aws

Guia do usuário

# AWS Ground Station

# AWS Ground Station: Guia do usuário

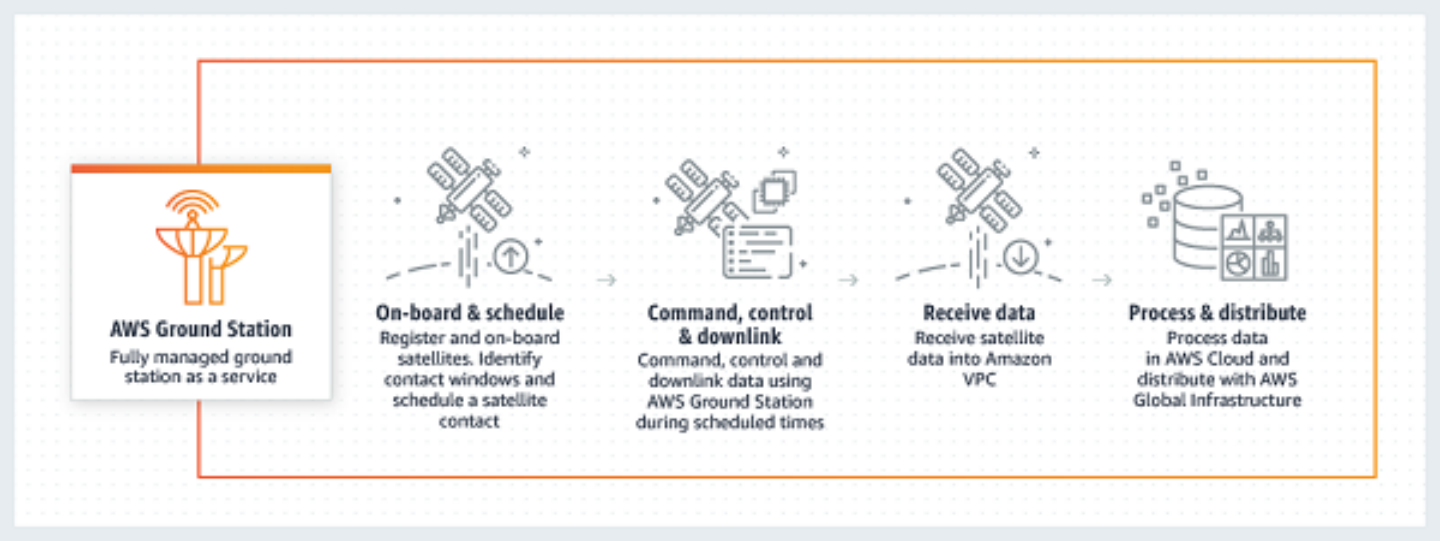
# Table of Contents

# O que AWS Ground Stationé

AWS Ground Station é um serviço totalmente gerenciado que fornece comunicações via satélite seguras, rápidas e previsíveis em uma infraestrutura global. Com AWS Ground Station, você não precisa mais criar, gerenciar ou escalar sua própria infraestrutura de estação terrestre. AWS Ground Station permite que você se concentre em inovar e experimentar rapidamente novos aplicativos que ingerem dados de satélite, em vez de gastar recursos na construção, operação e escalabilidade de suas próprias estações terrestres.

Usando a rede de fibra global de baixa latência e alta largura de banda da AWS, você pode começar a processar seus dados de satélite em segundos após a recepção no sistema de antena. Isso permite que você transforme dados brutos em informações processadas ou conhecimento analisado em questão de segundos.

## Casos de uso comuns




AWS Ground Station permite que você se comunique com seus satélites bidirecionalmente e oferece suporte aos seguintes casos de uso:

- Dados de downlink — Receba dados de seus satélites, transmitindo frequências de banda X e banda S, entregues a uma EC2 instância da Amazon em tempo real (formato VITA-49) ou diretamente para um bucket Amazon S3 em sua conta (formato PCAP). Além disso, para satélites que usam um esquema de modulação e codificação compatível, você pode escolher entre receber

dados desmodulados e decodificados ou amostras de frequência intermediária digital bruta (DigIF) (formato VITA-49).

- Dados de uplink — Envie dados e comandos para seus satélites, que recebem frequências de banda S, enviando dados DigIF (formato VITA-49) para serem transmitidos por. AWS Ground Station
- Eco de uplink — Valide os comandos enviados para sua espaçonave e execute outras tarefas avançadas recebendo o sinal transmitido em uma antena fisicamente localizada.
- Rádio definido por software (SDR) /processador front-end (FEP) — Use seu SDR existente, suas formas de onda existentes e gere and/or FEP, that's capable of running on an Amazon EC2 instance, to process your data in real-time to send/receive seus produtos de dados.
- Telemetria, Rastreamento e Comando (TT&C) — Execute TT&C usando uma combinação dos casos de uso listados anteriormente para gerenciar sua frota de satélites.
- Entrega de dados entre regiões — opere vários contatos simultâneos usando AWS Ground Station a rede global de antenas de uma única região da AWS.
- Digital twin — agendamento de testes, verificação de configurações e tratamento adequado de erros a um custo reduzido sem usar a capacidade da antena de produção.

## Próximas etapas

Recomendamos que você comece lendo as seguintes seções:

- Para aprender AWS Ground Station conceitos essenciais, consulteComo AWS Ground Station funciona.
- Para saber como configurar sua conta e seus recursos para uso AWS Ground Station, consulteConceitos básicos.
- Para usar programaticamente AWS Ground Station, consulte a Referência da AWS Ground Station API. A Referência da API descreve detalhadamente todas as operações AWS Ground Station da API. Ele também fornece exemplos de solicitações, respostas e erros para os protocolos de serviços da web compatíveis. Você pode usar a AWS CLI, ou um AWS SDK, na linguagem de sua escolha, para escrever código que interaja com. AWS Ground Station

# Como AWS Ground Station funciona

AWS Ground Station opera antenas terrestres para facilitar a comunicação com seu satélite. As características físicas do que as antenas podem fazer são resumidas e chamadas de capacidades. A localização física da antena, juntamente com seus recursos atuais, podem ser referenciados na AWS Ground Station Localizações seção. Entre em contato conosco pelo `<e-mail aws-groundstation@amazon.com>` se seu caso de uso exigir recursos adicionais, ofertas de localização adicionais ou localizações de antenas mais precisas.

Para usar uma das AWS Ground Station antenas, você deve reservar um horário em um local específico. Essa reserva é chamada de contato. Para agendar um contato com sucesso, são AWS Ground Station necessários dados adicionais para garantir seu sucesso.

- Seu satélite deve estar integrado a um ou mais locais — Isso garante que você tenha aprovação para operar os vários recursos no local solicitado.
- Seu satélite deve ter uma efeméride válida — Isso garante que as antenas tenham uma linha de visão e possam apontar com precisão para o satélite durante o contato.
- Você deve ter um perfil de missão válido — Isso permite que você personalize como esse contato se comportará, incluindo como você receberá e enviará dados para o seu satélite. Você pode utilizar vários perfis de missão para o mesmo veículo para criar contatos diferentes para se adequar a diferentes posturas operacionais ou cenários que você encontrar.

## Integração via satélite

A integração de um satélite AWS Ground Station é um processo de várias etapas que envolve coleta de dados, validação técnica, licenciamento de espectro, integração e testes. A seção de integração de satélites do guia guiará você nesse processo.

## Composição do perfil da missão

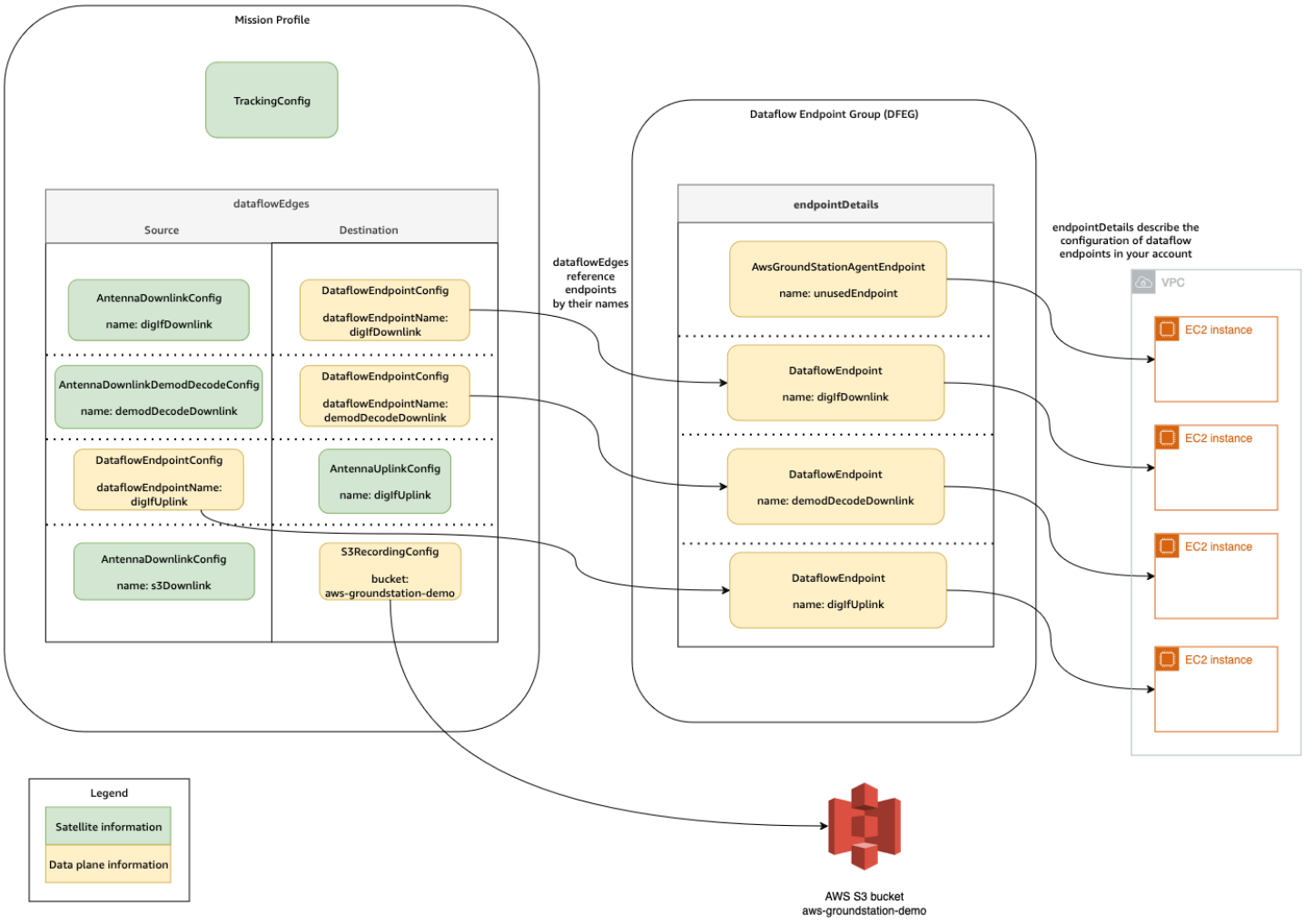
As informações de frequência do satélite, informações do plano de dados e outros detalhes são encapsulados em um perfil de missão. O perfil da missão é uma coleção de componentes de configuração. Isso permite que você reutilize componentes de configuração em diferentes perfis de missão, de acordo com seu caso de uso. Como os perfis de missão não fazem referência direta a satélites individuais, mas têm apenas informações sobre suas capacidades técnicas, os perfis de missão também podem ser reutilizados por vários satélites com a mesma configuração.

Um perfil de missão válido terá uma configuração de rastreamento e um ou mais fluxos de dados. A configuração de rastreamento especificará sua preferência de rastreamento durante um contato. Cada par de configurações em um fluxo de dados estabelece uma origem e um destino. Dependendo do seu satélite e de seus modos operacionais, o número exato de fluxos de dados variará em um perfil de missão para representar seus caminhos de comunicação de uplink e downlink, bem como quaisquer aspectos do processamento de dados.

- Para obter mais informações sobre como configurar seus recursos da Amazon VPC, Amazon S3 e EC2 Amazon que serão usados durante um contato, consulte. Trabalhe com fluxos de dados
- Para obter detalhes sobre como cada configuração se comporta, consulte. Use AWS Ground Station configurações
- Para obter detalhes específicos sobre todos os parâmetros esperados, consulteUse perfis de AWS Ground Station missão.
- Para obter exemplos de como vários perfis de missão podem ser criados para apoiar seu caso de uso, consulteExemplo de configurações de perfil de missão.

O diagrama a seguir mostra um exemplo de perfil de missão e os recursos adicionais necessários. Observe que o exemplo mostra um endpoint de fluxo de dados que não é necessário para esse perfil de missão, chamado UnusedEndpoint, para demonstrar a flexibilidade. O exemplo é compatível com os seguintes fluxos de dados:

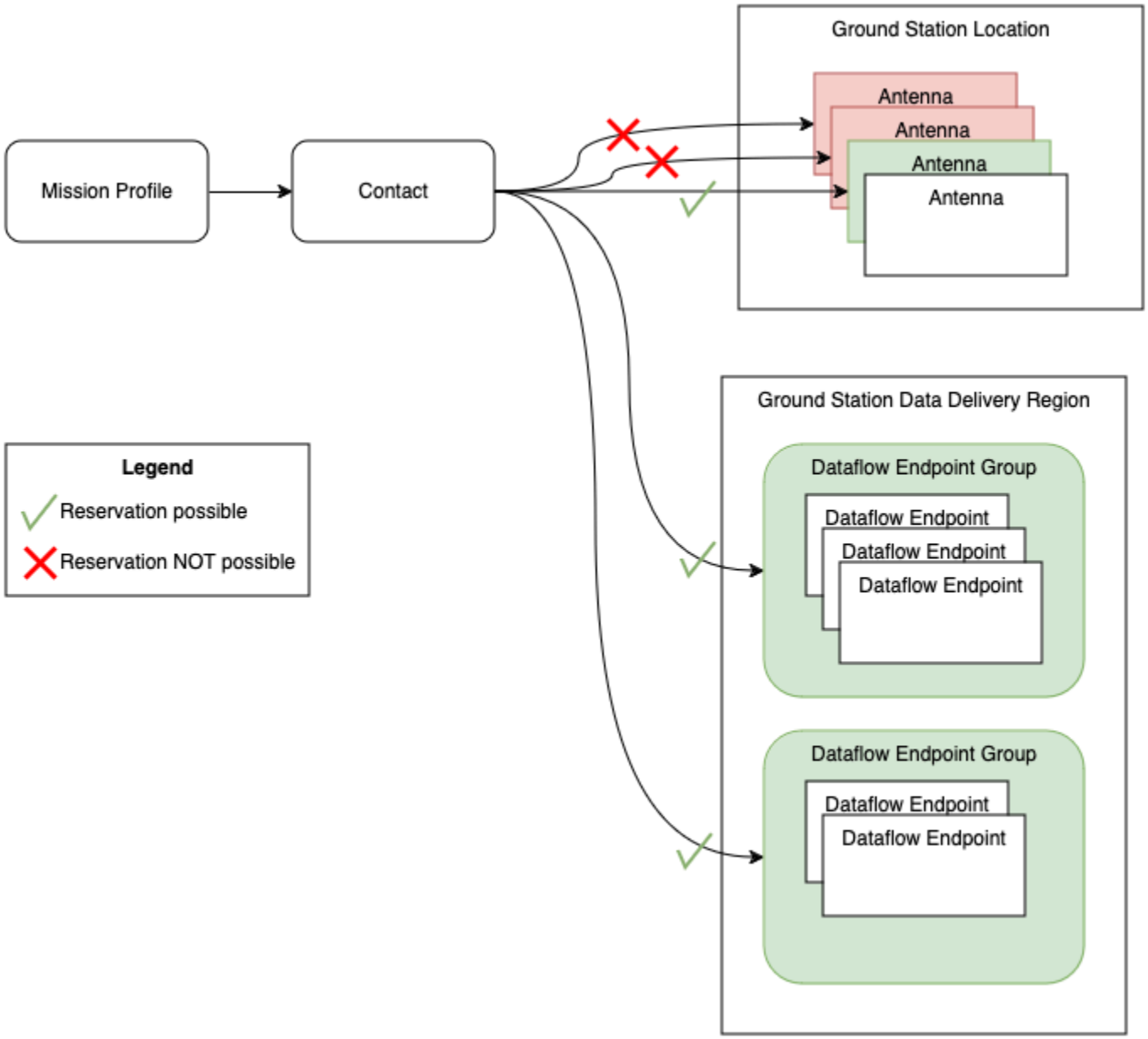
- Downlink síncrono de dados digitais de frequência intermediária para uma EC2 instância da Amazon que você gerencia. Denotado pelo nome. digIfDownlink
- Downlink assíncrono de dados digitais de frequência intermediária para um bucket Amazon S3. Indicado pelo nome do bucket. aws-groundstation-demo
- Downlink síncrono de dados desmodulados e decodificados para uma instância da Amazon EC2 que você gerencia. Denotado pelo nome. demodDecodeDownlink
- Uplink síncrono de dados de uma EC2 instância da Amazon que você gerencia para uma AWS Ground Station antena gerenciada. Denotado pelo nome. digIfUplink




# Agendamento de contatos

Com um perfil de missão válido, você pode solicitar um contato com seus satélites a bordo. A solicitação de reserva de contato é assíncrona para permitir que o serviço global de antenas alcance uma programação consistente em todas as regiões envolvidas. AWS Durante esse processo, várias antenas no local da estação terrestre solicitada são avaliadas para determinar se estão disponíveis e são capazes de processar o contato. Durante esse processo, seus endpoints de fluxo de dados configurados também são avaliados para determinar sua disponibilidade. Enquanto essa avaliação estiver ocorrendo, o status do contato estará em AGENDAMENTO.

Esse processo de agendamento assíncrono será concluído em até cinco minutos após a solicitação, mas normalmente termina em um minuto. Verifique o monitoramento baseado em eventos Automatize AWS Ground Station com eventos durante o horário de agendamento.




Contatos que podem ser realizados e têm disponibilidade resultam em contatos AGENDADOS. Com um contato agendado, os recursos necessários para realizar seu contato foram reservados nas regiões da AWS necessárias, conforme definido pelo seu perfil de missão. Contatos que não podem ser executados ou têm partes indisponíveis resultarão em contatos FAILED_TO_SCHEDULE. Consulte Solucionar problemas de contatos FAILED_TO_SCHEDULE para obter detalhes sobre a depuração.

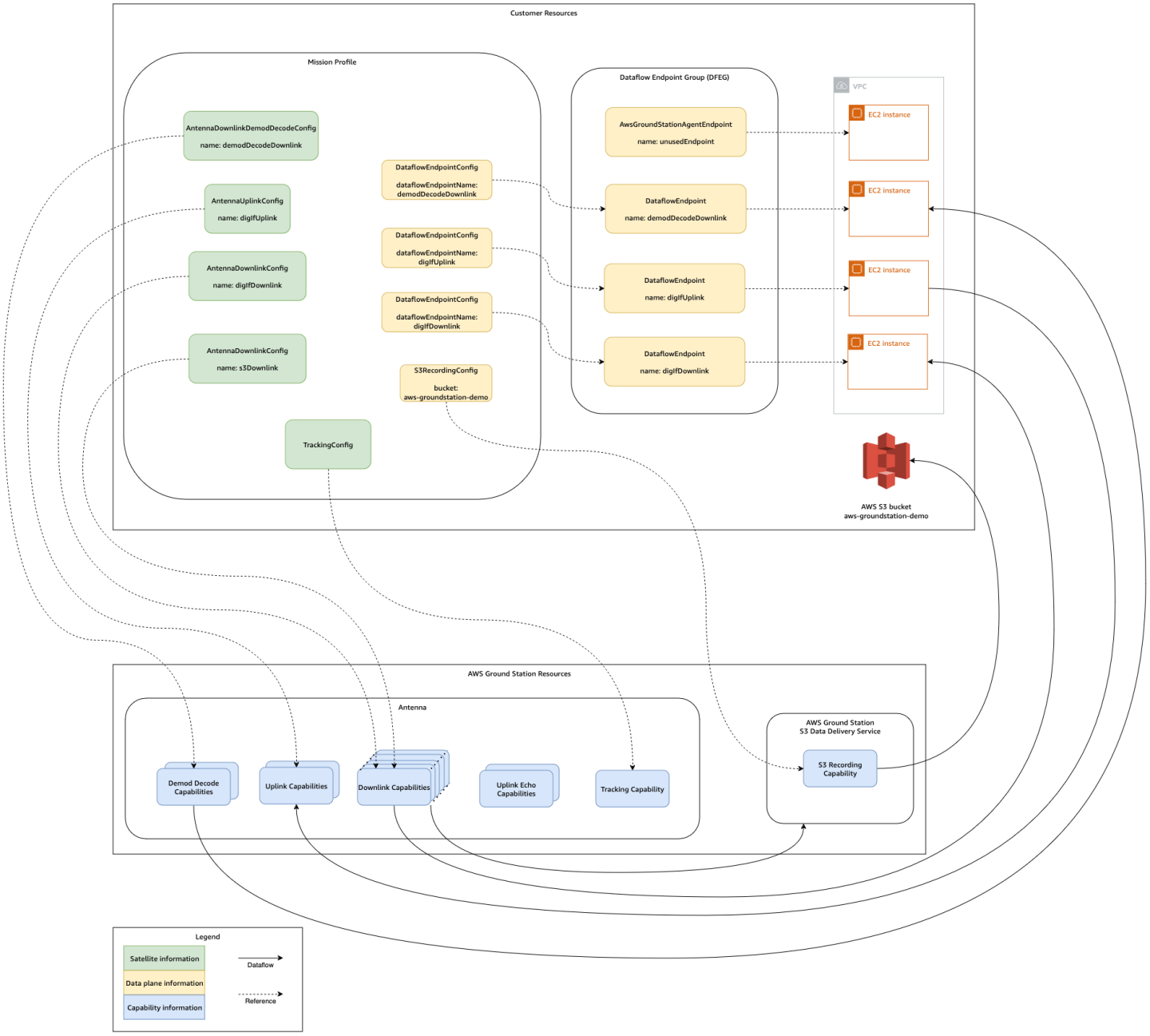
# Execução de contatos

AWS Ground Station orquestrará automaticamente seus recursos gerenciados pela AWS durante sua reserva de contato. Se aplicável, você é responsável por orquestrar EC2 os recursos definidos pelo seu perfil de missão como endpoints de fluxo de dados. AWS Ground Station fornece EventBridge eventos da AWS para automatizar a orquestração de seus recursos a fim de reduzir custos. Consulte Automatize AWS Ground Station com eventos para obter mais detalhes.

Durante o contato, a telemetria sobre o desempenho do seu contato é entregue à AWS. CloudWatch Para obter informações sobre como monitorar seu contato durante a execução, consulteEntenda o monitoramento com AWS Ground Station.

O diagrama a seguir dá continuidade ao exemplo anterior mostrando os mesmos recursos orquestrados durante o contato.

> **Note**
>
> Nem todos os recursos da antena foram usados neste exemplo. Por exemplo, há mais de uma dúzia de recursos de downlink de antena disponíveis em cada antena que suportam várias frequências e polarizações. Para obter mais detalhes sobre o número de cada tipo de capacidade disponível nas AWS Ground Station antenas e suas frequências e polarizações suportadas, consulte. AWS Ground Station Capacidades do site




Ao final do seu contato, AWS Ground Station avaliará o desempenho do seu contato e determinará o status final do contato. Contatos em que nenhum erro for detectado resultarão em um status de contato CONCLUÍDO. Os contatos em que erros de serviço causaram problemas na entrega de dados durante o contato resultarão em um AWS_FAILEDstatus. Os contatos em que erros do cliente ou do usuário causaram problemas na entrega de dados durante o contato resultarão em um status de FALHA. Erros fora de um horário de contato, ou seja, durante a pré-aprovação ou pós-aprovação, não são levados em consideração durante a adjudicação.

Consulte Entenda o ciclo de vida do contato para obter mais informações.

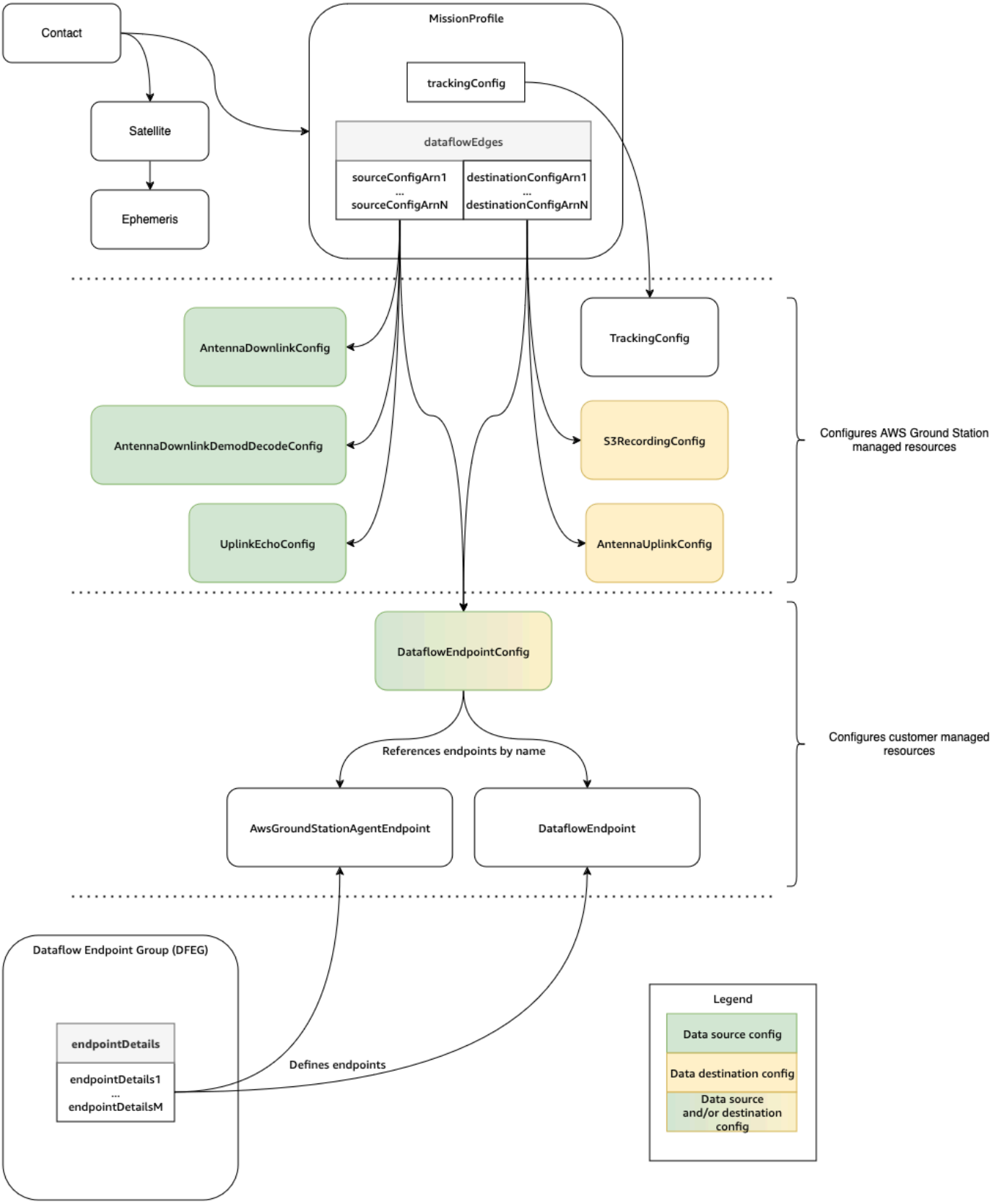
# Gêmeo digital

O recurso de gêmeos digitais AWS Ground Station permite que você agende contatos em relação a localizações virtuais de estações terrestres. Essas estações terrestres virtuais são réplicas exatas das estações terrestres de produção, incluindo recursos de antena, máscaras de local e coordenadas GPS reais. O recurso digital twin permite que você teste seu fluxo de trabalho de orquestração de contatos por uma fração do custo em comparação com as estações terrestres de produção. Consulte Use o recurso de gêmeos AWS Ground Station digitais para obter mais informações.

# Entenda os componentes AWS Ground Station principais

Esta seção fornece definições detalhadas dos principais componentes do AWS Ground Station.

O diagrama a seguir mostra os principais componentes AWS Ground Station e como eles se relacionam entre si. As setas indicam a direção das dependências entre os componentes, onde cada componente aponta para suas dependências.


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

Os tópicos a seguir descrevem detalhadamente os componentes AWS Ground Station principais.

Tópicos



## Use perfis de AWS Ground Station missão

Os perfis de missão contêm configurações e parâmetros de como os contatos são executados. Ao reservar um contato ou pesquisar contatos disponíveis, você fornece o perfil de missão que pretende usar. Os perfis de missão reúnem todas as suas configurações e definem para onde os dados serão direcionados durante o contato.

Os perfis de missão podem ser compartilhados entre satélites que compartilham as mesmas características de rádio. Você pode criar grupos adicionais de endpoints de fluxo de dados para limitar o máximo de contatos simultâneos que você deseja realizar para sua constelação.

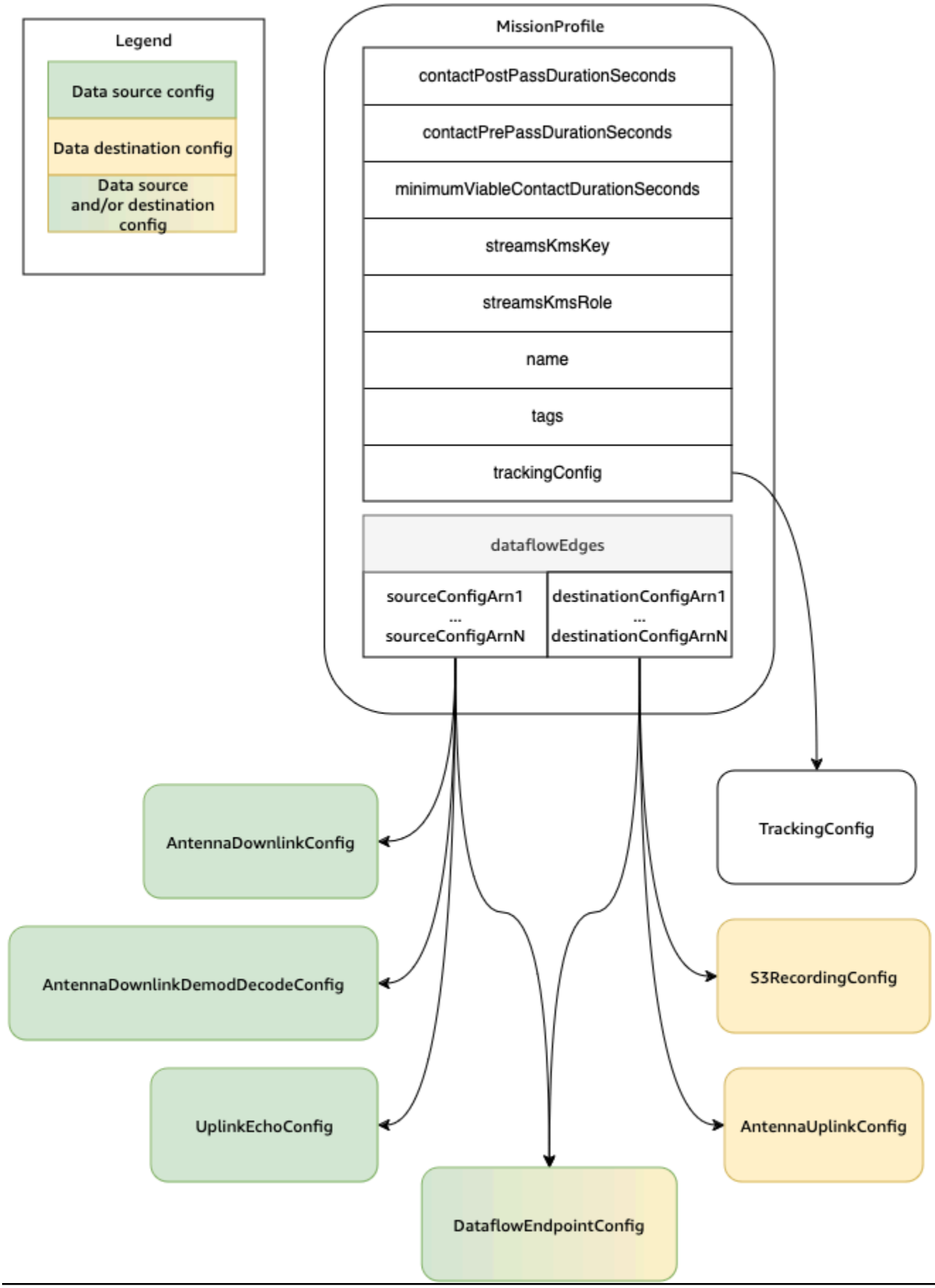
As configurações de rastreamento são especificadas como um campo exclusivo no perfil da missão. As configurações de rastreamento são usadas para especificar sua preferência de usar o rastreamento de programas e o rastreamento automático durante seu contato. Para obter mais informações, consulte Configuração de rastreamento.

Todas as outras configurações estão contidas no `dataflowEdges` campo do perfil da missão. Essas configurações podem ser consideradas como nós de fluxo de dados, cada um representando um recurso AWS Ground Station gerenciado que pode enviar ou receber dados e sua configuração associada. O `dataflowEdges` campo define quais nós de fluxo de dados de origem e destino (configurações) são necessários. Uma única borda de fluxo de dados é uma lista de duas configurações Amazon Resource Names ARNs () — a primeira é a configuração de origem e a segunda é a configuração de destino. Ao especificar uma borda de fluxo de dados entre duas configurações, você está dizendo AWS Ground Station de onde e para onde os dados devem fluir durante um contato. Para obter mais informações, consulte Use AWS Ground Station configurações.

O `contactPrePassDurationSeconds` e `contactPostPassDurationSeconds` permite que você especifique horários relativos ao contato em que você receberá uma notificação de CloudWatch evento. Para obter um cronograma de eventos relacionados ao seu contato, leiaEntenda o ciclo de vida do contato.

O campo `name` do perfil de missão ajuda a diferenciar entre os perfis de missão criados por você.

Os `streamsKmsRole` e `streamsKmsKey` são usados para definir a criptografia usada AWS Ground Station para sua entrega de dados com o AWS Ground Station Agent. Consulte Criptografia de dados durante o trânsito para 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

Uma lista completa de parâmetros e exemplos está incluída na documentação a seguir.

- AWS::GroundStation::MissionProfile CloudFormation tipo de recurso

## Use AWS Ground Station configurações

As configurações são recursos AWS Ground Station usados para definir os parâmetros para cada aspecto do seu contato. Adicione as configurações que você deseja para um perfil de missão, e esse perfil de missão será usado ao executar o contato. Você pode definir vários tipos de configuração diferentes. As configurações podem ser agrupadas em duas categorias:

- Configurações de rastreamento
- Configurações de fluxo de dados

A TrackingConfigé o único tipo de configuração de rastreamento. Ele é usado para definir a configuração de rastreamento automático da antena durante um contato e é necessário em um perfil de missão.

As configurações que podem ser usadas em um fluxo de dados do perfil de missão podem ser consideradas como nós de fluxo de dados, cada um representando um recurso AWS Ground Station gerenciado que pode enviar ou receber dados. Um perfil de missão requer pelo menos um par dessas configurações, com uma representando uma fonte de dados e outra representando um destino. Essas configurações estão resumidas na tabela a seguir.

| Nome da configuração | Origem/destino do fluxo de dados |
|---|---|
| AntennaDownlinkConfig | Origem |
| AntennaDownlinkDemodDecodeConfig | Origem |
| UplinkEchoConfig | Origem |
| S3 RecordingConfig | Destino |
| AntennaUplinkConfig | Destino |
| DataflowEndpointConfig | Origem e/ou destino |

Consulte a documentação a seguir para obter mais informações sobre como realizar operações em configurações usando AWS CloudFormation a AWS Command Line Interface API ou a AWS Ground Station API. Links para documentação de tipos de configuração específicos também são fornecidos abaixo.

- AWS::GroundStation::Config CloudFormation tipo de recurso
- Referência de configuração AWS CLI
- Referência de configuração da API

## Configuração de rastreamento

Você pode usar configurações de rastreamento no perfil de missão para determinar se autotrack deve ser habilitado durante seus contatos. Essa configuração tem um único parâmetro: `autotrack`. O parâmetro `autotrack` pode ter os seguintes valores:

- `REQUIRED`: o autotrack é necessário para seus contatos.
- `PREFERRED`: o autotrack é preferido para contatos, mas os contatos ainda podem ser executados sem o autotrack.
- `REMOVED`: o autotrack deve ser usado para seus contatos.

AWS Ground Station utilizará rastreamento programático que apontará com base em suas efemérides quando o rastreamento automático não for usado. Consulte Entenda como AWS Ground Station usa dados de efemérides de satélite para obter detalhes sobre como as efemérides são construídas.

O Autotrack usará o rastreamento do programa até que o sinal esperado seja encontrado. Quando isso ocorrer, ele continuará rastreando com base na intensidade do sinal.

Consulte a documentação a seguir para obter mais informações sobre como realizar operações em configurações de rastreamento usando AWS CloudFormation a AWS Command Line Interface API ou a AWS Ground Station API.

- AWS::GroundStation::Config TrackingConfig CloudFormation propriedade
- AWS CLI Referência de configuração (consulte a `trackingConfig -> (structure)` seção)
- TrackingConfig Referência de API

## Configuração de downlink de antena

Você pode usar as configurações de downlink da antena para configurar a antena durante o contato. Elas consistem em uma configuração espectral que especifica a largura de banda, a frequência e polarização que devem ser usadas durante o downlink de antena.

Essa configuração representa um nó de origem em um fluxo de dados. É responsável pela digitalização dos dados de radiofrequência. Os dados transmitidos desse nó seguirão o formato Signal Data/IP. Para obter informações mais detalhadas sobre como criar fluxos de dados com essa configuração, consulte Trabalhe com fluxos de dados

Se seu caso de uso de downlink exigir demodulação ou decodificação, consulte Configuração de decodificação de demodulação de downlink de antena .

Consulte a documentação a seguir para obter mais informações sobre como realizar operações nas configurações de downlink de antena usando AWS CloudFormation AWS Command Line Interface, a ou a API. AWS Ground Station

- AWS::GroundStation::Config AntennaDownlinkConfig CloudFormation propriedade
- AWS CLI Referência de configuração (consulte a `antennaDownlinkConfig -> (structure)` seção)
- AntennaDownlinkConfig Referência de API

## Configuração de decodificação de demodulação de downlink de antena

As configurações de decodificação de demod de downlink de antena são um tipo de configuração mais complexo e personalizável que você pode usar para executar contatos de downlink com demodulação e/ou decodificação. `<Se você estiver interessado em executar esses tipos de contatos, entre em conta` Nós lhe ajudaremos a definir a configuração e o perfil de missão certos para seu caso de uso.

Essa configuração representa um nó de origem em um fluxo de dados. Ele é responsável por digitalizar os dados de radiofrequência e realizar a desmodulação e decodificação conforme especificado. Os dados transmitidos desse nó seguirão o Demodulated/Decoded Data/IP formato. Para obter informações mais detalhadas sobre como criar fluxos de dados com essa configuração, consulte Trabalhe com fluxos de dados

Consulte a documentação a seguir para obter mais informações sobre como realizar operações nas configurações de decodificação de demod de downlink de antena usando AWS CloudFormation, a ou a AWS Command Line Interface API. AWS Ground Station

- AWS::GroundStation::Config AntennaDownlinkDemodDecodeConfig CloudFormation propriedade
- AWS CLI Referência de configuração (consulte a `antennaDownlinkDemodDecodeConfig -> (structure)` seção)
- AntennaDownlinkDemodDecodeConfig Referência da API

## Configuração de uplink de antena

Você pode usar configurações de uplink de antena para configurar a antena durante o contato uplink. Eles consistem em uma configuração de espectro com frequência, polarização e potência radiada isotrópica efetiva alvo (EIRP). Para obter informações sobre como configurar eco uplink, consulte Configuração de eco de uplink de antena.

Essa configuração representa um nó de destino em um fluxo de dados. Ele converterá o sinal de dados de radiofrequência digitalizado fornecido em um sinal analógico e o emitirá para o seu satélite receber. Espera-se que os dados transmitidos para esse nó atendam ao formato Signal Data/IP. Para obter informações mais detalhadas sobre como criar fluxos de dados com essa configuração, consulte Trabalhe com fluxos de dados

Consulte a documentação a seguir para obter mais informações sobre como realizar operações nas configurações de uplink de antena usando AWS CloudFormation AWS Command Line Interface, a ou a API. AWS Ground Station

- AWS::GroundStation::Config AntennaUplinkConfig CloudFormation propriedade
- AWS CLI Referência de configuração (consulte a `antennaUplinkConfig -> (structure)` seção)
- AntennaUplinkConfig Referência de API

## Configuração de eco de uplink de antena

As configurações de eco de uplink informam à antena como executar um eco de uplink. Um eco de uplink pode ser usado para validar comandos enviados para sua espaçonave e realizar outras tarefas avançadas. Isso é obtido gravando o sinal real transmitido pela AWS Ground Station antena (ou seja, o uplink). Isso ecoa o sinal enviado pela antena de volta ao ponto final do fluxo de dados

e deve corresponder ao sinal transmitido. A configuração de eco de uplink contém o ARN de uma configuração de uplink. A antena usa os parâmetros da configuração de uplink apontada pelo ARN ao executar um eco de uplink.

Essa configuração representa um nó de origem em um fluxo de dados. Os dados transmitidos desse nó atenderão ao formato Signal Data/IP. Para obter informações mais detalhadas sobre como criar fluxos de dados com essa configuração, consulte Trabalhe com fluxos de dados

Consulte a documentação a seguir para obter mais informações sobre como realizar operações em configurações de eco de uplink usando AWS CloudFormation AWS Command Line Interface, a ou a API. AWS Ground Station

- AWS::GroundStation::Config UplinkEchoConfig CloudFormation propriedade
- AWS CLI Referência de configuração (consulte a `uplinkEchoConfig -> (structure)` seção)
- UplinkEchoConfig Referência de API

## Configuração de endpoint de fluxo de dados

> **Note**
>
> As configurações de endpoint do Dataflow são usadas somente para entrega de dados para a Amazon EC2 e não para entrega de dados para o Amazon S3.

Você pode usar as configurações de endpoint de fluxo de dados para especificar qual endpoint de fluxo de dados em um grupo de endpoints de fluxo de dados do qual ou para o qual você deseja que os dados fluam durante um contato. Os dois parâmetros de uma configuração de endpoint do fluxo de dados especificam o nome e a região do endpoint do fluxo de dados. Ao reservar um contato, AWS Ground Station analisa o perfil de missão que você especificou e tenta encontrar um grupo de endpoints de fluxo de dados AWS na região que contenha todos os endpoints de fluxo de dados especificados pelas configurações de endpoint de fluxo de dados contidas em seu perfil de missão. Se um grupo de endpoints de fluxo de dados adequado for encontrado, o status do contato será SCHEDULADO, caso contrário, se tornará FAILED_TO_SCHEDULE. Para obter mais informações sobre os possíveis status de um contato, consulteAWS Ground Station status de contato.

A propriedade `dataflowEndpointName` do endpoint em uma configuração de ponto de extremidade de fluxo de dados especifica para qual endpoint de fluxo de dados em um grupo de endpoints de fluxo de dados os dados fluirão durante um contato.

A propriedade `dataflowEndpointRegion` especifica em qual região o endpoint do fluxo de dados reside. Se uma região for especificada na configuração do endpoint do fluxo de dados, AWS Ground Station procurará um endpoint do fluxo de dados na região especificada. Se nenhuma região for especificada, o padrão AWS Ground Station será a região da estação terrestre do contato. Um contato é considerado um contato de entrega de dados entre regiões se a região do seu endpoint de fluxo de dados não for a mesma da região da estação terrestre do contato. Consulte Trabalhe com fluxos de dados para obter mais informações sobre fluxos de dados entre regiões.

Veja Use grupos AWS Ground Station de endpoints do Dataflow dicas sobre como diferentes esquemas de nomenclatura para seus fluxos de dados podem beneficiar seu caso de uso.

Para obter informações mais detalhadas sobre como criar fluxos de dados com essa configuração, consulte Trabalhe com fluxos de dados

Consulte a documentação a seguir para obter mais informações sobre como realizar operações em configurações de endpoint de fluxo de dados usando AWS CloudFormation AWS Command Line Interface, a ou a API. AWS Ground Station

- AWS::GroundStation::Config DataflowEndpointConfig CloudFormation propriedade
- AWS CLI Referência de configuração (consulte a `dataflowEndpointConfig -> (structure)` seção)
- DataflowEndpointConfig Referência de API

## Config de gravação do Amazon S3

> **Note**
>
> As configurações de gravação do Amazon S3 são usadas somente para entrega de dados para o Amazon S3 e não são usadas para entrega de dados para a Amazon. EC2

Essa configuração representa um nó de destino em um fluxo de dados. Esse nó encapsulará os dados recebidos do nó de origem do fluxo de dados em dados pcap. Para obter informações mais detalhadas sobre como criar fluxos de dados com essa configuração, consulte Trabalhe com fluxos de dados

Você pode usar as configurações de gravação do S3 para especificar um bucket do Amazon S3 para o qual você deseja que os dados baixados sejam entregues junto com a convenção de nomenclatura usada. O seguinte especifica restrições e detalhes sobre esses parâmetros:

- O nome do bucket do Amazon S3 deve começar com `aws-groundstation`.
- O perfil do IAM deve ter uma política de confiança que permita à entidade principal do serviço `groundstation.amazonaws.com` assumir o perfil. Veja a seção Exemplo de Política de Confiança abaixo para um exemplo. Durante a criação da configuração, o ID do recurso de configuração não existe, a política de confiança deve usar um asterisco (*) no lugar *your-config-id* e pode ser atualizada após a criação com o ID do recurso de configuração.

Exemplo de política de confiança

Para obter mais informações sobre como atualizar a política de confiança de um perfil, consulte Gerenciar perfis do IAM no Guia do usuário do 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"
        }
      }
    }
  ]
}
```

- O perfil do IAM deve ter uma política do IAM que permita que a função execute a ação `s3:GetBucketLocation` no bucket e a ação `s3:PutObject` nos objetos do bucket. Se o bucket do Amazon S3 tiver uma política de bucket, a política também deverá permitir que o perfil do IAM execute essas ações. Veja a seção Exemplo de Política de Confiança abaixo para um exemplo.

Exemplo de política de funções

Para obter mais informações sobre como atualizar a política de confiança de uma função, consulte Gerenciar políticas do IAM no Guia do usuário do 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/*"
      ]
    }
  ]
}
```

- O prefixo será usado ao nomear o objeto de dados do S3. Você pode especificar chaves opcionais para substituição, esses valores serão substituídos pelas informações correspondentes dos seus detalhes de contato. Por exemplo, um prefixo de `{satellite_id}/{year}/{month}/{day}` será substituído e resultaria em uma saída como `fake_satellite_id/2021/01/10`

Teclas opcionais para substituição: `{satellite_id}` | `{config-name}` | | `{config-id}` | `{year}` | `{month}` | `{day}`

Consulte a documentação a seguir para obter mais informações sobre como realizar operações nas configurações de gravação do S3 usando a AWS CloudFormation API ou a AWS Command Line Interface AWS Ground Station API.

- AWS::GroundStation::Config Propriedade S3 RecordingConfig CloudFormation
- AWS CLI Referência de configuração (consulte a `s3RecordingConfig -> (structure)` seção)
- Referência da RecordingConfig API S3

## Use grupos AWS Ground Station de endpoints do Dataflow

Os endpoints do fluxo de dados definem o local em que você deseja que os dados sejam transmitidos de forma síncrona de ou para onde você deseja que os dados sejam transmitidos de forma síncrona durante os contatos. Os endpoints de fluxo de dados sempre são criados como parte de um grupo de endpoints de fluxo de dados. Com a inclusão de vários endpoints de fluxo de dados em um grupo, você está afirmando que todos os endpoints especificados podem ser usados juntos durante um único contato. Por exemplo, se um contato precisar enviar dados para três endpoints de fluxo de dados separados, você deve ter três endpoints em um único grupo de endpoints de fluxo de dados que correspondam às configurações do endpoint de fluxo de dados em seu perfil de missão.

> **Tip**
>
> Os endpoints do fluxo de dados são identificados por um nome de sua escolha ao executar contatos. Esses nomes não precisam ser exclusivos em toda a conta. Isso permite que vários contatos em diferentes satélites e antenas sejam executados ao mesmo tempo usando o mesmo perfil de missão. Isso pode ser útil se você tiver uma constelação de satélites com as mesmas características operacionais. Você pode escalar o número de grupos de endpoints de fluxo de dados para caber no número máximo de contatos simultâneos que sua constelação de satélites exige.

Quando um ou mais recursos em um grupo de endpoints de fluxo de dados está em uso para um contato, todo o grupo é reservado para a duração desse contato. É possível executar vários contatos

por vez, mas esses contatos devem ser executados em diferentes grupos de endpoints de fluxo de dados.

> **Important**
>
> Os grupos de endpoints do Dataflow devem estar em condições HEALTHY de programar contatos com eles. Para obter informações sobre como solucionar problemas em grupos de endpoints de fluxo de dados que não estão em um HEALTHY estado, consulte. Solucione o problema que DataflowEndpointGroups não está em um estado SAUDÁVEL

Consulte a documentação a seguir para obter mais informações sobre como realizar operações em grupos de endpoints de fluxo de dados usando a AWS CloudFormation API ou a AWS Command Line Interface API. AWS Ground Station

- AWS::GroundStation::DataflowEndpointGroup CloudFormation tipo de recurso
- Referência do Dataflow Endpoint Group AWS CLI
- Referência da API do Dataflow Endpoint Group

## Endpoints de fluxo de dados

Os membros de um grupo de endpoints de fluxo de dados são endpoints de fluxo de dados. Há dois tipos de endpoints de fluxo de dados: endpoints do AWS Ground Station agente e endpoints do Dataflow. Para os dois tipos de endpoints, você criará as construções de suporte (por exemplo, endereços IP) antes de criar o grupo de endpoints do fluxo de dados. Consulte Trabalhe com fluxos de dados as recomendações sobre qual tipo de endpoint de fluxo de dados usar e como configurar as construções de suporte.

As seções a seguir descrevem os dois tipos de endpoints compatíveis.

> **Important**
>
> Todos os endpoints de fluxo de dados em um único grupo de endpoints de fluxo de dados devem ser do mesmo tipo. Você não pode misturar endpoints do AWS Ground Station Agent com endpoints do Dataflow no mesmo grupo. Se seu caso de uso exigir os dois tipos de endpoints, você deverá criar grupos de endpoints de fluxo de dados separados para cada tipo.

### AWS Ground Station Endpoint do agente

O AWS Ground Station Agent Endpoint utiliza o AWS Ground Station Agente como um componente de software para encerrar conexões. Use um AWS Ground Station Agent Dataflow Endpoint quando quiser baixar mais de 50% dos dados de sinal digital. MHz Para construir um AWS Ground Station Agent Endpoint, você só preencherá o `AwsGroundStationAgentEndpoint` campo do. EndpointDetails Para obter mais informações sobre o AWS Ground Station agente, consulte o Guia do usuário completo do AWS Ground Station agente.

O `AwsGroundStationAgentEndpoint` contém o seguinte:

- `Name`- O nome do endpoint do fluxo de dados. Para que o contato use esse endpoint de fluxo de dados, esse nome deve corresponder ao nome usado na configuração do endpoint de fluxo de dados.
- `EgressAddress`- O endereço IP e da porta usados para extrair dados do Agente.
- `IngressAddress`- O endereço IP e da porta usados para inserir dados no Agente.

### Endpoint de fluxo de dados

O Dataflow Endpoint utiliza um aplicativo de rede como componente de software para encerrar conexões. Use o Dataflow Endpoint quando quiser fazer o uplink de dados de sinal digital, o downlink de menos de 50% dos dados de sinal digital ou o downlink de dados MHz de sinal demodulados/decodificados. Para criar um endpoint do Dataflow, você preencherá os campos `Endpoint` e `Security Details` do. EndpointDetails

O `Endpoint` contém o seguinte:

- `Name`- O nome do endpoint do fluxo de dados. Para que o contato use esse endpoint de fluxo de dados, esse nome deve corresponder ao nome usado na configuração do endpoint de fluxo de dados.
- `Address`- O endereço IP e da porta usados.

O `SecurityDetails` contém o seguinte:

- `roleArn`- O Amazon Resource Name (ARN) de uma função que AWS Ground Station assumirá a criação de interfaces de rede elástica (ENIs) em sua VPC. Eles ENIs servem como pontos de entrada e saída de dados transmitidos durante um contato.
- `securityGroupIds`: os grupos de segurança a serem anexados às interfaces de rede elástica.

- `subnetIds`- Uma lista de sub-redes nas quais você AWS Ground Station pode colocar interfaces de rede elásticas para enviar fluxos para suas instâncias. Se várias sub-redes forem especificadas, elas deverão ser roteáveis entre si. Se as sub-redes estiverem em zonas de disponibilidade diferentes (AZs), você poderá incorrer em cobranças de transferência de dados entre AZ.

O perfil do IAM transmitido no `roleArn` deve ter uma política de confiança que permita à entidade principal do serviço `groundstation.amazonaws.com` assumir o perfil. Veja a seção Exemplo de Política de Confiança abaixo para um exemplo. Durante a criação do endpoint, o ID do recurso do endpoint não existe, portanto, a política de confiança deve usar um asterisco (*) no lugar de. *your-endpoint-id* Isso pode ser atualizado após a criação para usar o ID do recurso do endpoint a fim de definir o escopo da política de confiança para esse grupo específico de endpoints do fluxo de dados.

A função do IAM deve ter uma política do IAM que AWS Ground Station permita configurar ENIs o. Veja a seção Exemplo de Política de Confiança abaixo para um exemplo.

Exemplo de política de confiança

Para obter mais informações sobre como atualizar a política de confiança de um perfil, consulte Gerenciar perfis do IAM no Guia do usuário do 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"
        }
      }
    }
```

```
  ]
}
```

Exemplo de política de funções

Para obter mais informações sobre como atualizar a política de confiança de uma função, consulte Gerenciar políticas do IAM no Guia do usuário do IAM.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups"
      ]
    }
  ]
}
```

# AWS Ground Station Agente de uso

O AWS Ground Station agente permite que você receba (downlink) fluxos de dados síncronos de frequência intermediária digital de banda larga (DigiF) durante os contatos do AWS Ground Station.

## Como funciona

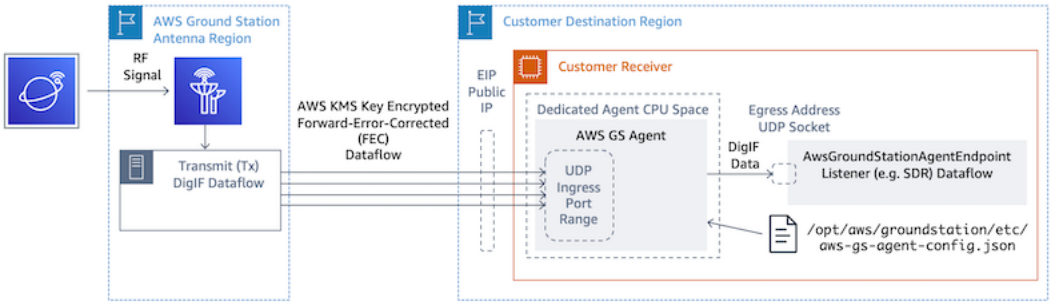
Você pode selecionar duas opções para entrega de dados:

1. Entrega de dados para uma EC2 instância - Entrega de dados para uma EC2 instância que você possui. Você gerencia o AWS Ground Station Agente. Essa opção pode ser mais adequada se você precisar de processamento de dados quase em tempo real. Consulte a Trabalhe com fluxos de dados seção para obter informações sobre entrega de EC2 dados.

2. Entrega de dados para um bucket S3 - A entrega de dados para seu bucket AWS S3 é totalmente gerenciada por. AWS Ground Station Consulte o guia Conceitos básicos para obter informações sobre a entrega de dados do S3.

Ambos os modos de entrega de dados exigem que você crie um conjunto de recursos da AWS. O uso de CloudFormation para criar seus recursos da AWS é altamente recomendado para garantir confiabilidade, precisão e capacidade de suporte. Cada contato só pode entregar dados para EC2 ou S3, mas não para ambos simultaneamente.

O diagrama a seguir mostra um fluxo de dados DigiF de uma região de AWS Ground Station antena para sua EC2 instância com seu rádio definido por software (SDR) ou ouvinte similar.




## Mais informações

Para obter informações mais detalhadas, consulte o Guia completo do usuário do AWS Ground Station agente.

# Conceitos básicos

Antes de começar, você deve se familiarizar com os conceitos básicos do. AWS Ground Station Para obter mais informações, consulte Como AWS Ground Station funciona.

Abaixo estão as melhores práticas para AWS Identity and Access Management (IAM) e quais permissões você precisará. Depois de configurar as funções apropriadas, você pode começar a seguir o restante das etapas.

## Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

1. Abra a https://portal.aws.amazon.com/billing/inscrição.
2. Siga as instruções online.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica ou uma mensagem de texto e inserir um código de verificação pelo teclado do telefone.

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário-raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar tarefas que exigem acesso de usuário-raiz.

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, você pode visualizar a atividade atual da sua conta e gerenciar sua conta acessando https://aws.amazon.com/e escolhendo Minha conta.

## Criar um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS AWS IAM Identity Center, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login AWS Management Consolecomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, insira a senha.

   Para obter ajuda ao fazer login usando o usuário-raiz, consulte Fazer login como usuário-raiz no Guia do usuário do Início de Sessão da AWS .
2. Habilite a autenticação multifator (MFA) para o usuário-raiz.

   Para obter instruções, consulte Habilitar um dispositivo de MFA virtual para seu usuário Conta da AWS raiz (console) no Guia do usuário do IAM.

Criar um usuário com acesso administrativo

1. Habilita o Centro de Identidade do IAM.

   Para obter instruções, consulte Habilitar o AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center .
2. No Centro de Identidade do IAM, conceda o acesso administrativo a um usuário.

   Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM no Guia AWS IAM Identity Center do usuário.

Iniciar sessão como o usuário com acesso administrativo

- Para fazer login com o seu usuário do Centro de Identidade do IAM, use o URL de login enviado ao seu endereço de e-mail quando o usuário do Centro de Identidade do IAM foi criado.

  Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte Como fazer login no portal de AWS acesso no Guia Início de Sessão da AWS do usuário.

Atribuir acesso a usuários adicionais

1. No Centro de Identidade do IAM, crie um conjunto de permissões que siga as práticas recomendadas de aplicação de permissões com privilégio mínimo.

Para obter instruções, consulte Criar um conjunto de permissões no Guia do usuário do AWS IAM Identity Center .

2. Atribua usuários a um grupo e, em seguida, atribua o acesso de autenticação única ao grupo.

   Para obter instruções, consulte Adicionar grupos no Guia do usuário do AWS IAM Identity Center .

## Adicione AWS Ground Station permissões à sua AWS conta

Para usar AWS Ground Station sem exigir um usuário administrativo, você precisa criar uma nova política e anexá-la à sua AWS conta.

1. Faça login no AWS Management Console e abra o console do IAM.
2. Crie uma política. Use as seguintes etapas:

   a. No painel de navegação, escolha Políticas e, em seguida, Criar Política.

   b. Na guia JSON, edite o JSON com um dos seguintes valores. Use o JSON que melhor funcione para a sua aplicação.

   - Para privilégios de Admin, defina Ação como groundstation:*, da seguinte forma:

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

   - Em privilégios Somente leitura, defina Ação como groundstation:get*, groundstation:list* e groundstation:describe*, da seguinte forma:

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

- Para obter segurança adicional por meio da autenticação multifatorial, defina Action como groundstation: * e Condition/Bool como aws ::true da seguinte forma: MultiFactorAuthPresent

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

3. No console do IAM, anexe a política criada para o usuário desejado.

Para obter mais informações sobre criar usuários do IAM e como anexar políticas, consulte o Guia do usuário do IAM.

# Satélite a bordo

A integração de um satélite AWS Ground Station é um processo de várias etapas que envolve coleta de dados, validação técnica, licenciamento de espectro, integração e testes. Também são necessários acordos de não divulgação (NDAs).

## Visão geral do processo de integração de clientes

A integração de satélites é um processo manual que pode ser encontrado na seção Satélites e recursos da página do AWS Ground Station console. A seguir, descrevemos o processo geral.

1. Revise a AWS Ground Station Localizações seção para determinar se seu satélite atende às características geográficas e de radiofrequência.
2. Para começar a integrar seu satélite à AWS Ground Station, envie um e-mail para `<aws-groundstation@amazon.com>` com um breve resumo da missão e das necessidades do satélite, incluindo o nome da sua organização, as frequências necessárias, quando os satélites serão ou serão lançados, o tipo de órbita do satélite e se você planeja usá-lo. Use o recurso de gêmeos AWS Ground Station digitais
3. Depois que sua solicitação for analisada e aprovada, AWS Ground Station solicitará o licenciamento regulatório nos locais específicos que você planeja usar. A duração dessa etapa variará dependendo dos locais e de quaisquer regulamentos existentes.
4. Depois que essa aprovação for obtida, seu satélite ficará visível para você usar. AWS Ground Station enviará uma notificação sobre a atualização bem-sucedida.

## (Opcional) Nomeando satélites

Após a integração, talvez você queira adicionar um nome ao seu registro de satélite para reconhecê-lo mais facilmente. O AWS Ground Station console tem a capacidade de exibir um nome definido pelo usuário para um satélite junto com o ID do Norad ao usar a página de contatos. A exibição do nome do satélite facilita muito a seleção do satélite correto durante o agendamento. Para fazer isso, as tags podem ser usadas.

A marcação de satélites do AWS Ground Station pode ser feita por meio da API de recursos de tag com a AWS CLI ou uma das AWS. SDKs Este guia abordará o uso da AWS Ground Station CLI para marcar o satélite público de transmissão Aqua (Norad ID 27424). `us-west-2`

AWS Ground Station CLI

O AWS CLI pode ser usado para interagir com AWS Ground Station. Antes de usar AWS CLI para marcar seus satélites, os seguintes AWS CLI pré-requisitos devem ser atendidos:

- Certifique-se de que AWS CLI esteja instalado. Para obter informações sobre a instalação AWS CLI, consulte Instalação da AWS CLI versão 2.
- Certifique-se de que AWS CLI esteja configurado. Para obter informações sobre configuração AWS CLI, consulte Configuração da AWS CLI versão 2.
- Salve as definições de configuração usadas com frequência e credenciais em arquivos que são mantidos pela AWS CLI. Você precisa dessas configurações e credenciais para reservar e gerenciar seus AWS Ground Station contatos. AWS CLI Para obter mais informações sobre como salvar suas configurações e configurações de credenciais, consulte Configuração e configurações do arquivo de credenciais.

Quando AWS CLI estiver configurado e pronto para uso, consulte a página de referência de comandos da CLI do AWS Ground Station para se familiarizar com os comandos disponíveis. Siga a estrutura de AWS CLI comandos ao usar esse serviço e prefixe seus comandos com `groundstation` para especificar AWS Ground Station como o serviço que você deseja usar. Para obter mais informações sobre a estrutura de AWS CLI comando, consulte Estrutura de comando na página da AWS CLI. Um exemplo de estrutura de comando é fornecido abaixo.

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

Nomeie um satélite

Primeiro, você precisa obter o ARN do(s) satélite(s) que deseja marcar. Isso pode ser feito por meio da API list-satellites na AWS CLI:

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

A execução do comando CLI acima retornará uma saída semelhante a esta:

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

Encontre o satélite que você deseja marcar e anote o `satelliteArn`. Uma ressalva importante para a marcação é que a API de recursos de tags requer um ARN regional, e o ARN retornado pelos satélites de lista é global. Para a próxima etapa, você deve aumentar o ARN com a região na qual gostaria de ver a tag (provavelmente a região em que você está agendando). Neste exemplo, usamos `us-west-2`. Com essa mudança, o ARN passará de:

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

para:

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

Para mostrar o nome do satélite no console, o satélite deve ter uma etiqueta com `"Name"` como a chave. Além disso, como estamos usando o AWS CLI, as aspas devem ser excluídas com uma barra invertida. A tag será semelhante a:

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

Em seguida, você chamará a API tag-resource para marcar o satélite. Isso pode ser feito da seguinte AWS CLI forma:

```
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"}'
```

Depois de fazer isso, você poderá ver o nome que definiu para o satélite no console do AWS Ground Station .

Alterar o nome de um satélite

Se você quiser alterar o nome de um satélite, basta chamar tag-resource com o ARN do satélite novamente com a mesma "Name" chave, mas com um valor diferente na tag. Isso atualizará a tag existente e mostrará o novo nome no console. Um exemplo de chamada para isso é semelhante a:

```
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"}'
```

Alterar o nome de um satélite

O nome definido para um satélite pode ser removido com a API untag-resource. Essa API precisa do ARN do satélite com a região em que a tag está e de uma lista de chaves de tag. O nome da chave da tag é "Name". Um exemplo de chamada para essa API usando a AWS CLI é este:

```
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
```

## Satélites de transmissão pública

Além de integrar seus próprios satélites, você pode solicitar a integração com satélites de transmissão pública compatíveis que forneçam um caminho de comunicação de downlink acessível ao público. Isso permite que você use AWS Ground Station para baixar dados desses satélites.

> **Note**
>
> Você não poderá fazer o uplink com esses satélites. Você só poderá usar os caminhos de comunicação de downlink acessíveis ao público.

AWS Ground Station suporta a integração dos seguintes satélites para baixar dados de transmissão direta:

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

Uma vez integrados, esses satélites podem ser acessados para uso imediato. AWS Ground Station mantém vários AWS CloudFormation modelos pré-configurados para facilitar o início do serviço. Veja exemplos Exemplo de configurações de perfil de missão de como AWS Ground Station pode ser usado.

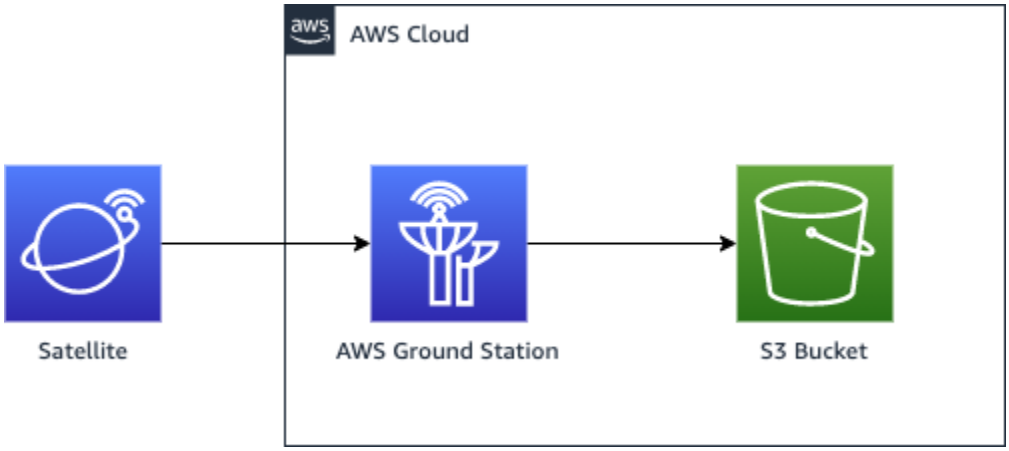
Para obter mais informações sobre esses satélites e os tipos de dados que são transmitidos, consulte Aqua, JPSS-1/NOAA-20 e SNPP e Terra.

# Planeje seus caminhos de comunicação de fluxo de dados

Você pode escolher entre comunicação síncrona e assíncrona para cada caminho de comunicação em seu satélite. Dependendo do seu satélite e do seu caso de uso, você pode precisar de um ou dos dois tipos. Os caminhos de comunicação síncrona permitem operações de uplink quase em tempo real, bem como operações de downlink de banda estreita e banda larga. Os caminhos de comunicação assíncrona suportam somente operações de downlink de banda estreita e banda larga.

## Entrega assíncrona de dados

Com a entrega de dados para o Amazon S3, seus dados de contato são entregues de forma assíncrona para um bucket do Amazon S3 em sua conta. Seus dados de contato são entregues como arquivos de captura de pacotes (pcap) para permitir a reprodução dos dados de contato em um rádio definido por software (SDR) ou para extrair os dados da carga útil dos arquivos pcap para processamento. Os arquivos pcap são entregues ao seu bucket Amazon S3 a cada 30 segundos, pois os dados de contato são recebidos pelo hardware da antena para permitir o processamento de dados de contato durante o contato, se desejado. Depois de recebidos, você pode processar os dados usando seu próprio software de pós-processamento ou usar outros serviços da AWS, como Amazon SageMaker AI ou Amazon Rekognition. A entrega de dados para o Amazon S3 só está disponível para baixar dados do seu satélite; não é possível vincular dados ao seu satélite a partir do Amazon S3.



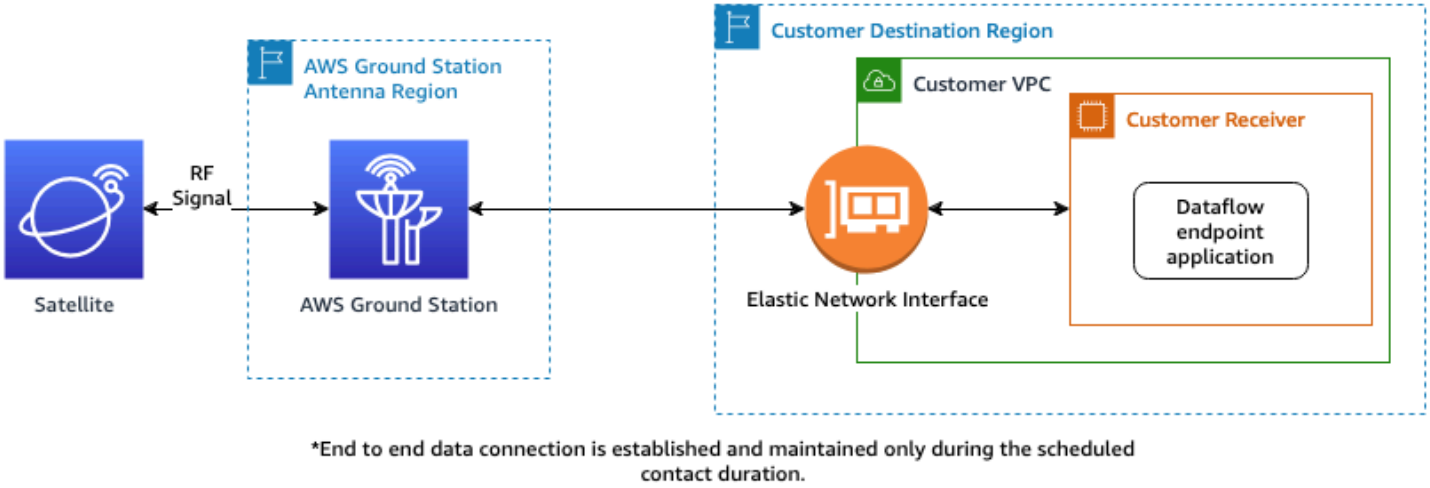

Para utilizar esse caminho, você precisará criar um bucket Amazon S3 AWS Ground Station para entregar os dados. Na próxima etapa, você também precisará criar uma Configuração de Gravação S3 na próxima etapa. Consulte as restrições sobre Config de gravação do Amazon S3 a nomenclatura de buckets e como especificar a convenção de nomenclatura usada para seus arquivos.

## Entrega síncrona de dados

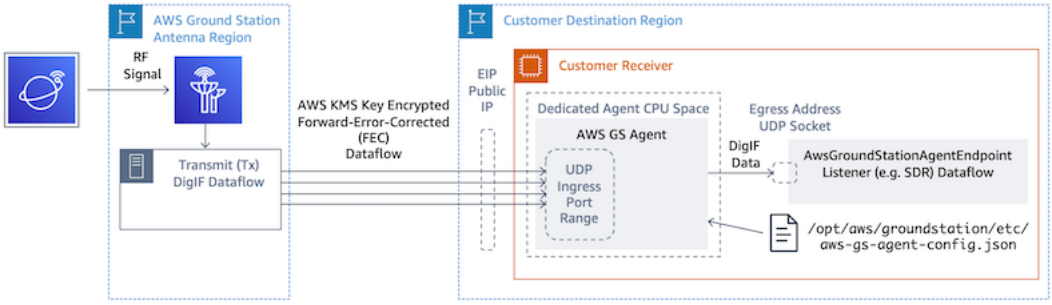
Com a entrega de dados para a Amazon EC2, seus dados de contato são transmitidos de e para sua EC2 instância da Amazon. Você pode processar seus dados em tempo real na sua EC2 instância da Amazon ou encaminhar os dados para pós-processamento.

Para utilizar um caminho síncrono, você precisará instalar e configurar suas EC2 instâncias da Amazon e criar um ou mais grupos de endpoints do Dataflow. Para configurar sua EC2 instância da Amazon, consulte Configurar e configurar a Amazon EC2 o. Para criar seu grupo de endpoints do Dataflow, consulte o. Use grupos AWS Ground Station de endpoints do Dataflow

O exemplo a seguir mostra o caminho de comunicação se você estiver usando a configuração do endpoint de fluxo de dados.




O seguinte mostra o caminho de comunicação se você estiver usando a configuração do AWS Ground Station Agente.




# Crie configurações

Nessa etapa, você identificou o satélite, os caminhos de comunicação e os recursos do IAM EC2, Amazon e Amazon S3, conforme necessário. Nesta etapa, você criará AWS Ground Station configurações que armazenam seus respectivos parâmetros.

## Configurações de entrega de dados

As primeiras configurações a serem criadas estão relacionadas a onde e como você deseja que os dados sejam entregues. Usando as informações da etapa anterior, você construirá muitos dos seguintes tipos de configuração.

- Config de gravação do Amazon S3- Entregue dados para seu bucket Amazon S3.
- Configuração de endpoint de fluxo de dados- Entregue dados para sua EC2 instância da Amazon.

## Configurações de satélite

As configurações do satélite relacionam como AWS Ground Station você pode se comunicar com seu satélite. Você referenciará as informações coletadasSatélite a bordo.

- Configuração de rastreamento- Define a preferência de como seu veículo é rastreado fisicamente durante um contato. Isso é necessário para a construção do perfil da missão.
- Configuração de downlink de antena- Forneça dados de radiofrequência digitalizados.
- Configuração de decodificação de demodulação de downlink de antena - Forneça dados de radiofrequência demodulados e decodificados.
- Configuração de uplink de antena- Vincule dados ao seu satélite.
- Configuração de eco de uplink de antena- Entregue um eco dos dados do seu sinal de uplink.

# Crie um perfil de missão

Com as configurações construídas na etapa anterior, você identificou como rastrear seu satélite e as formas possíveis de se comunicar com ele. Nesta etapa, você construirá um ou mais perfis de missão. Um perfil de missão representa a agregação das configurações possíveis em um comportamento esperado que pode ser programado e operado.

Para obter os parâmetros mais recentes, consulte o tipo AWS::GroundStation::MissionProfile CloudFormation de recurso

1. Dê um nome ao seu perfil de missão. Isso permite que você entenda rapidamente seu uso em seu sistema. Por exemplo, você pode ter a satellite-wideband-narrowband-nominal-operations e a satellite-narrowband-emergency-operationsse você tiver uma operadora de banda estreita separada para operações de emergência.
2. Defina sua configuração de rastreamento.
3. Defina suas durações mínimas de contato viáveis. Isso permite que você filtre contatos em potencial para atender às necessidades de sua missão.
4. Defina seus streamsKmsKeye streamsKmsRoleque são usados para criptografar seus dados durante o trânsito. Isso é usado para todos os fluxos de dados AWS Ground Station do Agente.
5. Defina seus fluxos de dados. Crie seus fluxos de dados para corresponder aos sinais da operadora usando as configurações que você criou na etapa anterior.

6. [Opcional] Defina a duração do contato antes e depois da passagem em segundos. Isso é usado para emitir eventos por contato antes e depois do contato, respectivamente. Consulte Automatize AWS Ground Station com eventos para obter mais informações.
7. [Opcional] Você pode associar Tags ao seu perfil de missão. Eles podem ser usados para ajudar a diferenciar programaticamente seus perfis de missão.

Você pode consultar oExemplo de configurações de perfil de missão, para ver apenas algumas das configurações possíveis.

## Entenda as próximas etapas

Agora que você tem um satélite a bordo e um perfil de missão válido, você está pronto para agendar contatos e se comunicar com seu satélite. AWS Ground Station

Você pode agendar um contato de uma das seguintes formas:

- O AWS Ground Station console.
- O comando AWS CLI reserve-contact.
- O AWS SDK. ReserveContact API.

Para obter informações sobre como AWS Ground Station rastreia a trajetória do seu satélite e como essas informações são usadas, consulte. Entenda como AWS Ground Station usa dados de efemérides de satélite

AWS Ground Station mantém vários AWS CloudFormation modelos pré-configurados para facilitar o início do serviço. Veja exemplos Exemplo de configurações de perfil de missão de como AWS Ground Station pode ser usado.

O processamento dos dados digitais de frequência intermediária ou dos dados desmodulados e decodificados fornecidos a você AWS Ground Station dependerá do seu caso de uso específico. As postagens de blog a seguir podem ajudar você a entender algumas das opções disponíveis:

- Observação automatizada da Terra usando a entrega de dados do AWS Ground Station Amazon S3 (e seu GitHub repositório associado awslabs/) aws-groundstation-eos-pipeline
- Virtualizando o segmento terrestre de satélites com AWS
- Observação da Terra usando AWS Ground Station: Um guia prático

- Construindo arquiteturas de downlink de dados de satélite de alto rendimento com AWS Ground Station WideBand DigiF e Amphinicy Blink SDR (e seu repositório associado aws-samples/) GitHub aws-groundstation-wbdigif-snpp

# AWS Ground Station Localizações

AWS Ground Station fornece uma rede global de estações terrestres próximas à nossa rede global de regiões de infraestrutura da AWS. Você pode configurar o uso desses locais em qualquer região da AWS compatível. Isso inclui a região da AWS na qual os dados são entregues.


## Encontrando a AWS região para a localização de uma estação terrestre

A rede AWS Ground Station global inclui estações terrestres que não estão fisicamente localizadas na região da AWS à qual estão conectadas. A lista de estações terrestres às quais você tem acesso pode ser recuperada por meio da resposta do SDK ListGroundStationda AWS. A lista completa das localizações das estações terrestres é apresentada abaixo, com mais informações em breve. Consulte o guia de integração para adicionar ou modificar as aprovações do site para seus satélites.

| Nome da Ground Station | Localização da Ground Station | Nome da região da AWS | Código de região da AWS | Observações |
|---|---|---|---|---|
| Alasca 1 | Alaska, EUA | Oeste dos EUA (Oregon) | us-west-2 | Não está fisicamente localizado em uma AWS região |
| Bahrein 1 | Bahrein | Oriente Médio (Barém) | me-south-1 | |
| Cidade do Cabo 1 | Cidade do Cabo, África do Sul | África (Cidade do Cabo) | af-south-1 | |
| Dubbo 1 | Dubbo, Austrália | Ásia-Pacífico (Sydney) | ap-southeast-2 | Não está fisicamente localizado em uma AWS região |
| Havaí 1 | Havaí, EUA | Oeste dos EUA (Oregon) | us-west-2 | Não está fisicamente localizado em uma AWS região |
| Irlanda 1 | Irlanda | Europa (Irlanda) | eu-west-1 | |
| Ohio 1 | Ohio, EUA | Leste dos EUA (Ohio) | us-east-2 | |
| Oregon 1 | Oregon, EUA | Oeste dos EUA (Oregon) | us-west-2 | |
| Punta Arenas 1 | Punta Arenas, Chile | América do Sul (São Paulo) | sa-east-1 | Não está fisicamente localizado em uma AWS região |
| Seul 1 | Seul, Coreia do Sul | Ásia-Pacífico (Seul) | ap-northeast-2 | |

| Nome da Ground Station | Localização da Ground Station | Nome da região da AWS | Código de região da AWS | Observações |
|---|---|---|---|---|
| Cingapura 1 | Cingapura | Ásia-Pacífico (Singapura) | ap-southeast-1 | |
| Estocolmo 1 | Estocolmo, Suécia | Europa (Estocolmo) | eu-north-1 | |

## AWS Ground Station regiões da AWS suportadas

Você pode entregar dados e configurar seus contatos por meio do SDK da AWS ou do AWS Ground Station console de regiões compatíveis da AWS. Você pode visualizar as regiões suportadas e seus endpoints associados nos AWS Ground Station endpoints e cotas.

## Disponibilidade do gêmeo digital

Use o recurso de gêmeos AWS Ground Station digitaisestá disponível em todas as regiões da AWS onde AWS Ground Station está disponível. As estações terrestres gêmeas digitais são cópias exatas das estações terrestres de produção com um prefixo modificador para o nome da estação terrestre de “Digital Twin”. Por exemplo, “Digital Twin Ohio 1" é uma estação terrestre dupla digital que é uma cópia exata da estação terrestre de produção “Ohio 1".

## AWS Ground Station máscaras do site

Cada localização AWS Ground Station da antena tem máscaras de site associadas. Essas máscaras impedem que as antenas desse local transmitam ou recebam quando apontam em algumas direções, normalmente perto do horizonte. As máscaras podem levar em consideração:

- Características do terreno geográfico ao redor da antena — Por exemplo, isso inclui coisas como montanhas ou edifícios, que bloqueariam um sinal de radiofrequência (RF) ou impediriam a transmissão.
- Interferência de radiofrequência (RFI) — Isso afeta tanto a capacidade de receber (fontes externas de RFI impactando um sinal de downlink nas antenas do AWS Ground Station) quanto de transmitir (o sinal de RF transmitido pelas antenas do AWS Ground Station impactando negativamente os receptores externos).

- Autorizações legais — As autorizações locais do site para operar o AWS Ground Station em cada região podem incluir restrições específicas, como um ângulo mínimo de elevação para transmissão.

Essas máscaras do site podem ser alteradas ao longo do tempo. Por exemplo, novos edifícios podem ser construídos perto de um local de antena, as fontes de RFI podem mudar ou a autorização legal pode ser renovada com restrições diferentes. As máscaras do site AWS Ground Station estão disponíveis para você sob um acordo de confidencialidade (NDA).

## Máscaras específicas para clientes

Além das máscaras de site do AWS Ground Station em cada local, você pode ter máscaras adicionais devido às restrições de sua própria autorização legal para se comunicar com seus satélites em uma determinada região. Essas máscaras podem ser configuradas no AWS Ground Station para garantir case-by-case a conformidade ao usar o AWS Ground Station para se comunicar com esses satélites. Entre em contato com a equipe do AWS Ground Station para obter detalhes.

## Impacto das máscaras do site nos horários de contato disponíveis

Há dois tipos de máscaras de site: máscaras de site de uplink (transmissão) e máscaras de site de downlink (recebimento).

Ao listar os horários de contato disponíveis usando a ListContacts operação, o AWS Ground Station retornará os tempos de visibilidade com base em quando seu satélite estará acima e abaixo da máscara de downlink. Os tempos de contato disponíveis são baseados nessa janela de visibilidade da máscara de downlink. Isso garante que você não reserve tempo quando seu satélite estiver abaixo da máscara de downlink.

As máscaras do site de uplink não são aplicadas aos horários de contato disponíveis, mesmo que o perfil da missão inclua uma configuração de uplink de antena em uma borda de fluxo de dados. Isso permite que você use todo o tempo de contato disponível para downlink, mesmo que o uplink não esteja disponível por partes desse tempo devido à máscara do site de uplink. No entanto, o sinal de uplink pode não ser transmitido por parte ou por todo o tempo reservado para um contato via satélite. Você é responsável por contabilizar a máscara de uplink fornecida ao programar as transmissões de uplink.

A parte de um contato que não está disponível para uplink varia dependendo da trajetória do satélite durante o contato, em relação à máscara do local de uplink no local da antena. Em regiões em que

as máscaras do site de uplink e downlink são semelhantes, essa duração normalmente será curta. Em outras regiões, em que a máscara de uplink pode ser consideravelmente maior do que a do local de downlink, isso pode fazer com que partes significativas, ou mesmo a totalidade, da duração do contato não estejam disponíveis para uplink. O tempo total de contato é cobrado de você, mesmo que partes do tempo reservado não estejam disponíveis para uplink.

## AWS Ground Station Capacidades do site

Para simplificar sua experiência, AWS Ground Station determina um conjunto comum de recursos para um tipo de antena e, em seguida, implanta várias antenas em um local de estação terrestre. Parte das etapas de integração garante que seu satélite seja compatível com os tipos de antena em um local específico. Ao reservar um contato, você determina indiretamente o tipo de antena usada. Isso garante que sua experiência em um determinado local da estação terrestre permaneça a mesma ao longo do tempo, independentemente de quais antenas estejam sendo usadas. O desempenho específico do seu contato variará devido a uma grande variedade de questões ambientais, como o clima no local.

Atualmente, todos os sites oferecem suporte aos seguintes recursos:

> **Note**
>
> Cada linha na tabela a seguir indica um caminho de comunicação independente, a menos que indicado de outra forma. Existem linhas duplicadas para refletir nossos recursos multicanais que permitem que vários caminhos de comunicação sejam usados simultaneamente.

| Tipo de capacidade | Faixa de frequência | Faixa de largura de banda | Polarization | Nome comum | Observações |
|---|---|---|---|---|---|
| downlink de antena | 750 - 8500 MHz | 50 - 400 MHz | RHCP | Downlink de banda larga de banda X | Esse recurso requer o uso do AWS Ground Station Agente. |
| downlink de antena | 750 - 8500 MHz | 50 - 400 MHz | RHCP | | |

| Tipo de capacidade | Faixa de frequência | Faixa de largura de banda | Polarization | Nome comum | Observações |
|---|---|---|---|---|---|
| downlink de antena | 750 - 8500 MHz | 50 - 400 MHz | RHCP | | Esse recurso não é suportado no Alaska 1 ou em Punta Arenas 1.<br><br>A largura de banda agregada não deve exceder 400 MHz por polarização em cada local.<br><br>Todas as faixas de frequência utilizadas não devem ser sobrepostas. |
| downlink de antena | 750 - 8500 MHz | 50 - 400 MHz | RHCP | | |
| downlink de antena | 750 - 8500 MHz | 50 - 400 MHz | RHCP | | |
| downlink de antena | 750 - 8500 MHz | 50 - 400 MHz | LHCP | | |
| downlink de antena | 750 - 8500 MHz | 50 - 400 MHz | LHCP | | |
| downlink de antena | 750 - 8500 MHz | 50 - 400 MHz | LHCP | | |
| downlink de antena | 750 - 8500 MHz | 50 - 400 MHz | LHCP | | |
| downlink de antena | 750 - 8500 MHz | 50 - 400 MHz | LHCP | | |
| downlink de antena | 2200 - 290 MHz | Até 40 MHz | RHCP | Downlink da banda S | Somente uma polarização pode ser usada por vez |
| downlink de antena | 2200 - 290 MHz | Até 40 MHz | LHCP | | |

| Tipo de capacidade | Faixa de frequência | Faixa de largura de banda | Polarization | Nome comum | Observações |
|---|---|---|---|---|---|
| downlink de antena | 750 - 8500 MHz | Até 40 MHz | RHCP | Downlink de banda estreita de banda X | Somente uma polarização pode ser usada por vez |
| downlink de antena | 750 - 8500 MHz | Até 40 MHz | LHCP | | |
| uplink de antena | 2025 - 2110 MHz | Até 40 MHz | RHCP | Uplink de banda S | Somente uma polarização pode ser usada por vez<br><br>EIRP 20-50 dBW |
| uplink de antena | 2025 - 2110 MHz | Até 40 MHz | LHCP | | |
| antenna-uplink-echo | 2025 - 2110 MHz | 2 MHz | RHCP | Eco de uplink | Corresponde às restrições de uplink da antena |
| antenna-uplink-echo | 2025 - 2110 MHz | 2 MHz | LHCP | | |
| antenna-downlink-demod-decode | 750 - 8500 MHz | Até 500 MHz | RHCP | Downlink desmodulado e decodificado em banda X | |
| antenna-downlink-demod-decode | 750 - 8500 MHz | Até 500 MHz | LHCP | | |
| rastreamento | N/D | N/D | N/D | N/D | Support para rastreamento automático e rastreamento de programas |

* RHCP = polarização circular com a mão direita e LHCP = polarização circular com a mão esquerda. Para obter mais informações sobre polarização, consulte Polarização circular.

# Entenda como AWS Ground Station usa dados de efemérides de satélite

Uma efeméride, efemérides no plural, é um arquivo ou estrutura de dados que fornece a trajetória de objetos astronômicos. Historicamente, esse arquivo se referia apenas a dados tabulares, mas, gradualmente, passou a direcionar para uma ampla variedade de arquivos de dados indicando a trajetória de uma espaçonave.

AWS Ground Station usa dados de efemérides para determinar quando os contatos ficam disponíveis para seu satélite e comanda corretamente as antenas na AWS Ground Station rede para apontar para o seu satélite. Por padrão, nenhuma ação é necessária para AWS Ground Station fornecer efemérides se seu satélite tiver um ID NORAD atribuído.

Tópicos



## Dados de efemérides padrão

Por padrão, AWS Ground Station usa dados publicamente disponíveis do Space-Track, e nenhuma ação é necessária para AWS Ground Station fornecer essas efemérides padrão. Essas efemérides são conjuntos de elementos de duas linhas (TLEs) associados ao ID NORAD do seu satélite. Todas as efemérides padrão têm uma prioridade zero. Como resultado, elas serão sempre substituídas por quaisquer efemérides personalizadas não expiradas enviadas por meio da API Ephemeris, que sempre deve ter uma prioridade de 1 ou mais.

Os satélites sem um ID NORAD devem carregar dados de efemérides personalizados para. AWS Ground Station Por exemplo, satélites que acabaram de ser lançados ou que foram intencionalmente omitidos do catálogo do Space-Track não teriam ID NORAD e precisariam ter efemérides personalizadas carregadas. Para obter mais informações sobre como fornecer uma efeméride personalizada, consulte: Fornecendo dados de efemérides personalizados.

# Forneça dados de efemérides personalizados

> **Important**
>
> A API Ephemeris está atualmente em um estado de visualização

O acesso à API Ephemeris é fornecido somente conforme a necessidade.
<Se você precisar fazer upload de dados de efemérides personalizados, entre em c
AWS Ground Station trata as efemérides como dados de uso individualizados. Se você usar esse recurso opcional, a AWS usará seus dados de efemérides para fornecer suporte à solução de problemas.

## Visão geral

A API Ephemeris permite que efemérides personalizadas sejam enviadas para AWS Ground Station uso com um satélite. Essas efemérides substituem as efemérides padrão do Space-Track (consulte:). Dados de efemérides padrão Oferecemos suporte ao recebimento de dados de efemérides nos formatos Orbit Ephemeris Message (OEM) e elemento de duas linhas (TLE).

O upload de efemérides personalizadas pode melhorar a qualidade do rastreamento, lidar com operações iniciais em que não há efemérides do Space-Track disponíveis e contabilizar as manobras. AWS Ground Station

> **Note**
>
> Ao fornecer efemérides personalizadas antes que um número de catálogo de satélite seja atribuído ao seu satélite, você pode usar 00000 para o campo de número de catálogo de satélite do TLE e 000 para a parte do número de lançamento do campo designador internacional dos metadados TLE ou OEM (por exemplo, 24000A para um veículo lançado em 2024).
>
> Para obter mais informações sobre o formato de TLEs, consulte Conjunto de elementos de duas linhas. Para obter mais informações sobre o formato do OEMs, consulteFormato de efemérides OEM.

# Formato de efemérides OEM

AWS Ground Station processa efemérides fornecidas pelo cliente OEM de acordo com o padrão CCSDS com algumas restrições extras. Os arquivos OEM devem estar no formato KVN. A tabela a seguir descreve os diferentes campos em um OEM e como AWS Ground Station difere do padrão CCSDS.

| Seção | Campo | É necessário o CCSDS | AWS Ground Station requerido | Observações |
|---|---|---|---|---|
| Cabeçalho | CCSDS_OEM_VERS | Sim | Sim | Valor exigido: 2,0 |
| | COMMENT | Não | Não | |
| | CLASSIFICAÇÃO | Não | Não | |
| | DATA_DE_CRIAÇÃO | Sim | Sim | |
| | ORIGINADORA | Sim | Sim | |
| | ID DA MENSAGEM | Não | Não | |
| Metadados | META_START | Sim | Sim | |
| | COMMENT | Não | Não | |
| | NOME_OBJETO | Sim | Sim | |
| | ID_OBJETO | Sim | Sim | |
| | NOME_CENTRAL | Sim | Sim | Valor exigido: Terra |
| | QUADRO_REFERÊNCIA | Sim | Sim | Valores aceitos: EME2 ITRF2 000.000 |

| Seção | Campo | É necessário o CCSDS | AWS Ground Station requerido | Observações |
|---|---|---|---|---|
| | REF_FRAME_EPOCH | Não | Não suportado* | Não é necessário porque os REF_ aceitos FRAMEs têm uma época implícita |
| | SISTEMA_TEMPO | Sim | Sim | Valor exigido: UTC |
| | HORÁRIO_INICIAL | Sim | Sim | |
| | HORÁRIO_DE_INÍCIO UTILIZÁVEL | Não | Não | |
| | HORÁRIO DE PARADA UTILIZÁVEL | Não | Não | |
| | HORÁRIO_DE_PARADA | Sim | Sim | |
| | INTERPOLAÇÃO | Não | Sim | Necessário para AWS Ground Station gerar ângulos de apontamento precisos para os contatos. |

| Seção | Campo | É necessário o CCSDS | AWS Ground Station requerido | Observações |
|---|---|---|---|---|
| | GRAU_DE_INTERPOLAÇÃO | Não | Sim | Necessário para AWS Ground Station gerar ângulos de apontamento precisos para os contatos. |
| | META_STOP | Sim | Sim | |
| Dados | X | Sim | Sim | Representado em `km` |
| | S | Sim | Sim | Representado em `km` |
| | Z | Sim | Sim | Representado em `km` |
| | X_PONTO | Sim | Sim | Representado em `km/s` |
| | Y_DOT | Sim | Sim | Representado em `km/s` |
| | Z_DOT | Sim | Sim | Representado em `km/s` |
| | X_DDOT | Não | Não | Representado em `km/s^2` |
| | Y_DDOT | Não | Não | Representado em `km/s^2` |
| | Z_DDOT | Não | Não | Representado em `km/s^2` |

| Seção | Campo | É necessário o CCSDS | AWS Ground Station requerido | Observações |
|---|---|---|---|---|
| Matriz de covariância | INÍCIO DA COVARIÂNCIA | Não | Não | |
| | EPOCH | Não | Não | |
| | COV_REF_FRAME | Não | Não | |
| | COVARIANCE_STOP | Não | Não | |

* Se alguma linha não suportada pelo AWS Ground Station for incluída no OEM fornecido, o OEM falhará na validação.

Os desvios importantes do padrão CCSDS para são: AWS Ground Station

- É necessário que o CCSDS_OEM_VERS seja. `2.0`
- REF_FRAME deve ser um ou. `EME2000` `ITRF2000`
- REF_FRAME_EPOCH não é suportado pelo. AWS Ground Station
- É necessário que CENTER_NAME seja. `Earth`
- É necessário que TIME_SYSTEM seja. `UTC`
- INTERPOLATION e INTERPOLATION_DEGREE são ambas necessárias para o CPE. AWS Ground Station

## Exemplo de efemérides de OEM no formato KVN

A seguir está um exemplo truncado de uma efeméride OEM no formato KVN para o satélite de transmissão pública 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
```

## Criando uma efeméride personalizada

Uma efeméride personalizada pode ser criada usando a ação CreateEphemeris na API do AWS Ground Station . Essa ação fará o upload de uma efeméride usando dados no corpo da solicitação ou de um bucket do S3 especificado.

É importante observar que o upload de uma efeméride define as efemérides como `VALIDATING` e inicia um fluxo de trabalho assíncrono que validará e gerará contatos potenciais a partir de suas efemérides. Somente quando uma efeméride passar por esse fluxo de trabalho e se tornar `ENABLED`, ela será usada para contatos. Você deve pesquisar o status das efemérides ou usar CloudWatch eventos DescribeEphemerispara rastrear as mudanças de status das efemérides.

Para solucionar uma efeméride inválida, consulte: Solucionar problemas de efemérides inválidas

## Exemplo: criar efemérides de um conjunto de elementos de duas linhas (TLE) por meio da API

A AWS SDKs CLI e pode ser usada para fazer upload de efemérides de um conjunto de elementos de duas linhas (TLE) por meio da chamada. AWS Ground Station CreateEphemeris Essa efeméride será usada no lugar dos dados de efemérides padrão de um satélite (consulte Dados de efemérides padrão). Este exemplo mostra como fazer isso usando o AWS SDK para Python (Boto3).

Um conjunto TLE é um objeto formatado em JSON que TLEs une um ou mais para construir uma trajetória contínua. O TLEs conjunto TLE deve formar um conjunto contínuo que possamos usar para construir uma trajetória (ou seja, sem lacunas no tempo entre TLEs um conjunto TLE). Um conjunto de TLE de exemplo é mostrado abaixo:

```
# 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**
>
> Os intervalos de tempo do TLEs em um conjunto de TLE devem corresponder exatamente para serem uma trajetória contínua e válida.

Um conjunto TLE pode ser carregado por meio do cliente AWS Ground Station boto3 da seguinte forma:

```
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)
                }
            }
        ]
      }
    })
```

Essa chamada retornará um EphemerisID que pode ser usado para referenciar as efemérides no futuro. Por exemplo, podemos usar o EphemerisId fornecido na chamada acima para pesquisar o status da efeméride:

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

Um exemplo de resposta da ação DescribeEphemeris é fornecido abaixo

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

É recomendável pesquisar a DescribeEphemerisrota ou usar CloudWatch eventos para rastrear o status das efemérides carregadas, pois elas devem passar por um fluxo de trabalho de validação assíncrona antes de serem configuradas `ENABLED` e se tornarem utilizáveis para agendar e executar contatos.

Observe que o ID NORAD TLEs em todo o conjunto TLE, `25994` nos exemplos acima, deve corresponder ao ID NORAD atribuído ao seu satélite no banco de dados do Space-Track.

## Exemplo: carregamento de dados do Ephemeris de um bucket do S3

Também é possível fazer upload de um arquivo de efemérides diretamente de um bucket do S3 apontando para o bucket e a chave do objeto. AWS Ground Station recuperará o objeto em seu nome. As informações sobre a criptografia de dados em repouso estão detalhadas em AWS Ground Station : Criptografia de dados em repouso para o AWS Ground Station

Abaixo está um exemplo de upload de um arquivo de efemérides OEM de um 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",
            }
        }
    })
```

Abaixo está um exemplo de dados retornados da ação DescribeEphemeris que está sendo chamada para as efemérides do OEM carregadas no bloco anterior do código de exemplo.

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

## Exemplo: uso de efemérides fornecidas pelo cliente com AWS Ground Station

Para obter instruções mais detalhadas sobre como usar efemérides fornecidas pelo cliente com AWS Ground Station, consulte Como usar efemérides fornecidas pelo cliente com (e seu repositório associado aws-samples/) AWS Ground Station GitHub aws-groundstation-cpe

# Entenda quais efemérides são usadas

As efemérides têm prioridade, prazo de validade e sinalizador ativado. Juntos, eles determinam quais efemérides são usadas para um satélite. Somente uma efeméride pode estar ativa para cada satélite.

A efeméride que será usada é a efeméride habilitada de maior prioridade, cujo prazo de expiração está no futuro. Um valor de prioridade maior indica uma prioridade mais alta. Os horários de contato

disponíveis retornados por ListContactssão baseados nessas efemérides. Se várias efemérides ENABLED tiverem a mesma prioridade, as efemérides criadas ou atualizadas mais recentemente serão usadas.

> **Note**
>
> AWS Ground Station tem uma cota de serviço no número de efemérides ENABLED fornecidas pelo cliente por satélite (consulte: Cotas de serviço). Para carregar dados de efemérides após atingir essa cota, exclua (usando `DeleteEphemeris`) ou desabilite (usando `UpdateEphemeris`) as efemérides de menor prioridade/mais recentes criadas pelo cliente.

Se nenhuma efeméride tiver sido criada, ou se nenhuma efeméride tiver ENABLED status, AWS Ground Station usará uma efeméride padrão para o satélite (do Space-Track), se disponível. Essa efeméride padrão tem prioridade zero.

## Efeito de novas efemérides em contatos previamente agendados

Use a DescribeContact API para visualizar os efeitos de novas efemérides em contatos previamente agendados, retornando os horários de visibilidade ativos.

Os contatos agendados antes do upload de uma nova efeméride manterão o horário de contato originalmente agendado, enquanto o rastreamento da antena usará as efemérides ativas. Se a posição da espaçonave, com base nas efemérides ativas, for muito diferente das efemérides anteriores, isso pode resultar na redução do tempo de contato do satélite com a antena devido à espaçonave operar fora da máscara do local de transmissão/recepção. Portanto, recomendamos que você cancele e reagende seus futuros contatos depois de carregar uma nova efeméride que seja muito diferente da efeméride anterior. Com a DescribeContact API, você pode determinar a parte do seu contato futuro que está inutilizável devido à operação da espaçonave fora da máscara do local de transmissão/recepção, comparando seu contato agendado com o retornado `startTime` e. `endTime` `visibilityStartTime` `visibilityEndTime` Se você optar por cancelar e reagendar seus futuros contatos, o intervalo de tempo de contato não deve estar fora do intervalo de tempo de visibilidade em mais de 30 segundos. Os contatos cancelados podem incorrer em custos quando cancelados muito perto do momento do contato. Para obter mais informações sobre contatos cancelados, consulte: Ground Station FAQs.

# Obtenha as efemérides atuais de um satélite

As efemérides atuais em uso AWS Ground Station por um satélite específico podem ser recuperadas chamando as ações ou. GetSatelliteListSatellites Ambos os métodos retornarão metadados para as efemérides atualmente em uso. Esses metadados de efemérides são diferentes para efemérides personalizadas enviadas para e efemérides padrão. AWS Ground Station

As efemérides padrão incluirão apenas campos `source` e `epoch`. Essa `epoch` é a época do conjunto de elementos de duas linhas que foi retirado do Space-Track e atualmente está sendo usado para calcular a trajetória do satélite.

Uma efeméride personalizada terá um valor `source` de `"CUSTOMER_PROVIDED"` e incluirá um identificador exclusivo no campo `ephemerisId`. Esse identificador exclusivo pode ser usado para consultar as efemérides por meio da ação DescribeEphemeris. Um `name` campo opcional será retornado se a efeméride receber um nome durante o upload AWS Ground Station por meio da ação. CreateEphemeris

É importante observar que as efemérides são atualizadas dinamicamente, AWS Ground Station portanto, os dados retornados são apenas um instantâneo das efemérides que estão sendo usadas no momento da chamada para a API.

## Exemplo de retorno **`GetSatellite`** para um satélite usando uma efeméride padrão

```
{
    "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
    }
}
```

## Exemplo de retorno **`GetSatellite`** para um satélite usando uma efeméride personalizada

```
{
      "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"
      }
  }
```

# Reverter para dados de efemérides padrão

Quando você carrega dados de efemérides personalizados, eles substituem os usos padrão de efemérides AWS Ground Station para aquele satélite específico. AWS Ground Station não usa as efemérides padrão novamente até que não haja efemérides atualmente habilitadas e não expiradas fornecidas pelo cliente disponíveis para uso. AWS Ground Station também não lista contatos após o prazo de expiração das efemérides atuais fornecidas pelo cliente, mesmo que haja uma efeméride padrão disponível após esse prazo de expiração.

Para voltar às efemérides padrão do Space-Track, você precisará fazer o seguinte:

- Exclua (usando DeleteEphemeris) ou desative (usando UpdateEphemeris) todas as efemérides habilitadas fornecidas pelo cliente. Você pode listar as efemérides fornecidas pelo cliente para um satélite usando ListEphemerides.
- Aguarde até que todas as efemérides existentes fornecidas pelo cliente expirem.

Você pode confirmar se a efeméride padrão está sendo usada chamando GetSatellite e verificando se o `source` da efeméride atual do satélite está `SPACE_TRACK`. Consulte Dados de efemérides padrão para obter mais informações sobre efemérides padrão.

# Trabalhe com fluxos de dados

AWS Ground Station usa uma relação de nó e borda para criar fluxos de dados para permitir o processamento de fluxo de seus dados. Cada nó é representado por uma configuração que descreve o processamento esperado. Para ilustrar esse conceito, considere um fluxo de dados de `antenna-downlink` até a. `s3-recording` O `antenna-downlink` nó representa a transformação analógica para digital do espectro de radiofrequência de acordo com os parâmetros definidos na configuração. O `s3-recording` representa um nó de computação que receberá os dados recebidos e os armazenará em seu bucket do S3. O fluxo de dados resultante é uma entrega assíncrona de dados de RF digitalizados para um bucket S3 com base em suas especificações.

Em seu perfil de missão, você pode criar vários fluxos de dados para atender às suas necessidades. As seções a seguir descrevem como configurar seus outros recursos da AWS para serem usados AWS Ground Station e oferecem recomendações para criar fluxos de dados. Para obter informações detalhadas sobre como cada nó se comporta, inclusive se ele é considerado um nó de origem ou destino, consulte. Use AWS Ground Station configurações

Tópicos

- AWS Ground Station interfaces de plano de dados
- Use a entrega de dados entre regiões
- Instalar e configurar o Amazon S3
- Configurar e configurar a Amazon VPC
- Configurar e configurar a Amazon EC2

# AWS Ground Station interfaces de plano de dados

A estrutura de dados resultante do fluxo de dados escolhido depende da origem do fluxo de dados. Detalhes desses formatos são fornecidos a você durante a integração de seus satélites. O seguinte resume os formatos usados para cada tipo de fluxo de dados.

- downlink de antena
  - (Largura de banda inferior a 54MHz) os dados são entregues como pacotes de dados de sinal/ formato IP VITA-49.
  - (Largura de banda greater-than-or-equal - até 54MHz) os dados são entregues como pacotes de AWS Ground Station Classe 2.

- antenna-downlink-demod-decode
  - Os dados são entregues como pacotes de Demodulated/Decoded Data/IP formato.
- uplink de antena
  - Os dados devem ser entregues como pacotes de dados de sinal/formato IP VITA-49.
- antenna-uplink-echo
  - Os dados são entregues como pacotes de dados de sinal/formato IP VITA-49.

## Use a entrega de dados entre regiões

O recurso de entrega de dados AWS Ground Station entre regiões oferece a flexibilidade de enviar seus dados de uma antena para qualquer região compatível AWS Ground Station da AWS. Isso significa que você pode manter sua infraestrutura em uma única região da AWS e agendar contatos em qualquer região à AWS Ground Station AWS Ground Station Localizações qual você esteja integrado.

Atualmente, a entrega de dados entre regiões está disponível em todas as regiões AWS Ground Station suportadas ao receber seus dados de contato em um Amazon S3 Bucket. AWS Ground Station gerenciará todos os aspectos da entrega para você.

A entrega de dados entre regiões para a Amazon EC2 com o AWS Ground Station agente está disponível em todas as antenna-to-destination regiões. Nenhuma configuração ou aprovação exclusiva é necessária para essa configuração.

A entrega de dados entre regiões para a Amazon EC2 usando um endpoint de fluxo de dados está disponível por padrão* nas regiões descritas abaixo. antenna-to-destination

- Região Leste dos EUA (Ohio) (us-east-2) para região Oeste dos EUA (Oregon) (us-west-2)
- Região Oeste dos EUA (Oregon) (us-west-2) para região Leste dos EUA (Ohio) (us-east-2)

Para usar a entrega de dados entre regiões para uma EC2 instância da Amazon, o endpoint do fluxo de dados deve ser criado na sua região atual da AWS e você dataflow-endpoint-configdeve especificar a mesma região.

As informações anteriores detalhando as regiões suportadas e os métodos de entrega de dados entre regiões estão resumidas na tabela a seguir.

| Método de recebimento | Região da antena | Região de recebimento |
| --- | --- | --- |
| Entrega de dados do Amazon S3 | Tudo integrado AWS Ground Station AWS Ground Station Localizações | Todas as AWS Ground Station regiões |
| AWS Ground Station Agente na Amazon EC2 | Tudo integrado AWS Ground Station AWS Ground Station Localizações | Todas as AWS Ground Station regiões |
| Endpoint de fluxo de dados na Amazon * EC2 | Região Leste dos EUA (Ohio) (us-east-2) | Região Oeste dos EUA (Oregon) (us-west-2) |
| | Região Oeste dos EUA (Oregon) (us-west-2) | Região Leste dos EUA (Ohio) (us-east-2) |

antenna-to-destination*Regiões adicionais não listadas exigem configurações especiais da Amazon EC2 e do software. Entre em contato conosco em `<aws-groundstation@amazon.com>` para obter instruções de integração.

## Instalar e configurar o Amazon S3

Você pode utilizar um bucket do Amazon S3 para receber seus sinais de downlink usando. AWS Ground Station Para criar o s3-recording-config de destino, você deve ser capaz de especificar um bucket do Amazon S3 e uma função do IAM que autorize a gravação de arquivos no bucket. AWS Ground Station

Consulte Config de gravação do Amazon S3 as restrições sobre o bucket do Amazon S3, a função do IAM ou a criação de AWS Ground Station configurações.

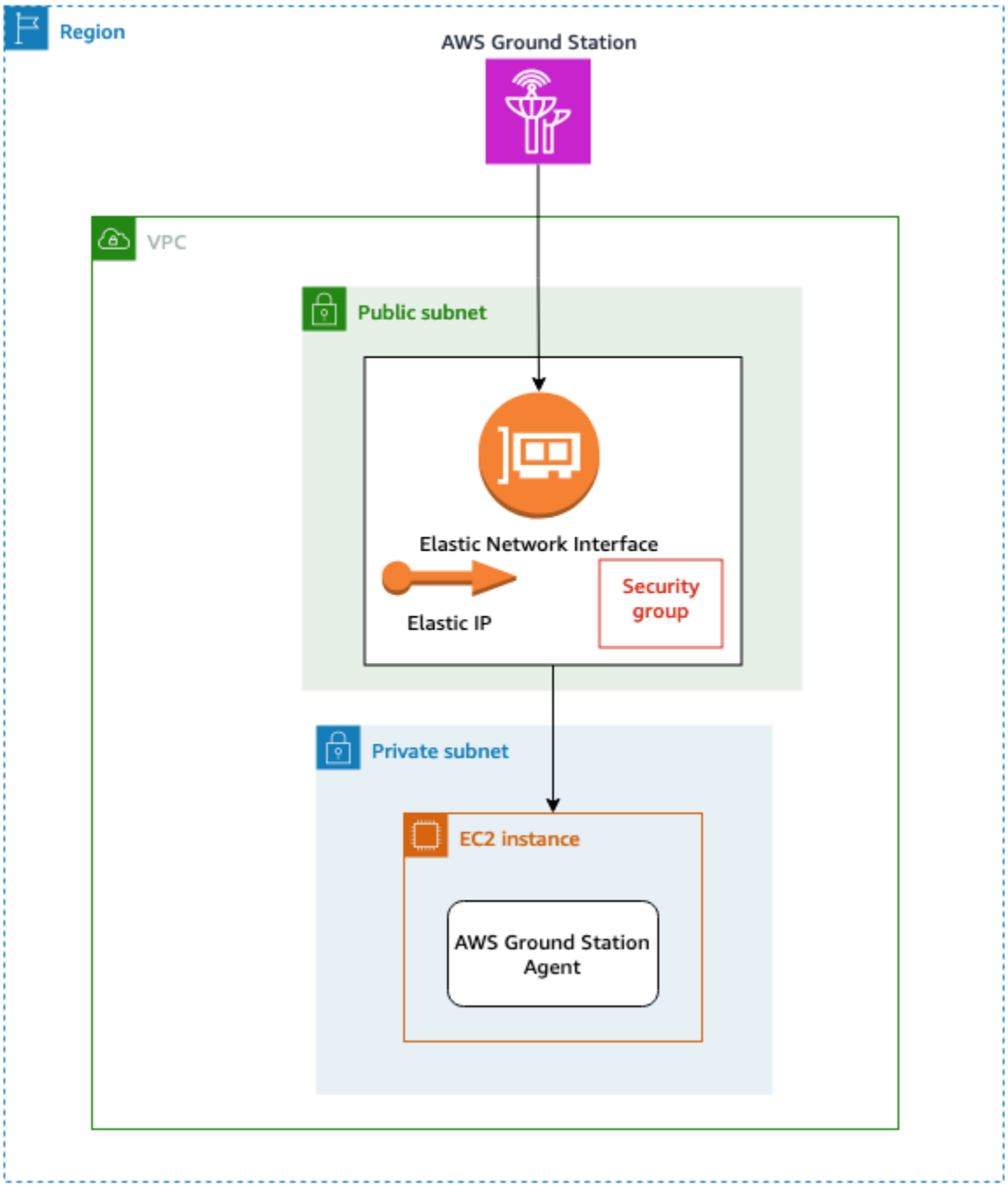
## Configurar e configurar a Amazon VPC

Um guia completo para configurar uma VPC está além do escopo deste guia. Para uma compreensão aprofundada, consulte o Guia do usuário da Amazon VPC.

Nesta seção, é descrito como seu endpoint Amazon EC2 e de fluxo de dados podem existir em uma VPC. AWS Ground Station não oferece suporte a vários pontos de entrega para um determinado fluxo de dados. Espera-se que cada fluxo de dados termine em um único receptor. EC2 Como

esperamos um único EC2 receptor, a configuração não é redundante Multi-AZ. Para ver exemplos completos de como usar sua VPC, consulte. Exemplo de configurações de perfil de missão

## Configuração de VPC com agente AWS Ground Station




Seus dados de satélite são fornecidos para uma instância do AWS Ground Station Agente próxima à antena. O AWS Ground Station agente extrairá e criptografará seus dados usando a AWS KMS chave que você fornecer. Cada faixa é enviada para seu Amazon EC2 Elastic IP (EIP) a partir da

antena de origem em todo o backbone da rede AWS. Os dados chegam à sua EC2 instância por meio da Amazon EC2 Elastic Network Interface (ENI) anexada. Uma vez na sua EC2 instância, o AWS Ground Station Agente instalado descriptografará seus dados e executará a correção de erros de encaminhamento (FEC) para recuperar os dados perdidos e, em seguida, os encaminhará para o IP e a porta especificados na sua configuração.

A lista abaixo destaca considerações de configuração exclusivas ao configurar sua VPC AWS Ground Station para entrega de agentes.

Grupo de segurança - É recomendável configurar um grupo de segurança dedicado somente ao AWS Ground Station tráfego. Esse grupo de segurança deve permitir o tráfego de entrada UDP no mesmo intervalo de portas especificado no seu grupo de endpoints do Dataflow. AWS Ground Station mantém uma lista de prefixos gerenciada pela AWS para restringir suas permissões somente AWS Ground Station a endereços IP. Consulte as listas de prefixos gerenciados da AWS para obter detalhes sobre como substituí-las em suas regiões de implantação. PrefixListId

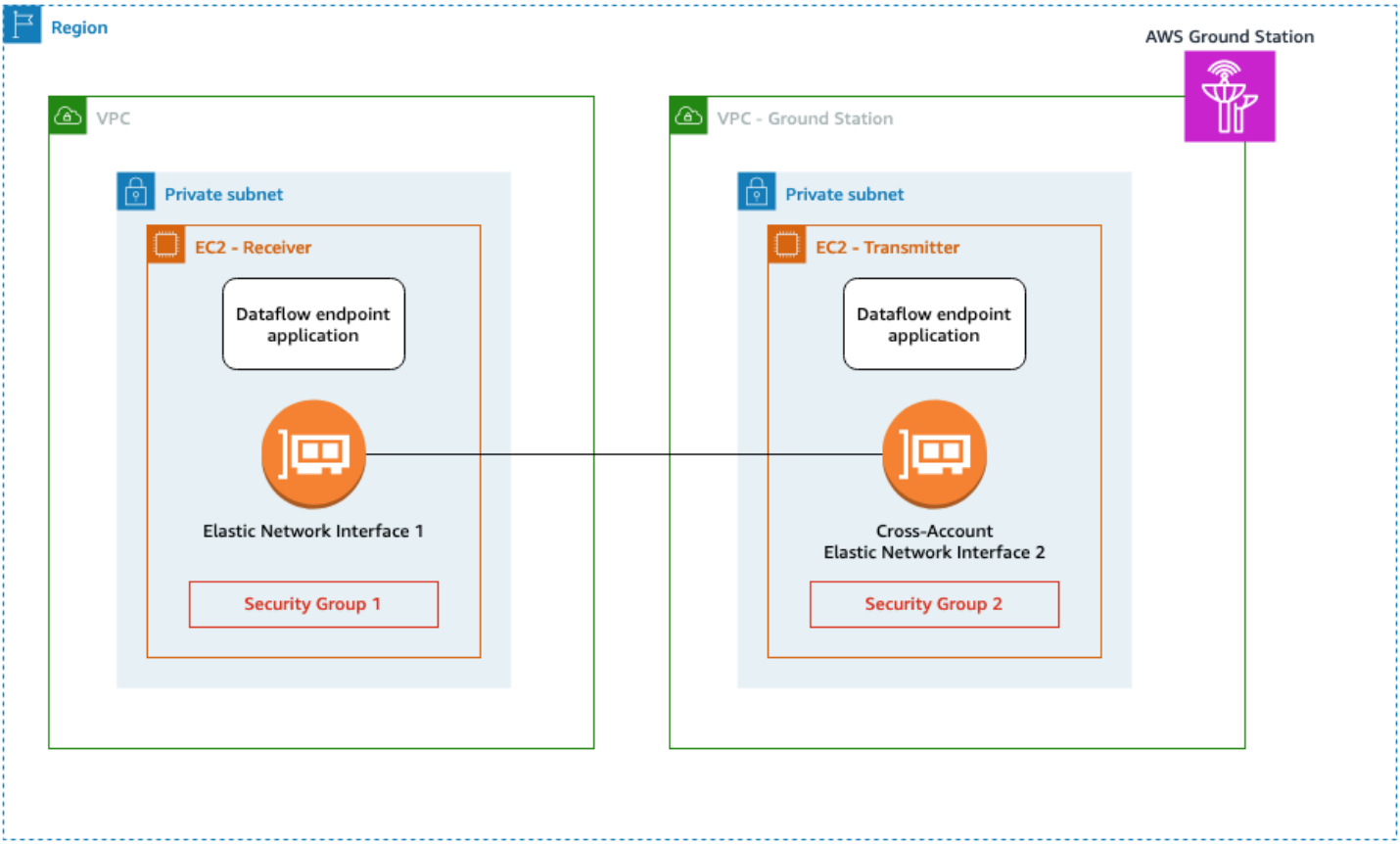
Interface de rede elástica (ENI) - Você precisará associar o grupo de segurança acima a essa ENI e colocá-la em sua sub-rede pública.

O CloudFormation modelo a seguir demonstra como criar a infraestrutura descrita nesta seção.

```
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
```

## Configuração de VPC com um endpoint de fluxo de dados




Seus dados de satélite são fornecidos a uma instância do aplicativo de endpoint de fluxo de dados que está próxima à antena. Em seguida, os dados são enviados por meio da Amazon EC2 Elastic Network Interface (ENI) entre contas de uma VPC de propriedade da. AWS Ground Station Em

seguida, os dados chegam à sua EC2 instância por meio da ENI anexada à sua EC2 instância da Amazon. O aplicativo de endpoint de fluxo de dados instalado o encaminhará para o IP e a porta especificados na configuração. O inverso desse fluxo ocorre nas conexões de uplink.

A lista abaixo destaca considerações de configuração exclusivas ao configurar sua VPC para entrega de endpoints de fluxo de dados.

Função do IAM — A função do IAM faz parte do endpoint do Dataflow e não é mostrada no diagrama. A função do IAM usada para criar e vincular a ENI entre contas à instância da AWS Ground Station Amazon EC2.

Grupo de segurança 1 - Esse grupo de segurança é anexado à ENI, que será associada à EC2 instância da Amazon em sua conta. Ele precisa permitir o tráfego UDP do Grupo de Segurança 2 nas portas especificadas em seu dataflow-endpoint-group.

Interface de rede elástica (ENI) 1 - Você precisará associar o grupo de segurança 1 a essa ENI e colocá-la em uma sub-rede.

Sub-rede - Você precisará garantir que haja pelo menos um endereço IP disponível por fluxo de dados para a EC2 instância da Amazon em sua conta. Para obter mais detalhes sobre o tamanho da sub-rede, consulte Blocos CIDR de sub-rede

Grupo de segurança 2 - Esse grupo de segurança é referenciado no Dataflow Endpoint. Esse grupo de segurança será anexado à ENI que AWS Ground Station será usada para colocar dados em sua conta.

Região - Para obter mais informações sobre as regiões suportadas para conexões entre regiões, consulteUse a entrega de dados entre regiões.

O CloudFormation modelo a seguir demonstra como criar a infraestrutura descrita nesta seção.

```
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
```

# Configurar e configurar a Amazon EC2

É necessário configurar adequadamente sua EC2 instância da Amazon para que a entrega síncrona do VITA-49 Signal/IP data or VITA-49 Extension data/IP seja entregue por meio do AWS Ground Station Agente ou de um endpoint de fluxo de dados. Dependendo de suas necessidades específicas, você pode executar o processador Front End (FE) ou o Software Defined Radio (SDR)

diretamente na mesma instância ou pode precisar utilizar EC2 instâncias adicionais. A seleção e instalação do seu FE ou SDR estão além do escopo deste guia do usuário. Para obter mais informações sobre os formatos de dados específicos, consulteAWS Ground Station interfaces de plano de dados.

Para obter informações sobre nossos termos de serviço, consulte os Termos AWS de Serviço.

## Software comum fornecido

AWS Ground Station fornece software comum para facilitar a configuração da sua EC2 instância Amazon.

### AWS Ground Station Agente

O AWS Ground Station agente recebe dados de downlink de frequência intermediária digital (DigiF) e emite dados descriptografados que permitem o seguinte:

- Capacidade de downlink do DigiF de 40 a 400 MHz de largura MHz de banda.
- Entrega de dados DigiF de alta taxa e baixa instabilidade para qualquer IP público (IP AWS elástico) na rede. AWS
- Entrega confiável de dados usando Forward Error Correction (FEC).
- Entrega segura de dados usando uma AWS KMS chave gerenciada pelo cliente para criptografia.

Para obter mais informações, consulte o Guia do usuário do AWS Ground Station agente.

### Aplicativo de endpoint Dataflow

Um aplicativo de rede usado AWS Ground Station para enviar e receber dados entre os locais da AWS Ground Station antena e suas EC2 instâncias da Amazon. Ele pode ser usado para o uplink e downlink de dados.

### Rádio definido por software (SDR)

Um rádio definido por software (SDR) que pode ser usado para modular/desmodular o sinal usado para se comunicar com seu satélite.

## AWS Ground Station Imagens de máquinas da Amazon (AMIs)

Para reduzir os tempos de construção e configuração dessas instalações, AWS Ground Station também oferece ofertas AMIs pré-configuradas. AMIs Com um aplicativo de rede de endpoint de

fluxo de dados e um rádio definido por software (SDR), são disponibilizados para sua conta após a conclusão da integração. Eles podem ser encontrados no EC2 console da Amazon pesquisando por estação terrestre em Amazon Machine Images (AMIs) privadas. Os AMIs with AWS Ground Station Agent são públicos e podem ser encontrados no EC2 console da Amazon pesquisando por groundstation em Amazon Machine Images (AMIs) públicas.

# Trabalhe com contatos

Você pode inserir dados de satélite, identificar localizações de antenas, comunicar-se e programar o horário da antena para satélites selecionados usando o AWS Ground Station console ou o AWS SDK no idioma de sua escolha. AWS CLI Você pode revisar, cancelar e reagendar reservas de contato até 15 minutos antes do início do contato*. Além disso, você pode ver os detalhes do seu plano de preços de minutos reservados se estiver usando o modelo de preços de minutos AWS Ground Station reservados.

AWS Ground Station oferece suporte à entrega de dados entre regiões. As configurações de endpoint do fluxo de dados que são parte do perfil da missão selecionado determinam para quais regiões os dados são entregues. Para obter mais informações sobre como usar a entrega de dados entre regiões, consulteUse a entrega de dados entre regiões.

Para agendar contatos, os recursos devem estar configurados. Se você não configurou seus recursos, consulteConceitos básicos. Quando ReserveContacté chamado, AWS Ground Station tira uma foto do perfil da missão e configura os recursos para uso durante a passagem de contato. As alterações nesses recursos usando o UpdateMissionProfilee não UpdateConfig APIs serão refletidas nos contatos reservados antes das atualizações. Se você precisar que as alterações de recursos sejam aplicadas a um contato já agendado, você deve primeiro cancelar o contato usando e CancelContact, em seguida, reagendá-lo usando. ReserveContact

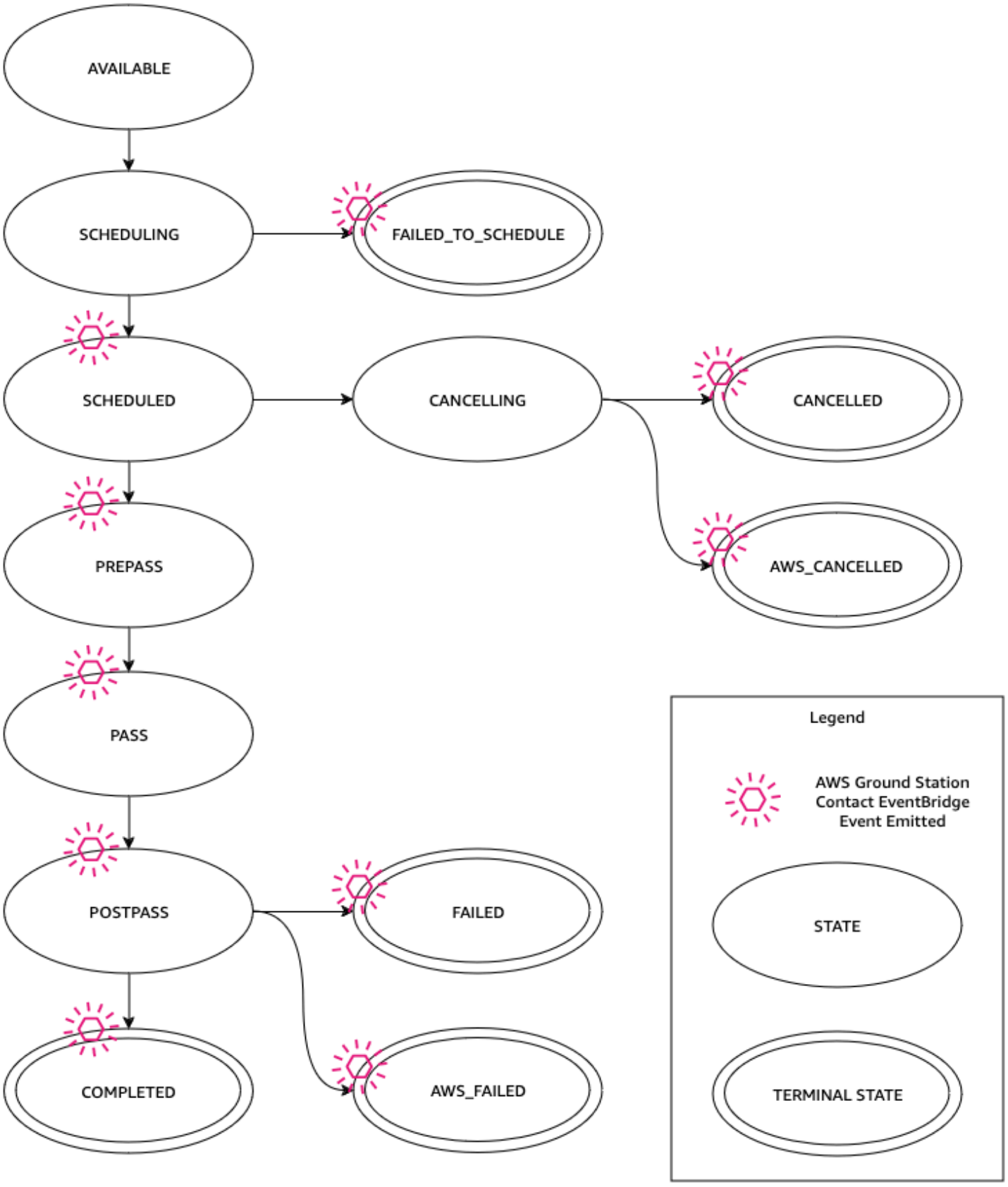
* Os contatos cancelados podem incorrer em custos quando cancelados muito perto do momento do contato. Para obter mais informações sobre contatos cancelados, consulte: Ground Station FAQs.

Tópicos



## Entenda o ciclo de vida do contato

Compreender o ciclo de vida do contato pode ajudar a determinar como configurar sua automação e durante os esforços de solução de problemas. O diagrama a seguir mostra o ciclo de vida do AWS Ground Station contato, bem como os eventos do Event Bridge emitidos durante o ciclo de vida. É importante observar que COMPLETED, FAILED, FAILED_TO_SCHEDULE, CANCELLED, AWS_CANCELLED e são estados terminais. AWS_FAILED Os contatos não sairão de um estado terminal. Consulte o AWS Ground Station status de contato para obter detalhes sobre o que cada status indica.


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 de contato

O status de um AWS Ground Station contato fornece informações sobre o que está acontecendo com esse contato em um determinado momento.

## Status de contato

A seguir está a lista de status que um contato pode ter:

- AVAILABLE: o contato está disponível para ser reservado.
- SCHEDULING: o contato está em processo de agendamento.
- SCHEDULED: o contato foi agendado com sucesso.
- FAILED_TO_SCHEDULE: o contato falhou ao agendar.
- PREPASS: o contato começará em breve e os recursos estão sendo preparados.
- PASS: o contato está sendo executado no momento e com o satélite está sendo comunicado.
- POSTPASS: a comunicação foi concluída e os recursos usados estão sendo limpos.
- CONCLUÍDO - O contato foi concluído sem erros.
- FALHA - O contato falhou devido a um problema com a configuração do recurso.
- AWS_FAILED- O contato falhou devido a um problema no AWS Ground Station serviço.
- CANCELLING: o contato está em processo de cancelamento.
- AWS_CANCELLED- O contato foi cancelado pelo AWS Ground Station serviço. A manutenção da antena ou do local e o desvio de efemérides são exemplos de quando isso pode acontecer.
- CANCELADO - O contato foi cancelado por você.

# Use o recurso de gêmeos AWS Ground Station digitais

O recurso digital twin AWS Ground Station fornece um ambiente onde você pode testar e integrar seu software de gerenciamento de missões de satélite e comando e controle. O recurso digital twin permite testar o agendamento, a verificação de configurações e o tratamento adequado de erros sem usar a capacidade da antena de produção. Testar sua AWS Ground Station integração com o recurso digital twin permite que você tenha maior confiança na capacidade do seu sistema de gerenciar suas operações de satélite sem problemas. Também permite testar AWS Ground Station APIs sem usar a capacidade de produção ou exigir licenciamento de espectro.

Para começar, sigaSatélite a bordo, solicitando a integração com o recurso de gêmeos digitais. Depois que seu satélite estiver integrado ao recurso de gêmeos digitais, você poderá agendar contatos com estações terrestres duplas digitais. A lista de estações terrestres às quais você tem acesso pode ser recuperada por meio da resposta do SDK ListGroundStationsda AWS. As estações terrestres gêmeas digitais são cópias exatas das estações terrestres listadas AWS Ground Station Localizações com um prefixo modificador para o nome da estação terrestre de “Digital Twin”. Isso inclui seus recursos de antena e metadados, incluindo, mas não se limitando a, máscara do local e coordenadas GPS reais. No momento, o recurso de gêmeos digitais não oferece suporte à entrega de dados conforme descrito emTrabalhe com fluxos de dados.

Uma vez integrado, o recurso digital twin emite os mesmos EventBridge eventos da Amazon e respostas de API que o serviço de produção, conforme descrito em. Automatize AWS Ground Station com eventos Esses eventos permitirão que você ajuste suas configurações e grupos de endpoints de fluxo de dados.

# Entenda o monitoramento com AWS Ground Station

O monitoramento é uma parte importante para manter a confiabilidade, a disponibilidade e o desempenho do AWS Ground Station. A AWS fornece as seguintes ferramentas de monitoramento para observar AWS Ground Station, relatar quando algo está errado e realizar ações automáticas quando apropriado.

- A Amazon EventBridge Events fornece um fluxo quase em tempo real de eventos do sistema que descrevem mudanças nos AWS recursos. EventBridge Os eventos permitem a computação automatizada baseada em eventos, pois você pode criar regras que observam determinados eventos e acionam ações automatizadas em outros AWS serviços quando esses eventos acontecem. Para obter mais informações sobre EventBridge eventos, consulte o Guia do usuário do Amazon EventBridge Events.
- AWS CloudTrailcaptura chamadas de API e eventos relacionados feitos por ou em nome de sua AWS conta e entrega os arquivos de log para um bucket do Amazon S3 que você especificar. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem a partir do qual as chamadas foram feitas e quando elas ocorreram. Para obter mais informações sobre AWS CloudTrail, consulte o Guia AWS CloudTrail do usuário.
- O Amazon CloudWatch Metrics captura métricas para seus contatos agendados durante o uso AWS Ground Station. CloudWatch As métricas permitem que você analise dados com base em seu canal, polarização e ID de satélite para identificar a intensidade do sinal e os erros em seus contatos. Para obter mais informações, consulte Usando CloudWatch métricas da Amazon.
- A AWS Notificações de Usuários pode ser usada para configurar canais de entrega para receber notificações sobre AWS Ground Station eventos. Você recebe uma notificação quando um evento corresponde a uma regra especificada. É possível receber notificações para eventos por meio de diversos canais, incluindo o e-mail, o Amazon Q Developer em aplicações de chat, notificações por chat ou notificações push do AWS Console Mobile Application. Você também pode ver as notificações na Central de Notificações do AWS Console. Notificações de Usuários agregação de suporte, que pode reduzir o número de notificações que você recebe durante eventos específicos.

Use os seguintes tópicos para monitorar o AWS Ground Station.

Tópicos

- Automatize AWS Ground Station com eventos
- Registre chamadas de AWS Ground Station API com AWS CloudTrail

- Veja métricas com a Amazon CloudWatch

# Automatize AWS Ground Station com eventos

> **Note**
>
> Este documento usa o termo “evento” por toda parte. CloudWatch Eventos e EventBridge são o mesmo serviço e API subjacentes. Regras para corresponder a eventos de entrada e roteá-los para destinos para processamento podem ser construídas usando qualquer um dos serviços.

Os eventos permitem que você automatize seus AWS serviços e responda automaticamente aos eventos do sistema, como problemas de disponibilidade de aplicativos ou alterações de recursos. Os eventos dos AWS serviços são entregues quase em tempo real. Você pode escrever regras simples para indicar quais eventos são do seu interesse, e as ações automatizadas a serem tomadas quando um evento corresponder à regra. Algumas das ações que podem ser acionadas automaticamente incluem o seguinte:

- Invocando uma função AWS Lambda
- Invocando o EC2 comando Amazon Run
- Transmitir o evento Amazon Kinesis Data Streams
- Ativando uma máquina de AWS Step Functions estado
- Notificar um tópico do Amazon SNS ou uma fila do Amazon SQS

Alguns exemplos de uso de eventos com AWS Ground Station incluem:

- Invocar uma função Lambda para automatizar o início e a interrupção de instâncias da EC2 Amazon com base no estado do evento.
- Publicar um tópico do Amazon SNS sempre que ocorre uma mudança de estado em um contato. Esses tópicos podem ser configurados para enviar avisos por e-mail no início ou no final dos contatos.

Para obter mais informações, consulte o Guia do usuário do Amazon EventBridge Events.

# AWS Ground Station Tipos de eventos

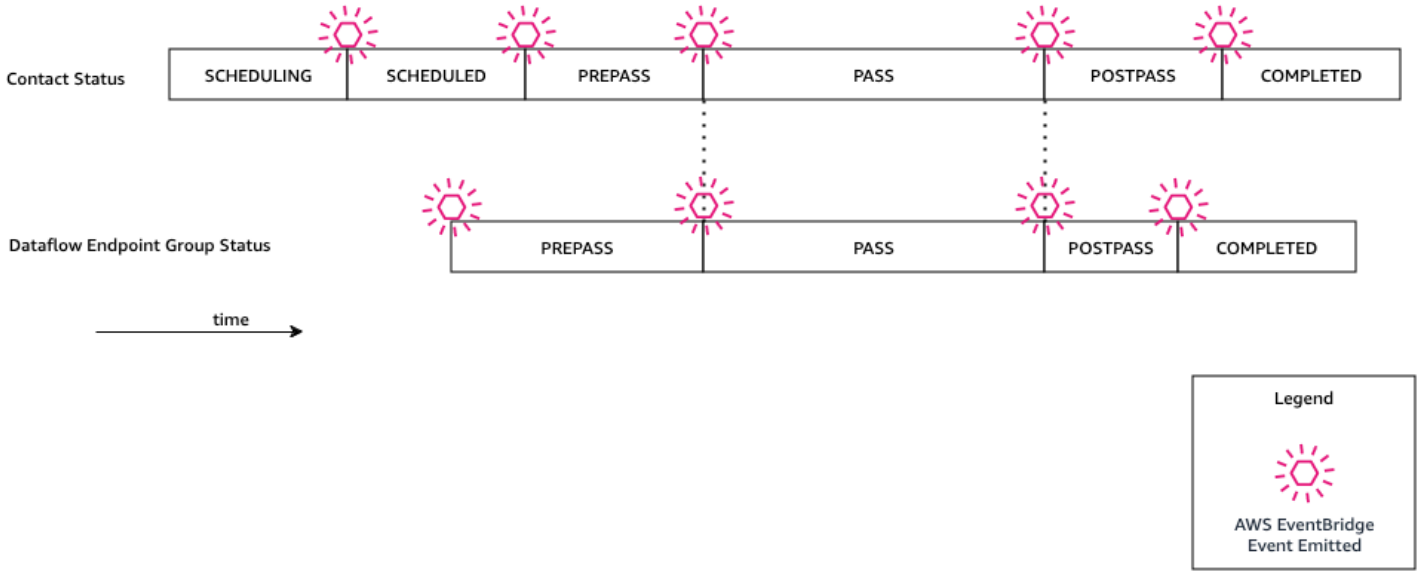
> **Note**
>
> Todos os eventos gerados pelo AWS Ground Station têm “aws.groundstation” como valor para “fonte”.

AWS Ground Station emite eventos relacionados a mudanças de estado para apoiar sua capacidade de personalizar sua automação. Atualmente, AWS Ground Station oferece suporte a eventos de mudança de estado de contato, eventos de alteração de grupos de endpoints de fluxo de dados e eventos de mudança de estado de efemérides. As seções a seguir fornecem informações detalhadas sobre cada tipo.

## Cronograma do evento de contato

AWS Ground Station emite eventos quando seu contato muda de estado. Para obter mais informações sobre quais são essas mudanças de estado e o que os próprios estados significam, consulteEntenda o ciclo de vida do contato. Todos os grupos de endpoints de fluxo de dados usados em seu contato têm um conjunto independente de eventos que também são emitidos. Durante esse mesmo período, também emitimos eventos para seu grupo de endpoints de fluxo de dados. O horário exato dos eventos de pré-passagem e pós-passagem pode ser configurado por você à medida que configura o perfil da missão e o grupo de endpoints do fluxo de dados.

O diagrama a seguir mostra os status e os eventos emitidos por um contato nominal e seu grupo de endpoints de fluxo de dados associado.




Alteração de estado do contato do Ground Station

Se você quiser realizar uma ação específica quando um contato futuro estiver mudando de estado, você pode configurar uma regra para automatizar essa ação. Isso é útil quando quiser receber notificações sobre as alterações de estado do contato. Se você quiser mudar quando receber esses eventos, você pode modificar o perfil da sua missão contactPrePassDurationSeconds contactPostPassDurationSeconds e. Os eventos são enviados para a região na qual o contato foi agendado.

Um exemplo de evento é fornecido abaixo.

```
{
    "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"
    }
}
```

Os possíveis valores para `contactStatus` são definidos em the section called “AWS Ground Station status de contato”.

Alteração de estado do grupo de endpoints do fluxo de dados do Ground Station

Se você quiser executar uma ação quando seu grupo de endpoints de fluxo de dados está sendo usado para receber dados, pode configurar uma regra para automatizar essa ação. Isso permitirá executar ações diferentes em resposta à alteração de estados do status do grupo de endpoints do fluxo de dados. Se você quiser alterar a data de recebimento desses eventos, use um grupo de endpoints de fluxo de dados com diferentes e. contactPrePassDurationSecondscontactPostPassDurationSeconds Esse evento será enviado para a região do grupo de endpoints do fluxo de dados.

Um exemplo é fornecido abaixo.

```
{
    "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"
    }
}
```

Os possíveis estados do `dataflowEndpointGroupState` incluem `PREPASS`, `PASS`, `POSTPASS` e `COMPLETED`.

## Eventos de efemérides

Mudança de estado da efeméride Ground Station

Se você quiser executar uma ação específica quando uma efeméride estiver mudando de estado, é possível configurar uma regra para automatizar essa ação. Isso permite que você execute ações diferentes em resposta à mudança de estado de uma efeméride. Por exemplo, você pode realizar uma ação quando uma efeméride tiver concluído a validação, e agora está `ENABLED`. A notificação desse evento será enviada para a região onde a efeméride foi enviada.

Um exemplo é fornecido abaixo.

```
{
    "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"
```

```
    }
}
```

Os possíveis estados do `ephemerisStatus` incluem `ENABLED`, `VALIDATING`, `INVALID ERROR`, `DISABLED` e `EXPIRED`

# Registre chamadas de AWS Ground Station API com AWS CloudTrail

AWS Ground Station é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço em AWS Ground Station. CloudTrail captura todas as chamadas de API AWS Ground Station como eventos. As chamadas capturadas incluem chamadas do AWS Ground Station console e chamadas de código para as operações AWS Ground Station da API. Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para. AWS Ground Station Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita AWS Ground Station, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para saber mais sobre isso CloudTrail, consulte o Guia AWS CloudTrail do usuário.

## AWS Ground Station Informações em CloudTrail

CloudTrail é ativado em sua AWS conta quando você cria a conta. Quando a atividade ocorre em AWS Ground Station, essa atividade é registrada em um CloudTrail evento junto com outros eventos AWS de serviço no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes em sua AWS conta. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos.

Para um registro contínuo dos eventos em sua AWS conta, incluindo eventos para AWS Ground Station, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as regiões da AWS. A trilha registra eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para obter mais informações, consulte:

- Visão Geral para Criar uma Trilha
- CloudTrail Serviços e integrações compatíveis
- Configurando notificações do Amazon SNS para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões e recebendo arquivos de CloudTrail log de várias contas

Todas AWS Ground Station as ações são registradas CloudTrail e documentadas na Referência da AWS Ground Station API. Por exemplo, chamadas para o `ReserveContact` `CancelContact` e `ListConfigs` as ações geram entradas nos arquivos de CloudTrail log.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar o seguinte:

- Se a solicitação foi feita com credenciais de usuário root ou AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado.
- Se a solicitação foi feita por outro AWS serviço.

Para obter mais informações, consulte Elemento userIdentity do CloudTrail .

## Entendendo as entradas do arquivo de AWS Ground Station log

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a `ReserveContact` ação.

Exemplo: 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"
```

```
}
```

# Veja métricas com a Amazon CloudWatch

Durante um contato, captura e envia dados AWS Ground Station automaticamente CloudWatch para análise. Seus dados podem ser visualizados no CloudWatch console da Amazon. Para obter mais informações sobre acesso e CloudWatch métricas, consulte Usando o Amazon CloudWatch Metrics.

## AWS Ground Station Métricas e dimensões

### Quais métricas estão disponíveis?

As métricas a seguir estão disponíveis em AWS Ground Station.

> **Note**
>
> As métricas específicas emitidas dependem dos AWS Ground Station recursos que estão sendo usados. Dependendo da sua configuração, somente um subconjunto das métricas abaixo pode ser emitido.

| Métrica | Dimensões da métrica | Descrição |
| --- | --- | --- |
| `AzimuthAngle` | SatelliteId | O ângulo de azimute da antena. O norte verdadeiro é 0 graus e o leste é 90 graus.<br><br>Unidades: graus |
| `BitErrorRate` | Canal, polarização, SatelliteId | A taxa de erros irrecuperáveis em bits, em um determina do número de transmissões |

| Métrica | Dimensões da métrica | Descrição |
| --- | --- | --- |
| | | de bits. Erros de bits são gerados por ruídos, distorções ou interferências<br><br>Unidades: erros de bits por unidade de tempo |
| `BlockErrorRate` | Canal, polarização, SatelliteId | A taxa de erros de blocos em um determina do número de blocos recebidos . Erros de blocos são causados por interferência.<br><br>Unidades: blocos com erros/núm ero total de blocos |
| `CarrierFrequencyRe covery_Cn0` | Categoria, Config, SatelliteId | Relação entre portadora e densidade de ruído por unidade de largura de banda.<br><br>Unidades: Decibel-hertz (dB-Hz) |

| Métrica | Dimensões da métrica | Descrição |
| --- | --- | --- |
| `CarrierFrequencyRecovery_Locked` | Categoria, Config, SatelliteId | Defina como 1 quando o loop de recuperação da frequência portadora do demodulador estiver bloqueado e 0 quando desbloqueado.<br><br>Unidades: sem unidades |
| `CarrierFrequencyRecovery_OffsetFrequency_Hz` | Categoria, Config, SatelliteId | O deslocamento entre o centro estimado do sinal e a frequência central ideal. Isso é causado pelo deslocamento Doppler e pelo deslocamento do oscilador local entre a espaçonave e o sistema de antenas.<br><br>Unidades: hertz (Hz) |

| Métrica | Dimensões da métrica | Descrição |
| --- | --- | --- |
| `ElevationAngle` | SatelliteId | O ângulo de elevação da antena. O horizonte é 0 graus e o zênite é 90 graus.<br><br>Unidades: graus |
| `Es/N0` | Canal, polarização, SatelliteId | A razão entre a energia por símbolo e a densidade espectral da potência sonora.<br><br>Unidades: decibéis (dB) |
| `ReceivedPower` | Polarização, SatelliteId | A intensidade do sinal medida no demodulador/decodificador.<br><br>Unidades: dBm (decibéis miliwatts) |

| Métrica | Dimensões da métrica | Descrição |
| --- | --- | --- |
| `SymbolTimingRecovery_ErrorVectorMagnitude` | Categoria, Config, SatelliteId | A magnitude do vetor de erro entre os símbolos recebidos e os pontos ideais da constelação.<br><br>Unidades: percentual |
| `SymbolTimingRecovery_Locked` | Categoria, Config, SatelliteId | Defina como 1 quando o loop de recuperação da frequência portadora do demodulador estiver bloqueado e 0 quando desbloqueado<br><br>Unidades: sem unidades |

| Métrica | Dimensões da métrica | Descrição |
| --- | --- | --- |
| `SymbolTimingRecovery_OffsetSymbolRate` | Categoria, Config, SatelliteId | O deslocamento entre a taxa de símbolo estimada e a taxa de símbolo de sinal ideal. Isso é causado pelo deslocamento Doppler e pelo deslocamento do oscilador local entre a espaçonave e o sistema de antenas.<br><br>Unidades: símbolos/segundo |

## Para quais dimensões são usadas AWS Ground Station?

Você pode filtrar AWS Ground Station dados usando as seguintes dimensões.

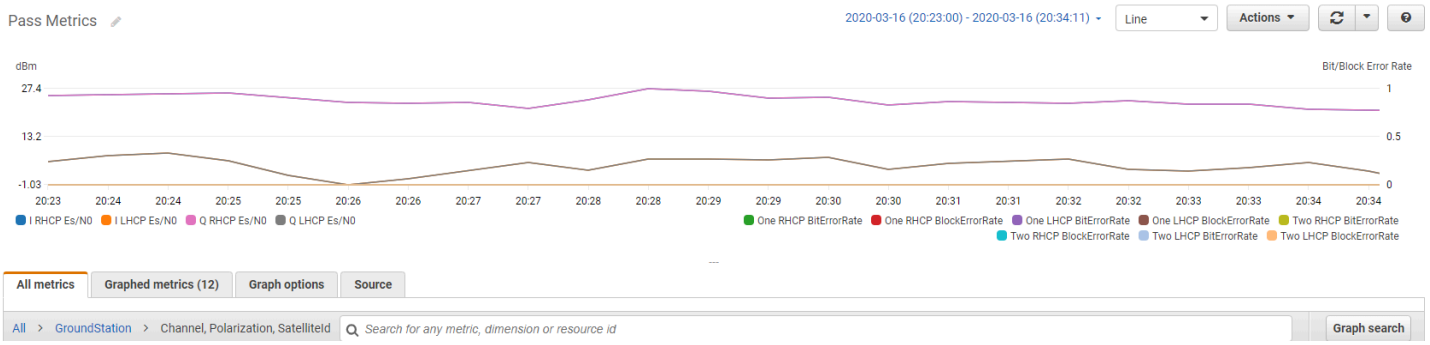
| Dimensão | Descrição |
| --- | --- |
| `Category` | Demodulação ou decodificação. |
| `Channel` | Os canais para cada contato incluem Um, Dois, I (em fase) e Q (quadratura). |
| `Config` | Um comando de configuração de decodificação de demod de downlink de antena. |

| Dimensão | Descrição |
| --- | --- |
| `Polarization` | A polarização para cada contato inclui PCE (Polarização circular à esquerda) ou PCD (Polarização circular à direita). |
| `SatelliteId` | O ID do satélite contém o ARN do satélite para seus contatos. |

## Visualizar métricas

Ao visualizar as métricas gráficas, é importante observar que a janela de agregação determina como as métricas serão exibidas. As métricas em um contato podem ser exibidas como dados por segundo por um período de três horas após os dados serem recebidos. Seus dados serão agregados pelo CloudWatch Metrics como dados por minuto após o término desse período de 3 horas. Se você precisar visualizar suas métricas em uma medição de dados por segundo, é recomendável visualizá-los dentro do período de 3 horas após o recebimento dos dados ou persisti-los fora das CloudWatch Métricas. Para obter mais informações sobre CloudWatch retenção, consulte CloudWatch Conceitos da Amazon - Retenção métrica.

Além disso, os dados capturados dentro dos primeiros 60 segundos não conterão informações suficientes para gerar métricas significativas e provavelmente não serão exibidos. Para visualizar métricas significativas, recomenda-se visualizar os dados após 60 segundos.

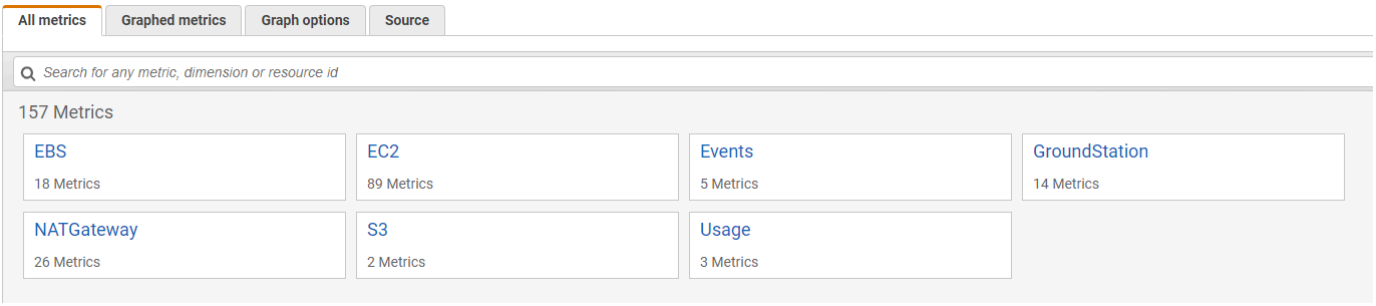



Para obter mais informações sobre a representação gráfica de AWS Ground Station métricas em CloudWatch, consulte Representação gráfica de métricas.

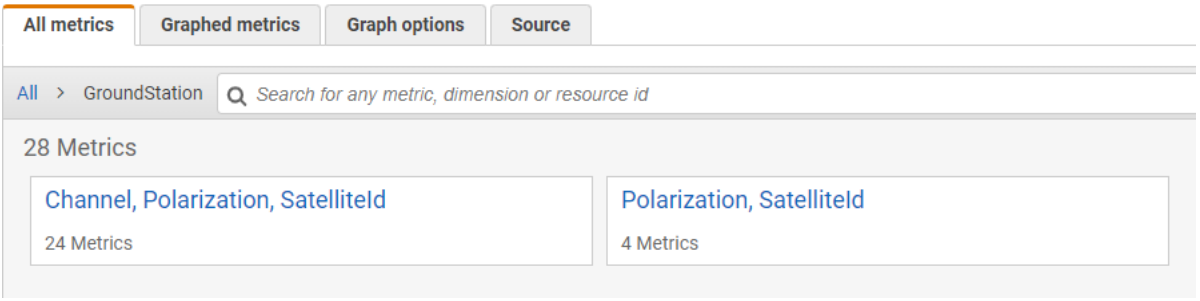
### Para visualizar as métricas usando o console

1. Abra o console de CloudWatch .

2. No painel de navegação, selecione Métricas.
3. Selecione o namespace GroundStation.




4. Selecione as dimensões métricas desejadas (por exemplo, Canal, Polarização SatelliteId).




5. A guia Todas as métricas exibe todas as métricas dessa dimensão no namespace. Você pode fazer o seguinte:

   a. Para classificar a tabela, use o cabeçalho da coluna.

   b. Para representar graficamente uma métrica, marque a caixa de seleção associada à métrica. Para selecionar todas as métricas, marque a caixa de seleção na linha de cabeçalho da tabela.

   c. Para filtrar por recurso, escolha o ID do recurso e, em seguida, escolha Adicionar à pesquisa.

   d. Para filtrar por métrica, selecione o nome da métrica e, em seguida, escolha Adicionar à pesquisa.

## Para visualizar métricas usando AWS CLI

1. Certifique-se de que AWS CLI esteja instalado. Para obter informações sobre a instalação AWS CLI, consulte Instalação da AWS CLI versão 2.

2. Use o get-metric-datamétodo da CloudWatch CLI para gerar um arquivo que pode ser modificado para especificar as métricas nas quais você está interessado e, em seguida, ser usado para consultar essas métricas.

   Para fazer isso, execute o seguinte:`aws cloudwatch get-metric-data --generate-cli-skeleton`. Isso gerará uma saída semelhante a:

```
{
   "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. Liste as CloudWatch métricas disponíveis executando`aws cloudwatch list-metrics`.

   Se você usou recentemente AWS Ground Station, o método deve retornar uma saída que contém entradas como:

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

   > **Note**
   >
   > Devido a uma limitação de CloudWatch, se já passaram mais de duas semanas desde a última vez que você usou AWS Ground Station, você precisará inspecionar manualmente a tabela de métricas disponíveis para encontrar os nomes e dimensões das métricas no namespace da `AWS/GroundStation` métrica. Para obter mais informações sobre a CloudWatch limitação, consulte: Exibir métricas disponíveis

4. Modifique o arquivo JSON que você criou na etapa 2 para corresponder aos valores necessários da etapa 3, por exemplo`SatelliteId`, e `Polarization` de suas métricas. Além disso, certifique-se de atualizar os `EndTime` valores`StartTime`, e para que correspondam ao seu contato. Por exemplo:

```
        {
           "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 publica métricas a cada 1 a 60 segundos, dependendo da métrica. As métricas não serão retornadas se o `Period` campo tiver um valor menor que o período de publicação da métrica.

5. Execute `aws cloudwatch get-metric-data` com o arquivo de configuração criado nas etapas anteriores. Um exemplo é fornecido abaixo.

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

As métricas serão fornecidas com marca temporal do contato. Um exemplo de saída de AWS Ground Station métricas é fornecido abaixo.


```
{
   "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": []
}
```

# Segurança em AWS Ground Station

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficiará de uma arquitetura de data center e rede criada para atender aos requisitos das organizações mais sensíveis à segurança. A AWS oferece ferramentas e recursos específicos para segurança e para ajudar você a atender seus objetivos de segurança. Essas ferramentas e recursos incluem segurança de rede, gerenciamento de configurações, controle de acesso e segurança de dados.

Ao usar AWS Ground Station, recomendamos que você siga as melhores práticas do setor e implemente a end-to-end criptografia. A AWS permite APIs que você integre criptografia e proteção de dados. Para obter mais informações sobre AWS segurança, consulte o whitepaper Introdução à segurança da AWS.

Use os tópicos a seguir para saber como proteger seus recursos do .

Tópicos



# Identity and Access Management para AWS Ground Station

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) a usar AWS Ground Station os recursos. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

- Como AWS Ground Station funciona com o IAM
- Exemplos de políticas baseadas em identidade para AWS Ground Station
- Solução de problemas AWS Ground Station de identidade e acesso

## Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz AWS Ground Station.

Usuário do serviço — Se você usar o AWS Ground Station serviço para realizar seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você usa mais AWS Ground Station recursos para fazer seu trabalho, talvez precise de permissões adicionais. Entender como o acesso é gerenciado pode ajudá-lo a solicitar as permissões corretas ao seu administrador. Se não for possível acessar um atributo no AWS Ground Station, consulte Solução de problemas AWS Ground Station de identidade e acesso.

Administrador de serviços — Se você é responsável pelos AWS Ground Station recursos da sua empresa, provavelmente tem acesso total AWS Ground Station a. É seu trabalho determinar quais AWS Ground Station recursos e recursos seus usuários do serviço devem acessar. Envie as solicitações ao administrador do IAM para alterar as permissões dos usuários de serviço. Revise as informações nesta página para compreender os conceitos básicos do IAM. Para saber mais sobre como sua empresa pode usar o IAM com AWS Ground Station, consulteComo AWS Ground Station funciona com o IAM.

Administrador do IAM: se você for um administrador do IAM, talvez queira saber detalhes sobre como pode gravar políticas para gerenciar acesso ao AWS Ground Station. Para ver exemplos de políticas AWS Ground Station baseadas em identidade que você pode usar no IAM, consulte. Exemplos de políticas baseadas em identidade para AWS Ground Station

## Autenticar com identidades

A autenticação é como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como o Usuário raiz da conta da AWS, como usuário do IAM ou assumindo uma função do IAM.

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Usuários (IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos

de identidades federadas. Quando você faz login como identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login em AWS, consulte Como fazer login Conta da AWS no Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para designar solicitações por conta própria, consulte Versão 4 do AWS Signature para solicitações de API no Guia do usuário do IAM.

Independente do método de autenticação usado, também pode ser necessário fornecer informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Autenticação multifator no Guia do usuário do AWS IAM Identity Center e Usar a autenticação multifator da AWS no IAM no Guia do usuário do IAM.

### Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário-raiz para tarefas diárias. Proteja as credenciais do usuário-raiz e use-as para executar as tarefas que somente ele puder executar. Para obter a lista completa das tarefas que exigem login como usuário-raiz, consulte Tarefas que exigem credenciais de usuário-raiz no Guia do Usuário do IAM.

### Identidade federada

Como prática recomendada, exija que usuários humanos, incluindo usuários que precisam de acesso de administrador, usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório de usuários corporativo, de um provedor de identidade da web AWS Directory Service, do diretório do Identity Center ou de qualquer usuário que acesse usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade.

Quando as identidades federadas são acessadas Contas da AWS, elas assumem funções, e as funções fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, é recomendável usar o AWS IAM Identity Center. Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas da AWS aplicativos. Para obter mais informações sobre o Centro de Identidade do IAM, consulte O que é o Centro de Identidade do IAM? no Guia do Usuário do AWS IAM Identity Center .

## Usuários e grupos do IAM

Um usuário do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, é recomendável contar com credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, é recomendável alternar as chaves de acesso. Para obter mais informações, consulte Alternar as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo no Guia do Usuário do IAM.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdminse conceder a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Casos de uso para usuários do IAM no Guia do usuário do IAM.

## Perfis do IAM

Uma função do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Para assumir temporariamente uma função do IAM no AWS Management Console, você pode alternar de um usuário para uma função do IAM (console). Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando uma URL personalizada. Para obter mais informações sobre métodos para usar perfis, consulte Métodos para assumir um perfil no Guia do usuário do IAM.

Perfis do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, é possível criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas por ele. Para ter mais informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidade de terceiros (federação) no Guia do usuário do IAM. Se usar o Centro de Identidade do IAM, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o Centro de Identidade do IAM correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de Permissões no Guia do Usuário do AWS IAM Identity Center .
- Permissões temporárias para usuários do IAM: um usuário ou um perfil do IAM pode presumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas: é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para conhecer a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.
- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos na Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões da entidade principal da chamada, usando um perfil de serviço ou um perfil vinculado ao serviço.
  - Sessões de acesso direto (FAS) — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado o principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Sessões de acesso direto.
  - Perfil de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.

- Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir o perfil de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para perfis vinculados ao serviço.

- Aplicativos em execução na Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma EC2 instância e fazendo solicitações AWS CLI de AWS API. Isso é preferível a armazenar chaves de acesso na EC2 instância. Para atribuir uma AWS função a uma EC2 instância e disponibilizá-la para todos os aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém a função e permite que os programas em execução na EC2 instância recebam credenciais temporárias. Para obter mais informações, consulte Usar uma função do IAM para conceder permissões a aplicativos executados em EC2 instâncias da Amazon no Guia do usuário do IAM.

## Gerenciar o acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e perfis não têm permissões. Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem assumir os perfis.

As políticas do IAM definem permissões para uma ação independentemente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função da AWS Management Console AWS CLI, da ou da AWS API.

## Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

## Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o atributo ao qual a política está anexada, a política define quais ações uma entidade principal especificado pode executar nesse atributo e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

## Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

O Amazon S3 e o AWS WAF Amazon VPC são exemplos de serviços que oferecem suporte. ACLs Para saber mais ACLs, consulte a visão geral da lista de controle de acesso (ACL) no Guia do desenvolvedor do Amazon Simple Storage Service.

## Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões: um limite de permissões é um recurso avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.
- Políticas de controle de serviço (SCPs) — SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em AWS Organizations. AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os recursos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as suas contas. O SCP limita as permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre Organizations e SCPs, consulte Políticas de controle de serviços no Guia AWS Organizations do Usuário.
- Políticas de controle de recursos (RCPs) — RCPs são políticas JSON que você pode usar para definir o máximo de permissões disponíveis para recursos em suas contas sem atualizar as políticas do IAM anexadas a cada recurso que você possui. O RCP limita as permissões para recursos nas contas dos membros e pode afetar as permissões efetivas para identidades, incluindo a Usuário raiz da conta da AWS, independentemente de pertencerem à sua organização. Para obter mais informações sobre Organizations e RCPs, incluindo uma lista Serviços da AWS desse suporte RCPs, consulte Políticas de controle de recursos (RCPs) no Guia AWS Organizations do usuário.
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em recursos. Uma negação explícita em qualquer uma dessas políticas

substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia do usuário do IAM.

### Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte Lógica de avaliação de políticas no Guia do usuário do IAM.

## Como AWS Ground Station funciona com o IAM

Antes de usar o IAM para gerenciar o acesso AWS Ground Station, saiba com quais recursos do IAM estão disponíveis para uso AWS Ground Station.

Recursos do IAM que você pode usar com AWS Ground Station

| Atributo do IAM | AWS Ground Station apoio |
|---|---|
| Políticas baseadas em identidade | Sim |
| Políticas baseadas em recurso | Não |
| Ações de políticas | Sim |
| Recursos de políticas | Sim |
| Chaves de condição de política (específicas do serviço) | Sim |
| ACLs | Não |
| ABAC (tags em políticas) | Sim |
| Credenciais temporárias | Sim |
| Permissões de entidade principal | Sim |
| Perfis de serviço | Não |

| Atributo do IAM | AWS Ground Station apoio |
| --- | --- |
| Funções vinculadas ao serviço | Sim |

Para ter uma visão de alto nível de como AWS Ground Station e outros AWS serviços funcionam com a maioria dos recursos do IAM, consulte AWS os serviços que funcionam com o IAM no Guia do usuário do IAM.

## Políticas baseadas em identidade para AWS Ground Station

Compatível com políticas baseadas em identidade: sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário do IAM, grupo de usuários ou perfil. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações e recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou perfil ao qual ela está anexada. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elemento de política JSON do IAM no Guia do usuário do IAM.

Exemplos de políticas baseadas em identidade para AWS Ground Station

Para ver exemplos de políticas AWS Ground Station baseadas em identidade, consulte. Exemplos de políticas baseadas em identidade para AWS Ground Station

## Políticas baseadas em recursos dentro AWS Ground Station

Compatibilidade com políticas baseadas em recursos: não

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico.

Para o atributo ao qual a política está anexada, a política define quais ações uma entidade principal especificado pode executar nesse atributo e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Para permitir o acesso entre contas, você pode especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em recursos. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso são diferentes Contas da AWS, um administrador do IAM na conta confiável também deve conceder permissão à entidade principal (usuário ou função) para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a uma entidade principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Consulte mais informações em Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

## Ações políticas para AWS Ground Station

Compatível com ações de políticas: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Action` de uma política JSON descreve as ações que podem ser usadas para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da operação de AWS API associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista de AWS Ground Station ações, consulte Ações definidas por AWS Ground Station na Referência de Autorização de Serviço.

As ações de política AWS Ground Station usam o seguinte prefixo antes da ação:

```
groundstation
```

Para especificar várias ações em uma única declaração, separe-as com vírgulas.

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

Para ver exemplos de políticas AWS Ground Station baseadas em identidade, consulte. Exemplos de políticas baseadas em identidade para AWS Ground Station

## Recursos políticos para AWS Ground Station

Compatível com recursos de políticas: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem compatibilidade com permissões em nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

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

Para ver uma lista dos tipos de AWS Ground Station recursos e seus ARNs, consulte Recursos definidos por AWS Ground Station na Referência de Autorização de Serviço. Para saber com quais ações é possível especificar o ARN de cada atributo, consulte Ações definidas pelo AWS Ground Station.

Para ver exemplos de políticas AWS Ground Station baseadas em identidade, consulte. Exemplos de políticas baseadas em identidade para AWS Ground Station

## Chaves de condição de política para AWS Ground Station

Compatível com chaves de condição de política específicas de serviço: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Condition` (ou bloco `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos de `Condition` em uma declaração ou várias chaves em um único elemento de `Condition`, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma `OR` operação lógica. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um recurso somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos da política do IAM: variáveis e tags no Guia do usuário do IAM.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

Para ver uma lista de chaves de AWS Ground Station condição, consulte Chaves de condição AWS Ground Station na Referência de autorização de serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte Ações definidas por AWS Ground Station.

Para ver exemplos de políticas AWS Ground Station baseadas em identidade, consulte. Exemplos de políticas baseadas em identidade para AWS Ground Station

## ACLs in AWS Ground Station

Suportes ACLs: Não

As listas de controle de acesso (ACLs) controlam quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

## ABAC com AWS Ground Station

Compatível com ABAC (tags em políticas): sim

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define as permissões com base em atributos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a entidades do IAM (usuários ou funções) e a vários AWS recursos. Marcar de entidades e atributos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso que ela estiver tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações em que o gerenciamento de políticas se torna um problema.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* ou chaves de condição `aws:TagKeys`.

Se um serviço for compatível com as três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço for compatível com as três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para obter mais informações sobre o ABAC, consulte Definir permissões com autorização do ABAC no Guia do usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Usar controle de acesso baseado em atributos (ABAC) no Guia do usuário do IAM.

## Usando credenciais temporárias com AWS Ground Station

Compatível com credenciais temporárias: sim

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS trabalhar com o IAM no Guia do usuário do IAM.

Você está usando credenciais temporárias se fizer login AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar funções, consulte Alternar para um perfil do IAM (console) no Guia do usuário do IAM.

Você pode criar manualmente credenciais temporárias usando a AWS API AWS CLI ou. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para obter mais informações, consulte Credenciais de segurança temporárias no IAM.

## Permissões principais entre serviços para AWS Ground Station

Compatibilidade com o recurso de encaminhamento de sessões de acesso (FAS): sim

Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado um principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Sessões de acesso direto.

## Funções de serviço para AWS Ground Station

Compatível com perfis de serviço: não

O perfil de serviço é um perfil do IAM que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.

> **Warning**
>
> Alterar as permissões de uma função de serviço pode interromper AWS Ground Station a funcionalidade. Edite as funções de serviço somente quando AWS Ground Station fornecer orientação para fazer isso.

## Funções vinculadas a serviços para AWS Ground Station

Compatibilidade com perfis vinculados a serviços: sim

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir o perfil de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para funções vinculadas ao serviço.

Para obter detalhes sobre como criar ou gerenciar perfis vinculados a serviços, consulte Serviços da AWS que funcionam com o IAM. Encontre um serviço na tabela que inclua um `Yes` na coluna Perfil vinculado ao serviço. Escolha o link Sim para visualizar a documentação do perfil vinculado a serviço desse serviço.

## Exemplos de políticas baseadas em identidade para AWS Ground Station

Por padrão, usuários e perfis não têm permissão para criar ou modificar recursos do AWS Ground Station . Eles também não podem realizar tarefas usando a AWS API AWS Management Console, AWS Command Line Interface (AWS CLI) ou. Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem assumir os perfis.

Para aprender a criar uma política baseada em identidade do IAM ao usar esses documentos de política em JSON de exemplo, consulte Criar políticas do IAM (console) no Guia do usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos por AWS Ground Station, incluindo o formato do ARNs para cada um dos tipos de recursos, consulte Ações, recursos e chaves de condição AWS Ground Station na Referência de Autorização de Serviço.

Tópicos

- Práticas recomendadas de política
- Usar o console do AWS Ground Station
- Permitir que os usuários visualizem suas próprias permissões

### Práticas recomendadas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir AWS Ground Station recursos em sua conta. Essas ações podem incorrer em custos para sua Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e passe para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso.

Para obter mais informações, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para funções de trabalho no Guia do usuário do IAM.

- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como AWS CloudFormation. Para obter mais informações, consulte Elementos da política JSON do IAM: condição no Guia do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de cem verificações de política e recomendações práticas para ajudar a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação de políticas do IAM Access Analyzer no Guia do Usuário do IAM.
- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte Configuração de acesso à API protegido por MFA no Guia do Usuário do IAM.

Para obter mais informações sobre as práticas recomendadas do IAM, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

## Usar o console do AWS Ground Station

Para acessar o AWS Ground Station console, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os AWS Ground Station recursos em seu Conta da AWS. Caso crie uma política baseada em identidade mais restritiva que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para a API AWS CLI ou para a AWS API. Em vez disso, permita o acesso somente a ações que correspondam à operação de API que estiverem tentando executar.

Para garantir que usuários e funções ainda possam usar o AWS Ground Station console, anexe também a política AWS Ground Station *ConsoleAccess* ou a política *ReadOnly* AWS gerenciada às entidades. Para obter informações, consulte Adicionar permissões a um usuário no Guia do usuário do IAM.

## Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como criar uma política que permita que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando a API AWS CLI ou 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": "*"
        }
    ]
}
```

## Solução de problemas AWS Ground Station de identidade e acesso

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com AWS Ground Station um IAM.

Tópicos

- Não estou autorizado a realizar uma ação em AWS Ground Station
- Não estou autorizado a realizar iam: PassRole
- Quero permitir que pessoas fora da minha Conta da AWS acessem meus AWS Ground Station recursos

### Não estou autorizado a realizar uma ação em AWS Ground Station

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, suas políticas deverão ser atualizadas para permitir que você realize a ação.

O erro do exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para visualizar detalhes sobre um atributo *`my-example-widget`* fictício, mas não tem as permissões `groundstation:`*`GetWidget`* fictícias.

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

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao recurso *`my-example-widget`* usando a ação `groundstation:`*`GetWidget`*.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

## Não estou autorizado a realizar iam: PassRole

Se você receber uma mensagem de erro informando que não está autorizado a executar a ação `iam:PassRole`, as suas políticas devem ser atualizadas para permitir que você passe uma função para o AWS Ground Station.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazê-lo, você deve ter permissões para passar o perfil para o serviço.

O exemplo de erro a seguir ocorre quando uma usuária do IAM chamada `marymajor` tenta utilizar o console para executar uma ação no AWS Ground Station. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

## Quero permitir que pessoas fora da minha Conta da AWS acessem meus AWS Ground Station recursos

É possível criar um perfil que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. É possível especificar quem é confiável para assumir o perfil. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se é AWS Ground Station compatível com esses recursos, consulteComo AWS Ground Station funciona com o IAM.
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Como fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui no Guia do usuário do IAM.

- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como fornecer acesso Contas da AWS a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para conhecer a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

# AWS políticas gerenciadas para AWS Ground Station

Uma política AWS gerenciada é uma política autônoma criada e administrada por AWS. AWS as políticas gerenciadas são projetadas para fornecer permissões para muitos casos de uso comuns, para que você possa começar a atribuir permissões a usuários, grupos e funções.

Lembre-se de que as políticas AWS gerenciadas podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque elas estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo as políticas gerenciadas pelo cliente que são específicas para seus casos de uso.

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que atualize uma política AWS gerenciada quando uma nova AWS service (Serviço da AWS) é lançada ou novas operações de API são disponibilizadas para serviços existentes.

Para obter mais informações, consulte Políticas gerenciadas pela AWS no Guia do usuário do IAM.

## AWS política gerenciada: AWSGround StationAgentInstancePolicy

É possível anexar a política `AWSGroundStationAgentInstancePolicy` às identidades do IAM.

Essa política concede permissões de AWS Ground Station agente à sua EC2 instância da Amazon, permitindo que a instância envie e receba dados durante os contatos da Ground Station. Todas as permissões nesta política são do serviço Ground Station.

Detalhes das permissões

Esta política inclui as seguintes permissões.

- `groundstation`— Permite que instâncias de endpoint de fluxo de dados chamem o Ground Station Agent. APIs

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

## AWS política gerenciada: AWSService RoleForGroundStationDataflowEndpointGroupPolicy

Você não pode se associar AWSService RoleForGroundStationDataflowEndpointGroupPolicy às suas entidades do IAM. Essa política está vinculada a uma função vinculada ao serviço que permite AWS Ground Station realizar ações em seu nome. Para mais informações, consulte Como usar funções vinculadas a serviços.

Essa política concede EC2 permissões que AWS Ground Station permitem encontrar IPv4 endereços públicos.

Detalhes das permissões

Esta política inclui as seguintes permissões.

- `ec2:DescribeAddresses`— AWS Ground Station Permite listar todos os IPs associados EIPs em seu nome.
- `ec2:DescribeNetworkInterfaces`— Permite AWS Ground Station obter informações sobre as interfaces de rede associadas às EC2 instâncias em seu nome.

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

## AWS Ground Station atualizações nas políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas AWS Ground Station desde que esse serviço começou a rastrear essas alterações. Para receber alertas automáticos sobre alterações nessa página, assine o feed RSS na página Histórico do AWS Ground Station documento.

| Alteração | Descrição | Data |
| --- | --- | --- |
| AWSGroundStationAgentInstancePolicy – Nova política | AWS Ground Station adicionou uma nova política para fornecer à instância do endpoint do fluxo de dados permissões para usar o AWS Ground Station Agent. | 12 de abril de 2023 |
| AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy – Nova política | AWS Ground Station adicionou uma nova política que concede EC2 permissões AWS Ground Station para permitir encontrar IPv4 endereços públicos associados EIPs e interfaces de rede associadas às EC2 instâncias. | 2 de novembro de 2022 |
| AWS Ground Station começou a rastrear as alterações | AWS Ground Station começou a rastrear as alterações nas políticas AWS gerenciadas. | 1 de março de 2021 |

# Use funções vinculadas a serviços para Ground Station

AWS Ground Station usa funções vinculadas ao serviço AWS Identity and Access Management (IAM). A função vinculada ao serviço é um tipo exclusivo de perfil do IAM vinculada diretamente ao Ground Station. As funções vinculadas ao serviço são predefinidas pela Ground Station e incluem todas as permissões que o serviço exige para ligar para outros AWS serviços em seu nome.

Uma função vinculada ao serviço facilita a configuração do Ground Station porque você não precisa adicionar as permissões necessárias manualmente. O Ground Station define as permissões das funções vinculadas ao serviço e, exceto se definido de outra forma, somente o Ground Station pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões, e essa política não pode ser anexada a nenhuma outra entidade do IAM.

Para obter informações sobre outros serviços que oferecem suporte a funções vinculadas a serviços, consulte AWS Serviços que funcionam com IAM e procure os serviços que têm Sim na coluna

Funções vinculadas ao serviço. Escolha Sim com um link para visualizar a documentação da função vinculada a esse serviço.

## Permissões de perfil vinculado a serviço para o Ground Station

A Ground Station usa a função vinculada ao serviço chamada — A AWSServiceRoleForGroundStationDataflowEndpointGroupAWS GroundStation usa essa função vinculada ao serviço para invocar e encontrar endereços públicos EC2 . IPv4

A função AWSService RoleForGroundStationDataflowEndpointGroup vinculada ao serviço confia nos seguintes serviços para assumir a função:

- `groundstation.amazonaws.com`

A política de permissões de função denominada AWSService RoleForGroundStationDataflowEndpointGroupPolicy permite que a Ground Station conclua as seguintes ações nos recursos especificados:

- Ação: `ec2:DescribeAddresses` em `all AWS resources (*)`

  A ação permite que a Ground Station liste todos os IPs associados EIPs a.
- Ação: `ec2:DescribeNetworkInterfaces` em `all AWS resources (*)`

  A ação permite que a Ground Station obtenha informações sobre as interfaces de rede associadas às EC2 instâncias

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua um perfil vinculado a serviço. Para obter mais informações, consulte Permissões de função vinculada a serviços no Guia do usuário do IAM.

## Criar uma função vinculada a serviços para o Ground Station

Não é necessário criar manualmente um perfil vinculado ao serviço. Quando você cria um DataflowEndpointGroup na AWS CLI ou na AWS API, o Ground Station cria a função vinculada ao serviço para você.

Se excluir esse perfil vinculado ao serviço e precisar criá-lo novamente, será possível usar esse mesmo processo para recriar o perfil em sua conta. Quando você cria um DataflowEndpointGroup, o Ground Station cria a função vinculada ao serviço para você novamente.

Você também pode usar o console do IAM para criar uma função vinculada ao serviço com o caso de EC2 uso de entrega de dados para a Amazon. Na AWS CLI ou na AWS API, crie uma função vinculada ao serviço com o nome do `groundstation.amazonaws.com` serviço. Para obter mais informações, consulte Criar uma função vinculada ao serviço no Manual do usuário do IAM. Se você excluir essa função vinculada ao serviço, será possível usar esse mesmo processo para criar a função novamente.

## Criar uma função vinculada a serviços para o Ground Station

O Ground Station não permite que você edite a função AWSService RoleForGroundStationDataflowEndpointGroup vinculada ao serviço. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, será possível editar a descrição do perfil usando o IAM. Para obter mais informações, consulte Editar uma função vinculada a serviço no Guia do usuário do IAM.

## Apagar uma função vinculada a serviços para o Ground Station

Se você não precisar mais usar um atributo ou serviço que requer uma função vinculada a serviço, é recomendável excluí-la. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida.

Você pode excluir uma função vinculada ao serviço somente após primeiro excluí-la DataflowEndpointGroups usando a função vinculada ao serviço. Isso protege você de revogar inadvertidamente as permissões do seu. DataflowEndpointGroups Se uma função vinculada ao serviço for usada com várias DataflowEndpointGroups, você deverá excluir todas as DataflowEndpointGroups que usam a função vinculada ao serviço antes de excluí-la.

> **Note**
>
> Se o serviço Ground Station estiver usando a função quando você tenta excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Para excluir os recursos da Ground Station usados pelo AWSService RoleForGroundStationDataflowEndpointGroup

- Exclua DataflowEndpointGroups por meio da AWS CLI ou da API da AWS.

Como excluir manualmente o perfil vinculado ao serviço usando o IAM

Use o console do IAM AWS CLI, o ou a AWS API para excluir a função AWSService RoleForGroundStationDataflowEndpointGroup vinculada ao serviço. Para obter mais informações, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

## Regiões compatíveis com funções vinculadas ao serviço do Ground Station

O Ground Station oferece suporte a perfis vinculados ao serviço em todas as regiões em que o serviço está disponível. Para obter mais informações, consulte a Tabela de regiões.

## Solução de problemas

`NOT_AUTHORIZED_TO_CREATE_SLR`- Isso indica que a função em sua conta que está sendo usada para chamar a CreateDataflowEndpointGroup API não tem a `iam:CreateServiceLinkedRole` permissão. Um administrador com a permissão `iam:CreateServiceLinkedRole` deve criar manualmente a função vinculada ao serviço para sua conta.

# Criptografia de dados em repouso para AWS Ground Station

AWS Ground Station fornece criptografia por padrão para proteger seus dados confidenciais em repouso usando chaves AWS de criptografia próprias.

- Chaves de propriedade da AWS — AWS Ground Station usa essas chaves por padrão para criptografar automaticamente dados e efemérides pessoais diretamente identificáveis. Você não pode visualizar, gerenciar ou usar chaves de propriedade da AWS nem auditar seu uso; no entanto, não é necessário realizar nenhuma ação ou alterar programas para proteger as chaves que criptografam os dados. Para obter mais informações, consulte Chaves de propriedade da AWS no Guia do desenvolvedor da AWS Key Management Service.

A criptografia de dados em repouso por padrão reduz a sobrecarga operacional e a complexidade envolvidas na proteção de dados confidenciais. Ao mesmo tempo, permite que você crie aplicativos seguros que atendam aos rigorosos requisitos regulatórios e de conformidade de criptografia.

AWS Ground Station impõe criptografia em todos os dados confidenciais em repouso. No entanto, para alguns AWS Ground Station recursos, como efemérides, você pode optar por usar uma chave gerenciada pelo cliente no lugar das chaves gerenciadas padrão. AWS

- Chaves gerenciadas pelo cliente -- AWS Ground Station suporta o uso de uma chave simétrica gerenciada pelo cliente que você cria, possui e gerencia para adicionar uma segunda camada de criptografia sobre a criptografia existente AWS . Como você tem controle total dessa camada de criptografia, você pode realizar tarefas como:
  - Estabelecer e manter as políticas de chave
  - Estabelecer e manter subsídios e IAM policies
  - Habilitar e desabilitar políticas de chaves
  - Alternar os materiais de criptografia de chave
  - Adicionar etiquetas
  - Criar réplicas de chaves
  - Chaves de agendamento para exclusão

  Para obter mais informações, consulte Chave gerenciada pelo cliente no Guia do desenvolvedor da AWS Key Management Service.

A tabela a seguir resume os recursos que oferecem AWS Ground Station suporte ao uso de Chaves Gerenciadas pelo Cliente

| Tipo de dados | Criptografia de chave própria da AWS | Criptografia de chave gerenciada pelo cliente (opcional) |
|---|---|---|
| Dados de efemérides usados para calcular a trajetória de um satélite | Habilitada | Habilitado |

> **Note**
>
> AWS Ground Station ativa automaticamente a criptografia em repouso usando chaves AWS próprias para proteger dados de identificação pessoal sem nenhum custo. No entanto, as cobranças do AWS KMS se aplicam ao uso de uma chave gerenciada pelo cliente. Para obter informações sobre a definição de preço, consulte Definição de preço do serviço de gerenciamento de chaves da AWS.

Para obter mais informações sobre o AWS KMS, consulte o Guia do desenvolvedor do AWS KMS.

## Como AWS Ground Station usa subsídios no AWS KMS

AWS Ground Station exige uma concessão de chave para usar sua chave gerenciada pelo cliente.

Quando você carrega uma efeméride criptografada com uma chave gerenciada pelo cliente, AWS Ground Station cria uma concessão de chave em seu nome enviando uma CreateGrant solicitação ao KMS. AWS As concessões no AWS KMS são usadas para dar AWS Ground Station acesso a uma chave KMS na sua conta.

AWS Ground Station exige que a concessão use sua chave gerenciada pelo cliente para as seguintes operações internas:

- Envie GenerateDataKeysolicitações ao AWS KMS para gerar chaves de dados criptografadas pela chave gerenciada pelo cliente.
- Envie solicitações de descriptografia ao AWS KMS para descriptografar as chaves de dados criptografadas para que elas possam ser usadas para criptografar seus dados.
- Envie solicitações de criptografia ao AWS KMS para criptografar os dados fornecidos.

É possível revogar o acesso à concessão, ou remover o acesso do serviço à chave gerenciada pelo cliente a qualquer momento. Se você fizer isso, AWS Ground Station não conseguirá acessar nenhum dos dados criptografados pela chave gerenciada pelo cliente, o que afeta as operações que dependem desses dados. Por exemplo, se você remover uma concessão de chave de uma efeméride atualmente em uso para um contato, não AWS Ground Station poderá usar os dados de efemérides fornecidos para apontar a antena durante o contato. Isso fará com que o contato termine em um estado de FALHA.

## Criar uma chave gerenciada pelo cliente

Você pode criar uma chave simétrica gerenciada pelo cliente usando o AWS Management Console ou o AWS APIs KMS.

### Para criar uma chave simétrica gerenciada pelo cliente

Siga as etapas para criar uma chave simétrica gerenciada pelo cliente no Guia do desenvolvedor do AWS Key Management Service.

## Política de chave

As políticas de chaves controlam o acesso à chave gerenciada pelo cliente. Cada chave gerenciada pelo cliente deve ter exatamente uma política de chaves, que contém declarações que determinam quem pode usar a chave e como pode usá-la. Ao criar a chave gerenciada pelo cliente, é possível especificar uma política de chave. Para obter mais informações, consulte Gerenciando o acesso às chaves gerenciadas pelo cliente no Guia do desenvolvedor do AWS Key Management Service.

Para usar sua chave gerenciada pelo cliente com seus AWS Ground Station recursos, as seguintes operações de API devem ser permitidas na política de chaves:

`kms:CreateGrant`: adiciona uma concessão a uma chave gerenciada pelo cliente. Concede acesso de controle a uma chave KMS especificada, o que permite o acesso AWS Ground Station necessário às operações de concessão. Para obter mais informações sobre o uso de concessões, consulte o Guia do desenvolvedor do AWS Key Management Service.

Isso permite que AWS a Amazon faça o seguinte:

- Ligar para GenerateDataKey para gerar uma chave de dados criptografada e armazená-la, porque a chave de dados não é usada imediatamente para criptografar.
- Chame o Decrypt para usar a chave de dados criptografada armazenada para acessar os dados criptografados.
- Chame Encrypt para usar a chave de dados para criptografar dados.
- Configure uma entidade principal aposentada para permitir que o serviço para `RetireGrant`.

`kms:DescribeKey`- Fornece os detalhes da chave gerenciada pelo cliente AWS Ground Station para permitir a validação da chave antes de tentar criar uma concessão com a chave fornecida.

A seguir estão exemplos de declarações de política do IAM que você pode adicionar para 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" : "*"
  }
]
```

Para obter mais informações sobre a especificação de permissões em uma política, consulte o Guia do desenvolvedor do AWS Key Management Service.

Para obter mais informações sobre como solucionar problemas de acesso à chave, consulte o Guia do desenvolvedor do AWS Key Management Service.

# Especificando uma chave gerenciada pelo cliente para AWS Ground Station

Você pode especificar uma chave gerenciada pelo cliente para fornecer criptografia para os seguintes recursos:

- Efemérides

Ao criar um recurso, você pode especificar a chave de dados fornecendo um kmsKeyArn

- kmsKeyArn- Um identificador de chave para uma chave gerenciada pelo cliente do AWS KMS

## AWS Ground Station contexto de criptografia

Um contexto de criptografia é um conjunto opcional de pares chave-valor que pode conter informações contextuais adicionais sobre os dados. AWS O KMS usa o contexto de criptografia como dados autenticados adicionais para oferecer suporte à criptografia autenticada. Quando você inclui um contexto de criptografia em uma solicitação para criptografar dados, o AWS KMS vincula o contexto de criptografia aos dados criptografados. Para descriptografar os dados, você inclui o mesmo contexto de criptografia na solicitação.

### AWS Ground Station contexto de criptografia

AWS Ground Station usa o contexto de criptografia diferente dependendo do recurso que está sendo criptografado e especifica um contexto de criptografia específico para cada concessão de chave criada.

### Contexto de criptografia de efemérides:

A concessão de chaves para criptografar efemérides: os recursos estão vinculados a um ARN de satélite específico

```
"encryptionContext": {
    "aws:groundstation:arn":
 "arn:aws:groundstation::111122223333:satellite/00a770b0-082d-45a4-80ed-SAMPLE"
}
```

> **Note**
>
> As doações de chaves são reutilizadas para o mesmo par chave-satélite.

## Usar o contexto de criptografia para monitoramento

Quando você usa uma chave simétrica gerenciada pelo cliente para criptografar suas efemérides, também pode utilizar o contexto de criptografia em registros de auditoria e logs para identificar como a chave gerenciada pelo cliente está sendo utilizada. O contexto de criptografia também aparece nos registros gerados pelo AWS CloudTrail ou Amazon CloudWatch Logs.

## Uso do contexto de criptografia para controlar o acesso à chave gerenciada pelo cliente

Você pode usar o contexto de criptografia nas políticas de chaves e políticas do IAM como `conditions` e controlar o acesso à sua chave simétrica gerenciada pelo cliente. Você também pode usar restrições no contexto de criptografia em uma concessão.

AWS Ground Station usa uma restrição de contexto de criptografia nas concessões para controlar o acesso à chave gerenciada pelo cliente em sua conta ou região. A restrição da concessão exige que as operações permitidas pela concessão usem o contexto de criptografia especificado.

Veja a seguir exemplos de declarações de políticas de chave para conceder acesso a uma chave gerenciada pelo cliente para um contexto de criptografia específico. A condição nesta declaração de política exige que as concessões tenham uma restrição de contexto de criptografia que especifique o contexto de criptografia.

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

## Monitorando suas chaves de criptografia para AWS Ground Station

Ao usar uma chave gerenciada pelo cliente do AWS KMS com seus AWS Ground Station recursos, você pode usar AWS CloudTrailnossos CloudWatch registros da Amazon para rastrear solicitações AWS Ground Station enviadas ao AWS KMS. Os exemplos a seguir são AWS CloudTrail eventos para`CreateGrant`, `GenerateDataKeyDecrypt`, `Encrypt` e `DescribeKey` para monitorar operações KMS chamadas pela AWS Ground Station para acessar dados criptografados pela chave gerenciada pelo cliente.

### **`CreateGrant`** (Cloudtrail)

Quando você usa uma chave gerenciada pelo cliente do AWS KMS para criptografar seus recursos de efemérides, AWS Ground Station envia uma `CreateGrant` solicitação em seu nome para acessar a chave KMS em sua conta. AWS A concessão AWS Ground Station criada é específica para o recurso associado à chave gerenciada pelo cliente do AWS KMS. Além disso, o AWS Ground Station usa a `RetireGrant` operação para remover uma concessão quando você exclui um recurso.

O evento de exemplo a seguir registra a operação `CreateGrant`:

```
{
    "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)

Quando você usa uma chave gerenciada pelo cliente do AWS KMS para criptografar seus recursos de efemérides, AWS Ground Station envia uma `DescribeKey` solicitação em seu nome para validar se a chave solicitada existe em sua conta.

O evento de exemplo a seguir registra a operação `DescribeKey`:

```
{
    "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)

Quando você usa uma chave gerenciada pelo cliente do AWS KMS para criptografar seus recursos de efemérides, AWS Ground Station envia uma `GenerateDataKey` solicitação ao KMS para gerar uma chave de dados com a qual criptografar seus dados.

O evento de exemplo a seguir registra a operação `GenerateDataKey`:

```
{
    "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)

Quando você usa uma chave gerenciada pelo cliente do AWS KMS para criptografar seus recursos de efemérides, AWS Ground Station usa a `Decrypt` operação para descriptografar as efemérides fornecidas se já estiverem criptografadas com a mesma chave gerenciada pelo cliente. Por exemplo, se uma efeméride estiver sendo carregada de um bucket do S3 e for criptografada nesse bucket com uma determinada chave.

O evento de exemplo a seguir registra a operação `Decrypt`:

```
{
    "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"
}
```

# Criptografia de dados durante o trânsito para AWS Ground Station

AWS Ground Station fornece criptografia por padrão para proteger seus dados confidenciais durante o trânsito. Os dados podem ser transmitidos entre as localizações das AWS Ground Station antenas e suas EC2 instâncias da Amazon de duas maneiras, dependendo da configuração do perfil da missão.

- AWS Ground Station Agente
- Endpoint de fluxo de dados

Cada método de streaming de dados lida com a criptografia de dados em trânsito de forma diferente. As seções a seguir descrevem cada método.

## AWS Ground Station Fluxos de agentes

AWS Ground Station O agente criptografa seus fluxos usando chaves gerenciadas pelo AWS KMS cliente. O AWS Ground Station agente em execução na sua EC2 instância da Amazon descriptografará automaticamente o stream para fornecer dados descriptografados.

A AWS KMS chave usada para criptografar um fluxo é especificada ao criar um `MissionProfile` no streamsKmsKeyparâmetro. Todas as permissões que concedem AWS Ground Station acesso às chaves são tratadas por meio da política de AWS KMS chaves anexada a. `streamsKmsKey`

## Streams de endpoint de fluxo de dados

Os fluxos de endpoint do Dataflow são criptografados usando o Datagram Transport Layer Security (DTLS). Isso é feito usando certificados autoassinados e não requer configuração adicional.

# Exemplo de configurações de perfil de missão

Os exemplos fornecidos mostram como pegar um satélite de transmissão pública e criar um perfil de missão que o suporte. Os modelos resultantes são fornecidos para ajudá-lo a estabelecer um contato público por satélite de transmissão e para ajudá-lo a tomar decisões sobre seus satélites.

Tópicos



## JPSS-1 - Satélite de transmissão pública (PBS) - Avaliação

Esta seção de exemplo corresponde aoVisão geral do processo de integração de clientes. Ele fornece uma breve análise de compatibilidade AWS Ground Station e prepara o terreno para os exemplos específicos a seguir.

Conforme mencionado na Satélites de transmissão pública seção, você pode utilizar satélites selecionados, ou caminhos de comunicação de um satélite, que estão disponíveis publicamente. Nesta seção, descrevemos o JPSS-1 nos termos. AWS Ground Station Para referência, utilizamos o Joint Polar Satellite System 1 (JPSS-1) Spacecraft High Rate Data (HRD) para Direct Broadcast Stations (DBS) Documento de Controle de Interface (ICD) de Radiofrequência (RF) para concluir o exemplo. Além disso, vale ressaltar que o JPSS-1 está associado ao NORAD ID 43013.

O satélite JPSS-1 oferece um uplink e três caminhos de comunicação diretos de downlink, conforme visto na Figura 1-1 do ICD. Desses quatro caminhos de comunicação, somente o único caminho de comunicação de downlink de dados de alta taxa (HRD) está disponível para consumo público. Com base nisso, você verá que esse caminho também terá dados muito mais específicos associados a ele. Os quatro caminhos são os seguintes:

- Caminho de comando (uplink) na frequência MHz central de 2067,27 com uma taxa de dados de 2 a 128 kbps. Esse caminho não está acessível ao público.

- Caminho de telemetria (downlink) na frequência MHz central de 2247,5 com uma taxa de dados de 1-524 kbps. Esse caminho não está acessível ao público.
- Caminho SMD (downlink) na frequência GHz central de 26.7034 com uma taxa de dados de 150-300 Mbps. Esse caminho não está acessível ao público.
- A RF para o caminho do HRD (downlink) na frequência MHz central de 7812 com uma taxa de dados de 15 Mbps. Tem uma MHz largura de banda de 30%, e é right-hand-circular-polarized. Quando você integra o JPSS-1 com AWS Ground Station, esse é o caminho de comunicação ao qual você tem acesso. Esse caminho de comunicação contém dados científicos de instrumentos, dados de engenharia de instrumentos, dados de telemetria de instrumentos e dados de manutenção de espaçonaves em tempo real.

Ao compararmos os possíveis caminhos de dados, vemos que os caminhos de comando (uplink), telemetria (downlink) e HRD (downlink) atendem aos recursos de frequência, largura de banda e uso simultâneo multicanal do. AWS Ground Station O caminho SMD não é compatível porque a frequência central está fora do alcance dos receptores existentes. Para obter mais informações sobre os recursos suportados, consulteAWS Ground Station Capacidades do site.

> **Note**
>
> Como o caminho SMD não é compatível com AWS Ground Station ele, ele não será representado nas configurações de exemplo.

> **Note**
>
> Como os caminhos de comando (uplink) e telemetria (downlink) não estão definidos no ICD, nem estão disponíveis para uso público, os valores fornecidos quando usados são nocionais.

## Satélite de transmissão pública utilizando a entrega de dados do Amazon S3

Este exemplo se baseia na análise feita na JPSS-1 - Satélite de transmissão pública (PBS) - Avaliação seção do guia do usuário.

Neste exemplo, você precisará assumir um cenário: capturar o caminho de comunicação do HRD como frequência intermediária digital e armazená-lo para processamento em lote no futuro. Isso economiza as amostras brutas de quadratura em fase (I/Q) de radiofrequência (RF) após a digitalização. Quando os dados estiverem em seu bucket do Amazon S3, você poderá demodular e decodificar os dados usando qualquer software que desejar. Consulte o MathWorks Tutorial para obter um exemplo detalhado de processamento. Depois de usar esse exemplo, você pode considerar a adição de componentes de preços à EC2 vista da Amazon para processar os dados e reduzir seus custos gerais de processamento.

## Caminhos de comunicação

Esta seção representa Planeje seus caminhos de comunicação de fluxo de dados como começar.

Todos os trechos de modelo a seguir pertencem à seção Recursos do AWS CloudFormation modelo.

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

> **Note**
>
> Para obter mais informações sobre o conteúdo de um AWS CloudFormation modelo, consulte as seções Modelo.

Considerando nosso cenário para fornecer um único caminho de comunicação para o Amazon S3, você sabe que terá um único caminho de entrega assíncrono. De acordo com a Entrega assíncrona de dados seção, você deve definir um bucket do 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]]]]]]
```

Além disso, você precisará criar as funções e políticas apropriadas AWS Ground Station para permitir o uso do 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 configurações

Esta seção representa Crie configurações como começar.

Você precisará de uma configuração de rastreamento para definir sua preferência de uso do autotrack. Selecionar PREFERRED como trilha automática pode melhorar a qualidade do sinal, mas não é necessário atender à qualidade do sinal devido à qualidade suficiente das efemérides JPSS-1.

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

Com base no caminho de comunicação, você precisará definir uma configuração de downlink de antena para representar a parte do satélite, bem como uma gravação s3 para se referir ao bucket Amazon S3 que você acabou de criar.

```
 # 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 perfil da missão

Esta seção representa Crie um perfil de missão como começar.

Agora que você tem as configurações associadas, pode usá-las para criar o fluxo de dados. Você usará os padrões para os demais parâmetros.

```
 # 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
```

## Juntando tudo

Com os recursos acima, agora você tem a capacidade de agendar contatos JPSS-1 para entrega assíncrona de dados a partir de qualquer um dos seus contatos integrados. AWS Ground Station [AWS Ground Station Localizações]

A seguir está um AWS CloudFormation modelo completo que inclui todos os recursos descritos nesta seção combinados em um único modelo que pode ser usado diretamente em AWS CloudFormation.

O AWS CloudFormation modelo nomeado `AquaSnppJpss-1TerraDigIfS3DataDelivery.yml` contém um bucket Amazon S3 e os AWS Ground Station recursos necessários para agendar contatos e receber dados de transmissão direta de sinal/IP VITA-49.

Se Aqua, SNPP, JPSS-1/NOAA-20 e Terra não estiverem integrados à sua conta, consulte. [Satélite a bordo]

> **Note**
>
> Você pode acessar o modelo acessando o bucket Amazon S3 de integração do cliente usando AWS credenciais válidas. Os links abaixo usam um bucket regional do Amazon S3. Altere o código da `us-west-2` região para representar a região correspondente na qual você deseja criar a AWS CloudFormation pilha.
> Além disso, as instruções a seguir usam YAML. No entanto, os modelos estão disponíveis no formato YAML ou JSON. Para usar o JSON, substitua a extensão do `.yml` arquivo por `.json` ao baixar o modelo.

Para baixar o modelo usando AWS CLI, use o seguinte comando:

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

É possível visualizar e fazer download do modelo no console navegando até o seguinte URL no seu navegador:

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

Você pode especificar o modelo diretamente AWS CloudFormation usando o seguinte link:

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

# Satélite de transmissão pública utilizando um ponto final de fluxo de dados (banda estreita)

Este exemplo se baseia na análise feita na JPSS-1 - Satélite de transmissão pública (PBS) - Avaliação seção do guia do usuário.

Para concluir este exemplo, você precisará assumir um cenário: capturar o caminho de comunicação do HRD como frequência intermediária digital (DigIF) e processá-lo conforme ele é recebido por um aplicativo de endpoint de fluxo de dados em uma instância da EC2 Amazon usando um SDR.

## Caminhos de comunicação

Esta seção representa Planeje seus caminhos de comunicação de fluxo de dados como começar. Neste exemplo, você criará duas seções em seu AWS CloudFormation modelo: seções de parâmetros e recursos.

> **Note**
>
> Para obter mais informações sobre o conteúdo de um AWS CloudFormation modelo, consulte as seções Modelo.

Para a seção Parâmetros, você adicionará os seguintes parâmetros. Você especificará valores para eles ao criar a pilha por meio do AWS CloudFormation console.

```
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**
>
> Você precisa criar um par de chaves e fornecer o nome para o EC2 `EC2Key` parâmetro Amazon. Consulte Criar um par de chaves para sua EC2 instância da Amazon.
> Além disso, você precisará fornecer a ID de AMI específica da região correta ao criar a AWS CloudFormation pilha. Consulte AWS Ground Station Imagens de máquinas da Amazon (AMIs).

Os trechos de modelo restantes pertencem à seção Recursos do AWS CloudFormation modelo.

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

Dado nosso cenário para fornecer um único caminho de comunicação para uma EC2 instância, você terá um único caminho de entrega síncrono. De acordo com a Entrega síncrona de dados seção, você deve instalar e configurar uma EC2 instância da Amazon com um aplicativo de endpoint de fluxo de dados e criar um ou mais grupos de endpoints de fluxo de dados.

```
  # 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
```

Além disso, você também precisará criar as políticas e funções apropriadas AWS Ground Station para permitir a criação de uma interface de rede elástica (ENI) em sua conta.

```
  # 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 configurações

Esta seção representa Crie configurações como começar.

Você precisará de uma configuração de rastreamento para definir sua preferência de uso do autotrack. Selecionar PREFERRED como trilha automática pode melhorar a qualidade do sinal, mas não é necessário atender à qualidade do sinal devido à qualidade suficiente das efemérides JPSS-1.

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

Com base no caminho de comunicação, você precisará definir uma configuração de antena-downlink para representar a parte do satélite, bem como uma configuração de endpoint de fluxo de dados para se referir ao grupo de endpoints de fluxo de dados que define os detalhes do endpoint.

```
  # 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 perfil da missão

Esta seção representa Crie um perfil de missão como começar.

Agora que você tem as configurações associadas, pode usá-las para criar o fluxo de dados. Você usará os padrões para os demais parâmetros.

```
 # 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
```

## Juntando tudo

Com os recursos acima, agora você tem a capacidade de agendar contatos JPSS-1 para entrega síncrona de dados a partir de qualquer um dos seus contatos integrados. AWS Ground Station AWS Ground Station Localizações

A seguir está um AWS CloudFormation modelo completo que inclui todos os recursos descritos nesta seção combinados em um único modelo que pode ser usado diretamente em AWS CloudFormation.

O AWS CloudFormation modelo nomeado foi `AquaSnppJpssTerraDigIF.yml` projetado para fornecer acesso rápido para começar a receber dados de frequência intermediária digitalizada (DigIF) para os satélites Aqua, SNPP, JPSS-1/NOAA-20 e Terra. Ele contém uma EC2 instância da Amazon e os AWS CloudFormation recursos necessários para receber dados brutos de transmissão direta do DigiF.

Se Aqua, SNPP, JPSS-1/NOAA-20 e Terra não estiverem integrados à sua conta, consulte. Satélite a bordo

> **Note**
>
> Você pode acessar o modelo acessando o bucket Amazon S3 de integração do cliente usando AWS credenciais válidas. Os links abaixo usam um bucket regional do Amazon S3. Altere o código da `us-west-2` região para representar a região correspondente na qual você deseja criar a AWS CloudFormation pilha.
> Além disso, as instruções a seguir usam YAML. No entanto, os modelos estão disponíveis no formato YAML ou JSON. Para usar JSON, substitua a extensão do `.yml` arquivo por `.json` ao baixar o modelo.

Para baixar o modelo usando AWS CLI, use o seguinte comando:

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

É possível visualizar e fazer download do modelo no console navegando até o seguinte URL no seu navegador:

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

Você pode especificar o modelo diretamente AWS CloudFormation usando o seguinte link:

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

Quais recursos adicionais o modelo define?

O `AquaSnppJpssTerraDigIF` modelo inclui os seguintes recursos adicionais:

- (Opcional) Acionadores de CloudWatch eventos - AWS Lambda Função que é acionada usando CloudWatch eventos enviados AWS Ground Station antes e depois de um contato. A AWS Lambda função iniciará e, opcionalmente, interromperá sua instância receptora.
- (Opcional) EC2 Verificação de contatos - A opção de usar o Lambda para configurar um sistema de verificação de suas EC2 instâncias da Amazon para contatos com notificação do SNS. É importante observar que isso pode incorrer em cobranças, dependendo do seu uso atual.
- Ground Station Amazon Machine Image Retrieval Lambda: a opção de selecionar qual software está instalado em sua instância e a AMI de sua escolha. As opções de software incluem `DDX 2.6.2 Only` e `DDX 2.6.2 with qRadio 3.6.0`. Essas opções continuarão a se expandir à medida que atualizações e recursos adicionais de software forem lançados.
- Perfis de missão adicionais - Perfis de missão para satélites de transmissão pública adicionais (Aqua, SNPP e Terra).
- Configurações adicionais de downlink de antena - Configurações de downlink de antena para satélites de transmissão pública adicionais (Aqua, SNPP e Terra).

Os valores e os parâmetros dos satélites nesse modelo já estão preenchidos. Esses parâmetros facilitam o uso AWS Ground Station imediato desses satélites. Você não precisa configurar seus próprios valores para usar AWS Ground Station ao usar esse modelo. No entanto, é possível personalizar os valores para que o modelo funcione para seu caso de uso.

Onde recebo os meus dados?

O grupo de endpoints do fluxo de dados é configurado para usar a interface de rede da instância do receptor que parte do modelo cria. A instância receptora usa um aplicativo de endpoint de fluxo de dados para receber o stream de dados da AWS Ground Station porta definida pelo endpoint de fluxo de dados. Após serem recebidos, os dados estarão disponíveis para consumo por meio da porta UDP 50000 no adaptador de loopback da instância do receptor. Para obter

mais informações sobre como configurar um grupo de endpoints de fluxo de dados, consulte. AWS::GroundStation::DataflowEndpointGroup

# Satélite de transmissão pública utilizando um endpoint de fluxo de dados (demodulado e decodificado)

Este exemplo se baseia na análise feita na JPSS-1 - Satélite de transmissão pública (PBS) - Avaliação seção do guia do usuário.

Para concluir este exemplo, você precisará assumir um cenário: você deseja capturar o caminho de comunicação do HRD como dados de transmissão direta demodulados e decodificados usando um endpoint de fluxo de dados. Este exemplo é um bom ponto de partida se você planeja processar os dados usando o software NASA Direct Readout Labs (RT-STPS e IPOPP).

## Caminhos de comunicação

Esta seção representa Planeje seus caminhos de comunicação de fluxo de dados como começar. Neste exemplo, você criará duas seções em seu AWS CloudFormation modelo: seções de parâmetros e recursos.

> **Note**
>
> Para obter mais informações sobre o conteúdo de um AWS CloudFormation modelo, consulte as seções Modelo.

Para a seção Parâmetros, você adicionará os seguintes parâmetros. Você especificará valores para eles ao criar a pilha por meio do AWS CloudFormation console.

```
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**
>
> Você precisa criar um par de chaves e fornecer o nome para o EC2 `EC2Key` parâmetro da Amazon. Consulte Criar um par de chaves para sua EC2 instância da Amazon.
> Além disso, você precisará fornecer a ID de AMI específica da região correta ao criar a AWS CloudFormation pilha. Consulte AWS Ground Station Imagens de máquinas da Amazon (AMIs).

Os trechos de modelo restantes pertencem à seção Recursos do AWS CloudFormation modelo.

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

Dado nosso cenário para fornecer um único caminho de comunicação para uma EC2 instância, você terá um único caminho de entrega síncrono. De acordo com a Entrega síncrona de dados seção, você deve instalar e configurar uma EC2 instância da Amazon com um aplicativo de endpoint de fluxo de dados e criar um ou mais grupos de endpoints de fluxo de dados.

```
  # 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
```

Você também precisará das políticas, funções e perfis apropriados para permitir AWS Ground Station a criação de uma interface de rede elástica (ENI) em sua conta.

```
 # 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 configurações

Esta seção representa Crie configurações o guia do usuário.

Você precisará de uma configuração de rastreamento para definir sua preferência de uso do autotrack. Selecionar PREFERRED como trilha automática pode melhorar a qualidade do sinal, mas não é necessário atender à qualidade do sinal devido à qualidade suficiente das efemérides JPSS-1.

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

Com base no caminho de comunicação, você precisará definir uma antenna-downlink-demod-decodeconfiguração para representar a parte do satélite, bem como uma configuração de endpoint de fluxo de dados para se referir ao grupo de endpoints de fluxo de dados que define os detalhes do endpoint.

> **Note**
>
> Para obter detalhes sobre como definir os valores para`DemodulationConfig`, e`DecodeConfig`, consulteConfiguração de decodificação de demodulação de downlink de antena .

```
 # 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 perfil da missão

Esta seção representa Crie um perfil de missão o guia do usuário.

Agora que você tem as configurações associadas, pode usá-las para criar o fluxo de dados. Você usará os padrões para os demais parâmetros.

```
 # 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
```

## Juntando tudo

Com os recursos acima, agora você tem a capacidade de agendar contatos JPSS-1 para entrega síncrona de dados a partir de qualquer um dos seus contatos integrados. AWS Ground Station AWS Ground Station Localizações

A seguir está um AWS CloudFormation modelo completo que inclui todos os recursos descritos nesta seção combinados em um único modelo que pode ser usado diretamente em AWS CloudFormation.

O AWS CloudFormation modelo nomeado foi `AquaSnppJpss.yml` projetado para fornecer acesso rápido para começar a receber dados dos satélites Aqua, SNPP e JPSS-1/NOAA-20. Ele contém uma EC2 instância da Amazon e os AWS Ground Station recursos necessários para agendar contatos e receber dados de transmissão direta demodulados e decodificados.

Se Aqua, SNPP, JPSS-1/NOAA-20 e Terra não estiverem integrados à sua conta, consulte. Satélite a bordo

> **Note**
>
> Você pode acessar o modelo acessando o bucket Amazon S3 de integração do cliente usando AWS credenciais válidas. Os links abaixo usam um bucket regional do Amazon S3. Altere o código da `us-west-2` região para representar a região correspondente na qual você deseja criar a AWS CloudFormation pilha.
> Além disso, as instruções a seguir usam YAML. No entanto, os modelos estão disponíveis no formato YAML ou JSON. Para usar o JSON, substitua a extensão do `.yml` arquivo por `.json` ao baixar o modelo.

Para baixar o modelo usando AWS CLI, use o seguinte comando:

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

É possível visualizar e fazer download do modelo no console navegando até o seguinte URL no seu navegador:

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

Você pode especificar o modelo diretamente AWS CloudFormation usando o seguinte link:

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

Quais recursos adicionais o modelo define?

O `AquaSnppJpss` modelo inclui os seguintes recursos adicionais:

- (Opcional) Acionadores de CloudWatch eventos - AWS Lambda Função que é acionada usando CloudWatch eventos enviados AWS Ground Station antes e depois de um contato. A AWS Lambda função iniciará e, opcionalmente, interromperá sua instância receptora.
- (Opcional) EC2 Verificação de contatos - A opção de usar o Lambda para configurar um sistema de verificação de suas EC2 instâncias da Amazon para contatos com notificação do SNS. É importante observar que isso pode incorrer em cobranças, dependendo do seu uso atual.
- Ground Station Amazon Machine Image Retrieval Lambda: a opção de selecionar qual software está instalado em sua instância e a AMI de sua escolha. As opções de software incluem `DDX 2.6.2 Only` e `DDX 2.6.2 with qRadio 3.6.0`. Se você quiser usar o DigiF Data Delivery de banda larga e o AWS Ground Station Agent, consulte. Satélite de transmissão pública utilizando AWS Ground Station Agent (banda larga) Essas opções continuarão a se expandir à medida que atualizações e recursos adicionais de software forem lançados.
- Perfis de missão adicionais - Perfis de missão para satélites de transmissão pública adicionais (Aqua, SNPP e Terra).
- Configurações adicionais de downlink de antena - Configurações de downlink de antena para satélites de transmissão pública adicionais (Aqua, SNPP e Terra).

Os valores e os parâmetros dos satélites nesse modelo já estão preenchidos. Esses parâmetros facilitam o uso AWS Ground Station imediato desses satélites. Você não precisa configurar seus

próprios valores para usá-los AWS Ground Station ao usar esse modelo. No entanto, é possível personalizar os valores para que o modelo funcione para seu caso de uso.

Onde recebo os meus dados?

O grupo de endpoints do fluxo de dados é configurado para usar a interface de rede da instância do receptor que parte do modelo cria. A instância receptora usa um aplicativo de endpoint de fluxo de dados para receber o stream de dados da AWS Ground Station porta definida pelo endpoint de fluxo de dados. Após serem recebidos, os dados estarão disponíveis para consumo por meio da porta UDP 50000 no adaptador de loopback da instância do receptor. Para obter mais informações sobre como configurar um grupo de endpoints de fluxo de dados, consulte. AWS::GroundStation::DataflowEndpointGroup

# Satélite de transmissão pública utilizando AWS Ground Station Agent (banda larga)

Este exemplo se baseia na análise feita na JPSS-1 - Satélite de transmissão pública (PBS) - Avaliação seção do guia do usuário.

Para concluir este exemplo, você precisará assumir um cenário: capturar o caminho de comunicação do HRD como frequência intermediária digital de banda larga (DigIF) e processá-lo conforme recebido pelo agente AWS Ground Station em uma instância da Amazon EC2 usando um SDR.

> **Note**
>
> O sinal real do caminho de comunicação JPSS HRD tem uma largura de banda de 30 MHz, mas você configurará a configuração de downlink da antena para tratá-lo como um sinal com uma MHz largura de banda de 100% para que ele possa fluir pelo caminho correto a ser recebido pelo Agente neste exemplo. AWS Ground Station

## Caminhos de comunicação

Esta seção representa Planeje seus caminhos de comunicação de fluxo de dados como começar. Neste exemplo, você precisará de uma seção adicional em seu AWS CloudFormation modelo que não tenha sido usada nos outros exemplos, a seção Mapeamentos.

> **Note**
>
> Para obter mais informações sobre o conteúdo de um AWS CloudFormation modelo, consulte as seções Modelo.

Você começará configurando uma seção de mapeamentos em seu AWS CloudFormation modelo para as listas de AWS Ground Station prefixos por região. Isso permite que as listas de prefixos sejam facilmente referenciadas pelo grupo de segurança de EC2 instâncias da Amazon. Para obter mais informações sobre como usar uma lista de prefixos, consulteConfiguração de VPC com agente 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
```

Para a seção Parâmetros, você adicionará os seguintes parâmetros. Você especificará valores para eles ao criar a pilha por meio do AWS CloudFormation console.

```
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**
>
> Você precisa criar um par de chaves e fornecer o nome para o EC2 `EC2Key` parâmetro da Amazon. Consulte Criar um par de chaves para sua EC2 instância da Amazon.
> Além disso, você precisará fornecer a ID de AMI específica da região correta ao criar a AWS CloudFormation pilha. Consulte AWS Ground Station Imagens de máquinas da Amazon (AMIs).

Os trechos de modelo restantes pertencem à seção Recursos do AWS CloudFormation modelo.

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

Dado nosso cenário para fornecer um único caminho de comunicação para uma EC2 instância da Amazon, você sabe que terá um único caminho de entrega síncrona. De acordo com a Entrega síncrona de dados seção, você deve instalar e configurar uma EC2 instância da Amazon com o AWS Ground Station Agent e criar um ou mais grupos de endpoints de fluxo de dados. Você começará configurando primeiro a Amazon VPC para o AWS Ground Station agente.

```
 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**
>
> Para obter mais informações sobre as configurações de VPC suportadas pelo AWS Ground Station agente, consulte Requisitos do AWS Ground Station agente - diagramas de VPC.

Em seguida, você configurará a EC2 instância 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
```

Você também precisará das políticas, funções e perfis apropriados para permitir AWS Ground Station a criação da interface de rede elástica (ENI) em sua conta.

```
 # 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 configurações

Esta seção representa Crie configurações como começar.

Você precisará de uma configuração de rastreamento para definir sua preferência de uso do autotrack. Selecionar PREFERRED como trilha automática pode melhorar a qualidade do sinal, mas não é necessário atender à qualidade do sinal devido à qualidade suficiente das efemérides JPSS-1.

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

Com base no caminho de comunicação, você precisará definir uma configuração de antena-downlink para representar a parte do satélite, bem como uma configuração de endpoint de fluxo de dados para se referir ao grupo de endpoints de fluxo de dados que define os detalhes do endpoint.

```
 # 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 perfil da missão

Esta seção representa Crie um perfil de missão como começar.

Agora que você tem as configurações associadas, pode usá-las para criar o fluxo de dados. Você usará os padrões para os demais parâmetros.

```
 # 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
```

## Juntando tudo

Com os recursos acima, agora você tem a capacidade de agendar contatos JPSS-1 para entrega síncrona de dados a partir de qualquer um dos seus contatos integrados. AWS Ground Station AWS Ground Station Localizações

A seguir está um AWS CloudFormation modelo completo que inclui todos os recursos descritos nesta seção combinados em um único modelo que pode ser usado diretamente em AWS CloudFormation.

O AWS CloudFormation modelo nomeado foi `DirectBroadcastSatelliteWbDigIfEc2DataDelivery.yml` projetado para fornecer acesso rápido para começar a receber dados de frequência intermediária digitalizada (DigIF) para os satélites Aqua, SNPP, JPSS-1/NOAA-20 e Terra. Ele contém uma EC2 instância da Amazon e os AWS CloudFormation recursos necessários para receber dados brutos de transmissão direta do DigiF usando o AWS Ground Station Agent.

Se Aqua, SNPP, JPSS-1/NOAA-20 e Terra não estiverem integrados à sua conta, consulte. Satélite a bordo

> **Note**
>
> Você pode acessar o modelo acessando o bucket Amazon S3 de integração do cliente usando AWS credenciais válidas. Os links abaixo usam um bucket regional do Amazon S3. Altere o código da `us-west-2` região para representar a região correspondente na qual você deseja criar a AWS CloudFormation pilha.
> Além disso, as instruções a seguir usam YAML. No entanto, os modelos estão disponíveis no formato YAML ou JSON. Para usar o JSON, substitua a extensão do `.yml` arquivo por `.json` ao baixar o modelo.

Para baixar o modelo usando AWS CLI, use o seguinte comando:

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

É possível visualizar e fazer download do modelo no console navegando até o seguinte URL no seu navegador:

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

Você pode especificar o modelo diretamente AWS CloudFormation usando o seguinte link:

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

Quais recursos adicionais o modelo define?

O `DirectBroadcastSatelliteWbDigIfEc2DataDelivery` modelo inclui os seguintes recursos adicionais:

- Interface de rede elástica da instância do receptor - (condicional) Uma interface de rede elástica é criada na sub-rede especificada por, PublicSubnetIdse fornecida. Isso é necessário se a instância do receptor estiver em uma sub-rede privada. A interface de rede elástica será associada ao EIP e anexada à instância do receptor.
- IP elástico da instância do receptor - Um IP elástico que se AWS Ground Station conectará a. Isso se conecta à instância do receptor ou à interface de rede elástica.
- Uma das seguintes associações de IP elástico:
  - Associação entre instância do receptor e IP elástico - A associação do IP elástico à sua instância do receptor, se não PublicSubnetIdfor especificada. Isso requer essa SubnetIdreferência a uma sub-rede pública.
  - Interface de rede elástica da instância receptora com associação de IP elástico - A associação do IP elástico à interface de rede elástica da instância receptora, se PublicSubnetIdfor especificada.
- (Opcional) Acionadores de CloudWatch eventos - AWS Lambda Função que é acionada usando CloudWatch eventos enviados AWS Ground Station antes e depois de um contato. A AWS Lambda função iniciará e, opcionalmente, interromperá sua instância receptora.
- (Opcional) Amazon EC2 Verification for Contacts - A opção de usar o Lambda para configurar um sistema de verificação de suas EC2 instâncias da Amazon para contatos com notificação do SNS. É importante observar que isso pode incorrer em cobranças, dependendo do seu uso atual.
- Perfis de missão adicionais - Perfis de missão para satélites de transmissão pública adicionais (Aqua, SNPP e Terra).
- Configurações adicionais de downlink de antena - Configurações de downlink de antena para satélites de transmissão pública adicionais (Aqua, SNPP e Terra).

Os valores e os parâmetros dos satélites nesse modelo já estão preenchidos. Esses parâmetros facilitam o uso AWS Ground Station imediato desses satélites. Você não precisa configurar seus próprios valores para usá-los AWS Ground Station ao usar esse modelo. No entanto, é possível personalizar os valores para que o modelo funcione para seu caso de uso.

Onde recebo os meus dados?

O grupo de endpoints do fluxo de dados é configurado para usar a interface de rede da instância do receptor que parte do modelo cria. A instância receptora usa o AWS Ground Station Agente para receber o fluxo de dados da AWS Ground Station porta definida pelo endpoint do fluxo de dados. Para obter mais informações sobre como configurar um grupo de endpoints de fluxo de dados, consulte. AWS::GroundStation::DataflowEndpointGroup Para obter mais informações sobre o AWS Ground Station agente, consulte O que é o AWS Ground Station agente?

# Solução de problemas

A documentação a seguir pode ajudá-lo a solucionar problemas que podem ocorrer durante o uso AWS Ground Station.

Tópicos



## Solucione problemas de contatos que entregam dados para a Amazon EC2

Se você não conseguir concluir um AWS Ground Station contato com sucesso, precisará verificar se sua EC2 instância da Amazon está em execução, verificar se seu aplicativo de endpoint de fluxo de dados está em execução e verificar se o stream do seu aplicativo de endpoint de fluxo de dados está configurado corretamente.

> **Note**
>
> DataDefender (DDX) é um exemplo de um aplicativo de endpoint de fluxo de dados atualmente suportado pelo AWS Ground Station

Pré-requisito

Os procedimentos a seguir pressupõem que uma EC2 instância da Amazon já esteja configurada. Para configurar uma EC2 instância da Amazon em AWS Ground Station, consulte Conceitos básicos.

### Etapa 1: verifique se sua EC2 instância está em execução

O procedimento a seguir mostra como encontrar sua EC2 instância da Amazon no console e iniciá-la se ela não estiver em execução.

1. Localize a EC2 instância da Amazon que foi usada para o contato que você está solucionando. Use as seguintes etapas:

   a. Em seu AWS CloudFormationpainel, selecione a pilha que contém sua EC2 instância da Amazon.

   b. Escolha a guia Recursos e localize sua EC2 instância da Amazon na coluna Logical ID. Verifique se a instância foi criada na coluna Status.

   c. Na coluna ID física, escolha o link para sua EC2 instância da Amazon. Isso levará você ao console de EC2 gerenciamento da Amazon.

2. No console EC2 de gerenciamento da Amazon, certifique-se de que seu estado de EC2 instância da Amazon esteja em execução.

3. Se a instância estiver sendo executada, siga para a próxima etapa. Se a instância não estiver em execução, inicie-a usando a seguinte etapa:

   • Com sua EC2 instância da Amazon selecionada, escolha Ações > Estado da instância > Iniciar.

## Etapa 2: Determinar o tipo de aplicativo de fluxo de dados usado

Se você estiver usando o AWS Ground Station Agente para entrega de dados, redirecione para a seção AWS Ground Station Agente de Solução de Problemas. Caso contrário, se você estiver usando o aplicativo DataDefender (DDX), continue the section called “Etapa 3: verificar se o aplicativo de fluxo de dados está em execução” usando.

## Etapa 3: verificar se o aplicativo de fluxo de dados está em execução

A verificação do status de DataDefender exige que você se conecte à sua instância na Amazon EC2. Para obter mais detalhes sobre como se conectar à sua instância, consulte Conecte-se à sua instância Linux.

O procedimento a seguir fornece etapas de solução de problemas usando comandos em um cliente SSH.

1. Abra um terminal ou prompt de comando e conecte-se à sua EC2 instância da Amazon usando SSH. Encaminhe a porta 80 do host remoto para visualizar a interface do usuário DataDefender da web. Os comandos a seguir demonstram como usar o SSH para se conectar a uma EC2 instância da Amazon por meio de um bastion com o encaminhamento de porta ativado.

> **Note**
>
> Você deve substituir<SSH KEY>,<BASTION HOST>, e por <HOST>sua chave ssh específica, nome do host bastion e nome do host da EC2 instância Amazon.

No 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>
```

No 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. Verifique se DataDefender (também chamado de DDX) está em execução fazendo grepping (verificando) um processo em execução chamado ddx na saída. O comando para grepping (verificação) para um processo em execução e um exemplo de saída bem-sucedida é fornecido a seguir.

```
[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
```

Se DataDefender estiver em execução, vá para the section called “Etapa 4: verificar se o stream do aplicativo de fluxo de dados está configurado” Caso contrário, continue para a próxima etapa.

3. Comece a DataDefender usar o comando show abaixo.

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

Se DataDefender estiver em execução depois de usar o comando, vá para the section called “Etapa 4: verificar se o stream do aplicativo de fluxo de dados está configurado” Caso contrário, continue para a próxima etapa.

4. Inspecione os arquivos a seguir usando os comandos abaixo para ver se houve algum erro durante a instalação e configuração DataDefender.

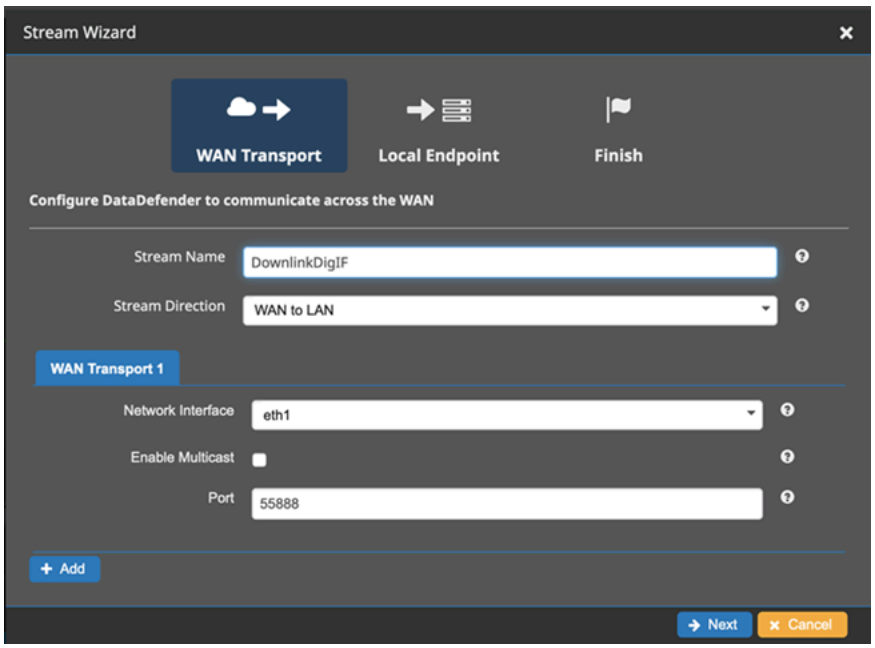
```
cat /var/log/user-data.log
          cat /opt/aws/groundstation/.startup.out
```

> **Note**
>
> Um problema comum descoberto ao inspecionar esses arquivos é que a Amazon VPC na qual sua instância da EC2 Amazon está sendo executada não tem acesso ao Amazon S3 para baixar os arquivos de instalação. Se você descobrir em seus registros que esse é o problema, verifique as configurações do Amazon VPC e do grupo de segurança da sua EC2 instância para garantir que eles não estejam bloqueando o acesso ao Amazon S3.

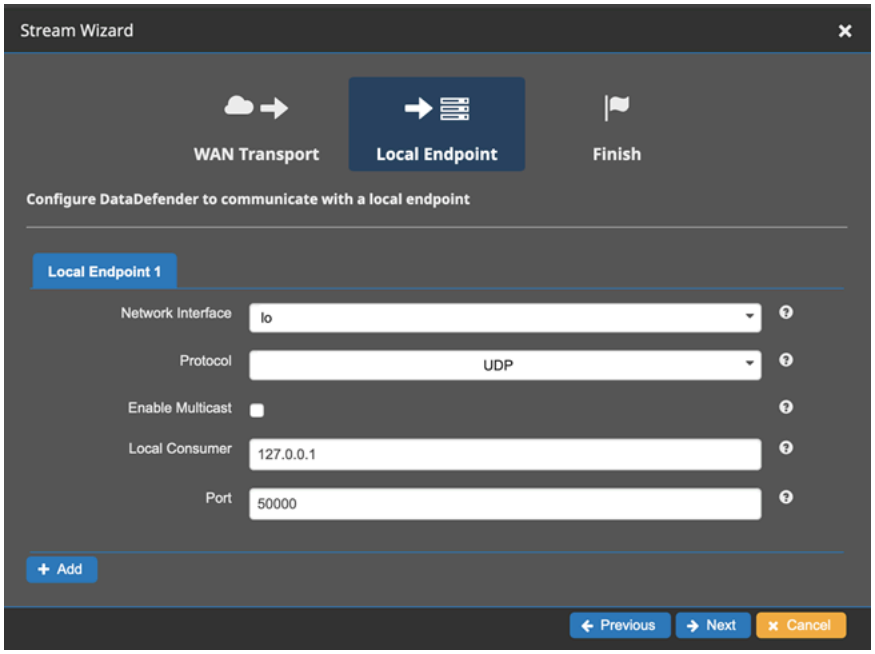
Se DataDefender estiver em execução após verificar as configurações da Amazon VPC, continue. the section called “Etapa 4: verificar se o stream do aplicativo de fluxo de dados está configurado” Se o problema persistir, entre em contato com o AWS Support e envie os arquivos de log com uma descrição do problema.

## Etapa 4: verificar se o stream do aplicativo de fluxo de dados está configurado

1. Em um navegador da Web, acesse sua interface de usuário DataDefender da Web inserindo o seguinte endereço na barra de endereço: localhost:8080. Depois, pressione Enter.
2. No DataDefenderpainel, escolha Ir para detalhes.
3. Selecione o fluxo na lista de fluxos e selecione Editar fluxo.
4. Na caixa de diálogo Assistente de fluxo, faça o seguinte:
   a. No painel Transporte de WAN, certifique-se de que WAN para LAN está selecionado para a Direção do fluxo.
   b. Na caixa Porta, certifique-se de que a porta WAN selecionada para o grupo de endpoints do fluxo de dados esteja presente. Por padrão, essa porta é 55888. Em seguida, escolha Próximo.




c. No painel Endpoint local, certifique-se de que uma porta válida esteja presente na caixa Porta. Por padrão, essa porta é 50000. Essa é a porta na qual você receberá seus dados depois DataDefender de recebê-los do AWS Ground Station serviço. Em seguida, escolha Próximo.




d. Selecione Concluir no menu restante se tiver alterado qualquer valor. Caso contrário, é possível cancelar no menu Assistente de fluxo.

Agora você garantiu que sua EC2 instância da Amazon esteja funcionando e DataDefender configurada adequadamente para receber dados da AWS Ground Station. Avance para the section called “Etapa 5: Certifique-se de ter endereços IP disponíveis suficientes na sub-rede da (s) instância (s) do receptor”.

## Etapa 5: Certifique-se de ter endereços IP disponíveis suficientes na sub-rede da (s) instância (s) do receptor

O procedimento a seguir mostra como encontrar o número de endereços IP disponíveis em uma instância do Amazon EC2 Receiver no console.

1. Para cada instância de EC2 receptor da Amazon usada para o contato, você está solucionando problemas. Use as seguintes etapas:

   a. Em seu AWS CloudFormationpainel, selecione a pilha que contém sua EC2 instância da Amazon.

   b. Escolha a guia Recursos e localize sua EC2 instância da Amazon na coluna Logical ID. Verifique se a instância foi criada na coluna Status.

   c. Na coluna ID física, escolha o link para sua EC2 instância da Amazon. Isso levará você ao console de EC2 gerenciamento da Amazon.

2. No console EC2 de gerenciamento da Amazon, localize e clique no link do ID de sub-rede no resumo da instância do EC2 receptor da Amazon. Isso levará você ao console de gerenciamento correspondente da Amazon VPC.

3. Selecione a sub-rede correspondente no console de gerenciamento da Amazon VPC e verifique os detalhes da sua sub-rede para ver os endereços disponíveis. IPv4  Se esse número não for pelo menos igual aos endpoints de fluxo de dados que usam essa instância de EC2 receptor da Amazon, faça o seguinte:

   a. Atualize a sub-rede correspondente do seu AWS CloudFormation modelo CidrBlockpara que seja dimensionada corretamente. Para obter mais detalhes sobre o tamanho da sub-rede, consulte Blocos CIDR de sub-rede.

   b. Reimplante sua pilha com seu modelo atualizado AWS CloudFormation .

Se você continuar enfrentando problemas, entre em contato com o AWS Support.

# Solucionar problemas de contatos com FALHA

Um contato terá o status de contato do terminal FALHOU quando AWS Ground Station detectar um problema com a configuração do seu recurso. Os casos de uso comuns que podem causar o status FAILED nos contatos são fornecidos abaixo, junto com as etapas para ajudar a solucionar problemas.

> **Note**
>
> Este guia é especificamente para o status de contato FAILED e não se destina a outros status de falha, como AWS_FAILED, AWS_CANCELLEDou FAILED_TO_SCHEDULE. Consulte mais informações sobre os status de contato em the section called “AWS Ground Station status de contato”

## Casos de uso FALHADOS do endpoint do Dataflow

Veja a seguir uma lista de casos de uso comuns que podem resultar em um status de contato FALHADO para fluxos de dados baseados em endpoints de fluxo de dados:

- O endpoint do Dataflow nunca se conecta — a conexão entre a AWS Ground Station Antenna e seu grupo de endpoints do Dataflow para um ou mais fluxos de dados nunca foi estabelecida.
- O endpoint do Dataflow se conecta tardiamente — a conexão entre a AWS Ground Station Antenna e seu grupo de endpoints do Dataflow para um ou mais fluxos de dados foi estabelecida após o horário de início do contato.
- A sub-rede do endpoint do Dataflow está sem endereços IP disponíveis. A solução de entrega de dados AWS Ground Station da Dataflow não consegue criar uma ENI na sua rede privada porque não tem nenhum endereço IP disponível na sub-rede da instância receptora.

Para qualquer caso de falha de endpoint de fluxo de dados, é recomendável examinar o seguinte:

- Confirme se a EC2 instância Amazon do receptor foi iniciada com sucesso, antes do horário de início do contato.
- Confirme se o software do endpoint de fluxo de dados estava funcionando durante o contato.
- Verifique se você tem pelo menos um endereço IP disponível por endpoint de fluxo de dados por sub-rede de instância receptora.

Consulte etapas de solução de problemas mais específicas na seção sobre Solucione problemas de contatos que entregam dados para a Amazon EC2.

### AWS Ground Station Casos de uso com FALHA do agente

Veja a seguir a lista de casos de uso comuns que podem resultar em um status de contato FAILED para fluxos de dados baseados no agente:

- AWS Ground Station Status do agente nunca reportado — O agente responsável por orquestrar a entrega de dados em seu grupo de endpoints do Dataflow para um ou mais fluxos de dados nunca reportou o status com êxito. AWS Ground Station Essa atualização de status deve ocorrer alguns segundos após a hora de término do contato.
- AWS Ground Station Agente iniciado tarde - O agente responsável por orquestrar a entrega de dados em seu grupo de endpoints do Dataflow para um ou mais fluxos de dados foi iniciado tarde, após o horário de início do contato.

Para qualquer caso de falha no fluxo de dados do AWS Ground Station Agente, é recomendável examinar o seguinte:

- Confirme se a EC2 instância Amazon do receptor foi iniciada com sucesso, antes do horário de início do contato.
- Confirme se a aplicação do agente estava funcionando no início e durante o contato.
- Confirme se o aplicativo do agente e a EC2 instância da Amazon não foram encerrados dentro de 15 segundos após o término do contato. Isso dá ao agente tempo suficiente para informar o status ao AWS Ground Station.

Consulte etapas de solução de problemas mais específicas na seção sobre Solucione problemas de contatos que entregam dados para a Amazon EC2.

## Solucionar problemas de contatos FAILED_TO_SCHEDULE

Um contato terminará em um estado FAILED_TO_SCHEDULE quando AWS Ground Station detectar um problema na configuração do seu recurso ou no sistema interno. Um contato que termina em um estado FAILED_TO_SCHEDULE, opcionalmente, fornecerá um contexto adicional. `errorMessage` Para obter informações sobre como descrever contatos, consulte a DescribeContactAPI.

Os casos de uso comuns que podem causar contatos FAILED_TO_SCHEDULE são fornecidos abaixo, junto com as etapas para ajudar a solucionar problemas.

> **Note**
>
> Este guia é específico para o status de contato FAILED_TO_SCHEDULE - e não se destina a outros status de falha, como, ou FAILED. AWS_FAILEDAWS_CANCELLED Consulte mais informações sobre os status de contato em the section called “AWS Ground Station status de contato”

## As configurações especificadas em sua Antenna Downlink Demod Decode Config não são suportadas.

O perfil da missão usado para agendar esse contato tinha uma antenna-downlink-demod-decode configuração que não era válida.

AntennaDownlinkDemodDecode Configuração existente anteriormente

- Se suas antenna-downlink-demod-decode configurações foram alteradas recentemente, volte para uma versão em funcionamento anterior antes de tentar agendar.
- Se essa foi uma alteração intencional em uma configuração existente ou em uma configuração existente anteriormente que não está mais sendo agendada com sucesso, siga a próxima etapa sobre como integrar uma nova configuração. AntennaDownlinkDemodDecode

AntennaDownlinkDemodDecode Configuração recém-criada

Entre em contato AWS Ground Station diretamente para integrar sua nova configuração.
Crie um caso com o AWS Support, incluindo `contactId` aquele que terminou no estado FAILED_TO_SCHEDULE

## Etapas gerais de solução de problemas

Se as etapas de solução de problemas anteriores não resolverem seu problema:

- Tente agendar novamente o contato ou agendar outro contato usando o mesmo perfil de missão. Para obter informações sobre como reservar um contato, consulte ReserveContact.

- Se você continuar recebendo o status FAILED_TO_SCHEDULE para esse perfil de missão, entre em contato com o AWS Support

## Solucione o problema que DataflowEndpointGroups não está em um estado SAUDÁVEL

Abaixo estão listados os motivos pelos quais seus grupos de endpoints de fluxo de dados podem não estar em um estado `HEALTHY`, bem como a ação corretiva apropriada a ser tomada.

- `NO_REGISTERED_AGENT`- Inicie sua EC2 instância, que registrará o agente. Observe que você deve ter um arquivo de configuração de controlador válido para que essa chamada seja bem-sucedida. Consulte o AWS Ground Station Agente de uso para obter detalhes sobre como configurar esse arquivo.
- `INVALID_IP_OWNERSHIP`- Use a DeleteDataflowEndpointGroup API para excluir o Dataflow Endpoint Group e, em seguida, use a CreateDataflowEndpointGroup API para recriar o Dataflow Endpoint Group usando endereços IP e portas associados à instância. EC2
- `UNVERIFIED_IP_OWNERSHIP`: o endereço IP ainda não foi validado. A validação ocorre periodicamente, então isso deve se resolver sozinho.
- `NOT_AUTHORIZED_TO_CREATE_SLR`: a conta não está autorizada a criar a função vinculada ao serviço necessária. Verifique as etapas de solução de problemas em Use funções vinculadas a serviços para Ground Station

## Solucionar problemas de efemérides inválidas

Quando uma efeméride personalizada é carregada, AWS Ground Station ela passa por um fluxo de trabalho de validação assíncrona antes de se tornar. `ENABLED` Esse fluxo de trabalho garante que os identificadores, os metadados e a trajetória do satélite sejam válidos.

Quando uma efeméride falha na validação, `DescribeEphemeris` retornará um EphemerisInvalidReason, que fornece uma visão sobre por que a efeméride falhou na validação. Os valores potenciais do EphemerisInvalidReasonsão os seguintes:

| Valor | Descrição | Ação de resolução de problemas |
| --- | --- | --- |
| METADATA_INVALID | Os identificadores de espaçonaves fornecidos, como ID de satélite, são inválidos | Verifique o ID NORAD ou outros identificadores fornecidos nos dados de efemérides |
| TIME_RANGE_INVALID | Os horários de início, término ou expiração são inválidos para as efemérides fornecidas | Certifique-se de que a hora de início seja anterior a “agora” (é recomendável definir a hora de início alguns minutos no passado), que a hora de término seja posterior à hora de início e que a hora de término seja após a hora de expiração |
| TRAJECTORY_INVALID | As efemérides fornecidas definem uma trajetória de espaçonave inválida | Confirme se a trajetória fornecida é contínua e se é para o satélite correto. |
| VALIDATION_ERROR | Ocorreu um erro de serviço interno ao processar efemérides para validação | Repetir o upload |

Um exemplo de resposta `DescribeEphemeris` para uma efeméride `INVALID` é fornecido abaixo:

```
{
  "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**
>
> Se o status de uma efeméride for`ERROR`, a efeméride não se `ENABLED` deve a um problema com o serviço. AWS Ground Station Você deve tentar fornecer as efemérides novamente via. `CreateEphemeris` A nova efeméride pode se tornar se o problema `ENABLED` for transitório.

> **Note**
>
> AWS Ground Station trata as efemérides como dados de uso individualizados. Se você usar esse recurso opcional, a AWS usará seus dados de efemérides para fornecer suporte à solução de problemas.

# Solucionar problemas de contatos que não receberam dados

É possível que um contato pareça bem-sucedido, mas ainda não tenha recebido nenhum dado. Isso pode significar que você recebe arquivos PCAP vazios ou nenhum arquivo PCAP se estiver usando a entrega de dados do S3. Isso pode acontecer por vários motivos. A seguir, são abordadas algumas das causas e como resolvê-las.

## Configuração de downlink incorreta

Cada contato que recebe dados de um satélite terá um associado Configuração de downlink de antena ouConfiguração de decodificação de demodulação de downlink de antena . Se a configuração especificada não concordar com o sinal transmitido por um satélite, não AWS Ground Station será capaz de receber o sinal transmitido. Isso fará com que nenhum dado seja recebido por AWS Ground Station.

Para corrigir isso, verifique se as configurações que você está usando concordam com o sinal transmitido pelo seu satélite. Por exemplo, verifique se você definiu a frequência central correta, a largura de banda, a polarização e, se necessário, os parâmetros de demodulação e decodificação.

## Manobra de satélite

Há momentos em que um satélite pode realizar uma manobra que desativa temporariamente alguns de seus sistemas de comunicação. A manobra também pode alterar significativamente a localização do satélite no céu. AWS Ground Station não conseguirá receber um sinal de um satélite que não esteja transmitindo um sinal ou se a efeméride usada fizer com que a AWS Ground Station antena aponte para um local no céu onde o satélite não esteja presente.

Se você estiver tentando se comunicar com um satélite de transmissão pública operado pela NOAA, poderá encontrar uma mensagem descrevendo uma interrupção ou manobra na página de mensagens de alerta por satélite da NOAA. A mensagem pode incluir um cronograma de quando se espera que a transmissão de dados seja retomada, ou isso pode ser publicado em uma mensagem subsequente.

Se você estiver se comunicando com seus próprios satélites, é sua responsabilidade entender suas operações de satélite e como isso pode afetar a comunicação com eles. AWS Ground Station Se você estiver realizando uma manobra que afetará a trajetória do satélite, isso pode incluir o fornecimento de dados de efemérides personalizados atualizados. Para obter mais informações sobre o fornecimento de dados de efemérides personalizados, consulte. Forneça dados de efemérides personalizados

## AWS Ground Station interrupção

Se AWS Ground Station fizer com que um contato falhe ou o cancele, AWS Ground Station definirá o status do contato como AWS_FAILED, ou AWS_CANCELLED. Para obter mais informações sobre o ciclo de vida do contato, consulte. Entenda o ciclo de vida do contato Em alguns casos, AWS Ground Station pode haver uma falha que impede que os dados sejam entregues à sua conta, mas não faz com que o contato tenha um AWS_CANCELLEDstatus AWS_FAILEDou. Quando isso acontece, AWS Ground Station deve publicar um evento específico da conta em seu painel AWS Health. Para obter mais informações sobre o painel AWS Health, consulte AWS Health User Guide.

# Cotas e limites

Você pode visualizar as regiões suportadas, seus endpoints associados e cotas em AWS Ground Station endpoints e cotas.

Você pode usar o console do Service Quotas, a API da AWS e a CLI da AWS para solicitar aumentos de cota, quando necessário.

# Termos de serviço

Para saber os termos do AWS Ground Station serviço, consulte os Termos de Serviço da AWS.

# Histórico do documento para o guia AWS Ground Station do usuário

A tabela a seguir descreve as mudanças importantes em cada versão do Guia AWS Ground Station do usuário.

| Alteração | Descrição | Data |
| --- | --- | --- |
| Atualização da documentação | Foi adicionado um esclarecimento sobre a utilização de contatos dos recursos configurados. | 04 de abril de 2025 |
| Novo recurso | Atualizou o guia do usuário para incluir gêmeos AWS Ground Station digitais. | 6 de agosto de 2024 |
| Atualização da documentação | Várias seções do guia do usuário foram atualizadas, incluindo novos diagramas, exemplos e muito mais. | 18 de julho de 2024 |
| Atualização da documentação | Feed RSS adicionado ao Guia do usuário. | 18 de julho de 2024 |
| Atualização da documentação | Divida o Guia do Usuário do AWS Ground Station Agente em um Guia do Usuário separado. | 18 de julho de 2024 |
| Novo recurso | Agora, os contatos podem ser programados em até 30 segundos fora dos intervalos de tempo de visibilidade. Os tempos de visibilidade estão incluídos nas DescribeContact respostas. | 26 de março de 2024 |

| | | |
|---|---|---|
| Atualização da documentação | Organização aprimorada e adição da seção “Seleção de EC2 instância e planejamento de CPU”. | 6 de março de 2024 |
| Atualização da documentação | Foram adicionadas novas práticas recomendadas ao Guia do Usuário do AWS Ground Station Agente para executar serviços e processos junto com o AWS Ground Station Agente. | 23 de fevereiro de 2024 |
| Atualização da documentação | Foi adicionada a página de notas de versão do agente. | 21 de fevereiro de 2024 |
| Atualização do modelo | Foi adicionado suporte para sub-rede pública separada no DataDelivery modelo DirectBroadcastSatelliteWbDigIfEc 2. | 14 de fevereiro de 2024 |
| Atualização da documentação | Foi adicionada referênci a à AWS Notificações de Usuários na documentação de monitoramento. | 6 de agosto de 2023 |
| Atualização da documentação | Foram adicionadas instruções para marcar satélites com um nome a ser exibido no AWS Ground Station console. | 26 de julho de 2023 |
| Novo recurso | Foi adicionado o Guia do Usuário do AWS Ground Station Agente para o lançamento do DigiF Data Delivery de banda larga | 12 de abril de 2023 |

| | | |
|---|---|---|
| Nova política AWS gerenciada | AWS Ground Station adicionou uma nova política chamada AWSGround StationAgentInstancePolicy. | 12 de abril de 2023 |
| Novo recurso | Atualizou o guia do usuário para o lançamento do CPE Preview. | 9 de novembro de 2022 |
| Nova política AWS gerenciada | AWS Ground Station adicionou a AWSService RoleForGroundStationDataflowEndpointGroup service-linked-role (SLR) que inclui uma nova política chamada AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy. | 2 de novembro de 2022 |
| Novo recurso | Atualizou o guia do usuário para incluir a integração com AWS CLI o. | 17 de abril de 2020 |
| Novo recurso | Atualizou o guia do usuário para incluir a integração com o CloudWatch Metrics. | 24 de fevereiro de 2020 |
| Novo modelo | Satélites de transmissão pública (AquaSnppJpss modelo) adicionados ao Guia do AWS Ground Station usuário. | 19 de fevereiro de 2020 |
| Novo recurso | Guia do usuário atualizado para incluir a entrega de dados entre regiões. | 5 de fevereiro de 2020 |

| | | |
|---|---|---|
| Atualização da documentação | Exemplos e descrições atualizados para monitoram ento AWS Ground Station com CloudWatch eventos. | 4 de fevereiro de 2020 |
| Atualização da documentação | Os locais de modelo foram atualizados e as seções Conceitos básicos e Solução de problemas foram revisadas. | 19 de dezembro de 2019 |
| Nova seção de solução de problemas | Uma seção de Solução de problemas foi adicionada ao Guia do Usuário do AWS Ground Station . | 7 de novembro de 2019 |
| Novo tópico de introdução | Atualizou o tópico Introdução, que inclui os AWS CloudForm ation modelos mais atuais. | 1 de julho de 2019 |
| Versão Kindle | Versão Kindle do Guia do Usuário do AWS Ground Station publicada. | 20 de junho de 2019 |
| Serviço e guia novos | Esta é a versão inicial AWS Ground Station e o Guia AWS Ground Station do Usuário. | 23 de maio de 2019 |

# AWS Glossário

Para obter a AWS terminologia mais recente, consulte o AWS glossário na Glossário da AWS Referência.

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.