Manual do usuário

AWS Ground Station

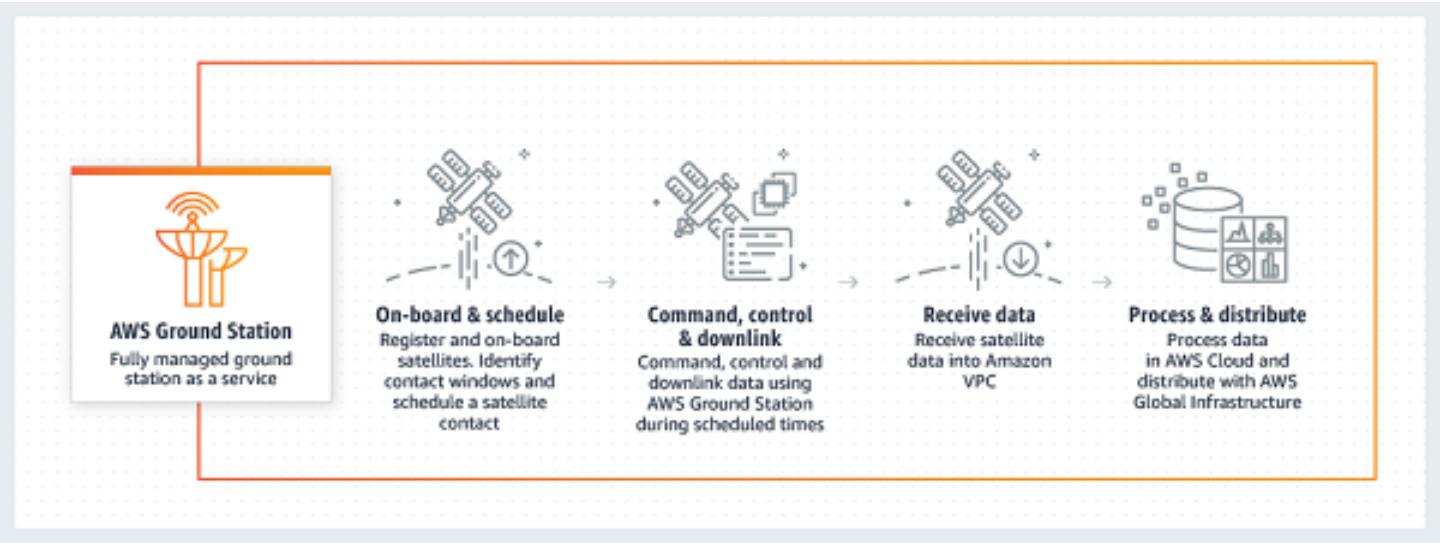
AWS Ground Station: Manual do usuário

Table of Contents

O que é o AWS Ground Station?

O AWS Ground Station é um serviço totalmente gerenciado que permite que você controle as comunicações por satélite, processe dados de satélite e dimensione suas operações de satélite. Isso significa que você não precisa mais criar ou gerenciar sua própria infraestrutura de estação terrestre.

O AWS Ground Station permite que você se concentre em inovar e testar rapidamente novos aplicativos que consomem dados de satélite e dimensionar dinamicamente o servidor e a utilização de armazenamento, em vez de gastar recursos para operar e manter suas próprias estações terrestres.



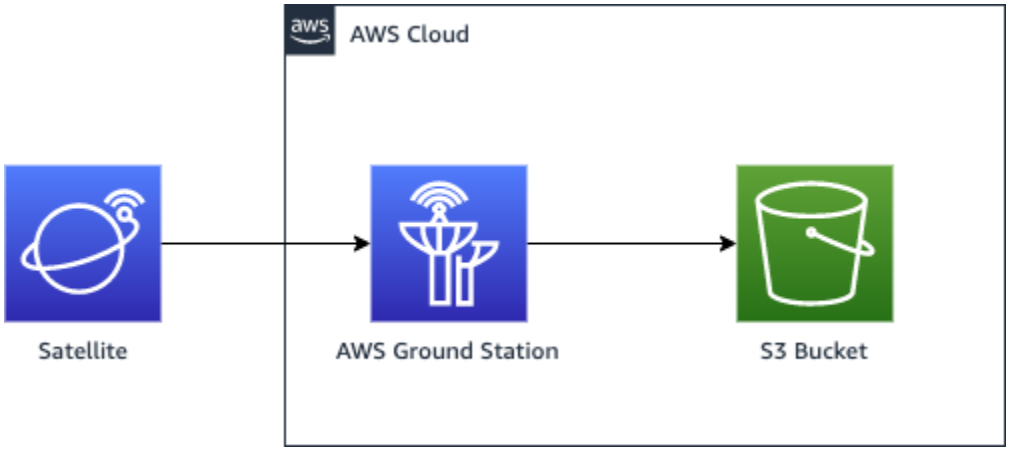
Como o AWS Ground Station funciona

A reserva de satélite também é conhecida como um contato. Seu satélite se comunica com uma AWS Ground Station antena durante os contatos. Você pode reservar contatos por meio de uma API ou do AWS console especificando informações de localização, horário e missão. Seus dados de contato podem ser transmitidos de e para uma instância do Amazon Elastic Compute Cloud (Amazon EC2) ou entregues de forma assíncrona a um bucket do Amazon Simple Storage Service (Amazon S3) em sua conta.

Você pode criar recursos de configuração extensíveis e reutilizáveis para ter controle sobre como as AWS Ground Station antenas são configuradas durante seus contatos. Com o uso de perfis de missão, você pode especificar a origem dos dados, em qual formato devem estar para onde devem ser enviados.

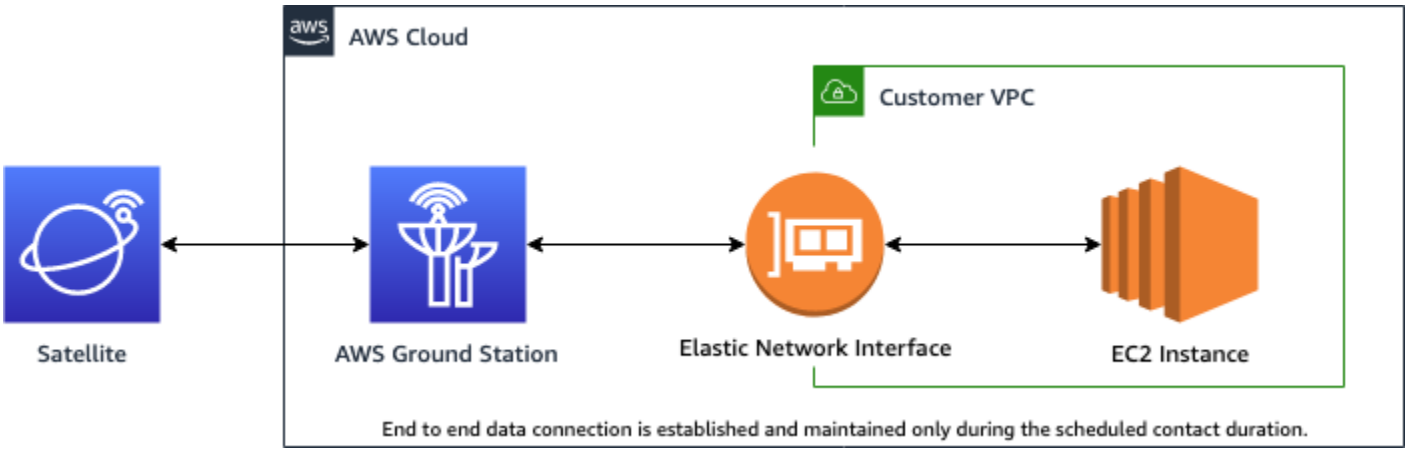
Entrega de dados para Amazon S3

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 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.



Entrega de dados para Amazon EC2

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



Mais informações

Com AWS Ground Station você pode acessar mais de 125 serviços via comunicações via satélite. Observe o seguinte:

- Você pode receber dados de RF de banda estreita em banda S (2.200 a 2.300 MHz) ou banda X (7.750 a 8.400 MHz) em larguras de banda de até 54 MHz.
  - Os dados de RF de banda S são digitalizados e fornecidos como streaming digital no formato de dados de sinal VITA-49/IP.
  - Os dados de frequência intermediária (FI) da banda X são digitalizados e fornecidos como streaming digital no formato de dados de sinal VITA-49/IP.
- Você pode receber dados demodulados/decodificados de banda larga em banda X (7.750 a 8.400 MHz) em larguras de banda de até 500 MHz
  - Os dados de frequência intermediária (FI) de banda X são demodulados, decodificados e fornecidos como streaming digital no formato de extensão VITA-49/IP.
- Você pode receber dados de banda larga de frequência intermediária digital (DigiF) de 40 MHz a 400 MHz de largura de banda por meio do Agente. AWS Ground Station
  - Consulte AWS Ground Station Guia do usuário do agente para obter mais informações sobre o AWS Ground Station Agent and Wideband DigiF Data Delivery.

- Você pode transmitir dados de RF em banda S (2.025 a 2.120 MHz) em larguras de banda de até 54 MHz.
  - Os dados de RF são fornecidos AWS Ground Station como um fluxo digital no formato VITA-49 Signal Data/IP.
- Você deve correr AWS Ground Station de uma AWS região que ofereça suporte AWS Ground Station. Para ver uma lista de regiões compatíveis, consulte a Tabela de regiões da infraestrutura global.
- É possível entregar dados a uma instância do EC2 em execução na mesma região que a antena, ou você pode usar a entrega de dados entre regiões para enviar os dados de uma antena para uma instância do EC2 na região da AWS preferida. As seguintes antenna-to-destination regiões estão disponíveis no momento:
  - 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)

Termos de Serviço

Você só pode usar os Serviços para armazenar, recuperar, consultar, fornecer e executar Seu conteúdo, que é de sua propriedade e está licenciado ou foi legalmente obtido por você. Como usado nestes Termos de Serviço, (a) "Seu conteúdo" inclui qualquer "Conteúdo da empresa" e qualquer "Conteúdo do cliente" e (b) "Conteúdo da AWS" inclui "Propriedades da Amazon". Como parte dos Serviços, você pode ter permissão para usar determinados programas de software (incluindo a documentação relacionada) fornecidos por nós ou por licenciadores de terceiros.

> **Important**
>
> Esse software não foi vendido nem distribuído para você, e você poderá usá-lo somente como parte dos Serviços. Você não poderá transferi-lo para fora dos Serviços sem autorização específica para assim fazê-lo.

Componentes principais

Grupos de endpoints, configurações e perfis de missão do Dataflow são os principais componentes do. AWS Ground Station Esses componentes determinam como você agenda os contatos, como as antenas se comunicam com os satélites e onde os dados são entregues. Antes de começar AWS

Ground Station, recomendamos que você aprenda sobre esses componentes. Os exemplos são fornecidos nas respectivas seções.

Tópicos

Grupos de endpoints de fluxo de dados

Os endpoints de fluxo de dados definem o local onde você deseja que o streaming de dados seja enviado ou recebido durante contatos. Os endpoints são identificados por um nome de sua escolha ao executar contatos. Esses nomes não precisam ser exclusivos. Isso permite que vários contatos sejam executados ao mesmo tempo usando o mesmo perfil de missão.

O endereço da lista de endpoints consiste no seguinte:

- `name`: endereço IP do endpoint de fluxo de dados.
- `port`: a porta à qual conectar-se.

Os detalhes de segurança de um endpoint consistem nos seguintes:

- `roleArn`- O Amazon Resource Name (ARN) de uma função que AWS Ground Station assumirá a criação de Elastic Network Interfaces (ENIs) em sua VPC. Essas ENIs servirão como pontos de entrada e saída dos dados transmitidos durante um contato.
- `securityGroupIds`: os grupos de segurança a serem anexados às interfaces de rede elástica.
- `subnetIds`- Uma lista de sub-redes onde AWS Ground Station coloca interfaces de rede elásticas para enviar fluxos para suas instâncias.

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 os ENIs. 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 uma função, consulte Gerenciar funções 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 funções 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"
      ]
    }
  ]
}
```

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.

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.

Os grupos de endpoints do Dataflow devem estar em condições `HEALTHY` de programar contatos com eles. 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 instância do EC2, que registrará o atendente. Observe que você deve ter um arquivo de configuração de controlador válido para que essa chamada seja bem-sucedida. Consulte o AWS Ground Station Guia do usuário do agente 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 do 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 Usar funções vinculadas ao serviço para o Ground Station

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::DataflowEndpointTipo de CloudFormation recurso de grupo
- Referência do Dataflow Endpoint Group AWS CLI
- Referência da API do Dataflow Endpoint Group

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.

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 endpoint de fluxo de dados

> **Note**
>
> As configurações de endpoint do Dataflow são usadas somente para entrega de dados para o 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 que contenha todos os endpoints de fluxo de dados especificados pelas configurações de endpoint de fluxo de dados contidas em seu perfil de missão.

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 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

Configuração de gravação S3

> **Note**
>
> As configurações de gravação no S3 são usadas apenas para a entrega de dados no Amazon S3 e não são usadas para a entrega de dados no Amazon EC2.

Você pode usar as configurações de gravação do S3 para especificar um bucket do Amazon S3 para o qual deseja que dados baixados sejam entregues. Os dois parâmetros de uma configuração

de gravação do S3 especificam o bucket do Amazon S3 e a função AWS Ground Station do IAM a serem assumidos ao entregar os dados ao seu bucket do Amazon S3. O perfil do IAM e o bucket do Amazon S3 especificados devem atender aos seguintes critérios:

- 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.
- 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 confiança

Para obter mais informações sobre como atualizar a política de confiança de uma função, consulte Gerenciar funções 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"
        }
      }
```

```
    }
  ]
}
```

Exemplo de política de funções

Para obter mais informações sobre como atualizar a política de confiança de uma função, consulte Gerenciar funções 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/*"
      ]
    }
  ]
}
```

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

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.

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. 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 demodulação de downlink de antena são um tipo de configuração mais complexa e personalizável que você pode usar para executar contatos de downlink com demodulação e decodificação. Se você estiver interessado em executar esses tipos de contatos, entre em contato com a AWS Ground Station equipe. Nós lhe ajudaremos a definir a configuração e o perfil de missão certos para seu caso de uso.

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 de 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 Config Uplink Echo.

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

Config Uplink Echo

As configurações de eco de uplink informam à antena como executar um eco de uplink. O sinal enviado pela antena é ecoado de volta para o endpoint de fluxo de dados. 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.

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

Perfis de 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.

Além das configurações de rastreamento, todas as configurações são contidas no campo `dataflowEdges` do perfil de missão. Uma única borda de fluxo de dados é uma lista de dois ARNs: o primeiro é a configuração de e o segundo é a configuração para. 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. As configurações de rastreamento não são usadas como parte de uma borda de fluxo de dados, mas são especificadas como um campo separado.

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

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

- AWS::GroundStation::MissionProfile CloudFormation tipo de recurso
- AWS CLI Referência do Perfil da Missão
- Referência da API do perfil da missão

Locais AWS Ground Station

Os clientes podem transmitir e receber dados usando antenas do AWS Ground Station nos seguintes locais: EUA (Oregon), EUA (Ohio), EUA (Alasca), Oriente Médio (Bahrein), Europa (Estocolmo), Ásia-Pacífico (Dubbo), Europa (Irlanda), África (Cidade do Cabo), EUA (Havaí), Ásia-Pacífico (Seul), Ásia-Pacífico (Singapura) e América do Sul (Punta Arenas).

Os clientes podem fornecer dados e configurar seus contatos com o console do AWS Ground Station nas seguintes regiões: Oeste dos EUA (Oregon), Leste dos EUA (Ohio), Oriente Médio (Bahrein), Europa (Estocolmo), Ásia-Pacífico (Dubbo), Europa (Irlanda), África (Cidade do Cabo), Leste dos EUA (Norte da Virgínia), Europa (Frankfurt), Ásia-Pacífico (Seul), Ásia-Pacífico (Singapura) e América do Sul (São Paulo).

Observação: você só pode criar recursos do AWS Ground Station nas regiões que hospedam o console do AWS Estações terrestres mencionado no parágrafo anterior.

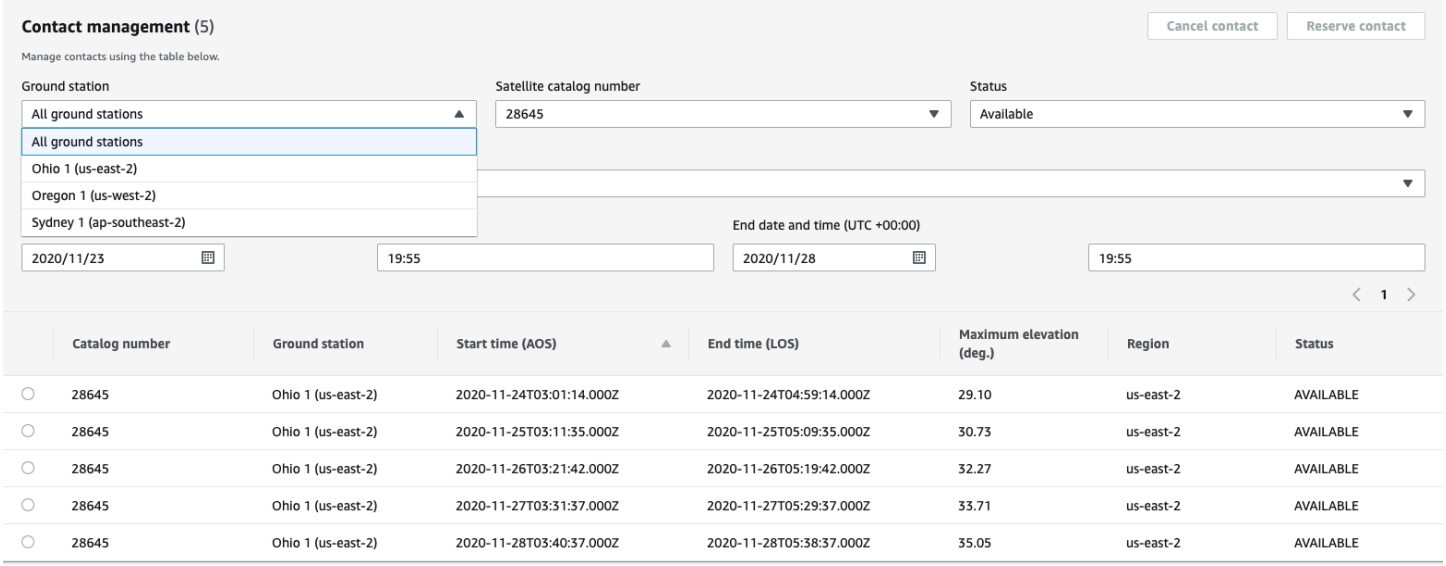
Tópicos

- Encontrar a região da AWS para uma estação terrestre

Encontrar a região da AWS para uma estação terrestre

A rede global da AWS inclui locais de estações terrestres que não estão fisicamente localizados na região da AWS à qual estão conectados. A listagem e a reserva de contatos em um desses locais de estações terrestres devem ser realizadas usando a região da AWS à qual a estação terrestre está conectada.

Há vários métodos para determinar a região da AWS de uma estação terrestre. A página do console do AWS Ground Station exibe a região da AWS da estação terrestre ao exibi-la na tabela de filtros e contatos, conforme mostrado na imagem abaixo. O SDK da AWS contém a região da AWS da estação terrestre na resposta ListGroundStation. Por fim, a AWS CLI inclui a região da AWS estação terrestre na resposta da lista de estações terrestres ListGroundStation.



Tópicos

- Exemplo de estação terrestre localizada fora de uma região da AWS

Exemplo de estação terrestre localizada fora de uma região da AWS

Hawaii 1 é um exemplo de localização de estação terrestre que não está fisicamente localizada na região da AWS à qual está conectada. A Estação terrestre Hawaii 1 está localizada no Havaí, EUA, mas está conectada à região us-west-2 (Oregon) da AWS. Para listar e reservar contatos usando Hawaii 1, você deve ter um perfil de missão configurado na região da AWS us-west-2 (Oregon) e usar a região da AWS us-west-2 (Oregon) no console do AWS Ground Station, na CLI da AWS ou no SDK da AWS.

- Para listar e reservar contatos para Hawaii 1 no console do AWS Ground Station, você deve usar o console do AWS Ground Station na região us-west-2 (Oregon).
- Para listar e reservar contatos para Hawaii 1 usando a AWS CLI, você deve especificar a região como us-west-2 usando o argumento da CLI `--region`.
- Para listar e reservar contatos para Hawaii 1 usando o AWS SDK, você deve definir a região do seu cliente como us-west-2. A forma como você define isso depende da linguagem de programação que você está usando. Um exemplo de como definir isso usando JavaScript está descrito na documentação do AWS SDK para JavaScript. Para obter mais informações, consulte o idioma específico de documentação do SDK.

Configuração AWS Ground Station

Antes de começar a usar AWS Ground Station, você precisa saber quais permissões AWS Identity and Access Management (IAM) você precisa e quais credenciais de veículo espacial fornecer. Use as etapas a seguir para configurar a conta.

Tópicos

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 https://portal.aws.amazon.com/billing/signup.
2. Siga as instruções on-line.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica e digitar um código de verificação no 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, é possível visualizar as atividades da conta atual e gerenciar sua conta acessando https://aws.amazon.com/ e selecionando 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, digite sua senha.

   Para obter ajuda ao fazer login usando o usuário raiz, consulte Signing in as the root user (Fazer login como usuário raiz) no Guia do usuário Início de Sessão da AWS .
2. Ative a autenticação multifator (MFA) para seu 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. Habilitar o IAM Identity Center.

   Para obter instruções, consulte Habilitar AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center .
2. No Centro de Identidade do IAM, conceda o acesso administrativo para 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 seu usuário IAM Identity Center, use a URL de login enviada ao seu endereço de e-mail quando você criou o usuário IAM Identity Center user.

  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 Create a permission set 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 Add groups no Guia do usuário do AWS IAM Identity Center .

Adicione permissões do Ground Station 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.

Integração de clientes

Para concluir o registro da sua AWS Ground Station conta, consulte a seção Satélites e recursos na página do AWS Ground Station console para obter detalhes sobre a integração. A AWS Ground Station equipe trabalhará com você para integrar seus satélites ao serviço. Após integrar o satélite, ele estará disponível para uso ao gerenciar um contato. As instruções para gerenciar um contato são fornecidas posteriormente em Listar e reservar contatos.

A integração do(s) satélite(s) permitirá acesso para receber e enviar dados de e para o satélite. Além de integrar os próprios satélites, os clientes também podem integrar os seguintes satélites para fazer downlink de dados de transmissão direta usando o AWS Ground Station:

- 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. Instruções e detalhes para acessar e usar esse modelo são fornecidos na seção Crie seus recursos usando um AWS CloudFormation modelo do guia do usuário.

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.

Próximos Passos

Sua AWS Ground Station conta agora está configurada e pronta para configuração. Continue em Conceitos básicos para configurar os recursos e usar o AWS Ground Station.

Começando com AWS Ground Station

AWS Ground Station permite que você comande, controle e faça o downlink de dados de seus satélites.

Com AWS Ground Station, você pode programar o acesso às antenas da estação terrestre por minuto e pagar somente pelo tempo de uso da antena. AWS Ground Station entrega seus dados de contato de forma assíncrona para um bucket do Amazon Simple Storage Service (Amazon S3) em sua conta ou de forma síncrona, transmitindo-os de e para uma instância do Amazon Elastic Compute Cloud (Amazon EC2) em sua conta. As etapas a seguir descrevem como configurar os recursos necessários para transmitir dados de contato de e para um bucket do Amazon S3. Consulte o guia Entrega de dados para Amazon EC2 para obter informações sobre a entrega de dados do Amazon EC2.

Tópicos

Conceitos básicos

Antes de começar, você deve se familiarizar com os conceitos básicos do. AWS Ground Station Para ter mais informações, consulte Componentes principais.

Em seguida, Pré-requisitos continue aprendendo sobre os pré-requisitos para começar. AWS Ground Station

Pré-requisitos

Antes de começar AWS Ground Station, verifique se você tem uma AWS conta com as credenciais adequadas. Siga as etapas em Configuração AWS Ground Station.

> **Note**
>
> Se você for usar o DigiF Data Delivery de banda larga, consulte o AWS Ground Station Guia do usuário do agente para ver as instruções.

Caso contrário, avance para Etapa 1: escolha um AWS CloudFormation modelo.

Etapa 1: escolha um AWS CloudFormation modelo

Depois de embarcar no satélite, você precisa definir perfis de missão para definir a configuração da AWS Ground Station antena para baixar os dados do seu satélite. Para ajudá-lo nesse processo, fornecemos AWS CloudFormation modelos pré-configurados para entrega de dados DigiF de banda estreita e banda larga que usam satélites de transmissão pública. Esses modelos facilitam o início do uso AWS Ground Station. Para obter mais informações sobre AWS CloudFormation, consulte O que é a AWS CloudFormation?

Dependendo do tipo de contato que você gostaria de receber, escolha o tipo de modelo de CFN apropriado na lista abaixo:

- Modelos de entrega de dados S3 de banda estreita AWS CloudFormation.
- Modelos de entrega de dados DigIf S3 de banda larga AWS CloudFormation.

Se você não quiser usar um dos AWS CloudFormation modelos predefinidos, você pode ver as instruções emConstruir o próprio modelo.

Modelos de entrega de dados S3 de banda estreita AWS CloudFormation

Modelos pré-configurados

Atualmente, é possível configurar vários fluxos de dados por contato para fluxo em seu bucket S3. Esses fluxos de dados estão disponíveis em dois formatos. Os fluxos de dados que contêm dados de sinal VITA-49/IP podem ser configurados para sinais S-Band e X-Band com até 54 MHz na largura de banda. Os dados de extensão VITA-49/IPs podem ser configurados para sinais demodulados e/ou decodificados X-Band com até 500 MHz na largura de banda.

AWS Ground Station fornece modelos para os dois formatos de fluxo de dados que demonstram como usar o serviço. Use este guia para encontrar o modelo certo para você.

Modelos disponíveis

É possível usar um modelo pré-configurado para receber dados de transmissão direta dos satélites Aqua, SNPP, JPSS-1/NOAA-20 e Terra. Esses AWS CloudFormationmodelos contêm os recursos necessários AWS Ground Station e do Amazon S3 para agendar e executar contatos e receber os dados em um bucket do Amazon S3 em sua conta. Se o Aqua, SNPP, JPSS-1/NOAA-20 e o Terra não estiverem integrados à conta, consulte Integração de clientes.

Modelos de entrega de dados em banda estreita

Se você estiver usando a entrega de dados de banda estreita para seu contato, use os AWS CloudFormation modelos abaixo.

- O AWS CloudFormation modelo nomeado `AquaSnppJpss-1DemodDecodeS3DataDelivery.yml` contém um bucket Amazon S3 e os AWS Ground Station recursos necessários para agendar contatos e receber dados de transmissão direta demodulados e decodificados. Esse modelo é um ótimo ponto de partida se deseja processar os dados usando o software NASA Direct Readout Labs (RT-STPS e IPOPP).

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

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

- 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. Esse modelo é um bom ponto de partida se você planeja processar os

dados usando um rádio definido por software (SDR) para demodular e decodificar os dados antes do pós-processamento.

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
```

Quais recursos o modelo define?

Ambos os modelos contêm os mesmos recursos, com a única diferença sendo as configurações da antena. Para obter mais informações, consulte Configuração de antena.

- Amazon S3 Bucket: o bucket para o qual os dados baixados serão entregues. O nome desse bucket começa com `aws-groundstation` para atender aos critérios descritos no Configuração de gravação do S3.
- Função do IAM - Uma função assumida pelo diretor de `groundstation.amazonaws.com` serviço que AWS Ground Station assume ao gravar os dados desvinculados em seu bucket do Amazon S3.
- Política de bucket do Amazon S3: uma política que permite que o perfil do IAM execute as seguintes ações em seu bucket do Amazon S3 e seus objetos:
  - `s3:GetBucketLocation`
  - `s3:PutObject`
- Configuração de rastreamento - Uma configuração de AWS Ground Station rastreamento que define como o sistema de antena rastreia seu satélite à medida que ele se move pelo céu.

- Configuração de gravação do S3 — AWS Ground Station Uma configuração de gravação do S3 que faz referência ao bucket do Amazon S3 e à função do IAM AWS Ground Station para uso ao entregar seus dados.
- Configuração da antena - AWS Ground Station Uma configuração de antena que especifica como configurar AWS Ground Station a antena durante um contato. O `AquaSnppJpss-1DemodDecodeS3DataDelivery.yml` modelo contém uma configuração de decodificação de demod de downlink de antena que configura a AWS Ground Station antena para demodular e decodificar os dados de downlink antes de entregá-los ao seu bucket do Amazon S3. `AquaSnppJpss-1TerraDigIfS3DataDelivery.yml`Em vez disso, contém uma configuração de downlink de antena que configura a AWS Ground Station antena para entregar os dados ao seu Amazon S3 como pacotes de sinal/IP VITA-49.
- Perfil de missão - Um perfil de AWS Ground Station missão que agrupa todas AWS Ground Station as configurações para permitir que você agende e execute contatos usando as configurações referenciadas.

Modelos de entrega de dados DigIf S3 de banda larga AWS CloudFormation

Modelos de entrega de dados DigiF de banda larga

Se você estiver usando a entrega de dados de frequência intermediária digital de banda larga (DigiF) para seu contato, use os modelos abaixo. AWS CloudFormation

- O AWS CloudFormation modelo nomeado `DirectBroadcastSatelliteWbDigIfS3DataDelivery.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 por meio do Agente. AWS Ground Station Esse modelo é um bom ponto de partida se você planeja processar os dados usando um rádio definido por software (SDR) para demodular e decodificar os dados antes do pós-processamento. Para obter mais informações sobre o AWS Ground Station Agente, consulteAWS Ground Station Guia do usuário do agente.

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

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

Quais recursos o modelo define?

- Amazon S3 Bucket: o bucket para o qual os dados baixados serão entregues. O nome desse bucket começa com `aws-groundstation` para atender aos critérios descritos no Configuração de gravação do S3.
- Função do IAM - Uma função assumida pelo diretor de `groundstation.amazonaws.com` serviço que AWS Ground Station assume ao gravar os dados desvinculados em seu bucket do Amazon S3.
- Política de bucket do Amazon S3: uma política que permite que o perfil do IAM execute as seguintes ações em seu bucket do Amazon S3 e seus objetos:
  - `s3:GetBucketLocation`
  - `s3:PutObject`
- AWS KMS Chave - Uma AWS KMS chave usada para criptografar fluxos de dados.
- Função chave da Ground Station - A função do IAM que AWS Ground Station assumirá o acesso e o uso da AWS KMS chave para descriptografar fluxos de dados
- Política de acesso à chave da Ground Station - A política do IAM que define as ações que AWS Ground Station podem ser tomadas na chave de entrega de dados
- Configuração de rastreamento - Uma configuração de AWS Ground Station rastreamento que define como o sistema de antena rastreia seu satélite à medida que ele se move pelo céu.
- Configuração de gravação do S3 — AWS Ground Station Uma configuração de gravação do S3 que faz referência ao bucket do Amazon S3 e à função do IAM AWS Ground Station para uso ao entregar seus dados.

- Configurações de antena para Aqua, SNPP, JPSS-1/NOAA-20 e Terra - Três configurações de antena separadas que especificam como configurar a AWS Ground Station antena durante um contato com Aqua, SNPP, JPSS-1/NOAA-20 e Terra. AWS Ground Station O modelo contém uma configuração de downlink de antena que configura a AWS Ground Station antena para entregar os dados ao seu Amazon S3 como pacotes de sinal/IP VITA-49.
- Perfis de missão para Aqua, SNPP, JPSS-1/NOAA-20 e Terra - Três perfis de AWS Ground Station missão separados que agrupam todas as configurações para permitir que você agende e execute contatos usando as AWS Ground Station configurações referenciadas com Aqua, SNPP, JPSS-1/NOAA-20 e Terra.

Construir o próprio modelo

Configurar os recursos para agendar e executar contatos para seus próprios satélites exige que você configure os AWS Ground Station recursos em sua conta para que correspondam às configurações do seu satélite. Isso é difícil de fazer sozinho. A AWS Ground Station equipe está disponível para ajudá-lo a configurar os AWS Ground Station recursos em sua conta para fazer downlink e uplink para seu satélite. Para configurar seu próprio satélite para uso AWS Ground Station, entre em contato com o AWS Support.

Etapa 2: Configurar uma AWS CloudFormation pilha

Depois de escolher o modelo que melhor se aplica ao seu caso de uso, configure uma AWS CloudFormation pilha. Os recursos criados neste procedimento serão configurados para a região em que você estiver ao criá-los.

1. Em AWS Management Console, escolha Serviços > CloudFormation.
2. No painel de navegação, escolha Pilhas. Escolha Criar pilha > com novos recursos (padrão).
3. Na página Criar pilha, especifique o modelo selecionado em the section called “Etapa 1: escolha um AWS CloudFormation modelo” executando um dos procedimentos a seguir.

   a. Selecione o URL do Amazon S3 como a origem do modelo e copie e cole o URL do modelo que você deseja usar no URL do Amazon S3. Em seguida, escolha Próximo.

   b. Selecione Carregar um arquivo de modelo como origem do modelo e escolha Escolher arquivo. Carregue o modelo que você fez download do the section called “Etapa 1: escolha um AWS CloudFormation modelo”. Em seguida, clique em Próximo.
4. Execute as seguintes etapas na página Especificar detalhes da pilha:

a. Digite um nome na caixa Nome da pilha. Recomendamos usar um nome simples para reduzir a possibilidade de erros no futuro.

b. Escolha Próximo.

5. Configure opções de pilha e opções avançadas para sua instância do Amazon EC2.

a. Adicione todas as tags e permissões nas seções Tags e Permissões.

b. Faça qualquer alteração na Política de pilha, Configuração de reversão, Opções de notificação e Opções de criação de pilha.

c. Escolha Próximo.

6. Depois de revisar os detalhes da pilha, selecione a confirmação de Recursos e escolha Criar pilha.

AWS Ground Station Guia do usuário do agente

Tópicos

Visão geral

O que é o AWS Ground Station agente?

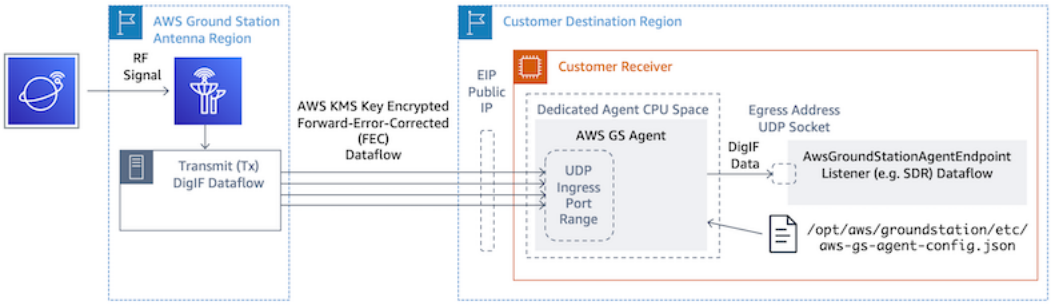
O AWS Ground Station Agent, disponível como RPM, permite que AWS Ground Station os clientes recebam (downlink) fluxos de dados síncronos de frequência intermediária digital de banda larga (DigiF) durante os contatos do AWS Ground Station. Os clientes podem selecionar duas opções para entrega de dados:

1. Entrega de dados para uma instância EC2 - Entrega de dados para uma instância EC2 de propriedade do cliente. AWS Ground Station os clientes gerenciam o AWS Ground Station Agente. Essa opção pode ser mais adequada se você precisar de processamento de dados quase em tempo real. Consulte o guia Entrega de dados para Amazon EC2 para obter informações sobre a entrega de dados do EC2.

2. Entrega de dados para um bucket S3: entrega de dados para um bucket AWS S3 de propriedade do cliente por meio de um serviço gerenciado da Ground Station. Consulte o guia Começando com AWS Ground Station para obter informações sobre a entrega de dados do S3.

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

> **Note**
>
> Como a entrega de dados do S3 é um serviço gerenciado da Ground Station, este guia se concentra na entrega de dados para sua(s) instância(s) do EC2.



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

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

Requisitos do atendente

> **Note**
>
> Este guia AWS Ground Station do agente pressupõe que você tenha embarcado na Ground Station usando o guia. Configuração AWS Ground Station

A instância EC2 do AWS Ground Station agente receptor requer um conjunto de recursos dependentes da AWS para entregar dados DigiF de forma confiável e segura aos seus endpoints.

1. Uma VPC na qual executar o receptor do EC2.
2. Uma chave do AWS KMS para criptografia/descriptografia de dados.
3. Uma chave SSH ou perfil de instância do EC2 configurado para o SSM Session Manager.
4. Regras de rede/grupo de segurança para permitir o seguinte:
    1. Tráfego UDP proveniente das portas especificadas AWS Ground Station no seu grupo de endpoints de fluxo de dados. O atendente reserva uma variedade de portas contíguas usadas para entregar dados ao(s) endpoint(s) do fluxo de dados de entrada.
    2. Acesso SSH à sua instância (nota: como alternativa, você pode usar o AWS Session Manager para acessar sua instância EC2).
    3. Acesso de leitura a um bucket do S3 acessível ao público para gerenciamento de atendentes.
    4. Tráfego SSL na porta 443, permitindo que o agente se comunique com o AWS Ground Station serviço.
    5. Tráfego da lista `com.amazonaws.global.groundstation` de prefixos AWS Ground Station gerenciados.

Além disso, é necessária uma configuração de VPC incluindo uma sub-rede pública. Consulte informações básicas sobre a configuração da sub-rede no Guia do usuário da VPC.

Configurações compatíveis:

1. Um IP elástico associado à instância do EC2 em uma sub-rede pública.
2. Um IP elástico associado a uma ENI em uma sub-rede pública, anexado à instância do EC2 (em qualquer sub-rede).

É possível usar o mesmo grupo de segurança da instância do EC2 ou especificar um com pelo menos o conjunto mínimo de regras que consiste em:

- Tráfego UDP proveniente das portas especificadas AWS Ground Station no seu grupo de endpoints de fluxo de dados.

Consulte a seção “Modelos de entrega de dados DigiF de banda larga” de, Escolher um modelo por exemplo, modelos de entrega de dados AWS CloudFormation EC2 com esses recursos pré-configurados.

Diagramas da VPC

Diagrama: um IP elástico associado à instância do EC2 em uma sub-rede pública

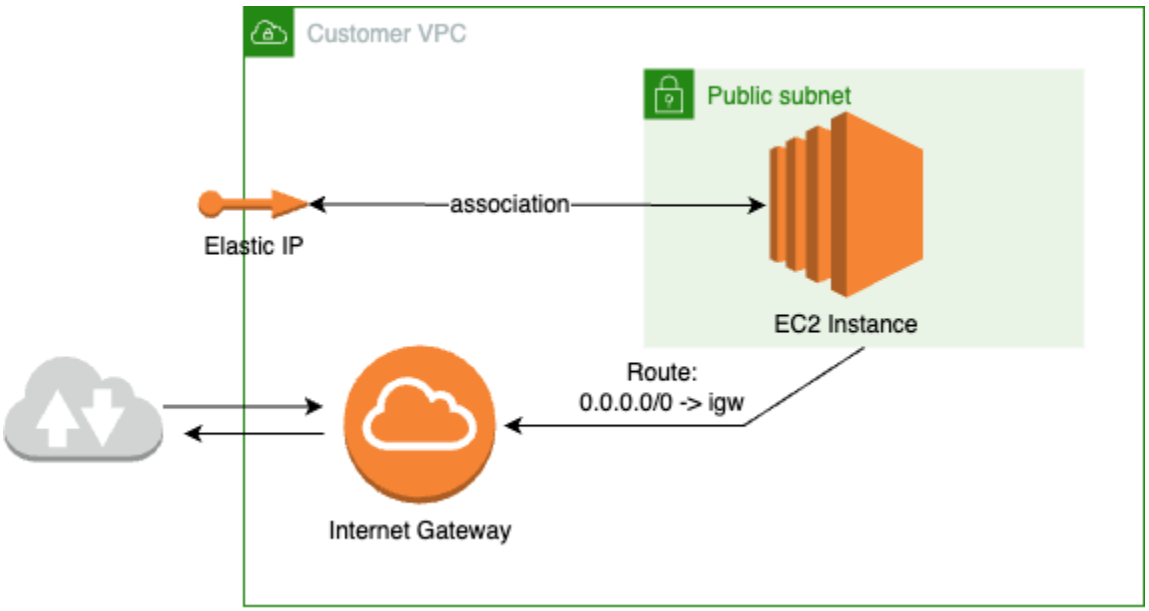
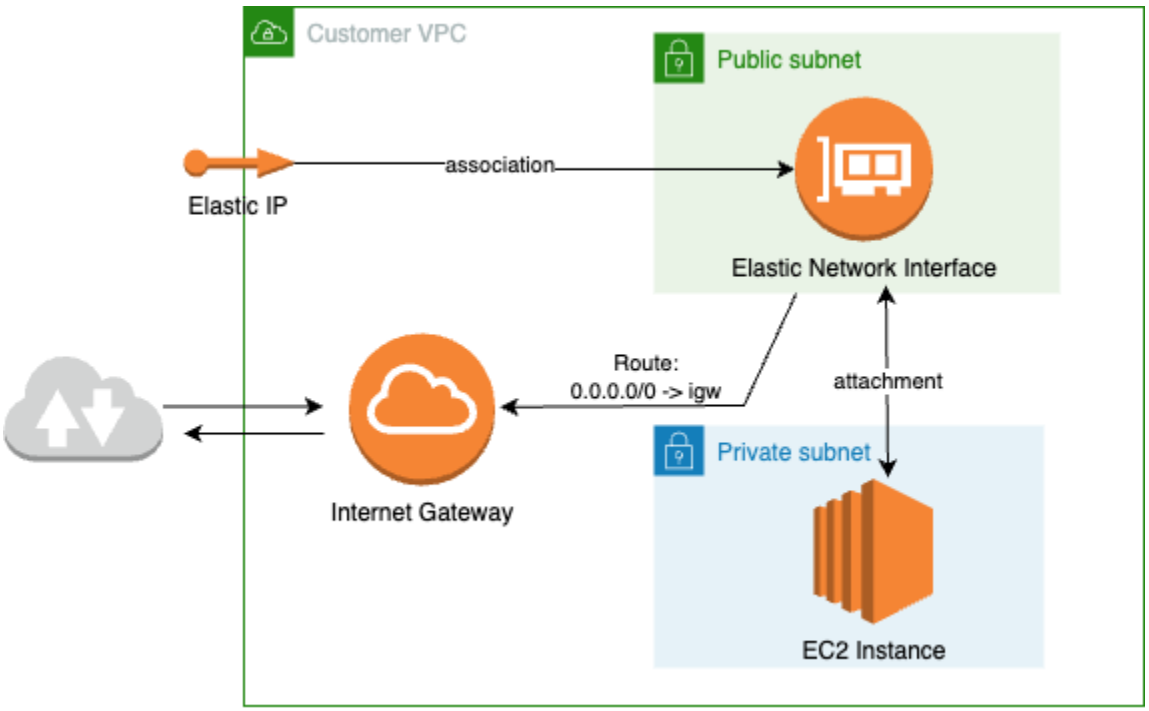


Diagrama: um IP elástico associado a uma ENI em uma sub-rede pública, anexado à instância do EC2 em uma sub-rede privada



Sistema operacional com suporte

Amazon Linux 2 com kernel 5.10+.

Os tipos de instâncias compatíveis estão listados em Seleção de instâncias do EC2 e planejamento de CPU

Entrega de dados via AWS Ground Station agente

Os diagramas abaixo fornecem uma visão geral de como os dados fluem AWS Ground Station durante os contatos de Frequência Intermediária Digital de Banda Larga (DigIF).

O AWS Ground Station agente cuidará da orquestração dos componentes do plano de dados para um contato. Antes de agendar um contato, o agente deve estar corretamente configurado, iniciado e registrado (o registro é automático na inicialização do agente) com AWS Ground Station. Além disso, o software de recebimento de dados (como um rádio definido por software) deve estar em execução e configurado para receber dados no endereço de AwsGroundStationAgentEndpointsaída.

Nos bastidores, o AWS Ground Station Agente receberá tarefas AWS Ground Station e desfará a AWS KMS criptografia aplicada em trânsito, antes de encaminhá-la para o endereço de saída do endpoint de destino onde seu Software Defined Radio (SDR) está ouvindo. O AWS Ground Station

Agente e seus componentes subjacentes respeitarão os limites da CPU definidos no arquivo de configuração para garantir que isso não afete o desempenho de outros aplicativos em execução na instância.

Os clientes devem ter o AWS Ground Station Agente em execução na instância receptora envolvida no contato. Um único AWS Ground Station agente é capaz de orquestrar vários fluxos de dados, conforme mostrado abaixo, se o cliente preferir receber todos os fluxos de dados em uma única instância receptora.

Vários fluxos de dados, único receptor

Exemplo de cenário:

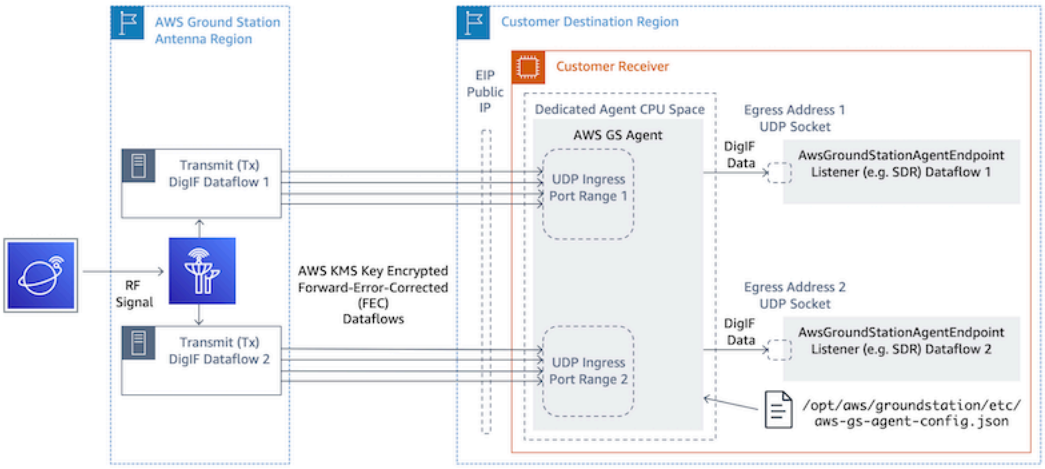
O cliente gostaria de receber dois downlinks de antena como fluxos de dados DigIF na mesma instância do receptor EC2. Os dois downlinks serão de 200 MHz e 100 MHz.

AwsGroundStationAgentEndpoints:

Haverá dois recursos `AwsGroundStationAgentEndpoint`, um para cada fluxo de dados. Ambos os endpoints terão o mesmo endereço IP público (`ingressAddress.socketAddress.name`). As entradas `portRange` não devem se sobrepor, pois os fluxos de dados estão sendo recebidos na mesma instância do EC2. Ambos `egressAddress.socketAddress.port` devem ser exclusivos.

Planejamento de CPU:

- 1 núcleo (2 vCPUs) para executar o único AWS Ground Station agente na instância.
- 6 núcleos (12 vCPU) para receber o DigiF Dataflow 1 (pesquisa de 200 MHz na tabela). Planejamento do núcleo da CPU
- 4 núcleos (8 vCPUs) para receber o DigiF Dataflow 2 (pesquisa de 100 MHz na tabela). Planejamento do núcleo da CPU
- Espaço total de CPU dedicado para agentes = 11 núcleos (22 vCPU) no mesmo soquete.



Vários fluxos de dados, vários receptores

Exemplo de cenário:

O cliente gostaria de receber dois downlinks de antena como fluxos de dados DigIF na mesma instância do receptor EC2. Ambos os downlinks serão de 400 MHz.

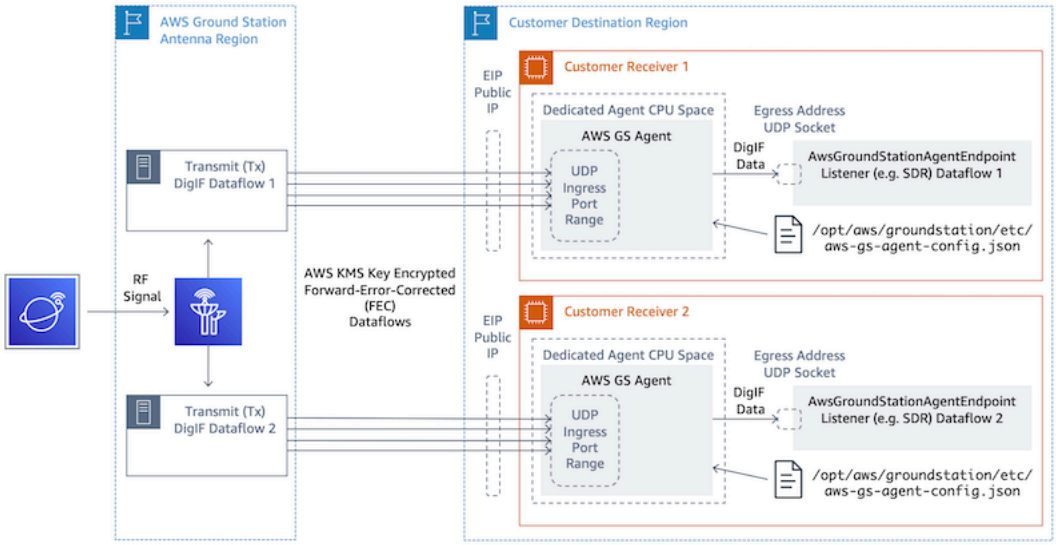
AwsGroundStationAgentEndpoints:

Haverá dois recursos `AwsGroundStationAgentEndpoint`, um para cada fluxo de dados. Ambos os endpoints terão o mesmo endereço IP público (`ingressAddress.socketAddress.name`). Não há restrição quanto aos valores das portas para qualquer um deles, `ingressAddress` ou `egressAddress`, pois os fluxos de dados são recebidos em uma infraestrutura separada e não entrarão em conflito uns com os outros.

Planejamento de CPU:

- Instância do receptor 1
  - 1 núcleo (2 vCPUs) para executar o único AWS Ground Station agente na instância.
  - 9 núcleos (18 vCPUs) para receber o DigiF Dataflow 1 (pesquisa de 400 MHz na tabela). Planejamento do núcleo da CPU
  - Espaço total de CPU dedicado para agentes = 10 núcleos (20 vCPU) no mesmo soquete.
- Instância do receptor 1
  - 1 núcleo (2 vCPUs) para executar o único AWS Ground Station agente na instância.
  - 9 núcleos (18 vCPUs) para receber o DigiF Dataflow 2 (pesquisa de 400 MHz na tabela). Planejamento do núcleo da CPU

- Espaço total de CPU dedicado para agentes = 10 núcleos (20 vCPU) no mesmo soquete.



Seleção de instâncias do EC2 e planejamento de CPU

Tipos de instâncias EC2 compatíveis.

O AWS Ground Station Agente requer núcleos de CPU dedicados para operar devido aos fluxos de trabalho de entrega de dados com uso intensivo de computação. Nós oferecemos suporte aos seguintes tipos de instâncias. Consulte Planejamento do núcleo da CPU para decidir qual tipo de instância é mais adequado ao seu caso de uso.

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão
c5.12xlarge	48	24
c5.18xlarge	72	36
c5.24xlarge	96	48
c5n.18xlarge	72	36
c5n.metal	72	36
c6i.32xlarge	128	64

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão
g4dn.12xlarge	48	24
g4dn.16xlarge	64	32
g4dn.metal	96	48
m4.16xlarge	64	32
m5.12xlarge	48	24
m5.24xlarge	96	48
m6i.32xlarge	128	64
p3dn.24xlarge	96	48
p4d.24xlarge	96	48
r5.24xlarge	96	48
r5.metal	96	48
r5n.24xlarge	96	48
r5n.metal	96	48
r6i.32xlarge	128	64

Planejamento do núcleo da CPU

O AWS Ground Station Agente exige núcleos de processador dedicados que compartilhem o cache L3 para cada fluxo de dados. O atendente foi projetado para aproveitar pares de CPU Hyper-threaded (HT) e exige que os pares HT sejam reservados para seu uso. Um par hyper-threaded é um par de CPUs virtuais (vCPU) contidas em um único núcleo. A tabela a seguir fornece um mapeamento da taxa de dados do fluxo de dados para o número necessário de núcleos reservados para o agente em um único fluxo de dados. Essa tabela pressupõe o Cascade Lake ou CPUs mais recentes e é válida para qualquer tipo de instância compatível. Se sua largura de banda estiver entre as entradas na tabela, selecione a próxima mais alta.

O agente precisa de um núcleo reservado adicional para gerenciamento e coordenação, portanto, o total de núcleos necessários será a soma dos núcleos necessários (da tabela abaixo) para cada fluxo de dados mais um único núcleo adicional (2 vCPUs).

AntennaDownlink Largura de banda (MHz)	Taxa de dados VITA-49,2 DigiF esperada (MB/s)	Número de núcleos (pares de CPU HT)	Total de vCPU
50	1000	3	6
100	2000	4	8
150	3000	5	10
200	4000	6	12
250	5000	6	12
300	6000	7	14
350	7000	8	16
400	8000	9	18

Coletando informações de arquitetura

`lscpu`fornece informações sobre a arquitetura do seu sistema. A saída básica mostra quais vCPUs (rotuladas como “CPU”) pertencem a quais nós NUMA (e cada nó NUMA compartilha um cache L3). Abaixo, examinamos uma `c5.24xlarge` instância para coletar as informações necessárias para configurar o AWS Ground Station Agente. Isso inclui informações úteis, como número de vCPUs, núcleos e associação entre vCPUs e nós.

```
> lscpu
Architecture: x86_64
CPU op-mode(s): 32-bit, 64-bit
Byte Order: Little Endian
CPU(s): 96
```

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

Os núcleos dedicados ao AWS Ground Station Agente devem incluir as duas vCPUs para cada núcleo atribuído. Todos os núcleos de um fluxo de dados devem existir no mesmo nó NUMA. A `-p` opção do `lscpu` comando nos fornece as associações básicas com a CPU necessárias para configurar o agente. Os campos relevantes são CPU (que é o que chamamos de vCPU), Core e L3 (que indica qual cache L3 é compartilhado por esse núcleo). Observe que na maioria dos processadores Intel, o NUMA Node é igual ao cache L3.

Considere o seguinte subconjunto da `lscpu -p` saída para a `c5.24xlarge` (abreviado e formatado para maior clareza).

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

```
19  3    0      0     3   3   3  0
```

Na saída, podemos ver que o Core 0 inclui as vCPUs 0 e 16, o Core 1 inclui as vCPUs 1 e 17, o Core 2 inclui as vCPUs 2 e 18. Em outras palavras, os pares hiperencadeados são: 0 e 16, 1 e 17, 2 e 18.

Exemplo de atribuição de CPU

Como exemplo, usaremos uma `c5.24xlarge` instância para um downlink de banda larga de polaridade dupla a 350 MHz. A partir da tabela, Planejamento do núcleo da CPU sabemos que um downlink de 350 MHz requer 8 núcleos (16 vCPUs) para um único fluxo de dados. Isso significa que essa configuração de polaridade dupla usando dois fluxos de dados requer um total de 16 núcleos (32 vCPUs) mais um núcleo (2 vCPUs) para o Agente.

Conhecemos a `lscpu` saída de `c5.24xlarge` `NUMA node0 CPU(s): 0-23,48-71` includes `NUMA node1 CPU(s): 24-47,72-95` e. Como o NUMA node0 tem mais do que precisamos, atribuiremos apenas a partir dos núcleos: 0-23 e 48-71.

Primeiro, selecionaremos 8 núcleos para cada fluxo de dados que compartilham um cache L3 ou um Nó NUMA. Em seguida, procuraremos as vCPUs correspondentes (denominadas “CPU”) na saída de entrada. `lscpu -p` Apêndice: `lscpu -p` saída (completa) para c5.24xlarge Um exemplo de processo de seleção principal pode ter a seguinte aparência:

- Reserve os núcleos 0-1 para o sistema operacional.
- Fluxo 1: selecione os núcleos 2-9 que são mapeados para vCPUs 2-9 e 50-57.
- Fluxo 2: selecione os núcleos 10-17 que são mapeados para vCPUs 10-17 e 58-65.
- Núcleo do agente: selecione o núcleo 18, que mapeia para as vCPUs 18 e 66.

Isso resulta em vCPUs 2-18 e 51-66, então a lista para fornecer o agente é. `[2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66]` Você deve garantir que seus próprios processos não estejam sendo executados nessas CPUs, conforme descrito emExecutando serviços e processos junto com o AWS Ground Station agente.

Observe que os núcleos específicos selecionados neste exemplo são um tanto arbitrários. Outros conjuntos de núcleos funcionariam desde que satisfizessem a exigência de todos compartilharem um cache L3 para cada fluxo de dados.

Apêndice: `lscpu -p` saída (completa) para c5.24xlarge

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

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

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

Instale o atendente

O AWS Ground Station Agente pode ser instalado das seguintes formas:

1. AWS CloudFormation modelo (recomendado).
2. Instalação manual no Amazon EC2.

Usando o CloudFormation modelo

O CloudFormation modelo de entrega de dados do EC2 cria os recursos necessários da AWS para entregar dados à sua instância do EC2. Esse AWS CloudFormation modelo usa a AMI AWS Ground Station gerenciada que tem o AWS Ground Station Agente pré-instalado. Em seguida, o script de inicialização da instância EC2 criada preenche o arquivo de configuração do atendente e aplica o ajuste de desempenho necessário (Ajuste de desempenho da instância EC2).

Etapa 1: criar recursos da AWS;

Crie sua pilha de recursos da AWS usando um modelo do Modelo DigiF de banda larga via satélite de transmissão direta (banda larga).

Etapa 2: conferir status do atendente

Por padrão, o atendente está configurado e ativo (iniciado). Para verificar o status do atendente, você pode se conectar à instância EC2 (SSH ou SSM Session Manager) e consultar AWS Ground Station Status do agente.

Instalação manual no Amazon EC2

Embora a Ground Station recomende o uso de CloudFormation modelos para provisionar seus recursos da AWS, pode haver casos de uso em que o modelo padrão pode não ser suficiente. Nesses casos, recomendamos que você personalize o modelo de acordo com suas necessidades. Se isso ainda não atender aos requisitos, você poderá criar recursos da AWS manualmente e instalar o atendente.

Etapa 1: criar recursos da AWS

Consulte Criando e configurando recursos manualmente para obter instruções sobre como configurar manualmente os recursos da AWS necessários para um contato.

O AwsGroundStationAgentEndpointrecurso define um endpoint para receber um fluxo de dados DigiF AWS Ground Station via Agent e é fundamental para obter um contato bem-sucedido. Embora a documentação da API esteja localizada na Referência da API, esta seção discutirá brevemente os conceitos relevantes para o AWS Ground Station Agente.

O endpoint `ingressAddress` é onde o AWS Ground Station agente receberá tráfego UDP AWS KMS criptografado da antena. `socketAddress name` é o IP público da instância do EC2 (do EIP anexado). `portRange` deve ter pelo menos 300 portas contíguas em um intervalo que tenha sido reservado para qualquer outro uso. Para obter instruções, consulte Portas de entrada de reserva: impactam a rede. Essas portas devem ser configuradas para permitir o tráfego de entrada UDP no grupo de segurança da VPC em que a instância receptora está sendo executada.

`egressAddress` do endpoint é onde o atendente entregará o fluxo de dados DigiF ao cliente. O cliente deve ter um aplicativo (por exemplo, SDR) recebendo os dados por meio de um soquete UDP nesse local.

Etapa 2: criar uma instância do EC2

As seguintes APIs são compatíveis:

1. AWS Ground Station A AMI - `groundstation-al2-gs-agent-ami-*` onde * é a data em que a AMI foi criada - vem com o agente instalado (recomendado).

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

Etapa 3: baixar e instalar o atendente

> **Note**
>
> As etapas desta seção devem ser concluídas se você não tiver escolhido a AMI do AWS Ground Station agente na etapa anterior.

Baixar o atendente

O AWS Ground Station agente está disponível em buckets S3 específicos da região e pode ser baixado em instâncias EC2 de suporte usando a linha de comando (CLI) da AWS, de `s3://groundstation-wb-digif-software-${AWS::Region}/aws-groundstation-agent/latest/amazon_linux_2_x86_64/aws-groundstation-agent.rpm` onde $ {AWS::Region} se refere a uma das regiões compatíveis do AWS Ground Station Console e do Data Delivery.

Exemplo: baixe a versão rpm mais recente da região us-east-2 da AWS localmente para a pasta / tmp.

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

Se precisar baixar uma versão específica do AWS Ground Station Agente, você pode baixá-la da pasta específica da versão no bucket do S3.

Exemplo: baixe a versão rpm 1.0.2716.0 da região us-east-2 da AWS localmente para a pasta /tmp.

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

> **Note**
>
> Se você quiser confirmar que o RPM que você baixou foi vendido AWS Ground Station, siga as instruções paraValidação da instalação RPM.

Instalar atendente

```
sudo yum install ${MY_RPM_FILE_PATH}

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

Etapa 4: configurar o atendente

Depois de instalar o agente, você deve atualizar o arquivo de configuração do agente. Consulte Configurando o agente.

Etapa 5: aplicar ajuste de desempenho

AWS Ground Station AMI do agente: se você escolheu a AMI do AWS Ground Station agente na etapa anterior, aplique os seguintes ajustes de desempenho.

- Ajuste interrupções de hardware e filas de recebimento: afeta a CPU e a rede
- Portas de entrada de reserva: impactam a rede
- Reinicializar

Outras AMIs: se você escolheu qualquer outra AMI na etapa anterior, aplique todos os ajustes listados em Ajuste de desempenho da instância EC2 e reinicie a instância.

Etapa 6: gerenciar o atendente

Para começar, pare e verifique o status do atendente, consulte Gerenciando o atendente.

Gerenciando o atendente

AWS Ground Station O agente fornece os seguintes recursos para configurar, iniciar, interromper, atualizar, rebaixar e desinstalar o agente usando ferramentas de comando Linux integradas.

Tópicos

AWS Ground Station Configuração do agente

Navegue até`/opt/aws/groundstation/etc`, que deve conter um único arquivo chamado aws-gs-agent-config .json. Consulte Arquivo de configuração do atendente

AWS Ground Station Início do agente

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

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

Deve produzir uma saída mostrando que o atendente está ativo.

```
aws-groundstation-agent.service - aws-groundstation-agent
Loaded: loaded (/usr/lib/systemd/system/aws-groundstation-agent.service; enabled;
 vendor preset: disabled)
```

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

AWS Ground Station Agente Stop

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

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

Deve produzir uma saída mostrando que o atendente está inativo (parado).

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

AWS Ground Station Atualização do agente

1. Faça download da versão mais recente do atendente. Consulte Baixar o atendente.
2. Interrompa o atendente.

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

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

3. Atualizar o atendente.

```
sudo yum update ${MY_RPM_FILE_PATH}

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

# reload the systemd configuration
sudo systemctl daemon-reload

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

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

AWS Ground Station Rebaixamento do agente

1. Baixe a versão do atendente de que você precisa. Consulte Baixar o atendente.
2. Rebaixe o atendente.

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

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

# downgrade the rpm
sudo yum downgrade ${MY_RPM_FILE_PATH}

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

# reload the systemd configuration
```

```
sudo systemctl daemon-reload

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

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

AWS Ground Station Desinstalação do agente

A desinstalação do agente renomeará /opt/aws/groundstation/etc/ .json para aws-gs-agent-config / opt/aws/groundstation/etc/ .json.rpmsave. aws-gs-agent-config Instalar o agente novamente na mesma instância gravará valores padrão para aws-gs-agent-config .json e precisará ser atualizado com os valores corretos correspondentes aos seus recursos da AWS. Consulte Arquivo de configuração do atendente.

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

AWS Ground Station Status do agente

O status do atendente é ativo (o atendente está em execução) ou inativo (o atendente está parado).

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

Um exemplo de saída mostra que o atendente está instalado, inativo (parado) e habilitado (inicia o serviço na inicialização).

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

```
Main PID: 84182 (code=exited, status=0/SUCCESS)
```

AWS Ground Station Informações de RPM do agente

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

A saída é a seguinte:

> **Note**
>
> A “versão” pode ser diferente com base na versão mais recente publicada pelo atendente.

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

Configurando o agente

Depois de instalar o atendente, você deve atualizar o arquivo de configuração do atendente em `/opt/aws/groundstation/etc/aws-gs-agent-config.json`.

Arquivo de configuração do atendente

Exemplo

```
{
  "capabilities": [
    "arn:aws:groundstation:eu-central-1:123456789012:dataflow-endpoint-group/
bb6c19ea-1517-47d3-99fa-3760f078f100"
  ],
  "device": {
  "privateIps": [
    "127.0.0.1"
  ],
  "publicIps": [
    "1.2.3.4"
  ],
  "agentCpuCores":
 [ 24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,72,73,74,75,76,77,78,79,80,81
}
```

Detalhamento do campo

Capacidades

Os recursos são especificados como nomes de recursos da Amazon do Dataflow Endpoint Group.

Obrigatório: verdadeiro

Formato: String Array

- Valores: capacidade ARNs → String

Exemplos:

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

Dispositivo

Esse campo contém campos adicionais necessários para enumerar o “dispositivo” EC2 atual.

Obrigatório: verdadeiro

Formato: objeto

Membros:

- privateIp
- publicIp
- agentCpuCores
- networkAdapters

privateIp

No momento, esse campo não é usado, mas está incluído para futuros casos de uso. Se nenhum valor for incluído, o padrão será [“127.0.0.1”]

Obrigatório: falso

Formato: String Array

- Valores: Endereços IP → String

Exemplo:

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

publicIp

IP elástico (EIP) por grupo de endpoint de fluxo de dados.

Obrigatório: verdadeiro

Formato: String Array

- Valores: Endereços IP → String

Exemplo:

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

agentCPUCores

Isso especifica quais núcleos virtuais são reservados para o aws-gs-agent processo. Consulte Planejamento do núcleo da CPU para ver os requisitos para definir esse valor adequadamente.

Obrigatório: verdadeiro

Formato: Int Array

- Valores: números principais → int

Exemplo:

```
"agentCpuCores": [

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

networkAdapters

Isso corresponde aos adaptadores Ethernet, ou interfaces conectadas aos ENIs, que receberão dados.

Obrigatório: falso

Formato: String Array

- Valores: nomes dos adaptadores Ethernet (pode encontrá-los executando `ifconfig`)

Exemplo:

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

Ajuste de desempenho da instância EC2

> **Note**
>
> Se você provisionou seus recursos da AWS usando CloudFormation modelos, esses ajustes serão aplicados automaticamente. Se você usou uma AMI ou criou manualmente sua instância do EC2, esses ajustes de desempenho devem ser aplicados para obter o desempenho mais confiável.

Lembre-se de reinicializar sua instância depois de aplicar qualquer ajuste.

Tópicos

Ajuste interrupções de hardware e filas de recebimento: afeta a CPU e a rede

Esta seção configura o uso principal da CPU do systemd, SMP IRQs, Receive Packet Steering (RPS) e Receive Flow Steering (RFS). Consulte Apêndice: Parâmetros recomendados para interrupção/

ajuste de RPS para ver um conjunto de configurações recomendadas com base no tipo de instância que você está usando.

1. Afaste os processos do systemd dos núcleos da CPU do atendente.
2. Redirecione as solicitações de interrupção de hardware para fora dos núcleos da CPU do atendente.
3. Configure o RPS para evitar que a fila de hardware de uma única placa de interface de rede se torne um gargalo no tráfego da rede.
4. Configure o RFS para aumentar a taxa de acertos de cache da CPU e, assim, reduzir a latência da rede.

O script `set_irq_affinity.sh` fornecido pelo RPM configura todas as opções acima para você. Adicione ao crontab para que ele seja aplicado em cada inicialização:

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

- `interrupt_core_list`Substitua por núcleos reservados para o kernel e o sistema operacional - normalmente o primeiro e o segundo, juntamente com pares de núcleos hiperencadeados. Isso não deve se sobrepor aos núcleos selecionados acima. (Por exemplo: '0,1,48,49' para uma instância hyper-threaded de 96 CPUs).
- `rps_core_mask` é uma máscara de bits hexadecimal que especifica quais CPUs devem processar pacotes de entrada, com cada dígito representando quatro CPUs. Também deve ser separado por vírgula a cada oito caracteres, começando pela direita. É recomendável permitir todas as CPUs e deixar que o cache cuide do balanceamento.
  - Para ver a lista de parâmetros recomendados para cada tipo de instância, consulte Apêndice: Parâmetros recomendados para interrupção/ajuste de RPS.
- Exemplo de instância de 96 CPUs:

```
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
```

Tune Rx Interrupt Coalescing: impactam a rede

A coalescência de interrupções ajuda a evitar inundar o sistema hospedeiro com muitas interrupções e ajuda a aumentar o throughput da rede. Com essa configuração, os pacotes são coletados e uma única interrupção é gerada a cada 128 microssegundos. Adicione ao crontab para que ele seja aplicado em cada inicialização:

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

- Substitua `interface` pela interface de rede (adaptador Ethernet) configurada para receber dados. Normalmente, é `eth0`, porque essa é a interface de rede padrão atribuída a uma instância do EC2.

Tune Rx Ring Buffer: impactam a rede

Aumente o número de entradas de anel para o buffer de anel Rx para evitar quedas ou sobrecargas de pacotes durante conexões intermitentes. Adicione ao crontab para que ele seja configurado corretamente em cada inicialização:

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

- Substitua `interface` pela interface de rede (adaptador Ethernet) configurada para receber dados. Normalmente, isso ocorre `eth0` porque essa é a interface de rede padrão atribuída a uma instância do EC2.
- Ao configurar uma instância c6i.32xlarge, o comando precisa ser modificado para definir o buffer de anel como `8192` em vez de `16384`.

Ajuste a CPU C-State: impactam a CPU

Defina o estado C da CPU para evitar a ociosidade, o que pode causar a perda de pacotes durante o início de um contato. Requer reinicialização da instância.

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

Portas de entrada de reserva: impactam a rede

Reserve todas as portas no intervalo de portas do endereço de entrada de `AwsGroundStationAgentEndpoint` para evitar conflitos com o uso do kernel. O conflito de uso da porta levará à falha no contato e na entrega de dados.

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

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

Reinicializar

Depois que todos os ajustes forem aplicados com êxito, reinicialize a instância para que os ajustes entrem em vigor.

```
sudo reboot
```

Apêndice: Parâmetros recomendados para interrupção/ajuste de RPS

Esta seção determina os valores de parâmetros recomendados para uso na seção Ajustar interrupções de hardware e filas de recebimento: impactam a CPU e a rede.

Família	Tipo de instância	${interrupt_core_list}	${rps_core_mask}
c6i	• c6i.32xlarge	• 0,1,64,65	• ffffffff, ffffffff, ffffffff, ffffffff
c5	• c5.24xlarge • c5.18xlarge • c5.12xlarge	• 0,1,48,49 • 0,1,36,37 • 0,1,24,25	• ffffffff, ffffffff, ffffffff • ff,ffffffff,ffffffff • ffff,ffffffff
c5n	• c5n.metal • c5n.18xlarge	• 0,1,36,37 • 0,1,36,37	• ff,ffffffff,ffffffff • ff,ffffffff,ffffffff
m5	• m5.24xlarge • m5.12xlarge	• 0,1,48,49 • 0,1,24,25	• ffffffff, ffffffff, ffffffff • ffff,ffffffff
r5	• r5.metal • r5.24xlarge	• 0,1,48,49 • 0,1,48,49	• ffffffff, ffffffff, ffffffff • ffffffff, ffffffff, ffffffff
r5n	• r5n.metal • r5n.24xlarge	• 0,1,48,49 • 0,1,48,49	• ffffffff, ffffffff, ffffffff

Família	Tipo de instância	${interrupt_core_list}	${rps_core_mask}
			• ffffffff, ffffffff, ffffffff
g4dn	• g4dn.metal • g4dn.16xlarge • g4dn.12xlarge	• 0,1,48,49 • 0,1,32,33 • 0,1,24,25	• ffffffff, ffffffff, ffffffff • ffffffff, ffffffff • ffff,ffffffff
p4d	• p4d.24xlarge	• 0,1,48,49	• ffffffff, ffffffff, ffffffff
p3dn	• p3dn.24xlarge	• 0,1,48,49	• ffffffff, ffffffff, ffffffff

Prepare-se para receber um contato DigiF

1. Analise o planejamento do núcleo da CPU para ver os fluxos de dados desejados e forneça uma lista dos núcleos que o atendente pode usar. Consulte Planejamento do núcleo da CPU.
2. Revise o arquivo de configuração do AWS Ground Station agente. Consulte AWS Ground Station Configuração do agente.
3. Confirme se o ajuste de desempenho necessário foi aplicado. Consulte Ajuste de desempenho da instância EC2.
4. Confirme se você está seguindo todas as melhores práticas mencionadas. Consulte Práticas recomendadas.
5. Confirme se o AWS Ground Station agente foi iniciado antes do horário de início do contato agendado por meio de:

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

6. Confirme se o AWS Ground Station agente está íntegro antes do horário de início do contato agendado por meio de:

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

   Verifique se o `agentStatus` do seu `awsGroundStationAgentEndpoint` está ATIVO e se o `auditResults` está SAUDÁVEL.

Práticas recomendadas

Práticas recomendadas para EC2

Siga as melhores práticas atuais do EC2 e garanta disponibilidade suficiente de armazenamento de dados.

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

Agendador Linux

O agendador Linux pode reordenar pacotes em soquetes UDP se os processos correspondentes não estiverem fixados em um núcleo específico. Qualquer thread que envie ou receba dados UDP deve se fixar em um núcleo específico durante a transmissão de dados.

AWS Ground Station Lista gerenciada de prefixos

É recomendável utilizar a lista de prefixos `com.amazonaws.global.groundstation` gerenciada pela AWS ao especificar as regras de rede para permitir a comunicação da antena. Consulte Trabalhar com as listas de prefixos gerenciados pela AWS para obter mais informações sobre Listas de Prefixos Gerenciadas pela AWS.

Limitação de contato único

O atendente AWS Ground Station oferece suporte a vários streams por contato, mas suporta apenas um único contato por vez. Para evitar problemas de agendamento, não compartilhe uma instância

em vários grupos de endpoints de fluxo de dados. Se uma única configuração de atendente estiver associada a vários ARNs DFEG diferentes, ela falhará no registro.

Executando serviços e processos junto com o AWS Ground Station agente

Ao iniciar serviços e processos na mesma instância do EC2 do AWS Ground Station agente, é importante vinculá-los a vCPUs que não estão sendo usadas pelo AWS Ground Station Agente e pelo kernel Linux, pois isso pode causar gargalos e até mesmo perda de dados durante os contatos. Esse conceito de vinculação a vCPUs específicas é conhecido como afinidade.

Núcleos a serem evitados:

- `agentCpuCores`de Arquivo de configuração do atendente
- `interrupt_core_list` do Ajuste interrupções de hardware e filas de recebimento: afeta a CPU e a rede.
  - Os valores padrão podem ser encontrados em Apêndice: Parâmetros recomendados para interrupção/ajuste de RPS

Como exemplo, usando uma **`c5.24xlarge`** instância

Se você especificou

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

e fugiu

```
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
```

em seguida, evite os seguintes núcleos:

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

Serviços de afinitização (systemd)

Os serviços recém-lançados serão automaticamente afinizados com os `interrupt_core_list` mencionados anteriormente. Se o caso de uso dos serviços lançados exigir núcleos adicionais ou precisar de núcleos menos congestionados, siga esta seção.

Verifique para qual afinidade seu serviço está configurado atualmente com o comando:

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

Se você ver um valor vazio como`CPUAffinity=`, isso significa que provavelmente usará os núcleos padrão do comando acima `...bin/set_irq_affinity.sh <using the cores here> ...`

Para substituir e definir uma afinidade específica, encontre a localização do arquivo de serviço executando:

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

Abra e modifique o arquivo (usando `vinano`, etc.) e coloque o `CPUAffinity=<core list>` na `[Service]` seção como:

```
[Unit]
...

[Service]
...
CPUAffinity=2,3

[Install]
...
```

Salve o arquivo e reinicie o serviço para aplicar a afinidade com:

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

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

Para obter mais informações, visite: Red Hat Enterprise Linux 8 - Gerenciando, monitorando e atualizando o kernel - Capítulo 27. Configurando políticas de CPU Affinity e NUMA usando systemd.

Processos de afinitização (scripts)

É altamente recomendável que scripts e processos recém-lançados sejam afinizados manualmente, pois o comportamento padrão do Linux permitirá que eles usem qualquer núcleo na máquina.

Para evitar conflitos fundamentais em qualquer processo em execução (como python, scripts bash etc.), inicie o processo com:

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

Se o processo já estiver em execução, use comandos como `pidoftop`, ou `ps` para encontrar a ID do processo (PID) do processo específico. Com o PID, você pode ver a afinidade atual com:

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

e pode modificá-lo com:

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

Para obter mais informações sobre o conjunto de tarefas, consulte conjunto de tarefas - página do manual Linux

Solução de problemas

O atendente falha ao iniciar

O AWS Ground Station Agente pode falhar ao iniciar devido a vários motivos, mas o cenário mais comum pode ser um arquivo de configuração do agente mal configurado. Depois de iniciar o atendente (consulte AWS Ground Station Início do agente), você pode obter um status como:

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

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

Solução de problemas

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

pode resultar em uma saída de:

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

A falha ao iniciar o atendente após “Carregar Config” indica um problema com a configuração do atendente. Consulte Arquivo de configuração do atendente para verificar a configuração do seu atendente.

AWS Ground Station Registros do agente

AWS Ground Station O agente grava informações sobre execuções de contatos, erros e status de saúde em arquivos de log na instância que executa o agente. Você pode visualizar os arquivos de log conectando-se manualmente a uma instância.

É possível visualizar logs do atendente em instâncias nos locais a seguir.

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

Não há contatos disponíveis

O agendamento de contatos requer um AWS Ground Station agente saudável. Confirme se seu AWS Ground Station agente foi iniciado e se está íntegro consultando a AWS Ground Station API por meio get-dataflow-endpoint-group de:

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

Verifique se o `agentStatus` do seu `awsGroundStationAgentEndpoint` está ATIVO e se o `auditResults` está SAUDÁVEL.

Como obter suporte

Entre em contato com a equipe da Ground Station por meio do AWS Support.

1. Forneça `contact_id` todos os contatos afetados. A AWS Ground Station equipe não pode investigar um contato específico sem essas informações.
2. Forneça detalhes sobre todas as etapas de solução de problemas já tomadas.
3. Forneça todas as mensagens de erro encontradas ao executar os comandos em nossa orientação de solução de problemas.

Notas de release do agente

Versão mais recente do agente

Versão 1.0.3555.0

Data de lançamento: 27/03/2024

Data de fim do Support: 31/08/2024

Somas de verificação de RPM:

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

Alterações:

- Adicione a métrica do Agente para a versão executável selecionada durante a inicialização da tarefa.
- Adicione suporte ao arquivo de configuração para evitar versões executáveis específicas quando outras versões estiverem disponíveis.
- Adicione diagnósticos de rede e roteamento.
- Recursos de segurança adicionais.
- Corrige o problema em que alguns erros de relatórios de métricas eram gravados em stdout/journal em vez de no arquivo de log.
- Lide com facilidade com erros de soquete inacessíveis na rede.
- Meça a perda e a latência de pacotes entre os agentes de origem e destino.
- Lance a aws-gs-datapipe versão 2.0 para oferecer suporte aos novos recursos do protocolo e à capacidade de atualizar contatos de forma transparente para o novo protocolo.

Versões obsoletas do agente

Versão 1.0.2942.0

Data de lançamento: 26/06/2023

Data de fim do Support: 31/05/2024

Somas de verificação de RPM:

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

Alterações:

- Foram adicionados registros de erros para quando o Agent RPM é atualizado no disco e precisa ser reiniciado o Agente para que as alterações entrem em vigor.
- Foi adicionada a validação do ajuste de rede para garantir que as etapas de ajuste do guia do usuário do Agente sejam seguidas e aplicadas corretamente.
- Corrija o erro que causava avisos errôneos nos registros do Agente sobre o arquivamento de registros.
- Detecção aprimorada de perda de pacotes.
- Instalação atualizada do Agente para evitar a instalação ou atualização do RPM se o Agente já estiver em execução.

Versão 1.0.2716.0

Data de lançamento: 15/03/2023

Data de fim do Support: 31/05/2024

Somas de verificação de RPM:

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

Alterações:

- Ative o upload de registros quando o agente tiver falhas durante a tarefa.
- Corrija o bug de compatibilidade do Linux nos scripts de ajuste de rede fornecidos.

Versão 1.0.2677.0

Data de lançamento: 15/02/2023

Data de fim do Support: 31/05/2024

Somas de verificação de RPM:

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

Alterações:

- Primeira versão do Agent disponível ao público em geral.

Validação da instalação RPM

A versão mais recente do RPM, o hash MD5 validado a partir do RPM e o hash SHA256 usando sha256sum são mostrados abaixo. Esses valores, combinados, podem ser usados para validar a versão RPM que está sendo usada para o atendente da estação terrestre.

Versão mais recente do agente

Versão 1.0.3555.0

Data de lançamento: 27/03/2024

Data de fim do Support: 31/08/2024

Somas de verificação de RPM:

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

Alterações:

- Adicione a métrica do Agente para a versão executável selecionada durante a inicialização da tarefa.
- Adicione suporte ao arquivo de configuração para evitar versões executáveis específicas quando outras versões estiverem disponíveis.
- Adicione diagnósticos de rede e roteamento.

- Recursos de segurança adicionais.
- Corrige o problema em que alguns erros de relatórios de métricas eram gravados em stdout/journal em vez de no arquivo de log.
- Lide com facilidade com erros de soquete inacessíveis na rede.
- Meça a perda e a latência de pacotes entre os agentes de origem e destino.
- Lance a aws-gs-datapipe versão 2.0 para oferecer suporte aos novos recursos do protocolo e à capacidade de atualizar contatos de forma transparente para o novo protocolo.

Verificar o RPM

As ferramentas necessárias para verificar essa instalação do RPM são:

- sha256sum
- rpm

Ambas as ferramentas vêm por padrão no Amazon Linux 2. Essas ferramentas ajudarão a validar se o RPM que você está usando é a versão correta. Primeiro, baixe o RPM mais recente do bucket S3 (consulte Baixar o atendente para obter instruções sobre como baixar o RPM). Depois que esse arquivo for baixado, haverá algumas coisas a serem verificadas:

- Calcule o sha256sum do arquivo RPM. Execute a ação a seguir na linha de comando da instância de computação que você está usando:

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

  Pegue esse valor e compare-o com a tabela acima. Isso mostra que o arquivo RPM baixado é um arquivo válido para uso e que o AWS Ground Station distribuiu aos clientes. Se os hashes não corresponderem, não instale o RPM e o exclua da instância de computação.
- Verifique também o hash MD5 do arquivo para garantir que o RPM não tenha sido comprometido. Para fazer isso, use a ferramenta de linha de comando RPM executando o seguinte comando:

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

Verifique se o hash MD5 listado aqui é o mesmo que o hash MD5 da versão que está na tabela acima. Depois que esses dois hashes forem validados em relação a essa tabela listada no AWS Docs, o cliente poderá ter certeza de que o RPM baixado e instalado é a versão segura e sem comprometimentos do RPM.

Listar e reservar contatos

Você pode inserir dados de satélite, identificar localizações de antenas, comunicar-se e programar tempo de antena para satélites selecionados usando o console do AWS Ground Station ou a AWS CLI. Você pode revisar, cancelar e reprogramar reservas de contato até oito dias antes do horário programado. 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, consulte Usar o serviço de entrega de dados entre regiões.

Para agendar contatos, os recursos devem estar configurados. Se você não tiver configurado os recursos, consulte Conceitos básicos.

Tópicos

- Usar o console do Ground Station
- Reservando e gerenciando contatos com AWS CLI

Usar o console do Ground Station

Você pode usar o AWS Ground Station console para reservar, visualizar e cancelar reservas de contatos. Para usar o AWS Ground Station console, abra o AWS Ground Station console e escolha Reservar contatos agora.

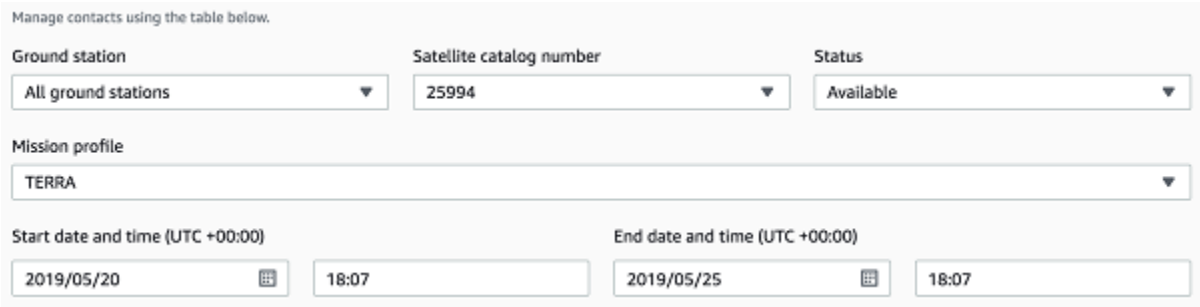
Use os tópicos a seguir para usar o AWS Ground Station console para reservar, visualizar e cancelar contatos.

Tópicos

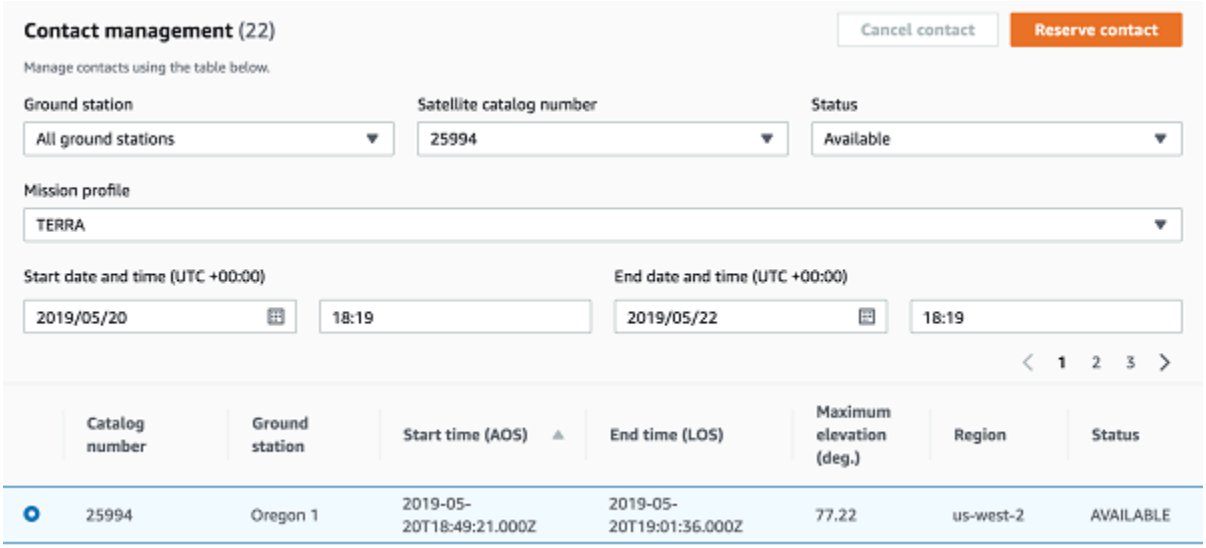
Reservar um contato

Depois de acessar o AWS Ground Station console, use seus recursos configurados para reservar contatos na tabela de gerenciamento de contatos.

1. Na tabela Gerenciamento de contatos, escolha os parâmetros que deseja usar para pesquisar contatos disponíveis. Verifique se está visualizando os contatos Disponíveis usando o filtro Status.



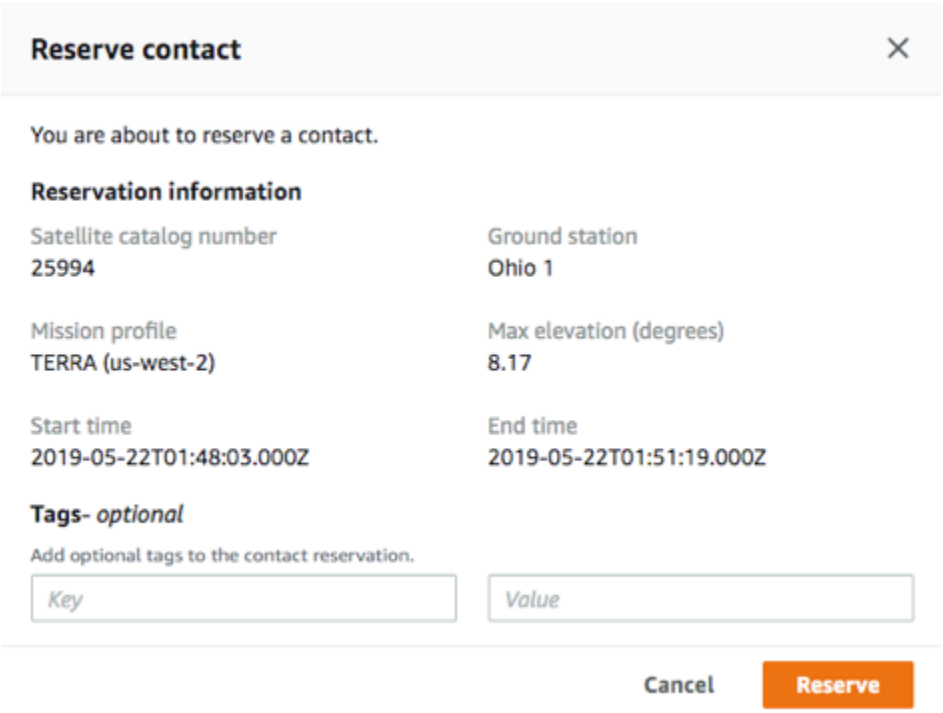
2. Selecione um contato que atenda aos seus requisitos e selecione Reservar contato.



3. Na caixa de diálogo Reservar contato, revise suas informações de reserva de contato.

   a. (Opcional) Em Tags, insira uma chave e um valor para cada tag que deseja adicionar.

   b. Escolha Reservar.

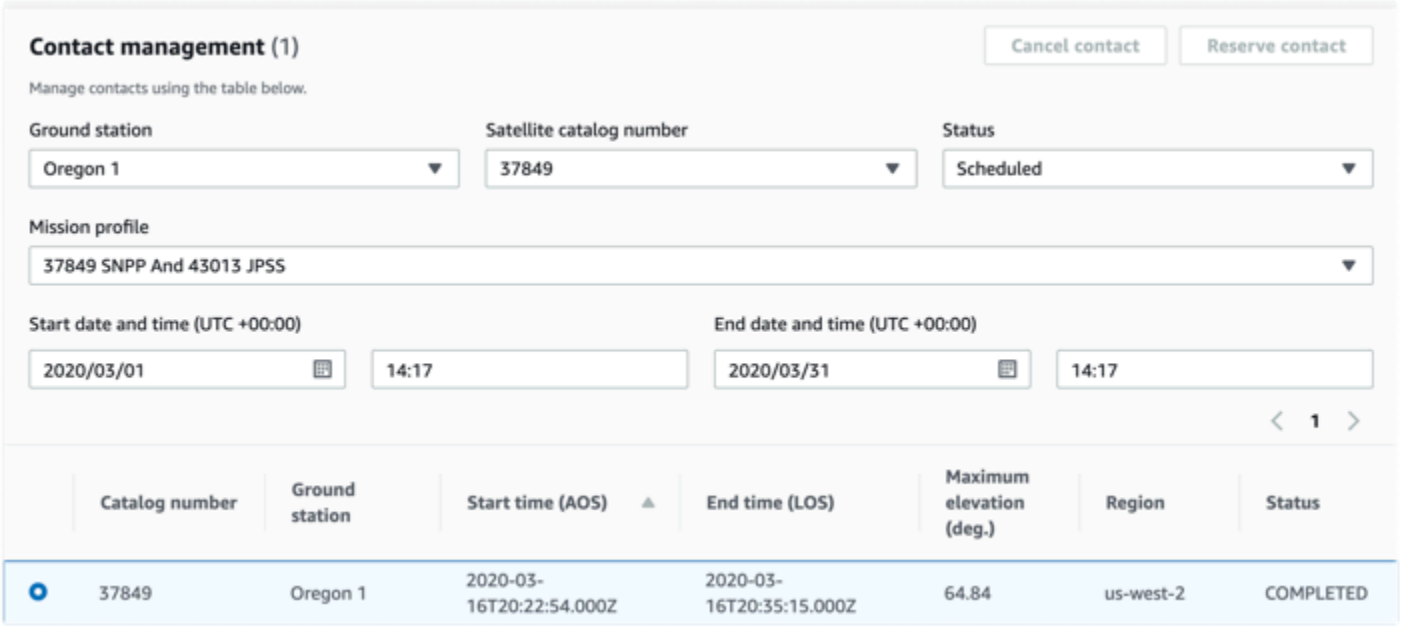


AWS Ground Station usará os dados de configuração do seu perfil de missão para executar um contato na estação terrestre especificada.

Exibir contatos agendados e concluídos

Depois de agendar contatos, você pode usar o AWS Ground Station console para ver os detalhes dos contatos agendados e concluídos.

Na tabela Gerenciamento de contatos, escolha os parâmetros que deseja usar para pesquisar contatos agendados e concluídos. Verifique se está visualizando os contatos Agendados ou Concluídos usando o filtro Status.

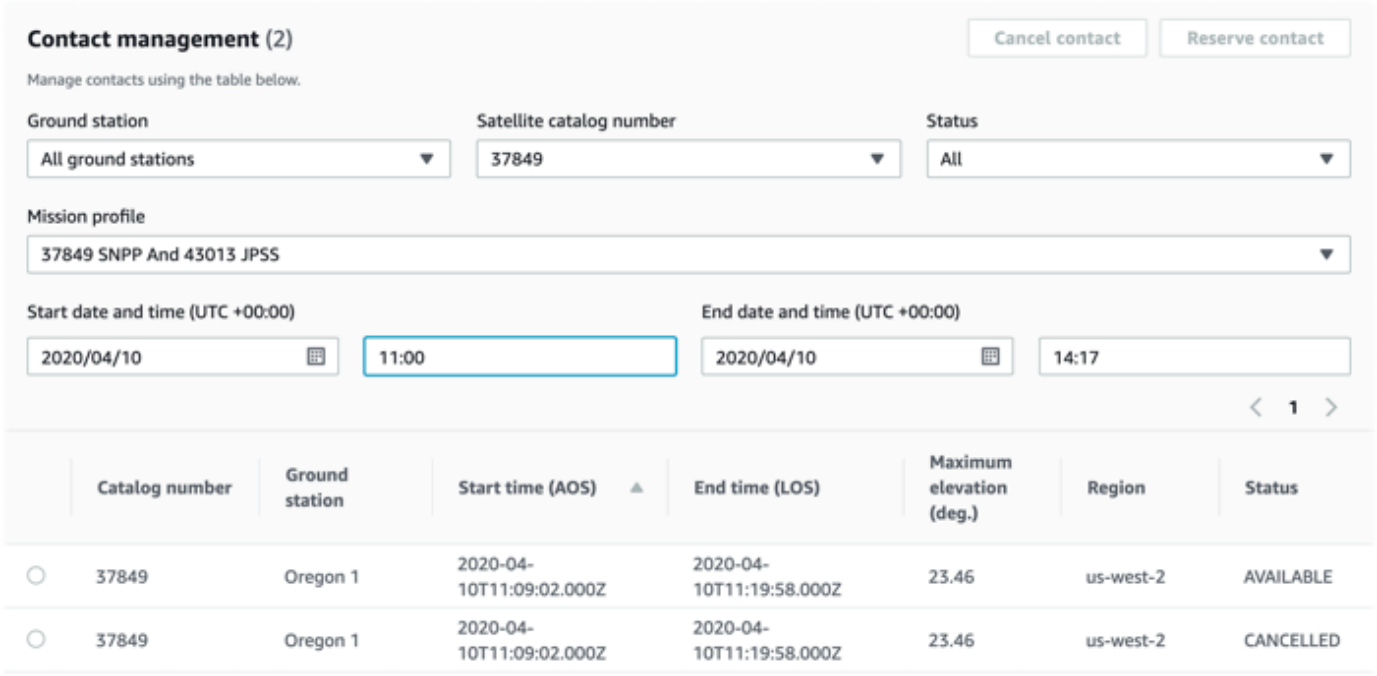


Os contatos agendados ou concluídos serão listados se corresponderem aos parâmetros.

Cancelar contatos

Você pode usar o AWS Ground Station console para cancelar contatos agendados

1. Na tabela Gerenciamento de contatos, escolha os parâmetros que deseja usar para pesquisar contatos agendados e concluídos. Verifique se está visualizando os contatos Agendados usando o filtro Status.
2. Escolha o contato que deseja cancelar na lista de contatos agendados. Depois, escolha Cancelar contato.
3. Na caixa de diálogo Cancelar contato, escolha Ok.



O status do contato será CANCELADO.

Nomeando satélites

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 tag-resource com a CLI da AWS ou um dos SDKs da AWS. 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 a configuração e as definições de credenciais, consulte Definições de configuração e 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 tag-resource 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 AWS Ground Station console.

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 chave "`Name`", mas com um valor diferente na tag. Isso atualizará a tag existente e mostrará o novo nome no console. Um exemplo de URL é:

```
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
```

Reservando e gerenciando contatos com AWS CLI

Você pode usar AWS CLI para reservar e gerenciar seus contatos em AWS Ground Station. Antes de usar AWS CLI para reservar e gerenciar contatos, 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 a configuração e as definições de credenciais, consulte Definições de configuração e 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]
```

Use os tópicos a seguir para reservar, visualizar e cancelar contatos com AWS CLI.

Tópicos

Exibir e listar contatos com AWS CLI

Para listar e visualizar `CANCELLEDCOMPLETED`, ou `SCHEDULED` contatar com AWS CLI, execute `aws groundstation list-contacts` com os seguintes parâmetros.

- Hora de início: especifique a hora de início do contato com `--start-time <value>`. O seguinte formato de valor de tempo é aceitável: `YYYY-MM-DDTHH:MM:SSZ`
- Hora de término: especifique a hora de término do contato com `--end-time <value>`. O seguinte formato de valor de tempo é aceitável: `YYYY-MM-DDTHH:MM:SSZ`
- Lista de status: especifique o status do contato com `--status-list <value>`. Os valores aceitáveis incluem `AVAILABLE`, `CANCELLED`, `COMPLETED` ou `SCHEDULED`. Para ver uma lista completa de valores válidos, consulte list-contacts.

Para listar e visualizar `AVAILABLE` contatos, são necessários AWS CLI os seguintes parâmetros, além dos listados acima.

- ID do Ground Station: especifique o ID do Ground Station com `--ground-station <value>`.
- ARN do perfil da missão: especifique o ARN do perfil da missão com `--mission-profile-arn <value>`.
- ARN do satélite: especifique o ARN do satélite com `--satellite-arn <value>`.

É possível usar comandos `list` para procurar recursos. Para obter mais informações sobre como especificar os parâmetros, consulte list-contacts

Um exemplo de comando para listar contatos disponíveis é fornecido abaixo.

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

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

Um exemplo de uma lista de contatos disponíveis é fornecido abaixo.

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

Reserve um contato com AWS CLI

AWS CLI oferece a opção de reservar contatos a cada minuto. Esse recurso é exclusivo do AWS CLI e não pode ser feito no AWS Ground Station console.

Para reservar contatos com AWS CLI, execute `aws groundstation reserve-contact` com os seguintes parâmetros.

- ID do Ground Station: especifique o ID do Ground Station com `--ground-station <value>`.
- ARN do perfil da missão: especifique o ARN do perfil da missão com `--mission-profile-arn <value>`.
- ARN do satélite: especifique o ARN do satélite com `--satellite-arn <value>`.
- Hora de início: especifique a hora de início do contato com `--start-time <value>`. O seguinte formato de valor de tempo é aceitável: `YYYY-MM-DDTHH:MM:SSZ`

- Hora de término: especifique a hora de término do contato com `--end-time <value>`. O seguinte formato de valor de tempo é aceitável: `YYYY-MM-DDTHH:MM:SSZ`

A reserva de contatos é um processo assíncrono. A resposta ao comando `reserve-contact` fornece o identificador do contato. Para determinar o resultado do processo de reserva assíncrona, use `describe-contact`. Para obter mais informações, consulte a seção Descreva um contato com AWS CLI abaixo.

É possível usar comandos `list` para procurar recursos. Para obter mais informações sobre como especificar os parâmetros, consulte reserve-contact.

Um exemplo de comando para reservar um contato é fornecido abaixo.

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

Um exemplo de contato reservado com êxito é fornecido abaixo.

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

Descreva um contato com AWS CLI

Para ver o status de um contato/reserva com AWS CLI, use o comando CLI`describe-contact`. Isso é útil para verificar o resultado do processo de reserva de contato assíncrono, monitorar o status de um contato em andamento e determinar o status de um contato finalizado.

Para descrever contatos com AWS CLI, execute `aws groundstation describe-contact` com os seguintes parâmetros.

- ID de contato: especifique o ID de contato com `--contact-id <value>`.

É possível usar comandos `list` para procurar recursos. Para obter mais informações sobre como especificar os parâmetros, consulte reserve-contact.

Um exemplo de comando para reservar um contato é fornecido abaixo.

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

Um exemplo de contato cancelado com êxito é fornecido abaixo.

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

Cancelar um contato com AWS CLI

Para cancelar um contato com AWS CLI, execute `aws groundstation cancel-contact` com os seguintes parâmetros.

- Região: especifique a região do Ground Station com `--region <value>`.
- ID de contato: especifique o ID de contato com `--contact-id <value>`.

É possível usar comandos `list` para procurar recursos. Para obter mais informações sobre como especificar os parâmetros, consulte cancel-contacts

Um exemplo de comando para reservar um contato é fornecido abaixo.

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

Um exemplo de contato cancelado com êxito é fornecido abaixo.

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

Entrega de dados para Amazon EC2

AWS Ground Station entrega seus dados de contato de forma assíncrona para um bucket do Amazon Simple Storage Service (Amazon S3) em sua conta ou de forma síncrona, transmitindo-os de e para uma instância do Amazon Elastic Compute Cloud (Amazon EC2) em sua conta. As etapas a seguir descrevem como configurar os recursos necessários para transmitir dados de contato de e para uma instância do Amazon EC2. Consulte o guia Começando com AWS Ground Station para obter informações sobre a entrega de dados do Amazon S3.

Tópicos

Etapa 1: criar par de chaves SSH do EC2

Se você ainda não tiver um, crie um novo par de chaves no console do Amazon EC2 para cada AWS região em que você planeja receber dados. Use as etapas abaixo.

1. No seu AWS Management Console, escolha uma AWS região na qual você planeja reservar contatos. Você precisa criar um par de chaves para cada AWS região que você escolher.

   > **Note**
   >
   > AWS Ground Station ainda não está disponível para todas as regiões. Certifique-se de que AWS Ground Station seja suportado pela AWS região desejada. Para obter mais informações sobre a localização das AWS Ground Station antenas, consulte as perguntas frequentes do AWS Ground Station.

2. Siga o guia Criar pares de chaves no Guia do usuário do Amazon EC2 para criar os pares de chaves.
3. Repita o procedimento para outras AWS regiões, se necessário.

Etapa 2: configurar sua VPC

A configuração completa de uma VPC está além do escopo deste guia. Se não tiver uma VPC existente que já está personalizada, você poderá usar a VPC padrão que é criada na sua conta da AWS . Recomendamos adicionar um Linux bastion à VPC para que você possa usar SSH nas suas instâncias do Amazon EC2 sem anexar um endereço IP público. Para obter mais informações sobre como configurar um Linux bastion em sua VPC, consulte Hosts do Linux Bastion na AWS.

Para sua conveniência, as instruções para adicionar rapidamente um host bastion ao seu ambiente Linux AWS estão abaixo. Embora isso não seja obrigatório, é uma prática recomendada.

1. Faça login na sua AWS conta.
2. Na página Hosts do Linus Bastion na Nuvem AWS: implantação de referência rápida, escolha Lançar início rápido (para nova VPC).
3. Na página Criar pilha, selecione Avançar. O modelo é preenchido com antecedência.
4. Na página de detalhes Especificar pilha, faça edições e alterações nas seguintes caixas:
   a. Digite um nome de pilha para seu host na caixa Nome da pilha.
   b. Em Zonas de disponibilidade, selecione as zonas de disponibilidade que deseja usar para as sub-redes na VPC. Devem ser selecionadas pelo menos duas zonas de disponibilidade.
   c. Para CIDR de acesso externo ao bastion permitido, insira o bloco CIDR do qual você gostaria de habilitar o acesso à SSH. Se não tiver certeza, você pode usar o valor de 0.0.0.0/0 para habilitar o acesso à SSH de qualquer host que tenha a chave SSH.
   d. Para Nome do par de chaves, escolha o nome do par de chaves que você criou em the section called “Etapa 1: criar par de chaves SSH do EC2”.
   e. Para o Tipo de instância Bastion, escolha t2.micro.

      > **Important**
      >
      > O tipo de instância t2.micro não está disponível para a região da Europa (Estocolmo) (eu-north-1). Se você estiver usando AWS Ground Station na região da Europa (Estocolmo) (eu-north-1), escolha t3.micro.

   f. Para o encaminhamento TCP, selecione verdadeiro.
   g. (Opcional) Faça outras edições e alterações conforme necessário. Para personalizar a implantação, você pode alterar a configuração da VPC, escolher o número e o tipo de

instâncias de host bastion, habilitar o encaminhamento TCP ou X11 e habilitar um banner padrão ou personalizado para os hosts bastion.

h. Escolha Próximo.

5. Na página Configurar opções de pilha, faça todas as alterações ou edições necessárias.
6. Escolha Próximo.
7. Revise os detalhes do bastion host e selecione as duas confirmações de recursos. A seguir, selecione Criar Stack.

Etapa 3: escolha e personalize um AWS CloudFormation modelo

Atualmente, é possível configurar vários fluxos de dados por contato para fluxo em sua VPC. Esses fluxos de dados estão disponíveis em dois formatos. Os fluxos de dados que contêm dados de sinal VITA-49/IP podem ser configurados para sinais S-Band e X-Band com até 54 MHz na largura de banda. Os dados de extensão VITA-49/IPs podem ser configurados para sinais demodulados e/ou decodificados X-Band com até 500 MHz na largura de banda.

Depois de integrar seu satélite, será necessário definir perfis de missão e criar instâncias para processar ou enviar por push e receber fluxos de dados no satélite. Para ajudá-lo nesse processo, fornecemos AWS CloudFormation modelos pré-configurados que usam satélites de transmissão pública. Esses modelos facilitam o início do uso AWS Ground Station. Para obter mais informações sobre AWS CloudFormation, consulte O que é a AWS CloudFormation?

É importante observar que você precisará de um software de processamento de dados ou de armazenamento de dados que ouça o lado do host local do Data Defender da instância do Amazon EC2. Este software é o que você usará para armazenar e/ou processar os dados entregues para a instância do EC2 durante um contato.

Definir as configurações da sua instância do Amazon EC2

Os AWS CloudFormation modelos fornecidos nesta seção são configurados para usar os tipos de instância m5.4xlarge do Amazon EC2 por padrão. No entanto, recomendamos que você personalize e escolha as configurações corretas de instância do Amazon EC2 para seu caso de uso. Requisitos como E/S de armazenamento e desempenho da CPU devem ser considerados ao escolher suas configurações de instância. Por exemplo, executar um modem de software em uma instância do receptor pode exigir instâncias otimizadas para computação com mais núcleos e uma velocidade de clock mais alta. A melhor maneira de determinar as configurações corretas de instância para seu

caso de uso é testar suas configurações de instância com sua workload, e o Amazon EC2 facilita a alternância entre as configurações de instância. Use os modelos e personalize as configurações de instância para suas necessidades.

Como recomendação geral, AWS Ground Station incentiva o uso de instâncias que oferecem suporte a redes aprimoradas para seus uplinks e downlinks, como o AWS Nitro System. Para obter mais informações sobre rede avançada, consulte Habilitar a rede avançada com o Elastic Network Adapter (ENA) em instâncias do Linux.

Além de configurar os tipos de instância do Amazon EC2, os modelos configuram AWS CloudFormation as Amazon Machine Images (AMI) básicas a serem usadas para a instância. A AWS Ground Station base contém o software necessário para receber dados do serviço pré-instalado em sua instância do EC2. Para obter mais informações sobre AMIs, consulte Imagens de máquina da Amazon (AMIs).

Criando e configurando recursos manualmente

Os AWS CloudFormation modelos de amostra nesta seção configuram todos os recursos necessários para começar a executar contatos de satélite. Se você preferir criar e configurar manualmente os recursos necessários para começar a executar os contatos de satélite, você precisará fazer o seguinte:

- Crie AWS Ground Station configurações. Para obter mais informações sobre a criação manual de AWS Ground Station configurações, consulte Create Config AWS CLI Command Reference ou Create Config API Reference.
- Crie um perfil de AWS Ground Station missão. Para obter mais informações sobre como criar manualmente um perfil de AWS Ground Station missão, consulte Criar perfil de missão na AWS CLI Command Reference ou Create Mission Profile API Reference.
- Crie um grupo de endpoints de AWS Ground Station fluxo de dados. Para obter mais informações sobre como criar manualmente um grupo de endpoints de fluxo de dados, consulte Create AWS Ground Station Dataflow Endpoint Group AWS CLI Command Reference ou Create Dataflow Endpoint Group API Reference.
- Criar uma instância do EC2. Para obter mais informações sobre como criar manualmente uma instância do EC2 para uso com AWS Ground Station, consulteCriar uma instância do Amazon EC2.
- Defina as configurações do grupo de segurança da sua instância do EC2 para permitir o envio de dados AWS Ground Station de/para sua instância do EC2. Para obter mais informações sobre

como definir manualmente as configurações do grupo de segurança da sua instância do EC2, consulte Criar referência de comando da AWS CLI de grupo de segurança ou Criar referência de API de grupo de segurança.

Escolher um modelo

AWS Ground Station fornece modelos que demonstram como usar o serviço e podem ser acessados de diferentes maneiras. Use este guia para encontrar o modelo certo para você.

Usar um modelo pré-configurado

É possível usar um modelo pré-configurado para receber dados de transmissão direta dos satélites Aqua, SNPP, JPSS-1/NOAA-20 e Terra. Esses modelos contêm os recursos do AWS CloudFormation necessários para agendar e realizar contatos. O `AquaSnppJpss` modelo inclui os AWS CloudFormation recursos necessários para receber dados de transmissão direta demodulados e decodificados. Use esse modelo como ponto de partida se deseja processar os dados usando o software NASA Direct Readout Labs (RT-STPS e IPOPP). O modelo `AquaSnppJpssTerraDigIF` abrange os recursos do AWS CloudFormation necessários para receber dados brutos de transmissão direta da frequência intermediária digitalizada (DigIF). Use este modelo como ponto de partida para processar os dados usando um rádio definido por software (SDR). O `DirectBroadcastSatelliteWbDigIfEc2DataDelivery` modelo inclui os AWS CloudFormation recursos necessários para receber dados brutos de transmissão direta de frequência intermediária digitalizada de banda larga (DigIF) por meio do Agente. AWS Ground Station

Modelos de entrega de dados em banda estreita:

- the section called “AquaSnppJpss Modelo (banda estreita)”
- the section called “AquaSnppJpssTerraDigModelo IF (banda estreita)”

Modelos de entrega de dados DigiF de banda larga:

- the section called “Modelo DigiF de banda larga via satélite de transmissão direta (banda larga)”

> **Important**
>
> Os satélites devem estar integrados ao serviço para acessar as AMIs com os modelos. AWS CloudFormation

Usar os próprios satélites

Configurar os próprios satélites requer um conjunto diferente de parâmetros e recursos. Isso é difícil de fazer sozinho. A AWS Ground Station equipe está disponível para ajudá-lo a configurar seus próprios satélites para uso e pode ajudá-lo a configurar recursos para fluxos de eco de downlink, uplink e uplink. Para configurar seu próprio satélite para uso AWS Ground Station, entre em contato com o AWS Support.

Acessar modelos

Você pode acessar os modelos no bucket do Amazon S3 regional abaixo. Nota: o link a seguir usa um endpoint regional do S3. <us-west-2>Mude para a região na qual você está criando a AWS CloudFormation pilha.

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

Também é possível fazer download dos modelos usando a AWS CLI. Para obter informações sobre como configurar o AWS CLI, consulte Configurando o. AWS CLI

AquaSnppJpss Modelo (banda estreita)

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 instância do Amazon EC2 e os AWS Ground Station recursos necessários para agendar contatos e receber dados de transmissão direta demodulados e decodificados. Esse modelo é um ótimo ponto de partida se deseja processar os dados usando o software NASA Direct Readout Labs (RT-STPS e IPOPP).

Se o Aqua, o SNPP e o JPSS-1/NOAA-20 não estiverem integrados à sua conta, consulte Integração de clientes.

> **Important**
>
> A instância do Amazon EC2 precisa ser interrompida antes de aplicar o modelo. Verifique se a instância está parada até estar pronto para usá-la.

Você pode acessar o modelo ao acessar o bucket do S3 de integração de clientes. Observe que os links abaixo usam um bucket regional do S3. <us-west-2>Mude para a região na qual você está criando a AWS CloudFormation pilha.

> **Note**
>
> As instruções a seguir usam YAML. No entanto, os modelos estão disponíveis no formato YAML ou JSON. Para usar JSON, substitua `<.yml>` por `<.json>`.

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 o modelo define?

O modelo `AquaSnppJpss` inclui os seguintes recursos:

- Função do serviço de entrega de dados - AWS Ground Station assume essa função para criar/excluir ENIs em sua conta para transmitir dados.
- (Opcional) Instância do receptor - A instância do Amazon EC2 que enviará/receberá dados de/para seu satélite usando. AWS Ground Station
  - Grupo de segurança da VPC: o grupo de segurança da Amazon EC2 para a instância de banco de dados.
  - Função da instância: a função da sua instância do Amazon EC2.
  - Perfil de instância: o perfil de instância do Amazon EC2.
  - Grupo com posicionamento em cluster: o posicionamento de grupo em que a instância do Amazon EC2 é executada.
- Dataflow Endpoint Security Group — O grupo de segurança ao qual a interface de rede elástica criada pela AWS Ground Station pertence. Por padrão, esse grupo de segurança permite AWS

Ground Station transmitir tráfego para qualquer endereço IP em sua VPC. É possível modificar isso de forma que limite o tráfego a um conjunto específico de endereços IP.

- Interface de rede de instância de receptor - Uma interface de rede elástica que fornece um endereço IP fixo AWS Ground Station para conexão. Isso é anexado à instância do receptor em `eth1`.
- Anexo da interface da instância do receptor: uma interface de rede elástica anexada à instância do Amazon EC2.
- (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) Verificação EC2 para contatos: a opção de usar o Lambda para configurar um sistema de verificação de suas instâncias do Amazon EC2 para contatos com notificação do SNS. É importante observar que isso pode incorrer em cobranças, dependendo do seu uso atual.
- Grupo de endpoints de fluxo de dados - O grupo de endpoints de AWS Ground Station fluxo de dados que define os endpoints usados para enviar/receber dados de/para seu satélite. Como parte da criação do grupo de endpoints do fluxo de dados, AWS Ground Station cria uma interface de rede elástica em sua conta para transmitir dados.
- Configuração de rastreamento - A configuração de AWS Ground Station rastreamento define como o sistema de antena rastreia seu satélite à medida que ele se move pelo céu.
- 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, use o. AquaSnppJpssTerraDigModelo IF (banda estreita) Essas opções continuarão a se expandir à medida que atualizações e recursos adicionais de software forem lançados.

Além disso, o modelo fornece os seguintes recursos para os satélites Aqua, SNPP, JPSS-1/NOAA-20:

- Uma configuração de demodulação/decodificação de downlink para JPSS-1/NOAA-20 e SNPP e uma configuração de demodulação/decodificação de downlink para Aqua.
- Um perfil de missão para JPSS-1/NOAA-20 e SNPP e um perfil de missão para Aqua.

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 Data Defender para receber o fluxo de AWS Ground Station dados da porta definida pelo endpoint do 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 Grupo. AWS::GroundStation::DataflowEndpoint

AquaSnppJpssTerraDigModelo IF (banda estreita)

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 instância do Amazon EC2 e os AWS CloudFormation recursos necessários para receber dados brutos de transmissão direta do DigiF. Esse modelo é um ótimo ponto de partida para o processamento de dados usando um rádio definido por software (SDR).

Se o Aqua, SNPP, JPSS-1/NOAA-20 e o Terra não estiverem integrados à conta, consulte Integração de clientes.

> **Important**
>
> A instância do Amazon EC2 precisa ser interrompida antes de aplicar o modelo. Verifique se a instância está parada até estar pronto para usá-la.

Você pode acessar o modelo ao acessar o bucket do S3 de integração de clientes. Observe que os links abaixo usam um bucket regional do S3. `<us-west-2>`Mude para a região na qual você está criando a AWS CloudFormation pilha.

> **Note**
>
> As instruções a seguir usam YAML. No entanto, os modelos estão disponíveis no formato YAML ou JSON. Para usar JSON, substitua `<.yml>` por `<.json>`.

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 o modelo define?

O modelo `AquaSnppJpssTerraDigIF` inclui os seguintes recursos:

- Função do serviço de entrega de dados - AWS Ground Station assume essa função para criar/excluir ENIs em sua conta para transmitir dados.
- (Opcional) Instância do receptor - A instância do Amazon EC2 que enviará/receberá dados de/para seu satélite usando. AWS Ground Station
  - Grupo de segurança da VPC: o grupo de segurança da Amazon EC2 para a instância de banco de dados.
  - Função da instância: a função da sua instância do Amazon EC2.
  - Perfil de instância: o perfil de instância do Amazon EC2.
  - Grupo com posicionamento em cluster: o posicionamento de grupo em que a instância do Amazon EC2 é executada.
- Dataflow Endpoint Security Group — O grupo de segurança ao qual a interface de rede elástica criada pela AWS Ground Station pertence. Por padrão, esse grupo de segurança permite AWS Ground Station transmitir tráfego para qualquer endereço IP em sua VPC. É possível modificar isso de forma que limite o tráfego a um conjunto específico de endereços IP.
- Interface de rede de instância de receptor - Uma interface de rede elástica que fornece um endereço IP fixo AWS Ground Station para conexão. Isso é anexado à instância do receptor em `eth1`.

- Anexo da interface da instância do receptor: uma interface de rede elástica anexada à instância do Amazon EC2.
- (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) Verificação EC2 para contatos: a opção de usar o Lambda para configurar um sistema de verificação de suas instâncias do Amazon EC2 para contatos com notificação do SNS. É importante observar que isso pode incorrer em cobranças, dependendo do seu uso atual.
- Grupo de endpoints de fluxo de dados - O grupo de endpoints de AWS Ground Station fluxo de dados que define os endpoints usados para enviar/receber dados de/para seu satélite. Como parte da criação do grupo de endpoints do fluxo de dados, AWS Ground Station cria uma interface de rede elástica em sua conta para transmitir dados.
- Configuração de rastreamento - A configuração de AWS Ground Station rastreamento define como o sistema de antena rastreia seu satélite à medida que ele se move pelo céu.
- Configuração do endpoint da frequência intermediária digitalizada do downlink: um endpoint definido usado para fazer downlink dos dados do satélite.
- 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.

Além disso, o modelo oferece os seguintes recursos para os satélites Aqua, SNPP, JPSS-1/NOAA-20 e Terra:

- Uma configuração de antena de DigIF do downlink para Aqua, SNPP, JPSS-1/NOAA-20 e Terra.
- Um perfil de missão para JPSS-1/NOAA-20 e SNPP, um perfil de missão para Aqua e um perfil de missão para 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 Data Defender para receber o fluxo de AWS Ground Station dados da porta definida pelo endpoint do 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 Grupo. AWS::GroundStation::DataflowEndpoint

Modelo DigiF de banda larga via satélite de transmissão direta (banda larga)

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 instância do Amazon EC2 e os AWS CloudFormation recursos necessários para receber dados brutos de transmissão direta do DigiF. Esse modelo é um ótimo ponto de partida para o processamento de dados usando um rádio definido por software (SDR).

Se o Aqua, SNPP, JPSS-1/NOAA-20 e o Terra não estiverem integrados à conta, consulte Integração de clientes.

> **Important**
>
> A instância do Amazon EC2 precisa ser interrompida antes de aplicar o modelo. Verifique se a instância está parada até estar pronto para usá-la.

Você pode acessar o modelo ao acessar o bucket do S3 de integração de clientes. Observe que os links abaixo usam um bucket regional do S3. `<us-west-2>`Mude para a região na qual você está criando a AWS CloudFormation pilha.

> **Note**
>
> As instruções a seguir usam YAML. No entanto, os modelos estão disponíveis no formato YAML ou JSON. Para usar JSON, substitua `<.yml>` por `<.json>`.

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 o modelo define?

O modelo `DirectBroadcastSatelliteWbDigIfEc2DataDelivery` inclui os seguintes recursos:

- (Opcional) Instância do receptor - A instância do Amazon EC2 que enviará/receberá dados de/para seu satélite usando. AWS Ground Station
  - Grupo de segurança da VPC: o grupo de segurança da Amazon EC2 para a instância de banco de dados.
  - Função da instância: a função da sua instância do Amazon EC2.
  - Perfil de instância: o perfil de instância do Amazon EC2.
  - Grupo com posicionamento em cluster: o posicionamento de grupo em que a instância do Amazon EC2 é executada.
- Chave de entrega de dados - AWS KMS Chave usada para criptografar fluxos de dados.
- Função chave da Ground Station - A função do IAM que AWS Ground Station assumirá o acesso e o uso da AWS KMS chave para descriptografar fluxos de dados
- Política de acesso à chave da Ground Station - A política do IAM que define as ações que AWS Ground Station podem ser tomadas na chave de entrega de dados
- 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) Verificação EC2 para contatos: a opção de usar o Lambda para configurar um sistema de verificação de suas instâncias do Amazon EC2 para contatos com notificação do SNS. É importante observar que isso pode incorrer em cobranças, dependendo do seu uso atual.
- Grupo de endpoints de fluxo de dados - O grupo de endpoints de AWS Ground Station fluxo de dados que define os endpoints usados para enviar/receber dados de/para seu satélite.
- Configuração de rastreamento - A configuração de AWS Ground Station rastreamento define como o sistema de antena rastreia seu satélite à medida que ele se move pelo céu.

Além disso, o modelo oferece os seguintes recursos para os satélites Aqua, SNPP, JPSS-1/NOAA-20 e Terra:

- Uma configuração de downlink para JPSS-1/NOAA-20 e SNPP, uma configuração de downlink para Aqua e uma configuração de downlink para Terra.
- Um perfil de missão para JPSS-1/NOAA-20 e SNPP, um perfil de missão para Aqua e um perfil de missão para 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 Grupo. AWS::GroundStation::DataflowEndpoint Para obter mais informações sobre o AWS Ground Station Agente, consulteAWS Ground Station Guia do usuário do agente.

Criar uma instância do Amazon EC2

> **Note**
>
> Não é necessário nem recomendado criar seus recursos AWS Ground Station (incluindo instâncias do Amazon EC2) manualmente, pois AWS Ground Station fornece AWS CloudFormation modelos predefinidos para isso (consulte Etapa 3: escolha e personalize um AWS CloudFormation modelo para obter mais informações). Se o uso AWS CloudFormation de modelos não funcionar para seu caso de uso, continue lendo.

AWS Ground Station fornece AMIs do Amazon EC2 que vêm pré-carregadas com o software necessário para realizar a entrega de dados em uma instância do Amazon EC2 para entrega de dados em banda estreita ou banda larga. DigIf

> **Important**
>
> Os satélites devem estar integrados ao serviço para acessar as AMIs. AWS Ground Station

Amazon EC2 AMI com DataDefender

Essa AMI vem pré-instalada com o DataDefender software e é usada para contatos de downlink de entrega de dados de banda estreita.

O esquema de nomenclatura para essa AMI é `groundstation-al2-ddx$DDX_VERSION-ami-$DATE_PUBLISHED`. Uma nova AMI DDX é publicada logo após a publicação de uma nova AMI AL2 Amazon EC2. Se AWS Ground Station decidir oferecer suporte a uma nova versão do DataDefender software, uma nova AMI será publicada usando a versão atualizada.

Seleção de uma AWS Ground Station AMI com DataDefender

Você pode acessar a AWS Ground Station AMI por meio da guia AMIs no console do Amazon EC2. Uma vez nessa página, as AMIs podem ser acessadas no filtro Imagens privadas.

Recomendamos classificar as AMIs pela data de publicação e usar a AMI publicada mais recentemente chamada `groundstation-al2-ddx$DDX_VERSION-ami-$DATE_PUBLISHED`.

Amazon EC2 AMI com o agente AWS Ground Station

Essa AMI vem pré-instalada com o AWS Ground Station Agente e é usada para contatos de downlink DigiF de banda larga.

O esquema de nomenclatura dessa AMI é `groundstation-al2-gs-agent-ami-*`, em que * é a data em que a AMI foi criada. Uma nova AMI de AWS Ground Station agente é publicada logo após a publicação de uma nova AMI AL2 do Amazon EC2 ou quando uma nova versão AWS Ground Station do Agent RPM é lançada.

Para obter mais informações sobre o AWS Ground Station Agente, consulteAWS Ground Station Guia do usuário do agente.

Seleção de uma AMI de AWS Ground Station agente

Você pode acessar a AMI do AWS Ground Station agente por meio da guia AMIs no console do Amazon EC2. Uma vez nessa página, as AMIs podem ser acessadas no filtro Imagens públicas.

Recomendamos classificar as AMIs pela data de publicação e usar a AMI publicada mais recentemente chamada `groundstation-al2-gs-agent-ami-$DATE_PUBLISHED`.

Etapa 4: Configurar uma AWS CloudFormation pilha

Depois de escolher o modelo que melhor se aplica ao seu caso de uso, configure uma AWS CloudFormation pilha. Os recursos criados neste procedimento serão configurados para a região em que você estiver ao criá-los. Isso inclui o perfil da missão e suas propriedades que determinam em qual região seus dados serão entregues.

1. Em AWS Management Console, escolha Serviços > CloudFormation.
2. No painel de navegação, escolha Pilhas. Escolha Criar pilha > com novos recursos (padrão).
3. Na página Criar pilha, especifique o modelo selecionado em the section called “Escolher um modelo” executando um dos procedimentos a seguir.

a. Selecione o URL do Amazon S3 como a origem do modelo e copie e cole o URL do modelo que você deseja usar no URL do Amazon S3. Em seguida, escolha Próximo.

b. Selecione Carregar um arquivo de modelo como origem do modelo e escolha Escolher arquivo. Carregue o modelo que você fez download do the section called “Escolher um modelo”. Em seguida, clique em Próximo.

4. Na página de detalhes Especificar pilha, faça as seguintes alterações:

a. Digite um nome na caixa Nome da pilha. Recomendamos usar um nome simples para reduzir a possibilidade de erros no futuro.

b. Para CloudWatchEventActions, escolha quais ações realizar para os gatilhos do CloudWatch evento antes e depois de um contato.

c. Para CreateEC2 VerificationForContacts, escolha se você deseja ou não configurar um sistema de verificação (utilizando Lambda) de suas instâncias do EC2 para contatos com notificação do SNS. É importante observar que isso pode incorrer em cobranças, dependendo do seu uso atual.

d. Para CreateReceiverInstance, escolha se você deseja ou não criar uma instância de receptor do Amazon EC2.

e. Escolha a chave SSH que foi criada em the section called “Etapa 1: criar par de chaves SSH do EC2”.

f. Escolha aquela SubnetIdna qual você deseja criar sua instância do Amazon EC2.

Se estiver usando o AWS Ground Station Agente, é necessária uma sub-rede pública, seja para o posicionamento da instância ou de uma interface de rede elástica. Se você especificar uma sub-rede privada SubnetIdna qual colocar sua instância, também deverá especificar uma sub-rede pública PublicSubnetId(veja abaixo) para usar com o Agente. AWS Ground Station

Para casos de uso que não sejam agentes, recomendamos colocar sua instância do Amazon EC2 em uma sub-rede privada como uma prática recomendada, embora isso não seja obrigatório. É possível usar os Linux Bastion Hosts na Nuvem AWS: implantação de referência de início rápido para automaticamente criar uma sub-rede privada se ainda não tiver configurado a sua conta com uma em the section called “Etapa 2: configurar sua VPC”.

> **Note**
>
> A organização pode ter outra sub-rede dedicada para a instância do Amazon EC2.

g. (Opcional) Escolha a PublicSubnetIdpara usar somente se estiver usando o AWS Ground Station Agente com uma instância em uma sub-rede privada. Isso é necessário se você especificou uma sub-rede privada em SubnetId.

   Essa sub-rede deve estar na sua conta na mesma zona de disponibilidade especificada por SubnetId. Fornecer um PublicSubnetIdresultará na criação de uma interface de rede elástica na sub-rede pública fornecida, anexada à sua instância. Essa interface é usada para acessar a rede do AWS Ground Station Agente a partir da sua instância, que é colocada na sub-rede privada especificada em SubnetId.

h. Escolha a pilha de VPC criada em the section called “Etapa 2: configurar sua VPC”.

i. Escolha Próximo.

5. Configure opções de pilha e opções avançadas para sua instância do Amazon EC2.

   a. Adicione todas as tags e permissões nas seções Tags e Permissões.

   b. Faça qualquer alteração na Política de pilha, Configuração de reversão, Opções de notificação e Opções de criação de pilha.

   c. Escolha Próximo.

6. Depois de revisar os detalhes da pilha, selecione a confirmação de Recursos e escolha Criar pilha.

Etapa 5: instalar e configurar o processador de FE/rádio

A instância do Amazon EC2 definida no AWS CloudFormation modelo não tem um processador Front End (FE) ou rádio definido por software (SDR) instalado por padrão. É necessário instalar um processador FE ou um SDR para processar pacotes VITA-49 transmitidos de/para o sistema de antenas do AWS Ground Station .

Como você instala e configura seu processador FE ou SDR depende de qual processador FE ou SDR está usando. A instalação de um processador FE ou SDR está além do escopo deste guia do usuário.

Para instalar e configurar o processador/rádio FE, entre em contato com o AWS Support.

> **Important**
>
> É uma prática recomendada executar seu processador FE ou SDR nas instâncias criadas pelo AWS CloudFormation modelo para garantir os benefícios dos fluxos de dados DTLS de/para o Data Defender.

Próximos Passos

Sua AWS Ground Station conta e seus recursos agora estão configurados e prontos para uso. Esses recursos estão disponíveis para uso no AWS Ground Station console, onde você pode inserir dados de satélite, identificar localizações de antenas, comunicar-se e programar o horário da antena para satélites selecionados. Você também pode começar a usar ferramentas diferentes para monitorar atividade e configurar alarmes.

Consulte os tópicos a seguir para obter mais informações:

- Listar e reservar contatos
- Monitoramento AWS Ground Station

Usar o serviço de 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 uma instância do Amazon EC2 na sua região da AWS. 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. Ele só está disponível nas seguintes antenna-to-destination regiões ao utilizar a entrega de dados para o Amazon EC2:

- 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, você deve ter um AWS CloudFormation modelo configurado. Para obter mais informações sobre como escolher e personalizar AWS CloudFormation modelos, consulteEtapa 3: escolha e personalize um AWS CloudFormation modelo.

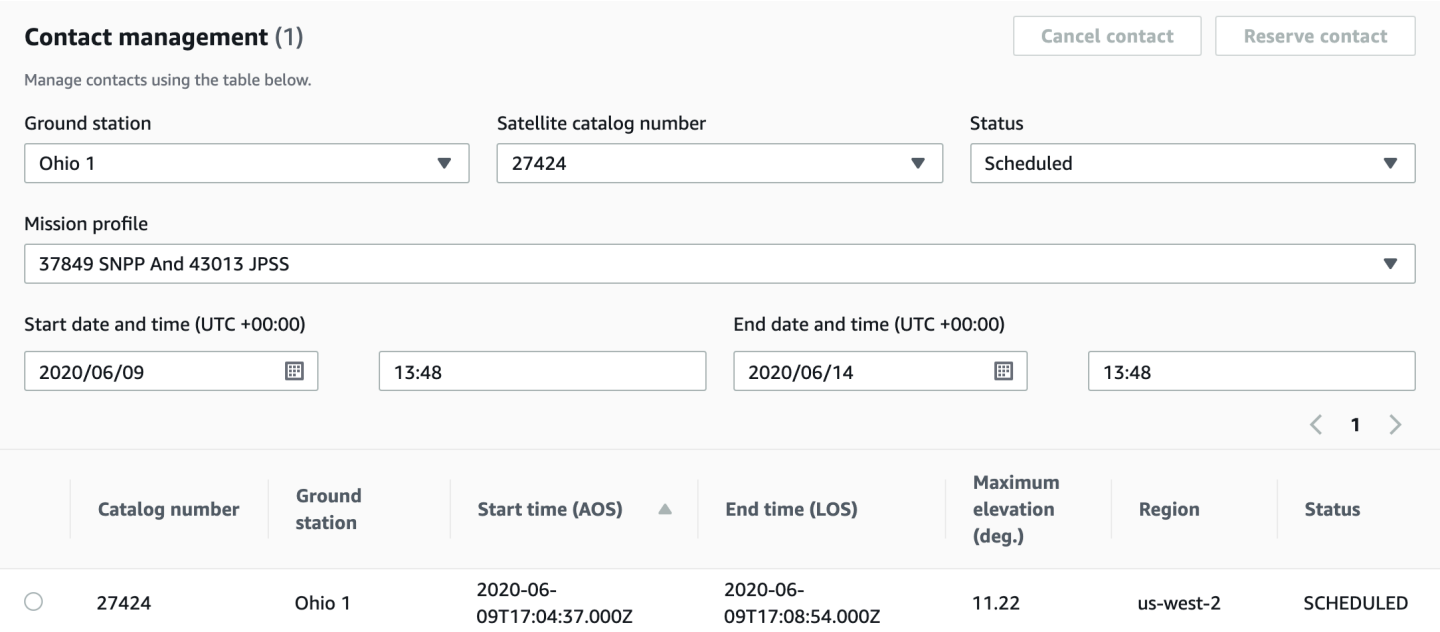
Use os tópicos a seguir para usar a entrega de dados entre regiões no AWS Ground Station.

Tópicos

Como usar a entrega de dados entre regiões no console

Ao reservar um contato no AWS Ground Station console, escolha o perfil da missão que está configurado para entregar os dados de contato à região desejada. Certifique-se de que todos os seus parâmetros estejam corretos e escolha Reservar contato. Se não vir o perfil de missão desejado no console, verifique se você criou o perfil de missão na região em que você está visualizando o console.

Depois de reservar seu contato, você poderá ver os contatos agendados para verificar se agendou a entrega de dados entre regiões visualizando a localização da antena da estação terrestre e a região de destino. A imagem a seguir mostra um contato agendado para a entrega de dados entre regiões. O contato é configurado para usar as antenas da estação terrestre de Ohio e entregar dados para Oregon.



Como usar a entrega de dados entre regiões com a CLI da AWS

Ao reservar um contato AWS CLI, escolha o perfil da missão que está configurado para entregar os dados de contato à região desejada. Especifique o ARN do perfil de missão desejado com `--mission-profile-arn <value>`. Certifique-se de que todos os seus parâmetros estejam corretos e execute o comando. Se você não vir o ARN do perfil de missão desejado ao visualizar e listar contatos, verifique se criou o perfil da missão na região em que está executando a AWS CLI.

Depois de reservar seu contato, você poderá ver os contatos agendados para verificar se agendou a entrega de dados entre regiões visualizando a localização da antena da estação terrestre e a região de destino. A saída a seguir mostra um contato agendado para a entrega de dados entre regiões. O contato é configurado para usar as antenas da estação terrestre de Ohio e entregar os dados para Oregon.


```
{
  "contactList": [
    {
      "contactId": "11111111-2222-3333-4444-555555555555",
      "contactStatus": "SCHEDULED",
      "endTime": "2020-05-05T03:16:35-06:00",
      "groundStation": "Ohio 1",
      "maximumElevation": {
        "unit": "DEGREE_ANGLE",
        "value": 26.74
```

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

Monitoramento 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 CloudWatch Events fornece um fluxo quase em tempo real de eventos do sistema que descrevem mudanças nos AWS recursos. CloudWatch 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 o Amazon CloudWatch Events, consulte o Guia do usuário do Amazon CloudWatch Events.
- O AWS 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. É possível identificar quais usuários e contas chamaram a AWS, o endereço IP de origem 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 o Amazon CloudWatch Metrics.
- 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 de eventos por meio de vários canais, incluindo e-mail, notificações de chat do AWS Chatbot ou notificações por push do AWS Console Mobile Application. Você também pode visualizar notificações na Central de Notificações do Console. O Notificações de Usuários oferece é compatível com agregação, o que pode reduzir o número de notificações que você recebe durante eventos específicos.

Use os seguintes tópicos para monitorar o AWS Ground Station.

Tópicos

Automatização com eventos AWS Ground Station

> **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. Ações que podem ser automaticamente acionadas incluem:

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

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

- Invocar uma função do Lambda para automatizar o início e a interrupção das instâncias do Amazon EC2 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 CloudWatch Events ou o Guia do usuário do Amazon EventBridge Events.

Eventos de exemplo

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

Alteração de estado do contato do Ground Station

Se você quer executar uma ação específica quando um próximo contato está mudando de estado, é possível 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 contactPrePassDurationSecondscontactPostPassDurationSeconds. Os eventos são enviados para a região na qual o contato foi agendado.

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:contact/11111111-1111-1111-1111-111111111111"
    ],
    "detailType": "Ground Station Contact State Change",
    "detail": {
```

```
        "contactId": "11111111-1111-1111-1111-111111111111",
        "groundstationId": "Ground Station 1",
        "missionProfileArn": "arn:aws:groundstation:us-west-2:123456789012:mission-
profile/11111111-1111-1111-1111-111111111111",
        "satelliteArn":
 "arn:aws:groundstation::123456789012:satellite/11111111-1111-1111-1111-111111111111",
        "contactStatus": "PASS"
    },
    "account": "123456789012"
}
```

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

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

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

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`

Registrando 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 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 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:

- 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 um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro AWS serviço.

Para obter mais informações, consulte o elemento CloudTrail UserIdentity.

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

```
}
```

Métricas com a Amazon CloudWatch

Durante um contato, captura e envia dados AWS Ground Station automaticamente CloudWatch para análise. Seus dados podem ser visualizados em um gráfico ou como código-fonte 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.

Métrica	Descrição
`AzimuthAngle`	O ângulo de azimute da antena. O norte verdadeiro é 0 graus e o leste é 90 graus. Unidades: graus
`BitErrorRate`	A taxa de erros irrecuperáveis em bits, em um determinado número de transmissões de bits. Erros de bits são gerados por ruídos, distorções ou interferências Unidades: erros de bits por unidade de tempo
`BlockErrorRate`	A taxa de erros de blocos em um determinado número de blocos recebidos. Erros de blocos são causados por interferência. Unidades: blocos com erros/número total de blocos
`CarrierFrequencyRecovery_Cn0`	Relação entre portadora e densidade de ruído por unidade de largura de banda. Unidades: Decibel-hertz (dB-Hz)

Métrica	Descrição
`CarrierFrequencyRecovery_Locked`	Defina como 1 quando o loop de recuperação da frequência portadora do demodulador estiver bloqueado e 0 quando desbloqueado. Unidades: sem unidades
`CarrierFrequencyRecovery_OffsetFrequency_Hz`	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. Unidades: hertz (Hz)
`ElevationAngle`	O ângulo de elevação da antena. O horizonte é 0 graus e o zênite é 90 graus. Unidades: graus
`Es/N0`	A razão entre a energia por símbolo e a densidade espectral da potência sonora. Unidades: decibéis (dB)
`ReceivedPower`	A intensidade do sinal medida no demodulador/decodificador. Unidades: dBm (decibéis miliwatts)
`SymbolTimingRecovery_ErrorVectorMagnitude`	A magnitude do vetor de erro entre os símbolos recebidos e os pontos ideais da constelação. Unidades: percentual

Métrica	Descrição
`SymbolTimingRecovery_Locked`	Defina como 1 quando o loop de recuperação da frequência portadora do demodulador estiver bloqueado e 0 quando desbloqueado Unidades: sem unidades
`SymbolTimingRecovery_Offset SymbolRate`	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. Unidades: símbolos/segundo

Para quais dimensões são usadas AWS Ground Station?

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

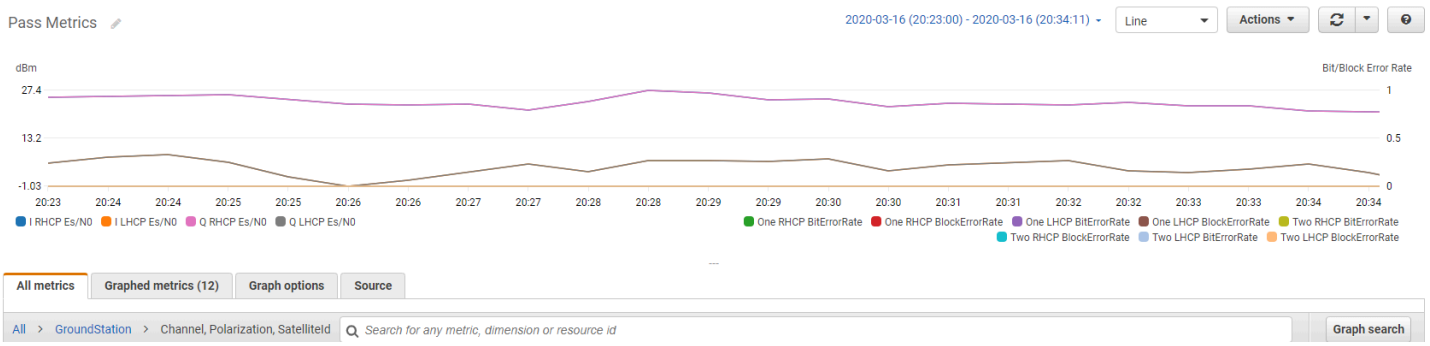
Dimensão	Descrição
`Channel`	Os canais para cada contato incluem Um, Dois, I (em fase) e Q (quadratura).
`Polarization`	A polarização para cada contato inclui PCE (Polarização circular à esquerda) ou PCD (Polarização circular à direita).
`SatelliteId`	O ID do satélite contém o ARN do satélite para seus 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.

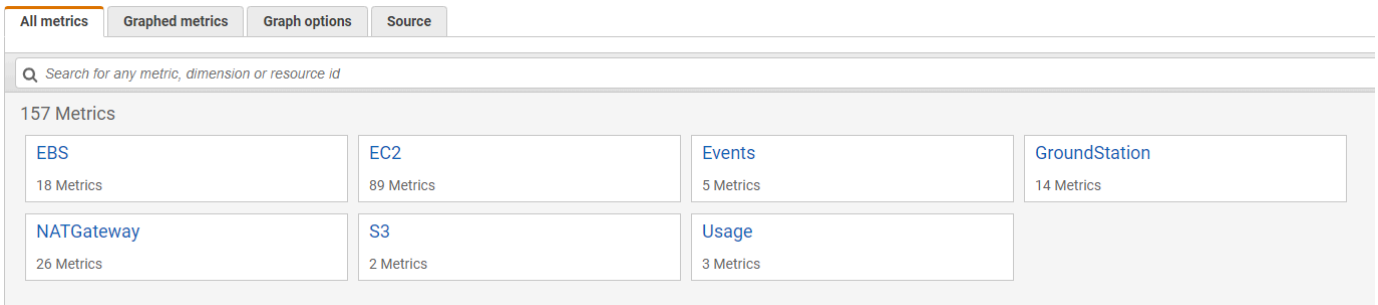
Além disso, os dados capturados dentro dos primeiros 60 segundos não conterão informações suficientes para gerar métricas significativas e provavelmente não serão exibidos. Para visualizar métricas significativas, recomenda-se visualizar os dados após 60 segundos.



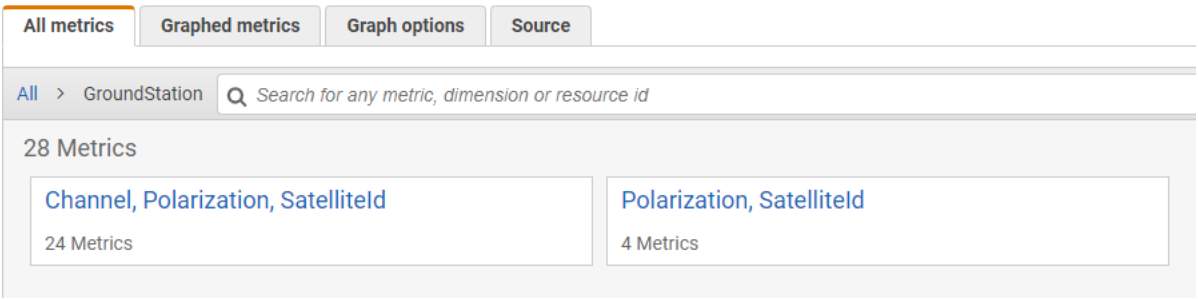
Para obter mais informações sobre a representação gráfica de AWS Ground Station métricas em CloudWatch, consulte Representação gráfica de métricas.

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 criar um gráfico de 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.
2. Crie um arquivo JSON de configuração do CloudWatch agente. Para obter instruções sobre como criar um arquivo de configuração do CloudWatch agente, consulte Criar o arquivo de configuração do CloudWatch agente.
3. Liste as CloudWatch métricas disponíveis executando`aws cloudwatch list-metrics`.
4. Modifique o arquivo JSON criado na etapa 2 para corresponder ao `SatellitID` das métricas.

   > **Note**
   >
   > Não reduza o `Period` campo para um valor abaixo de 60. AWS Ground Station publica métricas a cada 60 segundos e nenhuma métrica será retornada se o valor for reduzido.

5. Execute `aws cloudwatch get-metric-data` com os períodos de tempo de seus passes e do arquivo JSON de configuração do CloudWatch agente. Um exemplo é fornecido abaixo.

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

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

```
{
      “MetricDataResults”: [
          {
              “Id”: “myQuery”,
              “Label”: “Es/N0”,
              “Timestamps”: [
                  “2020-02-18T19:44:00Z”,
                  “2020-02-18T19:43:00Z”,
                  “2020-02-18T19:42:00Z”,
                  “2020-02-18T19:41:00Z”,
                  “2020-02-18T19:40:00Z”,
                  “2020-02-18T19:39:00Z”,
                  “2020-02-18T19:38:00Z”,
                  “2020-02-18T19:37:00Z”,
              ],
              “Values”: [
                  24.58344556958329,
                  24.251638725562216,
                  22.919391450230158,
                  22.83838908204037,
                  23.303086848486842,
                  22.845261784583364,
                  21.34531397048953,
                  19.171561698261222
              ],
              “StatusCode”: “Complete”
          }
      ]
      “Messages”: []
}
```

Solução de problemas

A documentação a seguir pode ajudá-lo a solucionar problemas que podem impedir que um AWS Ground Station contato seja concluído com êxito.

Tópicos

Solução de problemas de contatos que entregam dados para o Amazon EC2

Se você não conseguir concluir um AWS Ground Station contato com sucesso, precisará verificar se sua instância do Amazon EC2 está em execução, verificar se o Data Defender está em execução e verificar se o stream do Data Defender está configurado corretamente.

Pré-requisito

Os procedimentos a seguir presumem que já há uma instância do Amazon EC2 configurada. Para configurar uma instância do Amazon EC2 em AWS Ground Station, consulte Getting Started.

Etapa 1: verificar se a instância do EC2 está em execução

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

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

    b. Escolha a guia Recursos e localize a instância do Amazon EC2 na coluna ID lógico. Verifique se a instância foi criada na coluna Status.

    c. Na coluna ID físico, selecione o link para a instância do Amazon EC2. Isso levará você ao console de gerenciamento do Amazon EC2.

2. No console de gerenciamento do Amazon EC2, certifique-se de que seu estado de instância do Amazon EC2 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 a instância do Amazon EC2 selecionada, escolha Ações > Estado da instância > Iniciar.

Etapa 2: determinar o tipo de aplicação de fluxo de dados usada

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 a aplicação Data Defender (DDX), continue com the section called “Etapa 3: verificar se o Data Defender está em execução”.

Etapa 3: verificar se o Data Defender está em execução

A verificação do status do Data Defender requer que você se conecte à instância no Amazon EC2. Para obter mais detalhes sobre como se conectar à instância, consulte Conectar-se à instância do 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 a instância do Amazon EC2 usando o SSH. Encaminhe a porta 80 do host remoto para visualizar a interface do usuário da web do Data Defender. Os comandos a seguir demonstram como usar o SSH para conectar a uma instância do Amazon EC2 por meio de um bastion com encaminhamento de porta habilitado.

   > **Note**
   >
   > Substitua <SSH KEY>, <BASTION HOST> e <HOST> pela chave ssh específica, nome do bastion host e nome do host da instância do Amazon EC2.

   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 o Data Defender (também chamado de DDX) está em execução por meio de grepping (verificação) de 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 o Data Defender estiver em execução, vá para the section called “Etapa 4: verificar se o fluxo do Data Defender está configurado”. Caso contrário, siga para o próximo passo.

3. Inicie o Data Defender usando o comando abaixo.

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

   Se o Data Defender estiver em execução após usar o comando, vá para the section called “Etapa 4: verificar se o fluxo do Data Defender está configurado”. Caso contrário, siga para o próximo passo.

4. Inspecione os seguintes arquivos usando os comandos abaixo para verificar se há erros ao instalar e configurar o Data Defender.

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

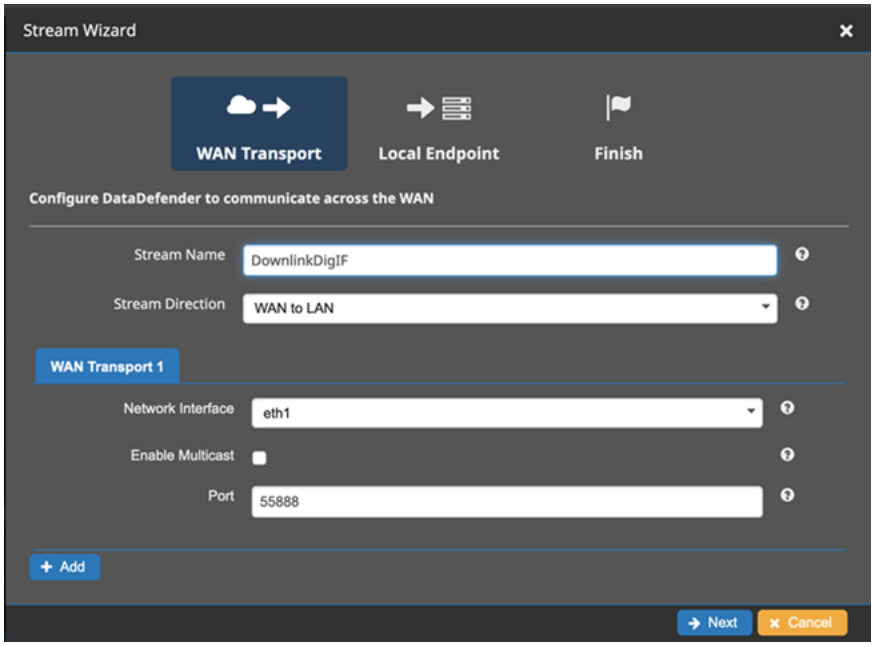
> **Note**
>
> Um problema comum descoberto ao inspecionar esses arquivos é que a instância do Amazon EC2 está executando não tem acesso ao Amazon S3 para fazer download dos arquivos de instalação. Caso descubra em seus registros que o problema é esse,

verifique as configurações da Amazon VPC e do grupo de segurança da instância do EC2 para garantir que não estejam bloqueando o acesso ao Amazon S3.

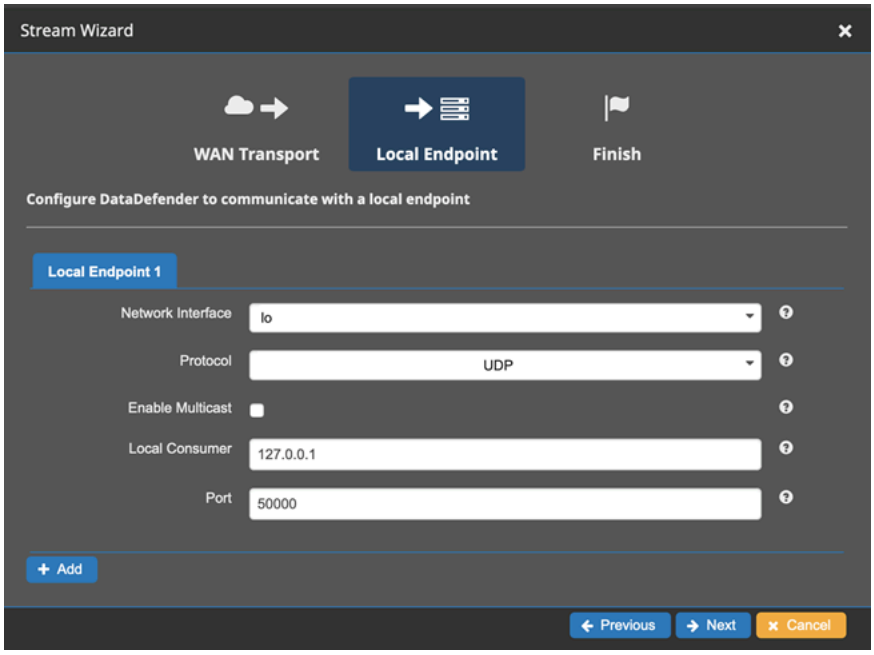
Se o Data Defender estiver em execução após verificar as configurações da Amazon VPC, vá para the section called “Etapa 4: verificar se o fluxo do Data Defender está configurado”. Se o problema persistir, entre em contato com o AWS Support e envie os arquivos de log com uma descrição do problema.

Etapa 4: verificar se o fluxo do Data Defender está configurado

1. Em um navegador da web, acesse a interface de usuário da web do DDX inserindo o seguinte endereço na barra de endereços: 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 que o Data Defender os receber do AWS Ground Station serviço. Em seguida, clique em 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 instância do Amazon EC2 e o Data Defender estejam funcionando e configurados adequadamente para receber dados do. AWS Ground Station Se continuar tendo problemas, entre em contato com o AWS Support.

Status de contato da Ground Station

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.
- COMPLETED: o contato foi concluído com sucesso.
- FAILED: o contato falhou devido a um problema com a configuração dos recursos do cliente.
- AWS_FAILED - O contato falhou devido a um problema no serviço. AWS Ground Station
- CANCELLING: o contato está em processo de cancelamento.
- AWS_CANCELLED - O contato foi cancelado pelo serviço. AWS Ground Station A manutenção da antena ou do local é um exemplo de quando isso pode acontecer.
- CANCELLED: o contato foi cancelado pelo cliente.

Guias de solução de

- the section called “Solução de problemas de contatos com o status FAILED”
- the section called “Solução de problemas de contatos FAILED_TO_SCHEDULE”

Solução de problemas de contatos com o status FAILED

Um contato terá um status de contato do terminal de FALHA quando AWS Ground Station for detectado um problema com a configuração dos recursos do cliente. 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 específico para o status de contato FAILED e não se destina a outros status de falha, como AWS_FAILED, AWS_CANCELLED ou FAILED_TO_SCHEDULE. Consulte mais informações sobre os status de contato em the section called “Status de contato da Ground Station”

Casos de uso do Data Defender (DDX) com o status FAILED

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 DDX:

- O DDX do cliente nunca se conecta - A conexão DDX entre a AWS Ground Station antena e o grupo de endpoints do fluxo de dados do cliente para um ou mais fluxos de dados nunca foi estabelecida.
- O DDX do cliente se conecta tardiamente - A conexão DDX entre a AWS Ground Station antena e o grupo de endpoints do Dataflow do cliente para um ou mais fluxos de dados foi estabelecida após o horário de início do contato.

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

- Confirme se a instância do Amazon EC2 do receptor foi iniciada com sucesso, antes da hora de início do contato.
- Confirme se o DDX estava funcionando durante o contato.

Consulte etapas de solução de problemas mais específicas na seção sobre the section called “Solução de problemas de contatos que entregam dados para o 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:

- Status nunca relatado pelo agente do cliente - O agente responsável por orquestrar a entrega de dados no grupo de endpoints do Customer Dataflow para um ou mais fluxos de dados nunca reportou o status com sucesso. AWS Ground Station Essa atualização de status deve ocorrer alguns segundos após a hora de término do contato.
- Agente do cliente inicia com atraso: o agente responsável por orquestrar a entrega de dados no grupo de endpoints do fluxo de dados do cliente para um ou mais fluxos de dados foi iniciado com atraso, após a hora 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 instância do Amazon EC2 do receptor foi iniciada com sucesso, antes da hora de início do contato.
- Confirme se a aplicação do agente estava funcionando no início e durante o contato.
- Confirme se a aplicação do agente e a instância do Amazon EC2 não foram encerradas em até 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 the section called “Solução de problemas de contatos que entregam dados para o Amazon EC2”.

Solução de problemas de contatos FAILED_TO_SCHEDULE

Um contato falhará no cronograma quando AWS Ground Station for detectado um problema na configuração dos recursos do cliente ou no sistema interno. Um contato que termina em um estado FAILED_TO_SCHEDULE, opcionalmente, fornecerá um contexto adicional. `errorMessage` Para obter informações sobre a descrição de contatos, consultethe section called “Descreva um contato com AWS CLI”.

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 AWS_FAILED, AWS_CANCELLED ou FAILED. Consulte mais informações sobre os status de contato em the section called “Status de contato da Ground Station”

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 que funcionava anteriormente 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. Consulte the section called “Reserve um contato com AWS CLI”.
- Se você continuar recebendo o status FAILED_TO_SCHEDULE para esse perfil de missão, entre em contato com o AWS Support

Segurança em AWS Ground Station

A segurança para com a nuvem na AWS é a nossa maior prioridade. Como um cliente da AWS, você se beneficiará de um datacenter e uma arquitetura de rede criados para atender os requisitos da maioria das organizações com exigências de 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 o AWS Ground Station, recomendamos seguir as melhores práticas do setor e implementar a criptografia de ponta a ponta. A AWS oferece APIs para você integrar criptografia e proteção de dados. Para obter mais informações sobre a segurança da AWS, consulte o whitepaper Introdução à segurança da AWS.

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

Tópicos

Gerenciamento de identidade e acesso para AWS Ground Station

O AWS Identity and Access Management (IAM) é um serviço da AWS service (Serviço da AWS) que ajuda a controlar o acesso aos recursos da AWS de forma segura. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (ter permissões) a usar os recursos do AWS Ground Station. O IAM é um AWS service (Serviço da AWS) que pode ser usado sem custo adicional.

Tópicos

- Exemplos de políticas baseadas em identidade para o AWS Ground Station
- Solução de problemas de identidade e acesso do AWS Ground Station

Público

O uso do AWS Identity and Access Management (IAM) varia dependendo do trabalho que for realizado no AWS Ground Station.

Usuário do serviço – Se você usar o serviço AWS Ground Station para fazer o trabalho, o administrador fornecerá as credenciais e as permissões necessárias. À medida que usar mais recursos do AWS Ground Station para fazer seu trabalho, você poderá precisar 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 recurso no AWS Ground Station, consulte Solução de problemas de identidade e acesso do AWS Ground Station.

Administrador do serviço – Se você for o responsável pelos recursos do AWS Ground Station na empresa, provavelmente terá acesso total ao AWS Ground Station. Cabe a você determinar quais funcionalidades e recursos do AWS Ground Station os usuários do serviço devem acessar. Assim, você deve enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Analise as informações nesta página para entender os conceitos básicos do IAM. Para saber mais sobre como a empresa pode usar o IAM com o AWS Ground Station, consulte Como o 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 o acesso ao AWS Ground Station. Para visualizar exemplos AWS Ground Station de políticas baseadas em identidade do que podem ser usadas no IAM, consulte Exemplos de políticas baseadas em identidade para o AWS Ground Station.

Como autenticar com identidades

A autenticação é a forma como você faz login na AWS usando suas credenciais de identidade. É necessário ser autenticado (fazer login na AWS) como o usuário raiz da Usuário raiz da conta da AWS, como usuário do IAM ou assumindo um perfil do IAM.

Você pode fazer login na AWS como uma identidade federada usando credenciais fornecidas por uma fonte de identidades. Os usuários do AWS IAM Identity Center (IAM Identity Center), a autenticação única da empresa e as suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como uma identidade federada, o administrador já

configurou anteriormente a federação de identidades utilizando perfis do IAM. Quando você acessa a AWS usando a federação, está indiretamente assumindo um perfil.

É possível fazer login no ou no portal de acesso da AWS Management Console dependendo do tipo de usuário que você é.AWS Para obter mais informações sobre como fazer login na AWS, consulte How to sign in to your Conta da AWS (Como fazer login na conta da) no Início de Sessão da AWS User Guide (Guia do usuário do).

Se você acessar a AWS programaticamente, a AWS fornecerá um kit de desenvolvimento de software (SDK) e uma interface da linha de comando (CLI) para você assinar criptograficamente as solicitações usando as suas credenciais. Se você não utilizar as ferramentas da AWS, deverá assinar as solicitações por conta própria. Para obter mais informações sobre como usar o método recomendado para assinar solicitações por conta própria, consulteAssinar AWSsolicitações de API da noGuia do usuário do IAM.

Independentemente do método de autenticação usado, também pode ser exigido que você forneça mais informações de segurança. Por exemplo, a AWS recomenda o uso da autenticação multifator (MFA) para aumentar a segurança de sua conta. Para saber mais, consulte Autenticação multifator no Guia do usuário do AWS IAM Identity Center e Usar a autenticação multifator (MFA) naAWS no Guia do usuário do IAM.

Usuário raiz da Conta da AWS

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos os atributos e Serviços da AWS na conta. Essa identidade, denominada usuário raiz da Conta da AWS, e é acessada por login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não utilizar 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 os usuários, inclusive os que precisam de acesso de administrador, usem a federação com um provedor de identidades para acessar Serviços da AWS usando credenciais temporárias.

Identidade federada é um usuário de seu diretório de usuários corporativos, um provedor de identidades da web AWS Directory Service, o , o diretório do Centro de Identidade ou qualquer usuário que acesse os Serviços da AWS usando credenciais fornecidas por meio de uma fonte de

identidade. Quando as identidades federadas acessam Contas da AWS, elas assumem perfis que fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos usar o .AWS IAM Identity Center Você pode criar usuários e grupos no Centro de Identidade do IAM ou se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todas as suas Contas da AWS e aplicações. 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 Conta da AWS que tem permissões específicas para uma única pessoa ou aplicação. Sempre que possível, recomendamos 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 utilização específicos que exijam credenciais de longo prazo com usuários do IAM, recomendamos alternar as chaves de acesso. Para obter mais informações, consulte Alterne 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 utilizar 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 IAMAdmins e atribuir a esse grupo permissões para administrar atributos 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 Quando criar um usuário do IAM (em vez de uma função) no Guia do usuário do IAM.

Perfis do IAM

Um perfil do IAM é uma identidade dentro da Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. É possível assumir temporariamente um perfil do IAM no AWS Management Console alternando perfis. É possível assumir um perfil chamando uma operação de API da AWS CLI ou da AWS, ou usando um URL personalizado. Para obter mais informações sobre métodos para o uso de perfis, consulte Uso de funções do IAM 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, você pode 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 pelo mesmo. Para obter mais informações sobre perfis para federação, consulte Criar uma função para um provedor de identidade de terceiros no Guia do usuário do IAM. Se você usar o IAM Identity Center, deverá configurar 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 assumir 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, alguns Serviços da AWS permitem que você anexe uma política diretamente a um atributo (em vez de usar um perfil como proxy). Para saber a diferença entre perfis e políticas baseadas em atributo para acesso entre contas, consulte Como os perfis do IAM diferem das políticas baseadas em atributo no Guia do usuário do IAM.
- Acesso entre serviços: alguns Serviços da AWS usam atributos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicações no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de chamada, usando um perfil de serviço ou um perfil vinculado ao serviço.
  - Encaminhamento de sessões de acesso (FAS): qualquer pessoa que utilizar uma função ou usuário do IAM para realizar ações na AWS é considerada uma entidade principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O recurso FAS utiliza as permissões da entidade principal que chama um AWS service (Serviço da AWS), combinadas às permissões do AWS service (Serviço da AWS) solicitante, para realizar solicitações para serviços downstream. As solicitações de FAS só são feitas quando um serviço recebe uma solicitação que exige interações com outros Serviços da AWS ou com recursos para serem concluídas. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.
  - Perfil de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para realizar 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 a serviço é um tipo de função de serviço vinculada a um AWS service (Serviço da AWS). O serviço pode assumir o perfil para executar uma ação em seu nome. Os perfis vinculados ao serviço aparecem em sua Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode exibir, mas não pode editar as permissões para perfis vinculados ao serviço.

- Aplicações em execução no Amazon EC2: é possível usar um perfil do IAM para gerenciar credenciais temporárias para aplicações em execução em uma instância do EC2 e fazer solicitações da AWS CLI ou da AWS API. É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir um perfil da AWS a uma instância do EC2 e disponibilizá-la para todas as suas aplicações, crie um perfil de instância que esteja anexado a ela. Um perfil de instância contém a perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Usar um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Para saber se deseja usar os perfis do IAM, consulte Quando criar um perfil do IAM (em vez de um usuário) no Guia do usuário do IAM.

Como gerenciar acesso usando políticas

Você controla o acesso na AWS criando políticas e anexando-as a identidades ou atributos da AWS. Uma política é um objeto na AWS que, quando associado a uma identidade ou atributo, define suas permissões. A AWS avalia essas políticas quando uma entidade principal (usuário, usuário raiz ou sessão de perfil) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas são armazenadas na 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 AWS as políticas JSON da para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

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

As políticas do IAM definem permissões para uma ação independente 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 perfil do AWS Management Console, da AWS CLI 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 Criar políticas do IAM no Guia do usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda mais como políticas embutidas ou políticas gerenciadas. As políticas embutidas são anexadas diretamente a um único usuário, grupo ou função. As políticas gerenciadas são políticas independentes que podem ser anexadas a vários usuários, grupos e perfis na Conta da AWS. As políticas gerenciadas incluem políticas gerenciadas pela AWS 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 recurso

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

Políticas baseadas em atributos são políticas em linha que estão localizadas nesse serviço. Não é possível usar as políticas gerenciadas da AWS do IAM em uma política baseada em atributos.

Listas de controle de acesso (ACLs)

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

Amazon S3, AWS WAF e Amazon VPC são exemplos de serviços compatíveis com ACLs. Para saber mais sobre ACLs, consulte Visão geral da lista de controle de acesso (ACL) no Guia do desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

A AWS aceita tipos de política 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 atributo 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 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 (UO) no AWS Organizations. O AWS Organizations é um serviço para agrupar e gerenciar centralmente várias Contas da AWS pertencentes à sua empresa. Se você habilitar todos os atributos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. O SCP limita as permissões para entidades em contas-membro, incluindo cada .Usuário raiz da conta da AWS Para obter mais informações sobre o Organizações e SCPs, consulte How SCPs work (Como os SCPs funcionam) noAWS Organizations Guia do usuário do .
- 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 atributo. 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 a AWS determina se deve permitir uma solicitação quando há vários tipos de política envolvidos, consulte Lógica da avaliaçãode políticas no Guia do usuário do IAM.

Como o AWS Ground Station funciona com o IAM

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

Recursos do IAM que você pode usar com o AWS Ground Station

atributo do IAM	Suporte a AWS Ground Station
Políticas baseadas em identidade	Sim
Políticas baseadas em recurso	Não
Ações de políticas	Sim
atributos 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
Funções vinculadas ao serviço	Sim

Para obter uma visualização de alto nível de como o AWS Ground Station e outros serviços da AWS funcionam com a maioria dos atributos do IAM, consulte AWSServiços Compatíveis com o IAM no Guia do Usuário do IAM.

Políticas baseadas em identidade para o AWS Ground Station

Suporta 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 Criar políticas do IAM no Guia do usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou atributos permitidos ou negados, bem 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 função à qual ela está anexada. Saiba mais sobre todos os elementos que podem ser usados em uma política JSON consultando Referência de Elementos de Política JSON do IAM no Guia do Usuário do IAM.

Exemplos de políticas baseadas em identidade para o AWS Ground Station

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

Políticas baseadas em recursos no AWS Ground Station

Oferece suporte a políticas baseadas em recurso	Não

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

Para o recurso ao qual a política está anexada, a política define quais ações uma entidade principal especificado pode executar nesse recurso e em que condições. Você precisa especificar uma entidade principal em uma política baseada em recurso. As entidades principais podem incluir contas, usuários, perfis, 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 atributo. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando a entidade principal e o atributo estão em diferentes Contas da AWS, um administrador do IAM da conta confiável também deve conceder à entidade principal (usuário ou perfil) permissão para acessar o atributo. 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 outra política baseada em identidade será necessária. Para obter mais informações, consulte Como as funções do IAM diferem de políticas baseadas em recursos no Guia do usuário do IAM.

Ações de políticas para o AWS Ground Station

Oferece suporte a ações de políticas	Sim

Os administradores podem usar as políticas de JSON da AWS para especificar quem tem acesso a 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 você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome que a operação de API da AWS 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 obter uma lista das ações do AWS Ground Station, consulte Ações definidas pelo AWS Ground Station na Referência de autorização do serviço.

As ações de políticas no AWS Ground Station usam o seguinte prefixo antes da ação:

```
groundstation
```

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

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

Veja exemplos de políticas baseadas em identidade AWS Ground Station consultando Exemplos de políticas baseadas em identidade para o AWS Ground Station.

Recursos de políticas para AWS Ground Station

Oferece suporte a atributos de políticas	Sim

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

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

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

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

Para ver uma lista de tipos de recursos AWS Ground Station 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 recurso, consulte Ações definidas peloAWS Ground Station.

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

Chaves de condição de políticas para AWS Ground Station

Suporta chaves de condição de política específicas de serviço	Sim

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

O elemento `Condition` (ou `Condition` bloco de) permite que você especifique condições nas quais uma instrução está em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usam 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 `Condition` em uma instrução ou várias chaves em um único `Condition` elemento, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, a AWS avaliará a condição usando uma operação lógica `OR`. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

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

A AWS oferece suporte a chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição globais da AWS, consulte AWSChaves de Contexto de Condição Globais da no Guia do Usuário do IAM.

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

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

ACLs no AWS Ground Station

Oferece suporte a ACLs	Não

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

ABAC com AWS Ground Station

Oferece suporte a ABAC (tags em políticas)	Sim

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Na AWS, esses atributos são chamados de tags. É possível anexar tags a entidades do IAM (usuários ou perfis) e a muitos atributos da AWS. A marcação 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 atributo que ela está tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações onde 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 `aws:TagKeys` chaves de condição.

Se um serviço oferecer suporte às três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de recursos, o valor será Parcial.

Para obter mais informações sobre o ABAC, consulte O que é 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) (Use attribute-based access control [ABAC]) no Guia do usuário do IAM.

Usar credenciais temporárias com o AWS Ground Station

Oferece suporte a 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 que funcionam com o IAM no Guia do usuário do IAM.

Você está usando credenciais temporárias se faz login no AWS Management Console usando qualquer método, exceto um nome de usuário e uma senha. Por exemplo, quando você acessa a AWS usando o link de autenticação única (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 perfis, consulte Alternar para um perfil (console) no Guia do usuário do IAM.

Você pode criar credenciais temporárias manualmente usando a AWS CLI ou a API da AWS. Em seguida, você pode usar essas credenciais temporárias para acessar aAWS .AWS A 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 de entidade principal entre serviços para o AWS Ground Station

Suporte para o recurso Encaminhamento de sessões de acesso (FAS)	Sim

Quando você usa um usuário ou perfil do IAM para executar ações na AWS, você é considerado uma entidade principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O recurso FAS utiliza as permissões da entidade principal que chama um AWS service (Serviço da AWS), combinadas às permissões do AWS service (Serviço da AWS) solicitante, para realizar solicitações para serviços downstream. As solicitações de FAS só são feitas quando um serviço recebe uma solicitação que exige interações com outros Serviços da AWS ou com recursos para serem concluídas. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhamento de sessões de acesso.

Funções de serviço para AWS Ground Station

Oferece suporte a perfis de serviço	Não

O perfil de serviço é um perfil do IAM que um serviço assume para realizar 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 um perfil de serviço pode prejudicar a funcionalidade AWS Ground Station. Edite funções de serviço somente quando AWS Ground Station fornecer orientação para fazê-lo.

Funções vinculadas ao serviço para o AWS Ground Station

Oferece suporte a perfis vinculados ao serviço	Sim

Um perfil vinculado ao serviço é um tipo de perfil de serviço vinculado a um AWS service (Serviço da AWS). O serviço pode presumir a função de executar uma ação em seu nome. Os perfis vinculados ao serviço aparecem em sua Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para perfis vinculados ao serviço.

Para obter detalhes sobre como criar ou gerenciar funções vinculadas a serviços, consulte Serviços do 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 esse serviço .

Exemplos de políticas baseadas em identidade para o AWS Ground Station

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos do AWS Ground Station. Eles também não podem executar tarefas usando o AWS Management Console, a AWS Command Line Interface (AWS CLI) ou a API AWS. Para conceder aos usuários permissão para executar ações nos recursos de que 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.

Saiba como criar uma política baseada em identidade do IAM usando esses exemplos de documento da política JSON consultando Criando Políticas do IAM no Guia do Usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos por AWS Ground Station, incluindo o formato dos ARNs para cada tipo de recurso, consulte Ações, recursos e chaves de condição para AWS Ground Station na Referência de autorização de serviço.

Tópicos

- Melhores práticas de políticas
- Usar o console do AWS Ground Station
- Permitir que usuários visualizem suas próprias permissões

Melhores práticas de políticas

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

- Comece com AWS as políticas gerenciadas pela e avance para as permissões de privilégio mínimo: para começar a conceder permissões a seus usuários e workloads, use as AWS políticas gerenciadas pela que concedem permissões para muitos casos de uso comuns. Elas estão disponíveis na sua Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente da AWS específicas para seus casos de uso. Para obter mais informações, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para perfis 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 atributos 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 atributos. 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 a ações de serviço, se elas forem

usadas por meio de um AWS service (Serviço da AWS) específico, como o AWS CloudFormation. Para obter mais informações, consulte Elementos de política JSON do IAM: Condition 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 100 verificações de política e recomendações acionáveis para ajudá-lo 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 houver um cenário que exija usuários do IAM ou um usuário raiz em sua Conta da AWS, ative 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 console do AWS Ground Station, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os recursos AWS Ground Station no 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 funções) com essa política.

Não é necessário conceder permissões mínimas do console para usuários que fazem chamadas somente à AWS CLI ou à AWS API. Em vez disso, permita o acesso somente a ações que correspondam a operação de API que estiverem tentando executar.

Para garantir que os usuários e funções ainda possam usar o console AWS Ground Station, anexe também a política AWS Ground Station `ConsoleAccess` ou `ReadOnly` AWS gerenciada às entidades. Para obter mais informações, consulte Adicionando Permissões a um Usuário no Guia do Usuário do IAM.

Permitir que usuários visualizem suas próprias permissões

Este exemplo mostra como é possível criar uma política que permite 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 de forma programática usando a AWS CLI ou a AWS API.

```
{
    "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 de identidade e acesso do AWS Ground Station

Use as seguintes informações para ajudar a diagnosticar e corrigir problemas comuns que podem ser encontrados ao trabalhar com o e o IAM.AWS Ground Station

Tópicos

Não tenho autorização para executar uma ação no 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 atributo *`my-example-widget`* usando a ação `groundstation:`*`GetWidget`*.

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

Não estou autorizado a executar 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 o serviço, em vez de criar uma nova função de serviço ou 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 você precisar de ajuda, entre em contato com seu administrador AWS. Seu administrador é a pessoa que forneceu suas credenciais de login.

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

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

Saiba mais consultando o seguinte:

- Para saber se o AWS Ground Station suporta esses recursos, consulte Como o AWS Ground Station funciona com o IAM.
- Saiba como conceder acesso a seus recursos em todos os Contas da AWS pertencentes a você, consulte Fornecendo Acesso a um Usuário do IAM em Outro Conta da AWS Pertencente a Você no Guia de Usuário do IAM.
- Para saber como conceder acesso a seus recursos para Contas da AWS terceirizadas, consulte Fornecimento de acesso a Contas da AWS pertencentes 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 saber a diferença entre usar perfis e políticas baseadas em atributos para acesso entre contas, consulte Como os perfis do IAM diferem de políticas baseadas em atributos no Guia do usuário do IAM.

Usar funções vinculadas ao serviço para o Ground Station

O AWS Ground Station usa funções vinculadas ao serviço do 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 a produtos são predefinidas pelo Ground Station e incluem todas as permissões que o produto requer para chamar outros produtos da AWS 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 compatíveis com funções vinculadas aos serviços, consulte serviços da AWS que funcionam com o IAM e procure os serviços que apresentam Sim na coluna Funções vinculadas aos serviços. 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

O Ground Station usa a função vinculada ao serviço chamada AWSServiceRoleForGroundStationDataflowEndpointGroup: o AWS GroundStation usa essa função vinculada ao serviço para invocar o EC2 para encontrar endereços IPv4 públicos.

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

- `groundstation.amazonaws.com`

A política de permissões de perfil vinculado ao serviço AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy permite que o 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 aos EIPs.

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

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

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua uma função vinculada ao 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 uma função vinculada ao serviço. Ao criar um DataflowEndpointGroup na AWS CLI ou na API da AWS, o Ground Station cria a função vinculada ao serviço para você.

Se excluir essa função vinculada ao serviço e precisar criá-la novamente, você poderá usar esse mesmo processo para recriar a função em sua conta. Ao criar um DataflowEndpointGroup, o Ground Station cria a função vinculada ao serviço para você.

Você também pode usar o console do IAM para criar uma função vinculada ao serviço com o caso de uso de Entrega de Dados para o Amazon EC2. Na AWS CLI ou na API do AWS, crie uma função vinculada ao serviço com o nome de serviço `groundstation.amazonaws.com`. 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 editar a função vinculada ao serviço vinculado AWSServiceRoleForGroundStationDataflowEndpointGroup. Depois que criar uma função vinculada ao serviço, você não poderá alterar o nome da função, pois várias entidades podem fazer referência a ela. Será possível editar a descrição da função 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 recurso 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 poderá excluir uma função vinculada ao serviço somente depois de excluir os DataflowEndpointGroups usando a função vinculada ao serviço. Isso evita que você revogue acidentalmente as permissões do DataflowEndpointGroups. Se uma função vinculada ao serviço é usada com vários grupos do DataflowEndpointGroups, você deve excluir todos os grupos do 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 do Ground Station usados por AWSServiceRoleForGroundStationDataflowEndpointGroup

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

Como excluir manualmente a função vinculada ao serviço usando o IAM

Use o console do IAM, a AWS CLI ou a API da AWS para excluir a função vinculada a serviço AWSServiceRoleForGroundStationDataflowEndpointGroup. Para obter mais informações, consulte Excluir uma função vinculada 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 da AWS.

Solução de problemas

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

Políticas gerenciadas pela AWS para o AWS Ground Station

Uma política gerenciada pela AWS é uma política independente criada e administrada pela AWS. As políticas gerenciadas pela AWS são criadas para fornecer permissões a vários casos de uso comuns a fim de que você possa começar a atribuir permissões a usuários, grupos e perfis.

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

Você não pode alterar as permissões definidas em políticas gerenciadas pela AWS. Se a AWS atualiza as permissões definidas em uma política gerenciada pela AWS, a atualização afeta todas as identidades de entidades principais (usuários, grupos e perfis) às quais a política está vinculada. É mais provável que a AWS atualize uma política gerenciada pela AWS quando um novo AWS service (Serviço da AWS) é lançado ou novas operações de API são disponibilizadas para os serviços existentes.

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

AWS adicionou uma nova política chamada AWSGroundStationAgentInstancePolicy

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

Essa política concede permissões do atendente AWS Ground Station a uma instância do cliente que permite que a instância envie e receba dados durante os contatos do Ground Station. Todas as permissões nesta política são do serviço Ground Station.

Detalhes da permissão

Esta política inclui as seguintes permissões.

- `groundstation`: permite que instâncias de endpoint de fluxo de dados chamem as APIs do atendente Ground Station.

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

AWS política gerenciada: AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy

Não é possível anexar a política AWSDMSFleetAdvisorServiceRolePolicy às entidades do IAM. Essa política é anexada a uma função vinculada ao serviço que permite que o AWS Ground Station realize ações em seu nome. Para mais informações, consulte Como usar funções vinculadas a serviços.

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

Detalhes da permissão

Esta política inclui as seguintes permissões.

- `ec2:DescribeAddresses`: permite AWS Ground Station listar todos os IPs associados aos EIPs em seu nome.

- `ec2:DescribeNetworkInterfaces`: permite AWS Ground Station obter informações sobre as interfaces de rede associadas às instâncias do EC2 em seu nome.

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

Atualizações do AWS Ground Station para políticas gerenciadas pela AWS

Visualizar detalhes sobre atualizações em políticas gerenciadas pela AWS para o AWS Ground Station desde que esse serviço começou a rastrear essas alterações. Para receber alertas automáticos sobre alterações feitas nesta página, inscreva-se no feed RSS na página de histórico de documentos do AWS Ground Station.

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 atendente AWS Ground Station.	12 de abril de 2023

Alteração	Descrição	Data
AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy: nova política	AWS Ground Station adicionou uma nova política que concede permissões do EC2 para permitir que o AWS Ground Station encontre endereços IPv4 públicos associados a EIPs e interfaces de rede associadas a instâncias do EC2.	2 de novembro de 2022
O AWS Ground Station iniciou o rastreamento das alterações	O AWS Ground Station começou a monitorar as alterações de políticas gerenciadas da AWS.	1 de março de 2021

Criptografia de dados em repouso para AWS Ground Station

AWS Ground Station fornece criptografia por padrão para proteger dados confidenciais do cliente 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 políticas do IAM
  - Habilitar e desabilitar políticas de chaves
  - Alternar os materiais de criptografia de chaves
  - Adicionar etiquetas
  - Criar aliases 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	Habilitado	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 em uma conta de cliente.

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

- Envie `GenerateDataKey` solicitações ao AWS KMS para gerar chaves de dados criptografadas pela chave gerenciada pelo cliente.

- Envie `Decrypt` solicitações ao AWS KMS para descriptografar as chaves de dados criptografadas para que elas possam ser usadas para criptografar seus dados.
- Envie `Encrypt` solicitações 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.

Crie uma chave gerenciada pelo cliente

Você pode criar uma chave simétrica gerenciada pelo cliente usando o AWS Management Console ou as APIs do AWS 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 seu 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, você pode especificar uma política de chaves. 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.
- Ligue `Decrypt` para usar a chave de dados criptografada armazenada para acessar os dados criptografados.
- Chamar para `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 contêm 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"
}
```

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.

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 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.

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. 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 (da 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 fazer o upload de 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: Perguntas frequentes sobre o Ground Station.

Obter 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. `GetSatellite` `ListSatellites` 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 AWS Ground Station 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"
      }
  }
```

Fornecimento de dados de efemérides personalizados

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

O acesso à API Ephemeris é fornecido somente conforme a necessidade. Os clientes que precisam fazer upload de dados de efemérides personalizados devem entrar em contato pelo e-mail aws-groundstation@amazon.com.

Visão geral

A API Ephemeris permite que efemérides personalizadas sejam enviadas para AWS Ground Station uso com um satélite. Essas efemérides substituem as padrão do Space Track (consulte: Dados de efemérides padrão).

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

Criar 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 em `DescribeEphemeris` ou usar os eventos do Cloudwatch para rastrear as mudanças de status das efemérides.

Para solucionar problemas de efemérides inválidas, consulte: Solução de problemas de efemérides inválidas

Crie uma efeméride do conjunto de TLE via API

O cliente AWS Ground Station boto3 pode ser usado 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).

Um conjunto de TLE é um objeto formatado em JSON que agrupa um ou mais TLEs para construir uma trajetória contínua. Os TLEs no conjunto de TLE devem formar um conjunto contínuo que possamos usar para construir uma trajetória (ou seja, sem lacunas no tempo entre os TLEs em um conjunto de 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 dos TLEs em um conjunto de TLE devem corresponder exatamente para serem uma trajetória válida e contínua.

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 ID de efeméride que pode ser usado para referenciar as efemérides no futuro. Por exemplo, podemos usar o ID de efeméride 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 rota `DescribeEphemeris` ou usar os eventos do Cloudwatch para rastrear o status das efemérides carregadas, pois elas precisam passar por um fluxo de trabalho de validação assíncrona antes de serem configuradas como `ENABLED` e se tornarem utilizáveis para agendar e executar contatos.

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

Fazer upload 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 = customer_client.create_ephemeris( name="2022-10-26 S3
 OEM Upload", satelliteId="fde41049-14f7-413e-bd7b-EXAMPLE01", enabled=True,
 expirationTime=datetime.now(timezone.utc) + timedelta(days=5), priority=2,
    ephemeris = {
        "oem": {
            "s3Object": {
                "bucket": "ephemeris-bucket-for-testing",
                "key": "test_data.oem",
            }
        }
    })
```

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"
        }
    }
}
```

Solução de problemas de efemérides inválidas

Quando uma efeméride personalizada é carregada para o 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, o `DescribeEphemeris` retornará uma EphemerisInvalidReason, que fornece uma visão sobre por que a efeméride falhou na validação. Os valores potenciais de EphemerisInvalidReason são 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"
      }
    }
  },
}
```

Revertendo 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.

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 adversamente 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 os clientes sob um acordo de confidencialidade (NDA).

Máscaras específicas para clientes

Além das máscaras de site do AWS Ground Station em cada local, cada cliente 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 os clientes não reservem ou paguem pelo tempo quando o satélite está 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 os clientes usem todo o tempo de contato disponível para o 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. Os clientes são responsáveis 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 do cliente, mesmo que partes do tempo reservado não estejam disponíveis para uplink.

Histórico do documento para o guia AWS Ground Station do usuário

A tabela a seguir descreve as mudanças importantes na documentação desde a última versão do AWS Ground Station.

Alteração	Descrição	Data de lançamento
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 instância do EC2 e planejamento de CPU”.	6 de março de 2024
Atualização da documentação	Foram adicionadas novas práticas recomenda das 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 DirectBro adcastSatelliteWbDigIfEc 2.	14 de fevereiro de 2024
Atualização da documentação	Foi adicionada referência à AWS Notificações de Usuários na documentação de monitoram ento.	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

Alteração	Descrição	Data de lançamento
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
Atualizações de políticas gerenciadas pela AWS — Nova política AWS gerenciada	AWS Ground Station adicionou uma nova política chamada AWSGroundStationAgentInstancePolicy.	12 de abril de 2023
Novo recurso	Atualizou o guia do usuário para o lançamento do CPE Preview.	9 de novembro de 2022
Atualizações de políticas gerenciadas pela AWS — Nova política AWS gerenciada	AWS Ground Station adicionou a AWSServiceRoleForGroundStationDataflowEndpointGroup 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 monitoramento AWS Ground Station com CloudWatch eventos.	4 de fevereiro de 2020

Alteração	Descrição	Data de lançamento
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 conceitos básicos	Atualizou o tópico Introdução, que inclui os AWS CloudFormation 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

Glossário do AWS

Para obter a terminologia mais recente da AWS, consulte o glossário da AWS na Referência do Glossário da AWS.

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.