aws

Panduan Pengguna

# AWS Ground Station

# AWS Ground Station: Panduan Pengguna

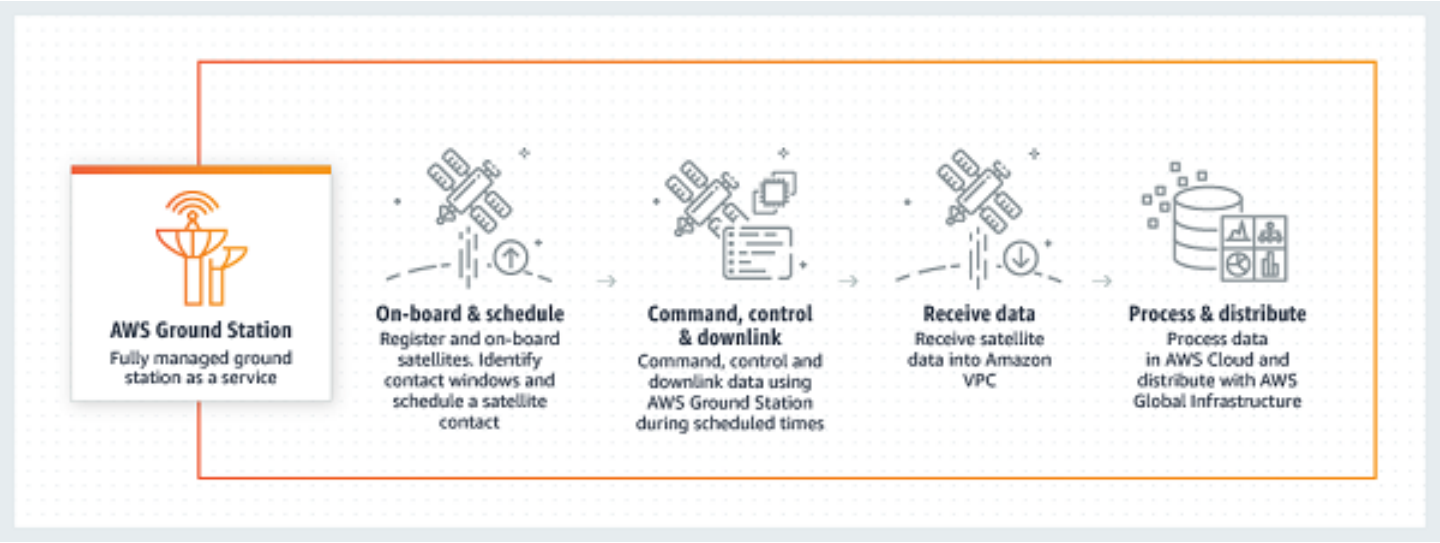
# Table of Contents

# Apa itu AWS Ground Station?

AWS Ground Station adalah layanan yang dikelola sepenuhnya yang menyediakan komunikasi satelit yang aman, cepat, dan dapat diprediksi di seluruh infrastruktur global. Dengan AWS Ground Station, Anda tidak lagi harus membangun, mengelola, atau menskalakan infrastruktur stasiun bumi Anda sendiri. AWS Ground Station memungkinkan Anda untuk fokus pada inovasi dan bereksperimen dengan cepat dengan aplikasi baru yang menyerap data satelit, daripada menghabiskan sumber daya untuk membangun, mengoperasikan, dan menskalakan stasiun bumi Anda sendiri.

Dengan menggunakan jaringan serat global dengan latensi rendah dan bandwidth tinggi AWS, Anda dapat mulai memproses data satelit Anda dalam hitungan detik setelah penerimaan di sistem antena. Ini memungkinkan Anda untuk mengubah data mentah menjadi informasi yang diproses atau pengetahuan yang dianalisis dalam hitungan detik.

## Kasus penggunaan umum




AWS Ground Station memungkinkan Anda untuk berkomunikasi dengan satelit Anda dua arah dan mendukung kasus penggunaan berikut:

- Data downlink — Menerima data dari satelit Anda, mentransmisikan frekuensi X-band dan S-band, dikirimkan ke EC2 instans Amazon secara real-time (format VITA-49), atau langsung ke bucket Amazon S3 di akun Anda (format PCAP). Selain itu, untuk satelit yang menggunakan skema modulasi dan pengkodean yang didukung, Anda dapat memilih antara menerima data yang

didemodulasi dan diterjemahkan, atau sampel frekuensi menengah digital mentah (DiGIF) (format VITA-49).

- Uplink data — Kirim data dan perintah ke satelit Anda, yang menerima frekuensi S-band, dengan mengirimkan data DiGIF (format VITA-49) untuk ditransmisikan oleh. AWS Ground Station
- Uplink echo — Validasi perintah yang dikirim ke pesawat ruang angkasa Anda, dan lakukan tugas-tugas lanjutan lainnya, dengan menerima sinyal yang ditransmisikan pada antena yang ditempatkan bersama secara fisik.
- Software Defined Radio (SDR) /Front End Processor (FEP) - Gunakan SDR and/or FEP, that's capable of running on an Amazon EC2 instance, to process your data in real-time to send/receive Anda yang ada bentuk gelombang yang ada, dan hasilkan produk data Anda.
- Telemetri, Pelacakan, dan Perintah (TT&C) — Lakukan TT&C menggunakan kombinasi kasus penggunaan yang terdaftar sebelumnya untuk mengelola armada satelit Anda.
- Pengiriman Data Lintas Wilayah — Mengoperasikan beberapa kontak simultan menggunakan AWS Ground Station jaringan antena global dari satu Wilayah AWS.
- Digital twin — Uji penjadwalan, verifikasi konfigurasi, dan penanganan kesalahan yang tepat dengan biaya yang lebih rendah tanpa menggunakan kapasitas antena produksi.

## Langkah selanjutnya

Kami menyarankan Anda untuk memulai dengan membaca bagian berikut:

- Untuk mempelajari AWS Ground Station konsep-konsep penting, lihatBagaimana cara AWS Ground Station kerja.
- Untuk mempelajari cara menyiapkan akun dan sumber daya yang akan digunakan AWS Ground Station, lihatMemulai .
- Untuk menggunakan secara terprogram AWS Ground Station, silakan merujuk ke Referensi AWS Ground Station API. Referensi API menjelaskan semua operasi API AWS Ground Station secara detail. Ini juga menyediakan permintaan sampel, tanggapan, dan kesalahan untuk protokol layanan web yang didukung. Anda dapat menggunakan AWS CLI, atau AWS SDK, dalam bahasa pilihan Anda, untuk menulis kode yang berinteraksi dengannya. AWS Ground Station

# Bagaimana cara AWS Ground Station kerja

AWS Ground Station mengoperasikan antena berbasis darat untuk memfasilitasi komunikasi dengan satelit Anda. Karakteristik fisik dari apa yang dapat dilakukan antena diabstraksikan dan disebut sebagai kemampuan. Lokasi fisik antena beserta kemampuannya saat ini dapat direferensikan di AWS Ground Station Lokasi bagian tersebut. Silakan hubungi kami di <aws-groundstation@amazon.com> jika kasus penggunaan Anda memerlukan kemampuan tambahan, penawaran lokasi tambahan, atau lokasi antena yang lebih tepat.

Untuk menggunakan salah satu AWS Ground Station antena, Anda harus memesan waktu di lokasi tertentu. Reservasi ini disebut sebagai kontak. Untuk berhasil menjadwalkan kontak, AWS Ground Station memerlukan data tambahan untuk memastikan keberhasilannya.

- Satelit Anda harus onboard ke satu atau beberapa lokasi — Ini memastikan Anda memiliki persetujuan untuk mengoperasikan berbagai kemampuan di lokasi yang diminta.
- Satelit Anda harus memiliki ephemeris yang valid — Ini memastikan antena memiliki garis pandang dan dapat secara akurat menunjuk ke satelit Anda selama kontak.
- Anda harus memiliki profil misi yang valid — Ini memungkinkan Anda untuk menyesuaikan bagaimana kontak ini akan berperilaku termasuk bagaimana Anda akan menerima dan mengirim data ke satelit Anda. Anda dapat menggunakan beberapa profil misi untuk kendaraan yang sama untuk membuat kontak yang berbeda agar sesuai dengan postur operasi atau skenario yang berbeda yang Anda temui.

## Orientasi satelit

Memasukkan satelit ke dalam AWS Ground Station adalah proses multistep yang melibatkan pengumpulan data, validasi teknis, lisensi spektrum, dengan integrasi dan pengujian. Bagian orientasi satelit dari panduan ini akan memandu Anda melalui proses ini.

## Komposisi profil misi

Informasi frekuensi satelit, informasi pesawat data, dan detail lainnya dienkapsulasi ke dalam profil misi. Profil misi adalah kumpulan komponen konfigurasi. Ini memungkinkan Anda untuk menggunakan kembali komponen konfigurasi di berbagai profil misi yang sesuai dengan kasus penggunaan Anda. Karena profil misi tidak secara langsung merujuk satelit individu, tetapi hanya

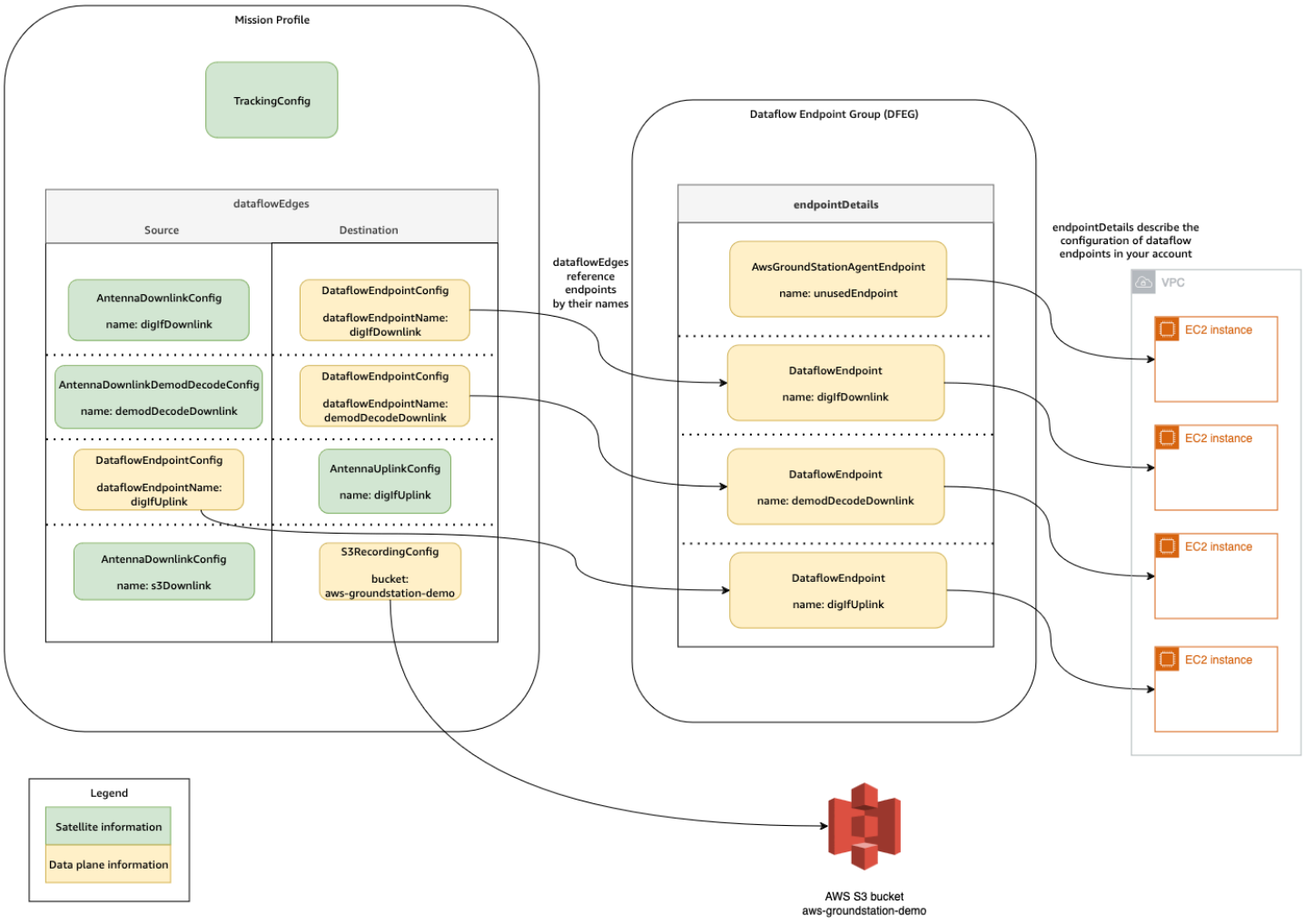
memiliki informasi tentang kemampuan teknis mereka, profil misi juga dapat digunakan kembali oleh beberapa satelit yang memiliki konfigurasi yang sama.

Profil misi yang valid akan memiliki konfigurasi pelacakan dan satu atau beberapa aliran data. Konfigurasi pelacakan akan menentukan preferensi Anda untuk melacak selama kontak. Setiap pasangan konfigurasi dalam aliran data menetapkan sumber dan tujuan. Bergantung pada satelit Anda dan mode operasionalnya, jumlah aliran data yang tepat akan bervariasi dalam profil misi untuk mewakili jalur komunikasi uplink dan downlink Anda serta aspek pemrosesan data apa pun.

- Untuk informasi selengkapnya tentang mengonfigurasi VPC Amazon, Amazon S3, dan sumber daya EC2 Amazon yang akan digunakan selama kontak, lihat. Bekerja dengan aliran data
- Untuk detail tentang bagaimana setiap konfigurasi berperilaku, lihat. Gunakan AWS Ground Station Konfigurasi
- Untuk detail spesifik tentang semua parameter yang diharapkan, lihatGunakan Profil AWS Ground Station Misi.
- Untuk contoh tentang bagaimana berbagai profil misi dapat dibuat untuk mendukung kasus penggunaan Anda, lihatContoh konfigurasi profil misi.

Diagram berikut menunjukkan contoh profil misi dan sumber daya tambahan yang dibutuhkan. Perhatikan bahwa contoh menunjukkan titik akhir aliran data yang tidak diperlukan untuk profil misi ini, bernama UnusedEndPoint, untuk menunjukkan fleksibilitas. Contoh ini mendukung aliran data berikut:

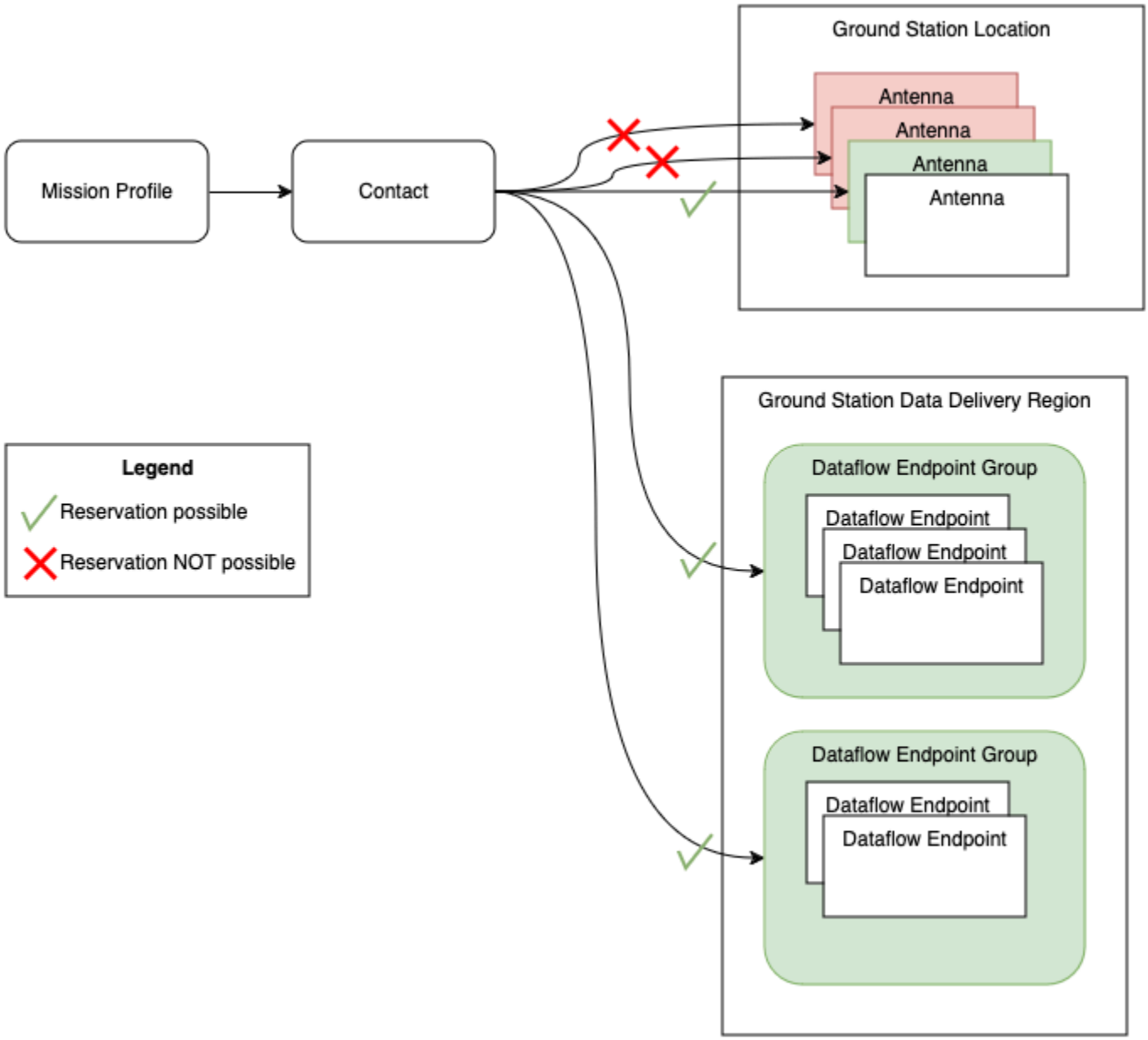
- Downlink sinkron data frekuensi menengah digital ke EC2 instans Amazon yang Anda kelola. Dilambangkan dengan nama. digIfDownlink
- Downlink asinkron data frekuensi menengah digital ke bucket Amazon S3. Dilambangkan dengan nama ember. aws-groundstation-demo
- Downlink sinkron data yang didemodulasi dan diterjemahkan ke instans Amazon EC2 yang Anda kelola. Dilambangkan dengan nama. demodDecodeDownlink
- Uplink sinkron data dari EC2 instans Amazon yang Anda kelola ke antena terkelola. AWS Ground Station Dilambangkan dengan nama. digIfUplink




# Penjadwalan kontak

Dengan profil misi yang valid, Anda dapat meminta kontak dengan satelit onboard Anda. Permintaan reservasi kontak bersifat asinkron untuk memberikan waktu bagi layanan antena global untuk mencapai jadwal yang konsisten di semua AWS Wilayah yang terlibat. Selama proses ini, berbagai antena di lokasi stasiun bumi yang diminta dievaluasi untuk menentukan apakah tersedia dan mampu memproses kontak. Selama proses ini, titik akhir aliran data Anda yang dikonfigurasi juga dievaluasi untuk menentukan ketersediaannya. Sementara evaluasi ini terjadi, status kontak akan dalam PENJADWALAN.

Proses penjadwalan asinkron ini akan selesai dalam waktu lima menit setelah permintaan, tetapi biasanya selesai dalam satu menit. Harap tinjau pemantauan berbasis acara Otomatisasi AWS Ground Station dengan Acara selama waktu penjadwalan.




Kontak yang dapat dilakukan dan memiliki ketersediaan menghasilkan kontak TERJADWAL. Dengan kontak terjadwal, sumber daya yang diperlukan untuk melakukan kontak Anda telah dipesan di seluruh Wilayah AWS yang diperlukan sebagaimana ditentukan oleh profil misi Anda. Kontak yang tidak dapat dilakukan, atau memiliki bagian yang tidak tersedia akan menghasilkan kontak FAILED_TO_SCHEDULE. Lihat Memecahkan masalah kontak FAILED_TO_SCHEDULE detail debugging.

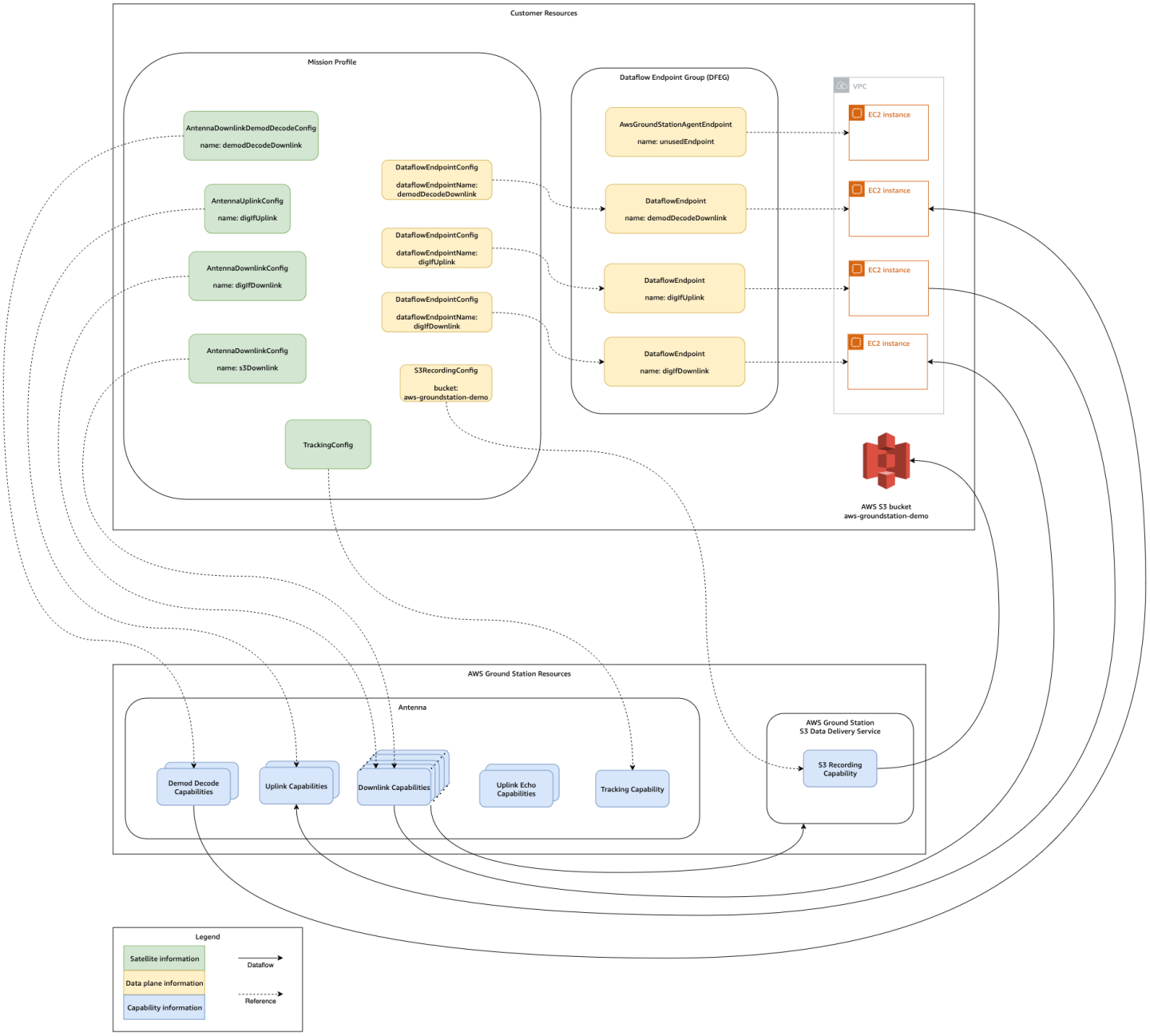
# Eksekusi kontak

AWS Ground Station akan secara otomatis mengatur sumber daya yang dikelola AWS Anda selama reservasi kontak Anda. Jika berlaku, Anda bertanggung jawab untuk mengatur EC2 sumber daya yang ditentukan oleh profil misi Anda sebagai titik akhir aliran data. AWS Ground Station menyediakan AWS EventBridge Events untuk mengotomatiskan orkestrasi sumber daya Anda untuk mengurangi biaya. Lihat Otomatisasi AWS Ground Station dengan Acara untuk detail selengkapnya.

Selama kontak, telemetri tentang kinerja kontak Anda dikirimkan ke AWS. CloudWatch Untuk informasi tentang cara memantau kontak Anda selama eksekusi, silakan lihatMemahami pemantauan dengan AWS Ground Station.

Diagram berikut melanjutkan contoh sebelumnya dengan menunjukkan sumber daya yang sama diatur selama kontak.

> **Note**
>
> Tidak semua kemampuan antena digunakan dalam contoh ini. Misalnya, ada lebih dari selusin kemampuan downlink antena yang tersedia di setiap antena yang mendukung beberapa frekuensi dan polarisasi. Untuk detail lebih lanjut tentang jumlah setiap jenis kemampuan yang tersedia dari AWS Ground Station antena, dan frekuensi dan polarisasi yang didukung, lihat. AWS Ground Station Kemampuan Situs




Di akhir kontak Anda, AWS Ground Station akan menilai kinerja kontak Anda dan akan menentukan status kontak akhir. Kontak di mana tidak ada kesalahan yang terdeteksi akan menghasilkan status kontak LENGKAP. Kontak di mana kesalahan layanan telah menyebabkan masalah pengiriman data selama kontak akan menghasilkan AWS_FAILEDstatus. Kontak di mana kesalahan klien atau pengguna menyebabkan masalah pengiriman data selama kontak akan menghasilkan status GAGAL. Kesalahan di luar waktu kontak, yaitu selama pre-pass atau post-pass, tidak diperhitungkan selama ajudikasi.

Untuk informasi selengkapnya, lihat Memahami siklus hidup kontak.

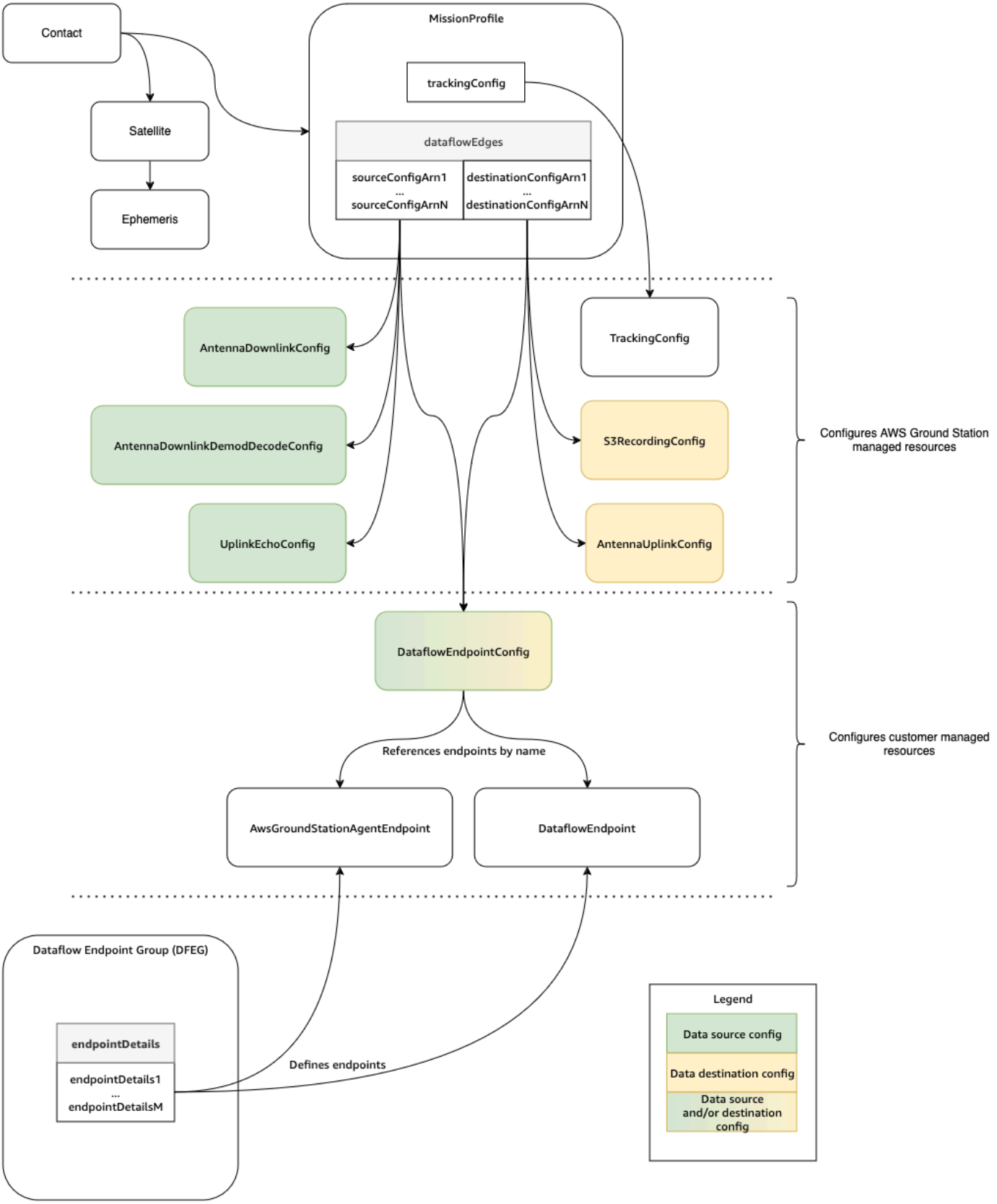
# Kembar digital

Fitur kembar digital untuk AWS Ground Station memungkinkan Anda menjadwalkan kontak dengan lokasi stasiun bumi virtual. Stasiun bumi virtual ini adalah replika yang tepat dari stasiun bumi produksi termasuk kemampuan antena, masker situs, dan koordinat GPS yang sebenarnya. Fitur kembar digital memungkinkan Anda untuk menguji alur kerja orkestrasi kontak Anda untuk sebagian kecil dari biaya dibandingkan dengan stasiun bumi produksi. Lihat Gunakan fitur kembar AWS Ground Station digital untuk informasi selengkapnya.

# Memahami komponen AWS Ground Station Inti

Bagian ini memberikan definisi terperinci untuk komponen inti AWS Ground Station.

Diagram berikut menunjukkan komponen inti AWS Ground Station dan bagaimana mereka berhubungan satu sama lain. Panah menunjukkan arah dependensi antar komponen, di mana setiap komponen menunjuk ke dependensinya.


Contact
Satellite
Ephemeris
MissionProfile
trackingConfig
dataflowEdges
sourceConfigArn1
...
sourceConfigArnN
destinationConfigArn1
...
destinationConfigArnN
AntennaDownlinkConfig
AntennaDownlinkDemodDecodeConfig
UplinkEchoConfig
TrackingConfig
S3RecordingConfig
AntennaUplinkConfig
Configures AWS Ground Station managed resources
DataflowEndpointConfig
References endpoints by name
AwsGroundStationAgentEndpoint
DataflowEndpoint
Configures customer managed resources
Dataflow Endpoint Group (DFEG)
endpointDetails
endpointDetails1
...
endpointDetailsM
Defines endpoints
Legend
Data source config
Data destination config
Data source and/or destination config

Topik berikut menjelaskan komponen AWS Ground Station inti secara rinci.

Topik



## Gunakan Profil AWS Ground Station 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.

Profil misi dapat dibagikan di seluruh satelit yang memiliki karakteristik radio yang sama. Anda dapat membuat grup titik akhir aliran data tambahan untuk mengikat kontak simultan maksimum yang ingin Anda lakukan untuk konstelasi Anda.

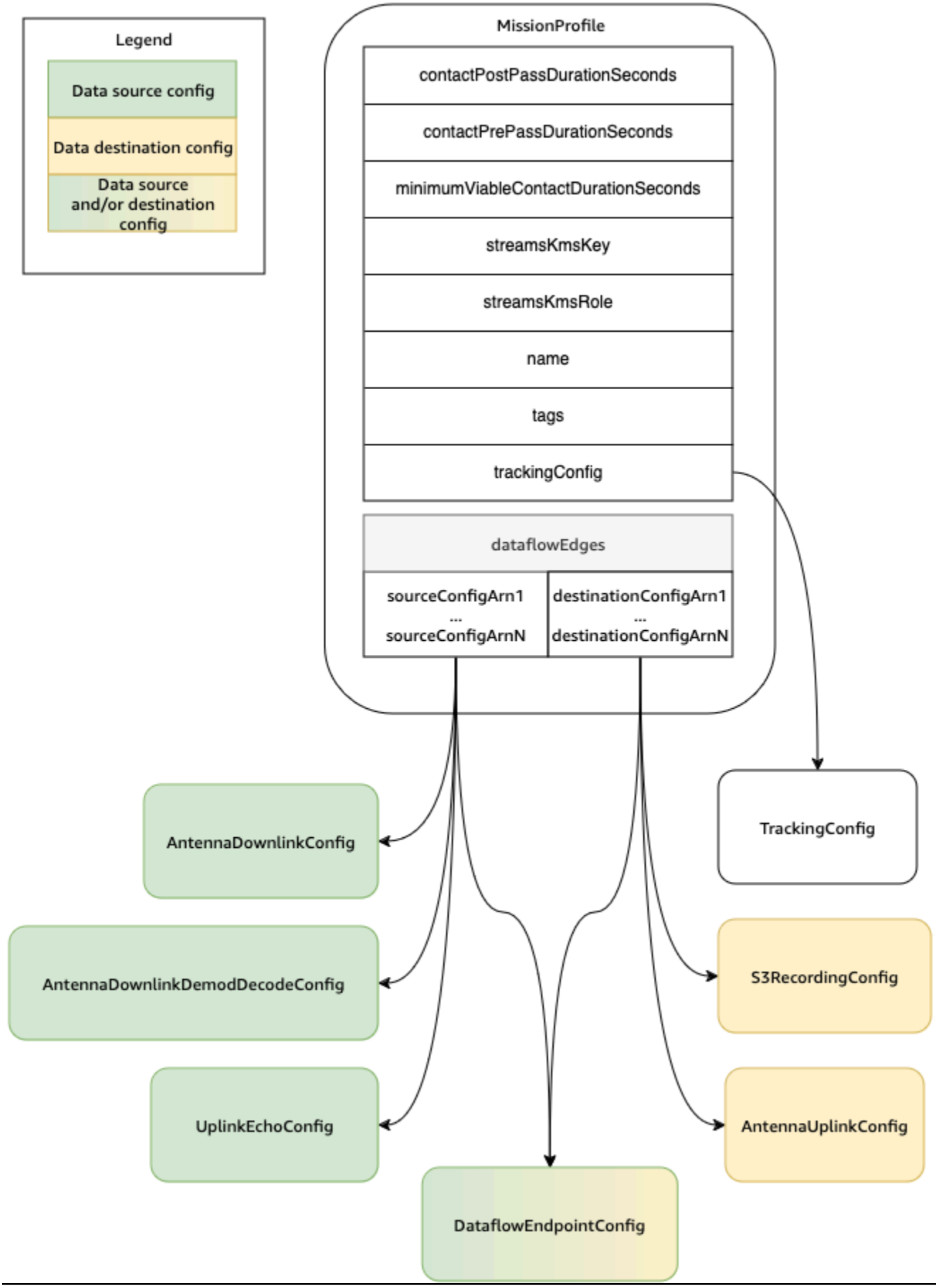
Konfigurasi pelacakan ditentukan sebagai bidang unik dalam profil misi. Konfigurasi pelacakan digunakan untuk menentukan preferensi Anda untuk menggunakan pelacakan program dan pelacakan otomatis selama kontak Anda. Untuk informasi selengkapnya, lihat Melacak Config.

Semua konfigurasi lainnya terkandung di `dataflowEdges` bidang profil misi. Konfigurasi ini dapat dianggap sebagai node aliran data yang masing-masing mewakili sumber daya AWS Ground Station terkelola yang dapat mengirim atau menerima data dan konfigurasi terkait. `dataflowEdges`Bidang menentukan node aliran data sumber dan tujuan (konfigurasi) mana yang diperlukan. Satu tepi aliran data adalah daftar dua konfigurasi Amazon Resource Names ARNs () —yang pertama adalah konfigurasi sumber dan yang kedua adalah konfigurasi tujuan. Dengan menentukan tepi aliran data antara dua konfigurasi, Anda memberi tahu AWS Ground Station dari mana dan ke mana data harus mengalir selama kontak. Untuk informasi selengkapnya, lihat Gunakan AWS Ground Station Konfigurasi.

Itu `contactPrePassDurationSeconds` dan `contactPostPassDurationSeconds` memungkinkan Anda untuk menentukan waktu relatif terhadap kontak di mana Anda akan menerima pemberitahuan CloudWatch Acara. Untuk jadwal acara yang terkait dengan kontak Anda, silakan bacaMemahami siklus hidup kontak.

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

`streamsKmsRole`Dan `streamsKmsKey` digunakan untuk menentukan enkripsi yang digunakan oleh AWS Ground Station untuk pengiriman data Anda dengan AWS Ground Station Agen. Silakan lihat[Enkripsi data selama transit untuk AWS Ground Station](#).


Legend
Data source config
Data destination config
Data source and/or destination config
MissionProfile
contactPostPassDurationSeconds
contactPrePassDurationSeconds
minimumViableContactDurationSeconds
streamsKmsKey
streamsKmsRole
name
tags
trackingConfig
dataflowEdges
sourceConfigArn1 ... sourceConfigArnN
destinationConfigArn1 ... destinationConfigArnN
AntennaDownlinkConfig
AntennaDownlinkDemodDecodeConfig
UplinkEchoConfig
TrackingConfig
S3RecordingConfig
AntennaUplinkConfig
DataflowEndpointConfig

Daftar lengkap parameter dan contoh disertakan pada dokumentasi berikut.

- AWS::GroundStation::MissionProfile CloudFormation jenis sumber daya

## Gunakan AWS Ground Station 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. Konfigurasi dapat dikelompokkan menjadi dua kategori:

- Melacak konfigurasi
- Konfigurasi aliran data

A TrackingConfigadalah satu-satunya jenis konfigurasi pelacakan. Ini digunakan untuk mengkonfigurasi pengaturan autotrack antena selama kontak, dan diperlukan dalam profil misi.

Konfigurasi yang dapat digunakan dalam aliran data profil misi dapat dianggap sebagai node aliran data yang masing-masing mewakili sumber daya AWS Ground Station terkelola yang dapat mengirim atau menerima data. Profil misi memerlukan setidaknya satu pasang konfigurasi ini, dengan satu mewakili sumber data, dan satu mewakili tujuan. Konfigurasi ini dirangkum dalam tabel berikut.

| Nama Config | Sumber/tujuan aliran data |
|---|---|
| AntennaDownlinkConfig | Sumber |
| AntennaDownlinkDemodDecodeConfig | Sumber |
| UplinkEchoConfig | Sumber |
| S3 RecordingConfig | Tujuan |
| AntennaUplinkConfig | Tujuan |
| DataflowEndpointConfig | Sumber dan/atau Tujuan |

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

## 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.

AWS Ground Station akan menggunakan pelacakan terprogram yang akan menunjuk berdasarkan ephemeris Anda saat autotrack tidak digunakan. Silakan referensi Memahami bagaimana AWS Ground Station menggunakan data ephemeris satelit untuk detail tentang bagaimana ephemeris dibangun.

Autotrack akan menggunakan pelacakan program sampai sinyal yang diharapkan ditemukan. Setelah itu terjadi, ia akan terus melacak berdasarkan kekuatan sinyal.

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.

Konfigurasi ini merupakan simpul sumber dalam aliran data. Ini bertanggung jawab untuk mendigitalkan data frekuensi radio. Data yang dialirkan dari node ini akan mengikuti Format Data/IP Sinyal. Untuk informasi lebih rinci tentang cara membuat aliran data dengan konfigurasi ini, lihat Bekerja dengan aliran data

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 demodulasi dan/atau decoding.
`<Jika Anda tertarik untuk mengeksekusi jenis kontak ini, hubungi AWS Ground Stat`
Kami akan membantu Anda menentukan konfigurasi dan profil misi yang tepat untuk kasus penggunaan Anda.

Konfigurasi ini merupakan simpul sumber dalam aliran data. Ini bertanggung jawab untuk mendigitalkan data frekuensi radio dan melakukan demodulasi dan decoding seperti yang ditentukan. Data yang dialirkan dari node ini akan mengikuti Demodulated/Decoded Data/IP Format. Untuk informasi lebih rinci tentang cara membuat aliran data dengan konfigurasi ini, lihat Bekerja dengan aliran data

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. Antena Uplink Echo Config

Konfigurasi ini merupakan node tujuan dalam aliran data. Ini akan mengubah sinyal data frekuensi radio digital yang disediakan menjadi sinyal analog dan memancarkannya untuk diterima satelit Anda. Data yang dialirkan ke node ini diharapkan memenuhi Format Data/IP Sinyal. Untuk informasi lebih rinci tentang cara membuat aliran data dengan konfigurasi ini, lihat Bekerja dengan aliran data

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

## Antena Uplink Echo Config

Konfigurasi gema uplink memberi tahu antena cara menjalankan gema uplink. Gema uplink dapat digunakan untuk memvalidasi perintah yang dikirim ke pesawat ruang angkasa Anda, dan melakukan tugas-tugas lanjutan lainnya. Ini dicapai dengan merekam sinyal aktual yang ditransmisikan oleh AWS Ground Station antena (yaitu uplink). Ini menggemakan sinyal yang dikirim oleh antena kembali ke titik akhir aliran data Anda dan harus sesuai dengan sinyal yang ditransmisikan. Konfigurasi gema

uplink berisi ARN dari konfigurasi uplink. Antena menggunakan parameter dari konfigurasi uplink yang ditunjuk oleh ARN saat menjalankan gema uplink.

Konfigurasi ini merupakan simpul sumber dalam aliran data. Data yang dialirkan dari node ini akan memenuhi Format Data/IP Sinyal. Untuk informasi lebih rinci tentang cara membuat aliran data dengan konfigurasi ini, lihat Bekerja dengan aliran data

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

## Konfigurasi Titik Akhir Dataflow

> **Note**
>
> Konfigurasi titik akhir Dataflow 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 dalam AWS Wilayah yang berisi semua titik akhir aliran data yang ditentukan oleh konfigurasi titik akhir aliran data yang terdapat dalam profil misi Anda. Jika grup titik akhir aliran data yang sesuai ditemukan, status kontak akan menjadi DIJADWALKAN, jika tidak maka akan menjadi FAILED_TO_SCHEDULE. Untuk informasi lebih lanjut tentang kemungkinan status kontak, lihatAWS Ground Station status kontak.

`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 Bekerja dengan aliran data untuk informasi lebih lanjut tentang aliran data lintas wilayah.

Lihat Gunakan grup AWS Ground Station titik akhir Dataflow tips tentang bagaimana skema penamaan yang berbeda untuk aliran data Anda dapat bermanfaat bagi kasus penggunaan Anda.

Untuk informasi lebih rinci tentang cara membuat aliran data dengan konfigurasi ini, lihat Bekerja dengan aliran data

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 Amazon S3

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

Konfigurasi ini merupakan node tujuan dalam aliran data. Node ini akan merangkum data yang masuk dari node sumber aliran data ke dalam data pcap. Untuk informasi lebih rinci tentang cara membuat aliran data dengan konfigurasi ini, lihat Bekerja dengan aliran data

Anda dapat menggunakan konfigurasi perekaman S3 untuk menentukan bucket Amazon S3 yang ingin dikirimkan data downlink bersama dengan konvensi penamaan yang digunakan. Berikut ini menentukan batasan dan rincian tentang parameter ini:

- 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 trust harus menggunakan tanda bintang (*) sebagai pengganti *your-config-id* dan dapat diperbarui setelah dibuat dengan id sumber daya konfigurasi.

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"
        }
      }
    }
  ]
}
```

- 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 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/*"
      ]
    }
  ]
}
```

- Awalan akan digunakan saat menamai objek data S3. Anda dapat menentukan kunci opsional untuk substitusi, nilai-nilai ini akan diganti dengan informasi yang sesuai dari detail kontak Anda. Misalnya, awalan `{satellite_id}/{year}/{month}/{day}` akan diganti dan akan menghasilkan output seperti `fake_satellite_id/2021/01/10`

  Kunci opsional untuk substitusi: `{satellite_id}` | `{config-name}` | `{config-id}` | `{year}` | `{month}` | `{day}`

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 bagians3RecordingConfig -> (structure))
- Referensi RecordingConfig API S3

## Gunakan grup AWS Ground Station titik akhir Dataflow

Titik akhir Dataflow menentukan lokasi tempat Anda ingin data dialirkan secara sinkron ke atau dari selama kontak. 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.

> **Tip**
>
> Titik akhir aliran data diidentifikasi dengan nama yang Anda pilih saat menjalankan kontak. Nama-nama ini tidak harus unik di seluruh akun. Hal ini memungkinkan beberapa kontak di satelit dan antena yang berbeda untuk dieksekusi pada saat yang sama menggunakan profil misi yang sama. Ini dapat berguna jika Anda memiliki konstelasi satelit yang memiliki karakteristik operasi yang sama. Anda dapat menskalakan jumlah grup titik akhir aliran data agar sesuai dengan jumlah maksimum kontak simultan yang dibutuhkan oleh konstelasi satelit 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.

> **Important**
>
> Grup titik akhir aliran data harus dalam HEALTHY keadaan untuk menjadwalkan kontak yang menggunakannya. Untuk informasi tentang cara memecahkan masalah grup

titik akhir aliran data yang tidak dalam status, lihat. HEALTHY Memecahkan masalah DataflowEndpointGroups tidak dalam keadaan SEHAT

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::DataflowEndpointGroup CloudFormation jenis sumber daya
- Referensi Dataflow Endpoint Group AWS CLI
- Referensi API Grup Titik Akhir Dataflow

## Titik akhir aliran data

Anggota grup titik akhir aliran data adalah titik akhir aliran data. Ada dua jenis titik akhir aliran data: titik akhir AWS Ground Station Agen, dan titik akhir Dataflow. Untuk kedua jenis titik akhir, Anda akan membuat konstruksi pendukung (misalnya alamat IP) sebelum membuat grup endpoint aliran data. Silakan lihat Bekerja dengan aliran data rekomendasi tentang jenis titik akhir aliran data mana yang akan digunakan dan cara mengatur konstruksi pendukung.

Bagian berikut menjelaskan kedua jenis endpoint yang didukung.

**Important**

Semua titik akhir aliran data dalam satu grup titik akhir aliran data harus dari jenis yang sama. Anda tidak dapat mencampur titik akhir AWS Ground Station Agen dengan titik akhir Dataflow dalam grup yang sama. Jika kasus penggunaan Anda memerlukan kedua jenis titik akhir, Anda harus membuat grup titik akhir aliran data terpisah untuk setiap jenis.

### AWS Ground Station Titik akhir agen

AWS Ground Station Agen Endpoint menggunakan AWS Ground Station Agen sebagai komponen perangkat lunak untuk mengakhiri koneksi. Gunakan Endpoint Dataflow AWS Ground Station Agen saat Anda ingin downlink lebih besar dari 50 Data Sinyal Digital. MHz Untuk membangun Endpoint AWS Ground Station Agen, Anda hanya akan mengisi `AwsGroundStationAgentEndpoint` bidang. EndpointDetails Untuk informasi selengkapnya tentang AWS Ground Station Agen, lihat Panduan Pengguna AWS Ground Station Agen selengkapnya.

`AwsGroundStationAgentEndpoint`Terdiri dari yang berikut:

- `Name`- Nama titik akhir aliran data. Agar kontak dapat menggunakan titik akhir aliran data ini, nama ini harus cocok dengan nama yang digunakan dalam konfigurasi titik akhir aliran data Anda.
- `EgressAddress`- Alamat IP dan port yang digunakan untuk mengeluarkan data dari Agen.
- `IngressAddress`- Alamat IP dan port yang digunakan untuk memasukkan data ke Agen.

Titik akhir aliran data

Dataflow Endpoint menggunakan aplikasi jaringan sebagai komponen perangkat lunak untuk mengakhiri koneksi. Gunakan Dataflow Endpoint saat Anda ingin meningkatkan Data Sinyal Digital, downlink kurang dari 50 Data Sinyal Digital, atau downlink Demodulasi/Decoded MHz Signal Data. Untuk membangun Dataflow Endpoint, Anda akan mengisi dan bidang. `Endpoint` `Security Details` EndpointDetails

`Endpoint`Terdiri dari yang berikut:

- `Name`- Nama titik akhir aliran data. Agar kontak dapat menggunakan titik akhir aliran data ini, nama ini harus cocok dengan nama yang digunakan dalam konfigurasi titik akhir aliran data Anda.
- `Address`- Alamat IP dan port yang digunakan.

`SecurityDetails`Terdiri dari yang berikut:

- `roleArn`- Nama Sumber Daya Amazon (ARN) dari peran yang AWS Ground Station akan diasumsikan untuk membuat Antarmuka Jaringan Elastis (ENIs) di VPC Anda. Ini ENIs berfungsi sebagai titik masuk dan keluar dari data yang dialirkan selama kontak.
- `securityGroupIds`- Grup keamanan untuk dilampirkan ke antarmuka jaringan elastis.
- `subnetIds`- Daftar subnet di mana AWS Ground Station dapat menempatkan antarmuka jaringan elastis untuk mengirim aliran ke instance Anda. Jika beberapa subnet ditentukan, mereka harus dapat dirutekan satu sama lain. Jika subnet berada di Availability Zone (AZs) yang berbeda, Anda mungkin dikenakan biaya transfer data lintas-AZ.

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. ENIs 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"
      ]
    }
  ]
}
```

## Gunakan AWS Ground Station Agen

AWS Ground Station Agen memungkinkan Anda menerima aliran data Wideband Digital Intermediate Frequency (DiGIF) sinkron (downlink) selama kontak AWS Ground Station.

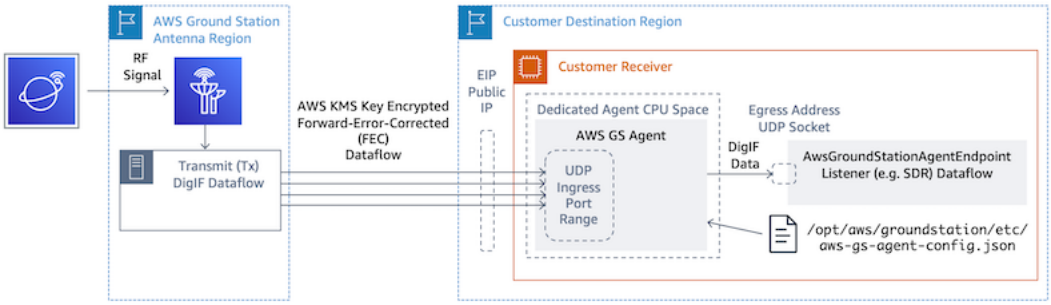
### Cara kerjanya

Anda dapat memilih dua opsi untuk pengiriman data:

1. Pengiriman data ke EC2 instance - Pengiriman data ke EC2 instance yang Anda miliki. Anda mengelola AWS Ground Station Agen. Opsi ini mungkin paling cocok untuk Anda jika Anda membutuhkan pemrosesan data mendekati waktu nyata. Lihat Bekerja dengan aliran data bagian untuk informasi tentang pengiriman EC2 data.
2. Pengiriman data ke bucket S3 - Pengiriman data ke bucket AWS S3 Anda dikelola sepenuhnya oleh. AWS Ground Station Lihat Memulai panduan untuk informasi tentang pengiriman data S3.

Kedua mode pengiriman data mengharuskan Anda membuat satu set sumber daya AWS. Penggunaan CloudFormation 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.

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




## Informasi tambahan

Untuk informasi lebih lanjut, silakan lihat Panduan Pengguna AWS Ground Station Agen lengkap.

# Memulai

Sebelum Anda mulai, Anda harus membiasakan diri dengan konsep dasar di AWS Ground Station. Untuk informasi selengkapnya, lihat Bagaimana cara AWS Ground Station kerja.

Di bawah ini adalah praktik terbaik untuk AWS Identity and Access Management (IAM) dan izin apa yang Anda perlukan. Setelah mengatur peran yang sesuai, Anda dapat mulai mengikuti langkah-langkah lainnya.

## Mendaftar untuk Akun AWS

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

Untuk mendaftar untuk Akun AWS

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

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

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

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

## Buat pengguna dengan akses administratif

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

Amankan Anda Pengguna root akun AWS

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

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

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

Buat pengguna dengan akses administratif

1. Aktifkan Pusat Identitas IAM.

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

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

Masuk sebagai pengguna dengan akses administratif

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

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

Tetapkan akses ke pengguna tambahan

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

   Untuk petunjuknya, lihat Membuat set izin di Panduan AWS IAM Identity Center Pengguna.

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

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

## Tambahkan AWS Ground Station izin 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.

# Satelit onboard

Memasukkan satelit ke dalam AWS Ground Station adalah proses multistep yang melibatkan pengumpulan data, validasi teknis, lisensi spektrum, dengan integrasi dan pengujian. Ada juga perjanjian non-pengungkapan (NDAs) yang diperlukan.

## Ikhtisar proses orientasi pelanggan

Orientasi satelit adalah proses manual yang dapat ditemukan di bagian Satelit dan Sumber Daya di halaman konsol. AWS Ground Station Berikut ini menjelaskan keseluruhan proses.

1. Tinjau AWS Ground Station Lokasi bagian untuk menentukan apakah satelit Anda memenuhi karakteristik frekuensi geografis dan radio.
2. Untuk memulai orientasi satelit Anda ke AWS Ground Station, silakan kirim email ke `<aws-groundstation@amazon.com>` dengan ringkasan singkat tentang misi dan kebutuhan satelit Anda, termasuk nama organisasi Anda, frekuensi yang diperlukan, kapan satelit akan diluncurkan atau diluncurkan, jenis orbit satelit, dan jika Anda berencana untuk menggunakannya. Gunakan fitur kembar AWS Ground Station digital
3. Setelah permintaan Anda ditinjau dan disetujui, AWS Ground Station akan mengajukan permohonan lisensi peraturan di lokasi tertentu yang Anda rencanakan untuk digunakan. Durasi langkah ini akan bervariasi tergantung pada lokasi dan peraturan yang ada.
4. Setelah persetujuan ini diperoleh, satelit Anda akan terlihat untuk Anda gunakan. AWS Ground Station akan mengirimi Anda pemberitahuan tentang pembaruan yang berhasil.

## (Opsional) Penamaan satelit

Setelah onboarding, Anda mungkin ingin menambahkan nama ke catatan satelit Anda agar lebih mudah mengenalinya. 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. SDKs 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 kredensil yang sering Anda gunakan dalam file yang dikelola oleh file. AWS CLI Anda memerlukan pengaturan dan kredensil ini untuk memesan dan mengelola AWS Ground Station kontak Anda. AWS CLI Untuk informasi selengkapnya tentang menyimpan konfigurasi dan setelan kredensialnya, lihat Pengaturan konfigurasi dan file kredensi.

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 diloloskan 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
```

## Satelit siaran publik

Selain orientasi satelit Anda sendiri, Anda dapat meminta untuk onboard dengan satelit siaran publik yang didukung yang menyediakan jalur komunikasi downlink yang dapat diakses publik. Ini memungkinkan Anda untuk menggunakan AWS Ground Station untuk downlink data dari satelit ini.

> **Note**
>
> Anda tidak akan dapat melakukan uplink ke satelit-satelit ini. Anda hanya akan dapat menggunakan jalur komunikasi downlink yang dapat diakses publik.

AWS Ground Station mendukung orientasi satelit berikut untuk menurunkan data siaran langsung:

- 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. Lihat Contoh konfigurasi profil misi contoh bagaimana AWS Ground Station bisa digunakan.

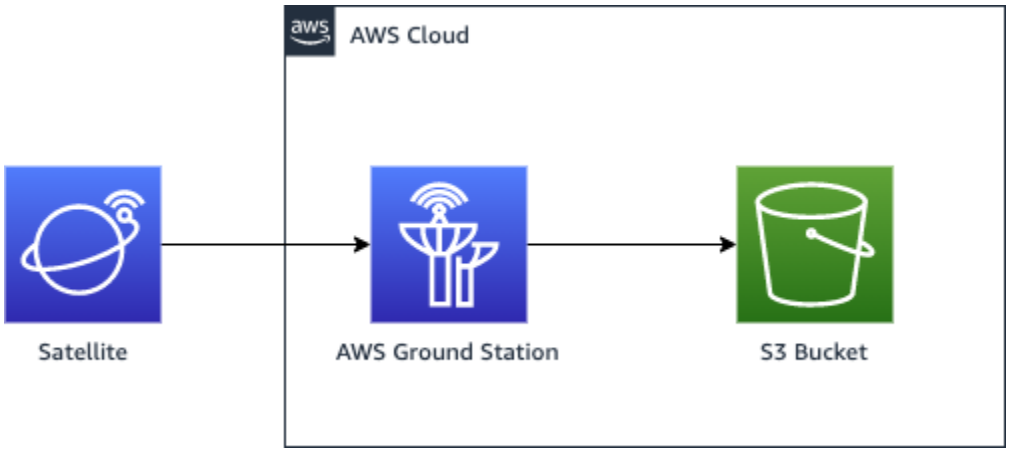
Untuk informasi lebih lanjut tentang satelit ini dan jenis data yang mereka kirimkan, lihat Aqua, JPSS-1/NOAA-20 dan SNPP, dan Terra.

# Rencanakan jalur komunikasi aliran data Anda

Anda memiliki pilihan antara komunikasi sinkron dan asinkron untuk setiap jalur komunikasi di satelit Anda. Tergantung pada satelit Anda dan kasus penggunaan Anda, Anda mungkin memerlukan satu atau kedua jenis. Jalur komunikasi sinkron memungkinkan uplink mendekati waktu nyata serta operasi downlink narrowband dan wideband. Jalur komunikasi asinkron hanya mendukung operasi downlink narrowband dan wideband.

## Pengiriman data asinkron

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 AI 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.




Untuk memanfaatkan jalur ini, Anda akan menggunakan kebutuhan untuk membuat bucket Amazon S3 AWS Ground Station untuk mengirimkan data ke dalamnya. Pada langkah berikutnya, Anda juga harus membuat S3 Recording Config di langkah berikutnya. Silakan referensi Config Perekaman

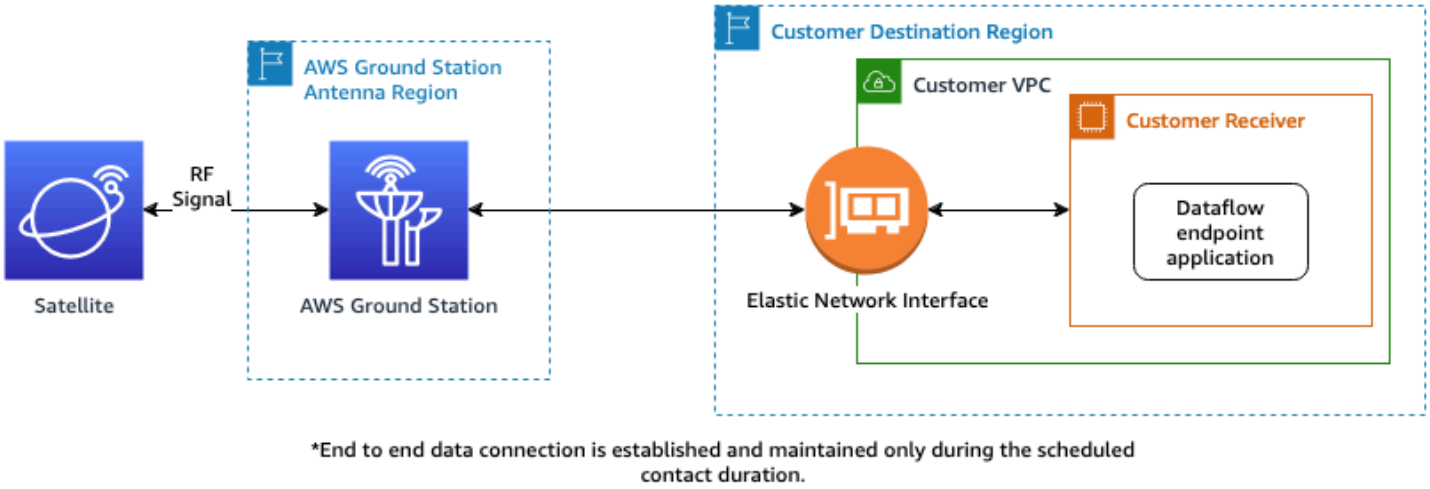
Amazon S3 untuk pembatasan penamaan bucket dan cara menentukan konvensi penamaan yang digunakan untuk file Anda.

## Pengiriman data sinkron

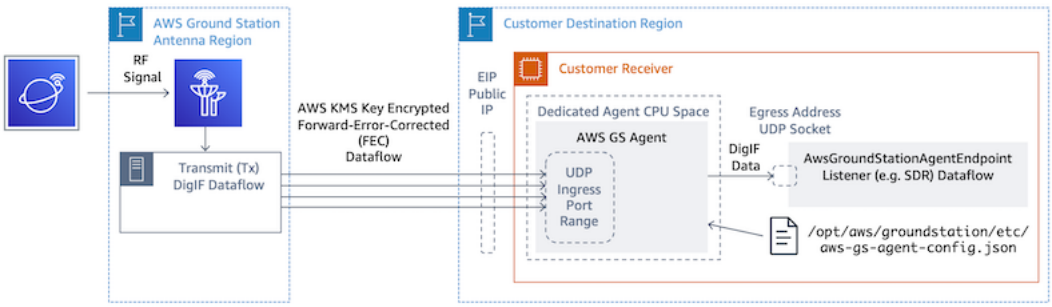
Dengan pengiriman data ke Amazon EC2, data kontak Anda dialirkan ke dan dari EC2 instans Amazon Anda. Anda dapat memproses data Anda secara real-time di EC2 instans Amazon Anda atau meneruskan data untuk pasca-pemrosesan.

Untuk memanfaatkan jalur sinkron, Anda akan menggunakan kebutuhan untuk mengatur dan mengonfigurasi EC2 instans Amazon Anda dan membuat satu atau beberapa Grup Titik Akhir Dataflow. Untuk mengonfigurasi referensi EC2 instans Amazon AndaSiapkan dan konfigurasikan Amazon EC2. Untuk membuat Dataflow Endpoint Group Anda, silakan referensi. Gunakan grup AWS Ground Station titik akhir Dataflow

Berikut ini menunjukkan jalur komunikasi jika Anda menggunakan konfigurasi titik akhir aliran data.




Berikut ini menunjukkan jalur komunikasi jika Anda menggunakan konfigurasi AWS Ground Station Agen.



# Buat konfigurasi

Dengan langkah ini Anda telah mengidentifikasi satelit, jalur komunikasi, dan sumber daya IAM, Amazon EC2, dan Amazon S3 sesuai kebutuhan. Pada langkah ini Anda akan membuat AWS Ground Station konfigurasi yang menyimpan parameter masing-masing.

## Konfigurasi pengiriman data

Konfigurasi pertama yang dibuat berhubungan dengan di mana dan bagaimana Anda ingin data dikirimkan. Menggunakan informasi dari langkah sebelumnya Anda akan membangun banyak jenis konfigurasi berikut.

- Config Perekaman Amazon S3- Kirimkan data ke bucket Amazon S3 Anda.
- Konfigurasi Titik Akhir Dataflow- Kirimkan data ke EC2 instans Amazon Anda.

## Konfigurasi satelit

Konfigurasi satelit menghubungkan bagaimana AWS Ground Station dapat berkomunikasi dengan satelit Anda. Anda akan mereferensikan informasi yang Anda kumpulkanSatelit onboard.

- Melacak Config- Menetapkan preferensi untuk bagaimana kendaraan Anda dilacak secara fisik selama kontak. Ini diperlukan untuk konstruksi profil misi.
- Konfigurasi Downlink Antena- Memberikan data frekuensi radio digital.
- Antena Downlink Demod Decode Config - Memberikan data frekuensi radio yang didemodulasi dan diterjemahkan.
- Konfigurasi Uplink Antena- Uplink data ke satelit Anda.
- Antena Uplink Echo Config- Kirimkan gema data sinyal uplink Anda.

# Buat profil misi

Dengan konfigurasi yang dibangun pada langkah sebelumnya, Anda telah mengidentifikasi cara melacak satelit Anda dan cara yang mungkin untuk berkomunikasi dengan satelit Anda. Pada langkah ini Anda akan membangun satu atau lebih profil misi. Profil misi mewakili agregasi konfigurasi yang mungkin ke dalam perilaku yang diharapkan yang kemudian dapat dijadwalkan dan dioperasikan.

Untuk parameter terbaru, silakan referensi jenis AWS::GroundStation::MissionProfile CloudFormation sumber daya

1. Beri nama profil misi Anda. Ini memungkinkan Anda untuk dengan cepat memahami penggunaannya dalam sistem Anda. Misalnya, Anda mungkin memiliki satellite-wideband-narrowband-nominal-operasi dan satellite-narrowband-emergency-operationsjika Anda memiliki pembawa pita sempit terpisah untuk operasi darurat.
2. Setel konfigurasi pelacakan Anda.
3. Tetapkan durasi kontak minimum Anda yang layak. Ini memungkinkan Anda untuk memfilter kontak potensial untuk memenuhi kebutuhan misi Anda.
4. Atur streamsKmsKeydan streamsKmsRoleyang digunakan untuk mengenkripsi data Anda selama transit. Ini digunakan untuk semua aliran data AWS Ground Station Agen.
5. Tetapkan aliran data Anda. Buat aliran data Anda agar sesuai dengan sinyal operator Anda menggunakan konfigurasi yang Anda buat di langkah sebelumnya.
6. [Opsional] Atur detik durasi kontak pra-pass dan pasca-pass Anda. Ini digunakan untuk memancarkan peristiwa per-kontak sebelum dan sesudah kontak, masing-masing. Untuk informasi selengkapnya, lihat Otomatisasi AWS Ground Station dengan Acara.
7. [Opsional] Anda dapat mengaitkan Tag ke profil misi Anda. Ini dapat digunakan untuk membantu membedakan profil misi Anda secara terprogram.

Anda dapat mereferensikanContoh konfigurasi profil misi, untuk melihat hanya beberapa konfigurasi potensial.

## Pahami langkah selanjutnya

Sekarang setelah Anda memiliki satelit onboard dan profil misi yang valid, Anda siap untuk menjadwalkan kontak dan berkomunikasi dengan satelit Anda. AWS Ground Station

Anda dapat menjadwalkan kontak dengan salah satu cara berikut:

- AWS Ground Station Konsol.
- Perintah AWS kontak cadangan CLI.
- AWS SDK. ReserveContact API.

Untuk informasi tentang bagaimana AWS Ground Station melacak lintasan satelit Anda dan bagaimana informasi itu digunakan, silakan referensi. Memahami bagaimana AWS Ground Station menggunakan data ephemeris satelit

AWS Ground Station memelihara sejumlah AWS CloudFormation template yang telah dikonfigurasi untuk membuat memulai dengan layanan lebih mudah. Lihat Contoh konfigurasi profil misi contoh bagaimana AWS Ground Station bisa digunakan.

Memproses data frekuensi menengah digital, atau data yang didemodulasi dan diterjemahkan yang diberikan kepada Anda dari AWS Ground Station akan tergantung pada kasus penggunaan spesifik Anda. Posting blog berikut dapat membantu Anda memahami beberapa opsi yang tersedia untuk Anda:

- Pengamatan Bumi otomatis menggunakan pengiriman data AWS Ground Station Amazon S3 (dan itu terkait GitHub repositori awslabs/) aws-groundstation-eos-pipeline
- Virtualisasi segmen darat satelit dengan AWS
- Pengamatan bumi menggunakan AWS Ground Station: Cara memandu
- Membangun arsitektur downlink data satelit throughput tinggi dengan AWS Ground Station WideBand DiGIF dan Amphinicy Blink SDR (dan repositori terkait aws-samples/) GitHub aws-groundstation-wbdigif-snpp

# AWS Ground Station Lokasi

AWS Ground Station menyediakan jaringan global stasiun bumi yang dekat dengan jaringan global wilayah infrastruktur AWS kami. Anda dapat mengonfigurasi penggunaan lokasi ini dari Wilayah AWS yang didukung. Ini termasuk Wilayah AWS tempat data dikirimkan.


## Menemukan AWS wilayah untuk lokasi stasiun bumi

Jaringan AWS Ground Station global mencakup lokasi stasiun bumi yang tidak secara fisik terletak di Wilayah AWS tempat mereka terhubung. Daftar stasiun bumi yang dapat Anda akses dapat diambil melalui respons AWS SDK ListGroundStation. Daftar lengkap lokasi stasiun bumi disajikan di bawah ini, dengan lebih banyak lagi segera hadir. Silakan merujuk ke panduan orientasi untuk menambah atau memodifikasi persetujuan situs untuk satelit Anda.

| Nama Ground Station | Lokasi Ground Station | Nama Wilayah AWS | Kode Wilayah AWS | Catatan |
|---|---|---|---|---|
| Alaska 1 | Alaska, Amerika Serikat | AS Barat (Oregon) | us-west-2 | Tidak secara fisik terletak di suatu AWS wilayah |
| Bahrain 1 | Bahrain | Timur Tengah (Bahrain) | me-south-1 | |
| Kota Tanjung 1 | Cape Town, Afrika Selatan | Afrika (Cape Town) | af-south-1 | |
| Dubbo 1 | Dubbo, Australia | Asia Pasifik (Sydney) | ap-southeast-2 | Tidak secara fisik terletak di suatu AWS wilayah |
| Hawaii 1 | Hawaii, Amerika Serikat | AS Barat (Oregon) | us-west-2 | Tidak secara fisik terletak di suatu AWS wilayah |
| Irlandia 1 | Ireland | Eropa (Irlandia) | eu-west-1 | |
| Ohio 1 | Ohio, Amerika Serikat | AS Timur (Ohio) | us-east-2 | |
| Oregon 1 | Oregon, Amerika Serikat | AS Barat (Oregon) | us-west-2 | |
| Punta Arena 1 | Punta Arenas, Cile | Amerika Selatan (Sao Paulo) | sa-east-1 | Tidak secara fisik terletak di suatu AWS wilayah |
| Seoul 1 | Seoul, Korea Selatan | Asia Pasifik (Seoul) | ap-northeast-2 | |

| Nama Ground Station | Lokasi Ground Station | Nama Wilayah AWS | Kode Wilayah AWS | Catatan |
|---|---|---|---|---|
| Singapura 1 | Singapura | Asia Pasifik (Singapura) | ap-southeast-1 | |
| Stockholm 1 | Stockholm, Swedia | Eropa (Stockholm) | eu-north-1 | |

## AWS Ground Station wilayah AWS yang didukung

Anda dapat mengirimkan data dan mengonfigurasi Kontak Anda melalui AWS SDK atau AWS Ground Station konsol dari Wilayah AWS yang didukung. Anda dapat melihat wilayah yang didukung dan titik akhir terkait di AWS Ground Station titik akhir dan kuota.

## Ketersediaan kembar digital

Gunakan fitur kembar AWS Ground Station digitaltersedia di semua Wilayah AWS AWS Ground Station jika tersedia. Stasiun ground kembar digital adalah salinan persis dari stasiun bumi produksi dengan awalan modifikasi ke Ground Station Nama “Digital Twin”. Misalnya, “Digital Twin Ohio 1" adalah stasiun darat kembar digital yang merupakan salinan persis dari stasiun bumi produksi “Ohio 1".

## AWS Ground Station topeng 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 tertentu, seperti sudut ketinggian 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 Anda berdasarkan perjanjian non-disclosure (NDA).

## Masker khusus pelanggan

Selain masker situs AWS Ground Station di setiap situs, Anda mungkin memiliki masker tambahan karena pembatasan otorisasi hukum Anda sendiri untuk berkomunikasi dengan satelit Anda 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 Anda tidak memesan waktu ketika satelit Anda 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. Ini memungkinkan Anda 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. Anda 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 Anda, bahkan jika sebagian dari waktu yang dipesan tidak tersedia untuk uplink.

# AWS Ground Station Kemampuan Situs

Untuk menyederhanakan pengalaman Anda, AWS Ground Station tentukan seperangkat kemampuan umum untuk jenis antena dan kemudian menyebarkan beberapa antena ke lokasi stasiun bumi. Bagian dari langkah orientasi memastikan satelit Anda kompatibel dengan jenis antena di lokasi tertentu. Ketika Anda memesan kontak, Anda secara tidak langsung menentukan jenis antena yang digunakan. Ini memastikan pengalaman Anda di lokasi stasiun bumi tertentu tetap sama dari waktu ke waktu terlepas dari antena mana yang digunakan. Kinerja spesifik kontak Anda akan bervariasi karena berbagai masalah lingkungan seperti cuaca di lokasi.

Saat ini, semua situs mendukung kemampuan berikut:

> **Note**
>
> Setiap baris dalam tabel berikut menunjukkan jalur komunikasi independen, kecuali dinyatakan lain. Baris duplikat ada untuk mencerminkan kemampuan multi-saluran kami yang memungkinkan beberapa jalur komunikasi digunakan secara bersamaan.

| Jenis Kemampuan | Rentang Frekuensi | Rentang Bandwidth | Polarisasi | Nama Umum | Catatan |
|---|---|---|---|---|---|
| antena-downlink | 7750 - 8500 MHz | 50 - 400 MHz | RHCP | Downlink pita lebar X-band | Kemampuan ini membutuhkan penggunaan AWS Ground Station Agen. |
| antena-downlink | 7750 - 8500 MHz | 50 - 400 MHz | RHCP | | |
| antena-downlink | 7750 - 8500 MHz | 50 - 400 MHz | RHCP | | |
| antena-downlink | 7750 - 8500 MHz | 50 - 400 MHz | RHCP | | Kemampuan ini tidak didukung di Alaska 1 atau |

| Jenis Kemampuan | Rentang Frekuensi | Rentang Bandwidth | Polarisasi | Nama Umum | Catatan |
|---|---|---|---|---|---|
| antena-downlink | 7750 - 8500 MHz | 50 - 400 MHz | RHCP | | Punta Arenas 1. |
| antena-downlink | 7750 - 8500 MHz | 50 - 400 MHz | LHCP | | Bandwidth agregat tidak boleh melebihi 400 MHz per polarisasi di setiap lokasi. |
| antena-downlink | 7750 - 8500 MHz | 50 - 400 MHz | LHCP | | |
| antena-downlink | 7750 - 8500 MHz | 50 - 400 MHz | LHCP | | |
| antena-downlink | 7750 - 8500 MHz | 50 - 400 MHz | LHCP | | Semua rentang frekuensi yang digunakan harus tidak tumpang tindih. |
| antena-downlink | 7750 - 8500 MHz | 50 - 400 MHz | LHCP | | |
| antena-downlink | 2200 - 2290 MHz | Hingga 40 MHz | RHCP | Downlink S-band | Hanya satu polarisasi yang dapat digunakan pada satu waktu |
| antena-downlink | 2200 - 2290 MHz | Hingga 40 MHz | LHCP | | |
| antena-downlink | 7750 - 8500 MHz | Hingga 40 MHz | RHCP | Downlink narrowband X-band | Hanya satu polarisasi yang dapat digunakan pada satu waktu |
| antena-downlink | 7750 - 8500 MHz | Hingga 40 MHz | LHCP | | |

| Jenis Kemampuan | Rentang Frekuensi | Rentang Bandwidth | Polarisasi | Nama Umum | Catatan |
|---|---|---|---|---|---|
| antena-uplink | 2025 - 2110 MHz | Hingga 40 MHz | RHCP | Tautan atas S-band | Hanya satu polarisasi yang dapat digunakan pada satu waktu<br><br>EIRP 20-50 dBW |
| antena-uplink | 2025 - 2110 MHz | Hingga 40 MHz | LHCP | | |
| antenna-uplink-echo | 2025 - 2110 MHz | 2 MHz | RHCP | Gema uplink | Cocokkan pembatasan antena-uplink |
| antenna-uplink-echo | 2025 - 2110 MHz | 2 MHz | LHCP | | |
| antenna-downlink-demod-decode | 7750 - 8500 MHz | Hingga 500 MHz | RHCP | Downlink X-band yang didemodulasi dan diterjemahkan | |
| antenna-downlink-demod-decode | 7750 - 8500 MHz | Hingga 500 MHz | LHCP | | |
| pelacakan | N/A | N/A | N/A | N/A | Support untuk pelacakan otomatis dan pelacakan program |

* RHCP = polarisasi melingkar tangan kanan, dan LHCP = polarisasi melingkar tangan kiri. Untuk informasi lebih lanjut tentang polarisasi, lihat Polarisasi melingkar.

# Memahami bagaimana AWS Ground Station menggunakan data ephemeris satelit

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 jika satelit Anda memiliki ID NORAD yang ditetapkan.

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 (TLEs) 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.

# Berikan data ephemeris khusus

> **Important**
>
> API ephemeris saat ini dalam status Pratinjau

Akses ke API Ephemeris disediakan hanya sesuai kebutuhan.
<Jika Anda memerlukan kemampuan untuk mengunggah data ephemeris khusus, Anda har
AWS Ground Station memperlakukan ephemerides sebagai Data Penggunaan Individual. Jika Anda menggunakan fitur opsional ini, AWS akan menggunakan data ephemeris Anda untuk memberikan dukungan pemecahan masalah.

## Gambaran Umum

API Ephemeris memungkinkan ephemerides khusus diunggah untuk digunakan dengan satelit. AWS Ground Station Ephemerides ini mengesampingkan ephemerides default dari Space-Track (lihat:). Data ephemeris standar Kami mendukung penerimaan data ephemeris dalam format Orbit Ephemeris Message (OEM), dan elemen dua baris (TLE).

Mengunggah ephemerides khusus dapat meningkatkan kualitas pelacakan, menangani operasi awal di mana tidak ada ephemerides Space-Track yang tersedia, dan memperhitungkan manuver. AWS Ground Station

> **Note**
>
> Saat memberikan ephemeris khusus sebelum nomor katalog satelit ditetapkan untuk satelit Anda, Anda dapat menggunakan 00000 untuk bidang nomor katalog satelit TLE, dan 000 untuk bagian nomor peluncuran bidang penunjuk internasional metadata TLE atau OEM (misalnya 24000A untuk kendaraan yang diluncurkan pada tahun 2024).
> Untuk informasi selengkapnya tentang format TLEs, lihat Kumpulan elemen dua baris. Untuk informasi lebih lanjut tentang format OEMs, lihatFormat ephemer OEM.

## Format ephemer OEM

AWS Ground Station memproses Ephemerides yang Disediakan Pelanggan OEM sesuai dengan standar CCSDS dengan beberapa batasan tambahan. File OEM harus dalam format KVN. Tabel

berikut menguraikan bidang yang berbeda dalam OEM dan bagaimana AWS Ground Station perbedaannya dari standar CCSDS.

| Bagian | Bidang | CCSDS diperlukan | AWS Ground Station diperlukan | Catatan |
|---|---|---|---|---|
| Header | CCSDS_OEM_VERS | Ya | Ya | Nilai yang dibutuhkan: 2.0 |
| | MENGOMENTARI | Tidak | Tidak | |
| | KLASIFIKASI | Tidak | Tidak | |
| | CREATION_DATE | Ya | Ya | |
| | PENCETUS | Ya | Ya | |
| | MESSAGE_ID | Tidak | Tidak | |
| Metadata | META_START | Ya | Ya | |
| | MENGOMENTARI | Tidak | Tidak | |
| | OBJECT_NAME | Ya | Ya | |
| | OBJECT_ID | Ya | Ya | |
| | CENTER_NAME | Ya | Ya | Nilai yang dibutuhkan: Bumi |
| | REF_FRAME | Ya | Ya | Nilai yang diterima: EME2 ITRF2 000.000 |

| Bagian | Bidang | CCSDS diperlukan | AWS Ground Station diperlukan | Catatan |
|---|---|---|---|---|
| | REF_FRAME_EPOCH | Tidak | Tidak didukung* | Tidak diperlukan karena REF_ yang diterima FRAMEs memiliki zaman implisit |
| | TIME_SISTEM | Ya | Ya | Nilai yang dibutuhkan: UTC |
| | START_TIME | Ya | Ya | |
| | DAPAT DIGUNAKAN_START_TIME | Tidak | Tidak | |
| | DAPAT DIGUNAKAN_STOP_TIME | Tidak | Tidak | |
| | BERHENTI_WAKTU | Ya | Ya | |
| | INTERPOLASI | Tidak | Ya | Diperlukan sehingga AWS Ground Station dapat menghasilkan sudut penunjuk yang akurat untuk kontak. |

| Bagian | Bidang | CCSDS diperlukan | AWS Ground Station diperlukan | Catatan |
|---|---|---|---|---|
| | INTERPOLASI_DERAJAT | Tidak | Ya | Diperlukan sehingga AWS Ground Station dapat menghasilkan sudut penunjuk yang akurat untuk kontak. |
| | META_STOP | Ya | Ya | |
| Data | X | Ya | Ya | Diwakili dalam `km` |
| | Y | Ya | Ya | Diwakili dalam `km` |
| | Z | Ya | Ya | Diwakili dalam `km` |
| | X_DOT | Ya | Ya | Diwakili dalam `km/s` |
| | Y_DOT | Ya | Ya | Diwakili dalam `km/s` |
| | Z_DOT | Ya | Ya | Diwakili dalam `km/s` |
| | X_DDOT | Tidak | Tidak | Diwakili dalam `km/s^2` |
| | Y_DDOT | Tidak | Tidak | Diwakili dalam `km/s^2` |

| Bagian | Bidang | CCSDS diperlukan | AWS Ground Station diperlukan | Catatan |
|---|---|---|---|---|
| | Z_DDOT | Tidak | Tidak | Diwakili dalam `km/s^2` |
| Matriks kovarians | COVARIANCE_START | Tidak | Tidak | |
| | EPOCH | Tidak | Tidak | |
| | COV_REF_FRAME | Tidak | Tidak | |
| | KOVARIANCE_STOP | Tidak | Tidak | |

* Jika ada baris yang tidak didukung oleh AWS Ground Station termasuk dalam OEM yang disediakan, OEM akan gagal validasi.

Penyimpangan penting dari standar CCSDS adalah: AWS Ground Station

- CCSDS_OEM_VERS harus. `2.0`
- REF_FRAME diperlukan untuk menjadi salah satu atau`EME2000`. `ITRF2000`
- REF_FRAME_EPOCH tidak didukung oleh. AWS Ground Station
- CENTER_NAME harus. `Earth`
- TIME_SYSTEM harus. `UTC`
- INTERPOLASI dan INTERPOLATION_DEGREE keduanya diperlukan untuk CPE. AWS Ground Station

## Contoh OEM ephemeris dalam format KVN

Berikut ini adalah contoh terpotong dari ephemeris OEM dalam format KVN untuk satelit penyiar publik JPSS-1.

```
CCSDS_OEM_VERS = 2.0

COMMENT Orbit data are consistent with planetary ephemeris DE-430

CREATION_DATE  = 2024-07-22T05:20:59
ORIGINATOR     = Raytheon-JPSS/CGS

META_START
OBJECT_NAME          = J1
OBJECT_ID            = 2017-073A
CENTER_NAME          = Earth
REF_FRAME            = EME2000
TIME_SYSTEM          = UTC
START_TIME           = 2024-07-22T00:00:00.000000
STOP_TIME            = 2024-07-22T00:06:00.000000
INTERPOLATION        = Lagrange
INTERPOLATION_DEGREE = 5
META_STOP

2024-07-22T00:00:00.000000   5.905147360000000e+02  -1.860082793999999e+03
  -6.944807075000000e+03  -5.784245796000000e+00   4.347501391999999e+00
 -1.657256863000000e+00
2024-07-22T00:01:00.000000   2.425572045154201e+02  -1.595860765983339e+03
  -7.030938457373539e+03  -5.810660250794190e+00   4.457103652219009e+00
 -1.212889340333023e+00
2024-07-22T00:02:00.000000  -1.063224256538050e+02  -1.325569732497146e+03
  -7.090262617183503e+03  -5.814973972202444e+00   4.549739160042560e+00
 -7.639633689161465e-01
2024-07-22T00:03:00.000000  -4.547973959231161e+02  -1.050238305712201e+03
  -7.122556683227951e+03  -5.797176562437553e+00   4.625064829516728e+00
 -3.121687831090774e-01
2024-07-22T00:04:00.000000  -8.015427368657785e+02  -7.709137891269565e+02
  -7.127699477194810e+03  -5.757338007808417e+00   4.682800822515077e+00
 1.407953645161997e-01
2024-07-22T00:05:00.000000  -1.145240083085062e+03  -4.886583601179489e+02
  -7.105671911254255e+03  -5.695608435738609e+00   4.722731329786999e+00
 5.932259682105052e-01
2024-07-22T00:06:00.000000  -1.484582479061495e+03  -2.045451985605701e+02
  -7.056557069672793e+03  -5.612218005854990e+00   4.744705579872771e+00
 1.043421397392599e+00
```

## Membuat ephemeris khusus

Ephemeris khusus dapat dibuat menggunakan CreateEphemeristindakan 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 DescribeEphemerisuntuk status ephemeris atau menggunakan CloudWatch peristiwa untuk melacak perubahan status ephemeris.

Untuk memecahkan masalah ephemeris yang tidak valid, lihat: Memecahkan masalah ephemerides yang tidak valid

## Contoh: Buat elemen dua baris (TLE) set ephemeris melalui API

The AWS SDKs, dan CLI 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). Contoh ini menunjukkan bagaimana melakukan ini menggunakan AWS SDK for Python (Boto3).

Set TLE adalah objek berformat JSON yang merangkai satu atau lebih TLEs bersama-sama untuk membangun lintasan kontinu. TLEs Dalam set TLE harus membentuk himpunan kontinu yang dapat kita gunakan untuk membangun lintasan (yaitu tidak ada celah waktu antara TLEs 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 TLEs 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 ephemerisid yang dapat digunakan untuk mereferensikan ephemeris di masa depan. Misalnya, kita dapat menggunakan ephemerisid yang disediakan dari panggilan di atas untuk melakukan polling untuk status ephemeris:

```
client.describe_ephemeris(ephemerisId=tle_ephemeris_id['ephemerisId'])
```

Contoh respons dari DescribeEphemeristindakan 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 DescribeEphemerisrute atau menggunakan CloudWatch peristiwa untuk melacak status ephemeris yang diunggah karena harus melalui alur kerja validasi asinkron sebelum disetel ke dan menjadi dapat digunakan untuk ENABLED menjadwalkan dan mengeksekusi kontak.

Perhatikan bahwa ID NORAD di semua set TLE, TLEs dalam contoh 25994 di atas, harus cocok dengan ID NORAD yang telah ditetapkan satelit Anda dalam database Space-Track.

## Contoh: 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 = ground_station_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 DescribeEphemeristindakan 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"
      }
    }
  }
}
```

## Contoh: Menggunakan ephemerides yang disediakan pelanggan dengan AWS Ground Station

Untuk petunjuk lebih rinci tentang penggunaan ephemerides yang disediakan pelanggan AWS Ground Station, lihat Menggunakan ephemerides yang disediakan pelanggan dengan (dan itu terkait repositori aws-samples/) AWS Ground Station GitHub aws-groundstation-cpe

# Memahami 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. Nilai prioritas yang lebih besar menunjukkan prioritas yang lebih tinggi. 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: Ground Station FAQs.

## Dapatkan ephemeris saat ini untuk satelit

Ephemeris saat ini digunakan oleh AWS Ground Station untuk satelit tertentu dapat diambil dengan memanggil atau tindakan. GetSatelliteListSatellites 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, 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"
      }
  }
```

## Kembalikan 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 GetSatellitedan memverifikasi bahwa ephemeris saat ini untuk satelit adalah. `source` SPACE_TRACK Lihat Data ephemeris standar untuk informasi lebih lanjut tentang ephemerides default.

# Bekerja dengan aliran data

AWS Ground Station menggunakan hubungan simpul dan tepi untuk membangun aliran data untuk memungkinkan pemrosesan aliran data Anda. Setiap node diwakili oleh konfigurasi yang menjelaskan pemrosesan yang diharapkan. Untuk mengilustrasikan konsep ini, pertimbangkan aliran data ke a. `antenna-downlink` `s3-recording` `antenna-downlink`Node mewakili transformasi analog ke digital dari spektrum frekuensi radio per parameter yang ditentukan pada konfigurasi. `s3-recording`Ini mewakili node komputasi yang akan menerima data masuk dan menyimpannya di bucket S3 Anda. Aliran data yang dihasilkan adalah pengiriman data asinkron dari data RF digital ke bucket S3 berdasarkan spesifikasi Anda.

Dalam profil misi Anda, Anda dapat membuat banyak aliran data untuk memenuhi kebutuhan Anda. Bagian berikut menjelaskan cara menyiapkan sumber daya AWS Anda yang lain untuk digunakan AWS Ground Station dan menawarkan rekomendasi untuk membuat aliran data. Untuk informasi rinci tentang bagaimana setiap node berperilaku, termasuk jika dianggap sebagai sumber atau node tujuan, silakan lihatGunakan AWS Ground Station Konfigurasi.

Topik



## AWS Ground Station antarmuka bidang data

Struktur data yang dihasilkan dari aliran data yang Anda pilih tergantung pada sumber aliran data. Rincian format ini diberikan kepada Anda selama orientasi satelit Anda. Berikut ini merangkum format yang digunakan untuk setiap jenis aliran data.

- antena-downlink
  - (Bandwidth kurang dari 54MHz) data dikirimkan sebagai paket VITA-49 Signal Data/IP Format.
  - (Bandwidth greater-than-or-equal -to 54MHz) data dikirimkan sebagai paket AWS Ground Station Kelas 2.

- antenna-downlink-demod-decode
  - Data dikirim sebagai paket Demodulated/Decoded Data/IP Format.
- antena-uplink
  - Data harus dikirimkan sebagai paket VITA-49 Signal Data/IP Format.
- antenna-uplink-echo
  - Data dikirimkan sebagai paket VITA-49 Signal Data/IP Format.

## Gunakan pengiriman data lintas wilayah

Fitur pengiriman data AWS Ground Station lintas wilayah memberi Anda fleksibilitas untuk mengirim data Anda dari antena ke Wilayah AWS yang AWS Ground Station didukung. Ini berarti Anda dapat memelihara infrastruktur Anda di satu Wilayah AWS dan menjadwalkan kontak pada siapa pun yang AWS Ground Station AWS Ground Station Lokasi Anda ikuti.

Pengiriman data lintas wilayah saat ini tersedia di semua wilayah yang AWS Ground Station didukung saat menerima data kontak Anda di Bucket Amazon S3. AWS Ground Station akan mengelola semua aspek pengiriman untuk Anda.

Pengiriman data lintas wilayah ke Amazon EC2 dengan AWS Ground Station Agen tersedia di semua antenna-to-destination wilayah. Tidak diperlukan konfigurasi atau persetujuan unik untuk pengaturan ini.

Pengiriman data lintas wilayah ke Amazon EC2 menggunakan titik akhir aliran data tersedia secara default* di wilayah yang dijelaskan di bawah ini. antenna-to-destination

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

Untuk menggunakan pengiriman data lintas wilayah ke EC2 instans Amazon, titik akhir data harus dibuat di Wilayah AWS Anda saat ini dan Anda dataflow-endpoint-configharus menentukan wilayah yang sama.

Informasi sebelumnya yang merinci wilayah yang didukung, dan metode pengiriman, untuk pengiriman data lintas wilayah dirangkum dalam tabel berikut.

| Metode Menerima | Wilayah Antena | Wilayah Penerima |
| --- | --- | --- |
| Pengiriman data Amazon S3 | Semua onboard AWS Ground Station AWS Ground Station Lokasi | Semua AWS Ground Station wilayah |
| AWS Ground Station Agen di Amazon EC2 | Semua onboard AWS Ground Station AWS Ground Station Lokasi | Semua AWS Ground Station wilayah |
| Titik akhir aliran data di Amazon* EC2 | Wilayah AS Timur (Ohio) (us-east-2) | Wilayah AS Barat (Oregon) (us-west-2) |
| | Wilayah AS Barat (Oregon) (us-west-2) | Wilayah AS Timur (Ohio) (us-east-2) |

* antenna-to-destination Wilayah tambahan yang tidak terdaftar memerlukan Amazon khusus EC2 dan pengaturan perangkat lunak. Silahkan hubungi kami di `<aws-groundstation@amazon.com>` untuk petunjuk orientasi.

## Siapkan dan konfigurasikan Amazon S3

Anda dapat menggunakan bucket Amazon S3 untuk menerima sinyal downlink Anda menggunakan. AWS Ground Station Untuk membuat konfigurasi s3-recording-tujuan, Anda harus dapat menentukan bucket Amazon S3 dan peran IAM yang mengizinkan untuk menulis file ke bucket. AWS Ground Station

Lihat Config Perekaman Amazon S3 batasan pada bucket Amazon S3, peran IAM, atau AWS Ground Station pembuatan konfigurasi.

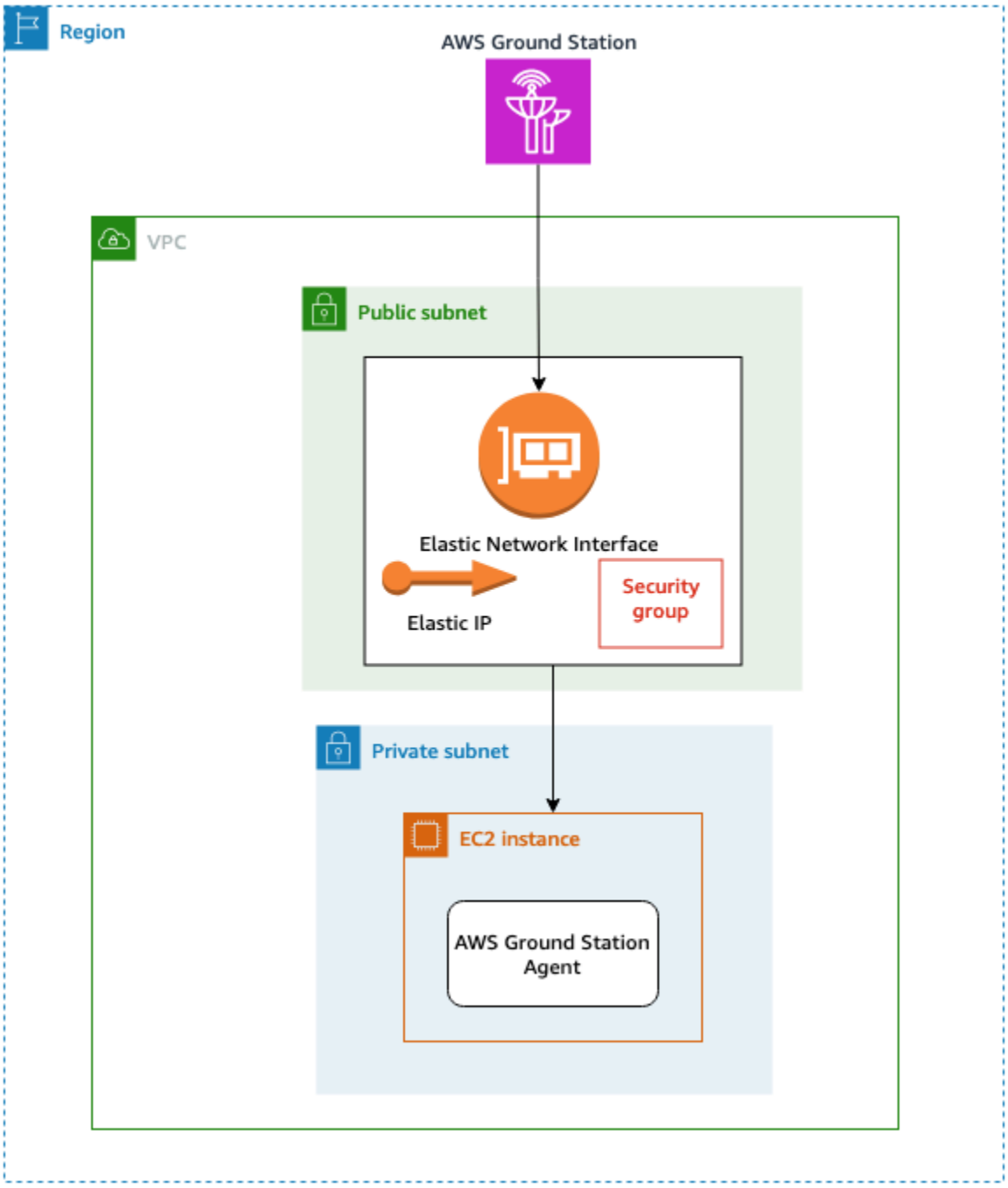
## Siapkan dan konfigurasikan Amazon VPC

Panduan lengkap untuk menyiapkan VPC berada di luar cakupan panduan ini. Untuk pemahaman mendalam, silakan merujuk ke Panduan Pengguna Amazon VPC.

Di bagian ini, dijelaskan bagaimana Amazon EC2 dan titik akhir aliran data Anda mungkin ada dalam VPC. AWS Ground Station tidak mendukung beberapa titik pengiriman untuk aliran data tertentu - diharapkan setiap aliran data berakhir ke satu penerima. EC2 Seperti yang kami harapkan satu EC2

penerima, konfigurasinya tidak berlebihan Multi-AZ. Untuk contoh lengkap yang akan menggunakan VPC Anda, silakan lihat. Contoh konfigurasi profil misi

## Konfigurasi VPC dengan Agen AWS Ground Station




Data satelit Anda diberikan ke instance AWS Ground Station Agen yang dekat dengan antena. AWS Ground Station Agen akan melakukan stripe dan kemudian mengenkripsi data Anda menggunakan AWS KMS kunci yang Anda berikan. Setiap strip dikirim ke Amazon EC2 Elastic IP (EIP) Anda dari

antena sumber di seluruh tulang punggung AWS Network. Data tiba di EC2 instans Anda melalui Amazon EC2 Elastic Network Interface (ENI) yang terpasang. Setelah di EC2 instans Anda, AWS Ground Station Agen yang diinstal akan mendekripsi data Anda dan melakukan koreksi kesalahan ke depan (FEC) untuk memulihkan data yang dijatuhkan, lalu meneruskannya ke IP dan port yang Anda tentukan dalam pengaturan Anda.

Daftar di bawah ini menyebutkan pertimbangan pengaturan unik saat menyiapkan VPC Anda AWS Ground Station untuk pengiriman Agen.

Grup Keamanan - Disarankan Anda membuat grup keamanan yang didedikasikan hanya untuk AWS Ground Station lalu lintas. Grup keamanan ini harus mengizinkan lalu lintas masuknya UDP pada rentang port yang sama yang Anda tentukan di Grup Titik Akhir Dataflow Anda. AWS Ground Station mempertahankan daftar awalan yang dikelola AWS untuk membatasi izin Anda hanya ke alamat IP. AWS Ground Station Lihat Daftar Awalan Terkelola AWS untuk detail tentang cara mengganti PrefixListIdwilayah penerapan Anda.

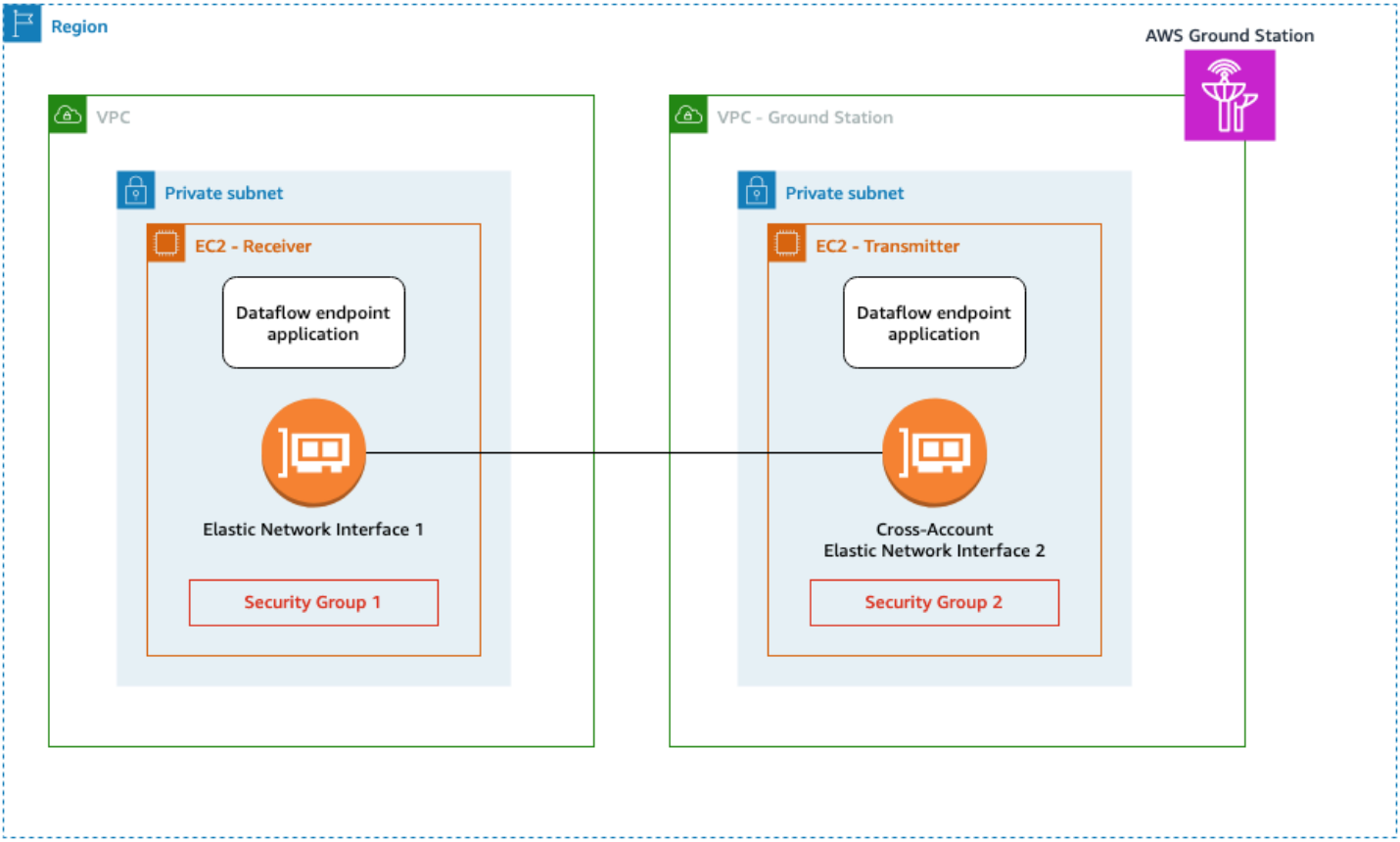
Elastic Network Interface (ENI) - Anda harus mengaitkan grup keamanan di atas dengan ENI ini dan menempatkannya di subnet publik Anda.

CloudFormation Template berikut menunjukkan cara membuat infrastruktur yang dijelaskan di bagian ini.

```
ReceiveInstanceEIP:
  Type: AWS::EC2::EIP
  Properties:
    Domain: 'vpc'

InstanceSecurityGroup:
  Type: AWS::EC2::SecurityGroup
  Properties:
    GroupDescription: AWS Ground Station receiver instance security group.
    VpcId:YourVpcId
    SecurityGroupIngress:
      # Add additional items here.
      - IpProtocol: udp
        FromPort: your-port-start-range
        ToPort: your-port-end-range
        PrefixListIds:
          - PrefixListId: com.amazonaws.global.groundstation
        Description: "Allow AWS Ground Station Downlink ingress."

InstanceNetworkInterface:
```

```
  Type: AWS::EC2::NetworkInterface
  Properties:
    Description: ENI for AWS Ground Station to connect to.
    GroupSet:
      - !Ref InstanceSecurityGroup
    SubnetId: A Public Subnet

ReceiveInstanceEIPAllocation:
  Type: AWS::EC2::EIPAssociation
  Properties:
    AllocationId:
      Fn::GetAtt: [ ReceiveInstanceEIP, AllocationId ]
    NetworkInterfaceId:
      Ref: InstanceNetworkInterface
```

## Konfigurasi VPC dengan titik akhir aliran data




Data satelit Anda disediakan ke instance aplikasi titik akhir aliran data yang dekat dengan antena. Data tersebut kemudian dikirim melalui lintas akun Amazon EC2 Elastic Network Interface (ENI) dari

VPC yang dimiliki oleh. AWS Ground Station Data kemudian tiba di EC2 instans Anda melalui ENI yang dilampirkan ke EC2 instans Amazon Anda. Aplikasi endpoint dataflow yang diinstal kemudian akan meneruskannya ke IP dan port yang Anda tentukan dalam pengaturan Anda. Kebalikan dari aliran ini terjadi untuk koneksi uplink.

Daftar di bawah ini menyebutkan pertimbangan penyiapan unik saat menyiapkan VPC Anda untuk pengiriman titik akhir aliran data.

Peran IAM - Peran IAM adalah bagian dari Dataflow Endpoint dan tidak ditampilkan dalam diagram. Peran IAM yang digunakan untuk membuat dan melampirkan ENI lintas akun ke instans AWS Ground Station Amazon EC2.

Grup Keamanan 1 - Grup keamanan ini dilampirkan ke ENI yang akan dikaitkan dengan EC2 instans Amazon di akun Anda. Ini perlu memungkinkan lalu lintas UDP dari Grup Keamanan 2 pada port yang ditentukan dalam Anda dataflow-endpoint-group.

Elastic Network Interface (ENI) 1 - Anda harus mengaitkan Security Group 1 dengan ENI ini dan menempatkannya di subnet.

Subnet - Anda harus memastikan bahwa setidaknya ada satu alamat IP yang tersedia per aliran data untuk EC2 instans Amazon di akun Anda. Untuk detail lebih lanjut tentang ukuran subnet lihat, blok CIDR Subnet

Grup Keamanan 2 - Grup keamanan ini direferensikan di Dataflow Endpoint. Grup keamanan ini akan dilampirkan ke ENI yang AWS Ground Station akan digunakan untuk menempatkan data ke akun Anda.

Wilayah - Untuk informasi selengkapnya tentang wilayah yang didukung untuk koneksi lintas wilayah, lihatGunakan pengiriman data lintas wilayah.

CloudFormation Template berikut menunjukkan cara membuat infrastruktur yang dijelaskan di bagian ini.

```
DataflowEndpointSecurityGroup:
  Type: AWS::EC2::SecurityGroup
  Properties:
    GroupDescription: Security Group for AWS Ground Station registration of Dataflow
 Endpoint Groups
    VpcId: YourVpcId

AWSGroundStationSecurityGroupEgress:
  Type: AWS::EC2::SecurityGroupEgress
```

```
  Properties:
    GroupId: !Ref DataflowEndpointSecurityGroup
    IpProtocol: udp
    FromPort: 55555
    ToPort: 55555
    CidrIp: 10.0.0.0/8
    Description: "Allow AWS Ground Station to send UDP traffic on port 55555 to the
 10/8 range."

InstanceSecurityGroup:
  Type: AWS::EC2::SecurityGroup
  Properties:
    GroupDescription: AWS Ground Station receiver instance security group.
    VpcId: YourVpcId
    SecurityGroupIngress:
      - IpProtocol: udp
        FromPort: 55555
        ToPort: 55555
        SourceSecurityGroupId: !Ref DataflowEndpointSecurityGroup
        Description: "Allow AWS Ground Station Ingress from
 DataflowEndpointSecurityGroup"

ReceiverSubnet:
  Type: AWS::EC2::Subnet
  Properties:
    # Ensure your CidrBlock will always have at least one available IP address per
 dataflow endpoint.
    # See https://docs.aws.amazon.com/vpc/latest/userguide/subnet-sizing.html for
 subent sizing guidelines.
    CidrBlock: "10.0.0.0/24"
    Tags:
      - Key: "Name"
        Value: "AWS Ground Station - Dataflow endpoint Example Subnet"
      - Key: "Description"
        Value: "Subnet for EC2 instance receiving AWS Ground Station data"
    VpcId: !Ref ReceiverVPC
```

# Siapkan dan konfigurasikan Amazon EC2

Konfigurasi EC2 instans Amazon Anda dengan benar diperlukan agar pengiriman VITA-49 Signal/IP data or VITA-49 Extension data/IP secara sinkron dikirimkan melalui AWS Ground Station Agen atau

titik akhir aliran data. Tergantung pada kebutuhan spesifik Anda, Anda dapat menggunakan prosesor Front End (FE) atau Software Defined Radio (SDR) secara langsung pada instance yang sama, atau Anda mungkin perlu menggunakan instance tambahan EC2. Pemilihan dan pemasangan FE atau SDR Anda berada di luar cakupan panduan pengguna ini. Untuk informasi selengkapnya tentang format data tertentu, lihatAWS Ground Station antarmuka bidang data.

Untuk informasi tentang persyaratan layanan kami, silakan lihat Ketentuan AWS Layanan.

## Perangkat Lunak Umum yang Disediakan

AWS Ground Station menyediakan perangkat lunak umum untuk memudahkan penyiapan EC2 instans Amazon Anda.

### 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.
- Tingkat tinggi, pengiriman data DigiF jitter rendah ke IP publik (IP AWS Elastis) di jaringan. AWS
- Pengiriman data yang andal menggunakan Forward Error Correction (FEC).
- Mengamankan pengiriman data menggunakan AWS KMS kunci terkelola pelanggan untuk enkripsi.

Untuk informasi selengkapnya, lihat Panduan Pengguna AWS Ground Station Agen.

### Aplikasi titik akhir Dataflow

Aplikasi jaringan yang digunakan oleh AWS Ground Station untuk mengirim dan menerima data antara lokasi AWS Ground Station antena, dan EC2 instans Amazon Anda. Ini dapat digunakan untuk uplink dan downlink data.

### Radio yang Ditetapkan Perangkat Lunak (SDR)

Software defined radio (SDR) yang dapat digunakan untuk memodulasi/mendemodulasi sinyal yang digunakan untuk berkomunikasi dengan satelit Anda.

# AWS Ground Station Gambar Mesin Amazon (AMIs)

Untuk mengurangi waktu pembuatan dan konfigurasi penginstalan ini, AWS Ground Station juga menawarkan yang telah dikonfigurasi sebelumnya AMIs. Aplikasi jaringan endpoint AMIs dengan aliran data dan radio yang ditentukan perangkat lunak (SDR) tersedia untuk akun Anda setelah orientasi Anda selesai. Mereka dapat ditemukan di EC2 konsol Amazon dengan mencari groundstation di Amazon Machine Images pribadi (AMIs). AWS Ground Station Agen AMIs with bersifat publik dan dapat ditemukan di EC2 konsol Amazon dengan mencari groundstation di Amazon Machine Images publik (AMIs).

# Bekerja dengan kontak

Anda dapat memasukkan data satelit, mengidentifikasi lokasi antena, berkomunikasi, dan menjadwalkan waktu antena untuk satelit yang dipilih dengan menggunakan AWS Ground Station konsol AWS CLI, atau AWS SDK dalam bahasa pilihan Anda. Anda dapat meninjau, membatalkan, dan menjadwal ulang reservasi kontak hingga 15 menit sebelum kontak mulai*. 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, lihatGunakan pengiriman data lintas wilayah.

Untuk menjadwalkan kontak, sumber daya Anda harus dikonfigurasi. Jika Anda belum mengonfigurasi sumber daya Anda, lihatMemulai . Ketika ReserveContactdipanggil, AWS Ground Station mengambil snapshot dari profil misi dan sumber daya konfigurasi untuk digunakan selama pass kontak. Perubahan pada sumber daya ini menggunakan UpdateMissionProfiledan tidak UpdateConfig APIs akan tercermin dalam kontak yang dicadangkan sebelum pembaruan. Jika Anda memerlukan perubahan sumber daya yang diterapkan ke kontak yang sudah dijadwalkan, Anda harus terlebih dahulu membatalkan kontak menggunakan CancelContact, dan kemudian menjadwal ulang menggunakan ReserveContact.

* Kontak yang dibatalkan dapat dikenakan biaya ketika dibatalkan terlalu dekat dengan waktu kontak. Untuk informasi selengkapnya tentang kontak yang dibatalkan, lihat: Ground Station FAQs.

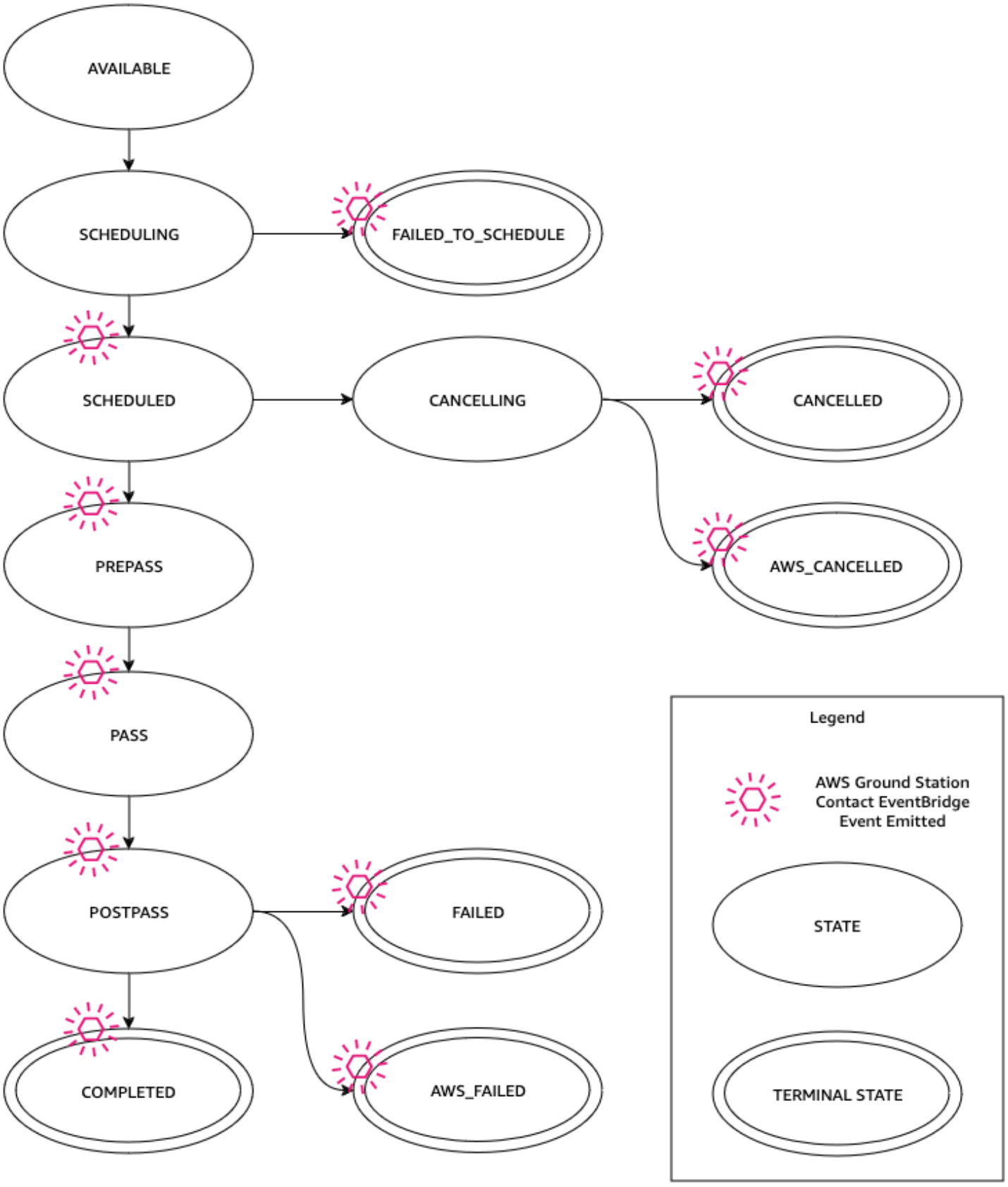
Topik



## Memahami siklus hidup kontak

Memahami siklus hidup kontak dapat membantu menentukan cara mengonfigurasi otomatisasi Anda dan selama upaya pemecahan masalah. Diagram berikut menunjukkan siklus hidup AWS Ground Station kontak serta Event Bridge Event yang dipancarkan selama siklus hidup. Penting untuk dicatat bahwa status terminal COMPLETED, FAILED, FAILED_TO_SCHEDULE, CANCELLED,, dan merupakan terminal. AWS_CANCELLED AWS_FAILED Kontak tidak akan bertransisi keluar dari

status terminal. Lihat detail AWS Ground Station status kontak tentang apa yang ditunjukkan oleh setiap status.


AVAILABLE
SCHEDULING
FAILED_TO_SCHEDULE
SCHEDULED
CANCELLING
CANCELLED
PREPASS
AWS_CANCELLED
PASS
POSTPASS
FAILED
COMPLETED
AWS_FAILED
Legend
AWS Ground Station Contact EventBridge Event Emitted
STATE
TERMINAL STATE

# AWS Ground Station status kontak

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 selesai tanpa kesalahan.
- GAGAL - Kontak gagal karena masalah dengan konfigurasi sumber daya Anda.
- AWS_FAILED- Kontak gagal karena masalah dalam AWS Ground Station layanan.
- PEMBATALAN - Kontak sedang dalam proses dibatalkan.
- AWS_CANCELLED- Kontak dibatalkan oleh AWS Ground Station layanan. Antena atau pemeliharaan situs, dan penyimpangan ephemeris adalah contoh kapan ini bisa terjadi.
- DIBATALKAN - Kontak dibatalkan oleh Anda.

# Gunakan fitur kembar AWS Ground Station digital

Fitur kembar digital untuk AWS Ground Station memberi Anda lingkungan di mana Anda dapat menguji dan mengintegrasikan manajemen misi satelit dan perangkat lunak perintah dan kontrol Anda. Fitur kembar digital memungkinkan Anda untuk menguji penjadwalan, verifikasi konfigurasi, dan penanganan kesalahan yang tepat tanpa menggunakan kapasitas antena produksi. Menguji AWS Ground Station integrasi Anda dengan fitur kembar digital memungkinkan Anda meningkatkan kepercayaan pada kemampuan sistem Anda untuk mengelola operasi satelit Anda dengan lancar. Ini juga memungkinkan Anda untuk menguji AWS Ground Station APIs tanpa menggunakan kapasitas produksi atau memerlukan lisensi spektrum.

Untuk memulai, ikutiSatelit onboard, meminta untuk masuk ke fitur kembar digital. Setelah satelit Anda terhubung ke fitur kembar digital, Anda dapat menjadwalkan kontak dengan stasiun darat kembar digital. Daftar stasiun bumi yang dapat Anda akses dapat diambil melalui respons AWS SDK ListGroundStations. Stasiun ground kembar digital adalah salinan persis dari stasiun bumi yang terdaftar AWS Ground Station Lokasi dengan awalan modifikasi ke Ground Station Nama “Digital Twin”. Ini termasuk kemampuan antena dan metadata mereka, termasuk, namun tidak terbatas pada, masker situs dan koordinat GPS yang sebenarnya. Saat ini, fitur kembar digital tidak mendukung pengiriman data seperti yang dijelaskan dalamBekerja dengan aliran data.

Setelah onboard, fitur kembar digital memancarkan EventBridge peristiwa Amazon dan respons API yang sama seperti layanan produksi seperti yang dijelaskan dalam. Otomatisasi AWS Ground Station dengan Acara Peristiwa ini akan memungkinkan Anda untuk menyempurnakan konfigurasi dan grup titik akhir aliran data Anda.

# Memahami pemantauan dengan 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 EventBridge Events memberikan 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 mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan 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 pemberitahuan untuk acara melalui beberapa saluran, termasuk email, Pengembang Amazon Q dalam pemberitahuan obrolan aplikasi obrolan, atau pemberitahuan AWS Console Mobile Applicationpush. Anda juga dapat melihat notifikasi di pusat Pemberitahuan AWS Konsol. Notifikasi Pengguna mendukung agregasi, yang dapat mengurangi jumlah notifikasi yang Anda terima selama acara tertentu.

Gunakan topik berikut untuk memantau AWS Ground Station.

Topik

- Otomatisasi AWS Ground Station dengan Acara
- Log panggilan AWS Ground Station API dengan AWS CloudTrail
- Lihat metrik dengan Amazon CloudWatch

# Otomatisasi AWS Ground Station dengan Acara

> **Note**
>
> Dokumen ini menggunakan istilah “acara” di seluruh. CloudWatch Acara 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 mengotomatiskan AWS layanan 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. Beberapa tindakan yang dapat dipicu secara otomatis termasuk yang berikut:

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

Beberapa contoh penggunaan acara dengan AWS Ground Station meliputi:

- Memanggil fungsi Lambda untuk mengotomatiskan awal dan penghentian instans EC2 Amazon 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 EventBridge Acara Amazon.

# AWS Ground Station Jenis Acara

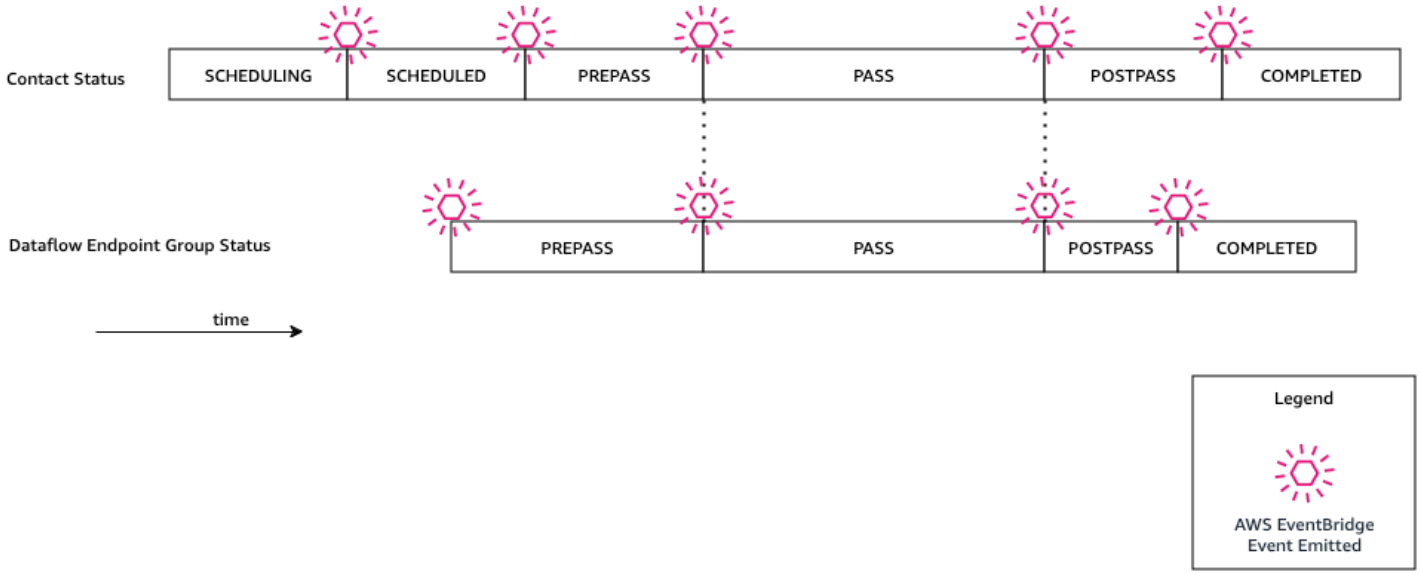
> **Note**
>
> Semua peristiwa yang dihasilkan oleh AWS Ground Station memiliki “aws.groundstation” sebagai nilai untuk “sumber”.

AWS Ground Station memancarkan peristiwa yang terkait dengan perubahan status untuk mendukung kemampuan Anda menyesuaikan otomatisasi Anda. Saat ini, AWS Ground Station mendukung peristiwa perubahan status kontak, peristiwa perubahan grup titik akhir aliran data, dan peristiwa perubahan status ephemeris. Bagian berikut memberikan informasi rinci tentang setiap jenis.

## Hubungi Timeline Acara

AWS Ground Station memancarkan peristiwa saat kontak Anda mengubah status. Untuk informasi lebih lanjut tentang apa perubahan keadaan itu, dan apa arti negara itu sendiri, lihatMemahami siklus hidup kontak. Setiap grup titik akhir aliran data yang digunakan dalam kontak Anda memiliki serangkaian peristiwa independen yang juga dipancarkan. Selama jangka waktu yang sama, kami juga memancarkan peristiwa untuk grup titik akhir aliran data Anda. Waktu yang tepat dari peristiwa pre-pass dan post-pass dapat dikonfigurasi oleh Anda saat Anda mengatur profil misi dan grup titik akhir aliran data Anda.

Diagram berikut menunjukkan status dan peristiwa yang dipancarkan untuk kontak nominal dan kelompok titik akhir aliran data terkait.




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 acara disediakan 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"
    }
}
```

Nilai yang mungkin untuk `contactStatus` didefinisikan dalamthe section called “AWS Ground Station status kontak”.

Ground Station Dataflow Endpoint Group Perubahan Status

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"
    }
}
```

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

## Acara Ephemeris

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`

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

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

Untuk informasi lain, lihat Elemen userIdentity CloudTrail .

## 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 mana pun 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_PRINCIPAL_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_PRINCIPAL_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": "Mozilla/5.0 Gecko/20100101 Firefox/123.0",
    "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"
}
```

# Lihat metrik dengan Amazon CloudWatch

Selama kontak, AWS Ground Station secara otomatis menangkap dan mengirim data CloudWatch untuk analisis. Data Anda dapat dilihat 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.

> **Note**
>
> Metrik spesifik yang dipancarkan tergantung pada AWS Ground Station kemampuan yang digunakan. Bergantung pada konfigurasi Anda, hanya sebagian dari metrik di bawah ini yang dapat dipancarkan.

| Metrik | Dimensi Metrik | Deskripsi |
| --- | --- | --- |
| `AzimuthAngle` | SatelliteId | Sudut azimuth antena. Utara sejati adalah 0 derajat dan timur 90 derajat.<br><br>Unit: derajat |
| `BitErrorRate` | Saluran, Polarisasi, SatelliteId | Tingkat kesalahan pada bit dalam jumlah transmisi bit tertentu. Kesalahan bit disebabkan oleh kebisinga |

| Metrik | Dimensi Metrik | Deskripsi |
| --- | --- | --- |
| | | n, distorsi, atau gangguan<br><br>Unit: Kesalahan bit per satuan waktu |
| `BlockErrorRate` | Saluran, Polarisasi, SatelliteId | Tingkat kesalahan blok dalam jumlah tertentu dari blok yang diterima. Kesalahan blok disebabkan oleh gangguan.<br><br>Unit: Blok yang salah/Jumlah total blok |
| `CarrierFrequencyRecovery_Cn0` | Kategori, Config, SatelliteId | Rasio kepadatan pembawa terhadap kebisingan per unit bandwidth.<br><br>Unit: Desibel-Hertz (dB-Hz) |

| Metrik | Dimensi Metrik | Deskripsi |
| --- | --- | --- |
| `CarrierFrequencyRecovery_Locked` | Kategori, Config, SatelliteId | Atur ke 1 saat loop pemulihan frekuensi pembawa demodulator terkunci dan 0 saat dibuka kuncinya.<br><br>Unit: tanpa unit |
| `CarrierFrequencyRecovery_OffsetFrequency_Hz` | Kategori, Config, SatelliteId | 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.<br><br>Satuan: hertz (Hz) |

| Metrik | Dimensi Metrik | Deskripsi |
| --- | --- | --- |
| `ElevationAngle` | SatelliteId | Sudut elevasi antena. Cakrawala adalah 0 derajat dan zenith adalah 90 derajat.<br><br>Unit: derajat |
| `Es/N0` | Saluran, Polarisasi, SatelliteId | Rasio energi per simbol terhadap kerapatan spektral daya kebisingan.<br><br>Unit: desibel (dB) |
| `ReceivedPower` | Polarisasi, SatelliteId | Kekuatan sinyal yang diukur dalam demodulator/decoder.<br><br>Satuan: desibel relatif terhadap miliwatt (dBm) |
| `SymbolTimingRecovery_ErrorVectorMagnitude` | Kategori, Config, SatelliteId | Besarnya vektor kesalahan antara simbol yang diterima dan titik konstelasi ideal.<br><br>Unit: persen |

| Metrik | Dimensi Metrik | Deskripsi |
| --- | --- | --- |
| `SymbolTimingRecovery_Locked` | Kategori, Config, SatelliteId | Setel ke 1 saat loop pemulihan waktu simbol demodulator terkunci dan 0 saat dibuka<br><br>Unit: tanpa unit |
| `SymbolTimingRecovery_OffsetSymbolRate` | Kategori, Config, SatelliteId | 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.<br><br>Unit: simbol/detik |

## Dimensi apa yang digunakan AWS Ground Station?

Anda dapat memfilter AWS Ground Station data menggunakan dimensi berikut.

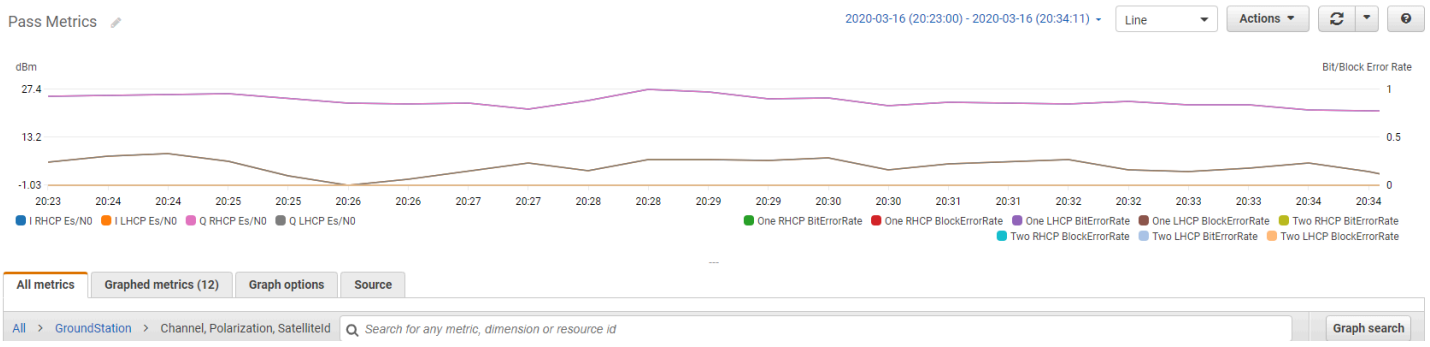
| Dimensi | Deskripsi |
| --- | --- |
| `Category` | Demodulasi atau Decode. |
| `Channel` | Saluran untuk setiap kontak termasuk Satu, Dua, I (dalam fase), dan Q (kuadratur). |

| Dimensi | Deskripsi |
| --- | --- |
| `Config` | Konfigurasi decode demod downlink antena arn. |
| `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 Untuk informasi selengkapnya tentang CloudWatch retensi, lihat CloudWatch Konsep Amazon - Retensi metrik.

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.

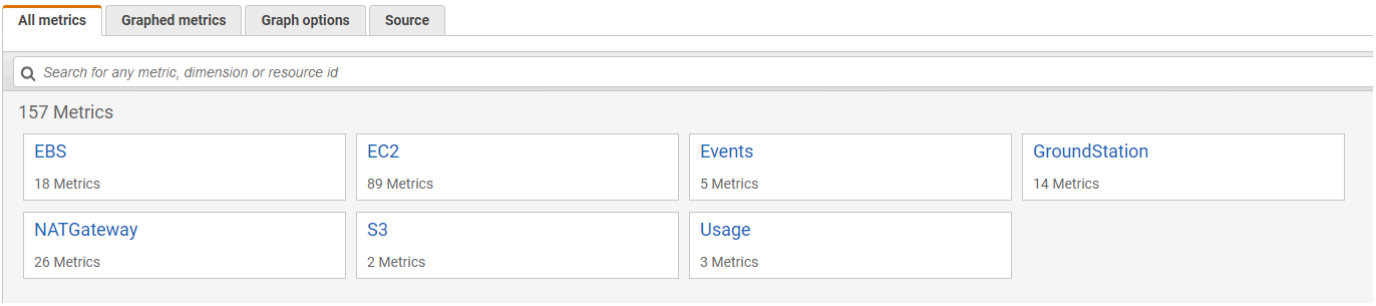



Untuk informasi selengkapnya tentang AWS Ground Station metrik grafik CloudWatch, lihat Metrik Grafik.

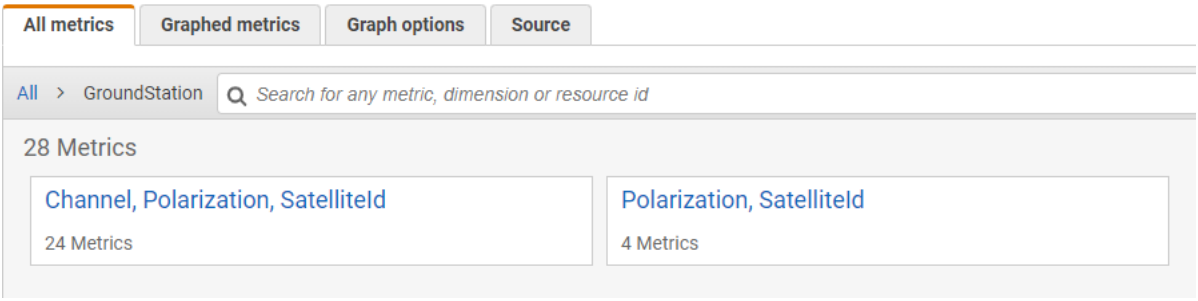
### Untuk melihat metrik menggunakan konsol

1. Buka konsol CloudWatch .

2. Di panel navigasi, 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 memfilter berdasarkan sumber daya, pilih ID sumber daya, lalu 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 versi 2.

2. Gunakan get-metric-datametode CloudWatch CLI untuk menghasilkan file yang dapat dimodifikasi untuk menentukan metrik yang Anda minati, dan kemudian digunakan untuk menanyakan metrik tersebut.

   Untuk melakukan ini, jalankan yang berikut:`aws cloudwatch get-metric-data --generate-cli-skeleton`. Ini akan menghasilkan output yang mirip dengan:

```
{
    "MetricDataQueries": [
        {
            "Id": "",
            "MetricStat": {
                "Metric": {
                    "Namespace": "",
                    "MetricName": "",
                    "Dimensions": [
                        {
                            "Name": "",
                            "Value": ""
                        }
                    ]
                },
                "Period": 0,
                "Stat": "",
                "Unit": "Seconds"
            },
            "Expression": "",
            "Label": "",
            "ReturnData": true,
            "Period": 0,
            "AccountId": ""
        } ],
    "StartTime": "1970-01-01T00:00:00",
    "EndTime": "1970-01-01T00:00:00",
    "NextToken": "",
    "ScanBy": "TimestampDescending",
    "MaxDatapoints": 0,
    "LabelOptions": {
        "Timezone": ""
    }
}
```

3. Buat daftar CloudWatch metrik yang tersedia dengan menjalankan`aws cloudwatch list-metrics`.

   Jika Anda baru saja menggunakan AWS Ground Station, metode harus mengembalikan output yang berisi entri seperti:

```
        ...
        {
           "Namespace": "AWS/GroundStation",
           "MetricName": "ReceivedPower",
           "Dimensions": [
              {
                 "Name": "Polarization",
                 "Value": "LHCP"
              },
              {
                 "Name": "SatelliteId",
                 "Value": "arn:aws:groundstation::111111111111:satellite/aaaaaaaa-
bbbb-cccc-dddd-eeeeeeeeeeee"
              }
           ]
        },
        ...
```

   > **Note**
   >
   > Karena keterbatasan CloudWatch, jika sudah lebih dari 2 minggu sejak terakhir kali digunakan AWS Ground Station, maka Anda perlu memeriksa tabel metrik yang tersedia secara manual untuk menemukan nama dan dimensi metrik di namespace `AWS/GroundStation` metrik. Untuk informasi selengkapnya tentang CloudWatch batasan, lihat: Lihat metrik yang tersedia

4. Ubah file JSON yang Anda buat di langkah 2 agar sesuai dengan nilai yang diperlukan dari langkah 3, misalnya`SatelliteId`, dan `Polarization` dari metrik Anda. Pastikan juga untuk memperbarui`StartTime`, dan `EndTime` nilai agar sesuai dengan kontak Anda. Sebagai contoh:

```
        {
           "MetricDataQueries": [
              {
                 "Id": "receivedPowerExample",
                 "MetricStat": {
                    "Metric": {
                       "Namespace": "AWS/GroundStation",
                       "MetricName": "ReceivedPower",
                       "Dimensions": [
                          {
                             "Name": "SatelliteId",
                             "Value":
 "arn:aws:groundstation::111111111111:satellite/aaaaaaaa-bbbb-cccc-dddd-
eeeeeeeeeeee"
                          },
                          {
                             "Name": "Polarization",
                             "Value": "RHCP"
                          }
                       ]
                    },
                    "Period": 300,
                    "Stat": "Maximum",
                    "Unit": "None"
                 },
                 "Label": "ReceivedPowerExample",
                 "ReturnData": true
              }
           ],
           "StartTime": "2024-02-08T00:00:00",
           "EndTime": "2024-04-09T00:00:00"
        }
```

> **Note**
>
> AWS Ground Station menerbitkan metrik setiap 1 hingga 60 detik, tergantung pada metrik. Metrik tidak akan dikembalikan jika `Period` bidang memiliki nilai kurang dari periode penerbitan untuk metrik.

5. Jalankan `aws cloudwatch get-metric-data` dengan file konfigurasi yang dibuat pada langkah sebelumnya. Contoh diberikan di bawah ini.

```
aws cloudwatch get-metric-data --cli-input-json file://
<nameOfConfigurationFileCreatedInStep2>.json
```

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


```
{
   "MetricDataResults": [
      {
         "Id": "receivedPowerExample",
         "Label": "ReceivedPowerExample",
         "Timestamps": [
            "2024-04-08T18:35:00+00:00",
            "2024-04-08T18:30:00+00:00",
            "2024-04-08T18:25:00+00:00"
         ],
         "Values": [
            -33.30191555023193,
            -31.46100273132324,
            -32.13915576934814
         ],
         "StatusCode": "Complete"
      }
   ],
   "Messages": []
}
```

# Keamanan di AWS Ground Station

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda akan mendapat 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 termasuk keamanan jaringan, manajemen konfigurasi, kontrol akses, dan keamanan data.

Saat menggunakan AWS Ground Station, kami menyarankan Anda mengikuti praktik terbaik industri dan menerapkan end-to-end enkripsi. AWS menyediakan APIs bagi Anda untuk mengintegrasikan enkripsi dan perlindungan data. Untuk informasi selengkapnya tentang AWS keamanan, lihat whitepaper Pengantar AWS Security.

Gunakan topik berikut untuk mempelajari cara mengamankan sumber daya Anda.

Topik



## 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

- 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 dasar 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 kredensi identitas Anda. Anda harus diautentikasi (masuk ke AWS) sebagai Pengguna root akun AWS, sebagai pengguna IAM, atau dengan mengasumsikan peran IAM.

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

menyiapkan federasi identitas menggunakan peran IAM. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

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

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensil Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Guna mengetahui informasi selengkapnya tentang penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, lihat AWS Signature Version 4 untuk permintaan API dalam Panduan Pengguna IAM.

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

### Akun AWS pengguna root

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

### Identitas gabungan

Sebagai praktik terbaik, mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS dengan menggunakan kredensi sementara.

Identitas federasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, direktori Pusat Identitas AWS Directory Service, atau pengguna mana pun yang mengakses Layanan AWS dengan menggunakan kredensil yang disediakan melalui sumber identitas. Ketika

identitas federasi mengakses Akun AWS, mereka mengambil peran, dan peran memberikan kredensi sementara.

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

## Pengguna dan grup IAM

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

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

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

## Peran IAM

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

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat Buat peran untuk penyedia identitas pihak ketiga dalam Panduan Pengguna IAM. Jika menggunakan Pusat Identitas IAM, Anda harus mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas tersebut diautentikasi, Pusat Identitas IAM akan mengorelasikan set izin ke peran dalam IAM. Untuk informasi tentang set izin, lihat Set izin dalam Panduan Pengguna AWS IAM Identity Center .
- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM guna mendapatkan berbagai izin secara sementara untuk tugas tertentu.
- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (prinsipal tepercaya) di akun lain untuk mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa Layanan AWS, Anda dapat melampirkan kebijakan langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM dalam Panduan Pengguna IAM.
- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Misalnya, saat Anda melakukan panggilan dalam suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.
  - Sesi akses teruskan (FAS) — Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses maju.
  - Peran layanan – Peran layanan adalah peran IAM yang dijalankan oleh layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Buat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.

  - Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.
- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan peran IAM untuk mengelola kredensi sementara untuk aplikasi yang berjalan pada EC2 instance dan membuat AWS CLI atau AWS permintaan API. Ini lebih baik untuk menyimpan kunci akses dalam EC2 instance. Untuk menetapkan AWS peran ke EC2 instance dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instans yang dilampirkan ke instance. Profil instance berisi peran dan memungkinkan program yang berjalan pada EC2 instance untuk mendapatkan kredensi sementara. Untuk informasi selengkapnya, lihat Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan di EC2 instans Amazon di Panduan Pengguna IAM.

## Mengelola akses menggunakan kebijakan

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

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Secara default, pengguna dan peran tidak memiliki izin. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

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

## Kebijakan berbasis identitas

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

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan yang dikelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat dilampirkan ke beberapa pengguna, grup, dan peran dalam. Akun AWS Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan yang dikelola atau kebijakan inline, lihat Pilih antara kebijakan yang dikelola dan kebijakan inline dalam Panduan Pengguna IAM.

## Kebijakan berbasis sumber daya

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

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

## Daftar kontrol akses (ACLs)

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

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

## Jenis-jenis kebijakan lain

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

- Batasan izin – Batasan izin adalah fitur lanjutan tempat Anda mengatur izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas ke entitas IAM (pengguna IAM atau peran IAM). Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batasan izin, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCPs) — SCPs adalah kebijakan JSON yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di. AWS Organizations AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur dalam organisasi, Anda dapat menerapkan kebijakan kontrol layanan (SCPs) ke salah satu atau semua akun Anda. SCP membatasi izin untuk entitas di akun anggota, termasuk masing-masing. Pengguna root akun AWS Untuk informasi selengkapnya tentang Organizations dan SCPs, lihat Kebijakan kontrol layanan di Panduan AWS Organizations Pengguna.
- Kebijakan kontrol sumber daya (RCPs) — RCPs adalah kebijakan JSON yang dapat Anda gunakan untuk menetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda tanpa memperbarui kebijakan IAM yang dilampirkan ke setiap sumber daya yang Anda miliki. RCP membatasi izin untuk sumber daya di akun anggota dan dapat memengaruhi izin efektif untuk identitas, termasuk Pengguna root akun AWS, terlepas dari apakah itu milik organisasi Anda. Untuk informasi selengkapnya tentang Organizations dan RCPs, termasuk daftar dukungan Layanan AWS tersebut RCPs, lihat Kebijakan kontrol sumber daya (RCPs) di Panduan AWS Organizations Pengguna.
- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya, lihat Kebijakan sesi dalam Panduan Pengguna IAM.

### Berbagai jenis kebijakan

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

## Bagaimana 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 |
| ACLs | Tidak |
| ABAC (tanda dalam kebijakan) | Ya |
| Kredensial sementara | Ya |
| Izin principal | 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 Tentukan izin IAM kustom dengan kebijakan terkelola pelanggan dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. Anda tidak dapat menentukan secara spesifik prinsipal dalam sebuah kebijakan berbasis identitas karena prinsipal berlaku bagi pengguna atau peran yang melekat kepadanya. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan JSON IAM dalam Panduan Pengguna IAM.

Contoh kebijakan berbasis identitas untuk 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 principal dalam akun yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun di IAM dalam Panduan Pengguna IAM.

## Tindakan kebijakan untuk AWS Ground Station

Mendukung tindakan kebijakan: Ya

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

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

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

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. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

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

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

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

Untuk melihat daftar jenis sumber daya dan jenis AWS Ground Station sumber daya ARNs, 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 oleh 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: Yes

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

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

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

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

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

Untuk melihat 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

## ACLs di AWS Ground Station

Mendukung ACLs: Tidak

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

## 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 tanda milik prinsipal cocok dengan tanda 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 tanda, berikan informasi tentang tanda 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 Tentukan izin dengan otorisasi 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 kredensi sementara dengan AWS Ground Station

Mendukung kredensial sementara: Ya

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

Anda menggunakan kredensi sementara jika Anda masuk AWS Management Console menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, ketika Anda mengakses AWS menggunakan tautan masuk tunggal (SSO) perusahaan Anda, proses tersebut secara otomatis membuat kredensil sementara. Anda juga akan secara otomatis membuat kredensial sementara ketika Anda masuk ke konsol sebagai seorang pengguna lalu beralih peran. Untuk informasi selengkapnya tentang peralihan peran, lihat Beralih dari pengguna ke peran IAM (konsol) dalam Panduan Pengguna IAM.

Anda dapat membuat kredenal sementara secara manual menggunakan API AWS CLI atau AWS . Anda kemudian dapat menggunakan kredensi sementara tersebut untuk mengakses. AWS AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensi sementara alih-

alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensial keamanan sementara di IAM.

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

> **Warning**
>
> Mengubah izin untuk peran layanan dapat merusak 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 mengubah sumber daya AWS Ground Station . 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 dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

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

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh AWS Ground Station, termasuk format ARNs untuk setiap jenis sumber daya, lihat Kunci tindakan, sumber daya, dan kondisi untuk AWS Ground Station dalam 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 yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi

selengkapnya, lihat Kebijakan yang dikelola AWS atau Kebijakan yang dikelola AWS untuk fungsi tugas dalam Panduan Pengguna IAM.

- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat Kebijakan dan izin dalam IAM dalam Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Kondisi dalam Panduan Pengguna IAM.
- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat Validasi kebijakan dengan IAM Access Analyzer dalam Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Anda, Akun AWS aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Amankan akses API dengan MFA dalam Panduan Pengguna IAM.

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

## 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 (ACLs), 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 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.

# AWS kebijakan terkelola untuk AWS Ground Station

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

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

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

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

## AWS kebijakan terkelola: AWSGround StationAgentInstancePolicy

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

Kebijakan ini memberikan izin AWS Ground Station Agen ke EC2 instans Amazon Anda yang memungkinkan instans mengirim dan menerima data selama kontak Ground Station. Semua izin dalam kebijakan ini berasal dari layanan Ground Station.

Detail izin

Kebijakan ini mencakup izin berikut.

- `groundstation`— Memungkinkan instance titik akhir aliran data untuk memanggil Agen Ground Station. APIs

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

## AWS kebijakan terkelola: AWSService RoleForGroundStationDataflowEndpointGroupPolicy

Anda tidak dapat melampirkan AWSService RoleForGroundStationDataflowEndpointGroupPolicy ke entitas IAM Anda. Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan AWS

Ground Station untuk melakukan tindakan atas nama Anda. Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan.

Kebijakan ini memberikan EC2 izin yang memungkinkan AWS Ground Station untuk menemukan alamat publik IPv4 .

Detail izin

Kebijakan ini mencakup izin berikut.

- `ec2:DescribeAddresses`— Memungkinkan AWS Ground Station untuk membuat daftar semua IPs yang terkait dengan EIPs atas nama Anda.
- `ec2:DescribeNetworkInterfaces`— Memungkinkan AWS Ground Station untuk mendapatkan informasi tentang antarmuka jaringan yang terkait dengan EC2 instance atas nama Anda.

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

## AWS Ground Station pembaruan kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola AWS Ground Station sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman Riwayat AWS Ground Station dokumen.

| Perubahan | Deskripsi | Tanggal |
| --- | --- | --- |
| AWSGroundStationAgentInstancePolicy – Kebijakan baru | AWS Ground Station menambahkan kebijakan baru untuk memberikan izin instans titik akhir aliran data untuk menggunakan AWS Ground Station Agent. | 12 April 2023 |
| AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy – Kebijakan baru | AWS Ground Station menambahkan kebijakan baru yang memberikan EC2 izin untuk memungkinkan AWS Ground Station menemukan IPv4 alamat publik yang terkait dengan EIPs dan antarmuka jaringan yang terkait dengan instance. EC2 | November 02, 2022 |
| AWS Ground Station mulai melacak perubahan | AWS Ground Station mulai melacak perubahan untuk kebijakan AWS terkelola. | Maret 01, 2021 |

# Gunakan peran terkait layanan untuk Ground Station

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

Peran terkait layanan membuat pengaturan Ground Station lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. Ground Station mendefinisikan izin peran terkait

layanan, dan kecuali ditentukan lain, hanya Ground Station yang dapat mengambil perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, serta bahwa kebijakan izin tidak dapat dilampirkan ke entitas IAM lainnya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, silakan lihat layanan AWS yang bisa digunakan dengan IAM dan carilah layanan yang memiliki opsi Ya di kolom Peran terkait layanan. Pilih Ya bersama tautan untuk melihat dokumentasi peran tertaut layanan untuk layanan tersebut.

## Izin peran terkait layanan untuk Ground Station

Ground Station menggunakan peran terkait layanan bernama — AWSServiceRoleForGroundStationDataflowEndpointGroupAWS GroundStation menggunakan peran terkait layanan ini untuk memanggil untuk menemukan alamat publik EC2 . IPv4

Peran AWSService RoleForGroundStationDataflowEndpointGroup terkait layanan mempercayai layanan berikut untuk mengambil peran:

- `groundstation.amazonaws.com`

Kebijakan izin peran bernama AWSService RoleForGroundStationDataflowEndpointGroupPolicy memungkinkan Ground Station menyelesaikan tindakan berikut pada sumber daya yang ditentukan:

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

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

  Tindakan memungkinkan Ground Station untuk mendapatkan informasi tentang antarmuka jaringan yang terkait dengan instance 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. Saat Anda membuat DataflowEndpointGroup di dalam AWS CLI atau AWS API, Ground Station membuat 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. Saat Anda membuat DataflowEndpointGroup, Ground Station menciptakan peran terkait layanan untuk Anda lagi.

Anda juga dapat menggunakan konsol IAM untuk membuat peran terkait layanan dengan kasus penggunaan Pengiriman Data ke Amazon EC2. Di AWS CLI atau AWS API, buat peran terkait layanan dengan nama `groundstation.amazonaws.com` layanan. Untuk informasi selengkapnya, lihat Membuat peran tertaut 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 mengedit peran AWSService RoleForGroundStationDataflowEndpointGroup 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 tertaut 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 DataflowEndpointGroups menggunakan peran terkait layanan. Ini melindungi Anda dari pencabutan izin secara tidak sengaja ke Anda. DataflowEndpointGroups Jika peran terkait layanan digunakan dengan beberapa peran DataflowEndpointGroups, Anda harus menghapus semua DataflowEndpointGroups yang menggunakan peran terkait layanan sebelum dapat menghapusnya.

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

Untuk menghapus sumber daya Ground Station yang digunakan oleh AWSService RoleForGroundStationDataflowEndpointGroup

- Hapus DataflowEndpointGroups melalui AWS CLI atau AWS API.

Untuk menghapus peran terkait layanan secara manual menggunakan IAM

Gunakan konsol IAM, the AWS CLI, atau AWS API untuk menghapus peran AWSService RoleForGroundStationDataflowEndpointGroup terkait layanan. 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 tersedia. Untuk informasi selengkapnya, lihat Tabel Wilayah.

## Pemecahan Masalah

`NOT_AUTHORIZED_TO_CREATE_SLR`- Ini menunjukkan peran dalam akun Anda yang sedang 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.

# Enkripsi data saat istirahat untuk AWS Ground Station

AWS Ground Station menyediakan enkripsi secara default untuk melindungi data sensitif Anda 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 secara

otomatis. 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

| Jenis 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 Anda.

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

- Kirim GenerateDataKeypermintaan ke AWS KMS untuk menghasilkan kunci data yang dienkripsi oleh kunci yang dikelola pelanggan Anda.
- Kirim permintaan Dekripsi ke AWS KMS untuk mendekripsi kunci data terenkripsi sehingga mereka dapat digunakan untuk mengenkripsi data Anda.
- Kirim permintaan Enkripsi 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 APIs KMS.

### 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 terkelola 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 GenerateDataKeyuntuk menghasilkan kunci data terenkripsi dan menyimpannya, karena kunci data tidak segera digunakan untuk mengenkripsi.

- Panggil Dekripsi untuk menggunakan kunci data terenkripsi yang disimpan untuk mengakses data terenkripsi.
- Panggil Enkripsi 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 terkelola 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"
}
```

# Enkripsi data selama transit untuk AWS Ground Station

AWS Ground Station menyediakan enkripsi secara default untuk melindungi data sensitif Anda selama transit. Data dapat dialirkan antara lokasi AWS Ground Station antena dan EC2 instans Amazon Anda dengan dua cara, tergantung pada konfigurasi profil misi.

- AWS Ground Station Agen
- Titik akhir aliran data

Setiap metode streaming data menangani enkripsi data dalam perjalanan secara berbeda. Bagian berikut menjelaskan setiap metode.

## AWS Ground Station Aliran agen

AWS Ground Station Agen mengenkripsi alirannya menggunakan kunci yang dikelola pelanggan. AWS KMS AWS Ground Station Agen yang berjalan di EC2 instans Amazon Anda akan secara otomatis mendekripsi aliran untuk menyediakan data yang didekripsi.

AWS KMS Kunci yang digunakan untuk mengenkripsi aliran ditentukan saat membuat parameter `MissionProfile` dalam. streamsKmsKey Semua izin yang memberikan AWS Ground Station akses ke kunci ditangani melalui kebijakan AWS KMS kunci yang dilampirkan. `streamsKmsKey`

# Aliran titik akhir aliran data

Aliran titik akhir Dataflow dienkripsi menggunakan Datagram Transport Layer Security (DTLS). Ini dilakukan dengan menggunakan sertifikat yang ditandatangani sendiri, dan tidak memerlukan konfigurasi tambahan.

# Contoh konfigurasi profil misi

Contoh yang diberikan menunjukkan bagaimana mengambil satelit siaran publik dan membuat profil misi yang mendukungnya. Template yang dihasilkan disediakan untuk membantu Anda mengambil kontak satelit siaran publik dan untuk membantu Anda membuat keputusan tentang satelit Anda.

Topik



## JPSS-1 - Public broadcast satellite (PBS) - Evaluasi

Bagian contoh ini cocok denganIkhtisar proses orientasi pelanggan. Ini memberikan analisis kompatibilitas singkat dengan AWS Ground Station dan menetapkan panggung untuk contoh-contoh spesifik yang mengikuti.

Seperti disebutkan di Satelit siaran publik bagian ini, Anda dapat menggunakan satelit tertentu, atau jalur komunikasi satelit, yang tersedia untuk umum. Pada bagian ini kami menjelaskan JPSS-1 dalam istilah. AWS Ground Station Sebagai referensi, kami menggunakan Joint Polar Satellite System 1 (JPSS-1) Spacecraft High Rate Data (HRD) ke Direct Broadcast Stations (DBS) Radio Frequency (RF) Interface Control Document (ICD) untuk melengkapi contoh. Juga, perlu dicatat bahwa JPSS-1 dikaitkan dengan NORAD ID 43013.

Satelit JPSS-1 menawarkan satu uplink dan tiga jalur komunikasi downlink langsung, seperti yang terlihat pada Gambar 1-1 dari ICD. Dari keempat jalur komunikasi ini, hanya jalur komunikasi downlink High Rate Data (HRD) tunggal yang tersedia untuk konsumsi publik. Berdasarkan ini, Anda akan melihat jalur ini akan memiliki data yang jauh lebih spesifik yang terkait dengannya juga. Keempat jalur tersebut adalah sebagai berikut:

- Jalur perintah (uplink) pada frekuensi MHz pusat 2067,27 dengan kecepatan data 2-128 kbps. Jalur ini tidak dapat diakses publik.
- Jalur telemetri (downlink) pada frekuensi MHz pusat 2247,5 dengan kecepatan data 1-524 kbps. Jalur ini tidak dapat diakses publik.

- Jalur SMD (downlink) pada frekuensi GHz tengah 26,7034 dengan kecepatan data 150-300 Mbps. Jalur ini tidak dapat diakses publik.
- RF untuk jalur HRD (downlink) pada frekuensi MHz pusat 7812 dengan kecepatan data 15 Mbps. Ini memiliki MHz bandwidth 30, dan adalah right-hand-circular-polarized. Saat Anda menggunakan JPSS-1 AWS Ground Station, ini adalah jalur komunikasi yang dapat Anda akses. Jalur komunikasi ini berisi data ilmu instrumen, data rekayasa instrumen, data telemetri instrumen, dan data rumah tangga pesawat ruang angkasa real-time.

Saat kami membandingkan jalur data potensial, kami melihat bahwa jalur perintah (uplink), telemetri (downlink), dan HRD (downlink) memenuhi frekuensi, bandwidth, dan kemampuan penggunaan bersamaan multi-saluran. AWS Ground Station Jalur SMD tidak kompatibel karena frekuensi pusat berada di luar jangkauan penerima yang ada. Untuk informasi selengkapnya tentang kemampuan yang didukung, lihatAWS Ground Station Kemampuan Situs.

> **Note**
>
> Karena jalur SMD tidak kompatibel AWS Ground Station dengannya tidak akan direpresentasikan dalam konfigurasi contoh.

> **Note**
>
> Karena jalur perintah (uplink) dan telemetri (downlink) tidak ditentukan dalam ICD, juga tidak tersedia untuk penggunaan umum, nilai yang diberikan saat digunakan adalah nosional.

## Satelit siaran publik memanfaatkan pengiriman data Amazon S3

Contoh ini dibangun dari analisis yang dilakukan di JPSS-1 - Public broadcast satellite (PBS) - Evaluasi bagian panduan pengguna.

Untuk contoh ini, Anda harus mengasumsikan skenario -- Anda ingin menangkap jalur komunikasi HRD sebagai frekuensi menengah digital dan menyimpannya untuk pemrosesan batch masa depan. Ini menghemat sampel kuadratur fase (I/Q) frekuensi radio mentah (RF) setelah didigitalkan. Setelah data ada di bucket Amazon S3 Anda, Anda dapat mendemodulasi dan memecahkan kode data menggunakan perangkat lunak apa pun yang Anda inginkan. Lihat MathWorks Tutorial untuk contoh rinci pemrosesan. Setelah menggunakan contoh ini, Anda dapat mempertimbangkan untuk

menambahkan komponen harga EC2 spot Amazon untuk memproses data dan menurunkan biaya pemrosesan Anda secara keseluruhan.

## Jalur komunikasi

Bagian ini Rencanakan jalur komunikasi aliran data Anda mewakili memulai.

Semua cuplikan template berikut termasuk dalam bagian Resources dari template. AWS CloudFormation

```
Resources:
  # Resources that you would like to create should be placed within the Resources
 section.
```

> **Note**
>
> Untuk informasi selengkapnya tentang isi AWS CloudFormation template, lihat bagian Template.

Mengingat skenario kami untuk mengirimkan jalur komunikasi tunggal ke Amazon S3, Anda tahu bahwa Anda akan memiliki satu jalur pengiriman asinkron. Per Pengiriman data asinkron bagian, Anda harus menentukan bucket Amazon S3.

```
  # The S3 bucket where AWS Ground Station will deliver the downlinked data.
  GroundStationS3DataDeliveryBucket:
    Type: AWS::S3::Bucket
    DeletionPolicy: Retain
    UpdateReplacePolicy: Retain
    Properties:
      # Results in a bucket name formatted like: aws-groundstation-data-{account id}-
{region}-{random 8 character string}
      BucketName: !Join ["-", ["aws-groundstation-data", !Ref AWS::AccountId, !Ref
 AWS::Region, !Select [0, !Split ["-", !Select [2, !Split ["/", !Ref AWS::StackId]]]]]]
```

Selain itu, Anda perlu membuat peran dan kebijakan yang sesuai AWS Ground Station untuk memungkinkan penggunaan bucket.

```
  # The IAM role that AWS Ground Station will assume to have permission find and write
  # data to your S3 bucket.
  GroundStationS3DataDeliveryRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Statement:
          - Action:
              - 'sts:AssumeRole'
            Effect: Allow
            Principal:
              Service:
                - groundstation.amazonaws.com
            Condition:
              StringEquals:
                "aws:SourceAccount": !Ref AWS::AccountId
              ArnLike:
                "aws:SourceArn": !Sub "arn:aws:groundstation:${AWS::Region}:
${AWS::AccountId}:config/s3-recording/*"

  # The S3 bucket policy that defines what actions AWS Ground Station can perform on
 your S3 bucket.
  GroundStationS3DataDeliveryBucketPolicy:
    Type: AWS::IAM::Policy
    Properties:
      PolicyDocument:
        Statement:
          - Action:
              - 's3:GetBucketLocation'
            Effect: Allow
            Resource:
              - !GetAtt GroundStationS3DataDeliveryBucket.Arn
          - Action:
              - 's3:PutObject'
            Effect: Allow
            Resource:
              - !Join [ "/", [ !GetAtt GroundStationS3DataDeliveryBucket.Arn, "*" ] ]
      PolicyName: GroundStationS3DataDeliveryPolicy
      Roles:
        - !Ref GroundStationS3DataDeliveryRole
```

# AWS Ground Station konfigurasi

Bagian ini Buat konfigurasi mewakili memulai.

Anda memerlukan konfigurasi pelacakan untuk mengatur preferensi Anda menggunakan autotrack. Memilih PREFERRED sebagai autotrack dapat meningkatkan kualitas sinyal, tetapi tidak diperlukan untuk memenuhi kualitas sinyal karena kualitas ephemeris JPSS-1 yang memadai.

```
 TrackingConfig:
   Type: AWS::GroundStation::Config
   Properties:
     Name: "JPSS Tracking Config"
     ConfigData:
       TrackingConfig:
         Autotrack: "PREFERRED"
```

Berdasarkan jalur komunikasi, Anda harus menentukan konfigurasi antena-downlink untuk mewakili bagian satelit serta perekaman s3 untuk merujuk ke bucket Amazon S3 yang baru saja Anda buat.

```
 # The AWS Ground Station Antenna Downlink Config that defines the frequency spectrum
used to
 # downlink data from your satellite.
 JpssDownlinkDigIfAntennaConfig:
   Type: AWS::GroundStation::Config
   Properties:
     Name: "JPSS Downlink DigIF Antenna Config"
     ConfigData:
       AntennaDownlinkConfig:
         SpectrumConfig:
           Bandwidth:
             Units: "MHz"
             Value: 30
           CenterFrequency:
             Units: "MHz"
             Value: 7812
           Polarization: "RIGHT_HAND"

 # The AWS Ground Station S3 Recording Config that defines the S3 bucket and IAM role
to use
```

```
  # when AWS Ground Station delivers the downlink data.
  S3RecordingConfig:
    Type: AWS::GroundStation::Config
    DependsOn: GroundStationS3DataDeliveryBucketPolicy
    Properties:
      Name: "JPSS S3 Recording Config"
      ConfigData:
        S3RecordingConfig:
          BucketArn: !GetAtt GroundStationS3DataDeliveryBucket.Arn
          RoleArn: !GetAtt GroundStationS3DataDeliveryRole.Arn
```

## AWS Ground Station profil misi

Bagian ini Buat profil misi mewakili memulai.

Sekarang setelah Anda memiliki konfigurasi terkait, Anda dapat menggunakannya untuk membangun aliran data. Anda akan menggunakan default untuk parameter yang tersisa.

```
  # The AWS Ground Station Mission Profile that groups the above configurations to
define how to downlink data.
  JpssAsynchMissionProfile:
    Type: AWS::GroundStation::MissionProfile
    Properties:
      Name: "43013 JPSS Asynchronous Data"
      MinimumViableContactDurationSeconds: 180
      TrackingConfigArn: !Ref TrackingConfig
      DataflowEdges:
        - Source: !Ref JpssDownlinkDigIfAntennaConfig
          Destination: !Ref S3RecordingConfig
```

## Menyatukannya

Dengan sumber daya di atas, Anda sekarang memiliki kemampuan untuk menjadwalkan kontak JPSS-1 untuk pengiriman data asinkron dari salah satu onboard Anda. AWS Ground Station AWS Ground Station Lokasi

Berikut ini adalah AWS CloudFormation template lengkap yang mencakup semua sumber daya yang dijelaskan dalam bagian ini digabungkan menjadi satu template yang dapat langsung digunakan AWS CloudFormation.

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.

Jika Aqua, SNPP, JPSS-1/NOAA-20, dan Terra tidak masuk ke akun Anda, lihat. Satelit onboard

> **Note**
>
> Anda dapat mengakses template dengan mengakses bucket Amazon S3 yang melakukan onboarding pelanggan menggunakan kredensi yang valid. AWS Tautan di bawah ini menggunakan bucket Amazon S3 regional. Ubah kode `us-west-2` wilayah untuk mewakili wilayah yang sesuai tempat Anda ingin membuat AWS CloudFormation tumpukan.
> Selain itu, petunjuk berikut menggunakan YAMAL. Namun, template tersedia dalam format YAMAL dan JSON. Untuk menggunakan JSON, ganti ekstensi `.yml` file dengan `.json` saat mengunduh templat.

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
```

# Satelit siaran publik menggunakan titik akhir aliran data (narrowband)

Contoh ini dibangun dari analisis yang dilakukan di JPSS-1 - Public broadcast satellite (PBS) - Evaluasi bagian panduan pengguna.

Untuk melengkapi contoh ini, Anda harus mengasumsikan skenario -- Anda ingin menangkap jalur komunikasi HRD sebagai frekuensi menengah digital (DiGIF) dan memprosesnya seperti yang diterima oleh aplikasi endpoint aliran data pada instance EC2 Amazon menggunakan SDR.

## Jalur komunikasi

Bagian ini Rencanakan jalur komunikasi aliran data Anda mewakili memulai. Untuk contoh ini, Anda akan membuat dua bagian dalam AWS CloudFormation template Anda: bagian Parameter dan Sumber Daya.

> **Note**
>
> Untuk informasi selengkapnya tentang isi AWS CloudFormation template, lihat bagian Template.

Untuk bagian Parameter, Anda akan menambahkan parameter berikut. Anda akan menentukan nilai untuk ini saat membuat tumpukan melalui AWS CloudFormation konsol.

```
Parameters:
  EC2Key:
    Description: The SSH key used to access the EC2 receiver instance. Choose any
 SSH key if you are not creating an EC2 receiver instance. For instructions on how to
 create an SSH key see https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/create-
key-pairs.html
    Type: AWS::EC2::KeyPair::KeyName
    ConstraintDescription: must be the name of an existing EC2 KeyPair.

  ReceiverAMI:
    Description: The Ground Station DDX AMI ID you want to use. Please note
 that AMIs are region specific. For instructions on how to retrieve an AMI
 see https://docs.aws.amazon.com/ground-station/latest/ug/dataflows.ec2-
configuration.html#dataflows.ec2-configuration.amis
    Type: AWS::EC2::Image::Id
```

> **Note**
>
> Anda perlu membuat key pair, dan memberikan nama untuk EC2 `EC2Key` parameter Amazon. Lihat Membuat key pair untuk EC2 instans Amazon Anda.

Selain itu, Anda harus memberikan ID AMI spesifik wilayah yang benar, saat membuat AWS CloudFormation tumpukan. Lihat AWS Ground Station Gambar Mesin Amazon (AMIs).

Cuplikan template yang tersisa termasuk dalam bagian Resources dari template. AWS CloudFormation

```
Resources:
  # Resources that you would like to create should be placed within the resource
 section.
```

Mengingat skenario kami untuk mengirimkan jalur komunikasi tunggal ke sebuah EC2 instance, Anda akan memiliki satu jalur pengiriman sinkron. Per Pengiriman data sinkron bagian, Anda harus menyiapkan dan mengonfigurasi EC2 instans Amazon dengan aplikasi titik akhir aliran data, dan membuat satu atau beberapa grup titik akhir aliran data.

```
  # The EC2 instance that will send/receive data to/from your satellite using AWS
 Ground Station.
  ReceiverInstance:
    Type: AWS::EC2::Instance
    Properties:
      DisableApiTermination: false
      IamInstanceProfile: !Ref GeneralInstanceProfile
      ImageId: !Ref ReceiverAMI
      InstanceType: m5.4xlarge
      KeyName: !Ref EC2Key
      Monitoring: true
      PlacementGroupName: !Ref ClusterPlacementGroup
      SecurityGroupIds:
        - Ref: InstanceSecurityGroup
      SubnetId: !Ref ReceiverSubnet
      BlockDeviceMappings:
        - DeviceName: /dev/xvda
          Ebs:
            VolumeType: gp2
            VolumeSize: 40
      Tags:
        - Key: Name
          Value: !Join [ "-" , [ "Receiver" , !Ref "AWS::StackName" ] ]
      UserData:
```

```
        Fn::Base64:
          |
          #!/bin/bash
          exec > >(tee /var/log/user-data.log|logger -t user-data -s 2>/dev/console)
2>&1
          echo `date +'%F %R:%S'` "INFO: Logging Setup" >&2

          GROUND_STATION_DIR="/opt/aws/groundstation"
          GROUND_STATION_BIN_DIR="${GROUND_STATION_DIR}/bin"
          STREAM_CONFIG_PATH="${GROUND_STATION_DIR}/customer_stream_config.json"

          echo "Creating ${STREAM_CONFIG_PATH}"
          cat << STREAM_CONFIG > "${STREAM_CONFIG_PATH}"
          {
            "ddx_streams": [
              {
                "streamName": "Downlink",
                "maximumWanRate": 4000000000,
                "lanConfigDevice": "lo",
                "lanConfigPort": 50000,
                "wanConfigDevice": "eth1",
                "wanConfigPort": 55888,
                "isUplink": false
              }
            ]
          }
          STREAM_CONFIG

          echo "Waiting for dataflow endpoint application to start"
          while netstat -lnt | awk '$4 ~ /:80$/ {exit 1}'; do sleep 10; done

          echo "Configuring dataflow endpoint application streams"
          python "${GROUND_STATION_BIN_DIR}/configure_streams.py" --configFileName
"${STREAM_CONFIG_PATH}"
          sleep 2
          python "${GROUND_STATION_BIN_DIR}/save_default_config.py"

          exit 0

  # The AWS Ground Station Dataflow Endpoint Group that defines the endpoints that AWS
Ground
  # Station will use to send/receive data to/from your satellite.
  DataflowEndpointGroup:
    Type: AWS::GroundStation::DataflowEndpointGroup
```

```
    Properties:
      ContactPostPassDurationSeconds: 180
      ContactPrePassDurationSeconds: 120
      EndpointDetails:
        - Endpoint:
            Name: !Join [ "-" , [ !Ref "AWS::StackName" , "Downlink" ] ] # needs to
match DataflowEndpointConfig name
            Address:
              Name: !GetAtt ReceiverInstanceNetworkInterface.PrimaryPrivateIpAddress
              Port: 55888
          SecurityDetails:
            SecurityGroupIds:
              - Ref: "DataflowEndpointSecurityGroup"
            SubnetIds:
              - !Ref ReceiverSubnet
            RoleArn: !GetAtt DataDeliveryServiceRole.Arn

  # The security group for your EC2 instance.
  InstanceSecurityGroup:
    Type: AWS::EC2::SecurityGroup
    Properties:
      GroupDescription: AWS Ground Station receiver instance security group.
      VpcId: !Ref ReceiverVPC
      SecurityGroupIngress:
        # To allow SSH access to the instance, add another rule allowing tcp port 22
from your CidrIp
        - IpProtocol: udp
          FromPort: 55888
          ToPort: 55888
          SourceSecurityGroupId: !Ref DataflowEndpointSecurityGroup
          Description: "AWS Ground Station Downlink Stream"

  # The security group that the ENI created by AWS Ground Station belongs to.
  DataflowEndpointSecurityGroup:
    Type: AWS::EC2::SecurityGroup
    Properties:
      GroupDescription: Security Group for AWS Ground Station registration of Dataflow
Endpoint Groups
      VpcId: !Ref ReceiverVPC
      SecurityGroupEgress:
        - IpProtocol: udp
          FromPort: 55888
          ToPort: 55888
          CidrIp: 10.0.0.0/8
```

```
          Description: "AWS Ground Station Downlink Stream To 10/8"
        - IpProtocol: udp
          FromPort: 55888
          ToPort: 55888
          CidrIp: 172.16.0.0/12
          Description: "AWS Ground Station Downlink Stream To 172.16/12"
        - IpProtocol: udp
          FromPort: 55888
          ToPort: 55888
          CidrIp: 192.168.0.0/16
          Description: "AWS Ground Station Downlink Stream To 192.168/16"

  # The placement group in which your EC2 instance is placed.
  ClusterPlacementGroup:
    Type: AWS::EC2::PlacementGroup
    Properties:
      Strategy: cluster

  ReceiverVPC:
    Type: AWS::EC2::VPC
    Properties:
      CidrBlock: "10.0.0.0/16"
      Tags:
        - Key: "Name"
          Value: "AWS Ground Station - PBS to dataflow endpoint Example VPC"
        - Key: "Description"
          Value: "VPC for EC2 instance receiving AWS Ground Station data"

  ReceiverSubnet:
    Type: AWS::EC2::Subnet
    Properties:
      # Ensure your CidrBlock will always have at least one available IP address per
dataflow endpoint.
      # See https://docs.aws.amazon.com/vpc/latest/userguide/subnet-sizing.html for
subent sizing guidelines.
      CidrBlock: "10.0.0.0/24"
      Tags:
        - Key: "Name"
          Value: "AWS Ground Station - PBS to dataflow endpoint Example Subnet"
        - Key: "Description"
          Value: "Subnet for EC2 instance receiving AWS Ground Station data"
      VpcId: !Ref ReceiverVPC

  # An ENI providing a fixed IP address for AWS Ground Station to connect to.
```

```
 ReceiverInstanceNetworkInterface:
   Type: AWS::EC2::NetworkInterface
   Properties:
     Description: Floating network interface providing a fixed IP address for AWS
Ground Station to connect to.
     GroupSet:
       - !Ref InstanceSecurityGroup
     SubnetId: !Ref ReceiverSubnet

 # Attach the ENI to the EC2 instance.
 ReceiverInstanceInterfaceAttachment:
   Type: AWS::EC2::NetworkInterfaceAttachment
   Properties:
     DeleteOnTermination: false
     DeviceIndex: "1"
     InstanceId: !Ref ReceiverInstance
     NetworkInterfaceId: !Ref ReceiverInstanceNetworkInterface
```

Selain itu, Anda juga perlu membuat kebijakan dan peran yang sesuai AWS Ground Station untuk memungkinkan Anda membuat elastic network interface (ENI) di akun Anda.

```
 # AWS Ground Station assumes this role to create/delete ENIs in your account in order
to stream data.
 DataDeliveryServiceRole:
   Type: AWS::IAM::Role
   Properties:
     Policies:
       - PolicyDocument:
           Statement:
             - Action:
                 - ec2:CreateNetworkInterface
                 - ec2:DeleteNetworkInterface
                 - ec2:CreateNetworkInterfacePermission
                 - ec2:DeleteNetworkInterfacePermission
                 - ec2:DescribeSubnets
                 - ec2:DescribeVpcs
                 - ec2:DescribeSecurityGroups
               Effect: Allow
               Resource: '*'
           Version: '2012-10-17'
         PolicyName: DataDeliveryServicePolicy
```

```
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service:
              - groundstation.amazonaws.com
            Action:
            - sts:AssumeRole

  # The EC2 instance assumes this role.
  InstanceRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: "Allow"
            Principal:
              Service:
                - "ec2.amazonaws.com"
            Action:
              - "sts:AssumeRole"
      Path: "/"
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess
        - arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceforEC2Role
        - arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy
        - arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforSSM

  # The instance profile for your EC2 instance.
  GeneralInstanceProfile:
    Type: AWS::IAM::InstanceProfile
    Properties:
      Roles:
        - !Ref InstanceRole
```

## AWS Ground Station konfigurasi

Bagian ini Buat konfigurasi mewakili memulai.

Anda memerlukan konfigurasi pelacakan untuk mengatur preferensi Anda menggunakan autotrack. Memilih PREFERRED sebagai autotrack dapat meningkatkan kualitas sinyal, tetapi tidak diperlukan untuk memenuhi kualitas sinyal karena kualitas ephemeris JPSS-1 yang memadai.

```
 TrackingConfig:
   Type: AWS::GroundStation::Config
   Properties:
     Name: "JPSS Tracking Config"
     ConfigData:
       TrackingConfig:
         Autotrack: "PREFERRED"
```

Berdasarkan jalur komunikasi, Anda harus menentukan konfigurasi antenna-downlink untuk mewakili bagian satelit, serta konfigurasi dataflow-endpoint untuk merujuk ke grup titik akhir aliran data yang mendefinisikan detail titik akhir.

```
 # The AWS Ground Station Antenna Downlink Config that defines the frequency spectrum
used to
 # downlink data from your satellite.
 SnppJpssDownlinkDigIfAntennaConfig:
   Type: AWS::GroundStation::Config
   Properties:
     Name: "SNPP JPSS Downlink DigIF Antenna Config"
     ConfigData:
       AntennaDownlinkConfig:
         SpectrumConfig:
           Bandwidth:
             Units: "MHz"
             Value: 30
           CenterFrequency:
             Units: "MHz"
             Value: 7812
           Polarization: "RIGHT_HAND"

 # The AWS Ground Station Dataflow Endpoint Config that defines the endpoint used to
downlink data
 # from your satellite.
 DownlinkDigIfEndpointConfig:
   Type: AWS::GroundStation::Config
```

```
    Properties:
      Name: "Aqua SNPP JPSS Downlink DigIF Endpoint Config"
      ConfigData:
        DataflowEndpointConfig:
          DataflowEndpointName: !Join [ "-" , [ !Ref "AWS::StackName" , "Downlink" ] ]
          DataflowEndpointRegion: !Ref AWS::Region
```

## AWS Ground Station profil misi

Bagian ini Buat profil misi mewakili memulai.

Sekarang setelah Anda memiliki konfigurasi terkait, Anda dapat menggunakannya untuk membangun aliran data. Anda akan menggunakan default untuk parameter yang tersisa.

```
 # The AWS Ground Station Mission Profile that groups the above configurations to
define how to
 # uplink and downlink data to your satellite.
 SnppJpssMissionProfile:
   Type: AWS::GroundStation::MissionProfile
   Properties:
     Name: "37849 SNPP And 43013 JPSS"
     ContactPrePassDurationSeconds: 120
     ContactPostPassDurationSeconds: 60
     MinimumViableContactDurationSeconds: 180
     TrackingConfigArn: !Ref TrackingConfig
     DataflowEdges:
       - Source: !Ref SnppJpssDownlinkDigIfAntennaConfig
         Destination: !Ref DownlinkDigIfEndpointConfig
```

## Menyatukannya

Dengan sumber daya di atas, Anda sekarang memiliki kemampuan untuk menjadwalkan kontak JPSS-1 untuk pengiriman data sinkron dari salah satu onboard Anda. AWS Ground Station AWS Ground Station Lokasi

Berikut ini adalah AWS CloudFormation template lengkap yang mencakup semua sumber daya yang dijelaskan dalam bagian ini digabungkan menjadi satu template yang dapat langsung digunakan AWS CloudFormation.

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 EC2 instans Amazon dan AWS CloudFormation sumber daya yang diperlukan untuk menerima data siaran langsung DiGIF mentah.

Jika Aqua, SNPP, JPSS-1/NOAA-20, dan Terra tidak masuk ke akun Anda, lihat. Satelit onboard

> **Note**
>
> Anda dapat mengakses template dengan mengakses bucket Amazon S3 orientasi pelanggan menggunakan kredensi yang valid. AWS Tautan di bawah ini menggunakan bucket Amazon S3 regional. Ubah kode `us-west-2` wilayah untuk mewakili wilayah yang sesuai tempat Anda ingin membuat AWS CloudFormation tumpukan.
> Selain itu, petunjuk berikut menggunakan YAMAL. Namun, template tersedia dalam format YAMAL dan JSON. Untuk menggunakan JSON, ganti ekstensi `.yml` file dengan `.json` saat mengunduh templat.

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 tambahan apa yang ditentukan oleh template?

`AquaSnppJpssTerraDigIF`Template mencakup sumber daya tambahan berikut:

- (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) EC2 Verifikasi untuk Kontak - Opsi untuk menggunakan Lambda untuk menyiapkan sistem verifikasi EC2 instans Amazon Anda untuk kontak dengan notifikasi SNS. Penting untuk dicatat bahwa ini mungkin dikenakan biaya tergantung pada penggunaan Anda saat ini.
- 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.
- Profil misi tambahan - Profil misi untuk satelit siaran publik tambahan (Aqua, SNPP, dan Terra).
- Konfigurasi antena-downlink tambahan - Konfigurasi downlink antena untuk satelit siaran publik tambahan (Aqua, SNPP, dan Terra).

Nilai dan parameter untuk satelit dalam template ini sudah terisi. Parameter ini memudahkan Anda untuk AWS Ground Station segera menggunakan 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 aplikasi titik akhir aliran data 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. AWS::GroundStation::DataflowEndpointGroup

# Satelit siaran publik menggunakan titik akhir aliran data (didemodulasi dan diterjemahkan)

Contoh ini dibangun dari analisis yang dilakukan di JPSS-1 - Public broadcast satellite (PBS) - Evaluasi bagian panduan pengguna.

Untuk melengkapi contoh ini, Anda harus mengasumsikan skenario -- Anda ingin menangkap jalur komunikasi HRD sebagai data siaran langsung yang didemodulasi dan diterjemahkan menggunakan

titik akhir aliran data. Contoh ini adalah titik awal yang baik jika Anda berencana untuk memproses data menggunakan perangkat lunak NASA Direct Readout Labs (RT-STPS dan IPOPP).

## Jalur komunikasi

Bagian ini Rencanakan jalur komunikasi aliran data Anda mewakili memulai. Untuk contoh ini, Anda akan membuat dua bagian dalam AWS CloudFormation template Anda: bagian Parameter dan Sumber Daya.

> **Note**
>
> Untuk informasi selengkapnya tentang isi AWS CloudFormation template, lihat bagian Template.

Untuk bagian Parameter, Anda akan menambahkan parameter berikut. Anda akan menentukan nilai untuk ini saat membuat tumpukan melalui AWS CloudFormation konsol.

```
Parameters:
  EC2Key:
    Description: The SSH key used to access the EC2 receiver instance. Choose any
 SSH key if you are not creating an EC2 receiver instance. For instructions on how to
 create an SSH key see https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/create-
key-pairs.html
    Type: AWS::EC2::KeyPair::KeyName
    ConstraintDescription: must be the name of an existing EC2 KeyPair.

  ReceiverAMI:
    Description: The Ground Station DDX AMI ID you want to use. Please note
 that AMIs are region specific. For instructions on how to retrieve an AMI
 see https://docs.aws.amazon.com/ground-station/latest/ug/dataflows.ec2-
configuration.html#dataflows.ec2-configuration.amis
    Type: AWS::EC2::Image::Id
```

> **Note**
>
> Anda perlu membuat key pair, dan memberikan nama untuk EC2 `EC2Key` parameter Amazon. Lihat Membuat key pair untuk EC2 instans Amazon Anda.

Selain itu, Anda harus memberikan ID AMI spesifik wilayah yang benar, saat membuat AWS CloudFormation tumpukan. Lihat AWS Ground Station Gambar Mesin Amazon (AMIs).

Cuplikan template yang tersisa termasuk dalam bagian Resources dari template. AWS CloudFormation

```
Resources:
  # Resources that you would like to create should be placed within the resource
 section.
```

Mengingat skenario kami untuk mengirimkan jalur komunikasi tunggal ke sebuah EC2 instance, Anda akan memiliki satu jalur pengiriman sinkron. Per Pengiriman data sinkron bagian, Anda harus menyiapkan dan mengonfigurasi EC2 instans Amazon dengan aplikasi titik akhir aliran data, dan membuat satu atau beberapa grup titik akhir aliran data.

```
  # The EC2 instance that will send/receive data to/from your satellite using AWS
 Ground Station.
  ReceiverInstance:
    Type: AWS::EC2::Instance
    Properties:
      DisableApiTermination: false
      IamInstanceProfile: !Ref GeneralInstanceProfile
      ImageId: !Ref ReceiverAMI
      InstanceType: m5.4xlarge
      KeyName: !Ref EC2Key
      Monitoring: true
      PlacementGroupName: !Ref ClusterPlacementGroup
      SecurityGroupIds:
        - Ref: InstanceSecurityGroup
      SubnetId: !Ref ReceiverSubnet
      BlockDeviceMappings:
        - DeviceName: /dev/xvda
          Ebs:
            VolumeType: gp2
            VolumeSize: 40
      Tags:
        - Key: Name
          Value: !Join [ "-" , [ "Receiver" , !Ref "AWS::StackName" ] ]
```

```
      UserData:
        Fn::Base64:
          |
          #!/bin/bash
          exec > >(tee /var/log/user-data.log|logger -t user-data -s 2>/dev/console)
2>&1
          echo `date +'%F %R:%S'` "INFO: Logging Setup" >&2

          GROUND_STATION_DIR="/opt/aws/groundstation"
          GROUND_STATION_BIN_DIR="${GROUND_STATION_DIR}/bin"
          STREAM_CONFIG_PATH="${GROUND_STATION_DIR}/customer_stream_config.json"

          echo "Creating ${STREAM_CONFIG_PATH}"
          cat << STREAM_CONFIG > "${STREAM_CONFIG_PATH}"
          {
            "ddx_streams": [
              {
                "streamName": "Downlink",
                "maximumWanRate": 4000000000,
                "lanConfigDevice": "lo",
                "lanConfigPort": 50000,
                "wanConfigDevice": "eth1",
                "wanConfigPort": 55888,
                "isUplink": false
              }
            ]
          }
          STREAM_CONFIG

          echo "Waiting for dataflow endpoint application to start"
          while netstat -lnt | awk '$4 ~ /:80$/ {exit 1}'; do sleep 10; done

          echo "Configuring dataflow endpoint application streams"
          python "${GROUND_STATION_BIN_DIR}/configure_streams.py" --configFileName
"${STREAM_CONFIG_PATH}"
          sleep 2
          python "${GROUND_STATION_BIN_DIR}/save_default_config.py"

          exit 0
```

```
 # The AWS Ground Station Dataflow Endpoint Group that defines the endpoints that AWS
Ground
```

```
 # Station will use to send/receive data to/from your satellite.
 DataflowEndpointGroup:
   Type: AWS::GroundStation::DataflowEndpointGroup
   Properties:
     ContactPostPassDurationSeconds: 180
     ContactPrePassDurationSeconds: 120
     EndpointDetails:
       - Endpoint:
           Name: !Join [ "-" , [ !Ref "AWS::StackName" , "Downlink" ] ] # needs to
match DataflowEndpointConfig name
           Address:
             Name: !GetAtt ReceiverInstanceNetworkInterface.PrimaryPrivateIpAddress
             Port: 55888
         SecurityDetails:
           SecurityGroupIds:
             - Ref: "DataflowEndpointSecurityGroup"
           SubnetIds:
             - !Ref ReceiverSubnet
           RoleArn: !GetAtt DataDeliveryServiceRole.Arn

 # The security group that the ENI created by AWS Ground Station belongs to.
 DataflowEndpointSecurityGroup:
   Type: AWS::EC2::SecurityGroup
   Properties:
     GroupDescription: Security Group for AWS Ground Station registration of Dataflow
Endpoint Groups
     VpcId: !Ref ReceiverVPC
     SecurityGroupEgress:
       - IpProtocol: udp
         FromPort: 55888
         ToPort: 55888
         CidrIp: 10.0.0.0/8
         Description: "AWS Ground Station Downlink Stream To 10/8"
       - IpProtocol: udp
         FromPort: 55888
         ToPort: 55888
         CidrIp: 172.16.0.0/12
         Description: "AWS Ground Station Downlink Stream To 172.16/12"
       - IpProtocol: udp
         FromPort: 55888
         ToPort: 55888
         CidrIp: 192.168.0.0/16
         Description: "AWS Ground Station Downlink Stream To 192.168/16"
```

```
 # The placement group in which your EC2 instance is placed.
 ClusterPlacementGroup:
   Type: AWS::EC2::PlacementGroup
   Properties:
     Strategy: cluster

 # The security group for your EC2 instance.
 InstanceSecurityGroup:
   Type: AWS::EC2::SecurityGroup
   Properties:
     GroupDescription: AWS Ground Station receiver instance security group.
     VpcId: !Ref ReceiverVPC
     SecurityGroupIngress:
       # To allow SSH access to the instance, add another rule allowing tcp port 22
from your CidrIp
       - IpProtocol: udp
         FromPort: 55888
         ToPort: 55888
         SourceSecurityGroupId: !Ref DataflowEndpointSecurityGroup
         Description: "AWS Ground Station Downlink Stream"

 ReceiverVPC:
   Type: AWS::EC2::VPC
   Properties:
     CidrBlock: "10.0.0.0/16"
     Tags:
       - Key: "Name"
         Value: "AWS Ground Station - PBS to dataflow endpoint Demod Decode Example
VPC"
       - Key: "Description"
         Value: "VPC for EC2 instance receiving AWS Ground Station data"

 ReceiverSubnet:
   Type: AWS::EC2::Subnet
   Properties:
     CidrBlock: "10.0.0.0/24"
     Tags:
       - Key: "Name"
         Value: "AWS Ground Station - PBS to dataflow endpoint Demod Decode Example
Subnet"
       - Key: "Description"
         Value: "Subnet for EC2 instance receiving AWS Ground Station data"
     VpcId: !Ref ReceiverVPC
```

```
 # An ENI providing a fixed IP address for AWS Ground Station to connect to.
 ReceiverInstanceNetworkInterface:
   Type: AWS::EC2::NetworkInterface
   Properties:
     Description: Floating network interface providing a fixed IP address for AWS
Ground Station to connect to.
     GroupSet:
       - !Ref InstanceSecurityGroup
     SubnetId: !Ref ReceiverSubnet

 # Attach the ENI to the EC2 instance.
 ReceiverInstanceInterfaceAttachment:
   Type: AWS::EC2::NetworkInterfaceAttachment
   Properties:
     DeleteOnTermination: false
     DeviceIndex: "1"
     InstanceId: !Ref ReceiverInstance
     NetworkInterfaceId: !Ref ReceiverInstanceNetworkInterface

 # The instance profile for your EC2 instance.
 GeneralInstanceProfile:
   Type: AWS::IAM::InstanceProfile
   Properties:
     Roles:
       - !Ref InstanceRole
```

Anda juga memerlukan kebijakan, peran, dan profil yang sesuai AWS Ground Station untuk memungkinkan Anda membuat elastic network interface (ENI) di akun Anda.

```
 # AWS Ground Station assumes this role to create/delete ENIs in your account in order
to stream data.
 DataDeliveryServiceRole:
   Type: AWS::IAM::Role
   Properties:
     Policies:
       - PolicyDocument:
           Statement:
             - Action:
                 - ec2:CreateNetworkInterface
                 - ec2:DeleteNetworkInterface
                 - ec2:CreateNetworkInterfacePermission
```

```
                - ec2:DeleteNetworkInterfacePermission
                - ec2:DescribeSubnets
                - ec2:DescribeVpcs
                - ec2:DescribeSecurityGroups
              Effect: Allow
              Resource: '*'
          Version: '2012-10-17'
        PolicyName: DataDeliveryServicePolicy
    AssumeRolePolicyDocument:
      Version: 2012-10-17
      Statement:
        - Effect: Allow
          Principal:
            Service:
            - groundstation.amazonaws.com
          Action:
          - sts:AssumeRole

# The EC2 instance assumes this role.
InstanceRole:
  Type: AWS::IAM::Role
  Properties:
    AssumeRolePolicyDocument:
      Version: "2012-10-17"
      Statement:
        - Effect: "Allow"
          Principal:
            Service:
              - "ec2.amazonaws.com"
          Action:
            - "sts:AssumeRole"
    Path: "/"
    ManagedPolicyArns:
      - arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess
      - arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceforEC2Role
      - arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy
      - arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforSSM
```

## AWS Ground Station konfigurasi

Bagian ini Buat konfigurasi mewakili panduan pengguna.

Anda memerlukan konfigurasi pelacakan untuk mengatur preferensi Anda menggunakan autotrack. Memilih PREFERRED sebagai autotrack dapat meningkatkan kualitas sinyal, tetapi tidak diperlukan untuk memenuhi kualitas sinyal karena kualitas ephemeris JPSS-1 yang memadai.

```
 TrackingConfig:
   Type: AWS::GroundStation::Config
   Properties:
     Name: "JPSS Tracking Config"
     ConfigData:
       TrackingConfig:
         Autotrack: "PREFERRED"
```

Berdasarkan jalur komunikasi, Anda harus menentukan konfigurasi untuk mewakili bagian satelit, serta antenna-downlink-demod-decodekonfigurasi dataflow-endpoint untuk merujuk ke grup titik akhir aliran data yang mendefinisikan detail titik akhir.

> **Note**
>
> Untuk detail tentang cara mengatur nilai untuk`DemodulationConfig`, dan`DecodeConfig`, silakan lihatAntena Downlink Demod Decode Config .

```
 # The AWS Ground Station Antenna Downlink Config that defines the frequency spectrum
used to
 # downlink data from your satellite.
 JpssDownlinkDemodDecodeAntennaConfig:
   Type: AWS::GroundStation::Config
   Properties:
     Name: "JPSS Downlink Demod Decode Antenna Config"
     ConfigData:
       AntennaDownlinkDemodDecodeConfig:
         SpectrumConfig:
           CenterFrequency:
             Value: 7812
             Units: "MHz"
           Polarization: "RIGHT_HAND"
           Bandwidth:
             Value: 30
```

```
            Units: "MHz"
        DemodulationConfig:
          UnvalidatedJSON: '{
            "type":"QPSK",
            "qpsk":{
              "carrierFrequencyRecovery":{
                "centerFrequency":{
                  "value":7812,
                  "units":"MHz"
                },
                "range":{
                  "value":250,
                  "units":"kHz"
                }
              },
              "symbolTimingRecovery":{
                "symbolRate":{
                  "value":15,
                  "units":"Msps"
                },
                "range":{
                  "value":0.75,
                  "units":"ksps"
                },
                "matchedFilter":{
                  "type":"ROOT_RAISED_COSINE",
                  "rolloffFactor":0.5
                }
              }
            }
          }'
        DecodeConfig:
          UnvalidatedJSON: '{
            "edges":[
              {
                "from":"I-Ingress",
                "to":"IQ-Recombiner"
              },
              {
                "from":"Q-Ingress",
                "to":"IQ-Recombiner"
              },
              {
                "from":"IQ-Recombiner",
```

```
                "to":"CcsdsViterbiDecoder"
              },
              {
                "from":"CcsdsViterbiDecoder",
                "to":"NrzmDecoder"
              },
              {
                "from":"NrzmDecoder",
                "to":"UncodedFramesEgress"
              }
            ],
            "nodeConfigs":{
              "I-Ingress":{
                "type":"CODED_SYMBOLS_INGRESS",
                "codedSymbolsIngress":{
                  "source":"I"
                }
              },
              "Q-Ingress":{
                "type":"CODED_SYMBOLS_INGRESS",
                "codedSymbolsIngress":{
                  "source":"Q"
                }
              },
              "IQ-Recombiner":{
                "type":"IQ_RECOMBINER"
              },
              "CcsdsViterbiDecoder":{
                "type":"CCSDS_171_133_VITERBI_DECODER",
                "ccsds171133ViterbiDecoder":{
                  "codeRate":"ONE_HALF"
                }
              },
              "NrzmDecoder":{
                "type":"NRZ_M_DECODER"
              },
              "UncodedFramesEgress":{
                "type":"UNCODED_FRAMES_EGRESS"
              }
            }
          }'
```

```
 # The AWS Ground Station Dataflow Endpoint Config that defines the endpoint used to
downlink data
 # from your satellite.
 DownlinkDemodDecodeEndpointConfig:
   Type: AWS::GroundStation::Config
   Properties:
     Name: "Aqua SNPP JPSS Downlink Demod Decode Endpoint Config"
     ConfigData:
       DataflowEndpointConfig:
         DataflowEndpointName: !Join [ "-" , [ !Ref "AWS::StackName" , "Downlink" ] ]
         DataflowEndpointRegion: !Ref AWS::Region
```

## AWS Ground Station profil misi

Bagian ini Buat profil misi mewakili panduan pengguna.

Sekarang setelah Anda memiliki konfigurasi terkait, Anda dapat menggunakannya untuk membangun aliran data. Anda akan menggunakan default untuk parameter yang tersisa.

```
 # The AWS Ground Station Mission Profile that groups the above configurations to
define how to
 # uplink and downlink data to your satellite.
 SnppJpssMissionProfile:
   Type: AWS::GroundStation::MissionProfile
   Properties:
     Name: "37849 SNPP And 43013 JPSS"
     ContactPrePassDurationSeconds: 120
     ContactPostPassDurationSeconds: 60
     MinimumViableContactDurationSeconds: 180
     TrackingConfigArn: !Ref TrackingConfig
     DataflowEdges:
       - Source: !Join [ "/", [ !Ref JpssDownlinkDemodDecodeAntennaConfig,
"UncodedFramesEgress" ] ]
         Destination: !Ref DownlinkDemodDecodeEndpointConfig
```

## Menyatukannya

Dengan sumber daya di atas, Anda sekarang memiliki kemampuan untuk menjadwalkan kontak JPSS-1 untuk pengiriman data sinkron dari salah satu onboard Anda. AWS Ground Station AWS Ground Station Lokasi

Berikut ini adalah AWS CloudFormation template lengkap yang mencakup semua sumber daya yang dijelaskan dalam bagian ini digabungkan menjadi satu template yang dapat langsung digunakan AWS CloudFormation.

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 EC2 instans Amazon dan AWS Ground Station sumber daya yang diperlukan untuk menjadwalkan kontak dan menerima data siaran langsung yang didemodulasi dan diterjemahkan.

Jika Aqua, SNPP, JPSS-1/NOAA-20, dan Terra tidak masuk ke akun Anda, lihat. Satelit onboard

> **Note**
>
> Anda dapat mengakses template dengan mengakses bucket Amazon S3 yang melakukan onboarding pelanggan menggunakan kredensi yang valid. AWS Tautan di bawah ini menggunakan bucket Amazon S3 regional. Ubah kode `us-west-2` wilayah untuk mewakili wilayah yang sesuai tempat Anda ingin membuat AWS CloudFormation tumpukan.
> Selain itu, petunjuk berikut menggunakan YAMAL. Namun, template tersedia dalam format YAMAL dan JSON. Untuk menggunakan JSON, ganti ekstensi `.yml` file dengan `.json` saat mengunduh templat.

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 tambahan apa yang ditentukan oleh template?

`AquaSnppJpss`Template mencakup sumber daya tambahan berikut:

- (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) EC2 Verifikasi untuk Kontak - Opsi untuk menggunakan Lambda untuk menyiapkan sistem verifikasi EC2 instans Amazon Anda untuk kontak dengan notifikasi SNS. Penting untuk dicatat bahwa ini mungkin dikenakan biaya tergantung pada penggunaan Anda saat ini.
- 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 Wideband DiGIF Data Delivery dan Agen, AWS Ground Station silakan lihat. Satelit siaran publik menggunakan AWS Ground Station Agen (pita lebar) Opsi ini akan terus berkembang saat pembaruan dan fitur perangkat lunak tambahan dirilis.
- Profil misi tambahan - Profil misi untuk satelit siaran publik tambahan (Aqua, SNPP, dan Terra).
- Konfigurasi antena-downlink tambahan - Konfigurasi downlink antena untuk satelit siaran publik tambahan (Aqua, SNPP, dan 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 aplikasi titik akhir aliran data 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. AWS::GroundStation::DataflowEndpointGroup

# Satelit siaran publik menggunakan AWS Ground Station Agen (pita lebar)

Contoh ini dibangun dari analisis yang dilakukan di JPSS-1 - Public broadcast satellite (PBS) - Evaluasi bagian panduan pengguna.

Untuk melengkapi contoh ini, Anda harus mengasumsikan skenario -- Anda ingin menangkap jalur komunikasi HRD sebagai frekuensi menengah digital pita lebar (DiGIF) dan memprosesnya seperti yang diterima oleh Agen AWS Ground Station pada EC2 instance Amazon menggunakan SDR.

> **Note**
>
> Sinyal jalur komunikasi JPSS HRD sebenarnya memiliki bandwidth 30 MHz, tetapi Anda akan mengonfigurasi konfigurasi antena-downlink untuk memperlakukannya sebagai sinyal dengan MHz bandwidth 100 sehingga dapat mengalir melalui jalur yang benar untuk diterima oleh Agen untuk contoh ini. AWS Ground Station

## Jalur komunikasi

Bagian ini Rencanakan jalur komunikasi aliran data Anda mewakili memulai. Untuk contoh ini, Anda akan memerlukan bagian tambahan dalam AWS CloudFormation template Anda yang belum digunakan dalam contoh lain, bagian Pemetaan.

> **Note**
>
> Untuk informasi selengkapnya tentang isi AWS CloudFormation template, lihat bagian Template.

Anda akan mulai dengan menyiapkan bagian Pemetaan di AWS CloudFormation template Anda untuk daftar AWS Ground Station awalan berdasarkan wilayah. Hal ini memungkinkan daftar awalan mudah direferensikan oleh grup keamanan EC2 instans Amazon. Untuk informasi selengkapnya tentang menggunakan daftar awalan, lihatKonfigurasi VPC dengan Agen AWS Ground Station.

```
Mappings:
  PrefixListId:
```

```
    us-east-2:
      groundstation: pl-087f83ba4f34e3bea
    us-west-2:
      groundstation: pl-0cc36273da754ebdc
    us-east-1:
      groundstation: pl-0e5696d987d033653
    eu-central-1:
      groundstation: pl-03743f81267c0a85e
    sa-east-1:
      groundstation: pl-098248765e9effc20
    ap-northeast-2:
      groundstation: pl-059b3e0b02af70e4d
    ap-southeast-1:
      groundstation: pl-0d9b804fe014a6a99
    ap-southeast-2:
      groundstation: pl-08d24302b8c4d2b73
    me-south-1:
      groundstation: pl-02781422c4c792145
    eu-west-1:
      groundstation: pl-03fa6b266557b0d4f
    eu-north-1:
      groundstation: pl-033e44023025215c0
    af-south-1:
      groundstation: pl-0382d923a9d555425
```

Untuk bagian Parameter, Anda akan menambahkan parameter berikut. Anda akan menentukan nilai untuk ini saat membuat tumpukan melalui AWS CloudFormation konsol.

```
Parameters:
  EC2Key:
    Description: The SSH key used to access the EC2 receiver instance. Choose any
 SSH key if you are not creating an EC2 receiver instance. For instructions on how to
 create an SSH key see https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/create-
key-pairs.html
    Type: AWS::EC2::KeyPair::KeyName
    ConstraintDescription: must be the name of an existing EC2 KeyPair.

  AZ:
    Description: "The AvailabilityZone that the resources of this stack will be created
 in. (e.g. us-east-2a)"
    Type: AWS::EC2::AvailabilityZone::Name
```

```
  ReceiverAMI:
    Description: The Ground Station Agent AMI ID you want to use. Please note
 that AMIs are region specific. For instructions on how to retrieve an AMI
 see https://docs.aws.amazon.com/ground-station/latest/ug/dataflows.ec2-
configuration.html#dataflows.ec2-configuration.amis
    Type: AWS::EC2::Image::Id
```

> **Note**
>
> Anda perlu membuat key pair, dan memberikan nama untuk EC2 `EC2Key` parameter Amazon. Lihat Membuat key pair untuk EC2 instans Amazon Anda.
> Selain itu, Anda harus memberikan ID AMI spesifik wilayah yang benar, saat membuat AWS CloudFormation tumpukan. Lihat AWS Ground Station Gambar Mesin Amazon (AMIs).

Cuplikan template yang tersisa termasuk dalam bagian Resources dari template. AWS CloudFormation

```
Resources:
  # Resources that you would like to create should be placed within the Resources
 section.
```

Mengingat skenario kami untuk mengirimkan jalur komunikasi tunggal ke EC2 instans Amazon, Anda tahu bahwa Anda akan memiliki satu jalur pengiriman sinkron. Per Pengiriman data sinkron bagian, Anda harus menyiapkan dan mengonfigurasi EC2 instans Amazon dengan AWS Ground Station Agen, dan membuat satu atau beberapa grup titik akhir aliran data. Anda akan mulai dengan terlebih dahulu menyiapkan VPC Amazon untuk Agen. AWS Ground Station

```
  ReceiverVPC:
    Type: AWS::EC2::VPC
    Properties:
      EnableDnsSupport: 'true'
      EnableDnsHostnames: 'true'
      CidrBlock: 10.0.0.0/16
      Tags:
      - Key: "Name"
        Value: "AWS Ground Station Example - PBS to AWS Ground Station Agent VPC"
```

```
      - Key: "Description"
        Value: "VPC for EC2 instance receiving AWS Ground Station data"

  PublicSubnet:
    Type: AWS::EC2::Subnet
    Properties:
      VpcId: !Ref ReceiverVPC
      MapPublicIpOnLaunch: 'true'
      AvailabilityZone: !Ref AZ
      CidrBlock: 10.0.0.0/20
      Tags:
      - Key: "Name"
        Value: "AWS Ground Station Example - PBS to AWS Ground Station Agent Public
Subnet"
      - Key: "Description"
        Value: "Subnet for EC2 instance receiving AWS Ground Station data"

  RouteTable:
    Type: AWS::EC2::RouteTable
    Properties:
      VpcId: !Ref ReceiverVPC
      Tags:
        - Key: Name
          Value: AWS Ground Station Example - RouteTable

  RouteTableAssociation:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref RouteTable
      SubnetId: !Ref PublicSubnet

  Route:
    Type: AWS::EC2::Route
    DependsOn: InternetGateway
    Properties:
      RouteTableId: !Ref RouteTable
      DestinationCidrBlock: '0.0.0.0/0'
      GatewayId: !Ref InternetGateway

  InternetGateway:
    Type: AWS::EC2::InternetGateway
    Properties:
      Tags:
        - Key: Name
```

```
          Value: AWS Ground Station Example - Internet Gateway

  GatewayAttachment:
    Type: AWS::EC2::VPCGatewayAttachment
    Properties:
      VpcId: !Ref ReceiverVPC
      InternetGatewayId: !Ref InternetGateway
```

> **Note**
>
> Untuk informasi selengkapnya tentang konfigurasi VPC yang didukung oleh AWS Ground Station Agen, lihat Persyaratan AWS Ground Station Agen - diagram VPC.

Selanjutnya, Anda akan mengatur EC2 instance Receiver Amazon.

```
  # The placement group in which your EC2 instance is placed.
  ClusterPlacementGroup:
    Type: AWS::EC2::PlacementGroup
    Properties:
      Strategy: cluster

  # This is required for the EIP if the receiver EC2 instance is in a private subnet.
  # This ENI must exist in a public subnet, be attached to the receiver and be
associated with the EIP.
  ReceiverInstanceNetworkInterface:
    Type: AWS::EC2::NetworkInterface
    Properties:
      Description: Floating network interface
      GroupSet:
        - !Ref InstanceSecurityGroup
      SubnetId: !Ref PublicSubnet

  # An EIP providing a fixed IP address for AWS Ground Station to connect to. Attach it
to the receiver instance created in the stack.
  ReceiverInstanceElasticIp:
    Type: AWS::EC2::EIP
    Properties:
      Tags:
        - Key: Name
          Value: !Join [ "-" , [ "EIP" , !Ref "AWS::StackName" ] ]
```

```
  # Attach the ENI to the EC2 instance if using a separate public subnet.
  # Requires the receiver instance to be in a public subnet (SubnetId should be the id
 of a public subnet)
  ReceiverNetworkInterfaceAttachment:
    Type: AWS::EC2::NetworkInterfaceAttachment
    Properties:
      DeleteOnTermination: false
      DeviceIndex: 1
      InstanceId: !Ref ReceiverInstance
      NetworkInterfaceId: !Ref ReceiverInstanceNetworkInterface

  # Associate EIP with the ENI if using a separate public subnet for the ENI.
  ReceiverNetworkInterfaceElasticIpAssociation:
    Type: AWS::EC2::EIPAssociation
    Properties:
      AllocationId: !GetAtt [ReceiverInstanceElasticIp, AllocationId]
      NetworkInterfaceId: !Ref ReceiverInstanceNetworkInterface

  # The EC2 instance that will send/receive data to/from your satellite using AWS
 Ground Station.
  ReceiverInstance:
    Type: AWS::EC2::Instance
    DependsOn: PublicSubnet
    Properties:
      DisableApiTermination: false
      IamInstanceProfile: !Ref GeneralInstanceProfile
      ImageId: !Ref ReceiverAMI
      AvailabilityZone: !Ref AZ
      InstanceType: c5.24xlarge
      KeyName: !Ref EC2Key
      Monitoring: true
      PlacementGroupName: !Ref ClusterPlacementGroup
      SecurityGroupIds:
        - Ref: InstanceSecurityGroup
      SubnetId: !Ref PublicSubnet
      Tags:
        - Key: Name
          Value: !Join [ "-" , [ "Receiver" , !Ref "AWS::StackName" ] ]
      # agentCpuCores list in the AGENT_CONFIG below defines the cores that the AWS
 Ground Station Agent is allowed to run on. This list can be changed to suit your use-
case, however if the agent isn't supplied with enough cores data loss may occur.
      UserData:
        Fn::Base64:
```

```
          Fn::Sub:
            - |
              #!/bin/bash
              yum -y update

              AGENT_CONFIG_PATH="/opt/aws/groundstation/etc/aws-gs-agent-config.json"
              cat << AGENT_CONFIG > "$AGENT_CONFIG_PATH"
              {
                "capabilities": [
                  "arn:aws:groundstation:${AWS::Region}:${AWS::AccountId}:dataflow-
endpoint-group/${DataflowEndpointGroupId}"
                ],
                "device": {
                  "privateIps": [
                    "127.0.0.1"
                  ],
                  "publicIps": [
                    "${EIP}"
                  ],
                  "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
                  ]
                }
              }
              AGENT_CONFIG

              systemctl start aws-groundstation-agent
              systemctl enable aws-groundstation-agent

              # <Tuning Section Start>
              # Visit the AWS Ground Station Agent Documentation in the User Guide for
 more details and guidance updates

              # Set IRQ affinity with list of CPU cores and Receive Side Scaling mask
              # Core list should be the first two cores (and hyperthreads) on each
 socket
              # Mask set to everything currently
              # https://github.com/torvalds/linux/blob/v4.11/Documentation/networking/
scaling.txt#L80-L96
              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
```

```
            # Reserving the port range defined in the GS agent ingress address in
the Dataflow Endpoint Group so the kernel doesn't steal any of them from the GS agent.
These ports are the ports that the GS agent will ingress data
            # across, so if the kernel steals one it could cause problems ingressing
data onto the instance.
            echo net.ipv4.ip_local_reserved_ports="42000-50000" >> /etc/sysctl.conf

            # </Tuning Section End>

            # We have to reboot for linux kernel settings to apply
            shutdown -r now

          - DataflowEndpointGroupId: !Ref DataflowEndpointGroup
            EIP: !Ref ReceiverInstanceElasticIp
```

```
 # The AWS Ground Station Dataflow Endpoint Group that defines the endpoints that AWS
Ground
 # Station will use to send/receive data to/from your satellite.
 DataflowEndpointGroup:
   Type: AWS::GroundStation::DataflowEndpointGroup
   Properties:
     ContactPostPassDurationSeconds: 180
     ContactPrePassDurationSeconds: 120
     EndpointDetails:
       - AwsGroundStationAgentEndpoint:
           Name: !Join [ "-" , [ !Ref "AWS::StackName" , "Downlink" ] ] # needs to
match DataflowEndpointConfig name
           EgressAddress:
             SocketAddress:
               Name: 127.0.0.1
               Port: 55000
           IngressAddress:
             SocketAddress:
               Name: !Ref ReceiverInstanceElasticIp
               PortRange:
                 Minimum: 42000
                 Maximum: 55000
```

Anda juga memerlukan kebijakan, peran, dan profil yang sesuai AWS Ground Station untuk memungkinkan pembuatan elastic network interface (ENI) di akun Anda.

```
 # The security group for your EC2 instance.
 InstanceSecurityGroup:
   Type: AWS::EC2::SecurityGroup
   Properties:
     GroupDescription: AWS Ground Station receiver instance security group.
     VpcId: !Ref ReceiverVPC
     SecurityGroupEgress:
       - CidrIp: 0.0.0.0/0
         Description: Allow all outbound traffic by default
         IpProtocol: "-1"
     SecurityGroupIngress:
       # To allow SSH access to the instance, add another rule allowing tcp port 22
from your CidrIp
       - IpProtocol: udp
         Description: Allow AWS Ground Station Incoming Dataflows
         ToPort: 50000
         FromPort: 42000
         SourcePrefixListId:
           Fn::FindInMap:
             - PrefixListId
             - Ref: AWS::Region
             - groundstation

  # The EC2 instance assumes this role.
 InstanceRole:
   Type: AWS::IAM::Role
   Properties:
     AssumeRolePolicyDocument:
       Version: "2012-10-17"
       Statement:
         - Effect: "Allow"
           Principal:
             Service:
               - "ec2.amazonaws.com"
           Action:
             - "sts:AssumeRole"
     Path: "/"
     ManagedPolicyArns:
       - arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess
       - arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceforEC2Role
       - arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy
       - arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforSSM
```

```
        - arn:aws:iam::aws:policy/AWSGroundStationAgentInstancePolicy
      Policies:
        - PolicyDocument:
            Statement:
              - Action:
                  - sts:AssumeRole
                Effect: Allow
                Resource: !GetAtt GroundStationKmsKeyRole.Arn
            Version: "2012-10-17"
          PolicyName: InstanceGroundStationApiAccessPolicy

  # The instance profile for your EC2 instance.
  GeneralInstanceProfile:
    Type: AWS::IAM::InstanceProfile
    Properties:
      Roles:
        - !Ref InstanceRole

  # The IAM role that AWS Ground Station will assume to access and use the KMS Key for
 data delivery
  GroundStationKmsKeyRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Statement:
          - Action: sts:AssumeRole
            Effect: Allow
            Principal:
              Service:
                - groundstation.amazonaws.com
            Condition:
              StringEquals:
                "aws:SourceAccount": !Ref AWS::AccountId
              ArnLike:
                "aws:SourceArn": !Sub "arn:${AWS::Partition}:groundstation:
${AWS::Region}:${AWS::AccountId}:mission-profile/*"
          - Action: sts:AssumeRole
            Effect: Allow
            Principal:
              AWS: !Sub "arn:${AWS::Partition}:iam::${AWS::AccountId}:root"

  GroundStationKmsKeyAccessPolicy:
    Type: AWS::IAM::Policy
    Properties:
```

```
      PolicyDocument:
        Statement:
          - Action:
              - kms:Decrypt
            Effect: Allow
            Resource: !GetAtt GroundStationDataDeliveryKmsKey.Arn
      PolicyName: GroundStationKmsKeyAccessPolicy
      Roles:
        - Ref: GroundStationKmsKeyRole

  GroundStationDataDeliveryKmsKey:
    Type: AWS::KMS::Key
    Properties:
      KeyPolicy:
        Statement:
          - Action:
              - kms:CreateAlias
              - kms:Describe*
              - kms:Enable*
              - kms:List*
              - kms:Put*
              - kms:Update*
              - kms:Revoke*
              - kms:Disable*
              - kms:Get*
              - kms:Delete*
              - kms:ScheduleKeyDeletion
              - kms:CancelKeyDeletion
              - kms:GenerateDataKey
              - kms:TagResource
              - kms:UntagResource
            Effect: Allow
            Principal:
              AWS: !Sub "arn:${AWS::Partition}:iam::${AWS::AccountId}:root"
            Resource: "*"
          - Action:
              - kms:Decrypt
              - kms:GenerateDataKeyWithoutPlaintext
            Effect: Allow
            Principal:
              AWS: !GetAtt GroundStationKmsKeyRole.Arn
            Resource: "*"
            Condition:
              StringEquals:
```

```
                "kms:EncryptionContext:sourceAccount": !Ref AWS::AccountId
              ArnLike:
                "kms:EncryptionContext:sourceArn": !Sub "arn:
${AWS::Partition}:groundstation:${AWS::Region}:${AWS::AccountId}:mission-profile/*"
          - Action:
              - kms:CreateGrant
            Effect: Allow
            Principal:
              AWS: !Sub "arn:${AWS::Partition}:iam::${AWS::AccountId}:root"
            Resource: "*"
            Condition:
              ForAllValues:StringEquals:
                "kms:GrantOperations":
                  - Decrypt
                  - GenerateDataKeyWithoutPlaintext
                "kms:EncryptionContextKeys":
                  - sourceArn
                  - sourceAccount
              ArnLike:
                "kms:EncryptionContext:sourceArn": !Sub "arn:
${AWS::Partition}:groundstation:${AWS::Region}:${AWS::AccountId}:mission-profile/*"
              StringEquals:
                "kms:EncryptionContext:sourceAccount": !Ref AWS::AccountId
        Version: "2012-10-17"
      EnableKeyRotation: true
```

## AWS Ground Station konfigurasi

Bagian ini Buat konfigurasi mewakili memulai.

Anda memerlukan konfigurasi pelacakan untuk mengatur preferensi Anda menggunakan autotrack. Memilih PREFERRED sebagai autotrack dapat meningkatkan kualitas sinyal, tetapi tidak diperlukan untuk memenuhi kualitas sinyal karena kualitas ephemeris JPSS-1 yang memadai.

```
  TrackingConfig:
    Type: AWS::GroundStation::Config
    Properties:
      Name: "JPSS Tracking Config"
      ConfigData:
        TrackingConfig:
          Autotrack: "PREFERRED"
```

Berdasarkan jalur komunikasi, Anda harus menentukan konfigurasi antenna-downlink untuk mewakili bagian satelit, serta konfigurasi dataflow-endpoint untuk merujuk ke grup titik akhir aliran data yang mendefinisikan detail titik akhir.

```
 # The AWS Ground Station Antenna Downlink Config that defines the frequency spectrum
used to
 # downlink data from your satellite.
 SnppJpssDownlinkDigIfAntennaConfig:
   Type: AWS::GroundStation::Config
   Properties:
     Name: "SNPP JPSS Downlink WBDigIF Antenna Config"
     ConfigData:
       AntennaDownlinkConfig:
         SpectrumConfig:
           Bandwidth:
             Units: "MHz"
             Value: 100
           CenterFrequency:
             Units: "MHz"
             Value: 7812
           Polarization: "RIGHT_HAND"

 # The AWS Ground Station Dataflow Endpoint Config that defines the endpoint used to
downlink data
 # from your satellite.
 DownlinkDigIfEndpointConfig:
   Type: AWS::GroundStation::Config
   Properties:
     Name: "Aqua SNPP JPSS Terra Downlink DigIF Endpoint Config"
     ConfigData:
       DataflowEndpointConfig:
         DataflowEndpointName: !Join [ "-" , [ !Ref "AWS::StackName" , "Downlink" ] ]
         DataflowEndpointRegion: !Ref AWS::Region
```

## AWS Ground Station profil misi

Bagian ini Buat profil misi mewakili memulai.

Sekarang setelah Anda memiliki konfigurasi terkait, Anda dapat menggunakannya untuk membangun aliran data. Anda akan menggunakan default untuk parameter yang tersisa.

```
 # The AWS Ground Station Mission Profile that groups the above configurations to
define how to
 # uplink and downlink data to your satellite.
 SnppJpssMissionProfile:
   Type: AWS::GroundStation::MissionProfile
   Properties:
     Name: !Sub 'JPSS WBDigIF gs-agent EC2 Delivery'
     ContactPrePassDurationSeconds: 120
     ContactPostPassDurationSeconds: 120
     MinimumViableContactDurationSeconds: 180
     TrackingConfigArn: !Ref TrackingConfig
     DataflowEdges:
       - Source: !Ref SnppJpssDownlinkDigIfAntennaConfig
         Destination: !Ref DownlinkDigIfEndpointConfig
     StreamsKmsKey:
       KmsKeyArn: !GetAtt GroundStationDataDeliveryKmsKey.Arn
     StreamsKmsRole: !GetAtt GroundStationKmsKeyRole.Arn
```

## Menyatukannya

Dengan sumber daya di atas, Anda sekarang memiliki kemampuan untuk menjadwalkan kontak JPSS-1 untuk pengiriman data sinkron dari salah satu onboard Anda. AWS Ground Station AWS Ground Station Lokasi

Berikut ini adalah AWS CloudFormation template lengkap yang mencakup semua sumber daya yang dijelaskan dalam bagian ini digabungkan menjadi satu template yang dapat langsung digunakan AWS CloudFormation.

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 EC2 instans Amazon dan AWS CloudFormation sumber daya yang diperlukan untuk menerima data siaran langsung DiGIF mentah menggunakan AWS Ground Station Agen.

Jika Aqua, SNPP, JPSS-1/NOAA-20, dan Terra tidak masuk ke akun Anda, lihat. Satelit onboard

> **Note**
>
> Anda dapat mengakses template dengan mengakses bucket Amazon S3 orientasi pelanggan menggunakan kredensi yang valid. AWS Tautan di bawah ini menggunakan bucket Amazon S3 regional. Ubah kode `us-west-2` wilayah untuk mewakili wilayah yang sesuai tempat Anda ingin membuat AWS CloudFormation tumpukan.
> Selain itu, petunjuk berikut menggunakan YAMAL. Namun, template tersedia dalam format YAMAL dan JSON. Untuk menggunakan JSON, ganti ekstensi `.yml` file dengan `.json` saat mengunduh templat.

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 tambahan apa yang didefinisikan template?

`DirectBroadcastSatelliteWbDigIfEc2DataDelivery`Template mencakup sumber daya tambahan berikut:

- 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) Pemicu CloudWatch Acara - 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) EC2 Verifikasi Amazon untuk Kontak - Opsi untuk menggunakan Lambda untuk menyiapkan sistem verifikasi EC2 instans Amazon Anda untuk kontak dengan notifikasi SNS. Penting untuk dicatat bahwa ini mungkin dikenakan biaya tergantung pada penggunaan Anda saat ini.
- Profil misi tambahan - Profil misi untuk satelit siaran publik tambahan (Aqua, SNPP, dan Terra).
- Konfigurasi antena-downlink tambahan - Konfigurasi downlink antena untuk satelit siaran publik tambahan (Aqua, SNPP, dan Terra).

Nilai dan parameter untuk satelit dalam template ini sudah terisi. Parameter ini memudahkan Anda untuk AWS Ground Station segera menggunakan 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. AWS::GroundStation::DataflowEndpointGroup Untuk informasi lebih lanjut tentang AWS Ground Station Agen, lihat Apa itu AWS Ground Station Agen?

# Pemecahan Masalah

Dokumentasi berikut dapat membantu Anda memecahkan masalah yang mungkin terjadi saat menggunakan. AWS Ground Station

Topik



## Memecahkan masalah kontak yang mengirimkan data ke Amazon EC2

Jika Anda tidak berhasil menyelesaikan AWS Ground Station kontak, Anda harus memverifikasi bahwa EC2 instans Amazon Anda berjalan, memverifikasi bahwa aplikasi titik akhir aliran data Anda berjalan, dan memverifikasi bahwa aliran aplikasi titik akhir aliran data Anda dikonfigurasi dengan benar.

> **Note**
>
> DataDefender (DDX) adalah contoh aplikasi endpoint aliran data yang saat ini didukung oleh AWS Ground Station

Prasyarat

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

### Langkah 1: Verifikasi bahwa EC2 instans Anda sedang berjalan

Prosedur berikut menunjukkan cara menemukan EC2 instans Amazon Anda di konsol dan memulainya jika tidak berjalan.

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

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

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

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

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

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

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

## Langkah 2: Tentukan jenis aplikasi aliran data 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 DataDefender (DDX) terusthe section called “Langkah 3: Verifikasi bahwa aplikasi aliran data sedang berjalan”.

## Langkah 3: Verifikasi bahwa aplikasi aliran data sedang berjalan

Memverifikasi status DataDefender mengharuskan Anda untuk terhubung ke instans Anda 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 command prompt dan sambungkan ke EC2 instans Amazon Anda dengan menggunakan SSH. Teruskan port 80 dari host jarak jauh untuk melihat UI DataDefender web. Perintah berikut menunjukkan cara menggunakan SSH untuk terhubung ke EC2 instans Amazon melalui benteng dengan port forwarding diaktifkan.

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

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 DataDefender (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 DataDefender sedang berjalan, lewati ke the section called “Langkah 4: Verifikasi bahwa aliran aplikasi aliran data Anda dikonfigurasi” Jika tidak, lanjutkan ke langkah berikutnya.

3. Mulai DataDefender gunakan perintah tampilkan di bawah ini.

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

Jika DataDefender berjalan setelah menggunakan perintah, lompat ke the section called “Langkah 4: Verifikasi bahwa aliran aplikasi aliran 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 DataDefender.

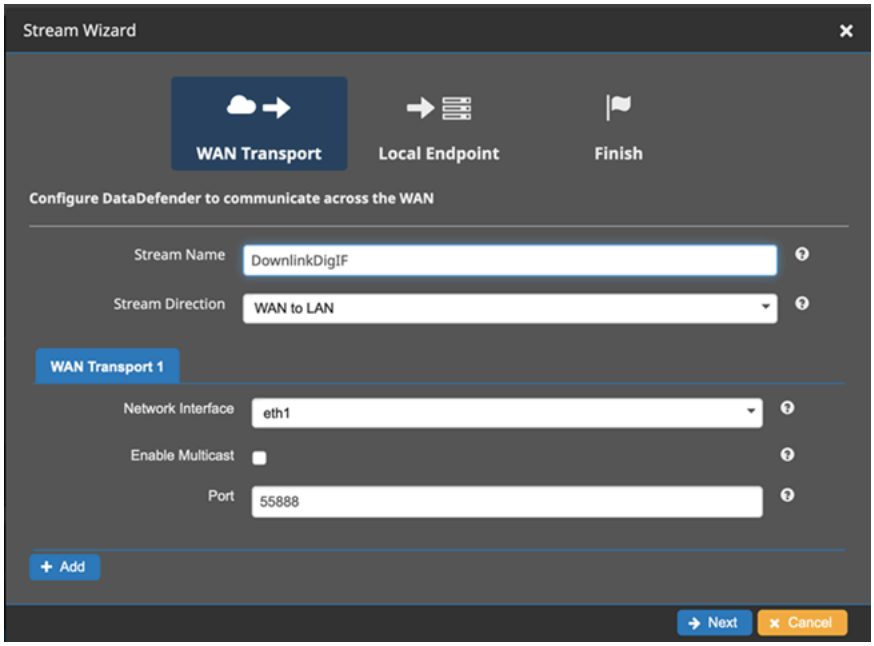
```
cat /var/log/user-data.log
          cat /opt/aws/groundstation/.startup.out
```

> **Note**
>
> Masalah umum yang ditemukan saat memeriksa file-file ini adalah bahwa VPC Amazon tempat instans EC2 Amazon 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 EC2 instans Anda untuk memastikan mereka tidak memblokir akses ke Amazon S3.

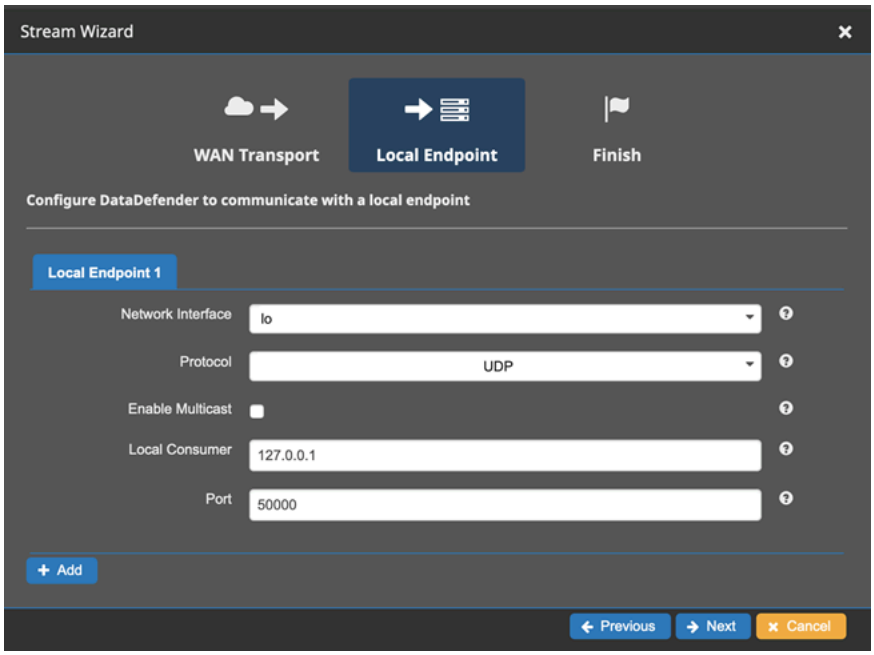
Jika DataDefender berjalan setelah memeriksa pengaturan VPC Amazon Anda, lanjutkan ke. the section called “Langkah 4: Verifikasi bahwa aliran aplikasi aliran data Anda dikonfigurasi” Jika masalah berlanjut, hubungi AWS Support dan kirim file log Anda dengan deskripsi masalah Anda.

## Langkah 4: Verifikasi bahwa aliran aplikasi aliran data Anda dikonfigurasi

1. Di browser web, akses antarmuka pengguna DataDefender web 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 DataDefender setelah 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 EC2 instans Amazon Anda dan DataDefender keduanya berjalan dan dikonfigurasi dengan benar untuk menerima data dari AWS Ground Station. Lanjutkan ke the section called “Langkah 5: Pastikan Anda memiliki cukup alamat IP yang tersedia di subnet instance penerima Anda”.

## Langkah 5: Pastikan Anda memiliki cukup alamat IP yang tersedia di subnet instance penerima Anda

Prosedur berikut menunjukkan cara menemukan jumlah alamat IP yang tersedia di instance EC2 penerima Amazon di konsol.

1. Untuk setiap instance EC2 penerima Amazon yang digunakan untuk kontak yang sedang Anda atasi masalah. Gunakan langkah-langkah berikut:

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

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

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

2. Di konsol EC2 manajemen Amazon, temukan dan klik tautan Subnet ID di Ringkasan Instance instans EC2 penerima Amazon Anda. Ini akan membawa Anda ke konsol manajemen VPC Amazon yang sesuai.

3. Pilih subnet yang cocok di konsol manajemen VPC Amazon dan periksa Detail subnet Anda untuk alamat yang tersedia. IPv4  Jika nomor ini setidaknya tidak sebanyak titik akhir aliran data yang menggunakan instance EC2 penerima Amazon ini, lakukan hal berikut:

   a. Perbarui subnet sesuai AWS CloudFormation template Anda CidrBlockagar berukuran benar. Untuk detail lebih lanjut tentang ukuran subnet lihat, subnet CIDR memblokir.

   b. Tempatkan kembali tumpukan Anda dengan template yang diperbarui AWS CloudFormation .

Jika Anda terus mengalami masalah, hubungi AWS Support.

# Memecahkan masalah kontak GAGAL

Kontak akan memiliki status kontak terminal FAILED saat AWS Ground Station mendeteksi masalah dengan konfigurasi sumber daya Anda. 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,, atau AWS_FAILEDAWS_CANCELLEDFAILED_TO_SCHEDULE. Untuk informasi selengkapnya tentang status kontak, lihat the section called “AWS Ground Station status kontak”

## Kasus penggunaan titik akhir aliran data GAGAL

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

- Titik akhir Dataflow tidak pernah terhubung - Koneksi antara AWS Ground Station Antena dan Grup Titik Akhir Dataflow Anda untuk satu atau lebih aliran data tidak pernah dibuat.
- Titik akhir Dataflow terhubung terlambat - Koneksi antara AWS Ground Station Antena dan Grup Titik Akhir Dataflow Anda untuk satu atau lebih aliran data dibuat setelah waktu mulai kontak.
- Subnet endpoint Dataflow kehabisan alamat IP yang tersedia - AWS Ground Station solusi pengiriman data tidak dapat membuat ENI di jaringan pribadi Anda karena tidak memiliki alamat IP yang tersedia di subnet instance penerima.

Untuk kasus kegagalan titik akhir aliran data apa pun, disarankan untuk melihat hal-hal berikut:

- Konfirmasikan EC2 instans Amazon penerima berhasil dimulai, sebelum waktu mulai kontak.
- Konfirmasikan perangkat lunak titik akhir aliran data aktif dan berjalan selama kontak.
- Pastikan Anda memiliki setidaknya satu alamat IP yang tersedia per titik akhir aliran data per subnet instance penerima.

Lihat bagian Memecahkan masalah kontak yang mengirimkan data ke Amazon EC2 untuk langkah-langkah pemecahan masalah yang lebih spesifik.

## AWS Ground Station Kasus penggunaan agen GAGAL

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

- AWS Ground Station Status Agen Tidak Pernah Dilaporkan - Agen yang bertanggung jawab untuk mengatur pengiriman data di Grup Titik Akhir Dataflow Anda untuk satu atau lebih aliran data yang tidak pernah berhasil melaporkan statusnya. AWS Ground Station Pembaruan status ini akan terjadi dalam beberapa detik dari waktu akhir kontak.
- AWS Ground Station Agen Mulai Terlambat - Agen yang bertanggung jawab untuk mengatur pengiriman data di Grup Titik Akhir Dataflow Anda 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 EC2 instans Amazon penerima berhasil dimulai, sebelum waktu mulai kontak.
- Konfirmasikan aplikasi Agen sudah aktif dan berjalan di awal dan selama kontak.
- Konfirmasikan aplikasi Agen dan EC2 instans Amazon tidak dimatikan dalam waktu 15 detik setelah kontak berakhir. Ini memberi Agen waktu yang cukup untuk melaporkan status ke AWS Ground Station.

Lihat bagian Memecahkan masalah kontak yang mengirimkan data ke Amazon EC2 untuk langkah-langkah pemecahan masalah yang lebih spesifik.

# Memecahkan masalah kontak FAILED_TO_SCHEDULE

Kontak akan berakhir dalam status FAILED_TO_SCHEDULE saat AWS Ground Station mendeteksi masalah baik dengan konfigurasi sumber daya Anda 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, lihat DescribeContactAPI.

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,, atau GAGAL. AWS_FAILEDAWS_CANCELLED Untuk informasi selengkapnya tentang status kontak, lihat the section called “AWS Ground Station status kontak”

## 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. Untuk informasi tentang cara memesan kontak, lihat ReserveContact.
- Jika Anda terus menerima status FAILED_TO_SCHEDULE untuk profil misi ini, hubungi AWS Support

# Memecahkan masalah DataflowEndpointGroups tidak dalam keadaan SEHAT

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 EC2 contoh Anda, yang akan mendaftarkan agen. Perhatikan bahwa Anda harus memiliki file konfigurasi pengontrol yang valid agar panggilan ini berhasil. Lihat Gunakan AWS Ground Station 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 instance. 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 Gunakan peran terkait layanan untuk Ground Station

# Memecahkan masalah ephemerides yang tidak valid

Ketika ephemeris khusus diunggah ke AWS Ground Station dalamnya 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 potensial dari EphemerisInvalidReasonadalah sebagai berikut:

| Nilai | Deskripsi | Tindakan Pemecahan Masalah |
|---|---|---|
| METADATA_TIDAK VALID | Pengidentifikasi pesawat ruang angkasa yang disediakan seperti ID satelit tidak valid | Periksa ID NORAD atau pengidentifikasi lain yang disediakan dalam data ephemeris |

| Nilai | Deskripsi | Tindakan Pemecahan Masalah |
| --- | --- | --- |
| TIME_RANGE_TIDAK VALID | 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 | Ephemeris yang disediaka n mendefinisikan lintasan pesawat ruang angkasa yang tidak valid | Konfirmasikan bahwa lintasan yang disediakan kontinu dan untuk satelit yang benar. |
| VALIDATION_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"
      }
    }
```

```
  },
}
```

> **Note**
>
> Jika status ephemeris adalah`ERROR`, ephemeris bukan `ENABLED` karena masalah dengan layanan. AWS Ground Station Anda harus mencoba memberikan ephemeris lagi melalui. `CreateEphemeris` Ephemeris baru bisa menjadi `ENABLED` jika masalahnya sementara.

> **Note**
>
> AWS Ground Station memperlakukan ephemerides sebagai Data Penggunaan Individual. Jika Anda menggunakan fitur opsional ini, AWS akan menggunakan data ephemeris Anda untuk memberikan dukungan pemecahan masalah.

# Memecahkan masalah kontak yang tidak menerima data

Mungkin saja kontak tampak berhasil, tetapi masih tidak menerima data apa pun. Ini mungkin berarti bahwa Anda menerima file PCAP yang kosong, atau tidak ada file PCAP sama sekali jika Anda menggunakan pengiriman data S3. Ini bisa terjadi karena sejumlah alasan. Berikut ini membahas beberapa penyebab, dan bagaimana mengatasinya.

## Konfigurasi downlink salah

Setiap kontak yang menerima data dari satelit akan memiliki kontak terkait Konfigurasi Downlink Antena atauAntena Downlink Demod Decode Config . Jika konfigurasi yang ditentukan tidak sesuai dengan sinyal yang ditransmisikan oleh satelit, tidak AWS Ground Station akan dapat menerima sinyal yang ditransmisikan. Ini akan mengakibatkan tidak ada data yang diterima oleh AWS Ground Station.

Untuk memperbaikinya, harap verifikasi bahwa konfigurasi yang Anda gunakan setuju dengan sinyal yang dikirimkan oleh satelit Anda. Misalnya, verifikasi bahwa Anda telah menetapkan frekuensi pusat, bandwidth, polarisasi, dan jika diperlukan, parameter demodulasi dan decoding yang benar.

## Manuver satelit

Ada kalanya satelit dapat melakukan manuver yang untuk sementara menonaktifkan beberapa sistem komunikasinya. Manuver juga dapat secara signifikan mengubah lokasi satelit di langit. AWS Ground Station tidak akan dapat menerima sinyal dari satelit yang tidak mentransmisikan sinyal, atau jika ephemeris yang digunakan menyebabkan AWS Ground Station antena menunjuk ke lokasi di langit di mana satelit tidak ada.

Jika Anda mencoba berkomunikasi dengan satelit siaran publik yang dioperasikan oleh NOAA, Anda mungkin dapat menemukan pesan yang menjelaskan pemadaman atau manuver di halaman Pesan Peringatan Satelit NOAA. Pesan dapat mencakup garis waktu kapan transmisi data diharapkan untuk dilanjutkan, atau ini dapat diposting dalam pesan berikutnya.

Jika Anda berkomunikasi dengan satelit Anda sendiri, Anda bertanggung jawab untuk memahami operasi satelit Anda, dan bagaimana hal ini dapat berdampak pada komunikasi. AWS Ground Station Jika Anda melakukan manuver yang akan memengaruhi lintasan satelit, ini mungkin termasuk menyediakan data ephemeris khusus yang diperbarui. Untuk informasi selengkapnya tentang penyediaan data ephemeris khusus, lihat. Berikan data ephemeris khusus

## AWS Ground Station pemadaman

Jika AWS Ground Station menyebabkan kontak gagal, atau membatalkannya, AWS Ground Station akan mengatur status kontak ke AWS_FAILED, atau AWS_CANCELLED. Untuk informasi selengkapnya tentang siklus hidup kontak, lihat. Memahami siklus hidup kontak Dalam beberapa kasus, AWS Ground Station mungkin mengalami kegagalan yang mencegah data dikirim ke akun Anda, tetapi tidak mengakibatkan kontak berada dalam AWS_CANCELLEDstatus AWS_FAILEDatau. Ketika ini terjadi, AWS Ground Station sebaiknya posting acara khusus akun ke dasbor AWS Kesehatan Anda. Untuk informasi selengkapnya tentang dasbor AWS Kesehatan, lihat Panduan Pengguna AWS Kesehatan.

# Kuota dan batas

Anda dapat melihat wilayah yang didukung, titik akhir terkait, dan kuota di AWS Ground Station titik akhir dan kuota.

Anda dapat menggunakan konsol Kuota Layanan, AWS API, dan AWS CLI untuk meminta peningkatan kuota, bila diperlukan.

# Ketentuan layanan

Untuk persyaratan AWS Ground Station layanan, silakan merujuk ke Ketentuan Layanan AWS.

# Riwayat Dokumen untuk Panduan AWS Ground Station Pengguna

Tabel berikut menjelaskan perubahan penting dalam setiap rilis Panduan AWS Ground Station Pengguna.

| Perubahan | Deskripsi | Tanggal |
| --- | --- | --- |
| Pembaruan Dokumentasi | Menambahkan klarifikasi tentang pemanfaatan kontak sumber daya yang dikonfigu rasi. | April 4, 2025 |
| Fitur Baru | Memperbarui panduan pengguna untuk menyertakan kembar AWS Ground Station digital. | Agustus 6, 2024 |
| Pembaruan Dokumentasi | Memperbarui banyak bagian dari panduan pengguna, termasuk diagram baru, contoh, dan banyak lagi. | Juli 18, 2024 |
| Pembaruan Dokumentasi | Menambahkan umpan RSS ke Panduan Pengguna. | Juli 18, 2024 |
| Pembaruan Dokumentasi | Pisahkan Panduan Pengguna AWS Ground Station Agen menjadi Panduan Pengguna terpisah. | Juli 18, 2024 |
| Fitur Baru | Kontak sekarang dapat dijadwalkan hingga 30 detik di luar rentang waktu visibilit as. Waktu visibilitas termasuk dalam DescribeContact tanggapan. | Maret 26, 2024 |

| | | |
|---|---|---|
| Pembaruan Dokumentasi | Organisasi yang ditingkatkan dan menambahkan bagian "Pemilihan EC2 Instans dan Perencanaan CPU”. | Maret 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. | Februari 21, 2024 |
| Pembaruan Template | Ditambahkan dukungan untuk subnet publik terpisah dalam DataDelivery template DirectBroadcastSatelliteWbDigIfEc 2. | Februari 14, 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 |
| Fitur Baru | Menambahkan Panduan Pengguna AWS Ground Station Agen untuk rilis Pengiriman Data DiGIF Wideband | 12 April 2023 |

| | | |
|---|---|---|
| Kebijakan AWS terkelola baru | AWS Ground Station menambahkan kebijakan baru bernama AWSGround StationAgentInstancePolicy. | 12 April 2023 |
| Fitur Baru | Memperbarui panduan pengguna untuk rilis Pratinjau CPE. | 9 November 2022 |
| Kebijakan AWS terkelola baru | AWS Ground Station menambahkan AWSServic e RoleForGroundStati onDataflowEndpointGroup service-linked-role (SLR) yang menyertakan kebijakan baru bernama AWSServic eRoleForGroundStationDataf lowEndpointGroupPolicy. | 2 November 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 |
| 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 |

# AWS Glosarium

Untuk AWS terminologi terbaru, lihat AWS glosarium di Referensi.Glosarium AWS

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