berjalan setelah menggunakan perintah, lewati ke the section called “Langkah 4: Verifikasi bahwa Aliran Pembela Data Anda Dikonfigurasi” Jika tidak, lanjutkan ke langkah berikutnya.

4. Periksa file berikut menggunakan perintah di bawah ini untuk melihat apakah ada kesalahan saat menginstal dan mengkonfigurasi Data Defender.

```
cat /var/log/user-data.log
cat /opt/aws/groundstation/.startup.out
```

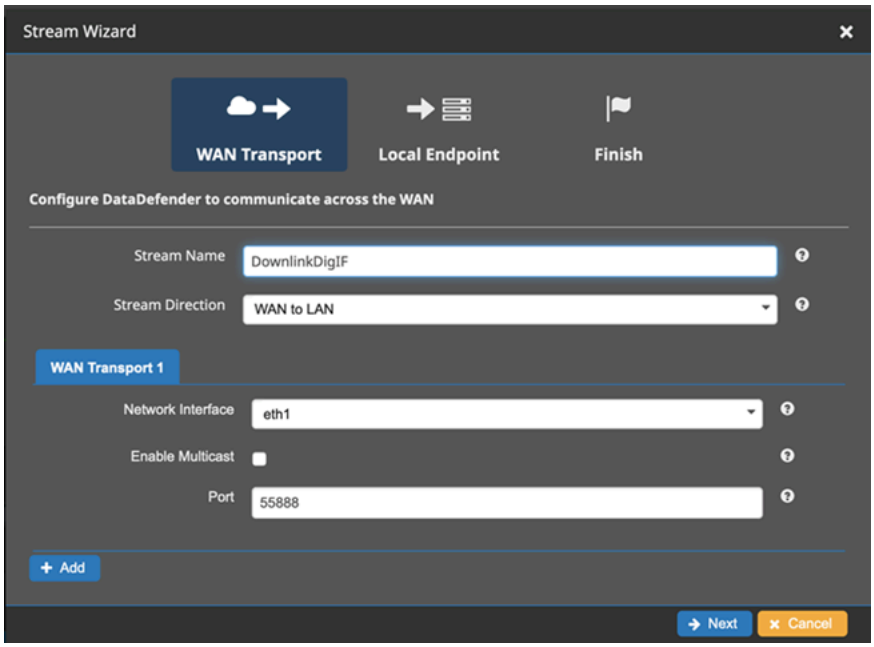
> **Note**
>
> Masalah umum yang ditemukan saat memeriksa file-file ini adalah bahwa VPC Amazon tempat instans Amazon EC2 Anda berjalan tidak memiliki akses ke Amazon S3 untuk mengunduh file instalasi. Jika Anda menemukan di log Anda bahwa ini adalah

masalahnya, periksa pengaturan Amazon VPC dan grup keamanan instans EC2 Anda untuk memastikan mereka tidak memblokir akses ke Amazon S3.

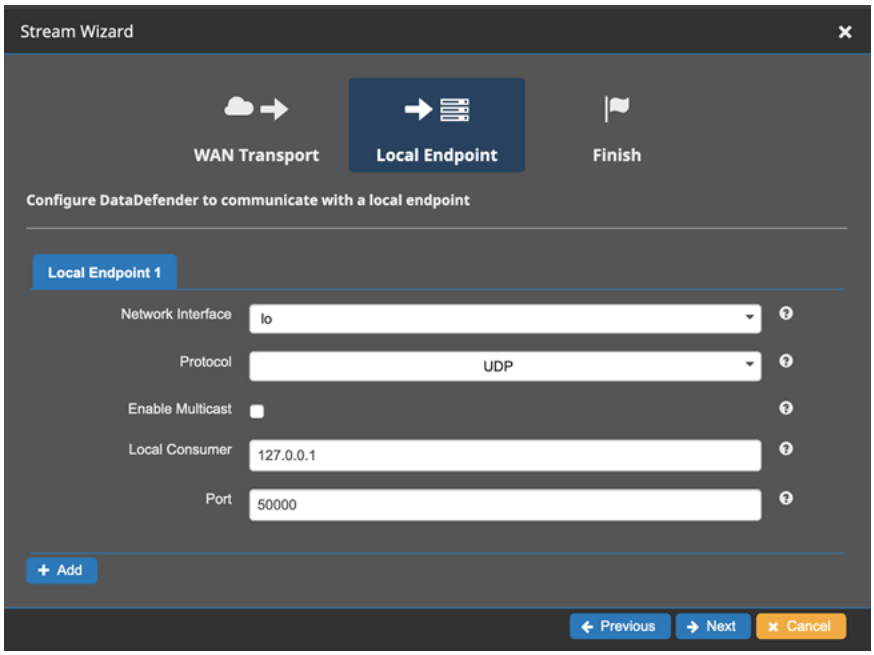
Jika Data Defender berjalan setelah memeriksa pengaturan VPC Amazon Anda, lanjutkan ke. the section called “Langkah 4: Verifikasi bahwa Aliran Pembela Data Anda Dikonfigurasi” Jika masalah berlanjut, hubungi AWS Support dan kirim file log Anda dengan deskripsi masalah Anda.

Langkah 4: Verifikasi bahwa Aliran Pembela Data Anda Dikonfigurasi

1. Di browser web, akses Antarmuka Pengguna Web DDX Anda dengan memasukkan alamat berikut di bilah alamat: localhost:8080. Kemudian, tekan Enter.
2. Di DataDefenderdasbor, pilih Buka Detail.
3. Pilih aliran Anda dari daftar aliran, dan pilih Edit Stream.
4. Di kotak dialog Stream Wizard, lakukan hal berikut:
   a. Di panel Transportasi WAN, pastikan WAN ke LAN dipilih untuk Arah Aliran.
   b. Di kotak Port, pastikan port WAN yang Anda pilih untuk grup endpoint aliran data Anda ada. Secara default, port ini adalah 55888. Lalu, pilih Selanjutnya.



c. Di panel Endpoint Lokal, pastikan port yang valid ada di kotak Port. Secara default, port ini adalah 50000. Ini adalah port tempat Anda akan menerima data Anda setelah Data Defender menerimanya dari AWS Ground Station layanan. Lalu, pilih Selanjutnya.



d. Pilih Selesai di menu yang tersisa jika Anda telah mengubah nilai apa pun. Jika tidak, Anda dapat membatalkan menu Stream Wizard.

Anda sekarang telah memastikan bahwa instans Amazon EC2 dan Data Defender berjalan dan dikonfigurasi dengan benar untuk menerima data. AWS Ground Station Jika Anda terus mengalami masalah, hubungi AWS Support.

Status Kontak Ground Station

Status AWS Ground Station kontak memberikan wawasan tentang apa yang terjadi pada kontak itu pada waktu tertentu.

Status Kontak

Berikut ini adalah daftar status yang dapat dimiliki kontak:

- TERSEDIA - Kontak tersedia untuk dipesan.
- PENJADWALAN - Kontak sedang dalam proses penjadwalan.
- DIJADWALKAN - Kontak berhasil dijadwalkan.

- FAILED_TO_SCHEDULE - Kontak gagal menjadwalkan.
- PREPASS - Kontak akan segera dimulai dan sumber daya sedang dipersiapkan.
- PASS - Kontak saat ini sedang dijalankan dan satelit sedang dikomunikasikan.
- POSTPASS - Komunikasi telah selesai dan sumber daya yang digunakan sedang dibersihkan.
- SELESAI - Kontak berhasil diselesaikan.
- GAGAL - Kontak gagal karena masalah dengan konfigurasi sumber daya pelanggan.
- AWS_FAILED - Kontak gagal karena masalah dalam layanan. AWS Ground Station
- PEMBATALAN - Kontak sedang dalam proses dibatalkan.
- AWS_CANCELLED - Kontak dibatalkan oleh layanan. AWS Ground Station Antena atau pemeliharaan situs adalah salah satu contoh kapan ini bisa terjadi.
- DIBATALKAN - Kontak dibatalkan oleh pelanggan.

Panduan Pemecahan Masalah

- the section called “Pemecahan Masalah Kontak GAGAL”
- the section called “Pemecahan Masalah Kontak FALED_TO_SCHEDULE”

Pemecahan Masalah Kontak GAGAL

Kontak akan memiliki status kontak terminal FAILED ketika AWS Ground Station mendeteksi masalah dengan konfigurasi sumber daya pelanggan. Kasus penggunaan umum yang dapat menyebabkan kontak GAGAL disediakan di bawah ini, bersama dengan langkah-langkah untuk membantu memecahkan masalah.

> **Note**
>
> Panduan ini khusus untuk status kontak GAGAL - dan tidak ditujukan untuk status kegagalan lainnya, seperti AWS_FAILED, AWS_CANCELLED, atau FAILED_TO_SCHEDULE. Untuk informasi selengkapnya tentang status kontak, lihat the section called “Status Kontak Ground Station”

Data Defender (DDX) GAGAL Menggunakan Kasus

Berikut ini adalah daftar kasus penggunaan umum yang dapat mengakibatkan status kontak GAGAL untuk aliran data berbasis DDX:

- Pelanggan DDX Never Connects - Koneksi DDX antara AWS Ground Station Antena dan Customer Dataflow Endpoint Group untuk satu atau lebih aliran data tidak pernah dibuat.
- Pelanggan DDX Connects Late - Koneksi DDX antara AWS Ground Station Antena dan Customer Dataflow Endpoint Group untuk satu atau lebih aliran data dibuat setelah waktu mulai kontak.

Untuk kasus kegagalan aliran data DDX, disarankan untuk melihat hal-hal berikut:

- Konfirmasikan instans Amazon EC2 penerima berhasil dimulai, sebelum waktu mulai kontak.
- Konfirmasikan DDX aktif dan berjalan selama kontak.

Lihat bagian the section called “Memecahkan Masalah Kontak yang Mengirimkan Data ke Amazon EC2” untuk langkah-langkah pemecahan masalah yang lebih spesifik.

AWS Ground Station Agen GAGAL Menggunakan Kasus

Berikut ini adalah daftar kasus penggunaan umum yang dapat mengakibatkan status kontak GAGAL untuk aliran data berbasis Agen:

- Agen Pelanggan Tidak Pernah Melaporkan Status - Agen yang bertanggung jawab untuk mengatur pengiriman data pada Grup Titik Akhir Dataflow Pelanggan untuk satu atau lebih aliran data tidak pernah berhasil melaporkan status ke. AWS Ground Station Pembaruan status ini akan terjadi dalam beberapa detik dari waktu akhir kontak.
- Agen Pelanggan Mulai Terlambat - Agen yang bertanggung jawab untuk mengatur pengiriman data pada Grup Titik Akhir Dataflow Pelanggan untuk satu atau lebih aliran data dimulai terlambat, setelah waktu mulai kontak.

Untuk kasus kegagalan aliran data AWS Ground Station Agen, disarankan untuk melihat hal-hal berikut:

- Konfirmasikan instans Amazon EC2 penerima berhasil dimulai, sebelum waktu mulai kontak.
- Konfirmasikan aplikasi Agen sudah aktif dan berjalan di awal dan selama kontak.

- Konfirmasikan aplikasi Agen dan instans Amazon EC2 tidak dimatikan dalam waktu 15 detik setelah kontak berakhir. Ini memberi Agen waktu yang cukup untuk melaporkan status ke AWS Ground Station.

Lihat bagian the section called “Memecahkan Masalah Kontak yang Mengirimkan Data ke Amazon EC2” untuk langkah-langkah pemecahan masalah yang lebih spesifik.

Pemecahan Masalah Kontak FALED_TO_SCHEDULE

Kontak akan FAILED_TO_SCHEDULE ketika AWS Ground Station mendeteksi masalah baik dengan konfigurasi sumber daya pelanggan atau dalam sistem internal. Kontak yang berakhir dengan status FAILED_TO_SCHEDULE secara opsional akan menyediakan konteks tambahan untuk. `errorMessage` Untuk informasi tentang menjelaskan kontak, lihatthe section called “Jelaskan Kontak dengan AWS CLI”.

Kasus penggunaan umum yang dapat menyebabkan kontak FAILED_TO_SCHEDULE disediakan di bawah ini, bersama dengan langkah-langkah untuk membantu memecahkan masalah.

> **Note**
>
> Panduan ini khusus untuk status kontak FAILED_TO_SCHEDULE - dan tidak ditujukan untuk status kegagalan lainnya, seperti AWS_FAILED, AWS_CANCELLED, atau FAILED. Untuk informasi selengkapnya tentang status kontak, lihat the section called “Status Kontak Ground Station”

Pengaturan yang ditentukan dalam Antenna Downlink Demod Decode Config tidak didukung

Profil misi yang digunakan untuk menjadwalkan kontak ini memiliki antenna-downlink-demod-decode konfigurasi yang tidak valid.

AntennaDownlinkDemodDecode Konfigurasi yang sudah ada sebelumnya

- Jika antenna-downlink-demod-decode konfigurasi Anda baru saja diubah - putar kembali ke versi yang sebelumnya berfungsi sebelum mencoba menjadwalkan.

- Jika ini adalah perubahan yang disengaja pada konfigurasi yang ada, atau konfigurasi yang sudah ada sebelumnya yang tidak lagi berhasil menjadwalkan - ikuti langkah berikutnya tentang cara mengaktifkan konfigurasi baru. AntennaDownlinkDemodDecode

AntennaDownlinkDemodDecode Konfigurasi yang baru dibuat

Hubungi AWS Ground Station langsung ke onboard konfigurasi baru Anda. Buat kasus dengan AWS Support termasuk `contactId` yang diakhiri dengan status FAILED_TO_SCHEDULE

Langkah Pemecahan Masalah Umum

Jika langkah pemecahan masalah sebelumnya tidak menyelesaikan masalah Anda:

- Coba kembali penjadwalan kontak atau jadwalkan kontak lain menggunakan profil misi yang sama. Lihat the section called “Reservasi Kontak dengan AWS CLI”.
- Jika Anda terus menerima status FAILED_TO_SCHEDULE untuk profil misi ini, hubungi AWS Support

Keamanan di AWS Ground Station

Keamanan cloud di AWS merupakan prioritas tertinggi. Sebagai pelanggan AWS, Anda akan mendapatkan manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan. AWS menyediakan alat dan fitur khusus keamanan untuk membantu Anda memenuhi tujuan keamanan Anda. Alat dan fitur ini mencakup keamanan jaringan, manajemen konfigurasi, kontrol akses, dan keamanan data.

Saat menggunakanAWS Ground Station, kami sarankan Anda mengikuti praktik terbaik industri dan menerapkan end-to-end enkripsi. AWS menyediakan API bagi Anda untuk mengintegrasikan enkripsi dan perlindungan data. Untuk informasi lebih lanjut tentangAWS keamanan, lihat AWS Security.

Gunakan topik berikut untuk mempelajari cara mengamankan sumber daya Anda.

Topik

- Identity and Access Management untuk AWS Ground Station
- Menggunakan peran terkait layanan untuk Ground Station
- Kebijakan terkelola AWS untuk AWS Ground Station

Identity and Access Management untuk AWS Ground Station

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. AWS Ground Station IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

- Audiens
- Mengautentikasi dengan identitas
- Mengelola akses menggunakan kebijakan
- Bagaimana AWS Ground Station bekerja dengan IAM
- Contoh kebijakan berbasis identitas untuk AWS Ground Station

- Memecahkan masalah AWS Ground Station identitas dan akses

Audiens

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

Pengguna layanan — Jika Anda menggunakan AWS Ground Station layanan untuk melakukan pekerjaan Anda, maka administrator Anda memberi Anda kredensi dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak AWS Ground Station 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 AWS Ground Station, lihat Memecahkan masalah AWS Ground Station identitas dan akses.

Administrator layanan — Jika Anda bertanggung jawab atas AWS Ground Station sumber daya di perusahaan Anda, Anda mungkin memiliki akses penuh ke AWS Ground Station. Tugas Anda adalah menentukan AWS Ground Station 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 AWS Ground Station, lihatBagaimana AWS Ground Station 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 AWS Ground Station. Untuk melihat contoh kebijakan AWS Ground Station berbasis identitas yang dapat Anda gunakan di IAM, lihat. Contoh kebijakan berbasis identitas untuk AWS Ground Station

Mengautentikasi dengan identitas

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

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

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensil Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. 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 kredensil yang disediakan melalui sumber identitas. Ketika identitas federasi mengakses Akun AWS, mereka mengambil peran, dan peran memberikan kredensi sementara.

Untuk manajemen akses terpusat, kami sarankan Anda menggunakan AWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat Identitas IAM, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua aplikasi Akun AWS dan aplikasi Anda. Untuk informasi tentang Pusat Identitas IAM, lihat Apakah itu Pusat Identitas IAM? dalam Panduan Pengguna AWS IAM Identity Center .

Pengguna dan grup IAM

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

Grup IAM adalah identitas yang menentukan sekumpulan pengguna IAM. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat 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 AWS Ground Station bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses AWS Ground Station, pelajari fitur IAM yang tersedia untuk digunakan. AWS Ground Station

Fitur IAM yang dapat Anda gunakan AWS Ground Station

Fitur IAM	AWS Ground Station dukungan
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
kunci-kunci persyaratan kebijakan (spesifik layanan)	Ya
ACL	Tidak
ABAC (tanda dalam kebijakan)	Ya
Kredensial sementara	Ya
Izin prinsipal	Ya
Peran layanan	Tidak
Peran terkait layanan	Ya

Untuk mendapatkan tampilan tingkat tinggi tentang cara AWS Ground Station 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 AWS Ground Station

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 AWS Ground Station

Untuk melihat contoh kebijakan AWS Ground Station berbasis identitas, lihat. Contoh kebijakan berbasis identitas untuk AWS Ground Station

Kebijakan berbasis sumber daya dalam AWS Ground Station

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 AWS Ground Station

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.

Untuk melihat daftar AWS Ground Station tindakan, lihat Tindakan yang ditentukan oleh AWS Ground Station dalam Referensi Otorisasi Layanan.

Tindakan kebijakan AWS Ground Station menggunakan awalan berikut sebelum tindakan:

```
groundstation
```

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

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

Untuk melihat contoh kebijakan AWS Ground Station berbasis identitas, lihat. Contoh kebijakan berbasis identitas untuk AWS Ground Station

Sumber daya kebijakan untuk AWS Ground Station

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 daftar jenis AWS Ground Station sumber daya dan ARNnya, lihat Sumber daya yang ditentukan oleh AWS Ground Station dalam Referensi Otorisasi Layanan. Untuk mempelajari tindakan yang dapat menentukan ARN setiap sumber daya, lihat Tindakan yang ditentukan AWS Ground Station.

Untuk melihat contoh kebijakan AWS Ground Station berbasis identitas, lihat. Contoh kebijakan berbasis identitas untuk AWS Ground Station

Kunci kondisi kebijakan untuk AWS Ground Station

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 daftar kunci AWS Ground Station kondisi, lihat Kunci kondisi untuk AWS Ground Station dalam Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat Tindakan yang ditentukan oleh AWS Ground Station.

Untuk melihat contoh kebijakan AWS Ground Station berbasis identitas, lihat. Contoh kebijakan berbasis identitas untuk AWS Ground Station

ACL di AWS Ground Station

Mendukung ACL	Tidak

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

ABAC dengan AWS Ground Station

Mendukung ABAC (tanda dalam kebijakan)	Ya

Kontrol akses berbasis atribut (ABAC) adalah strategi otorisasi yang menentukan izin berdasarkan atribut. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke banyak AWS sumber daya. Penandaan ke entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian rancanglah kebijakan ABAC untuk mengizinkan operasi ketika tag milik prinsipal cocok dengan tag yang ada di sumber daya yang ingin diakses.

ABAC sangat berguna di lingkungan yang berkembang dengan cepat dan berguna di situasi saat manajemen kebijakan menjadi rumit.

Untuk mengendalikan akses berdasarkan tag, berikan informasi tentang tag di elemen kondisi dari kebijakan menggunakan kunci kondisi `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi untuk hanya beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi selengkapnya tentang ABAC, lihat Apa itu ABAC? dalam Panduan Pengguna IAM. Untuk melihat tutorial yang menguraikan langkah-langkah pengaturan ABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) dalam Panduan Pengguna IAM.

Menggunakan kredensyal sementara dengan AWS Ground Station

Mendukung penggunaan kredensial sementara	Ya

Beberapa Layanan AWS tidak berfungsi saat Anda masuk menggunakan kredensyal 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 kredensi sementara. Anda juga akan secara otomatis membuat kredensial sementara ketika Anda masuk ke konsol sebagai seorang pengguna lalu beralih peran. Untuk informasi selengkapnya tentang peralihan peran, lihat Peralihan peran (konsol) dalam Panduan Pengguna IAM.

Anda dapat membuat kredensyal sementara secara manual menggunakan API AWS CLI atau AWS . Anda kemudian dapat menggunakan kredensyal sementara tersebut untuk mengakses.

AWS AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensi sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensial keamanan sementara di IAM.

Izin utama lintas layanan untuk AWS Ground Station

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 AWS Ground Station

Mendukung peran layanan	Tidak

Peran layanan adalah sebuah 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 AWS Ground Station fungsionalitas. Edit peran layanan hanya jika AWS Ground Station memberikan panduan untuk melakukannya.

Peran terkait layanan untuk AWS Ground Station

Mendukung peran terkait layanan	Ya

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 pembuatan atau manajemen peran terkait layanan, lihat Layanan AWS yang berfungsi 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 AWS Ground Station

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi AWS Ground Station 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 menggunakan contoh dokumen kebijakan JSON ini, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh AWS Ground Station, termasuk format ARN untuk setiap jenis sumber daya, lihat Kunci tindakan, sumber daya, dan kondisi AWS Ground Station di Referensi Otorisasi Layanan.

Topik

- Praktik terbaik kebijakan
- Menggunakan konsol AWS Ground Station
- Mengizinkan pengguna melihat izin mereka sendiri

Praktik terbaik kebijakan

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

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan terkelola AWS pelanggan yang spesifik 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.

Menggunakan konsol AWS Ground Station

Untuk mengakses AWS Ground Station konsol, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang AWS Ground Station 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 AWS Ground Station konsol, lampirkan juga kebijakan AWS Ground Station *ConsoleAccess* atau *ReadOnly* AWS terkelola ke entitas. Untuk informasi selengkapnya, lihat Menambah izin untuk pengguna dalam Panduan Pengguna IAM.

Mengizinkan pengguna melihat izin mereka sendiri

Contoh ini menunjukkan cara membuat kebijakan yang mengizinkan pengguna IAM melihat kebijakan inline dan terkelola yang dilampirkan ke identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau menggunakan API atau secara terprogram. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
```

```
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Memecahkan masalah AWS Ground Station identitas dan akses

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

Topik

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

Saya tidak berwenang untuk melakukan tindakan di AWS Ground Station

Jika Anda menerima pesan kesalahan bahwa Anda tidak memiliki otorisasi untuk melakukan tindakan, kebijakan Anda harus diperbarui agar Anda dapat melakukan tindakan tersebut.

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

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

Dalam hal ini, kebijakan untuk pengguna `mateojackson` harus diperbarui untuk mengizinkan akses ke sumber daya *`my-example-widget`* dengan menggunakan tindakan `groundstation:`*`GetWidget`*.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya tidak berwenang untuk melakukan iam: PassRole

Jika Anda menerima kesalahan yang tidak diizinkan untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran AWS Ground Station.

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 AWS Ground Station. 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 AWS Ground Station 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 AWS Ground Station mendukung fitur-fitur ini, lihatBagaimana AWS Ground Station 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.

Menggunakan peran terkait layanan untuk Ground Station

AWS Ground Station menggunakan AWS Identity and Access Management (IAM) peran tertaut layanan. Peran terkait layanan adalah jenis IAM role unik yang terhubung langsung ke Ground Station. Peran terkait layanan ditentukan sebelumnya oleh Ground Station dan mencakup semua izin yang diperlukan layanan untuk menghubungiAWS layanan lainnya atas nama Anda.

Peran terkait layanan memudahkan pengaturan Ground Station menjadi lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. Ground Station menentukan izin peran terkait layanan, kecuali jika ditentukan berbeda, hanya Ground Station yang dapat mengasumsikan perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, serta bahwa kebijakan izin tidak dapat dilampirkan ke entitas IAM lainnya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat Layanan AWS yang Bekerja bersama IAM dan mencari layanan yang memiliki Ya dalam Peran Terkait Layanan. Pilih Ya dengan tautan untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Izin peran terkait layanan untuk Ground Station

Ground Station menggunakan peran terkait layanan yang diberi nama AWSServiceRoleForGroundStationDataflowEndpointGroup— AWS GroundStation menggunakan peran terkait layanan ini untuk memanggil EC2 untuk menemukan alamat IPv4 publik.

Peran AWSServiceRoleForGroundStationDataflowEndpointGroup terkait layanan memercayai layanan berikut untuk mengambil peran:

- `groundstation.amazonaws.com`

Kebijakan izin peran yang diberi nama AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy memungkinkan Ground Station untuk menyelesaikan tindakan berikut pada sumber daya yang ditentukan:

- Tindakan: `ec2:DescribeAddresses` pada `all AWS resources (*)`

  Tindakan memungkinkan Ground Station untuk daftar semua IP yang terkait dengan EIP.
- Tindakan: `ec2:DescribeNetworkInterfaces` pada `all AWS resources (*)`

  Tindakan memungkinkan Ground Station untuk mendapatkan informasi tentang antarmuka jaringan yang terkait dengan instans EC2

Anda harus mengonfigurasi izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat Izin peran tertaut layanan dalam Panduan Pengguna IAM.

Membuat peran terkait layanan untuk Ground Station

Anda tidak perlu membuat peran terkait layanan secara manual. Ketika Anda membuat DataflowEndpointGroup di dalamAWS CLI atauAWS API, Ground Station membuatkan peran terkait layanan untuk Anda.

Jika Anda menghapus peran tertaut layanan ini, dan ingin membuatnya lagi, Anda dapat mengulangi proses yang sama untuk membuat kembali peran tersebut di akun Anda. Ketika Anda membuat DataflowEndpointGroup, Ground Station membuat peran terkait layanan untuk Anda kembali.

Anda juga dapat menggunakan konsol IAM untuk membuat peran terkait layanan dengan kasus penggunaan Pengiriman Data ke Amazon EC2. Di AWS CLI atau API AWS, buat peran yang terhubung dengan layanan dengan nama layanan `groundstation.amazonaws.com`. Untuk informasi lebih lanjut, lihat Membuat peran terkait layanan dalam Panduan Pengguna IAM. Jika Anda menghapus peran tertaut layanan ini, Anda dapat mengulang proses yang sama untuk membuat peran tersebut lagi.

Mengedit peran terkait layanan untuk Ground Station

Ground Station tidak mengizinkan Anda untuk mengedit peran AWSServiceRoleForGroundStationDataflowEndpointGroup terkait layanan. Setelah Anda membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat mengedit penjelasan peran menggunakan IAM. Untuk informasi selengkapnya, lihat Mengedit peran yang terkait dengan layanan dalam Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk Ground Station

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran terkait layanan, kami merekomendasikan Anda menghapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan yang tidak dipantau atau dipelihara secara aktif.

Anda dapat menghapus peran terkait layanan hanya setelah pertama kali menghapus peran terkait layanan DataflowEndpointGroups menggunakan peran terkait layanan. Hal ini melindungi Anda dari secara tidak sengaja mencabut izin untuk Anda DataflowEndpointGroups. Jika peran terkait layanan digunakan dengan beberapa DataflowEndpointGroups, Anda harus menghapus semua DataflowEndpointGroups yang menggunakan peran terkait layanan sebelum Anda dapat menghapusnya.

> **Note**
>
> Jika layanan Ground Station menggunakan peran tersebut ketika Anda mencoba menghapus sumber daya, penghapusan mungkin gagal. Jika hal itu terjadi, tunggu beberapa menit dan coba mengoperasikannya lagi.

Untuk menghapus sumber daya Ground Station yang digunakan oleh AWSServiceRoleForGroundStationDataflowEndpointGroup

- Hapus DataflowEndpointGroups melalui AWS CLI atau AWS API.

Untuk menghapus peran terkait layanan secara manual menggunakan IAM

Gunakan konsol IAM, AWS CLI, atau AWS API untuk menghapus peran terkait layanan AWSServiceRoleForGroundStationDataflowEndpointGroup. Untuk informasi selengkapnya, lihat Menghapus peran tertaut layanan dalam Panduan Pengguna IAM.

Wilayah yang didukung untuk peran terkait layanan Ground Station

Ground Station mendukung penggunaan peran terkait layanan di semua wilayah tempat layanan yang tersedia. Untuk informasi selengkapnya, lihat Tabel Wilayah.

Pemecahan Masalah

`NOT_AUTHORIZED_TO_CREATE_SLR`- Ini menunjukkan peran dalam akun Anda yang digunakan untuk memanggil CreateDataflowEndpointGroup API tidak memiliki`iam:CreateServiceLinkedRole` izin. Administrator dengan`iam:CreateServiceLinkedRole` izin harus secara manual membuat Peran Tertaut Layanan untuk akun Anda.

Kebijakan terkelola AWS untuk AWS Ground Station

SebuahAWSkebijakan terkelola adalah kebijakan mandiri yang dibuat dan dikelola olehAWS.AWSkebijakan terkelola dirancang untuk memberikan izin untuk banyak kasus penggunaan umum sehingga Anda dapat mulai menetapkan izin kepada pengguna, grup, dan peran.

Perlu diingat bahwaAWSkebijakan terkelola mungkin tidak memberikan izin paling sedikit hak istimewa untuk kasus penggunaan spesifik Anda karena tersedia untuk semuaAWSpelanggan untuk digunakan. Kami menyarankan Anda mengurangi izin lebih lanjut dengan mendefinisikankebijakan yang dikelola pelanggan yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ditentukan dalamAWSkebijakan yang dikelola. JikaAWSmemperbarui izin yang didefinisikan dalamAWSkebijakan terkelola, pembaruan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan.AWSkemungkinan besar akan memperbaruiAWSkebijakan terkelola saat baruLayanan AWSdiluncurkan atau operasi API baru tersedia untuk layanan yang ada.

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

Kebijakan terkelola AWS: AWSGroundStationAgentInstancePolicy

Anda dapat melampirkan kebijakan `AWSGroundStationAgentInstancePolicy` ke identitas-identitas IAM Anda.

Kebijakan ini memberikan izin Agen Stasiun Darat AWS kepada instans pelanggan yang memungkinkan instans mengirim dan menerima data selama kontak Stasiun Darat. Semua izin dalam kebijakan ini berasal dari layanan Stasiun Darat.

Rincian perizinan

Kebijakan ini mencakup izin berikut.

- `groundstation`- Memungkinkan instans endpoint dataflow untuk memanggil API Agen Stasiun Tanah.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "groundstation:RegisterAgent",
                "groundstation:UpdateAgentStatus",
                "groundstation:GetAgentConfiguration"
            ],
            "Resource": "*"
        }
    ]
}
```

Kebijakan terkelola AWS: AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy

Anda tidak dapat melampirkan AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy ke entitas IAM Anda. Kebijakan ini dilampirkan ke peran terkait layanan yang mengizinkan AWS Ground

Station untuk melakukan tindakan atas nama Anda. Untuk informasi lebih lanjut, lihatMenggunakan peran terkait layanan.

Kebijakan ini memberikan izin EC2 yang memungkinkanAWS Ground Stationuntuk menemukan alamat IPv4 publik.

Rincian perizinan

Kebijakan ini mencakup izin berikut.

- `ec2:DescribeAddresses`- MemungkinkanAWS Ground Stationuntuk mencantumkan semua IP yang terkait dengan EIP atas nama Anda.
- `ec2:DescribeNetworkInterfaces`- MemungkinkanAWS Ground Stationuntuk mendapatkan informasi tentang antarmuka jaringan yang terkait dengan instans EC2 atas nama Anda.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeAddresses",
                "ec2:DescribeNetworkInterfaces"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS Ground Station memperbarui pada kebijakan terkelola AWS

Lihat detail tentang pembaruan terhadap kebijakan terkelola AWS untuk AWS Ground Station sejak layanan ini mulai melacak perubahan-perubahan tersebut. Untuk peringatan otomatis tentang

perubahan pada halaman ini, berlangganan umpan RSS di halaman Riwayat dokumen AWS Ground Station.

Perubahan	Deskripsi	Tanggal
AWSGroundStationAgentInstancePolicy – Kebijakan baru	AWS Ground Stationmenambahkan kebijakan baru untuk memberikan izin instans titik akhir dataflow untuk menggunakan Agen AWS Ground Station.	April 12, 2023
AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy – Kebijakan baru	AWS Ground Stationmenambahkan kebijakan baru yang memberikan izin EC2 untuk mengizinkanAWS Ground Stationuntuk menemukan alamat IPv4 publik yang terkait dengan EIP dan antarmuka jaringan yang terkait dengan instans EC2.	November 02, 2022
AWS Ground Station mulai melacak perubahan	AWS Ground Stationmulai melacak perubahan untukAWSkebijakan yang dikelola.	01 Maret 2021

Enkripsi Data saat istirahat untuk AWS Ground Station

AWS Ground Station menyediakan enkripsi secara default untuk melindungi data pelanggan sensitif saat istirahat menggunakan kunci enkripsi yang AWS dimiliki.

- Kunci yang dimiliki AWS - AWS Ground Station menggunakan kunci ini secara default untuk mengenkripsi data pribadi dan ephemerides yang dapat diidentifikasi secara langsung. Anda tidak dapat melihat, mengelola, atau menggunakan kunci milik AWS, atau mengaudit penggunaannya; Namun, tidak perlu mengambil tindakan apa pun atau mengubah program untuk melindungi kunci yang mengenkripsi data. Untuk informasi selengkapnya, lihat kunci yang dimiliki AWS di Panduan Pengembang AWS Key Management Service.

Enkripsi data saat istirahat secara default membantu dengan mengurangi overhead operasional dan kompleksitas yang terlibat dalam melindungi data sensitif. Pada saat yang sama, ini memungkinkan membangun aplikasi aman yang memenuhi kepatuhan enkripsi yang ketat, serta persyaratan peraturan.

AWS Ground Station memberlakukan enkripsi pada semua data sensitif, saat istirahat, namun, untuk beberapa AWS Ground Station sumber daya, seperti ephemerides, Anda dapat memilih untuk menggunakan kunci yang dikelola pelanggan sebagai pengganti kunci terkelola default. AWS

- Kunci terkelola pelanggan - AWS Ground Station mendukung penggunaan kunci terkelola pelanggan simetris yang Anda buat, miliki, dan kelola untuk menambahkan lapisan enkripsi kedua di atas enkripsi yang AWS dimiliki yang ada. Karena Anda memiliki kontrol penuh atas lapisan enkripsi ini, Anda dapat melakukan tugas-tugas seperti:
  - Menetapkan dan memelihara kebijakan utama
  - Menetapkan dan memelihara kebijakan dan hibah IAM
  - Mengaktifkan dan menonaktifkan kebijakan utama
  - Memutar bahan kriptografi kunci
  - Menambahkan tanda
  - Membuat alias kunci
  - Kunci penjadwalan untuk penghapusan

  Untuk informasi selengkapnya, lihat kunci terkelola pelanggan di Panduan Pengembang AWS Key Management Service.

Tabel berikut merangkum sumber daya yang AWS Ground Station mendukung penggunaan Customer Managed Keys

Tipe data	Enkripsi kunci yang dimiliki AWS	Enkripsi kunci yang dikelola pelanggan (Opsional)
Data Ephemeris digunakan untuk menghitung lintasan Satelit	Diaktifkan	Diaktifkan

> **Note**
>
> AWS Ground Station secara otomatis mengaktifkan enkripsi saat istirahat menggunakan kunci yang AWS dimiliki untuk melindungi data yang dapat diidentifikasi secara pribadi tanpa biaya. Namun, biaya AWS KMS berlaku untuk menggunakan kunci yang dikelola pelanggan. Untuk informasi selengkapnya tentang harga, lihat harga AWS Key Management Service. Untuk informasi selengkapnya tentang AWS KMS, lihat Panduan Pengembang AWS KMS.

Bagaimana AWS Ground Station menggunakan hibah di KMS AWS

AWS Ground Station memerlukan hibah kunci untuk menggunakan kunci yang dikelola pelanggan Anda.

Saat Anda mengunggah ephemeris yang dienkripsi dengan kunci yang dikelola pelanggan, AWS Ground Station buat hibah kunci atas nama Anda dengan mengirimkan permintaan ke KMS. CreateGrant AWS Hibah di AWS KMS digunakan untuk memberikan AWS Ground Station akses ke kunci KMS di akun pelanggan.

AWS Ground Station memerlukan hibah untuk menggunakan kunci yang dikelola pelanggan Anda untuk operasi internal berikut:

- Kirim `GenerateDataKey` permintaan ke AWS KMS untuk menghasilkan kunci data yang dienkripsi oleh kunci yang dikelola pelanggan Anda.
- Kirim `Decrypt` permintaan ke AWS KMS untuk mendekripsi kunci data terenkripsi sehingga mereka dapat digunakan untuk mengenkripsi data Anda.

- Kirim `Encrypt` permintaan ke AWS KMS untuk mengenkripsi data yang disediakan.

Anda dapat mencabut akses ke hibah, atau menghapus akses layanan ke kunci yang dikelola pelanggan kapan saja. Jika Anda melakukannya, AWS Ground Station tidak akan dapat mengakses data apa pun yang dienkripsi oleh kunci yang dikelola pelanggan, yang memengaruhi operasi yang bergantung pada data tersebut. Misalnya, jika Anda menghapus hibah kunci dari ephemeris yang saat ini digunakan untuk kontak maka tidak AWS Ground Station akan dapat menggunakan data ephemeris yang disediakan untuk mengarahkan antena selama kontak. Ini akan menyebabkan kontak berakhir dalam keadaan GAGAL.

Buat kunci terkelola pelanggan

Anda dapat membuat kunci terkelola pelanggan simetris dengan menggunakan AWS Management Console, atau AWS KMS API.

Untuk membuat kunci terkelola pelanggan simetris

Ikuti langkah-langkah untuk Membuat kunci terkelola pelanggan simetris di Panduan Pengembang Layanan Manajemen AWS Kunci.

Kebijakan kunci

Kebijakan utama mengontrol akses ke kunci yang dikelola pelanggan Anda. Setiap kunci yang dikelola pelanggan harus memiliki persis satu kebijakan utama, yang berisi pernyataan yang menentukan siapa yang dapat menggunakan kunci dan bagaimana mereka dapat menggunakannya. Saat membuat kunci terkelola pelanggan, Anda dapat menentukan kebijakan kunci. Untuk informasi selengkapnya, lihat Mengelola akses ke kunci yang dikelola pelanggan di Panduan Pengembang Layanan Manajemen AWS Kunci.

Untuk menggunakan kunci terkelola pelanggan dengan AWS Ground Station sumber daya Anda, operasi API berikut harus diizinkan dalam kebijakan kunci:

`kms:CreateGrant`- Menambahkan hibah ke kunci yang dikelola pelanggan. Memberikan akses kontrol ke kunci KMS tertentu, yang memungkinkan akses ke operasi AWS Ground Station hibah memerlukan. Untuk informasi selengkapnya tentang Menggunakan Hibah, lihat Panduan Pengembang Layanan Manajemen AWS Utama.

Ini memungkinkan Amazon AWS untuk melakukan hal berikut:

- Panggilan `GenerateDataKey` untuk menghasilkan kunci data terenkripsi dan menyimpannya, karena kunci data tidak segera digunakan untuk mengenkripsi.
- Panggilan `Decrypt` untuk menggunakan kunci data terenkripsi yang disimpan untuk mengakses data terenkripsi.
- Panggil `Encrypt` untuk menggunakan kunci data untuk mengenkripsi data.
- Siapkan kepala sekolah yang pensiun untuk memungkinkan layanan. `RetireGrant`

`kms:DescribeKey`- Memberikan rincian kunci yang dikelola pelanggan AWS Ground Station untuk memungkinkan memvalidasi kunci sebelum mencoba membuat hibah pada kunci yang disediakan.

Berikut ini adalah contoh pernyataan kebijakan IAM yang dapat Anda tambahkan AWS Ground Station

```
"Statement" : [
  {"Sid" : "Allow access to principals authorized to use AWS Ground Station",
    "Effect" : "Allow",
    "Principal" : {
      "AWS" : "*"
    },
    "Action" : [
      "kms:DescribeKey",
      "kms:CreateGrant"
    ],
    "Resource" : "*",
    "Condition" : {
    "StringEquals" : {
        "kms:ViaService" : "groundstation.amazonaws.com",
        "kms:CallerAccount" : "111122223333"
    }
  },
  {"Sid": "Allow access for key administrators",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:root"
    },
    "Action" : [
      "kms:*"
      ],
    "Resource": "arn:aws:kms:region:111122223333:key/key_ID"
  },
  {"Sid" : "Allow read-only access to key metadata to the account",
```

```
    "Effect" : "Allow",
    "Principal" : {
      "AWS" : "arn:aws:iam::111122223333:root"
    },
    "Action" : [
      "kms:Describe*",
      "kms:Get*",
      "kms:List*",
      "kms:RevokeGrant"
    ],
    "Resource" : "*"
  }
]
```

Untuk informasi selengkapnya tentang menentukan izin dalam kebijakan, lihat Panduan Pengembang Layanan Manajemen AWS Kunci.

Untuk informasi selengkapnya tentang akses kunci pemecahan masalah, lihat Panduan Pengembang Layanan Manajemen AWS Kunci.

Menentukan kunci yang dikelola pelanggan untuk AWS Ground Station

Anda dapat menentukan kunci yang dikelola pelanggan untuk mengenkripsi sumber daya berikut:

- Ephemeris

Saat Anda membuat sumber daya, Anda dapat menentukan kunci data dengan menyediakan kmsKeyArn

- kmsKeyArn- Pengidentifikasi kunci untuk kunci yang dikelola pelanggan AWS KMS

AWS Ground Station konteks enkripsi

Konteks enkripsi adalah kumpulan opsional pasangan kunci-nilai yang berisi informasi kontekstual tambahan tentang data. AWS KMS menggunakan konteks enkripsi sebagai data otentikasi tambahan untuk mendukung enkripsi yang diautentikasi. Saat Anda menyertakan konteks enkripsi dalam permintaan untuk mengenkripsi data, AWS KMS mengikat konteks enkripsi ke data terenkripsi. Untuk mendekripsi data, Anda menyertakan konteks enkripsi yang sama dalam permintaan.

AWS Ground Station konteks enkripsi

AWS Ground Station menggunakan konteks enkripsi yang berbeda tergantung pada sumber daya yang dienkripsi dan menentukan konteks enkripsi khusus untuk setiap hibah kunci yang dibuat.

Konteks Enkripsi Ephemeris:

Hibah kunci untuk mengenkripsi sumber daya ephemeris terikat pada ARN satelit tertentu

```
"encryptionContext": {
    "aws:groundstation:arn":
 "arn:aws:groundstation::111122223333:satellite/00a770b0-082d-45a4-80ed-SAMPLE"
}
```

> **Note**
>
> Hibah kunci digunakan kembali untuk pasangan kunci-satelit yang sama.

Menggunakan konteks enkripsi untuk pemantauan

Saat Anda menggunakan kunci terkelola pelanggan simetris untuk mengenkripsi ephemerides Anda, Anda juga dapat menggunakan konteks enkripsi dalam catatan audit dan log untuk mengidentifikasi bagaimana kunci yang dikelola pelanggan digunakan. Konteks enkripsi juga muncul di log yang dihasilkan oleh AWS CloudTrail atau Amazon CloudWatch Logs.

Menggunakan konteks enkripsi untuk mengontrol akses ke kunci terkelola pelanggan Anda

Anda dapat menggunakan konteks enkripsi dalam kebijakan utama dan kebijakan IAM `conditions` untuk mengontrol akses ke kunci terkelola pelanggan simetris Anda. Anda juga dapat menggunakan kendala konteks enkripsi dalam hibah.

AWS Ground Station menggunakan batasan konteks enkripsi dalam hibah untuk mengontrol akses ke kunci yang dikelola pelanggan di akun atau wilayah Anda. Batasan hibah mengharuskan operasi yang diizinkan oleh hibah menggunakan konteks enkripsi yang ditentukan.

Berikut ini adalah contoh pernyataan kebijakan kunci untuk memberikan akses ke kunci yang dikelola pelanggan untuk konteks enkripsi tertentu. Kondisi dalam pernyataan kebijakan ini mengharuskan hibah memiliki batasan konteks enkripsi yang menentukan konteks enkripsi.

```
{"Sid": "Enable DescribeKey",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/ExampleReadOnlyRole"
     },
     "Action": "kms:DescribeKey",
     "Resource": "*"
},{"Sid": "Enable CreateGrant",
     "Effect": "Allow",
     "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/ExampleReadOnlyRole"
     },
     "Action": "kms:CreateGrant",
     "Resource": "*",
     "Condition": {
        "StringEquals": {
            "kms:EncryptionContext:aws:groundstation:arn":
 "arn:aws:groundstation::111122223333:satellite/00a770b0-082d-45a4-80ed-SAMPLE"
        }
     }
}
```

Memantau kunci enkripsi Anda untuk AWS Ground Station

Saat Anda menggunakan kunci terkelola pelanggan AWS KMS dengan AWS Ground Station sumber daya Anda, Anda dapat menggunakan AWS CloudTrailatau CloudWatch log Amazon untuk melacak permintaan yang AWS Ground Station dikirim ke AWS KMS. Contoh berikut adalah AWS CloudTrail peristiwa untuk`CreateGrant`,, `GenerateDataKeyDecrypt`, `Encrypt` dan `DescribeKey` untuk memantau operasi KMS yang dipanggil oleh AWS Ground Station untuk mengakses data yang dienkripsi oleh kunci yang dikelola pelanggan Anda.

`CreateGrant`(Cloudtrail)

Saat Anda menggunakan kunci yang dikelola pelanggan AWS KMS untuk mengenkripsi sumber daya ephemeris Anda, AWS Ground Station kirimkan `CreateGrant` permintaan atas nama Anda untuk mengakses kunci KMS di akun Anda. AWS Hibah AWS Ground Station yang dibuat khusus untuk

sumber daya yang terkait dengan kunci yang dikelola pelanggan AWS KMS. Selain itu, AWS Ground Station menggunakan `RetireGrant` operasi untuk menghapus hibah saat Anda menghapus sumber daya.

Contoh peristiwa berikut mencatat `CreateGrant` operasi:


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AAAAAAAAAAAAAAAAAAAAA:SampleUser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/SampleUser01",
        "accountId": "111122223333",
        "accessKeyId": "ASIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AAAAAAAAAAAAAAAAAAAAA",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-02-22T22:22:22Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2022-02-22T22:22:22Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "111.11.11.11",
    "userAgent": "ExampleDesktop/1.0 (V1; OS)",
    "requestParameters": {
        "operations": [
            "GenerateDataKeyWithoutPlaintext",
            "Decrypt",
            "Encrypt"
        ],
        "constraints": {
```

```
            "encryptionContextSubset": {
                "aws:groundstation:arn":
 "arn:aws:groundstation::111122223333:satellite/00a770b0-082d-45a4-80ed-SAMPLE"
            }
        },
        "granteePrincipal": "groundstation.us-west-2.amazonaws.com",
        "retiringPrincipal": "groundstation.us-west-2.amazonaws.com",
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "responseElements": {
        "grantId":
 "0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE"
    },
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

`DescribeKey`(Cloudtrail)

Saat Anda menggunakan kunci terkelola pelanggan AWS KMS untuk mengenkripsi sumber daya ephemeris Anda, AWS Ground Station kirimkan `DescribeKey` permintaan atas nama Anda untuk memvalidasi bahwa kunci yang diminta ada di akun Anda.

Contoh peristiwa berikut mencatat `DescribeKey` operasi:

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
```

```
        "principalId": "AAAAAAAAAAAAAAAAAAAAA:SampleUser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/User/Role",
        "accountId": "111122223333",
        "accessKeyId": "ASIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AAAAAAAAAAAAAAAAAAAAA",
                "arn": "arn:aws:iam::111122223333:role/Role",
                "accountId": "111122223333",
                "userName": "User"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-02-22T22:22:22Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2022-02-22T22:22:22Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DescribeKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
```

```
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

GenerateDataKey(Cloudtrail)

Saat Anda menggunakan kunci yang dikelola pelanggan AWS KMS untuk mengenkripsi sumber daya ephemeris Anda, AWS Ground Station kirimkan `GenerateDataKey` permintaan ke KMS untuk menghasilkan kunci data yang dapat digunakan untuk mengenkripsi data Anda.

Contoh peristiwa berikut mencatat `GenerateDataKey` operasi:

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2022-02-22T22:22:22Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keySpec": "AES_256",
        "encryptionContext": {
            "aws:groundstation:arn":
 "arn:aws:groundstation::111122223333:satellite/00a770b0-082d-45a4-80ed-SAMPLE",
            "aws:s3:arn":
 "arn:aws:s3:::customerephemerisbucket/0034abcd-12ab-34cd-56ef-123456SAMPLE"
        },
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
```

```
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "sharedEventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventCategory": "Management"
}
```

`Decrypt`(Cloudtrail)

Saat Anda menggunakan kunci yang dikelola pelanggan AWS KMS untuk mengenkripsi sumber daya ephemeris Anda, AWS Ground Station gunakan `Decrypt` operasi untuk mendekripsi ephemeris yang disediakan jika sudah dienkripsi dengan kunci terkelola pelanggan yang sama. Misalnya jika ephemeris sedang diunggah dari bucket S3 dan dienkripsi dalam ember itu dengan kunci yang diberikan.

Contoh peristiwa berikut mencatat `Decrypt` operasi:

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2022-02-22T22:22:22Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "encryptionContext": {
            "aws:groundstation:arn":
 "arn:aws:groundstation::111122223333:satellite/00a770b0-082d-45a4-80ed-SAMPLE",
            "aws:s3:arn":
 "arn:aws:s3:::customerephemerisbucket/0034abcd-12ab-34cd-56ef-123456SAMPLE"
        },
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
    },
```

```
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "sharedEventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventCategory": "Management"
}
```

Data Satelit Ephemeris

Ephemeris, ephemerides jamak, adalah file atau struktur data yang menyediakan lintasan objek astronomi. Secara historis, file ini hanya mengacu pada data tabular tetapi, secara bertahap, telah mengarahkan ke berbagai file data yang menunjukkan lintasan pesawat ruang angkasa.

AWS Ground Station menggunakan data ephemeris untuk menentukan kapan kontak tersedia untuk satelit Anda dan memerintahkan antena dengan benar di AWS Ground Station Jaringan untuk menunjuk ke satelit Anda. Secara default tidak ada tindakan yang diperlukan untuk menyediakan AWS Ground Station ephemerides.

Topik

Data Ephemeris Standar

Secara default, AWS Ground Station menggunakan data yang tersedia untuk umum dari Space-Track, dan tidak ada tindakan yang diperlukan untuk memasok AWS Ground Station ephemerides default ini. Ephemerides ini adalah set elemen dua baris yang terkait dengan ID NORAD satelit Anda. Semua ephemerides default memiliki prioritas 0. Akibatnya, mereka akan diganti, selalu, oleh ephemerides khusus yang tidak kedaluwarsa yang diunggah melalui API ephemeris, yang harus selalu memiliki prioritas 1, atau lebih besar.

Satelit tanpa ID NORAD, harus mengunggah data ephemeris khusus ke. AWS Ground Station Misalnya, satelit yang baru saja diluncurkan atau yang sengaja dihilangkan dari katalog Space-Track tidak akan memiliki ID NORAD dan perlu mengunggah ephemerides khusus. Untuk informasi lebih lanjut tentang menyediakan ephemeris khusus, lihat: Menyediakan Data Ephemeris Kustom.

Ephemeris Mana Yang Digunakan

Ephemerides memiliki prioritas, waktu kedaluwarsa, dan flag yang diaktifkan. Bersama-sama, ini menentukan ephemeris mana yang digunakan untuk satelit. Hanya satu ephemeris yang dapat aktif untuk setiap satelit.

Ephemeris yang akan digunakan adalah ephemeris dengan prioritas tertinggi yang waktu kedaluwarsa di masa depan. Waktu kontak yang tersedia yang dikembalikan oleh ListContactsdidasarkan pada ephemeris ini. Jika beberapa `ENABLED` ephemerides memiliki prioritas yang sama, ephemeris yang terbaru dibuat atau diperbarui akan digunakan.

> **Note**
>
> AWS Ground Station memiliki kuota layanan pada jumlah ephemerides yang `ENABLED` disediakan pelanggan per satelit (lihat: Service Quotas). Untuk mengunggah data ephemeris setelah mencapai kuota ini, hapus (menggunakan`DeleteEphemeris`) atau nonaktifkan (menggunakan`UpdateEphemeris`) ephemerides yang disediakan pelanggan dengan prioritas terendah/paling awal yang dibuat.

Jika tidak ada ephemeris yang dibuat, atau jika tidak ada ephemerides yang memiliki `ENABLED` status, AWS Ground Station akan menggunakan ephemeris default untuk satelit (dari Space Track), jika tersedia. Ephemeris default ini memiliki prioritas 0.

Pengaruh Ephemerides baru pada Kontak yang Dijadwalkan Sebelumnya

Gunakan DescribeContact API untuk melihat efek ephemerides baru pada kontak yang dijadwalkan sebelumnya dengan mengembalikan waktu visibilitas aktif.

Kontak yang dijadwalkan sebelum mengunggah ephemeris baru akan mempertahankan waktu kontak yang dijadwalkan semula, sedangkan pelacakan antena akan menggunakan ephemeris aktif. Jika posisi pesawat ruang angkasa, berdasarkan ephemeris aktif, sangat berbeda dari ephemeris sebelumnya, ini dapat mengakibatkan berkurangnya waktu kontak satelit dengan antena karena pesawat ruang angkasa yang beroperasi di luar topeng situs transmit/penerimaan. Oleh karena itu, kami menyarankan Anda membatalkan dan menjadwal ulang kontak future Anda setelah Anda mengunggah ephemeris baru yang sangat berbeda dari ephemeris sebelumnya. Dengan DescribeContact API, Anda dapat menentukan bagian dari kontak future Anda yang tidak dapat digunakan karena pesawat ruang angkasa yang beroperasi di luar masker situs transmit/terima dengan membandingkan kontak terjadwal Anda `startTime` dan `endTime` dengan yang

dikembalikan dan. `visibilityStartTime` `visibilityEndTime` Jika Anda memilih untuk membatalkan dan menjadwal ulang kontak masa depan Anda, rentang waktu kontak tidak boleh berada di luar rentang waktu visibilitas lebih dari 30 detik. Kontak yang dibatalkan dapat dikenakan biaya jika dibatalkan terlalu dekat dengan waktu kontak. Untuk informasi selengkapnya tentang kontak yang dibatalkan, lihat: FAQ Ground Station.

Mendapatkan Ephemeris Saat Ini untuk Satelit

Ephemeris saat ini digunakan oleh AWS Ground Station untuk satelit tertentu dapat diambil dengan memanggil atau tindakan. `GetSatellite` `ListSatellites` Kedua metode ini akan mengembalikan metadata untuk ephemeris yang saat ini digunakan. Metadata ephemeris ini berbeda untuk ephemerides khusus yang diunggah ke dan untuk ephemerides default. AWS Ground Station

Ephemerides default hanya akan menyertakan `source` dan bidang. `epoch` `epoch`Ini adalah zaman dari set elemen dua baris yang ditarik dari Space Track AWS Ground Station, dan saat ini sedang digunakan untuk menghitung lintasan satelit.

Ephemeris khusus akan memiliki `source` nilai `"CUSTOMER_PROVIDED"` dan akan menyertakan pengidentifikasi unik di lapangan. `ephemerisId` Pengidentifikasi unik ini dapat digunakan untuk menanyakan ephemeris melalui tindakan. `DescribeEphemeris` `name`Bidang opsional akan dikembalikan jika ephemeris diberi nama saat diunggah AWS Ground Station melalui tindakan. `CreateEphemeris`

Penting untuk dicatat bahwa ephemerides diperbarui secara dinamis AWS Ground Station sehingga data yang dikembalikan hanyalah snapshot dari ephemeris yang digunakan pada saat panggilan ke API.

Contoh **`GetSatellite`** pengembalian untuk satelit menggunakan ephemeris default

```
{
    "satelliteId": "e1cfe0c7-67f9-4d98-bad2-06dbfc2d14a2",
    "satelliteArn": "arn:aws:groundstation::111122223333:satellite/e1cfe0c7-67f9-4d98-
bad2-06dbfc2d14a2",
    "noradSatelliteID": 12345,
    "groundStations": [
        "Example Ground Station 1",
        "Example Ground Station 2"
    ],
```

```
    "currentEphemeris": {
        "source": "SPACE_TRACK",
        "epoch": 8888888888
    }
}
```

Contoh **`GetSatellite`** untuk satelit menggunakan ephemeris khusus

```
{
      "satelliteId": "e1cfe0c7-67f9-4d98-bad2-06dbfc2d14a2",
      "satelliteArn": "arn:aws:groundstation::111122223333:satellite/
e1cfe0c7-67f9-4d98-bad2-06dbfc2d14a2",
      "noradSatelliteID": 12345,
      "groundStations": [
          "Example Ground Station 1",
          "Example Ground Station 2"
      ],
      "currentEphemeris": {
          "source": "CUSTOMER_PROVIDED",
          "ephemerisId": "e1cfe0c7-67f9-4d98-bad2-06dbfc2d14a2",
          "name": "My Ephemeris"
      }
  }
```

Menyediakan Data Ephemeris Kustom

> **Warning**
>
> API ephemeris saat ini dalam status Pratinjau

Akses ke API Ephemeris disediakan hanya sesuai kebutuhan. Pelanggan yang membutuhkan kemampuan untuk mengunggah data ephemeris khusus harus menghubungi aws-groundstation@amazon.com.

Gambaran Umum

API Ephemeris memungkinkan ephemerides khusus untuk diunggah untuk digunakan dengan satelit. AWS Ground Station Ephemerides ini mengesampingkan ephemerides default dari Space Track (lihat: Data Ephemeris Default).

Mengunggah ephemerides pelanggan dapat meningkatkan kualitas pelacakan, menangani operasi awal di mana tidak ada ephemerides Space Track yang tersedia, dan untuk AWS Ground Station memperhitungkan manuver.

Membuat Ephemeris khusus

Ephemeris khusus dapat dibuat menggunakan `CreateEphemeris` tindakan di API. AWS Ground Station Tindakan ini akan mengunggah ephemeris menggunakan data baik di badan permintaan atau dari bucket S3 yang ditentukan.

Penting untuk dicatat bahwa mengunggah ephemeris menyetel ephemeris `VALIDATING` dan memulai alur kerja asinkron yang akan memvalidasi dan menghasilkan kontak potensial dari ephemeris Anda. Hanya setelah ephemeris melewati alur kerja ini dan menjadi `ENABLED` akan digunakan untuk kontak. Anda harus melakukan polling `DescribeEphemeris` untuk status ephemeris atau menggunakan peristiwa Cloudwatch untuk melacak perubahan status ephemeris.

Untuk memecahkan masalah ephemeris yang tidak valid, lihat: Memecahkan Masalah Ephemerides Tidak Valid

Buat TLE Set Ephemeris melalui API

Klien AWS Ground Station boto3 dapat digunakan untuk mengunggah elemen dua baris (TLE) yang disetel ephemeris melalui panggilan. AWS Ground Station `CreateEphemeris` Ephemeris ini akan digunakan sebagai pengganti data ephemeris default untuk satelit (lihat Data Ephemeris Default).

Set TLE adalah objek berformat JSON yang merangkai satu atau lebih TLE bersama-sama untuk membangun lintasan kontinu. TLE dalam set TLE harus membentuk himpunan kontinu yang dapat kita gunakan untuk membangun lintasan (yaitu tidak ada celah waktu antara TLE dalam set TLE). Contoh set TLE ditunjukkan di bawah ini:

```
# example_tle_set.json
[
    {
        "tleLine1": "1 25994U 99068A   20318.54719794  .00000075  00000-0  26688-4 0
 9997",
        "tleLine2": "2 25994  98.2007  30.6589 0001234  89.2782  18.9934
 14.57114995111906",
        "validTimeRange": {
            "startTime": 12345,
            "endTime": 12346
```

```
        }
    },
    {
        "tleLine1": "1 25994U 99068A   20318.54719794  .00000075  00000-0  26688-4 0
 9997",
        "tleLine2": "2 25994  98.2007  30.6589 0001234  89.2782  18.9934
 14.57114995111906",
        "validTimeRange": {
            "startTime": 12346,
            "endTime": 12347
        }
    }
]
```

> **Note**
>
> Rentang waktu TLE dalam set TLE harus sama persis untuk menjadi lintasan berkelanjutan yang valid.

Satu set TLE dapat diunggah melalui klien AWS Ground Station boto3 sebagai berikut:

```
tle_ephemeris_id = ground_station_boto3_client.create_ephemeris( name="Example
 Ephemeris", satelliteId="2e925701-9485-4644-b031-EXAMPLE01", enabled=True,
 expirationTime=datetime.now(timezone.utc) + timedelta(days=3), priority=2,
    ephemeris = {
      "tle": {
        "tleData": [
            {
                "tleLine1": "1 25994U 99068A   20318.54719794  .00000075  00000-0
 26688-4 0  9997",
                "tleLine2": "2 25994  98.2007  30.6589 0001234  89.2782  18.9934
 14.57114995111906",
                "validTimeRange": {
                    "startTime": datetime.now(timezone.utc),
                    "endTime": datetime.now(timezone.utc) + timedelta(days=7)
                }
            }
        ]
      }
    })
```

Panggilan ini akan mengembalikan Id ephemeris yang dapat digunakan untuk referensi ephemeris di masa depan. Misalnya, kita dapat menggunakan ID ephemeris yang disediakan dari panggilan di atas untuk melakukan polling untuk status ephemeris:

```
client.describe_ephemeris(ephemerisId=tle_ephemeris_id['ephemerisId'])
```

Contoh respons dari `DescribeEphemeris` tindakan disediakan di bawah ini

```
{
  "creationTime": 1620254718.765,
  "enabled": true,
  "name": "Example Ephemeris",
  "ephemerisId": "fde41049-14f7-413e-bd7b-EXAMPLE01",
  "priority": 2,
  "status": "VALIDATING",
  "suppliedData": {
    "tle": {
      "ephemerisData": "[{\"tleLine1\": \"1 25994U 99068A   20318.54719794  .00000075
 00000-0  26688-4 0  9997\",\"tleLine2\": \"2 25994  98.2007  30.6589 0001234  89.2782
  18.9934 14.57114995111906\",\"validTimeRange\": {\"startTime\": 1620254712000,
\"endTime\": 1620859512000}}]"
    }
  }
}
```

Disarankan untuk melakukan polling `DescribeEphemeris` rute atau menggunakan peristiwa Cloudwatch untuk melacak status ephemeris yang diunggah karena harus melalui alur kerja validasi asinkron sebelum disetel ke dan dapat digunakan untuk menjadwalkan dan mengeksekusi kontak. `ENABLED`

Perhatikan bahwa ID NORAD di semua TLE dalam set TLE, 25994 dalam contoh di atas, harus cocok dengan ID NORAD yang telah ditetapkan satelit Anda dalam database Space Track.

Mengunggah data Ephemeris dari bucket S3

Dimungkinkan juga untuk mengunggah file ephemeris langsung dari bucket S3 dengan menunjuk ke bucket dan kunci objek. AWS Ground Station akan mengambil objek atas nama Anda. Informasi tentang enkripsi data saat istirahat AWS Ground Station dirinci dalam: Enkripsi Data Saat Istirahat Untuk AWS Ground Station

Di bawah ini adalah contoh mengunggah file ephemeris OEM dari bucket S3

```
s3_oem_ephemeris_id = customer_client.create_ephemeris( name="2022-10-26 S3
 OEM Upload", satelliteId="fde41049-14f7-413e-bd7b-EXAMPLE01", enabled=True,
 expirationTime=datetime.now(timezone.utc) + timedelta(days=5), priority=2,
    ephemeris = {
        "oem": {
            "s3Object": {
                "bucket": "ephemeris-bucket-for-testing",
                "key": "test_data.oem",
            }
        }
    })
```

Di bawah ini adalah contoh data yang dikembalikan dari `DescribeEphemeris` tindakan yang dipanggil untuk ephemeris OEM yang diunggah di blok kode contoh sebelumnya.

```
{
    "creationTime": 1620254718.765,
    "enabled": true,
    "name": "Example Ephemeris",
    "ephemerisId": "fde41049-14f7-413e-bd7b-EXAMPLE02",
    "priority": 2,
    "status": "VALIDATING",
    "suppliedData": {
    "oem": {
        "sourceS3Object": {
            "bucket": "ephemeris-bucket-for-testing",
            "key": "test_data.oem"
        }
    }
}
```

Pemecahan Masalah tidak valid

Ketika ephemeris kustom diunggah keAWS Ground Station itu akan melalui alur kerja validasi asinkron sebelum menjadi`ENABLED`. Alur kerja ini memastikan bahwa pengidentifikasi satelit, metadata, dan lintasan valid.

Ketika Ephemeris gagal validasi,`DescribeEphemeris` akan mengembalikan EphemerisInvalidReason, yang memberikan wawasan mengapa ephemeris gagal validasi. Nilai potensinya EphemerisInvalidReasonadalah sebagai berikut:

Nilai	Deskripsi	Tindakan Pemecahan Masalah tidak valid
METADATA_TIDAK VALID	Asalkan pengidentifikasi pesawat ruang angkasa seperti ID satelit tidak valid	Periksa NORAD ID atau pengenal lain yang disediakan dalam data ephemeris
TIME_RANGE_INVALID	Waktu mulai, akhir, atau kedaluwarsa tidak valid untuk ephemeris yang disediakan	Pastikan waktu Mulai sebelum `sekarang` (disarankan untuk mengatur waktu mulai beberapa menit di masa lalu), bahwa waktu akhir adalah setelah waktu mulai, dan bahwa waktu akhir adalah setelah waktu kedaluwarsa
TRAJECTORY_INVALID	Asalkan ephemeris mendefini sikan lintasan pesawat ruang angkasa yang tidak valid	Konfirmasikan bahwa lintasan yang disediakan terus menerus dan untuk satelit yang benar.
VALIDASI_ERROR	Terjadi kesalahan layanan internal saat memproses ephemeris untuk validasi	Coba lagi Unggah

Contoh`DescribeEphemeris` respons untuk`INVALID` ephemeris disediakan di bawah ini:

```
{
  "creationTime": 1000000000.00,
  "enabled": false,
  "ephemerisId": "d5a8a6ac-8a3a-444e-927e-EXAMPLE1",
  "name": "Example",
  "priority": 2,
  "status": "INVALID",
  "invalidReason": "METADATA_INVALID",
  "suppliedData": {
    "tle": {
      "sourceS3Object": {
```

```
        "bucket": "my-s3-bucket",
        "key": "myEphemerisKey",
        "version": "ephemerisVersion"
      }
    }
  },
}
```

Mengembalikan Ke Data Ephemeris Default

Saat Anda mengunggah data ephemeris khusus, itu akan mengganti penggunaan AWS Ground Station ephemerides default untuk satelit tertentu. AWS Ground Station tidak menggunakan ephemeris default lagi sampai saat ini tidak ada ephemerides yang disediakan pelanggan yang belum kedaluwarsa yang saat ini tersedia untuk digunakan. AWS Ground Station juga tidak mencantumkan kontak melewati waktu kedaluwarsa ephemeris yang disediakan pelanggan saat ini, bahkan jika ada ephemeris default yang tersedia melewati waktu kedaluwarsa tersebut.

Untuk kembali ke ephemerides Space Track default, Anda perlu melakukan salah satu hal berikut:

- Hapus (menggunakan`DeleteEphemeris`) atau menonaktifkan (menggunakan`UpdateEphemeris`) semua ephemerides yang disediakan pelanggan yang diaktifkan. Anda dapat membuat daftar ephemerides yang disediakan pelanggan untuk menggunakan satelit. `ListEphemerides`
- Tunggu semua ephemerides yang disediakan pelanggan yang ada kedaluwarsa.

Anda dapat mengonfirmasi bahwa ephemeris default sedang digunakan dengan memanggil `GetSatellite` dan memverifikasi bahwa ephemeris saat ini untuk satelit adalah. `source` `SPACE_TRACK` Lihat Data Ephemeris Default untuk informasi selengkapnya tentang ephemerides default.

AWS Ground Station Masker Situs

Setiap lokasi AWS Ground Station antena memiliki topeng situs terkait. Masker ini memblokir antena di lokasi itu agar tidak mentransmisikan atau menerima saat menunjuk ke beberapa arah, biasanya dekat dengan cakrawala. Topeng dapat memperhitungkan:

- Fitur medan geografis yang mengelilingi antena. Misalnya, ini termasuk hal-hal seperti gunung atau bangunan, yang akan memblokir sinyal frekuensi radio (RF) atau mencegah transmisi.
- Interferensi Frekuensi Radio (RFI) Ini memengaruhi kemampuan untuk menerima (sumber RFI eksternal yang memengaruhi sinyal downlink ke antena AWS Ground Station) dan transmisi (sinyal RF yang ditransmisikan oleh antena AWS Ground Station berdampak buruk pada penerima eksternal).
- Otorisasi hukum. Otorisasi situs lokal untuk mengoperasikan AWS Ground Station di setiap wilayah dapat mencakup pembatasan khusus, seperti sudut elevasi minimum untuk transmisi.

Masker situs ini dapat berubah seiring waktu. Misalnya, bangunan baru dapat dibangun di dekat lokasi antena, sumber RFI dapat berubah, atau otorisasi hukum dapat diperbarui dengan pembatasan yang berbeda. Masker situs AWS Ground Station tersedia untuk pelanggan berdasarkan perjanjian non-disclosure (NDA).

Masker Khusus Pelanggan

Selain masker situs AWS Ground Station di setiap situs, setiap pelanggan mungkin memiliki masker tambahan karena pembatasan otorisasi hukum mereka sendiri untuk berkomunikasi dengan satelit mereka di wilayah tertentu. Masker semacam itu dapat dikonfigurasi di AWS Ground case-by-case Station untuk memastikan kepatuhan saat menggunakan AWS Ground Station untuk berkomunikasi dengan satelit ini. Hubungi tim AWS Ground Station untuk detailnya.

Dampak Masker Situs pada Waktu Kontak yang Tersedia

Ada dua jenis masker situs: topeng situs uplink (kirim), dan topeng situs downlink (terima).

Saat mencantumkan waktu kontak yang tersedia menggunakan ListContacts operasi, AWS Ground Station akan mengembalikan waktu visibilitas berdasarkan kapan satelit Anda akan naik di atas dan disetel di bawah downlink mask. Waktu kontak yang tersedia didasarkan pada jendela visibilitas

downlink mask ini. Ini memastikan bahwa pelanggan tidak memesan atau membayar waktu ketika satelit mereka berada di bawah downlink mask.

Masker situs Uplink tidak diterapkan pada waktu kontak yang tersedia, bahkan jika Profil Misi menyertakan Konfigurasi Uplink Antena di tepi aliran data. Hal ini memungkinkan pelanggan untuk menggunakan semua waktu kontak yang tersedia untuk downlink, bahkan jika uplink mungkin tidak tersedia untuk sebagian waktu itu karena topeng situs uplink. Namun, sinyal uplink mungkin tidak ditransmisikan untuk beberapa atau sepanjang waktu yang disediakan untuk kontak satelit. Pelanggan bertanggung jawab untuk menghitung masker uplink yang disediakan saat menjadwalkan transmisi uplink.

Bagian kontak yang tidak tersedia untuk uplink bervariasi tergantung pada lintasan satelit selama kontak, relatif terhadap topeng situs uplink di lokasi antena. Di daerah di mana topeng situs uplink dan downlink serupa, durasi ini biasanya akan pendek. Di wilayah lain, di mana topeng uplink mungkin jauh lebih tinggi daripada topeng situs downlink, ini dapat mengakibatkan sebagian besar, atau bahkan semua, durasi kontak tidak tersedia untuk uplink. Waktu kontak penuh ditagih kepada pelanggan, bahkan jika sebagian dari waktu yang dipesan tidak tersedia untuk uplink.

Riwayat Dokumen untuk Panduan AWS Ground Station Pengguna

Tabel berikut menjelaskan perubahan penting pada dokumentasi sejak rilis terakhir AWS Ground Station.

Perubahan	Deskripsi	Tanggal Rilis
Fitur Baru	Kontak sekarang dapat dijadwalkan hingga 30 detik di luar rentang waktu visibilitas. Waktu visibilitas termasuk dalam DescribeContact tanggapan.	26 Mar 2024
Pembaruan Dokumentasi	Organisasi yang ditingkatkan dan menambahkan bagian “Pemilihan Instans EC2 dan Perencanaan CPU”.	Mar 6, 2024
Pembaruan Dokumentasi	Menambahkan praktik terbaik baru ke Panduan Pengguna AWS Ground Station Agen untuk menjalankan layanan dan proses bersama AWS Ground Station Agen.	Februari 23, 2024
Pembaruan Dokumentasi	Ditambahkan halaman Catatan Rilis Agen.	21 Februari 2024
Pembaruan Template	Ditambahkan dukungan untuk subnet publik terpisah dalam DataDelivery template DirectBroadcastSatelliteWbDigIfEc 2.	14 Februari 2024
Pembaruan Dokumentasi	Menambahkan rujukan ke AWS Notifikasi Pengguna dalam dokumentasi pemantauan.	Agustus 6, 2023
Pembaruan Dokumentasi	Menambahkan instruksi untuk menandai satelit dengan nama yang akan ditampilkan di konsol. AWS Ground Station	26 Juli 2023

Perubahan	Deskripsi	Tanggal Rilis
Fitur Baru	Menambahkan Panduan Pengguna AWS Ground Station Agen untuk rilis Pengiriman Data DiGIF Wideband	12 April 2023
Pembaruan kebijakan terkelola AWS — Kebijakan AWS terkelola baru	AWS Ground Station menambahkan kebijakan baru bernama AWSGroundStationAgentInstancePolicy.	12 April 2023
Fitur Baru	Memperbarui panduan pengguna untuk rilis Pratinjau CPE.	9 November 2022
Pembaruan kebijakan terkelola AWS — Kebijakan AWS terkelola baru	AWS Ground Station menambahkan AWSServiceRoleForGroundStationDataflowEndpointGroup service-linked-role (SLR) yang menyertakan kebijakan baru bernama AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy.	November 02, 2022
Fitur Baru	Memperbarui panduan pengguna untuk menyertakan integrasi dengan AWS CLI.	17 April 2020
Fitur Baru	Memperbarui panduan pengguna untuk menyertakan integrasi dengan CloudWatch Metrik.	24 Februari 2020
Template Baru	Satelit Siaran Publik (AquaSnppJpss Template) ditambahkan ke Panduan Pengguna.AWS Ground Station	19 Februari 2020
Fitur Baru	Memperbarui panduan pengguna untuk menyertakan pengiriman data lintas wilayah.	5 Februari 2020
Pembaruan Dokumentasi	Contoh dan deskripsi yang diperbarui untuk pemantauan AWS Ground Station dengan CloudWatch Acara.	4 Februari 2020

Perubahan	Deskripsi	Tanggal Rilis
Pembaruan Dokumentasi	Lokasi template telah diperbarui dan bagian Memulai dan Pemecahan Masalah telah direvisi.	19 Desember 2019
Bagian Pemecahan Masalah Baru	Bagian pemecahan masalah ditambahkan ke AWS Ground Station Panduan Pengguna.	7 November 2019
Topik Memulai Baru	Memperbarui topik Memulai, yang mencakup AWS CloudFormation template terbaru.	1 Juli 2019
Versi Kindle	Versi Kindle yang diterbitkan dari Panduan AWS Ground Station Pengguna.	20 Juni 2019
Layanan dan panduan baru	Ini adalah rilis awal AWS Ground Station dan Panduan AWS Ground Station Pengguna.	23 Mei 2019

AWSGlosarium

Untuk AWS terminologi terbaru, lihat AWSglosarium di Referensi. Glosarium AWS

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