Guía del usuario

AWS Ground Station

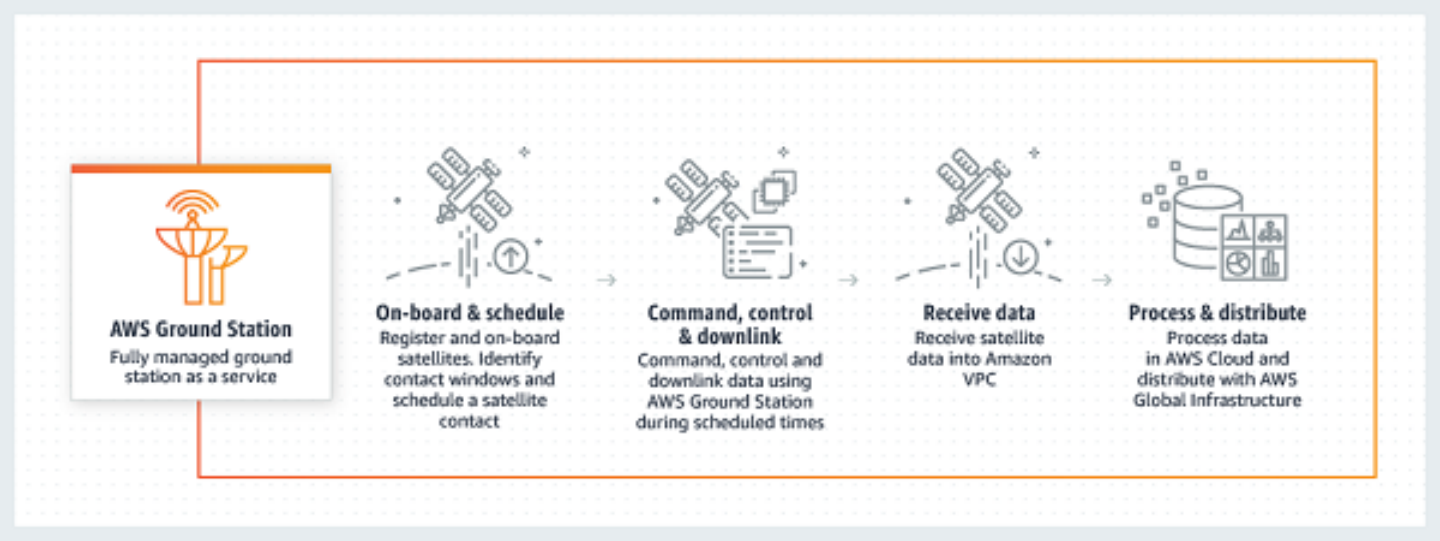
AWS Ground Station: Guía del usuario

Table of Contents

¿Qué es AWS Ground Station?

AWS Ground Station es un servicio completamente administrado que le permite controlar las comunicaciones por satélite, procesar los datos del satélite y escalar las operaciones del satélite. Es decir, ya no tiene que crear ni administrar su propia infraestructura de estación terrestre.

AWS Ground Station le permite centrarse en la innovación y en probar rápidamente nuevas aplicaciones que adquieran datos de los satélites y amplíen dinámicamente el uso del servidor y del sistema de almacenamiento, en lugar de dedicar recursos a gestionar y mantener su propias estaciones terrestres.



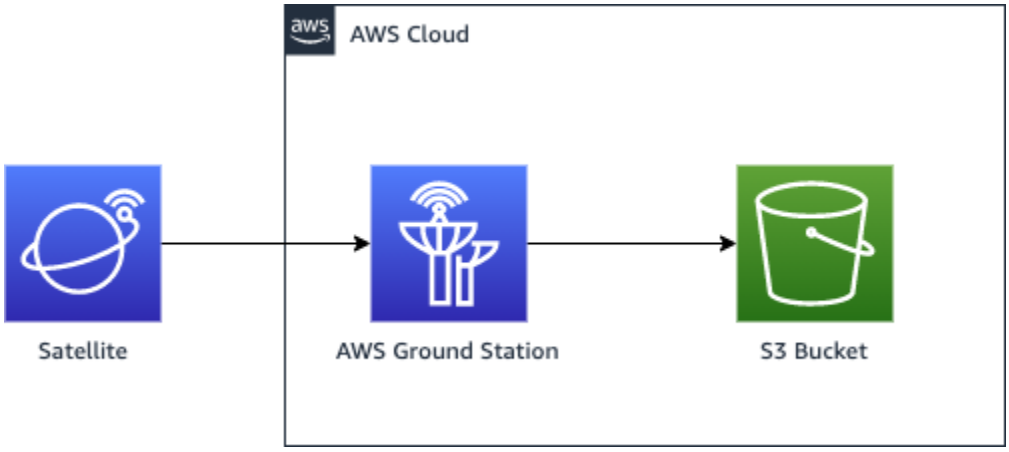
Cómo funciona AWS Ground Station

La reserva de un satélite también se denomina contacto. El satélite se comunica con una AWS Ground Station antena durante los contactos. Puede reservar contactos a través de una API o de la AWS consola especificando la ubicación, la hora y la información de la misión. Los datos de sus contactos pueden transmitirse a y desde una instancia de Amazon Elastic Compute Cloud (Amazon EC2) o entregarse de forma asíncrona a un bucket de Amazon Simple Storage Service (Amazon S3) de su cuenta.

Puede crear recursos de configuración ampliables y reutilizables para controlar cómo se configuran AWS Ground Station las antenas durante sus contactos. Al utilizar perfiles de misión, puede especificar de dónde proceden los datos, cuál debe ser su formato y dónde enviarlos.

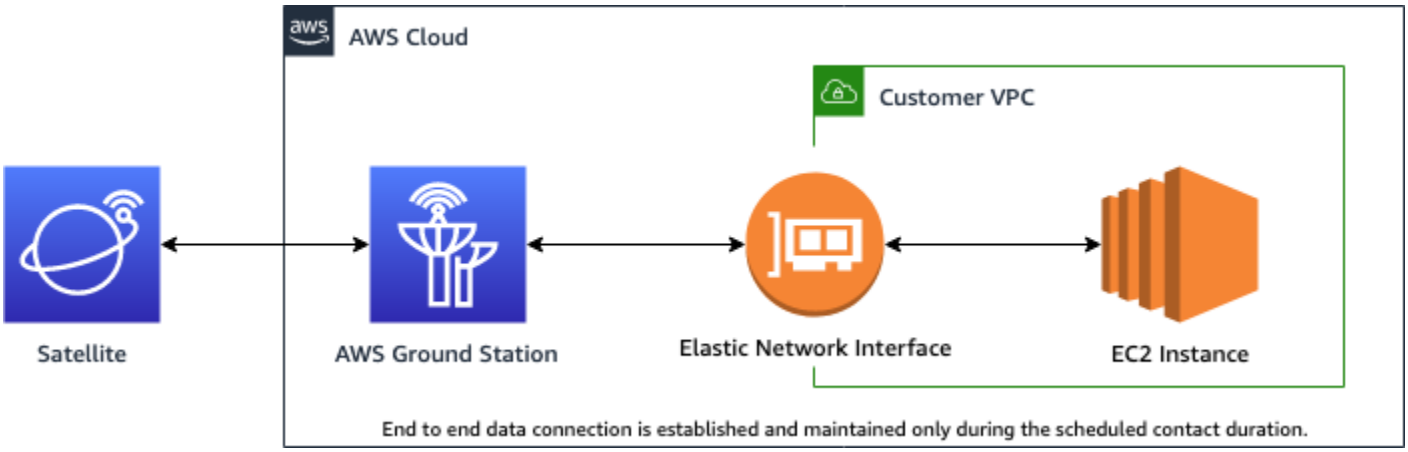
Envío de datos a Amazon EC2

Con la entrega de datos a Amazon S3, los datos de contacto se envían de forma asíncrona a un bucket de Amazon S3 de su cuenta. Sus datos de contacto se entregan como archivos de captura de paquetes (pcap) para permitir la reproducción de los datos de contacto en una radio definida por software (SDR) o para extraer los datos de carga útil de los archivos pcap para su procesamiento. Los archivos pcap se envían a su bucket de Amazon S3 cada 30 segundos a medida que el hardware de la antena recibe los datos de contacto para permitir el procesamiento de los datos de contacto durante el contacto si lo desea. Una vez recibidos, puede procesar los datos con su propio software de posprocesamiento o utilizar otros servicios de AWS, como Amazon SageMaker o Amazon Rekognition. La entrega de datos a Amazon S3 solo está disponible para datos de enlace descendente desde su satélite; no es posible vincular datos de subida a su satélite desde Amazon S3.



Envío de datos a Amazon EC2

Con la entrega de datos a Amazon EC2, sus datos de contacto se transmiten desde y hacia su instancia de Amazon EC2. Puede procesar los datos en tiempo real en su instancia de Amazon EC2 o reenviarlos para su posterior procesamiento.



Más información

Con él AWS Ground Station puede acceder a más de 125 servicios a través de comunicaciones por satélite. Tenga en cuenta lo siguiente:

- Puede recibir datos de RF de banda estrecha en banda S (de 2200 a 2300 MHz) o en banda X (de 7750 a 8400 MHz) en anchos de banda de hasta 54 MHz.
  - Los datos de RF de banda S se digitalizan y se proporcionan como una secuencia digital en formato VITA-49 Signal Data/IP.
  - Los datos de frecuencia intermedia (IF) de banda X se digitalizan y se proporcionan como una secuencia digital en formato VITA-49 Signal Data/IP.
- Puede recibir datos desmodulados/descodificados de banda ancha en banda X (de 7750 a 8400 MHz) en anchos de banda de hasta 500 MHz
  - Los datos de frecuencia intermedia (IF) de banda X se desmodulan, descodifican y se proporcionan como una secuencia digital en formato VITA-49 Extension Data/IP.
- Puede recibir datos de frecuencia intermedia digital (DigiF) de banda ancha de 40 MHz a 400 MHz de ancho de banda a través del Agente. AWS Ground Station
  - Consulte AWS Ground Station Guía del usuario del agente para obtener más información sobre el AWS Ground Station agente y la entrega de datos DigiF de banda ancha.

- Puede transmitir datos RF en banda S (de 2025 a 2120 MHz) en anchos de banda de hasta 54 MHz.
  - Los datos de RF se proporcionan AWS Ground Station como una transmisión digital en formato VITA-49 Signal Data/IP.
- Debe correr AWS Ground Station desde una AWS región que lo admita. AWS Ground Station Para consultar una lista de regiones admitidas, consulte la Tabla de regionesde infraestructura global.
- Puede enviar datos a una instancia de Amazon EC2 que se ejecute en la misma región que la antena o puede utilizar la entrega de datos entre regiones para enviar sus datos desde una antena a una instancia de Amazon EC2 en la región de AWS que prefiera. Las siguientes antenna-to-destination regiones están disponibles actualmente:
  - Región EE. UU. Este (Ohio) (us-east-2) a región EE. UU. Oeste (Oregón) (us-west-2)
  - Región EE. UU. Oeste (Oregón) (us-west-2) a región EE. UU. Este (Ohio) (us-east-2)

Condiciones del servicio

Solo puede usar los Servicios para almacenar, recuperar, consultar, servir y ejecutar Contenido de su propiedad, para el que tenga licencia o que haya obtenido legalmente. En estas Condiciones del servicio, (a) "su Contenido" hace referencia a cualquier "Contenido de la empresa" y a cualquier "Contenido del cliente" y (b) "Contenido de AWS" hace referencia a las "Propiedades de Amazon". Como parte de los Servicios, es posible que tenga permiso para utilizar determinado software (incluida la documentación relacionada) proporcionado por nosotros o por licenciantes externos.

> **Important**
>
> Este software no se le vende ni se le distribuye, y puede usarlo únicamente como parte de los Servicios. No puede transferirlo fuera de los Servicios sin disponer de una autorización específica.

Componentes básicos

Los grupos de puntos finales, las configuraciones y los perfiles de misión del flujo de datos son componentes principales de. AWS Ground Station Estos componentes determinan cómo programar sus contactos, cómo las antenas se comunican con sus satélites y dónde se entregan sus datos. Antes de empezar AWS Ground Station, le recomendamos que conozca estos componentes. Se ofrecen ejemplos en sus respectivas secciones.

Temas

Grupos de punto de enlace de flujo de datos

Los puntos de enlace de flujo de datos definen las ubicaciones de origen y de destino en las que desea que se transmitan los datos durante los contactos. Los puntos de enlace se identifican mediante el nombre que elija al ejecutar contactos. Estos nombres no tienen por qué ser únicos. Esto permite ejecutar varios contactos a la vez utilizando el mismo perfil de misión.

La dirección de la lista de puntos de enlace consta de los elementos siguientes:

- `name`: dirección IP de este punto de enlace de flujo de datos.
- `port`: el puerto de conexión.

Los detalles de seguridad de un punto de enlace constan de los elementos siguientes:

- `roleArn`- El nombre de recurso de Amazon (ARN) de un rol que AWS Ground Station asumirá la creación de interfaces de red elásticas (ENI) en la VPC. Estos ENI sirven como puntos de entrada y salida de datos transmitidos durante un contacto.
- `securityGroupIds`: los grupos de seguridad que adjuntar a las interfaces de redes elásticas.
- `subnetIds`- Una lista de subredes donde se AWS Ground Station colocan las interfaces de red elásticas para enviar transmisiones a las instancias.

El rol de IAM que se pasa a `roleArn` debe tener una política de confianza que permita a la entidad principal del servicio `groundstation.amazonaws.com` asumir el rol. Consulte la política de confianza de ejemplo a continuación para ver un ejemplo. Durante la creación del punto final, el identificador del recurso del punto final no existe, por lo que la política de confianza debe usar un asterisco (`*`) en lugar de él. *`your-endpoint-id`* Esto se puede actualizar después de la creación para usar el id. de recurso de punto de conexión a fin de incluir la política de confianza en ese grupo de puntos de conexión de flujo de datos específico.

El rol de IAM debe tener una política de IAM que permita AWS Ground Station configurar los ENI. Consulte la política de roles de ejemplo a continuación para ver un ejemplo.

Política de confianza de ejemplo

Para obtener más información acerca de cómo actualizar la política de confianza de un rol, consulte Administrar roles de IAM en la Guía del usuario de 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"
        }
      }
    }
  ]
}
```

Política de roles de ejemplo

Para obtener más información acerca de cómo actualizar o adjuntar una política de roles, consulte Administrar políticas de IAM en la Guía del usuario de IAM.

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

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

Los puntos de enlace de flujo de datos siempre se crean como parte de un grupo de punto de enlace de flujo de datos. Al incluir varios puntos de enlace de flujo de datos en un grupo, indica que todos los puntos de enlace especificados se pueden utilizar en conjunto durante un único contacto. Por ejemplo, si un contacto necesita enviar datos a tres puntos de enlace de flujo de datos distintos, debe contar con tres puntos de enlace en un único grupo de puntos de enlace de flujo de datos que coincidan con las configuraciones de los puntos de enlace de flujo de datos de su perfil de misión.

Cuando uno o varios recursos de un grupo de punto de enlace de flujo de datos estén en uso para un contacto, el grupo al completo se reserva durante dicho contacto. Puede ejecutar varios contactos a la vez, pero dichos contactos deben ejecutarse en diferentes grupos del punto de conexión de flujo de datos.

Los grupos del punto de conexión de flujo de datos deben estar en un estado `HEALTHY` para programar que los contactos los utilicen. A continuación se enumeran los motivos por los que es posible que sus grupos del punto de conexión de flujo de datos no se encuentren en un estado `HEALTHY`, así como las medidas correctivas adecuadas que se deben tomar.

- `NO_REGISTERED_AGENT`- Inicie la instancia EC2, que registrará el agente. enga en cuenta que debe tener un archivo de configuración del controlador válido para que esta llamada se realice correctamente. Consulte la AWS Ground Station Guía del usuario del agente para obtener más información sobre la configuración de ese archivo.
- `INVALID_IP_OWNERSHIP`- Utilice la DeleteDataflowEndpointGroup API para eliminar el grupo de puntos de conexión de Dataflow y, a continuación, utilice la CreateDataflowEndpointGroup API para volver a crear el grupo de puntos de conexión de Dataflow con las direcciones IP y los puertos asociados a la instancia de EC2.
- `UNVERIFIED_IP_OWNERSHIP`- La dirección IP aún no se ha validado. La validación se realiza periódicamente, por lo que debería resolverse por sí sola.

- `NOT_AUTHORIZED_TO_CREATE_SLR`- La cuenta no está autorizada para crear el rol vinculado al servicio necesario. Consulte los pasos de solución de problemas en Uso de funciones vinculadas a servicios para la estación terrestre

Consulte la siguiente documentación para obtener más información sobre cómo realizar operaciones en grupos de puntos finales de flujos de datos mediante la API o la API. AWS CloudFormation AWS Command Line Interface AWS Ground Station

- AWS::GroundStation::DataflowEndpointTipo de recurso de grupo CloudFormation
- Referencia de Dataflow Endpoint Group AWS CLI
- Referencia de la API del grupo del punto de conexión de flujo de datos

Configuraciones

Las configuraciones son recursos que se AWS Ground Station utilizan para definir los parámetros de cada aspecto de su contacto. Añada las configuraciones que desee a un perfil de misión y, a continuación, dicho perfil de misión se utilizará al ejecutar el contacto. Puede definir varios tipos distintos de configuraciones.

Consulte la siguiente documentación para obtener más información sobre cómo realizar operaciones en las configuraciones mediante la AWS CloudFormation API o la AWS Command Line Interface AWS Ground Station API. A continuación, también se proporcionan enlaces a la documentación para tipos de configuración específicos.

- AWS::GroundStation::Config CloudFormation tipo de recurso
- Config AWS CLI reference
- Referencia de la API de Config

Configuración de punto de enlace de flujo de datos

> **Note**
>
> Las configuraciones de punto de conexión de Dataflow solo se utilizan para la entrega de datos a Amazon EC2 y no se utilizan para la entrega de datos a Amazon S3.

Puede utilizar las configuraciones de punto de conexión del flujo de datos para especificar desde qué punto de conexión del flujo de datos de un grupo de puntos de conexión del flujo de datos o hacia qué punto de conexión del flujo de datos desea que fluyan los datos durante un contacto. Los dos parámetros de una configuración de punto de enlace de flujo de datos especifican el nombre y la región del punto de enlace de flujo de datos. Al reservar un contacto, AWS Ground Station analiza el perfil de la misión que especificó e intenta encontrar un grupo de puntos finales del flujo de datos que contenga todos los puntos finales del flujo de datos especificados en las configuraciones de puntos finales del flujo de datos incluidas en el perfil de la misión.

La propiedad `dataflowEndpointName` de una configuración de punto de conexión del flujo de datos especifica a qué punto de conexión del flujo de datos de un grupo de puntos de conexión del flujo de datos fluirán los datos durante un contacto.

La propiedad `dataflowEndpointRegion` especifica en qué región reside el punto de conexión del flujo de datos. Si se especifica una región en la configuración del punto final del flujo de datos, busca un punto final del flujo de datos en la región especificada. AWS Ground Station Si no se especifica ninguna región, AWS Ground Station se utilizará de forma predeterminada la región de la estación terrestre del contacto. Se considera que un contacto es un contacto de entrega de datos entre regiones si la región de su punto de conexión del flujo de datos no es la misma que la región de la estación terrestre del contacto.

Consulte la siguiente documentación para obtener más información sobre cómo realizar operaciones en las configuraciones de los puntos finales del flujo de datos mediante la AWS CloudFormation API o la AWS Command Line Interface API. AWS Ground Station

- AWS::GroundStation::Config DataflowEndpointConfig CloudFormation propiedad
- Config AWS CLI reference (consulte la `dataflowEndpointConfig -> (structure)` sección)
- DataflowEndpointConfig Referencia de la API

Configuración de grabación de S3

> **Note**
>
> Las configuraciones de grabación de S3 solo se utilizan para la entrega de datos a Amazon S3 y no se utilizan para la entrega de datos a Amazon EC2.

Puede utilizar las configuraciones de grabación de S3 para especificar un bucket de Amazon S3 al que desea que se entreguen los datos de enlace descendente. Los dos parámetros de una configuración de grabación de S3 especifican el bucket de Amazon S3 y la función de IAM que AWS Ground Station deben asumirse al entregar los datos a su depósito de Amazon S3. El rol de IAM y el bucket de Amazon S3 especificados deben cumplir los siguientes criterios:

- El nombre del bucket de Amazon S3 debe comenzar por `aws-groundstation`.
- El rol de IAM debe tener una política de confianza que permita a la entidad principal del servicio `groundstation.amazonaws.com` asumir el rol. Consulte la política de confianza de ejemplo a continuación para ver un ejemplo. Durante la creación de la configuración, el identificador del recurso de configuración no existe, la política de confianza debe utilizar un asterisco (`*`) en lugar del identificador del recurso de configuración *`your-config-id`*y, una vez creada, se puede actualizar con el identificador del recurso de configuración.
- El rol de IAM debe tener una política de IAM que le permita realizar la acción `s3:GetBucketLocation` en el bucket y `s3:PutObject` en los objetos del bucket. Si el bucket de Amazon S3 tiene una política de bucket, la política de bucket también debe permitir que el rol de IAM lleve a cabo estas acciones. Consulte la política de roles de ejemplo a continuación para ver un ejemplo.

Política de confianza de ejemplo

Para obtener más información acerca de cómo actualizar la política de confianza de un rol, consulte Administrar roles de IAM en la Guía del usuario de 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"
        }
      }
    }
  ]
}
```

Política de roles de ejemplo

Para obtener más información acerca de cómo actualizar o adjuntar una política de roles, consulte Administrar políticas de IAM en la Guía del usuario de 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 la siguiente documentación para obtener más información sobre cómo realizar operaciones en S3 grabando configuraciones mediante la AWS CloudFormation API o la AWS Command Line Interface AWS Ground Station API.

- AWS::GroundStation::Config Propiedad S3 RecordingConfig CloudFormation
- Config AWS CLI reference (consulte la `s3RecordingConfig -> (structure)` sección)
- Referencia de RecordingConfig la API de S3

Configuración de seguimiento

Puede utilizar configuraciones de seguimiento en el perfil de misión para determinar si se debe habilitar el seguimiento automático durante sus contactos. Esta configuración tiene un único parámetro: `autotrack`. El parámetro `autotrack` puede tener los siguientes valores:

- `REQUIRED`: el seguimiento automático es obligatorio para sus contactos.
- `PREFERRED`: el seguimiento automático es preferible para los contactos, pero se pueden seguir ejecutando sin él.
- `REMOVED`: no se debe utilizar el seguimiento automático para sus contactos.

Consulte la siguiente documentación para obtener más información sobre cómo realizar operaciones de seguimiento de configuraciones mediante AWS CloudFormation la AWS Command Line Interface API o la AWS Ground Station API.

- AWS::GroundStation::Config TrackingConfig CloudFormation propiedad
- Config AWS CLI reference (consulte la `trackingConfig -> (structure)` sección)
- TrackingConfig Referencia de la API

Configuración de enlace de bajada de antena

Puede utilizar configuraciones de enlace descendente de antena para configurar el enlace descendente de antena durante su contacto. Consisten en una configuración espectral que especifica el ancho de banda, la frecuencia y la polarización que se deben utilizar durante su contacto de enlace descendente. Si su caso de uso de enlace descendente requiere desmodulación o descodificación, consulte la Configuración de descodificación y desmodulación de enlace de bajada de antena.

Consulte la siguiente documentación para obtener más información sobre cómo realizar operaciones en las configuraciones de enlace descendente de la antena mediante AWS CloudFormation la API AWS Command Line Interface o la AWS Ground Station API.

- AWS::GroundStation::Config AntennaDownlinkConfig CloudFormation propiedad
- Config AWS CLI reference (consulte la `antennaDownlinkConfig -> (structure)` sección)
- AntennaDownlinkConfig Referencia de la API

Configuración de descodificación y desmodulación de enlace de bajada de antena

Las configuraciones de descodificación y desmodulación de enlace de bajada de antena son un tipo de configuración más complejo y personalizable que puede utilizar para ejecutar un contacto de enlace de bajada con desmodulación o descodificación. Si te interesa ejecutar este tipo de contactos, ponte en contacto con el AWS Ground Station equipo. Le ayudaremos a definir la configuración y el perfil de misión correctos según su caso de uso.

Consulte la siguiente documentación para obtener más información sobre cómo realizar operaciones en las configuraciones de decodificación demod de enlace descendente de antenas mediante AWS CloudFormation la API o la API AWS Command Line Interface. AWS Ground Station

- AWS::GroundStation::Config AntennaDownlinkDemodDecodeConfig CloudFormation propiedad
- Config AWS CLI reference (consulte la `antennaDownlinkDemodDecodeConfig -> (structure)` sección)
- AntennaDownlinkDemodDecodeConfig Referencia de la API

Configuración de enlace de subida de antena

Puede utilizar configuraciones de enlace ascendente de antena para configurar la antena durante su contacto de enlace ascendente. Constan de una configuración de espectro con frecuencia, polarización y potencia radiada isotrópica efectiva (EIRP) objetivo. Para obtener información acerca de cómo configurar una repetición de enlace ascendente, consulte Configuración de Echo de enlace ascendente.

Consulte la siguiente documentación para obtener más información sobre cómo realizar operaciones en las configuraciones de enlace ascendente de la antena mediante AWS CloudFormation la API AWS Command Line Interface o la AWS Ground Station API.

- AWS::GroundStation::Config AntennaUplinkConfig CloudFormation propiedad
- Config AWS CLI reference (consulte la `antennaUplinkConfig -> (structure)` sección)
- AntennaUplinkConfig Referencia de la API

Configuración de Echo de enlace ascendente

Las configuraciones de repetición de enlace de subida indican a la antena cómo ejecutar una repetición de enlace de subida. Esta devuelve los comandos enviados por la antena a su punto de enlace de flujo de datos. Una configuración de repetición de enlace de subida contiene el ARN de una configuración de enlace de subida. La antena emplea los parámetros de la configuración de enlace de subida indicada por el ARN al ejecutar una repetición de enlace de subida.

Consulte la siguiente documentación para obtener más información sobre cómo realizar operaciones en configuraciones de eco de enlace ascendente mediante la AWS CloudFormation API o la AWS Command Line Interface AWS Ground Station API.

- AWS::GroundStation::Config UplinkEchoConfig CloudFormation propiedad
- Config AWS CLI reference (consulte la `uplinkEchoConfig -> (structure)` sección)
- UplinkEchoConfig Referencia de la API

Perfiles de misión

Los perfiles de misión cuentan con configuraciones y parámetros para el modo en que se ejecutan los contactos. Cuando reserva un contacto o busca los contactos disponibles, suministra el perfil de misión que pretende emplear. Los perfiles de misión combinan todas las configuraciones y definen cómo se configurará y dónde irán los datos durante el contacto.

Aparte de las configuraciones seguimiento, todas las configuraciones están incluidas en el campo `dataflowEdges` del perfil de misión. Una única periferia de flujo de datos es una lista de dos ARN: el primero es la configuración de origen y el segundo es la configuración de destino. Al especificar un límite de flujo de datos entre dos configuraciones, se sabe AWS Ground Station desde dónde y hacia dónde deben fluir los datos durante un contacto. Las configuraciones de seguimiento no se utilizan como parte de una periferia de flujo de datos, pero se especifican como un campo independiente.

El campo `name` del perfil de misión ayuda a distinguir los perfiles de misión que se crean.

Consulte la siguiente documentación para obtener más información sobre cómo realizar operaciones en los perfiles de misión mediante la AWS CloudFormation API o la AWS Command Line Interface API. AWS Ground Station

- AWS::GroundStation::MissionProfile CloudFormation tipo de recurso
- AWS CLI Referencia del perfil de la misión

- Referencia de la API del perfil de misión

Ubicaciones de AWS Ground Station

Los clientes pueden transmitir y recibir datos utilizando las antenas de AWS Ground Station en las siguientes ubicaciones: EE.UU. (Oregón), EE.UU. (Ohio), EE.UU. (Alaska), Medio Oriente (Baréin), Europa (Estocolmo), Asia Pacífico (Dubbo), Europa (Irlanda), África (Ciudad del Cabo), EE.UU. (Hawái), Asia Pacífico (Seúl), Asia Pacífico (Singapur) y Sudamérica (Punta Arenas).

Los clientes pueden enviar datos y configurar sus contactos con la consola AWS Ground Station en las siguientes regiones: Oeste de EE. UU. (Oregón), Este de EE. UU. (Ohio), Medio Oriente (Baréin), Europa (Estocolmo), Asia Pacífico (Dubbo), Europa (Irlanda), África (Ciudad del Cabo), Este de EE. UU. (Norte de Virginia), Europa (Fráncfort), Asia Pacífico (Seúl), Asia Pacífico (Singapur) y América del Sur (São Paulo).

Nota: Solo puede crear recursos de AWS Ground Station en las regiones que albergan la consola de AWS Ground Station mencionada en el párrafo anterior.

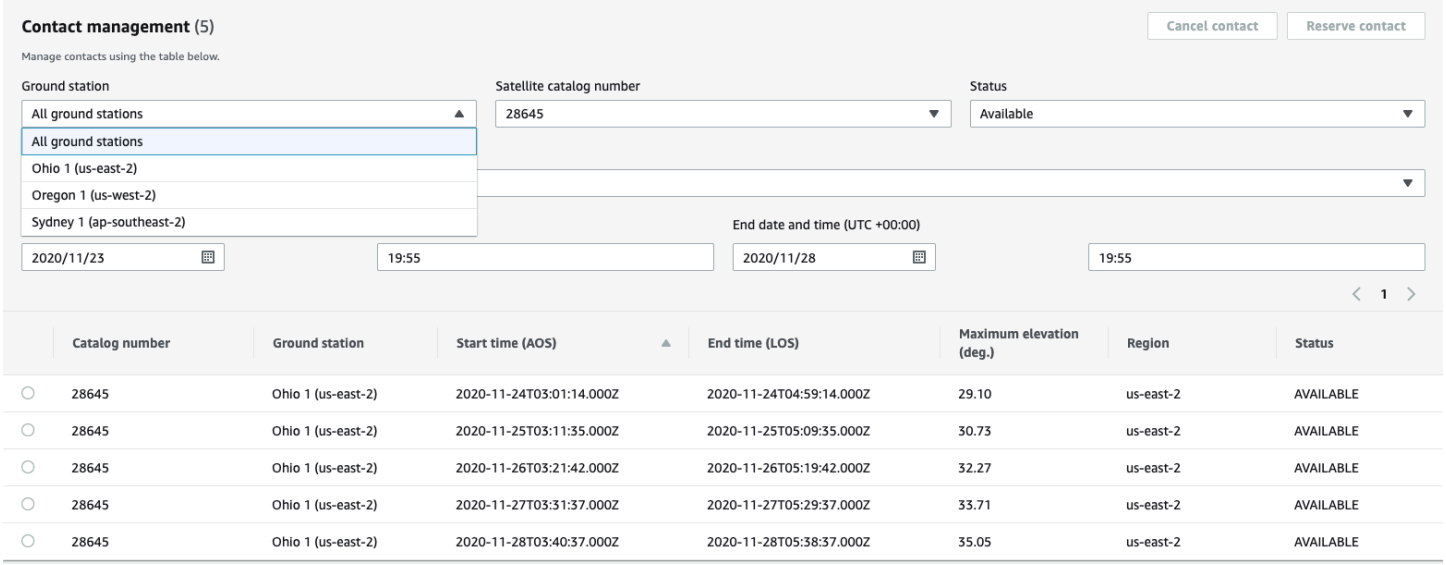
Temas

- Resultado de la búsqueda de la región de AWS para una Ground Station

Resultado de la búsqueda de la región de AWS para una Ground Station

La red global de AWS incluye ubicaciones de Ground Station que no se encuentran físicamente en la región de AWS a la que están conectadas. El listado y la reserva de contactos en una de estas ubicaciones de Ground Station se deben realizar utilizando la región de AWS a la que está conectada la Ground Station.

Existen varios métodos para determinar la región de AWS de una Ground Station. La página de la consola de AWS Ground Station muestra la región de AWS de la Ground Station cuando se visualiza en la tabla de filtros y contactos, tal y como se indica en la siguiente imagen. El SDK de AWS contiene la región AWS de la Ground Station en la respuesta ListGroundStation. Por último, AWS CLI contiene la región de AWS de la Ground Station en la respuesta list-ground-stations.



Temas

- Ejemplo de Ground Station situada fuera de una región AWS

Ejemplo de Ground Station situada fuera de una región AWS

Hawaii 1 es un ejemplo de ubicación de una Ground Station que no se encuentra físicamente en la región de AWS a la que está conectada. La Ground Station Hawaii 1 se encuentra en Hawai, EE.UU., pero está conectada a la región de AWS us-west-2 (Oregón). Para enumerar y reservar contactos utilizando Hawaii 1, debe tener un perfil de misión onfigurado en la región de AWS us-

west-2 (Oregón) y utilizar la región de AWS us-west-2 (Oregón) en la consola de AWS Ground Station console, AWS CLI, o SDK de AWS.

- Para enumerar y reservar contactos para Hawaii 1 en la consola de la AWS Ground Station, debe utilizar la consola de la AWS Ground Station console en la región us-west-2 (Oregon).
- Para enumerar y reservar contactos para Hawaii 1 mediante AWS CLI, debe especificar la región como us-west-2 con el comando `--region`CLI.
- Para enumerar y reservar contactos para Hawaii 1 mediante el SDK de AWS, debe establecer la región de su cliente en us-west-2. El modo de configurarlo depende del lenguaje de programación que utilice. En la documentación de SDK de AWS para JavaScript se describe un ejemplo de cómo configurar esto utilizando JavaScript. Para obtener más información, consulte la documentación del SDK específica de cada idioma.

Configuración AWS Ground Station

Antes de empezar a utilizarlos AWS Ground Station, necesita saber qué permisos AWS Identity and Access Management (IAM) necesita y qué credenciales de vehículo espacial debe proporcionar. Utilice los siguientes pasos para configurar su cuenta.

Temas

Inscríbase para obtener un Cuenta de AWS

Si no tiene uno Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirte a una Cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

   Cuando te registras en una Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea una. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. Puede ver la actividad de la cuenta y administrar la cuenta en cualquier momento entrando en https://aws.amazon.com/ y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

Después de crear un usuario administrativo Cuenta de AWS, asegúrelo Usuario raíz de la cuenta de AWS AWS IAM Identity Center, habilite y cree un usuario administrativo para no usar el usuario root en las tareas diarias.

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión AWS Management Consolecomo propietario de la cuenta seleccionando el usuario root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.

   Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Iniciar sesión como usuario raíz en la Guía del usuario de AWS Sign-In .
2. Active la autenticación multifactor (MFA) para el usuario raíz.

   Para obtener instrucciones, consulte Habilitar un dispositivo MFA virtual para el usuario Cuenta de AWS raíz (consola) en la Guía del usuario de IAM.

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

   Consulte las instrucciones en Activar AWS IAM Identity Center en la Guía del usuario de AWS IAM Identity Center .
2. En IAM Identity Center, conceda acceso administrativo a un usuario.

   Para ver un tutorial sobre su uso Directorio de IAM Identity Center como fuente de identidad, consulte Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la Guía del AWS IAM Identity Center usuario.

Iniciar sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, utilice la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

  Para obtener ayuda para iniciar sesión con un usuario del Centro de identidades de IAM, consulte Iniciar sesión en el portal de AWS acceso en la Guía del AWS Sign-In usuario.

Concesión de acceso a usuarios adicionales

1. En IAM Identity Center, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos de privilegios mínimos.

   Para conocer las instrucciones, consulte Create a permission set en la Guía del usuario de AWS IAM Identity Center .

2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

   Para conocer las instrucciones, consulte Add groups en la Guía del usuario de AWS IAM Identity Center .

Agrega permisos de Ground Station a tu AWS cuenta

Para utilizarla AWS Ground Station sin necesidad de un usuario administrativo, debe crear una nueva política y adjuntarla a su AWS cuenta.

1. Inicie sesión en la consola de IAM AWS Management Console y ábrala.
2. Cree una política nueva. Utilice los siguientes pasos:

   a. En el panel de navegación, seleccione Policies (Políticas) y, a continuación, seleccione Create policy (Crear política).

   b. En la pestaña JSON, edite el JSON con uno de los siguientes valores. Utilice el JSON que mejor funcione en la aplicación.

      - Para los privilegios administrativos de Ground Station, configure Action cómo groundstation:* de la siguiente forma:

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

```
      ]
    }
  ]
}
```

- En Privilegios de solo lectura, establezca Action (Acción) en groundstation:Get*, groundstation:List* y groundstation:Describe* de la siguiente forma:

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

- Para mayor seguridad mediante la autenticación multifactor, defina Action en groundstation: * y Condition/Bool en aws ::true de la siguiente manera: MultiFactorAuthPresent

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

```
}
```

3. En la consola de IAM, asocie la política que ha creado al usuario deseado.

Para obtener más información acerca de los usuarios de IAM y la asociación de políticas, consulte la guía del usuario de IAM.

Incorporación de clientes

Para completar el registro de tu AWS Ground Station cuenta, consulta la sección Satélites y recursos de la página de la AWS Ground Station consola para obtener información sobre la incorporación. El AWS Ground Station equipo trabajará con usted para incorporar sus satélites al servicio. Una vez que haya incorporado su satélite, este estará disponible para su uso durante la administración de un contacto. Las instrucciones para administrar un contacto se detallan en Enumeración y reserva de contactos.

Al incorporar sus satélites, obtendrá acceso para enviar y recibir datos desde y hacia el satélite. Además de incorporar sus propios satélites, los clientes también pueden subir a bordo de los siguientes satélites para enlazar los datos de transmisión directa mediante AWS Ground Station:

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

Una vez incorporados, podrá acceder a estos satélites para su uso inmediato. AWS Ground Station mantiene una serie de AWS CloudFormation plantillas preconfiguradas para facilitar la puesta en marcha del servicio. Las instrucciones y los detalles para acceder a esta plantilla y utilizarla se proporcionan en la sección Cree sus recursos mediante una AWS CloudFormation plantilla de la guía del usuario.

Para obtener más información acerca de estos satélites y el tipo de datos que transmiten, consulte Aqua y JPSS-1/NOAA-20 y SNPP y Terra.

Siguientes pasos

Su AWS Ground Station cuenta ya está configurada y lista para su configuración. Continúe con Introducción para configurar los recursos para utilizar AWS Ground Station.

Cómo empezar con AWS Ground Station

AWS Ground Station le permite ordenar, controlar y transferir datos desde sus satélites.

Con AWS Ground Stationél, puede programar el acceso a las antenas de las estaciones terrestres por minuto y pagar solo por el tiempo de uso de la antena. AWS Ground Station entrega sus datos de contacto de forma asíncrona a un bucket de Amazon Simple Storage Service (Amazon S3) de su cuenta o de forma sincrónica transmitiéndolos desde y hacia una instancia de Amazon Elastic Compute Cloud (Amazon EC2) de su cuenta. En los siguientes pasos se describe cómo configurar los recursos necesarios para recibir datos de contacto de forma asíncrona en un bucket de Amazon S3. Consulte la guía de Envío de datos a Amazon EC2 para obtener información sobre el envío de datos a Amazon EC2.

Temas

Conceptos básicos

Antes de empezar, debe familiarizarse con los conceptos básicos de AWS Ground Station. Para obtener más información, consulte Componentes básicos.

Luego, continúe Requisitos previos para conocer los requisitos previos para comenzar. AWS Ground Station

Requisitos previos

Antes de empezar AWS Ground Station, asegúrate de tener una AWS cuenta con las credenciales adecuadas. Siga los pasos de Configuración AWS Ground Station.

> **Note**
>
> Si va a utilizar la entrega de datos DigiF de banda ancha, consulte AWS Ground Station Guía del usuario del agente para ver las instrucciones.

De lo contrario, siga en Paso 1: Elige una AWS CloudFormation plantilla.

Paso 1: Elige una AWS CloudFormation plantilla

Una vez embarcado en el satélite, es necesario definir los perfiles de misión para definir la configuración de la AWS Ground Station antena para el enlace descendente de los datos del satélite. Para ayudarlo con este proceso, proporcionamos AWS CloudFormation plantillas preconfiguradas para la entrega de datos DigiF de banda estrecha y banda ancha que utilizan satélites de transmisión pública. Estas plantillas le permiten empezar a utilizarlas fácilmente. AWS Ground Station Para obtener más información AWS CloudFormation, consulte ¿Qué es AWS CloudFormation?

Según el tipo de contacto que desees contratar, elige el tipo de plantilla CFN adecuado de la siguiente lista:

- Plantillas de entrega de datos S3 de banda estrecha AWS CloudFormation.
- Plantillas de entrega de datos DigIf S3 de banda ancha AWS CloudFormation.

Si no quiere utilizar una de las AWS CloudFormation plantillas prediseñadas, puede ver las instrucciones enCreación de una plantilla propia.

Plantillas de entrega de datos S3 de banda estrecha AWS CloudFormation

Plantillas prediseñadas

En la actualidad puede configurar varias transmisiones de datos por contacto para que fluyan hacia el bucket de S3. Estas secuencias de datos están disponibles en dos formatos diferentes. Las secuencias de datos que contienen datos de VITA-49 Signal/IP se pueden configurar para señales de banda S y banda X de hasta 54 MHz de ancho de banda. Los datos/IP de extensión VITA-49 se pueden configurar para señales de banda X desmoduladas y/o descodificadas de hasta 500 MHz de ancho de banda.

AWS Ground Station proporciona plantillas para ambos formatos de flujo de datos que muestran cómo utilizar el servicio. Utilice esta guía para encontrar la plantilla adecuada para usted.

Plantillas disponibles

Puede utilizar una plantilla preconfigurada para recibir datos de transmisión directa de los satélites Aqua, SNPP, JPSS-1/NOAA-20 y Terra. Estas AWS CloudFormationplantillas contienen los recursos

necesarios AWS Ground Station y los de Amazon S3 para programar y ejecutar los contactos y recibir los datos en un bucket de Amazon S3 de su cuenta. Si no se incorporan satélites Aqua, SNPP, JPSS-1/NOAA-20 y Terra en la cuenta, consulte Incorporación de clientes.

Plantillas de entrega de datos de banda estrecha

Si utiliza la entrega de datos de banda estrecha para su contacto, utilice las AWS CloudFormation plantillas que aparecen a continuación.

- La AWS CloudFormation plantilla denominada `AquaSnppJpss-1DemodDecodeS3DataDelivery.yml` contiene un bucket de Amazon S3 y los AWS Ground Station recursos necesarios para programar contactos y recibir datos de transmisión directa desmodulados y decodificados. Esta plantilla es un buen punto de partida si tiene previsto procesar los datos utilizando el software Direct Readout Labs (RT-STPS e IPOPP) de la NASA.

  Para descargar la plantilla mediante AWS CLI, utilice el siguiente comando:

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

  La plantilla puede verse y descargarse en la consola desde la siguiente URL en su navegador:

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

  Puede especificar la plantilla directamente en AWS CloudFormation el siguiente enlace:

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

- La AWS CloudFormation plantilla denominada `AquaSnppJpss-1TerraDigIfS3DataDelivery.yml` contiene un bucket de Amazon S3 y los AWS Ground Station recursos necesarios para programar contactos y recibir datos de transmisión directa de señal o IP del VITA-49. Esta plantilla es un buen punto de partida si planea procesar los datos con una radio definida por software (SDR) para demodular y decodificar los datos antes del posprocesamiento.

  Para descargar la plantilla mediante AWS CLI, utilice el siguiente comando:

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

La plantilla puede verse y descargarse en la consola desde la siguiente URL en su navegador:

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

Puede especificar la plantilla directamente en AWS CloudFormation el siguiente enlace:

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

¿Qué recursos define la plantilla?

Ambas plantillas contienen los mismos recursos, con la única diferencia de que están configuradas las antenas. Para obtener más información, consulte la columna Antenna Config.

- Bucket de Amazon S3: el bucket al que se entregarán los datos del enlace descendente. El nombre de este bucket comienza por `aws-groundstation` para cumplir los criterios descritos en S3 Recording Config.
- Función de IAM: función que asume el director del `groundstation.amazonaws.com` servicio y que AWS Ground Station asume al escribir los datos enlazados descendentes en su bucket de Amazon S3.
- Política de bucket de Amazon S3: política que permite al rol de IAM realizar las siguientes acciones en el bucket de Amazon S3 y sus objetos:
  - `s3:GetBucketLocation`
  - `s3:PutObject`
- Config de rastreo: una configuración AWS Ground Station de rastreo que define cómo el sistema de antenas rastrea el satélite a medida que se mueve por el cielo.
- Config de grabación de AWS Ground Station S3: una configuración de grabación de S3 que hace referencia al bucket de Amazon S3 y a la función de IAM AWS Ground Station para utilizarla al entregar los datos.
- Config de AWS Ground Station antena: configuración de antena que especifica cómo configurar la AWS Ground Station antena durante un contacto. La

`AquaSnppJpss-1DemodDecodeS3DataDelivery.yml` plantilla contiene una configuración de decodificación de demodo de enlace descendente de antena que configura la AWS Ground Station antena para demodular y decodificar los datos de enlace descendente antes de enviarlos a su bucket de Amazon S3. `AquaSnppJpss-1TerraDigIfS3DataDelivery.yml`En cambio, contiene una configuración de enlace descendente de antena que configura la AWS Ground Station antena para entregar los datos a su Amazon S3 como paquetes de señal/IP del VITA-49.

- Perfil de misión: un perfil de AWS Ground Station misión que agrupa todas las AWS Ground Station configuraciones para permitirle programar y ejecutar contactos utilizando las configuraciones a las que se hace referencia.

Plantillas de entrega de datos DigIf S3 de banda ancha AWS CloudFormation

Plantillas de entrega de datos DigiF de banda ancha

Si utiliza la entrega de datos de frecuencia intermedia digital de banda ancha (DigiF) para su contacto, utilice las plantillas que aparecen a continuación. AWS CloudFormation

- La AWS CloudFormation plantilla denominada `DirectBroadcastSatelliteWbDigIfS3DataDelivery.yml` contiene un bucket de Amazon S3 y los AWS Ground Station recursos necesarios para programar contactos y recibir datos de transmisión directa de señal o IP del VITA-49 a través del agente. AWS Ground Station Esta plantilla es un buen punto de partida si planea procesar los datos con una radio definida por software (SDR) para demodular y decodificar los datos antes del posprocesamiento. Para obtener más información sobre el agente, consulte. AWS Ground Station AWS Ground Station Guía del usuario del agente

  Para descargar la plantilla mediante AWS CLI, utilice el siguiente comando:

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

  La plantilla puede verse y descargarse en la consola desde la siguiente URL en su navegador:

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

Puede especificar la plantilla directamente en AWS CloudFormation el siguiente enlace:

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

¿Qué recursos define la plantilla?

- Bucket de Amazon S3: el bucket al que se entregarán los datos del enlace descendente. El nombre de este bucket comienza por `aws-groundstation` para cumplir los criterios descritos en S3 Recording Config.
- Función de IAM: función que asume el director del `groundstation.amazonaws.com` servicio y que AWS Ground Station asume al escribir los datos enlazados descendentes en su bucket de Amazon S3.
- Política de bucket de Amazon S3: política que permite al rol de IAM realizar las siguientes acciones en el bucket de Amazon S3 y sus objetos:
  - `s3:GetBucketLocation`
  - `s3:PutObject`
- AWS KMS Clave: clave que se utiliza AWS KMS para cifrar los flujos de datos.
- Función clave de Ground Station: la función de IAM que AWS Ground Station asumirá para acceder y utilizar la AWS KMS clave para descifrar los flujos de datos
- Política de acceso a la clave de Ground Station: la política de IAM que define las acciones que AWS Ground Station se pueden realizar con la clave de entrega de datos
- Config de rastreo: una configuración AWS Ground Station de rastreo que define cómo el sistema de antenas rastrea el satélite a medida que se mueve por el cielo.
- Config de grabación de AWS Ground Station S3: una configuración de grabación de S3 que hace referencia al bucket de Amazon S3 y a la función de IAM AWS Ground Station para utilizarla al entregar los datos.
- Configuraciones de antena para Aqua, SNPP, JPSS-1/NOAA-20 y Terra: tres configuraciones de AWS Ground Station antena independientes que especifican cómo configurar la AWS Ground Station antena durante un contacto con Aqua, SNPP, JPSS-1/NOAA-20 y Terra. La plantilla contiene una configuración de enlace descendente de antena que configura la AWS Ground Station antena para entregar los datos a su Amazon S3 como paquetes de señal/IP del VITA-49.

- Perfiles de misión para Aqua, SNPP, JPSS-1/NOAA-20 y Terra: tres perfiles de AWS Ground Station misión independientes que agrupan todas las configuraciones para permitirle programar y ejecutar contactos utilizando las AWS Ground Station configuraciones a las que se hace referencia en Aqua, SNPP, JPSS-1/NOAA-20 y Terra.

Creación de una plantilla propia

Para configurar los recursos para programar y ejecutar los contactos de sus propios satélites, debe configurar los recursos de la cuenta para que coincidan con los ajustes del satélite. AWS Ground Station Esto es difícil de hacer por su cuenta. El AWS Ground Station equipo está disponible para ayudarte a configurar los AWS Ground Station recursos de tu cuenta para que se conecten a tu satélite desde y hacia arriba. Para configurar su propio satélite para usarlo AWS Ground Station, póngase en contacto con AWS Support.

Paso 2: Configurar una AWS CloudFormation pila

Tras elegir la plantilla que mejor se adapte a su caso de uso, configure una AWS CloudFormation pila. Los recursos que se crean en este procedimiento se configuran en la región en la que se encuentra al crearlos.

1. En AWS Management Console, elija Servicios > CloudFormation.
2. En el panel de navegación, seleccione Stacks (Pilas). Elija Create stack (Crear pila) > With new resources (standard) (Con nuevos recursos [estándar]).
3. En la página Create Stack (Crear pila), especifique la plantilla que ha seleccionado en the section called “Paso 1: Elige una AWS CloudFormation plantilla” mediante una de las siguientes acciones.

    a. Seleccione la URL de Amazon S3 como el origen de plantilla y copie y pegue la URL de la plantilla que desea utilizar en URL de Amazon S3. A continuación, elija Siguiente.

    b. Seleccione Upload a template file (Cargar un archivo de plantilla) como el origen de plantilla y elija Choose File (Seleccionar archivo). Cargue la plantilla que ha descargado en the section called “Paso 1: Elige una AWS CloudFormation plantilla”. A continuación, elija Siguiente.
4. Realice los siguientes pasos en la página Specify stack details:

    a. Introduzca un nombre en la casilla Stack Name (Nombre de pila). Recomendamos utilizar un nombre sencillo para reducir las posibilidades de que se produzcan errores en el futuro.

b. Elija Siguiente.

5. Configure las opciones de pila y las opciones avanzadas de la instancia de Amazon EC2.

   a. Añada cualquier etiqueta y permiso en las secciones Tags (Etiquetas) y Permissions (Permisos).

   b. Realice cualquier cambio en la Stack policy (Política de pila), la Rollback configuration (Configuración de reversión), las Notification options (Opciones de notificación) y las Stack creation options (Opciones de creación de pilas).

   c. Elija Siguiente.

6. Después de revisar los detalles de la pila, seleccione el reconocimiento Capabilities (Capacidades) y seleccione Create stack (Crear pila).

AWS Ground Station Guía del usuario del agente

Temas

Información general

¿Qué es el AWS Ground Station agente?

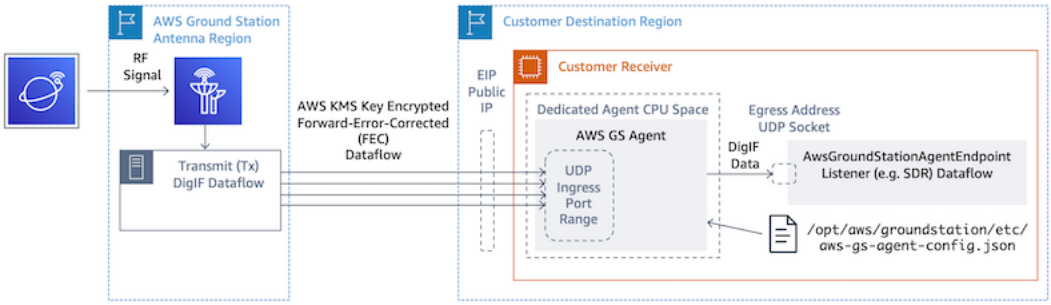
El AWS Ground Station Agent, disponible como RPM, permite a AWS Ground Station los clientes recibir (enlace descendente) flujos de datos síncronos de frecuencia intermedia digital de banda ancha (DigiF) durante los contactos con AWS Ground Station. Los clientes pueden seleccionar dos opciones para la entrega de datos:

1. Entrega de datos a una instancia EC2: entrega de datos a una instancia EC2 propiedad del cliente. AWS Ground Station los clientes administran el agente AWS Ground Station . Esta opción puede ser la más adecuada si necesita un procesamiento de datos casi en tiempo real. Consulte la guía de Envío de datos a Amazon EC2 para obtener información sobre el envío de datos a EC2.

2. Entrega de datos a un bucket de S3: entrega de datos a un bucket de AWS S3 propiedad del cliente a través de un servicio gestionado de Ground Station. Consulte la guía de Cómo empezar con AWS Ground Station para obtener información sobre el envío de datos a S3.

Ambos modos de entrega de datos requieren que los clientes creen un conjunto de recursos de AWS. Se recomienda encarecidamente el uso de CloudFormation plantillas para crear los recursos de AWS a fin de garantizar la fiabilidad, la precisión y la compatibilidad. Cada contacto solo puede entregar datos a EC2 o S3, pero no a ambos simultáneamente.

> **Note**
>
> Dado que la entrega de datos de S3 es un servicio gestionado por Ground Station, esta guía se centra en la entrega de datos a sus instancias EC2.



Flujo de datos DigiF desde una región de AWS Ground Station antena a su instancia EC2 con su radio definida por software (SDR) o un oyente similar.

Características del AWS Ground Station agente

El AWS Ground Station agente recibe datos de enlace descendente de frecuencia intermedia digital (DigiF) y saca los datos descifrados que permiten lo siguiente:

- Capacidad de enlace descendente DigiF de 40 MHz a 400 MHz de ancho de banda.
- Entrega de datos DigiF a alta velocidad y baja fluctuación a cualquier IP pública (AWS Elastic IP) de la red de AWS.
- Entrega de datos fiable mediante la corrección de errores de reenvío (FEC).
- Entrega segura de datos mediante una clave de cifrado gestionada AWS KMS por el cliente.

Requisitos del agente

> **Note**
>
> Esta guía para AWS Ground Station agentes asume que se ha incorporado a Ground Station utilizando la Configuración AWS Ground Station guía.

La instancia EC2 de AWS Ground Station Agent Receiver requiere un conjunto de recursos de AWS dependientes para entregar los datos de DigiF de forma fiable y segura a sus puntos de conexión.

1. Una VPC para lanzar el receptor de EC2.
2. Una clave de AWS KMS para el cifrado y descifrado de datos.
3. Una clave SSH o un perfil de instancia EC2 configurado para el administrador de sesiones SSM.
4. Reglas de red/grupo de seguridad que permiten lo siguiente:
    1. Tráfico UDP procedente de los puertos especificados AWS Ground Station en el grupo de puntos de conexión de su flujo de datos. El agente reserva un rango de puertos contiguos que se utilizan para entregar datos a los puntos de conexión del flujo de datos de entrada.
    2. Acceso SSH a su instancia (Nota: también puede utilizar AWS Session Manager para acceder a su instancia EC2).
    3. Acceso de lectura a un bucket de S3 de acceso público para la administración de agentes.
    4. El tráfico SSL en el puerto 443 permite al agente comunicarse con el AWS Ground Station servicio.
    5. Tráfico de la lista `com.amazonaws.global.groundstation` de prefijos AWS Ground Station gestionada.

Además, se requiere una configuración de la VPC que incluya una subred pública. Consulte la Guía del usuario de la VPC para obtener información sobre la configuración de subredes.

Configuraciones compatibles:

1. Una IP elástica asociada a su instancia EC2 en una subred pública.
2. Una IP elástica asociada a un ENI en una subred pública, conectada a su instancia EC2 (en cualquier subred).

Puede utilizar el mismo grupo de seguridad que su instancia EC2 o especificar uno con, al menos, el conjunto mínimo de reglas compuesto por:

- Tráfico UDP procedente de los puertos especificados AWS Ground Station en el grupo de puntos finales del flujo de datos.

Consulte la sección «Plantillas de entrega de datos DigiF de banda ancha» de, Elija una plantilla por ejemplo, las plantillas de entrega de datos de AWS CloudFormation EC2 con estos recursos preconfigurados.

Diagramas de una VPC

Diagrama: una IP elástica asociada a su instancia EC2 en una subred pública

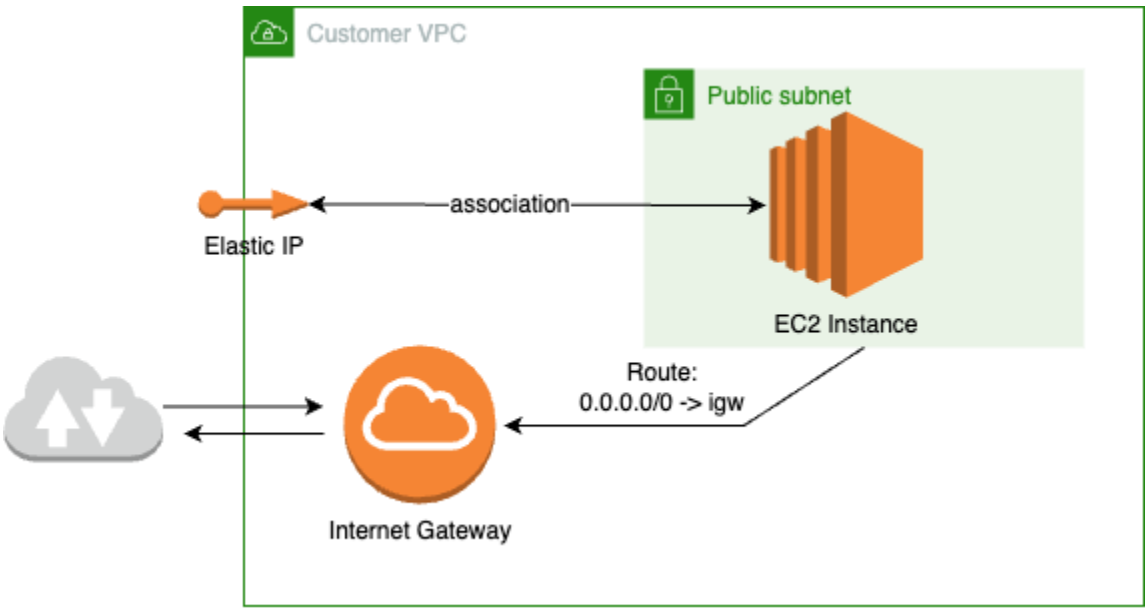
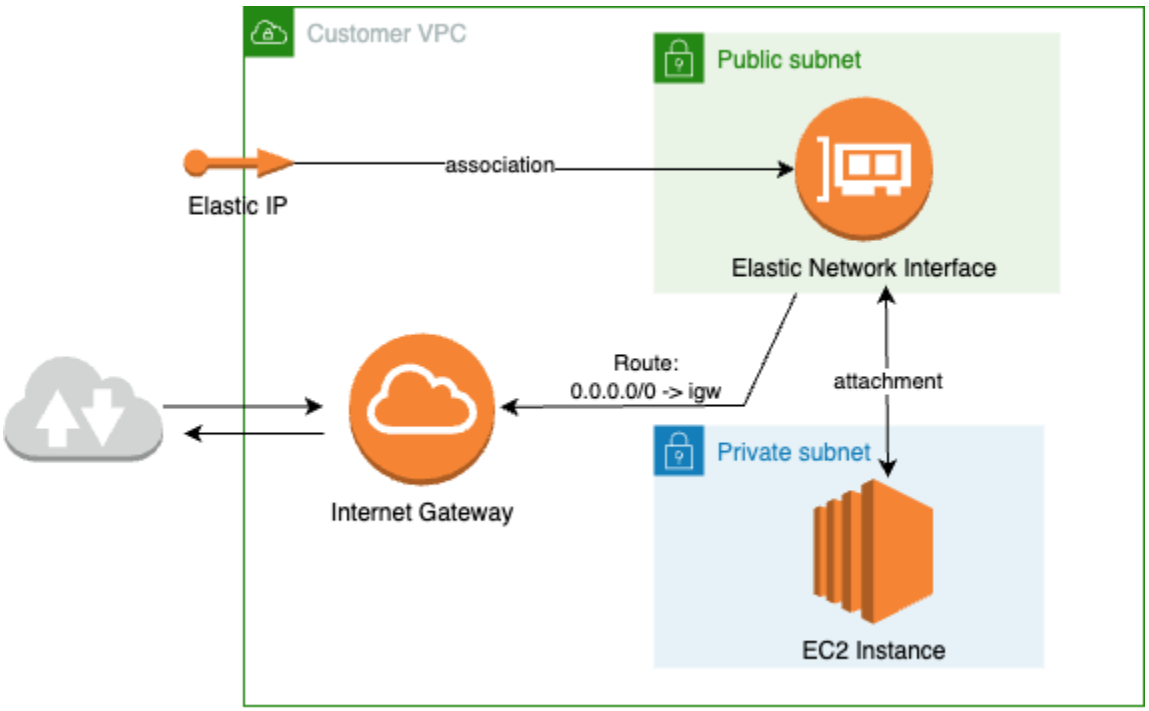


Diagrama: una IP elástica asociada a un ENI en una subred pública, conectada a su instancia EC2 en una subred privada



Sistemas operativos compatible

Amazon Linux 2 con kernel 4.14.186

Los tipos de instancias compatibles se enumeran en Selección de instancias EC2 y planificación de la CPU

Entrega de datos mediante AWS Ground Station un agente

Los siguientes diagramas proporcionan una descripción general de cómo fluyen los datos AWS Ground Station durante los contactos de frecuencia intermedia digital de banda ancha (DigiF).

El AWS Ground Station agente se encargará de organizar los componentes del plano de datos de un contacto. Antes de programar un contacto, el agente debe estar correctamente configurado, iniciado y registrado (el registro es automático al iniciar el agente) en él. AWS Ground Station Además, el software de recepción de datos (como una radio definida por software) debe estar funcionando y configurado para recibir datos en la dirección de AwsGroundStationAgentEndpointsalida.

Entre bastidores, el AWS Ground Station agente recibirá tareas desde el AWS KMS cifrado aplicado en tránsito AWS Ground Station y lo deshará antes de reenviarlo a la dirección de salida del terminal de destino, donde escucha la radio definida por software (SDR). El AWS Ground Station agente

y sus componentes subyacentes respetarán los límites de CPU establecidos en el archivo de configuración para garantizar que esto no afecte al rendimiento de otras aplicaciones que se ejecuten en la instancia.

Los clientes deben tener el AWS Ground Station agente ejecutándose en la instancia receptora implicada en el contacto. Un solo AWS Ground Station agente puede organizar varios flujos de datos, como se indica a continuación, si el cliente prefiere recibir todos los flujos de datos en una sola instancia receptora.

Varios flujos de datos, un solo receptor

Escenario de ejemplo:

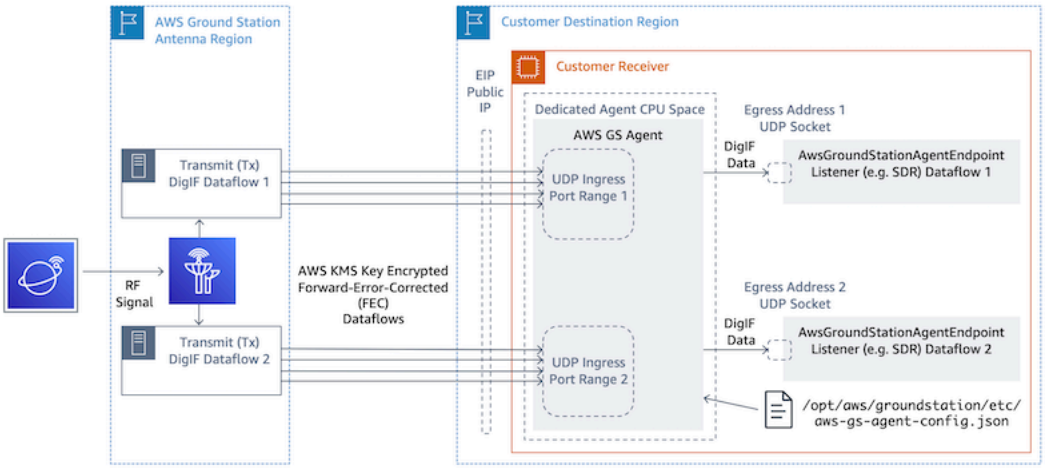
El cliente quiere recibir dos enlaces descendentes de antena como flujos de datos DigIF en la misma instancia de receptor EC2. Los dos enlaces descendentes serán de 200 MHz y 100 MHz.

AwsGroundStationAgentEndpoints:

Habrá dos recursos de `AwsGroundStationAgentEndpoint`, uno para cada flujo de datos. Ambos puntos de conexión tendrán la misma dirección IP pública (`ingressAddress.socketAddress.name`). Los `portRange` de entrada no deben solaparse, ya que los flujos de datos se reciben en la misma instancia EC2. Ambos `egressAddress.socketAddress.port` deben ser únicos.

Planificación de la CPU:

- 1 núcleo (2 vCPU) para ejecutar el único AWS Ground Station agente en la instancia.
- 6 núcleos (12 vCPU) para recibir DigiF Dataflow 1 (búsqueda de 200 MHz en la tabla). Planificación del núcleo de CPU
- 4 núcleos (8 vCPU) para recibir DigiF Dataflow 2 (búsqueda de 100 MHz en la tabla). Planificación del núcleo de CPU
- Espacio total de CPU del agente dedicado = 11 núcleos (22 vCPU) en el mismo socket.



Múltiples flujos de datos, múltiples receptores

Escenario de ejemplo:

El cliente quiere recibir dos enlaces descendentes de antena como flujos de datos DigIF en la misma instancia de receptor EC2. Ambos enlaces descendentes serán de 400 MHz.

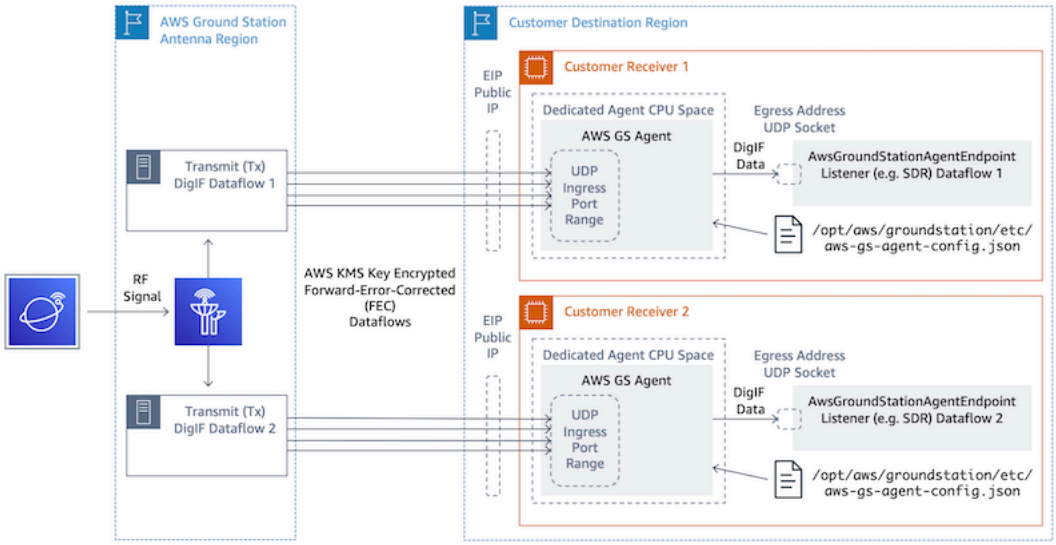
AwsGroundStationAgentEndpoints:

Habrá dos recursos de `AwsGroundStationAgentEndpoint` recursos, uno para cada flujo de datos. Ambos puntos de conexión tendrán la misma dirección IP pública (`ingressAddress.socketAddress.name`). No hay restricciones en los valores de los puertos para `ingressAddress` y `egressAddress`, ya que los flujos de datos se reciben en infraestructuras separadas y no entrarán en conflicto entre sí.

Planificación de la CPU:

- Instancia de receptor 1
  - 1 núcleo (2 vCPU) para ejecutar el único AWS Ground Station agente en la instancia.
  - 9 núcleos (18 vCPU) para recibir DigiF Dataflow 1 (consulta a 400 MHz en la tabla). Planificación del núcleo de CPU
  - Espacio total de CPU del agente dedicado = 10 núcleos (20 vCPU) en el mismo socket.
- Instancia de receptor 2
  - 1 núcleo (2 vCPU) para ejecutar el único AWS Ground Station agente en la instancia.
  - 9 núcleos (18 vCPU) para recibir DigiF Dataflow 2 (consulta a 400 MHz en la tabla). Planificación del núcleo de CPU

- Espacio total de CPU del agente dedicado = 10 núcleos (20 vCPU) en el mismo socket.



Selección de instancias EC2 y planificación de la CPU

Tipos de instancias admitidas

El AWS Ground Station agente requiere núcleos de CPU dedicados para funcionar debido a los flujos de trabajo de entrega de datos que requieren un uso intensivo de cómputo. Admitimos los siguientes tipos de instancias. Consulte Planificación del núcleo de CPU para decidir qué tipo de instancia se adapta mejor a su caso de uso.

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados
c5.12xlarge	48	24
c5.18xlarge	72	36
c5.24xlarge	96	48
c5n.18xlarge	72	36
c5n.metal	72	36

Tipo de instancia	vCPU predeterminadas	Núcleos de CPU predeterminados
c6i.32xlarge	128	64
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

Planificación del núcleo de CPU

El AWS Ground Station agente requiere núcleos de procesador dedicados que compartan la caché L3 para cada flujo de datos. El agente está diseñado para aprovechar los pares de CPU Hyper-Threading (HT) y requiere que los pares HT estén reservados para su uso. Un par hiperproceso es un par de CPU virtuales (vCPU) que se encuentran dentro de un único núcleo. La siguiente tabla proporciona un mapeo de la velocidad de datos del flujo de datos al número requerido de núcleos

reservados para el agente en un solo flujo de datos. En esta tabla se presupone que Cascade Lake o CPUs más recientes es válida para cualquier tipo de instancia compatible. Si tu ancho de banda se encuentra entre las entradas de la tabla, selecciona la siguiente más alta.

El agente necesita un núcleo reservado adicional para la administración y la coordinación, por lo que el total de núcleos necesarios será la suma de los núcleos necesarios (según el gráfico siguiente) para cada flujo de datos más un núcleo adicional (2 vCPU).

AntennaDownlink Ancho de banda (MHz)	Velocidad de datos DigiF prevista para el VITA-49.2 (MB/s)	Número de núcleos (pares de CPU HT)	vCPU total
50	1 000	3	6
100	2000	4	8
150	3 000	5	10
200	4000	6	12
250	5000	6	12
300	6000	7	14
350	7000	8	16
400	8000	9	18

Recopilación de información sobre la arquitectura

`lscpu`proporciona información sobre la arquitectura del sistema. El resultado básico muestra qué VCPU (denominadas «CPU») pertenecen a qué nodos NUMA (y cada nodo NUMA comparte una caché L3). A continuación, examinamos una `c5.24xlarge` instancia para recopilar la información necesaria para configurar el agente. AWS Ground Station Esto incluye información útil como el número de vCPU, los núcleos y la asociación de vCPU a nodo.

```
> 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    <------
```

Los núcleos dedicados al AWS Ground Station agente deben incluir las dos vCPU para cada núcleo asignado. Todos los núcleos de un flujo de datos deben estar en el mismo nodo NUMA. La `-p` opción del `lscpu` comando nos proporciona las asociaciones entre el núcleo y la CPU necesarias para configurar el agente. Los campos relevantes son CPU (que es lo que denominamos vCPU), Core y L3 (que indica qué caché L3 comparte ese núcleo). Tenga en cuenta que en la mayoría de los procesadores Intel, el nodo NUMA es igual a la caché L3.

Considere el siguiente subconjunto de la `lscpu -p` salida `c5.24xlarge` (abreviado y formateado para mayor claridad).

```
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
```

En el resultado, podemos ver que Core 0 incluye las vCPU 0 y 16, el Core 1 incluye las vCPU 1 y 17, y el Core 2 incluye las vCPU 2 y 18. En otras palabras, los pares de hiperprocesos son: 0 y 16, 1 y 17, 2 y 18.

Ejemplo de asignación de CPU

Como ejemplo, utilizaremos una `c5.24xlarge` instancia para un enlace descendente de banda ancha de doble polaridad a 350 MHz. De la tabla anterior, Planificación del núcleo de CPU sabemos que un enlace descendente de 350 MHz requiere 8 núcleos (16 VCPU) para el flujo de datos único. Esto significa que esta configuración de doble polaridad que utiliza dos flujos de datos requiere un total de 16 núcleos (32 vCPU) más un núcleo (2 vCPU) para el agente.

Sabemos que el resultado de incluye y. `lscpu` `c5.24xlarge` `NUMA node0 CPU(s): 0-23,48-71` `NUMA node1 CPU(s): 24-47,72-95` Como NUMA node0 tiene más de lo que necesitamos, solo asignaremos desde los núcleos: 0-23 y 48-71.

En primer lugar, seleccionaremos 8 núcleos para cada flujo de datos que compartan una caché L3 o un nodo NUMA. A continuación, buscaremos las vCPU correspondientes (denominadas «CPU») en `lscpu -p` la entrada de salida. Apéndice: `lscpu -p` salida (completa) para c5.24xlarge Un ejemplo de proceso de selección de núcleos podría tener el siguiente aspecto:

- Reserve los núcleos 0-1 para el sistema operativo.
- Flujo 1: seleccione los núcleos 2-9 que se asignen a las vCPU 2-9 y 50-57.
- Flujo 2: seleccione los núcleos 10-17 que se asignen a las vCPU 10-17 y 58-65.
- Núcleo del agente: seleccione el núcleo 18 que se asigna a las vCPU 18 y 66.

Esto da como resultado vCPU 2-18 y 51-66, por lo que la lista para proporcionar el agente es. `[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]` Debe asegurarse de que sus propios procesos no se ejecuten en estas CPU, tal y como se describe en. Ejecución de servicios y procesos junto con el agente AWS Ground Station

Tenga en cuenta que los núcleos específicos seleccionados en este ejemplo son algo arbitrarios. Otros conjuntos de núcleos funcionarían siempre que satisfagan el requisito de compartir todos una caché L3 para cada flujo de datos.

Apéndice: **`lscpu -p`** salida (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
```

Instalación del agente

El AWS Ground Station agente se puede instalar de las siguientes maneras:

1. AWS CloudFormation plantilla (recomendada).
2. Instalación manual en Amazon EC2.

Uso de CloudFormation la plantilla

La CloudFormation plantilla de entrega de datos de EC2 crea los recursos de AWS necesarios para entregar datos a su instancia de EC2. Esta AWS CloudFormation plantilla utiliza la AMI AWS Ground Station gestionada que tiene el AWS Ground Station agente preinstalado. A continuación, el script de arranque de la instancia EC2 creada rellena el archivo de configuración del agente y aplica los ajustes de rendimiento necesarios (Ajuste del rendimiento de la instancia EC2).

Paso 2: crear los recursos de AWS

Cree su pila de recursos de AWS mediante una plantilla de Plantilla DigiF de banda ancha por satélite de transmisión directa (banda ancha).

Paso 2: verificación del estado del agente

De forma predeterminada, el agente está configurado y activo (iniciado). Para comprobar el estado del agente, puede conectarse a la instancia EC2 (SSH o SSM Session Manager) y consultar AWS Ground Station Estado del agente.

Instalación manual en EC2

Si bien Ground Station recomienda usar CloudFormation plantillas para aprovisionar sus recursos de AWS, puede haber casos de uso en los que la plantilla estándar no sea suficiente. En estos casos, le recomendamos que personalice la plantilla para adaptarla a sus necesidades. Si eso sigue sin cumplir sus requisitos, puede crear manualmente sus recursos de AWS e instalar el agente.

Paso 2: crear los recursos de AWS

Consulte Creación y configuración de recursos manualmente para saber cómo configurar manualmente los recursos de AWS necesarios para un contacto.

El AwsGroundStationAgentEndpointrecurso define un punto final para recibir un flujo de datos DigiF a través del AWS Ground Station agente y es fundamental para establecer un contacto exitoso. Si bien la documentación de la API se encuentra en la referencia de la API, en esta sección se analizarán brevemente los conceptos relevantes para el agente. AWS Ground Station

El punto final `ingressAddress` es donde el AWS Ground Station agente recibirá el tráfico UDP AWS KMS cifrado de la antena. `socketAddress name` es la IP pública de la instancia EC2 (de la EIP adjunta). `portRange` debe tener al menos 300 puertos contiguos en un rango que se haya reservado para cualquier otro uso. Para obtener instrucciones, consulte Reserve los puertos de entrada: impacta en la red. Estos puertos deben configurarse para permitir el tráfico de entrada UDP en el grupo de seguridad de la VPC en la que se ejecuta la instancia receptora.

El `egressAddress` del punto de conexión es donde el agente entregará el flujo de datos DigiF al cliente. El cliente debe tener una aplicación (por ejemplo, SDR) que reciba los datos a través de un conector UDP en esta ubicación.

Paso 2: crear una instancia EC2

Las AMI que se admiten son las siguientes:

1. AWS Ground Station La AMI (`groundstation-al2-gs-agent-ami-*`donde * es la fecha en que se creó la AMI) viene con el agente instalado (recomendado).
2. `amzn2-ami-kernel-5.10-hvm-x86_64-gp2`.

Paso 2: descargar e instalar el agente

> **Note**
>
> Los pasos de esta sección deben completarse si no eligió la AMI del AWS Ground Station agente en el paso anterior.

Descargar el agente

El AWS Ground Station agente está disponible en buckets de S3 específicos de la región y se puede descargar para admitir instancias EC2 mediante la línea de comandos (CLI) de AWS, desde `s3://groundstation-wb-digif-software-${AWS::Region}/aws-groundstation-agent/latest/amazon_linux_2_x86_64/aws-groundstation-agent.rpm` donde $ {AWS::Region} hace referencia a una de las regiones de entrega de datos y consola de AWS Ground Station compatibles.

Ejemplo: descargue la versión rpm más reciente de la región us-east-2 de AWS de forma local a la carpeta /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
```

Si necesita descargar una versión específica del AWS Ground Station agente, puede descargarla desde la carpeta específica de la versión en el depósito de S3.

Ejemplo: descargue la versión 1.0.2716.0 de RPM de la región us-east-2 de AWS de forma local a la carpeta /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**
>
> Si quiere confirmar que se vendió el RPM que descargó AWS Ground Station, siga las instrucciones correspondientesValidación de la instalación de RPM.

Instalar el agente

```
sudo yum install ${MY_RPM_FILE_PATH}

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

Paso 4: configurar el agente

Tras instalar el agente, debe actualizar el archivo de configuración del agente. Consulte Configuración del agente.

Paso 5: aplicar ajustes de rendimiento

AWS Ground Station AMI de agente: si eligió la AMI de AWS Ground Station agente en el paso anterior, aplique los siguientes ajustes de rendimiento.

- Ajusta las interrupciones del hardware y las colas de recepción, lo que afecta a la CPU y a la red
- Reserve los puertos de entrada: impacta en la red
- Reboot

Otras AMI: si eligió cualquier otra AMI en el paso anterior, aplique todos los ajustes enumerados en Ajuste del rendimiento de la instancia EC2 y reinicie la instancia.

Paso 6: administrar el agente

Para iniciar, detener y comprobar el estado del agente, consulteAdministrar el agente.

Administrar el agente

AWS Ground Station El agente proporciona las siguientes funciones para configurar, iniciar, detener, actualizar, degradar y desinstalar el agente mediante las herramientas de comandos integradas en Linux.

Temas

- AWS Ground Station Configuración del agente
- AWS Ground Station Inicio del agente
- AWS Ground Station Agente: ¡Stop
- AWS Ground Station Actualización del agente
- AWS Ground Station Bajar de categoría de agente
- AWS Ground Station Desinstalación del agente
- AWS Ground Station Estado del agente
- AWS Ground Station Información sobre RPM del agente

AWS Ground Station Configuración del agente

Navegue hasta`/opt/aws/groundstation/etc`, que debe contener un único archivo denominado aws-gs-agent-config .json. Consulte Archivo de configuración del agente

AWS Ground Station Inicio del agente

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

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

Debería producir un resultado que muestre que el agente está activo.

```
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
```

Debería producir un resultado que muestre que el agente está inactivo (detenido).

```
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 Actualización del agente

1. Descargue la versión más reciente del agente. Consulte Descargar el agente.
2. Detenga el agente de .

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

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

3. Actualización del agente

```
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 Bajar de categoría de agente

1. Descarga la versión de agente que necesites. Consulte Descargar el agente.
2. Descargue el agente.

```
# 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 Desinstalación del agente

Al desinstalar el agente, se cambiará el nombre de /opt/aws/groundstation/etc/ .json a /opt/aws/groundstation/etc/ .json.rpmsaveaws-gs-agent-config. aws-gs-agent-config Si se vuelve a instalar el agente en la misma instancia, se escribirán los valores predeterminados para aws-gs-agent-config .json y será necesario actualizarlos con los valores correctos correspondientes a sus recursos de AWS. Consulte Archivo de configuración del agente.

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

AWS Ground Station Estado del agente

El estado del agente es activo (el agente está en ejecución) o inactivo (el agente está detenido).

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

Un ejemplo de resultado muestra que el agente está instalado, en estado inactivo (detenido) y activado (inicia el servicio al arrancar).

```
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 Información sobre RPM del agente

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

La salida es la siguiente:

> **Note**
>
> La versión puede variar según la última versión publicada por el agente.

```
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
```

Configuración del agente

Tras instalar el agente, debe actualizar el archivo de configuración del agente en `/opt/aws/groundstation/etc/aws-gs-agent-config.json`.

Archivo de configuración del agente

Ejemplo

```
{
  "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
}
```

Desglose de campos

capacidades

Las capacidades se especifican como nombres de recursos de Amazon de Dataflow Endpoint Group.

Obligatorio: true

Formato: matriz de cadenas

- Valores: capacidad ARN → Cadena

Ejemplos:

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

dispositivo

Este campo contiene los campos adicionales necesarios para enumerar el dispositivo EC2 actual.

Obligatorio: true

Formato: objeto

Miembros:

- privateIps
- publicIps
- agentCpuCores
- networkAdapters

privateIps

Este campo no se utiliza actualmente, pero se incluye para futuros casos de uso. Si no se incluye ningún valor, el valor predeterminado será [«127.0.0.1»]

Obligatorio: false

Formato: matriz de cadenas

- Valores: Direcciones IP → Cadena

Ejemplo:

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

publicIps

IP elástica (EIP) para cada grupo de puntos de conexión de flujo de datos.

Obligatorio: true

Formato: matriz de cadenas

- Valores: Direcciones IP → Cadena

Ejemplo:

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

agentCpuCores

Esto especifica qué núcleos virtuales están reservados para el aws-gs-agent proceso. Consulte Planificación del núcleo de CPU para conocer los requisitos para establecer este valor de forma adecuada.

Obligatorio: true

Formato: matriz int

- Valores: Números básicos → int

Ejemplo:

```
"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

Esto corresponde a los adaptadores de Ethernet, o interfaces conectadas a los ENI, que recibirán los datos.

Obligatorio: false

Formato: matriz de cadenas

- Valores: nombres de adaptadores de Ethernet (puede encontrarlos ejecutando `ifconfig`)

Ejemplo:

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

Ajuste del rendimiento de la instancia EC2

> **Note**
>
> Si aprovisionó sus recursos de AWS mediante CloudFormation plantillas, estos ajustes se aplican automáticamente. Si utilizó una AMI o creó manualmente la instancia EC2, debe aplicar estos ajustes de rendimiento para lograr el rendimiento más fiable.

Recuerde reiniciar la instancia después de aplicar cualquier ajuste.

Temas

- Ajusta las interrupciones del hardware y las colas de recepción, lo que afecta a la CPU y a la red
- La fusión de interrupciones de Tune Rx afecta a la red
- Tune Rx Ring Buffer: afecta a la red
- Ajustar el estado C de la CPU: afecta a la CPU
- Reserve los puertos de entrada: impacta en la red
- Reboot

Ajusta las interrupciones del hardware y las colas de recepción, lo que afecta a la CPU y a la red

En esta sección, se configura el uso del núcleo de la CPU de systemd, SMP IRQ, Receive Packet Steering (RPS) y Receive Flow Steering (RFS). Consulte Apéndice: Parámetros recomendados para Interrupt/RPS Tune para ver el conjunto de ajustes recomendados en función del tipo de instancia que utilice.

1. Aleja los procesos de systemd de los núcleos de CPU de los agentes.
2. Redirija las solicitudes de interrupción de hardware lejos de los núcleos de la CPU de los agentes.
3. Configure el RPS para evitar que la cola de hardware de una sola tarjeta de interfaz de red se convierta en un cuello de botella en el tráfico de la red.
4. Configure RFS para aumentar la tasa de aciertos de la memoria caché de la CPU y reducir así la latencia de la red.

El script de `set_irq_affinity.sh` proporcionado por el RPM configura todas las opciones anteriores automáticamente. Añádelo a crontab para que se aplique en cada arranque:

```
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`Sustitúyalos por núcleos reservados para el núcleo y el sistema operativo; normalmente, el primero y el segundo junto con los pares de núcleos con subprocesos múltiples. Esto no debe superponerse con los núcleos seleccionados anteriormente. (Por ejemplo, «0,1,48,49» para una instancia de 96 CPU con hipersubprocesos).
- `rps_core_mask` es una máscara de bits hexadecimal que especifica qué CPU deben procesar los paquetes entrantes, en la que cada dígito representa 4 CPU. También debe estar separada por comas cada 8 caracteres empezando por la derecha. Se recomienda utilizar todas las CPU y dejar que el almacenamiento en caché se encargue del equilibrio.
  - Para ver la lista de parámetros recomendados para cada tipo de instancia, consulte Apéndice: Parámetros recomendados para Interrupt/RPS Tune.
- Ejemplo para una instancia de 96 CPU:

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

La fusión de interrupciones de Tune Rx afecta a la red

La fusión de interrupciones ayuda a evitar que el sistema de host se inunde con demasiadas interrupciones y a aumentar el rendimiento de la red. Con esta configuración, se recopilan los paquetes y se genera una única interrupción cada 128 microsegundos. Añádelo a crontab para que se aplique en cada arranque:

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

- Sustituya `interface` por la interfaz de red (adaptador Ethernet) configurada para recibir datos. Normalmente, `eth0` se trata de la interfaz de red predeterminada asignada a una instancia EC2.

Tune Rx Ring Buffer: afecta a la red

Aumente el número de entradas de anillo en el búfer de anillo Rx para evitar que los paquetes se caigan o se sobrecarguen durante las conexiones interrumpidas. Añádalo al crontab para que quede correctamente configurado en cada arranque:

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

- Sustituya `interface` por la interfaz de red (adaptador Ethernet) configurada para recibir datos. Normalmente, `eth0` se trata de la interfaz de red predeterminada asignada a una instancia EC2.
- Si configura una instancia c6i.32xlarge, es necesario modificar el comando para configurar el búfer circular en `8192`, en lugar de en `16384`

Ajustar el estado C de la CPU: afecta a la CPU

Configure el estado C de la CPU para evitar que se quede inactiva, lo que puede provocar la pérdida de paquetes durante el inicio de un contacto. Requiere reinicio de instancias.

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

Reserve los puertos de entrada: impacta en la red

Reserve todos los puertos del rango de puertos de su dirección de entrada de `AwsGroundStationAgentEndpoint` para evitar conflictos con el uso del núcleo. Un conflicto en el uso de los puertos provocará un fallo en el contacto y en la entrega de datos.

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

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

Reboot

Cuando todas las afinaciones se hayan aplicado correctamente, reinicie la instancia para que se apliquen los cambios.

```
sudo reboot
```

Apéndice: Parámetros recomendados para Interrupt/RPS Tune

Esta sección determina los valores de los parámetros recomendados para usarlos en la sección de ajustes de las interrupciones del hardware y las colas de recepción: afecta a la CPU y la red.

Familia	Tipo de instancia	${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

Familia	Tipo de instancia	${interrupt_core_list}	${rps_core_mask}
r5n	• r5n.metal • r5n.24xlarge	• 0,1,48,49 • 0,1,48,49	• ffffffff, ffffffff, ffffffff • ffffffff, ffffffff, ffffffff
G4dn	• g4dn.metal • g4dn.16xlarge • g4dn.12xlarge	• 0,1,48,49 • 0,1,32,33 • 0,1,24,25	• ffffffff, ffffffff, ffffffff • ffffffff, ffffffff • ffff,ffffffff
p4d	• p4d.24xlarge	• 0,1,48,49	• ffffffff, ffffffff, ffffffff
p3dn	• p3dn.24xlarge	• 0,1,48,49	• ffffffff, ffffffff, ffffffff

Prepárese para tener un contacto en DigiF

1. Revise la planificación del núcleo de la CPU para ver los flujos de datos deseados y proporcione una lista de los núcleos que el agente puede usar. Consulte Planificación del núcleo de CPU.
2. Revise el archivo de configuración del AWS Ground Station agente. Consulte AWS Ground Station Configuración del agente.
3. Confirme que se han aplicado los ajustes de rendimiento necesarios. Consulte Ajuste del rendimiento de la instancia EC2.
4. Confirme que está siguiendo todas las prácticas recomendadas indicadas. Consulte Prácticas recomendadas.

5. Confirme que el AWS Ground Station agente se haya iniciado antes de la hora de inicio programada del contacto mediante:

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

6. Confirme que el AWS Ground Station agente está en buen estado antes de la hora de inicio programada del contacto mediante:

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

   Compruebe que `agentStatus` de `awsGroundStationAgentEndpoint` está ACTIVO y que `auditResults` FUNCIONA CORRECTAMENTE.

Prácticas recomendadas

Prácticas recomendadas de EC2

Siga las prácticas recomendadas de EC2 y garantice una disponibilidad suficiente de almacenamiento de datos.

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

Programador de Linux

El programador de Linux puede reordenar los paquetes en los sockets UDP si los procesos correspondientes no están anclados a un núcleo específico. Cualquier subproceso que envíe o reciba datos UDP debe fijarse a un núcleo específico durante la transmisión de datos.

AWS Ground Station Lista de prefijos gestionados

Se recomienda utilizar la lista de prefijos gestionada por AWS `com.amazonaws.global.groundstation` al especificar las reglas de red para permitir la comunicación desde la antena. Para obtener más información sobre las listas de prefijos administradas por AWS, consulte Trabajar con listas de prefijos administradas por AWS

Limitación de contacto único

El agente de AWS Ground Station admite varias transmisiones por contacto, pero solo admite un contacto a la vez. Para evitar problemas de programación, no comparta una instancia entre varios grupos de puntos de conexión de flujos de datos. Si la configuración de un solo agente está asociada a varios ARN de DFEG diferentes, no se registrará.

Ejecución de servicios y procesos junto con el agente AWS Ground Station

Al lanzar servicios y procesos en la misma instancia EC2 que el AWS Ground Station agente, es importante vincularlos a las VCPU que el agente y el núcleo de Linux no utilizan, ya que esto puede provocar cuellos de botella e incluso AWS Ground Station la pérdida de datos durante los contactos. Este concepto de unión a vCPU específicas se conoce como afinidad.

Núcleos que se deben evitar:

- `agentCpuCores`de Archivo de configuración del agente
- `interrupt_core_list` de Ajusta las interrupciones del hardware y las colas de recepción, lo que afecta a la CPU y a la red.
  - Los valores predeterminados se pueden encontrar en Apéndice: Parámetros recomendados para Interrupt/RPS Tune

Como ejemplo, usar una **`c5.24xlarge`** instancia

Si especificó

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

y corrió

```
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
```

luego evita los siguientes núcleos:

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

Servicios de afinización (systemd)

Los servicios recién lanzados se afinizarán automáticamente con los mencionados anteriormente. `interrupt_core_list` Si el caso de uso de sus servicios lanzados requiere núcleos adicionales o necesita núcleos menos congestionados, siga esta sección.

Compruebe la afinidad con la que está configurado su servicio actualmente con el comando:

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

Si ves un valor vacío`CPUAffinity=`, por ejemplo, significa que probablemente usará los núcleos predeterminados del comando anterior `...bin/set_irq_affinity.sh <using the cores here> ...`

Para anular y establecer una afinidad específica, busca la ubicación del archivo de servicio ejecutando:

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

Abra y modifique el archivo (usando `vinano`, etc.) y colóquelo `CPUAffinity=<core list>` en la `[Service]` sección de la siguiente manera:

```
[Unit]
...

[Service]
...
CPUAffinity=2,3

[Install]
...
```

Guarde el archivo y reinicie el servicio para aplicar la afinidad con:

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

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

Para obtener más información, visite: Red Hat Enterprise Linux 8: Administración, supervisión y actualización del núcleo, capítulo 27. Configuración de las políticas NUMA y de afinidad de la CPU mediante systemd.

Procesos de afinización (scripts)

Se recomienda encarecidamente afinizar manualmente los scripts y procesos recién lanzados, ya que el comportamiento predeterminado de Linux les permitirá utilizar cualquier núcleo de la máquina.

Para evitar conflictos fundamentales en cualquier proceso en ejecución (como python, scripts bash, etc.), inicie el proceso con:

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

Si el proceso ya se está ejecutando, utilice comandos como `pidoftop`, o `ps` busque el ID de proceso (PID) del proceso específico. Con el PID puede ver la afinidad actual con:

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

y puede modificarla con:

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

Para obtener más información sobre el conjunto de tareas, consulte la página de manual de taskset: Linux

Solución de problemas

El agente no se puede iniciar

Es posible que el AWS Ground Station agente no se inicie debido a varios motivos, pero el escenario más común podría ser un archivo de configuración del agente mal configurado. Tras iniciar el agente (consulte AWS Ground Station Inicio del agente), es posible que obtenga un estado como el siguiente:

```
#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)
```

Solución de problemas

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

podría dar como resultado una salida 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.
```

Si no se inicia el agente después de Loading Config, se debe a un problema con la configuración del agente. Consulte Archivo de configuración del agente para verificar la configuración del agente.

AWS Ground Station Registros del agente

AWS Ground Station El agente escribe información sobre las ejecuciones, los errores y el estado de los contactos en los archivos de registro de la instancia que ejecuta el agente. Puede ver los archivos de registro conectándose manualmente a una instancia.

Puede ver los registros del agente en la siguiente ubicación.

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

No hay contactos disponibles

Para programar los contactos se necesita un AWS Ground Station agente en buen estado. Confirme que su AWS Ground Station agente se ha iniciado y que está en buen estado consultando la AWS Ground Station API a través get-dataflow-endpoint-group de:

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

Compruebe que `agentStatus` de `awsGroundStationAgentEndpoint` está ACTIVO y que `auditResults` FUNCIONA CORRECTAMENTE.

Cómo obtener soporte

Póngase en contacto con el equipo de Ground Station a través de AWS Support.

1. Indique `contact_id` para los contactos afectados. El AWS Ground Station equipo no puede investigar a un contacto específico sin esta información.
2. Proporcione detalles sobre todos los pasos de solución de problemas que ya se hayan tomado.
3. Escribe cualquier mensaje de error que encuentres al ejecutar los comandos en nuestra guía de solución de problemas.

Notas de la versión del agente

Última versión del agente

Versión 1.0.3555.0

Fecha de lanzamiento: 27/03/2024

Fecha de fin de soporte: 31/08/2024

Sumas de verificación de RPM:

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

Cambios:

- Agregue la métrica del agente para la versión ejecutable seleccionada durante el inicio de la tarea.
- Agregue soporte para archivos de configuración para evitar versiones ejecutables específicas cuando haya otras versiones disponibles.
- Agregue diagnósticos de red y enrutamiento.
- Funciones de seguridad adicionales.
- Se solucionó el problema por el que algunas métricas que informaban de errores se escribían en stdout/journal en lugar de en un archivo de registro.
- Maneje correctamente los errores de sockets inalcanzables de la red.
- Mida la pérdida de paquetes y la latencia entre los agentes de origen y destino.

- Publique aws-gs-datapipe la versión 2.0 para admitir las nuevas funciones del protocolo y la capacidad de actualizar los contactos al nuevo protocolo de forma transparente.

Versiones de agentes obsoletas

Versión 1.0.2942.0

Fecha de lanzamiento: 26/06/2023

Fecha de fin de soporte: 31/05/2024

Sumas de verificación de RPM:

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

Cambios:

- Se agregaron registros de errores para cuando el agente RPM se actualiza en el disco y es necesario reiniciarlo para que los cambios surtan efecto.
- Se agregó la validación del ajuste de la red para garantizar que se sigan y apliquen correctamente los pasos de ajuste de la guía del usuario del agente.
- Se ha corregido un error que provocaba advertencias erróneas en los registros del agente sobre el archivado de registros.
- Detección de pérdida de paquetes mejorada.
- Se actualizó la instalación del agente para impedir la instalación o actualización del RPM si el agente ya está en ejecución.

Versión 1.0.2716.0

Fecha de lanzamiento: 15/03/2023

Fecha de fin de soporte: 31/05/2024

Sumas de verificación de RPM:

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

Cambios:

- Habilite la carga de registros cuando el agente experimente errores durante la tarea.
- Corrige un error de compatibilidad con Linux en los scripts de ajuste de red proporcionados.

Versión 1.0.2677.0

Fecha de lanzamiento: 15/02/2023

Fecha de fin de soporte: 31/05/2024

Sumas de verificación de RPM:

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

Cambios:

- Primera versión de Agent disponible de forma general.

Validación de la instalación de RPM

A continuación se muestran la versión más reciente de RPM, el hash MD5 validado desde RPM y el hash SHA256 mediante sha256sum. Estos valores, combinados, se pueden utilizar para validar la versión RPM que se utiliza para el agente de la estación terrestre.

Versión más reciente del agente

Versión 1.0.3555.0

Fecha de lanzamiento: 27/03/2024

Fecha de fin de soporte: 31/08/2024

Sumas de verificación de RPM:

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

Cambios:

- Agregue la métrica del agente para la versión ejecutable seleccionada durante el inicio de la tarea.
- Agregue soporte para archivos de configuración para evitar versiones ejecutables específicas cuando haya otras versiones disponibles.
- Agregue diagnósticos de red y enrutamiento.
- Funciones de seguridad adicionales.
- Se solucionó el problema por el que algunas métricas que informaban de errores se escribían en stdout/journal en lugar de en un archivo de registro.
- Maneje correctamente los errores de sockets inalcanzables de la red.
- Mida la pérdida de paquetes y la latencia entre los agentes de origen y destino.
- Publique aws-gs-datapipe la versión 2.0 para admitir las nuevas funciones del protocolo y la capacidad de actualizar los contactos al nuevo protocolo de forma transparente.

Verifique las RPM

Las herramientas que necesitará para poder verificar la instalación de este RPM son:

- sha256sum
- RPM

Ambas herramientas vienen de forma predeterminada en Amazon Linux 2. Estas herramientas ayudarán a validar que el RPM que está utilizando es la versión correcta. En primer lugar, descargue el último RPM del bucket de S3 (consulte Descargar el agente para saber cómo descargar el RPM). Una vez descargado el archivo, habrá que comprobar algunas cosas:

- Calcule la suma sha256del archivo RPM. Realice la siguiente acción desde la línea de comandos de la instancia de procesamiento que esté utilizando:

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

  Tome este valor y compárelo con la tabla anterior. Esto demuestra que el archivo RPM que se descarga es un archivo válido para su uso y que AWS Ground Station ha distribuido a los clientes. Si los hash no coinciden, no instale el RPM y elimínelo de la instancia de procesamiento.

- Compruebe también el hash MD5 del archivo para asegurarse de que el RPM no se haya visto comprometido. Para ello, ejecute el siguiente comando en la herramienta de línea de comandos de RPM:

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

  Compruebe que el hash MD5 que se muestra aquí es el mismo que el hash MD5 de la versión que aparece en la tabla anterior. Una vez que estos dos hash se hayan validado con esta tabla que aparece en los documentos de AWS, el cliente puede estar seguro de que el RPM que se descargó e instaló es la versión segura y sin restricciones del RPM.

Enumeración y reserva de contactos

Puede especificar los datos de los satélites, identificar las ubicaciones de las antenas y programar el tiempo de antena para los satélites seleccionados al utilizar la consola de AWS Ground Station o AWS CLI. Puede revisar, cancelar y reprogramar las reservas de contacto con hasta ocho días de antelación al tiempo programado. Además, puede ver los detalles de su plan de precios de minutos reservados si utiliza el modelo de precios de minutos AWS Ground Station reservados.

AWS Ground Station admite la entrega de datos entre regiones. Las configuraciones de puntos de enlace del flujo de datos que forman parte del perfil de misión seleccionado determinan a qué región o regiones se envían los datos. Para obtener más información acerca del uso de la entrega de datos entre regiones, consulte Uso del servicio de entrega de datos entre regiones.

Para programar contactos, los recursos deben estar configurados. Si no ha configurado los recursos, consulte Introducción.

Temas

- Uso de la consola de Ground Station.
- Reserva y administra contactos con AWS CLI

Uso de la consola de Ground Station.

Puede utilizar la AWS Ground Station consola para reservar, ver y cancelar las reservas de contactos. Para usar la AWS Ground Station consola, ábrela AWS Ground Station y selecciona Reservar contactos ahora.

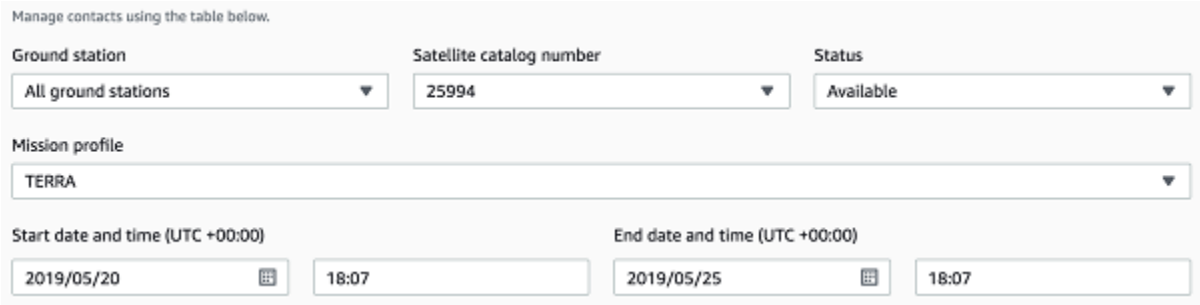
Use los siguientes temas para usar la AWS Ground Station consola para reservar, ver y cancelar contactos.

Temas

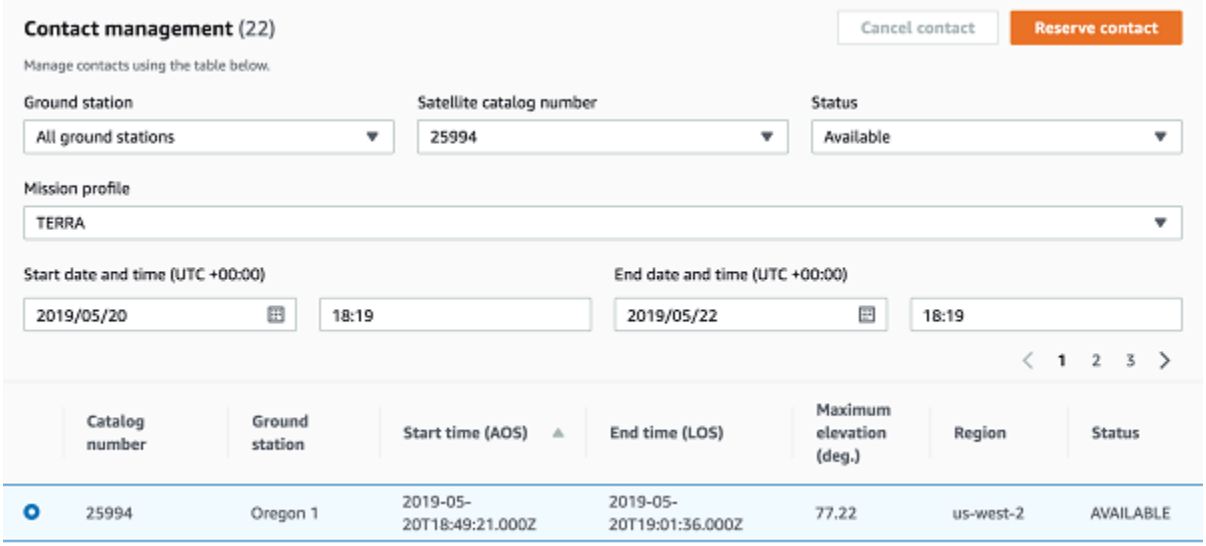
Reservar un contacto

Tras acceder a la AWS Ground Station consola, utilice los recursos configurados para reservar los contactos en la tabla de administración de contactos.

1. En la tabla Administración de contactos seleccione los parámetros que desea utilizar para buscar contactos disponibles. Asegúrese de que está viendo los contactos disponibles con el filtro Estado.



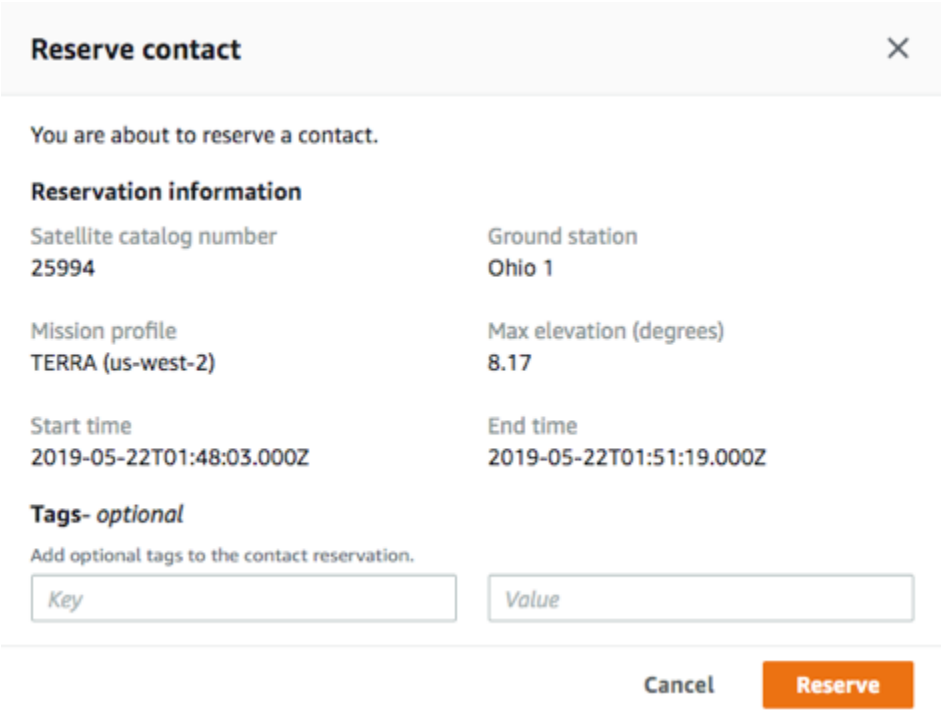
2. Elija un contacto que satisfaga sus requisitos y, a continuación, elija Reserve Contact (Reservar contacto).



3. En el cuadro de diálogo Reserve Contact (Reservar contacto), revise la información de la reserva de contacto.

   a. (opcional) En Tags (Etiquetas), escriba una clave y un valor para cada etiqueta que desee añadir.

   b. Elija Reserve (Reservar).

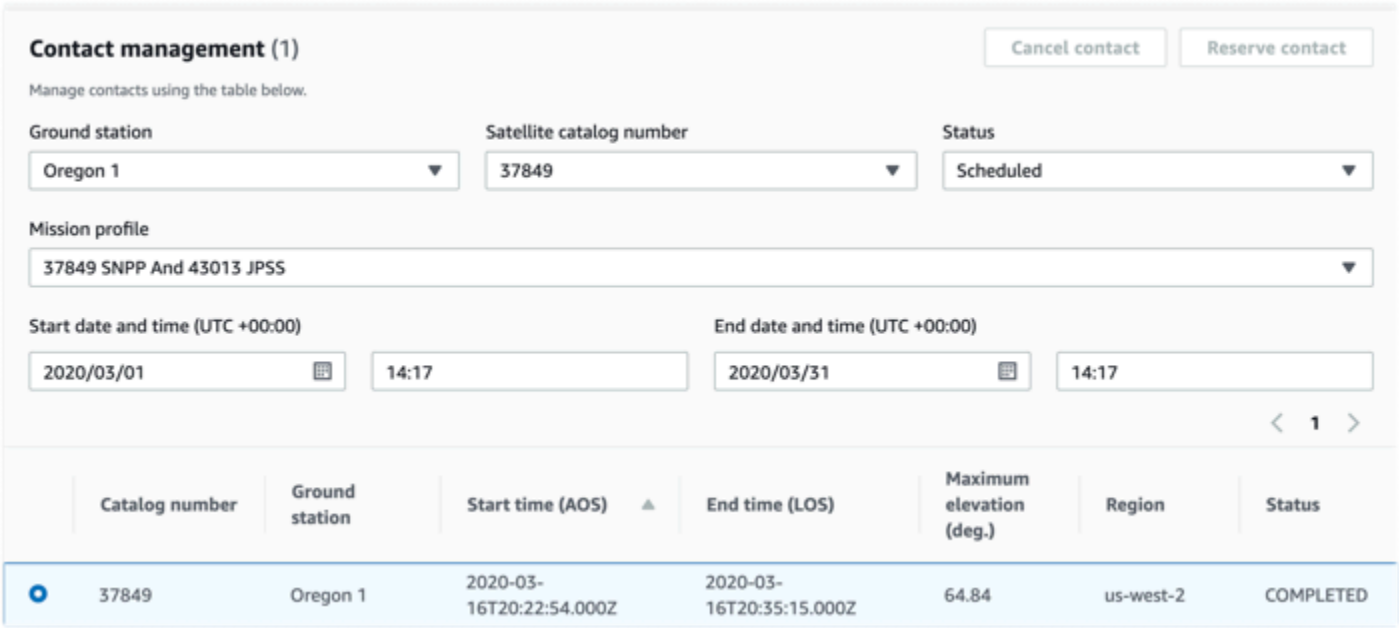


AWS Ground Station utilizará los datos de configuración del perfil de su misión para ejecutar un contacto en la estación terrestre especificada.

Ver contactos programados y completados

Una vez que haya programado los contactos, podrá utilizar la AWS Ground Station consola para ver los detalles de los contactos programados y finalizados.

En la tabla Administración de contactos seleccione los parámetros que desea utilizar para buscar los contactos programados y completados. Asegúrese de que está viendo los contactos programados o completados con el filtro Estado.



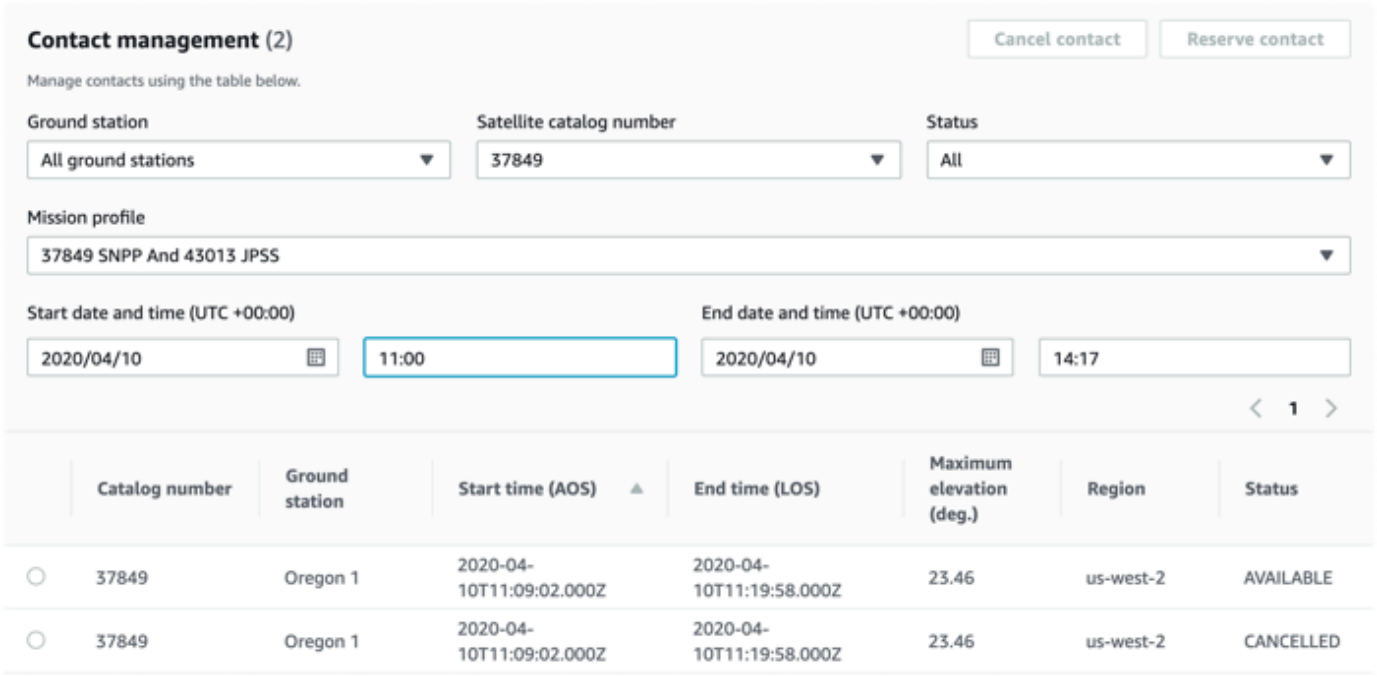
Sus contactos programados o completados se mostrarán si los contactos coinciden con los parámetros.

Cancelación de contactos

Puedes usar la AWS Ground Station consola para cancelar los contactos programados

1. En la tabla Administración de contactos seleccione los parámetros que desea utilizar para buscar los contactos programados y completados. Asegúrese de que está viendo los contactos programados con el filtro Estado.
2. Seleccione el contacto que desea cancelar en la lista de contactos programados. A continuación, seleccione Cancelar contacto.

3. En el cuadro de diálogo Cancelar contacto seleccione Aceptar.



El estado de los contactos será CANCELADO.

Nomenclatura de satélites

La AWS Ground Station consola tiene la capacidad de mostrar un nombre definido por el usuario para un satélite junto con el ID de Norad cuando se utiliza la página de contactos. Si se muestra el nombre del satélite, es mucho más fácil seleccionar el satélite correcto a la hora de la programación. Para ello, se pueden utilizar etiquetas.

El etiquetado de satélites de AWS Ground Station puede realizarse a través de la API tag-resource con AWS CLI o uno de los SDK de AWS. Esta guía explicará el uso de la AWS Ground Station CLI para etiquetar el satélite de transmisión pública Aqua (Norad ID 27424). `us-west-2`

AWS Ground Station CLI

Se AWS CLI puede usar para interactuar con. AWS Ground Station Antes de AWS CLI utilizarlos para etiquetar sus satélites, deben cumplirse los siguientes AWS CLI requisitos previos:

- Asegúrese de que AWS CLI esté instalado. Para obtener información sobre la instalación AWS CLI, consulte Instalación de la versión 2 de la AWS CLI.

- Asegúrese de que AWS CLI esté configurada. Para obtener información sobre la configuración AWS CLI, consulte Configuración de la versión 2 de la AWS CLI.
- Guarde las opciones de configuración y las credenciales que utiliza con frecuencia en archivos que son mantenidos por la AWS CLI. Necesita estos ajustes y credenciales para reservar y administrar sus AWS Ground Station contactos AWS CLI. Para obtener más información sobre cómo guardar su configuración y la configuraciones de credenciales, consulte Configuración y configuraciones del archivo de credenciales .

Una vez AWS CLI configurado y listo para su uso, consulte la página de referencia de comandos de la CLI de AWS Ground Station para familiarizarse con los comandos disponibles. Siga la estructura de AWS CLI comandos cuando utilice este servicio y añada el prefijo `groundstation` a sus comandos para especificar AWS Ground Station el servicio que desea utilizar. Para obtener más información sobre la estructura de AWS CLI comandos, consulte Estructura de comandos en la página de la CLI de AWS. A continuación, se proporciona una estructura de comandos de ejemplo.

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

Nombrar un satélite

Lo primero que debe hacer es obtener el ARN del satélite o satélites que desea etiquetar. Esto se puede hacer a través de la API list-satellites de la AWS CLI:

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

Al ejecutar el comando CLI anterior se obtendrá un resultado similar al siguiente:

```
{
    "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"
        }
```

```
    ]
}
```

Busque el satélite que desea etiquetar y anote su `satelliteArn`. Una advertencia importante para el etiquetado es que la API tag-resource necesita un ARN regional, y el ARN devuelto por list-satellites es global. Para el siguiente paso, debe aumentar el ARN con la región en la que le gustaría ver la etiqueta (probablemente la región en la que programa). En este ejemplo, utilizaremos `us-west-2`. Con este cambio, el ARN pasará de:

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

a:

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

Para mostrar el nombre del satélite en la consola, el satélite debe tener una etiqueta con "`Name`" como clave. Además, dado que utilizamos las comillas AWS CLI, las comillas deben ir precedidas de una barra invertida. La etiqueta tendrá un aspecto similar a

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

A continuación, debe llamar a la API tag-resource para etiquetar el satélite. Esto se puede hacer de la siguiente AWS CLI manera:

```
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\"}
```

Después de hacer esto, podrás ver el nombre que configuraste para el satélite en la AWS Ground Station consola.

Cambiar el nombre de un satélite

Si desea cambiar el nombre de un satélite, puede simplemente llamar de nuevo a tag-resource con el ARN del satélite con la misma clave "`Name`", pero con un valor distinto en la etiqueta. Esto

actualizará la etiqueta existente y mostrará el nuevo nombre en la consola. Un ejemplo de llamada es el siguiente

```
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\"}
```

Eliminar el nombre de un satélite

El nombre configurado para un satélite puede eliminarse con la API untag-resource. Esta API necesita el ARN del satélite con la región en la que se encuentra la etiqueta y una lista de claves de etiqueta. Para el nombre, la clave de etiqueta es "Name". Un ejemplo de llamada a esta API utilizando AWS CLI es el siguiente:

```
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
```

Reserva y administra contactos con AWS CLI

Puede usarlo AWS CLI para reservar y administrar sus contactos en AWS Ground Station. Antes de utilizarlo AWS CLI para reservar y gestionar contactos, se deben cumplir los siguientes AWS CLI requisitos previos:

- Asegúrese de que AWS CLI esté instalado. Para obtener información sobre la instalación AWS CLI, consulte Instalación de la versión 2 de la AWS CLI.
- Asegúrese de que AWS CLI esté configurada. Para obtener información sobre la configuración AWS CLI, consulte Configuración de la versión 2 de la AWS CLI.
- Guarde las opciones de configuración y las credenciales que utiliza con frecuencia en archivos que son mantenidos por la AWS CLI. Necesita estos ajustes y credenciales para reservar y administrar sus AWS Ground Station contactos AWS CLI. Para obtener más información sobre cómo guardar su configuración y la configuraciones de credenciales, consulte Configuración y configuraciones del archivo de credenciales .

Una vez AWS CLI configurado y listo para su uso, consulte la página de referencia de comandos de la CLI de AWS Ground Station para familiarizarse con los comandos disponibles. Siga la estructura

de AWS CLI comandos cuando utilice este servicio y añada el prefijo `groundstation` a sus comandos para especificar AWS Ground Station el servicio que desea utilizar. Para obtener más información sobre la estructura de AWS CLI comandos, consulte Estructura de comandos en la página de la CLI de AWS. A continuación, se proporciona una estructura de comandos de ejemplo.

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

Utilice los siguientes temas para reservar, ver y cancelar contactos con AWS CLI.

Temas

- Vea y enumere los contactos con AWS CLI
- Reserve un contacto con AWS CLI
- Describa un contacto con AWS CLI
- Cancela un contacto con AWS CLI

Vea y enumere los contactos con AWS CLI

Para enumerar y ver `CANCELLEDCOMPLETED`, o `SCHEDULED` los contactos con AWS CLI, ejecute `aws groundstation list-contacts` con los siguientes parámetros.

- Hora de inicio: especifique la hora de inicio de su contacto con `--start-time <value>`. El siguiente es un formato de valor de tiempo aceptable: `YYYY-MM-DDTHH:MM:SSZ`
- Hora de finalización: especifique la hora de finalización de su contacto con `--end-time <value>`. El siguiente es un formato de valor de tiempo aceptable: `YYYY-MM-DDTHH:MM:SSZ`
- Lista de estado: especifique el estado de su contacto con `--status-list <value>`. Los valores aceptables incluyen `AVAILABLE`, `CANCELLED`, `COMPLETED` o `SCHEDULED`. Para ver una lista completa de valores válidos, consulte list-contacts.

Para enumerar y ver AWS CLI los `AVAILABLE` contactos se requieren los siguientes parámetros además de los enumerados anteriormente.

- ID de Ground Station: especifique el ID de su Ground Station con `--ground-station <value>`.
- ARN del perfil de la misión: especifique el ARN de su perfil de misión con `--mission-profile-arn <value>`.
- ARN satélite: especifique su ARN satélite con `--satellite-arn <value>`.

Puede utilizar los comandos `list` para buscar recursos. Para obtener más información sobre cómo especificar los parámetros, consulte list-contacts

A continuación se proporciona un comando de ejemplo para enumerar los contactos disponibles.

```
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'
```

A continuación se proporciona una lista de ejemplo de contactos disponibles.

```
{
  "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 un contacto con AWS CLI

AWS CLI te da la opción de reservar contactos por minuto. Esta función es exclusiva de la AWS Ground Station consola AWS CLI y no se puede utilizar en ella.

Para reservar contactos AWS CLI, ejecútelo `aws groundstation reserve-contact` con los siguientes parámetros.

- ID de Ground Station: especifique el ID de su Ground Station con `--ground-station <value>`.
- ARN del perfil de la misión: especifique el ARN de su perfil de misión con `--mission-profile-arn <value>`.
- ARN satélite: especifique su ARN satélite con `--satellite-arn <value>`.
- Hora de inicio: especifique la hora de inicio de su contacto con `--start-time <value>`. El siguiente es un formato de valor de tiempo aceptable: `YYYY-MM-DDTHH:MM:SSZ`
- Hora de finalización: especifique la hora de finalización de su contacto con `--end-time <value>`. El siguiente es un formato de valor de tiempo aceptable: `YYYY-MM-DDTHH:MM:SSZ`

La reserva de contactos es un proceso asíncrono. La respuesta al comando `reserve-contact` proporciona el identificador del contacto. Para conocer el resultado del proceso de reserva asíncrono, utilice `describe-contact`. Para obtener más información, consulte la sección titulada Describa un contacto con AWS CLI.

Puede utilizar los comandos `list` para buscar recursos. Para más información sobre cómo especificar sus parámetros, consulte reserve-contact

A continuación se proporciona un comando de ejemplo para reservar un contacto.

```
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'
```

A continuación se proporciona un ejemplo de un contacto reservado correctamente.

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

Describa un contacto con AWS CLI

Para ver el estado de un contacto/reserva con AWS CLI, utilice el comando `describe-contact` CLI. Esto resulta útil para verificar el resultado del proceso de reserva de contacto asíncrono, supervisar el estado de un contacto en curso y determinar el estado de un contacto finalizado.

Para describir los contactos con AWS CLI, ejecute `aws groundstation describe-contact` con los siguientes parámetros.

- ID de contacto: especifique su ID de contacto con `--contact-id <value>`.

Puede utilizar los comandos `list` para buscar recursos. Para más información sobre cómo especificar sus parámetros, consulte describe-contac

A continuación se proporciona un comando de ejemplo para describir un contacto.

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

A continuación se ofrece un ejemplo de contacto programado correctamente.

```
{
  "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"
}
```

Cancela un contacto con AWS CLI

Para cancelar un contacto con AWS CLI, ejecute `aws groundstation cancel-contact` con los siguientes parámetros.

- Región: especifique la región de su Ground Station con `--region <value>`.
- ID de contacto: especifique el ID de contacto con `--contact-id <value>`.

Puede utilizar los comandos `list` para buscar recursos. Para obtener más información sobre cómo especificar los parámetros, consulte cancel-contacts

A continuación se proporciona un comando de ejemplo para reservar un contacto.

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

A continuación se proporciona un ejemplo de un contacto cancelado correctamente.

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

Envío de datos a Amazon EC2

AWS Ground Station entrega sus datos de contacto de forma asíncrona a un bucket de Amazon Simple Storage Service (Amazon S3) de su cuenta o de forma sincrónica transmitiéndolos desde y hacia una instancia de Amazon Elastic Compute Cloud (Amazon EC2) de su cuenta. En los siguientes pasos se describe cómo configurar los recursos necesarios para transmitir datos de contacto desde y hacia una instancia de Amazon EC2. Consulte la guía Cómo empezar con AWS Ground Station para obtener información sobre el envío de datos a Amazon S3.

Temas

Paso 1: Crear un par de claves SSH de EC2

Si aún no tiene uno, cree un nuevo key pair en la consola de Amazon EC2 para cada AWS región en la que vaya a recibir datos. Utilice los pasos que se indican a continuación.

1. En la suya AWS Management Console, elija AWS la región en la que planea reservar los contactos. Debe crear un key pair para cada AWS región que elija.

   > **Note**
   >
   > AWS Ground Station aún no está disponible para todas las regiones. Asegúrese de que AWS Ground Station sea compatible con la AWS región que desee. Para obtener más información sobre las ubicaciones de las AWS Ground Station antenas, consulte las preguntas frecuentes sobre AWS Ground Station.

2. Siga la guía Creación de pares de claves de la Guía del usuario de Amazon EC2 para crear los pares de claves.
3. Repita el procedimiento para otras AWS regiones si es necesario.

Paso 2: Configurar la VPC

Esta guía no describe la configuración completa de una VPC. Si no dispone de una VPC ya personalizada, puede utilizar la VPC predeterminada que se crea en su cuenta de AWS . Le recomendamos que añada un bastión Linux a su VPC para poder utilizar SSH en sus instancias de Amazon EC2 sin necesidad de asociar una dirección IP pública. Para obtener más información acerca de la configuración de un bastión de Linux en la VPC, consulte Hosts bastiones de Linux en AWS.

Para su comodidad, a continuación encontrará instrucciones para añadir rápidamente un host bastión a su entorno Linux. AWS Aunque no es obligatorio, es una práctica recomendada.

1. Inicie sesión en su AWS cuenta.
2. En la página Linux Bastion Hosts on the AWS Cloud: Quick Start Reference Deployment (Hosts bastiones de Linux en la nube de AWS: Implementación de referencia de inicio rápido), seleccione Launch Quick Start (for new VPC) (Lanzar inicio rápido [para una VPC nueva]).
3. En la página Create Stack (Crear pila), seleccione Next (Siguiente). La plantilla se rellena previamente.
4. En la página de detalles Specify stack (Especificar pila), realice cambios y modificaciones en las siguientes casillas:

    a. Introduzca un nombre de pila para el host en la casilla Stack Name (Nombre de pila).

    b. En Availability Zones (Zonas de disponibilidad), seleccione las zonas de disponibilidad que desea utilizar para las subredes de la VPC. Se deben seleccionar al menos dos zonas de disponibilidad.

    c. En Allowed bastion external access CIDR (CIDR de acceso externo del bastión permitido), introduzca el bloque de CIDR desde el que desea habilitar el acceso SSH. Si no está seguro, puede utilizar el valor 0.0.0.0/0 para habilitar el acceso SSH desde cualquier host que tenga la clave de SSH.

    d. En Key pair name (Nombre de par de claves), seleccione el nombre del par de claves que ha creado en the section called “Paso 1: Crear un par de claves SSH de EC2”.

    e. En Bastion instance type (Tipo de instancia Bastion), elija t2.micro.

> **Important**
>
> El tipo de instancia t2.micro no está disponible para la región de Europa (Estocolmo) (eu-north-1). Si lo utiliza AWS Ground Station en la región de Europa (Estocolmo) (eu-north-1), elija t3.micro.

f. En TCP forwarding (Reenvío de TCP), elija true.

g. (Opcional) Realice otros cambios y modificaciones si es necesario. Para personalizar la implementación, puede cambiar la configuración de VPC, elegir la cantidad y el tipo de instancias del host bastión, habilitar el reenvío de TCP o X11 y habilitar un aviso predeterminado o personalizado para los hosts bastión.

h. Elija Siguiente.

5. En la página Configure stack options (Configurar opciones de pila), realice los cambios y modificaciones necesarios.
6. Elija Siguiente.
7. Revise los detalles del host bastión y seleccione los dos reconocimientos de actividades de Capabilities (Funcionalidades). A continuación, elija Create stack (Crear pila).

Paso 3: Elige y personaliza una plantilla AWS CloudFormation

En la actualidad puede configurar varias transmisiones de datos por contacto para que fluyan hacia la VPC. Estas secuencias de datos están disponibles en dos formatos diferentes. Las secuencias de datos que contienen datos de VITA-49 Signal/IP se pueden configurar para señales de banda S y banda X de hasta 54 MHz de ancho de banda. Los datos/IP de extensión VITA-49 se pueden configurar para señales de banda X desmoduladas y/o descodificadas de hasta 500 MHz de ancho de banda.

Después de incorporar el satélite, se deben definir perfiles de misión y crear instancias para procesar o enviar transmisiones de datos desde o hacia el satélite. Para ayudarlo en este proceso, proporcionamos AWS CloudFormation plantillas preconfiguradas que utilizan satélites de transmisión pública. Estas plantillas le permiten empezar a AWS Ground Station utilizarlas fácilmente. Para obtener más información AWS CloudFormation, consulte ¿Qué es AWS CloudFormation?

Es importante tener en cuenta que necesita tener un software de procesamiento de datos o un software de almacenamiento de datos que escuche el lado local del Data Defender de la instancia de

Amazon EC2. Este software es el que utilizará para almacenar y/o procesar los datos enviados a la instancia de Amazon EC2 durante un contacto.

Configuración de los ajustes de su instancia de Amazon EC2

Las AWS CloudFormation plantillas que se proporcionan en esta sección están configuradas para usar los tipos de instancias Amazon EC2 m5.4xlarge de forma predeterminada. Sin embargo, le recomendamos que personalice y elija la configuración de instancia de Amazon EC2 adecuada para su caso. Al elegir la configuración de la instancia, se deben tener en cuenta requisitos como E/S de almacenamiento y rendimiento de la CPU. Por ejemplo, ejecutar un módem de software en una instancia de receptor puede requerir instancias optimizadas para el equipo con más núcleos y una velocidad de reloj más alta. La mejor forma de determinar la configuración de instancia adecuada para su caso de uso es probar la configuración de instancia con su carga de trabajo, y Amazon EC2 facilita el cambio entre configuraciones de instancia. Utilice las plantillas y personalice la configuración de instancia según sus necesidades.

Como recomendación general, se AWS Ground Station recomienda el uso de instancias que admitan redes mejoradas para sus enlaces ascendentes y descendentes, como AWS Nitro System. Para obtener más información acerca de las redes mejoradas, consulte Habilitación de redes mejoradas con Elastic Network Adapter (ENA) en instancias de Linux.

Además de configurar los tipos de instancias de Amazon EC2, las AWS CloudFormation plantillas configuran las imágenes de máquina de Amazon (AMI) base que se utilizarán en la instancia. La AWS Ground Station base contiene el software necesario para recibir los datos del servicio preinstalado en la instancia EC2. Para obtener más información sobre las AMI, consulte Imágenes de máquina de Amazon (AMI).

Creación y configuración de recursos manualmente

AWS CloudFormation Las plantillas de muestra de esta sección configuran todos los recursos necesarios para empezar a ejecutar los contactos satelitales. Si prefiere crear y configurar manualmente los recursos necesarios para comenzar a ejecutar contactos satélite, deberá hacer lo siguiente:

- Cree AWS Ground Station configuraciones. Para obtener más información sobre la creación manual de AWS Ground Station configuraciones, consulte Create Config AWS CLI Command Reference o Create Config API Reference.

- Cree un perfil de AWS Ground Station misión. Para obtener más información sobre la creación manual de un perfil de AWS Ground Station misión, consulte Crear perfil de misión (AWS CLI Command Reference) o Crear perfil de misión (API Reference).
- Cree un grupo de puntos finales AWS Ground Station de flujo de datos. Para obtener más información sobre la creación manual de un grupo de puntos de enlace de flujo de datos, consulte Create AWS Ground Station Dataflow Endpoint Group AWS CLI Command Reference o Create Dataflow Endpoint Group API Reference.
- Cree una instancia de EC2. Para obtener más información sobre la creación manual de una instancia EC2 para usarla con ella, consulte. AWS Ground StationCrear una instancia de Amazon EC2
- Configure los ajustes del grupo de seguridad de la instancia EC2 AWS Ground Station para permitir el envío de datos hacia/desde la instancia EC2. Para obtener más información sobre cómo configurar manualmente los ajustes del grupo de seguridad de la instancia EC2, consulte Create Security Group AWS CLI Command Reference o Create Security Group API Reference.

Elija una plantilla

AWS Ground Station proporciona plantillas que muestran cómo utilizar el servicio y se puede acceder a ellas de diferentes maneras. Utilice esta guía para encontrar la plantilla adecuada para usted.

Uso de una plantilla preconfigurada

Puede utilizar una plantilla preconfigurada para recibir datos de transmisión directa de los satélites Aqua, SNPP, JPSS-1/NOAA-20 y Terra. Estas plantillas contienen los recursos de AWS CloudFormation necesarios para programar y ejecutar contactos. La `AquaSnppJpss` plantilla incluye los AWS CloudFormation recursos necesarios para recibir datos de transmisión directa desmodulados y decodificados. Utilice esta plantilla como punto de partida si tiene previsto procesar los datos utilizando el software Direct Readout Labs (RT-STPS e IPOPP) de la NASA. La plantilla `AquaSnppJpssTerraDigIF` comprende los recursos de AWS CloudFormation necesarios para recibir datos de difusión directa digitalizados de frecuencia intermedia (DigIF) en bruto. Utilice esta plantilla como punto de partida para procesar los datos utilizando una radio definida por software (SDR). La `DirectBroadcastSatelliteWbDigIfEc2DataDelivery` plantilla incluye los AWS CloudFormation recursos necesarios para recibir datos de transmisión directa de frecuencia intermedia digitalizada de banda ancha (DigiF) sin procesar a través del Agente. AWS Ground Station

Plantillas de entrega de datos de banda estrecha:

- the section called “AquaSnppJpss Plantilla (banda estrecha)”
- the section called “AquaSnppJpssTerraDigPlantilla IF (banda estrecha)”

Plantillas de entrega de datos DigiF de banda ancha:

- the section called “Plantilla DigiF de banda ancha por satélite de transmisión directa (banda ancha)”

> **Important**
>
> Los satélites deben estar integrados en el servicio para poder acceder a las AMI con las plantillas. AWS CloudFormation

Usando sus propios satélites

La configuración de sus propios satélites requiere un conjunto diferente de parámetros y recursos. Esto es difícil de hacer por su cuenta. El AWS Ground Station equipo está disponible para ayudarlo a configurar sus propios satélites para su uso y puede ayudarlo a configurar los recursos para las transmisiones de eco de enlace descendente, enlace ascendente y enlace ascendente. Para configurar su propio satélite para usarlo AWS Ground Station, póngase en contacto con AWS Support.

Acceso a plantillas

Puede acceder a las plantillas en el bucket de Amazon S3 regional siguiente. Tenga en cuenta que el vínculo siguiente utiliza un punto de enlace regional de S3. Cambie `<us-west-2>` a la región en la que va a crear la AWS CloudFormation pila.

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

También puede descargar las plantillas utilizando la AWS CLI. Para obtener información sobre cómo configurar el AWS CLI, consulte Configuración del AWS CLI.

AquaSnppJpss Plantilla (banda estrecha)

La AWS CloudFormation plantilla nombrada `AquaSnppJpss.yml` está diseñada para proporcionarle un acceso rápido y empezar a recibir datos de los satélites Aqua, SNPP y JPSS-1/NOAA-20.

Contiene una instancia de Amazon EC2 y los AWS Ground Station recursos necesarios para programar contactos y recibir datos de transmisión directa desmodulados y decodificados. Esta plantilla es un buen punto de partida si tiene previsto procesar los datos utilizando el software Direct Readout Labs (RT-STPS e IPOPP) de la NASA.

Si no se incorporan satélites Aqua, SNPP y JPSS-1/NOAA-20 en la cuenta, consulte Incorporación de clientes.

Important

Es necesario detener la instancia de Amazon EC2 antes de aplicar la plantilla. Asegúrese de que la instancia esté detenida hasta que esté listo para usarla.

Puede acceder a la plantilla accediendo al bucket de S3 de incorporación del cliente. Tenga en cuenta que los enlaces siguientes utilizan un bucket de S3 regional. Cambie `<us-west-2>` a la región en la que va a crear la pila. AWS CloudFormation

Note

Las siguientes instrucciones usan YAML. Sin embargo, las plantillas están disponibles en formato YAML y JSON. Para usar JSON, reemplace `<.yml>` por `<.json>`.

Para descargar la plantilla mediante AWS CLI, utilice el siguiente comando:

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

La plantilla puede verse y descargarse en la consola desde la siguiente URL en su navegador:

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

Puede especificar la plantilla directamente en AWS CloudFormation el siguiente enlace:

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

¿Qué recursos define la plantilla?

La plantilla `AquaSnppJpss` incluye los siguientes recursos:

- Función de servicio de entrega de datos: AWS Ground Station asume esta función para crear o eliminar ENI en su cuenta con el fin de transmitir datos.
- Instancia de recepción (opcional): la instancia de Amazon EC2 que enviará o recibirá datos hacia/desde su satélite mediante. AWS Ground Station
  - Grupo de seguridad de la instancia: el grupo de seguridad de su instancia de Amazon EC2.
  - Rol de instancia: el rol de su instancia de Amazon EC2.
  - Perfil de instancia: el perfil de instancia de la instancia de Amazon EC2.
  - Grupo con ubicación en clúster: el grupo de ubicación en el que se lanza su instancia de Amazon EC2.
- Grupo de seguridad de punto final de Dataflow: el grupo de seguridad al que AWS Ground Station pertenece la interfaz de red elástica creada por. De forma predeterminada, este grupo de seguridad permite AWS Ground Station transmitir tráfico a cualquier dirección IP de la VPC. Puede modificar esto de forma que limite el tráfico a un conjunto específico de direcciones IP.
- Interfaz de red de instancias receptoras: una interfaz de red elástica que proporciona una dirección IP fija AWS Ground Station a la que conectarse. Esto se asocia a la instancia del receptor en `eth1`.
- Receiver Instance Interface Attachment (Accesorio de interfaz de instancia de receptor): interfaz de red elástica que se conecta a la instancia de Amazon EC2.
- Activadores de CloudWatch eventos (opcionales): AWS Lambda función que se activa mediante CloudWatch eventos enviados AWS Ground Station antes y después de un contacto. La AWS Lambda función iniciará y, opcionalmente, detendrá la instancia de Receiver.
- Verificación EC2 para contactos (opcional): la opción de usar Lambda para configurar un sistema de verificación de las instancias de Amazon EC2 para los contactos con notificaciones de SNS. Es importante tener en cuenta que esto puede conllevar gastos en función del uso actual.
- Grupo de puntos finales del flujo de datos: el grupo de puntos finales del AWS Ground Station flujo de datos que define los puntos finales que se utilizan para enviar o recibir datos hacia/desde su satélite. Como parte de la creación del grupo de puntos finales del flujo de datos, AWS Ground Station crea una interfaz de red elástica en su cuenta para transmitir datos.
- Config de rastreo: la configuración AWS Ground Station de rastreo define cómo el sistema de antenas rastrea tu satélite a medida que se mueve por el cielo.
- Ground Station Amazon Machine Image Retrieval Lambda: la opción de seleccionar el software que se instalará en la instancia y la AMI que prefiera. Las opciones de software incluyen DDX

`2.6.2 Only` y `DDX 2.6.2 with qRadio 3.6.0`. Si desea utilizar la entrega de datos DigiF de banda ancha y el AWS Ground Station agente, utilice el. AquaSnppJpssTerraDigPlantilla IF (banda estrecha) Estas opciones seguirán ampliándose a medida que se publiquen actualizaciones y características adicionales del software.

Además, la plantilla proporciona los siguientes recursos para los satélites Aqua, SNPP, JPSS-1/NOAA-20:

- Una configuración de desmodulación/descodificación de descarga para JPSS-1/NOAA-20 y SNPP, y una configuración de desmodulación/descodificación de descarga para Aqua
- Un perfil de misión para JPSS-1/NOAA-20 y SNPP, y un perfil de misión para Aqua

Los valores y parámetros de los satélites de esta plantilla ya se han rellenado. Estos parámetros facilitan su uso AWS Ground Station inmediato con estos satélites. No necesita configurar sus propios valores para utilizarlos AWS Ground Station cuando utilice esta plantilla. Sin embargo, puede personalizar los valores para que la plantilla funcione para su caso de uso.

¿Dónde recibo los datos?

El grupo de puntos de enlace del flujo de datos se configura para que se utilice la interfaz de red de la instancia del receptor que crea parte de la plantilla. La instancia receptora usa Data Defender para recibir el flujo de datos desde AWS Ground Station el puerto definido por el punto final del flujo de datos. Una vez recibidos, los datos están disponibles para su consumo a través del puerto UDP 50000 en el adaptador de bucle invertido de la instancia del receptor. Para obtener más información sobre la configuración de un grupo de puntos finales de flujo de datos, consulte Grupo. AWS::GroundStation::DataflowEndpoint

AquaSnppJpssTerraDigPlantilla IF (banda estrecha)

La AWS CloudFormation plantilla nombrada `AquaSnppJpssTerraDigIF.yml` está diseñada para brindarle acceso rápido para comenzar a recibir datos digitalizados de frecuencia intermedia (DigiF) para los satélites Aqua, SNPP, JPSS-1/NOAA-20 y Terra. Contiene una instancia de Amazon EC2 y los AWS CloudFormation recursos necesarios para recibir datos de transmisión directa de DigiF sin procesar. Esta plantilla es un buen punto de partida para procesar los datos utilizando una radio definida por software (SDR).

Si no se incorporan satélites Aqua, SNPP, JPSS-1/NOAA-20 y Terra en la cuenta, consulte Incorporación de clientes.

> **Important**
>
> Es necesario detener la instancia de Amazon EC2 antes de aplicar la plantilla. Asegúrese de que la instancia esté detenida hasta que esté listo para usarla.

Puede acceder a la plantilla accediendo al bucket de S3 de incorporación del cliente. Tenga en cuenta que los enlaces siguientes utilizan un bucket de S3 regional. Cambie `<us-west-2>` a la región en la que va a crear la AWS CloudFormation pila.

> **Note**
>
> Las siguientes instrucciones usan YAML. Sin embargo, las plantillas están disponibles en formato YAML y JSON. Para usar JSON, reemplace `<.yml>` por `<.json>`.

Para descargar la plantilla mediante AWS CLI, utilice el siguiente comando:

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

La plantilla puede verse y descargarse en la consola desde la siguiente URL en su navegador:

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

Puede especificar la plantilla directamente en AWS CloudFormation el siguiente enlace:

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

¿Qué recursos define la plantilla?

La plantilla `AquaSnppJpssTerraDigIF` incluye los siguientes recursos:

- Función de servicio de entrega de datos: AWS Ground Station asume esta función para crear o eliminar ENI en su cuenta con el fin de transmitir datos.
- Instancia de recepción (opcional): la instancia de Amazon EC2 que enviará o recibirá datos hacia/desde su satélite mediante. AWS Ground Station

  - Grupo de seguridad de la instancia: el grupo de seguridad de su instancia de Amazon EC2.
  - Rol de instancia: el rol de su instancia de Amazon EC2.
  - Perfil de instancia: el perfil de instancia de la instancia de Amazon EC2.
  - Grupo con ubicación en clúster: el grupo de ubicación en el que se lanza su instancia de Amazon EC2.
- Grupo de seguridad de punto final de Dataflow: el grupo de seguridad al que AWS Ground Station pertenece la interfaz de red elástica creada por. De forma predeterminada, este grupo de seguridad permite AWS Ground Station transmitir tráfico a cualquier dirección IP de la VPC. Puede modificar esto de forma que limite el tráfico a un conjunto específico de direcciones IP.
- Interfaz de red de instancias receptoras: una interfaz de red elástica que proporciona una dirección IP fija AWS Ground Station a la que conectarse. Esto se asocia a la instancia del receptor en `eth1`.
- Receiver Instance Interface Attachment (Accesorio de interfaz de instancia de receptor): interfaz de red elástica que se conecta a la instancia de Amazon EC2.
- Activadores de CloudWatch eventos (opcionales): AWS Lambda función que se activa mediante CloudWatch eventos enviados AWS Ground Station antes y después de un contacto. La AWS Lambda función iniciará y, opcionalmente, detendrá la instancia de Receiver.
- Verificación EC2 para contactos (opcional): la opción de usar Lambda para configurar un sistema de verificación de las instancias de Amazon EC2 para los contactos con notificaciones de SNS. Es importante tener en cuenta que esto puede conllevar gastos en función del uso actual.
- Grupo de puntos finales del flujo de datos: el grupo de puntos finales del AWS Ground Station flujo de datos que define los puntos finales que se utilizan para enviar o recibir datos hacia/desde su satélite. Como parte de la creación del grupo de puntos finales del flujo de datos, AWS Ground Station crea una interfaz de red elástica en su cuenta para transmitir datos.
- Config de rastreo: la configuración AWS Ground Station de rastreo define cómo el sistema de antenas rastrea tu satélite a medida que se mueve por el cielo.
- Downlink DigIF Endpoint Config (Configuración de punto de enlace DigIF de enlace de bajada): un punto de enlace definido utilizado para enlace de bajada de datos desde su satélite.
- Ground Station Amazon Machine Image Retrieval Lambda: la opción de seleccionar el software que se instalará en la instancia y la AMI que prefiera. Las opciones de software incluyen `DDX 2.6.2 Only` y `DDX 2.6.2 with qRadio 3.6.0`. Estas opciones seguirán ampliándose a medida que se publiquen actualizaciones y características adicionales del software.

Además, la plantilla proporciona los siguientes recursos para los satélites Aqua, SNPP, JPSS-1/NOAA-20 y Terra:

- Una configuración de antena DigIF de enlace de bajada para Aqua, SNPP, JPSS-1/NOAA-20 y Terra.
- Un perfil de misión para JPSS-1/NOAA-20 y SNPP, un perfil de misión para Aqua y un perfil de misión para Terra.

Los valores y parámetros de los satélites de esta plantilla ya se han rellenado. Estos parámetros facilitan su uso AWS Ground Station inmediato con estos satélites. No necesita configurar sus propios valores para utilizarlos AWS Ground Station cuando utilice esta plantilla. Sin embargo, puede personalizar los valores para que la plantilla funcione para su caso de uso.

¿Dónde recibo los datos?

El grupo de puntos de enlace del flujo de datos se configura para que se utilice la interfaz de red de la instancia del receptor que crea parte de la plantilla. La instancia receptora usa Data Defender para recibir el flujo de datos desde AWS Ground Station el puerto definido por el punto final del flujo de datos. Una vez recibidos, los datos están disponibles para su consumo a través del puerto UDP 50000 en el adaptador de bucle invertido de la instancia del receptor. Para obtener más información sobre la configuración de un grupo de puntos finales de flujo de datos, consulte Grupo. AWS::GroundStation::DataflowEndpoint

Plantilla DigiF de banda ancha por satélite de transmisión directa (banda ancha)

La AWS CloudFormation plantilla nombrada `DirectBroadcastSatelliteWbDigIfEc2DataDelivery.yml` está diseñada para brindarle acceso rápido para comenzar a recibir datos digitalizados de frecuencia intermedia (DigiF) para los satélites Aqua, SNPP, JPSS-1/NOAA-20 y Terra. Contiene una instancia de Amazon EC2 y los AWS CloudFormation recursos necesarios para recibir datos de transmisión directa de DigiF sin procesar. Esta plantilla es un buen punto de partida para procesar los datos utilizando una radio definida por software (SDR).

Si no se incorporan satélites Aqua, SNPP, JPSS-1/NOAA-20 y Terra en la cuenta, consulte Incorporación de clientes.

> **Important**
>
> Es necesario detener la instancia de Amazon EC2 antes de aplicar la plantilla. Asegúrese de que la instancia esté detenida hasta que esté listo para usarla.

Puede acceder a la plantilla accediendo al bucket de S3 de incorporación del cliente. Tenga en cuenta que los enlaces siguientes utilizan un bucket de S3 regional. Cambie `<us-west-2>` a la región en la que va a crear la AWS CloudFormation pila.

> **Note**
>
> Las siguientes instrucciones usan YAML. Sin embargo, las plantillas están disponibles en formato YAML y JSON. Para usar JSON, reemplace `<.yml>` por `<.json>`.

Para descargar la plantilla mediante AWS CLI, utilice el siguiente comando:

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

La plantilla puede verse y descargarse en la consola desde la siguiente URL en su navegador:

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

Puede especificar la plantilla directamente en AWS CloudFormation el siguiente enlace:

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

¿Qué recursos define la plantilla?

La plantilla `DirectBroadcastSatelliteWbDigIfEc2DataDelivery` incluye los siguientes recursos:

- Instancia de recepción (opcional): la instancia de Amazon EC2 que enviará o recibirá datos hacia/desde su satélite mediante. AWS Ground Station

  - Grupo de seguridad de la instancia: el grupo de seguridad de su instancia de Amazon EC2.
  - Rol de instancia: el rol de su instancia de Amazon EC2.
  - Perfil de instancia: el perfil de instancia de la instancia de Amazon EC2.
  - Grupo con ubicación en clúster: el grupo de ubicación en el que se lanza su instancia de Amazon EC2.
- Clave de entrega de datos: AWS KMS clave utilizada para cifrar los flujos de datos.
- Función clave de Ground Station: la función de IAM que AWS Ground Station asumirá para acceder y utilizar la AWS KMS clave para descifrar los flujos de datos
- Política de acceso a la clave de Ground Station: la política de IAM que define las acciones que AWS Ground Station se pueden realizar con la clave de entrega de datos
- Interfaz de red elástica de instancia de receptor: (condicional) Se crea una interfaz de red elástica en la subred especificada PublicSubnetIdsi se proporciona. Esto es obligatorio si la instancia del receptor está en una subred privada. La interfaz de red elástica se asociará a la EIP y se adjuntará a la instancia receptora.
- IP elástica de la instancia de recepción: una IP elástica a la que AWS Ground Station se conectará. Esto se conecta a la instancia del receptor o a la interface de red elástica.
- Una de las siguientes asociaciones de IP elástica:
  - Asociación de instancia de receptor a IP elástica: asociación de la IP elástica a la instancia de receptor, si no PublicSubnetIdse especifica. Esto requiere que haga SubnetIdreferencia a una subred pública.
  - Interfaz de red elástica de instancia de receptor a asociación de IP elástica: asociación de la IP elástica a la interfaz de red elástica de la instancia de recepción, si PublicSubnetIdse especifica.
- Activadores de CloudWatch eventos (opcionales): AWS Lambda función que se activa mediante CloudWatch eventos enviados AWS Ground Station antes y después de un contacto. La AWS Lambda función iniciará y, opcionalmente, detendrá la instancia de Receiver.
- Verificación EC2 para contactos (opcional): la opción de usar Lambda para configurar un sistema de verificación de las instancias de Amazon EC2 para los contactos con notificaciones de SNS. Es importante tener en cuenta que esto puede conllevar gastos en función del uso actual.
- Grupo de puntos finales del flujo de datos: el grupo de puntos finales del AWS Ground Station flujo de datos que define los puntos finales que se utilizan para enviar o recibir datos hacia/desde su satélite.
- Config de rastreo: la configuración AWS Ground Station de rastreo define cómo el sistema de antenas rastrea tu satélite a medida que se mueve por el cielo.

Además, la plantilla proporciona los siguientes recursos para los satélites Aqua, SNPP, JPSS-1/NOAA-20 y Terra:

- Una configuración de enlace descendente para JPSS-1/NOAA-20 y SNPP, una configuración de enlace descendente para Aqua y una configuración de enlace descendente para Terra.
- Un perfil de misión para JPSS-1/NOAA-20 y SNPP, un perfil de misión para Aqua y un perfil de misión para Terra.

Los valores y parámetros de los satélites de esta plantilla ya se han rellenado. Estos parámetros facilitan su uso AWS Ground Station inmediato con estos satélites. No necesita configurar sus propios valores para utilizarlos AWS Ground Station cuando utilice esta plantilla. Sin embargo, puede personalizar los valores para que la plantilla funcione para su caso de uso.

¿Dónde recibo los datos?

El grupo de puntos de enlace del flujo de datos se configura para que se utilice la interfaz de red de la instancia del receptor que crea parte de la plantilla. La instancia receptora usa el AWS Ground Station agente para recibir el flujo de datos desde AWS Ground Station el puerto definido por el punto final del flujo de datos. Para obtener más información sobre la configuración de un grupo de puntos finales de flujo de datos, consulte Grupo. AWS::GroundStation::DataflowEndpoint Para obtener más información sobre el AWS Ground Station agente, consulte. AWS Ground Station Guía del usuario del agente

Crear una instancia de Amazon EC2

> **Note**
>
> No es necesario ni recomendable crear los recursos AWS Ground Station (incluidas las instancias de Amazon EC2) de forma manual, ya que se AWS Ground Station proporcionan AWS CloudFormation plantillas prediseñadas para ello (consulte Paso 3: Elige y personaliza una plantilla AWS CloudFormation para obtener más información). Si el uso de AWS CloudFormation plantillas no funciona para su caso de uso, continúe leyendo.

AWS Ground Station proporciona AMI de Amazon EC2 que vienen precargadas con el software necesario para realizar la entrega de datos en una instancia de Amazon EC2 para la entrega de datos de banda estrecha o banda ancha. DigIf

> **Important**
>
> Los satélites deben estar integrados en el servicio para poder acceder a las AMI. AWS Ground Station

AMI Amazon EC2 con DataDefender

Esta AMI viene preinstalada con el DataDefender software y se utiliza para los contactos de enlace descendente de entrega de datos de banda estrecha.

El esquema de nomenclatura de esta AMI es `groundstation-al2-ddx$DDX_VERSION-ami-$DATE_PUBLISHED`. Se publica una nueva AMI DDX poco después de la publicación de una nueva AMI AL2 de Amazon EC2. Si AWS Ground Station decide admitir una nueva versión del DataDefender software, se publicará una nueva AMI con la versión actualizada.

Selección de una AWS Ground Station AMI con DataDefender

Puede acceder a la AWS Ground Station AMI a través de la pestaña AMI de la consola Amazon EC2. Una vez en esa página, podrá acceder a las AMI con el filtro Imágenes privadas.

Se recomienda ordenar las AMI por la fecha de publicación y utilizar la AMI publicada más recientemente denominada `groundstation-al2-ddx$DDX_VERSION-ami-$DATE_PUBLISHED`.

AMI de Amazon EC2 con el agente AWS Ground Station

Esta AMI viene preinstalada con el AWS Ground Station agente y se utiliza para los contactos de enlace descendente DigiF de banda ancha.

El esquema de nomenclatura de esta AMI es `groundstation-al2-gs-agent-ami-*` donde * es la fecha en que se creó la AMI. Una nueva AMI de AWS Ground Station agente se publica poco después de la publicación de una nueva AMI AL2 de Amazon EC2 o cuando se publica una nueva versión AWS Ground Station del RPM de agente.

Para obtener más información sobre el AWS Ground Station agente, consulte. AWS Ground Station Guía del usuario del agente

Selección de un AWS Ground Station agente (AMI)

Puede acceder a la AMI del AWS Ground Station agente a través de la pestaña AMI de la consola Amazon EC2. Una vez en esa página, podrá acceder a las AMI con el filtro Imágenes privadas.

Se recomienda ordenar las AMI por la fecha de publicación y utilizar la AMI publicada más recientemente denominada `groundstation-al2-gs-agent-ami-$DATE_PUBLISHED`.

Paso 4: Configurar una pila AWS CloudFormation

Tras elegir la plantilla que mejor se adapte a su caso de uso, configure una AWS CloudFormation pila. Los recursos que se crean en este procedimiento se configuran en la región en la que se encuentra al crearlos. Esto incluye el perfil de la misión y sus propiedades que determinan en qué región se entregan los datos.

1. En AWS Management Console, elija Servicios > CloudFormation.
2. En el panel de navegación, seleccione Stacks (Pilas). Elija Create stack (Crear pila) > With new resources (standard) (Con nuevos recursos [estándar]).
3. En la página Create Stack (Crear pila), especifique la plantilla que ha seleccionado en the section called “Elija una plantilla” mediante una de las siguientes acciones.

    a. Seleccione la URL de Amazon S3 como el origen de plantilla y copie y pegue la URL de la plantilla que desea utilizar en URL de Amazon S3. A continuación, elija Siguiente.

    b. Seleccione Upload a template file (Cargar un archivo de plantilla) como el origen de plantilla y elija Choose File (Seleccionar archivo). Cargue la plantilla que ha descargado en the section called “Elija una plantilla”. A continuación, elija Siguiente.
4. En la página de detalles Specify stack (Especificar pila), realice los siguientes cambios:

    a. Introduzca un nombre en la casilla Stack Name (Nombre de pila). Recomendamos utilizar un nombre sencillo para reducir las posibilidades de que se produzcan errores en el futuro.

    b. Para CloudWatchEventActions, elija qué acciones realizar para que los CloudWatch eventos se activen antes y después de un contacto.

    c. Para CreateEC2 VerificationForContacts, elija si desea o no configurar un sistema de verificación (mediante Lambda) de sus instancias EC2 para los contactos con notificaciones de SNS. Es importante tener en cuenta que esto puede conllevar gastos en función del uso actual.

    d. Para CreateReceiverInstance, elija si desea crear o no una instancia de receptor Amazon EC2.

    e. Elija la clave de SSH que ha creado en the section called “Paso 1: Crear un par de claves SSH de EC2”.

    f. Elija la SubnetIdinstancia en la que desea crear su instancia de Amazon EC2.

Si usa el AWS Ground Station agente, se requiere una subred pública, ya sea para colocar la instancia o una interfaz de red elástica; si especifica una subred privada SubnetIden la que colocar la instancia, también debe especificar una subred pública PublicSubnetId(consulte a continuación) para usarla con el agente. AWS Ground Station

Para los casos de uso que no sean agentes, recomendamos colocar la instancia de Amazon EC2 en una subred privada como práctica recomendada, aunque no es obligatorio. Puede utilizar Linux Bastion Hosts on the AWS Cloud: Quick Start Reference Deployment para crear automáticamente una subred privada si no hay configurado ya su cuenta con una en the section called “Paso 2: Configurar la VPC”.

> **Note**
>
> La organización debe tener otra subred dedicada a la instancia de Amazon EC2.

g. (Opcional) Elija esta opción PublicSubnetIdpara usarla solo si usa el AWS Ground Station agente con una instancia de una subred privada. Esto es obligatorio si especificó una subred privada en. SubnetId

   Esta subred debe estar en su cuenta en la misma zona de disponibilidad que la especificada por. SubnetId Si proporciona una, PublicSubnetIdse creará una interfaz de red elástica en la subred pública proporcionada, adjunta a la instancia. Esta interfaz se utiliza para que el AWS Ground Station agente acceda a la red desde su instancia, que se encuentra en la subred privada especificada en. SubnetId

h. Elija la pila de VPC que ha creado en the section called “Paso 2: Configurar la VPC”.

i. Elija Siguiente.

5. Configure las opciones de pila y las opciones avanzadas de la instancia de Amazon EC2.

   a. Añada cualquier etiqueta y permiso en las secciones Tags (Etiquetas) y Permissions (Permisos).

   b. Realice cualquier cambio en la Stack policy (Política de pila), la Rollback configuration (Configuración de reversión), las Notification options (Opciones de notificación) y las Stack creation options (Opciones de creación de pilas).

   c. Elija Siguiente.

6. Después de revisar los detalles de la pila, seleccione el reconocimiento Capabilities (Capacidades) y seleccione Create stack (Crear pila).

Paso 5: instalar y configurar la radio/el procesador FE

La instancia Amazon EC2 definida en la AWS CloudFormation plantilla no tiene un procesador front-end (FE) ni una radio definida por software (SDR) instalados de forma predeterminada. Debe instalar un procesador FE o SDR para procesar los paquetes VITA-49 transmitidos a/desde el sistema de antena de AWS Ground Station .

La instalación y configuración de su procesador FE o SDR dependen del procesador FE o SDR que utilice. La instalación de un procesador FE o SDR no entra dentro del ámbito de esta guía de usuario.

Para instalar y configurar la radio/el procesador FE, póngase en contacto con AWS Support.

> **Important**
>
> Se recomienda ejecutar el procesador FE o el SDR en las instancias creadas por la AWS CloudFormation plantilla para garantizar las ventajas de los flujos de datos DTLS hacia/desde Data Defender.

Siguientes pasos

Su AWS Ground Station cuenta y sus recursos ya están configurados y listos para su uso. Estos recursos están disponibles para su uso en la AWS Ground Station consola, donde puede introducir datos de satélites, identificar las ubicaciones de las antenas, comunicarse y programar la hora de la antena para satélites seleccionados. También puede comenzar a utilizar diferentes herramientas para supervisar la actividad y configurar alarmas.

Utilice los temas siguientes para obtener más información.

- Enumeración y reserva de contactos
- Monitorización AWS Ground Station

Uso del servicio de entrega de datos entre regiones

La AWS Ground Station función de entrega de datos entre regiones le brinda la flexibilidad de enviar sus datos desde una antena a una instancia de Amazon EC2 en su región de AWS. La entrega de datos entre regiones está disponible actualmente en todas las regiones AWS Ground Station admitidas al recibir sus datos de contacto en un bucket de Amazon S3. Solo está disponible en las siguientes antenna-to-destination regiones cuando se utiliza la entrega de datos a Amazon EC2:

- Región EE. UU. Este (Ohio) (us-east-2) a región EE. UU. Oeste (Oregón) (us-west-2)
- Región EE. UU. Oeste (Oregón) (us-west-2) a región EE. UU. Este (Ohio) (us-east-2)

Para utilizar la entrega de datos entre regiones, debe tener configurada una AWS CloudFormation plantilla. Para obtener más información sobre cómo elegir y personalizar AWS CloudFormation plantillas, consulte. Paso 3: Elige y personaliza una plantilla AWS CloudFormation

Utilice los temas siguientes para utilizar la entrega de datos entre regiones de AWS Ground Station.

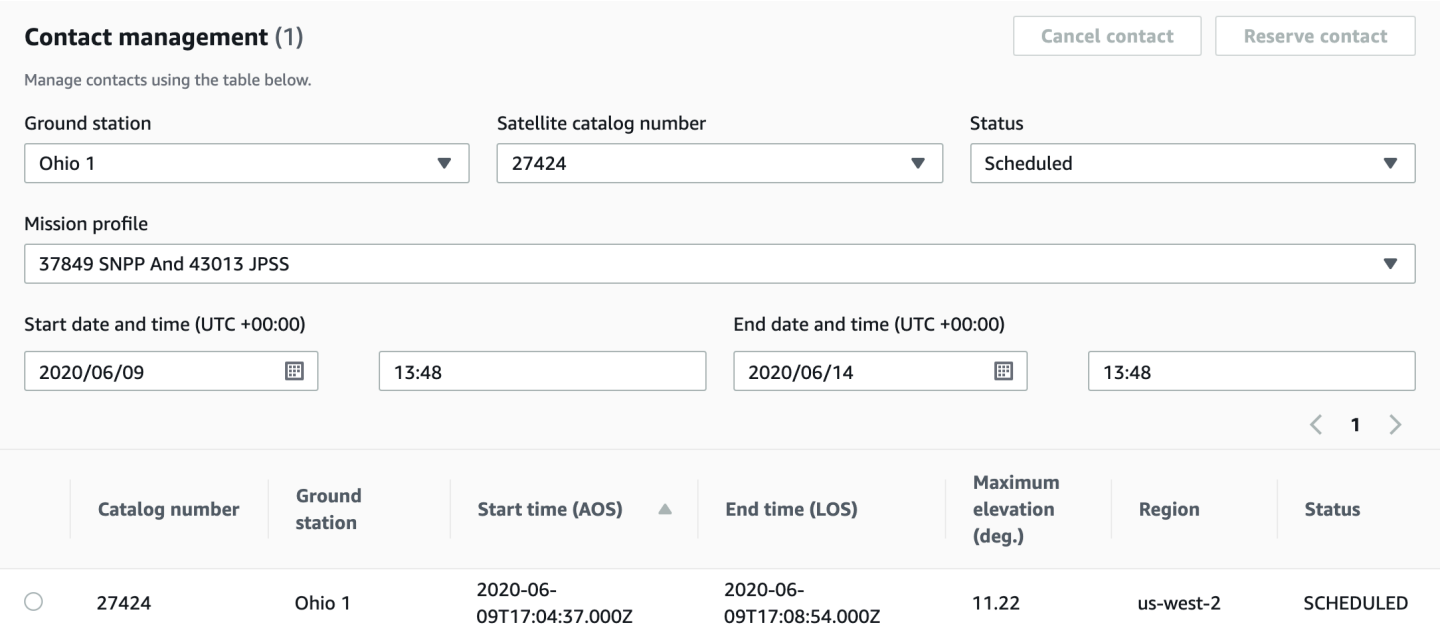
Temas

- Para utilizar la entrega de datos entre regiones en la consola
- Para utilizar la entrega de datos entre regiones con la CLI de AWS

Para utilizar la entrega de datos entre regiones en la consola

Cuando reserves un contacto en la AWS Ground Station consola, elige el perfil de misión que esté configurado para enviar los datos de contacto a la región que desees. Asegúrese de que todos los parámetros son correctos y elija Reservar contacto. Si no ve el perfil de misión deseado en la consola, compruebe que ha creado el perfil de misión en la región en la que está viendo la consola.

Después de reservar el contacto, puede ver los contactos programados para verificar que ha programado la entrega de datos entre regiones consultando la ubicación de la antena de la estación terrestre y la región de destino. La imagen siguiente muestra un contacto que está programado para la entrega de datos entre regiones. El contacto está configurado para usar las antenas de la estación terrestre de Ohio y entregar datos a Oregón.



Para utilizar la entrega de datos entre regiones con la CLI de AWS

Cuando reserves un contacto en AWS CLI, elige el perfil de misión que esté configurado para enviar los datos de contacto a la región que desees. Especifique el ARN del perfil de misión que desee con `--mission-profile-arn <value>`. Asegúrese de que todos los parámetros son correctos y ejecute el comando. Si no ve el ARN del perfil de misión deseado al consultar y mostrar contactos, compruebe que ha creado el perfil de misión en la región en la que está ejecutando la AWS CLI.

Después de reservar el contacto, puede ver los contactos programados para verificar que ha programado la entrega de datos entre regiones consultando la ubicación de la antena de la estación terrestre y la región de destino. La siguiente salida muestra un contacto que está programado para la entrega de datos entre regiones. El contacto está configurado para usar las antenas de la estación terrestre de Ohio y entregar los datos a Oregón.


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

Monitorización AWS Ground Station

La monitorización es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de AWS Ground Station. AWS proporciona las siguientes herramientas de supervisión para observar AWS Ground Station, informar cuando algo va mal y tomar medidas automáticas cuando sea necesario.

- Amazon CloudWatch Events ofrece una transmisión casi en tiempo real de los eventos del sistema que describen los cambios en AWS los recursos. CloudWatch Events permite la computación automatizada basada en eventos, ya que puede escribir reglas que vigilen determinados eventos y activen acciones automatizadas en otros AWS servicios cuando se producen estos eventos. Para obtener más información sobre Amazon CloudWatch Events, consulte la Guía del usuario de Amazon CloudWatch Events.
- AWS EventBridge Events ofrece una transmisión casi en tiempo real de los eventos del sistema que describen los cambios en AWS los recursos. EventBridge Events permite automatizar la informática basada en eventos, ya que puede escribir reglas que vigilen determinados eventos y activen acciones automatizadas en otros AWS servicios cuando estos se producen. Para obtener más información sobre EventBridge los eventos, consulte la Guía del usuario de Amazon EventBridge Events.
- AWS CloudTrailcaptura las llamadas a la API y los eventos relacionados realizados por su AWS cuenta o en su nombre y entrega los archivos de registro a un bucket de Amazon S3 que especifique. También puede identificar qué usuarios y cuentas llamaron a AWS, la dirección IP de origen de las llamadas y el momento en que se hicieron. Para obtener más información al respecto AWS CloudTrail, consulte la Guía AWS CloudTrail del usuario.
- Amazon CloudWatch Metrics captura las métricas de tus contactos programados cuando las utilizas AWS Ground Station. CloudWatch Las métricas le permiten analizar los datos en función del canal, la polarización y la identificación del satélite para identificar la intensidad de la señal y los errores en sus contactos. Para obtener más información, consulta Uso de Amazon CloudWatch Metrics.
- AWS se Notificaciones de usuario puede usar para configurar canales de entrega para recibir notificaciones sobre AWS Ground Station eventos. Recibirá una notificación cuando un evento coincida con una regla que especifique. Puede recibir notificaciones de eventos a través de varios canales, como correo electrónico, notificaciones por chat de AWS Chatbot o notificaciones de inserción de AWS Console Mobile Application. También puede ver las notificaciones en el Centro

de notificaciones de la consola. Las Notificaciones de usuario admiten la agregación, lo que puede reducir el número de notificaciones que recibe durante eventos específicos.

Utilice los temas siguientes para monitorear AWS Ground Station.

Temas

- Automatizar AWS Ground Station con eventos
- Registrar llamadas a la AWS Ground Station API con AWS CloudTrail
- Métricas con Amazon CloudWatch

Automatizar AWS Ground Station con eventos

> **Note**
>
> En este documento se utiliza el término «evento» en todas partes. CloudWatch Los eventos y EventBridge son el mismo servicio y API subyacentes. Con cualquiera de los dos servicios se pueden crear reglas para hacer coincidir los eventos entrantes y dirigirlos a los objetivos para su procesamiento.

Los eventos le permiten automatizar sus AWS servicios y responder automáticamente a los eventos del sistema, como los problemas de disponibilidad de las aplicaciones o los cambios en los recursos. Los eventos de AWS los servicios se entregan casi en tiempo real. Puede crear reglas sencillas para indicar qué eventos le resultan de interés, así como qué acciones automatizadas se van a realizar cuando un evento cumple una de las reglas. Entre las acciones que se pueden activar automáticamente se incluyen las siguientes:

- Invocar una función AWS Lambda
- Invocar Ejecutar comando de Amazon EC2
- Desviar el evento a Amazon Kinesis Data Streams
- Activar una máquina de AWS Step Functions estados
- Notificar un tema o una cola de Amazon SNS AWS SMS

Algunos ejemplos del uso de eventos con incluyen: AWS Ground Station

- Invocar una función de Lambda para automatizar el inicio y la detención de instancias de Amazon EC2 en función del estado del evento.
- Publicar en un tema de Amazon SNS cada vez que un contacto cambie de estado. Estos temas se pueden configurar para enviar avisos por correo electrónico al inicio o al final de los contactos.

Para obtener más información, consulte la Guía del usuario de Amazon CloudWatch Events o la Guía del usuario de Amazon EventBridge Events.

Eventos de ejemplo

> **Note**
>
> Todos los eventos generados por AWS Ground Station tienen "aws.groundstation" como valor de "source".

Cambio de estado del contacto de Ground Station

Si desea realizar una acción concreta cuando un contacto próximo cambie de estado, puede configurar una regla de para automatizar esta acción. Esto es útil para cuando desee recibir notificaciones acerca de los cambios de estado del contacto. Si quieres cambiar la fecha de recepción de estos eventos, puedes modificar el perfil de tu misión contactPrePassDurationSecondsy contactPostPassDurationSeconds. Los eventos se envían a la región desde la que se haya programado el contacto.

A continuación, se proporciona un ejemplo.

```
{
    "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"
}
```

Los valores posibles para `contactStatus` se definen en the section called “Estado de los contactos de Ground Station”.

Cambio de estado del grupo de puntos de enlace del flujo de datos de Ground Station

Si desea realizar una acción cuando se utiliza el grupo de puntos de enlace del flujo de datos para recibir datos, puede configurar una regla de para automatizar esta acción. Esto le permitirá realizar diferentes acciones en respuesta a los cambios de estado del grupo de puntos de enlace del flujo de datos. Si desea cambiar la fecha de recepción de estos eventos, utilice un grupo de puntos finales de flujo de datos con un y diferente contactPrePassDurationSeconds. contactPostPassDurationSeconds Este evento se enviará a la región del grupo de puntos de enlace del flujo de datos.

A continuación, se proporciona un ejemplo.

```
{
    "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"
}
```

Los posibles estados de `dataflowEndpointGroupState` son `PREPASS`, `PASS`, `POSTPASS` y `COMPLETED`.

Cambio de estado de las efemérides de Ground Station

Si desea realizar una acción cuando una efeméride cambia de estado, puede configurar una regla para automatizar esta acción. Esto le permite realizar diferentes acciones como respuesta al cambio de estado de una efeméride. Por ejemplo, puede realizar una acción si una efeméride ha completado la validación y ahora está `ENABLED` La notificación de este evento se enviará a la región en la que se cargaron las efemérides.

A continuación, se proporciona un ejemplo.

```
    {
    "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"
    }
    }
```

Los posibles estados de `ephemerisStatus` son `ENABLED`, `VALIDATING`, `INVALID`, `ERROR`, `DISABLED`, `EXPIRED`

Registrar llamadas a la AWS Ground Station API con AWS CloudTrail

AWS Ground Station está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en AWS Ground Station. CloudTrail captura todas las llamadas a la API AWS Ground Station como eventos. Las llamadas capturadas incluyen llamadas desde la AWS Ground Station consola y llamadas en código a las operaciones de la AWS Ground Station API. Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos para AWS Ground Station. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por usted CloudTrail, puede determinar a AWS Ground Station qué dirección IP se realizó la solicitud, quién la realizó, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, consulte la Guía AWS CloudTrail del usuario.

AWS Ground Station Información en CloudTrail

CloudTrail está habilitada en su AWS cuenta al crear la cuenta. Cuando se produce una actividad en AWS Ground Station, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puedes ver, buscar y descargar los eventos recientes en tu AWS cuenta. Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos.

Para tener un registro continuo de los eventos de tu AWS cuenta, incluidos los eventos de tu cuenta AWS Ground Station, crea una ruta. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las regiones de AWS. La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros AWS servicios para analizar más a

fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- CloudTrail Integraciones y servicios compatibles
- Configuración de las notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de CloudTrail registro de varias regiones y recibir archivos de CloudTrail registro de varias cuentas

Todas AWS Ground Station las acciones se registran CloudTrail y se documentan en la referencia de la AWS Ground Station API. Por ejemplo, las llamadas a `CancelContact` y `ListConfigs` las acciones generan entradas en los archivos de CloudTrail registro. `ReserveContact`

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario root o AWS Identity and Access Management (IAM).
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro AWS servicio.

Para obtener más información, consulte el elemento CloudTrail UserIdentity.

Descripción AWS Ground Station de las entradas de los archivos de registro

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que demuestra la `ReserveContact` acción.

Ejemplo: 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 con Amazon CloudWatch

Durante un contacto, captura y envía AWS Ground Station automáticamente los datos CloudWatch para su análisis. Tus datos se pueden ver en un gráfico o como código fuente en la CloudWatch consola de Amazon. Para obtener más información sobre el acceso y CloudWatch las métricas, consulta Uso de Amazon CloudWatch Metrics.

AWS Ground Station Métricas y dimensiones

¿Qué métricas están disponibles?

Las siguientes métricas están disponibles en AWS Ground Station.

Métrica	Descripción
`AzimuthAngle`	El ángulo azimut de la antena. El norte verdadero está a 0 grados y el este a 90 grados. Unidades: grados
`BitErrorRate`	Tasa de error en bits en un número determinado de transmisiones de bits. El ruido, la distorsión o las interferencias causan los errores de bits. Unidades: errores de bits por unidad de tiempo
`BlockErrorRate`	La tasa de errores de los bloques en un número dado de bloques recibidos. Las interferencias causan los errores de bloque. Unidades: Bloques erróneos/Número total de bloques

Métrica	Descripción
CarrierFrequencyRecovery_Cn0	Relación portadora/densidad de ruido por unidad de ancho de banda. Unidades: decibelio-hercio (dB-HZ)
CarrierFrequencyRecovery_Locked	Se establece en 1 cuando el bucle de recuperación de frecuencia portadora del desmodulador está bloqueado y en 0 cuando está desbloqueado. Unidades: sin unidades
CarrierFrequencyRecovery_OffsetFrequency_Hz	El desfase entre el centro estimado de la señal y la frecuencia central ideal. Esto se debe al desplazamiento Doppler y al desfase del oscilador local entre la nave espacial y el sistema de antenas. Unidades: hercios (Hz)
ElevationAngle	El ángulo de elevación de la antena. El horizonte está a 0 grados y el cenit a 90 grados. Unidades: grados
Es/N0	Relación entre la energía por símbolo y la densidad espectral de potencia del ruido. Unidades: decibelios (dB)
ReceivedPower	La intensidad de la señal medida en el desmodulador/descodificador. Unidades: decibelios relativos a milivatios (dBm)
SymbolTimingRecovery_ErrorVectorMagnitude	La magnitud del vector de error entre los símbolos recibidos y los puntos de constelación ideales. Unidades: porcentaje

Métrica	Descripción
`SymbolTimingRecovery_Locked`	Se establece en 1 cuando el bucle de recuperación de temporización de símbolos del desmodulador está bloqueado y en 0 cuando está desbloqueado. Unidades: sin unidades
`SymbolTimingRecovery_Offset SymbolRate`	El desfase entre la tasa de símbolos estimada y la tasa de símbolos de la señal ideal. Esto se debe al desplazamiento Doppler y al desfase del oscilador local entre la nave espacial y el sistema de antenas. Unidades: Símbolos/segundo

¿Para qué dimensiones se utilizan AWS Ground Station?

Puede filtrar AWS Ground Station los datos mediante las siguientes dimensiones.

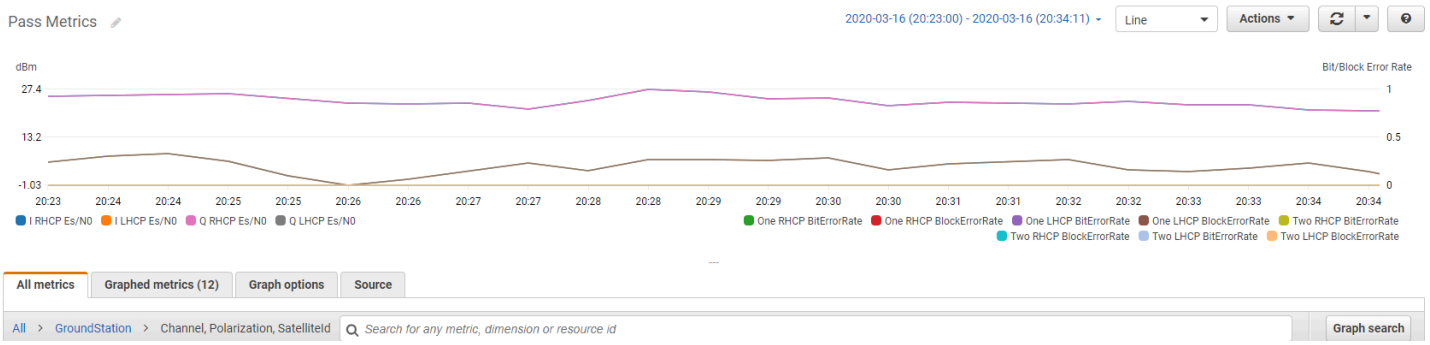
Dimensión	Descripción
`Channel`	Los canales para cada contacto incluyen Uno, Dos, I (en fase) y Q (cuadratura).
`Polarization`	La polarización para cada contacto incluye LHCP (Izquierda Circular Polarizada) o RHCP (Derecha Circular Polarizada).
`SatelliteId`	El ID del satélite contiene el ARN del satélite para sus contactos.

Visualización de métricas

Al consultar las métricas gráficas, es importante tener en cuenta que la ventana de agregación determina cómo se mostrarán las métricas. Cada métrica de un contacto se puede mostrar como datos por segundo durante tres horas después de la recepción de los datos. CloudWatch Metrics agregará tus datos como datos por minuto una vez transcurrido ese período de 3 horas. Si necesitas

ver tus métricas en una medición de datos por segundo, te recomendamos que consultes tus datos en un periodo de 3 horas tras su recepción o que los mantengas fuera de CloudWatch Metrics.

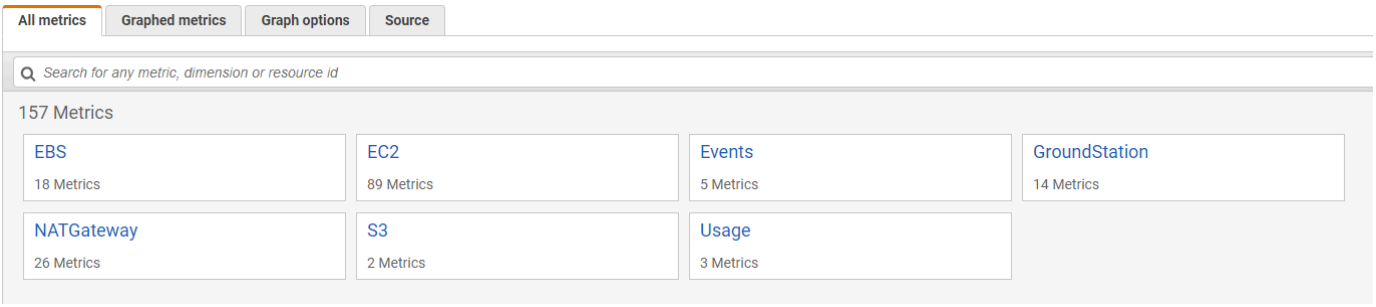
Además, los datos capturados en los primeros 60 segundos no contendrán suficiente información para producir métricas significativas y es probable que no se muestren. Para consultar las métricas significativas, se recomienda consultar los datos después de 60 segundos.



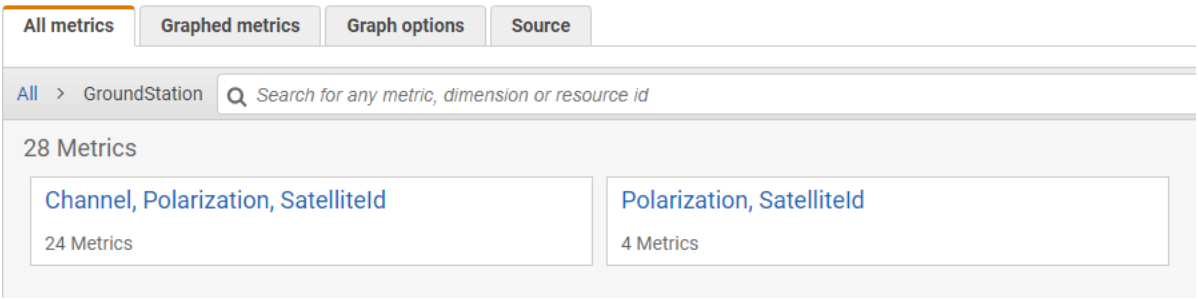
Para obtener más información sobre la representación gráfica de AWS Ground Station las métricas CloudWatch, consulta Cómo graficar las métricas.

Para consultar las métricas desde la consola de

1. Abra la consola de AWS CloudFormation.
2. En el panel de navegación, seleccione Métricas.
3. Seleccione el espacio de nombres de GroundStation.



4. Seleccione las dimensiones métricas que desee (por ejemplo, canal, polarización,. SatelliteId



5. La pestaña All metrics muestra todas las métricas para dicha dimensión en el espacio de nombres. Puede hacer lo siguiente:

   a. Para ordenar la tabla, utilice el encabezado de columna.

   b. Para representar gráficamente una métrica, seleccione la casilla de verificación asociada a la métrica. Para seleccionar todas las métricas, seleccione la casilla de verificación en la fila de encabezado de la tabla.

   c. Para filtrar por recurso, seleccione el ID de recurso y, a continuación, elija Add to search (Añadir a la búsqueda).

   d. Para filtrar por métrica, elija el nombre de la métrica y, a continuación, seleccione Add to search (Añadir a búsqueda).

Para ver las métricas mediante AWS CLI

1. Asegúrese de que AWS CLI esté instalado. Para obtener información sobre la instalación AWS CLI, consulte Instalación de la AWS CLI.
2. Cree un archivo JSON de configuración del CloudWatch agente. Para obtener instrucciones sobre cómo crear un archivo de configuración del CloudWatch agente, consulte Crear el archivo de configuración del CloudWatch agente.
3. Enumere las CloudWatch métricas disponibles ejecutándolas`aws cloudwatch list-metrics`.
4. Modifique el archivo JSON que creó en el paso 2 para que coincida con el `SatellitID` de sus métricas.

> **Note**
>
> No reduzca el `Period` campo a un valor inferior a 60. AWS Ground Station publica las métricas cada 60 segundos y no se devolverá ninguna métrica si se reduce el valor.

5. Ejecute `aws cloudwatch get-metric-data` con los períodos de tiempo de sus pases y el archivo JSON de configuración del CloudWatch agente. A continuación, se proporciona un ejemplo.

```
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
```

Las métricas se proporcionarán con marcas de tiempo de su contacto. A continuación, se proporciona un ejemplo de resultado de AWS Ground Station las métricas.

```
{
      “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”: []
}
```

Solución de problemas

La siguiente documentación puede ayudarle a solucionar problemas que pueden impedir que un AWS Ground Station contacto se complete correctamente.

Temas

Solución de problemas de contactos que envían datos a Amazon EC2

Si no puede completar correctamente un AWS Ground Station contacto, tendrá que comprobar que la instancia de Amazon EC2 se está ejecutando, comprobar que Data Defender se está ejecutando y comprobar que la transmisión de Data Defender está configurada correctamente.

Requisito previo

Los siguientes procedimientos asumen que ya se ha configurado una instancia de Amazon EC2. Para configurar una instancia de Amazon EC2 en AWS Ground Station, consulte Introducción.

Paso 1: Compruebe que la instancia EC2 está en ejecución

1. Busque la instancia de Amazon EC2 que se utilizó pcon el contacto cuyo problema está solucionando. Utilice los siguientes pasos:

   a. En su CloudFormationpanel de control, seleccione la pila que contiene su instancia de Amazon EC2.

   b. Seleccione la pestaña Recursos y localice su instancia de Amazon EC2 en la columna Logical ID. Asegúrese de que la instancia se ha creado en la columna Status (Estado).

   c. En la columna ID física, seleccione el enlace de su instancia de Amazon EC2. Esto le llevará a la consola de administración de Amazon EC2.

2. En la consola de administración de Amazon EC2, asegúrese de que el estado de su instancia de Amazon EC2 se está ejecutando.

3. Si la instancia se está ejecutando, continúe en el paso siguiente. Si la instancia no está en ejecución, iníciela siguiendo este paso.

   - Con su instancia de Amazon EC2 seleccionada, seleccione Actions (Acciones) > Instance State (Estado de la instancia) > Start (Iniciar).

Paso 2: Determinar el tipo de aplicación de flujo de datos utilizada

Si utiliza el AWS Ground Station agente para la entrega de datos, redirija a la sección AWS Ground Station Agente de solución de problemas.

De lo contrario, si utiliza la aplicación Data Defender (DDX), continúe en the section called “Paso 3: Comprobar que Data Defender está en ejecución”.

Paso 3: Comprobar que Data Defender está en ejecución

Para verificar el estado de Data Defender es necesario que se conecte a la instancia en Amazon EC2. Para obtener más información acerca de cómo conectarse a la instancia, consulte Conexión con la instancia de Linux.

El siguiente procedimiento contiene pasos para solucionar problemas utilizando comandos en un cliente SSH.

1. Abra un terminal o símbolo del sistema y conéctese a la instancia de Amazon EC2 mediante SSH. Reenvíe el puerto 80 del host remoto para poder ver la interfaz de usuario web de Data Defender. Los siguientes comandos indican cómo utilizar SSH para conectarse a una instancia de Amazon EC2 a través de un bastión con el reenvío de puertos habilitado.

   > **Note**
   >
   > Debe sustituir <SSH KEY>, <BASTION HOST> y <HOST> por su clave ssh, el nombre del host del bastión y el nombre del host de la instancia de Amazon EC2 específicos.

   Para 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>
   ```

Para 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. Compruebe que Data Defender (también llamado DDX) está en ejecución buscando con grep en la salida un proceso en ejecución denominado ddx. A continuación, se muestra el comando para buscar con grep un proceso en ejecución y una salida de ejemplo correcta.

```
[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
```

   Si Data Defender se está ejecutando, vaya a the section called “Paso 4: Comprobar que la secuencia de Data Defender está configurada”; en caso contrario, continúe con el siguiente paso.

3. Inicie Data Defender usando el comando que se muestra a continuación.

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

   Si Data Defender se está ejecutando después de usar el comando, vaya a the section called “Paso 4: Comprobar que la secuencia de Data Defender está configurada”; en caso contrario, continúe con el siguiente paso.

4. Inspeccione los siguientes archivos utilizando los siguientes comandos para ver si hubo algún error al instalar y configurar Data Defender.

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

> **Note**
>
> Un problema común detectado al inspeccionar estos archivos es que la Amazon VPC en la que se ejecuta la instancia de Amazon EC2 no tiene acceso a Amazon S3 para descargar los archivos de instalación. Si descubre en sus registros que este es el

problema, compruebe la configuración de Amazon VPC y del grupo de seguridad de su instancia EC2 para asegurarse de que no están bloqueando el acceso a Amazon S3.

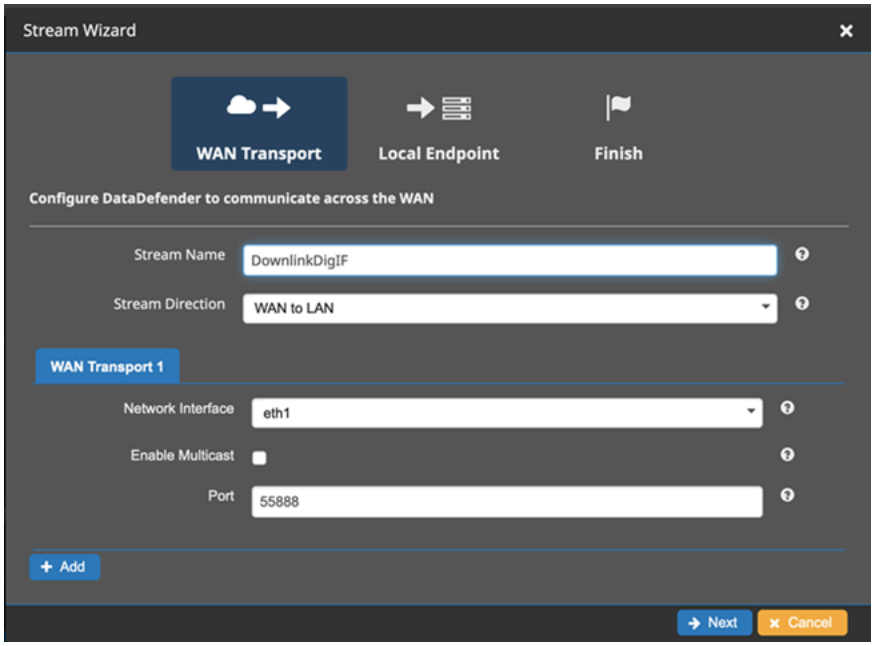
Si Data Defender se está ejecutando después de comprobar la configuración de su Amazon VPC, continúe con el the section called “Paso 4: Comprobar que la secuencia de Data Defender está configurada”. Si el problema persiste, póngase en contacto con AWS Support y envíe los archivos de registro con una descripción del problema.

Paso 4: Comprobar que la secuencia de Data Defender está configurada

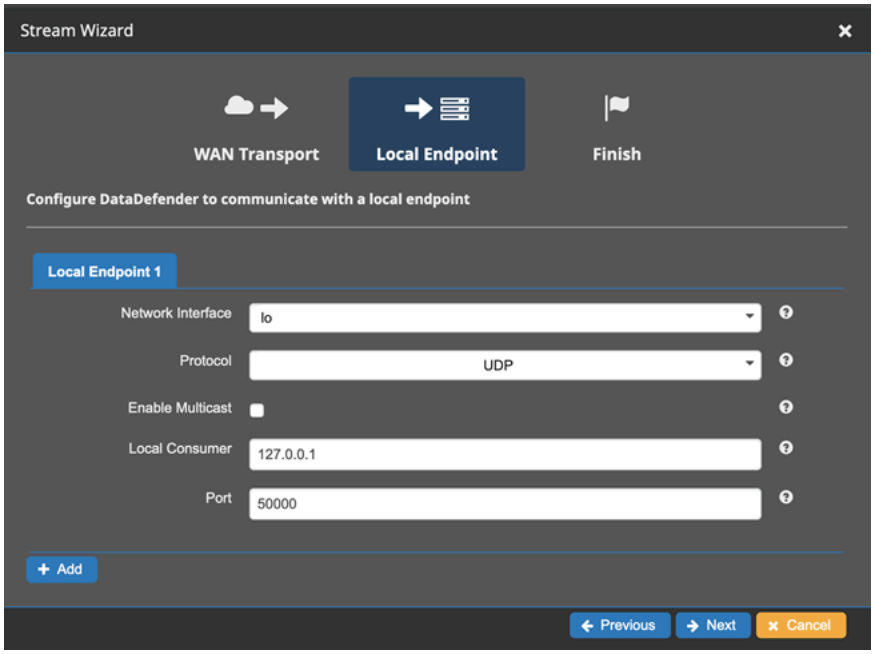
1. En un explorador web, acceda a la interfaz de usuario web de DDX escribiendo la siguiente dirección en la barra de direcciones: localhost:8080. A continuación, pulse Intro.
2. En el DataDefenderpanel de control, selecciona Ir a detalles.
3. Seleccione una secuencia en la lista de secuencias y elija Edit Stream (Editar secuencia).
4. En el cuadro de diálogo Stream Wizard (Asistente para secuencias), haga lo siguiente:

    a. En el panel WAN Transport (Transporte WAN), compruebe que la opción WAN to LAN (WAN a LAN) esté seleccionada en Stream Direction (Dirección de secuencia).

    b. En el cuadro Port (Puerto), compruebe que el puerto WAN que ha elegido para el grupo de puntos de enlace del flujo de datos esté presente. De forma predeterminada, este puerto es 55888. A continuación, elija Siguiente.



c. En el panel Local Endpoint (Punto de enlace local), asegúrese de que hay un puerto válido presente en el cuadro Port (Puerto). De forma predeterminada, este puerto es 50000. Este es el puerto en el que recibirá sus datos una vez que Data Defender los haya recibido del AWS Ground Station servicio. A continuación, elija Siguiente.



d. Si ha cambiado algún valor, elija Finish (Finalizar) en los demás menús. De lo contrario, puede cancelar todo en el menú Stream Wizard (Asistente para secuencias).

Ahora se ha asegurado de que su instancia de Amazon EC2 y Data Defender se estén ejecutando y configurando correctamente para recibir datos. AWS Ground Station Si continúa experimentando problemas, póngase en contacto con AWS Support.

Estado de los contactos de Ground Station

El estado de un AWS Ground Station contacto proporciona información sobre lo que le está sucediendo a ese contacto en un momento dado.

Estados de los contactos

A continuación se muestra la lista de estados que puede tener un contacto:

- AVAILABLE: el contacto está disponible para su reserva.
- SCHEDULING: el contacto está en proceso de reserva.
- SCHEDULED: el contacto se ha reservado correctamente.
- FAILED_TO_SCHEDULE: El contacto no pudo reservarse.
- PREPASS: El contacto comenzará pronto y se están preparando los recursos.
- PASS: El contacto se está ejecutando y se está comunicando con el satélite.
- POSTPASS: la comunicación ha finalizado y se están limpiando los recursos utilizados.
- COMPLETED: El contacto se ha completado correctamente.
- FAILED: El contacto ha fallado debido a un problema con la configuración de recursos del cliente.
- AWS_FAILED: el contacto ha fallado debido a un problema en el AWS Ground Station servicio.
- CANCELLING: El contacto está en proceso de cancelación.
- AWS_CANCELLED: el servicio canceló el contacto. AWS Ground Station Un ejemplo es el mantenimiento de antenas o emplazamientos.
- CANCELLED: El contacto ha sido cancelado por el cliente.

Guías para solucionar problemas

- the section called “Solución de problemas de contactos FAILED”
- the section called “Solución de problemas de contactos de FAILED_TO_SCHEDULE”

Solución de problemas de contactos FAILED

Un contacto tendrá el estado de contacto de terminal FALLIDO cuando AWS Ground Station detecte un problema con la configuración de los recursos del cliente. A continuación, se proporcionan los casos de uso frecuentes que pueden provocar contactos FAILED, junto con los pasos que pueden ayudar a solucionar el problema.

> **Note**
>
> Esta guía está destinada específicamente para el estado de contacto FAILED y no a otros estados de error, como AWS_FAILED, AWS_CANCELLED o FAILED_TO_SCHEDULE. Para obtener más información sobre los estados del contacto, consulte the section called “Estado de los contactos de Ground Station”

Casos de uso FAILED de Data Defender (DDX)

A continuación se muestra la lista de casos de uso frecuentes que pueden provocar un estado de contacto FAILED en los flujos de datos basados en DDX:

- El DDX del cliente nunca se conecta: nunca se estableció la conexión DDX entre AWS Ground Station Antenna y el grupo de puntos finales del flujo de datos del cliente para uno o más flujos de datos.
- El DDX del cliente se conecta tarde: la conexión DDX entre AWS Ground Station Antenna y Customer Dataflow Endpoint Group para uno o más flujos de datos se estableció después de la hora de inicio del contacto.

En caso de que se produzca un error en el flujo de datos de un agente de DDX, se recomienda tener en cuenta lo siguiente:

- Confirme que la instancia Amazon EC2 receptora se haya iniciado correctamente antes de la hora de inicio del contacto.
- Confirme que el DDX estaba funcionando durante el contacto.

Consulte la sección en the section called “Solución de problemas de contactos que envían datos a Amazon EC2” para ver los pasos de solución de problemas más específicos.

AWS Ground Station Casos de uso fallidos del agente

A continuación se muestra la lista de casos de uso frecuentes que pueden provocar un estado de contacto FAILED en los flujos de datos basados en agentes:

- El agente del cliente nunca informó del estado: el agente responsable de organizar la entrega de datos en el grupo de puntos finales del flujo de datos del cliente para uno o más flujos de datos al que nunca se informó correctamente sobre el estado. AWS Ground Station Esta actualización de estado debería producirse a los pocos segundos de la hora de finalización del contacto.
- El agente del cliente comenzó tarde: el agente responsable de orquestar la entrega de datos en el grupo de puntos de conexión del flujo de datos del cliente para uno o varios flujos de datos comenzó tarde, después de la hora de inicio del contacto.

Para cualquier caso de fallo en el flujo de datos de un AWS Ground Station agente, se recomienda tener en cuenta lo siguiente:

- Confirme que la instancia Amazon EC2 receptora se haya iniciado correctamente antes de la hora de inicio del contacto.
- Confirme que la aplicación del agente estaba en funcionamiento al inicio y durante el contacto.
- Confirme que la aplicación del agente y la instancia Amazon EC2 no se hayan cerrado 15 segundos después de finalizar el contacto. De este modo, el agente dispondrá de tiempo suficiente para informar sobre su estado a AWS Ground Station.

Consulte la sección en the section called “Solución de problemas de contactos que envían datos a Amazon EC2” para ver los pasos de solución de problemas más específicos.

Solución de problemas de contactos de FAILED_TO_SCHEDULE

Un contacto emitirá un error en el proceso de programación cuando AWS Ground Station detecte un problema en la configuración de los recursos del cliente o en el sistema interno. Un contacto que termine en el estado FAILED_TO_SCHEDULE proporcionará opcionalmente un contexto adicional. `errorMessage` Para obtener información sobre la descripción de los contactos, consulte. the section called “Describa un contacto con AWS CLI”

A continuación, se indican los casos de uso más comunes que pueden provocar que los contactos no se ejecuten correctamente, junto con los pasos para ayudar a solucionar los problemas.

> **Note**
>
> Esta guía está destinada específicamente al estado de contacto FAILED_TO_SCHEDULE y no a otros estados de error, como AWS_FAILED, AWS_CANCELLED o FAILED. Para obtener más información sobre los estados del contacto, consulte the section called “Estado de los contactos de Ground Station”

No se admiten los ajustes especificados en su Antenna Downlink Demod Decode Config.

El perfil de misión que se utilizó para programar este contacto tenía una antenna-downlink-demod-decode configuración que no era válida.

AntennaDownlinkDemodDecode Configuración existente anteriormente

- Si tus antenna-downlink-demod-decode configuraciones se han modificado recientemente, vuelve a una versión que funcionaba anteriormente antes de intentar programarlas.
- Si se trata de un cambio intencionado en una configuración existente o en una configuración anterior que ya no se está programando correctamente, sigue el siguiente paso para incorporar una nueva AntennaDownlinkDemodDecode configuración.

AntennaDownlinkDemodDecode Configuración recién creada

Póngase en contacto AWS Ground Station directamente para incorporar su nueva configuración. Cree un caso con AWS Support que incluya el `contactId` que haya finalizado en el estado FAILED_TO_SCHEDULE

Soluciones de problemas generales

Si los pasos de solución de problemas anteriores no resolvieron el problema:

- Vuelva a intentar programar el contacto o programe otro contacto con el mismo perfil de misión. Consulte the section called “Reserve un contacto con AWS CLI”.
- Si sigue recibiendo el estado FAILED_TO_SCHEDULE para este perfil de misión, póngase en contacto con AWS Support

Seguridad en AWS Ground Station

La seguridad en la nube de AWS es la mayor prioridad. Como cliente de AWS, se beneficiará de una arquitectura de red y un centro de datos diseñados para satisfacer los requisitos de seguridad de las organizaciones más exigentes. AWS proporciona herramientas y características de seguridad que le ayudarán a cumplir sus requisitos de seguridad. Estas herramientas y características incluyen seguridad de la red, administración de la configuración, control del acceso y seguridad de los datos.

Al utilizar AWS Ground Station, recomendamos que siga las prácticas recomendadas del sector y que implemente el cifrado integral. AWS proporciona API para que integre el cifrado y la protección de los datos. Para obtener más información acerca de la seguridad de AWS, consulte el documento técnico Introducción a la seguridad de AWS.

Utilice los siguientes temas para aprender a proteger los recursos de .

Temas

- Identity and Access Management para AWS Ground Station
- Uso de funciones vinculadas a servicios para la estación terrestre
- Políticas administradas de AWS para AWS Ground Station

Identity and Access Management para AWS Ground Station

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los AWS recursos. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos. AWS Ground Station La IAM es una Servicio de AWS opción que puede utilizar sin coste adicional.

Temas

- Público
- Autenticación con identidades
- Administración de acceso mediante políticas
- ¿Cómo AWS Ground Station funciona con IAM

- Ejemplos de políticas basadas en la identidad para AWS Ground Station
- Solución de problemas de AWS Ground Station identidad y acceso

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo en el que se realice. AWS Ground Station

Usuario del servicio: si utiliza el AWS Ground Station servicio para realizar su trabajo, el administrador le proporcionará las credenciales y los permisos que necesita. A medida que vaya utilizando más AWS Ground Station funciones para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una característica en AWS Ground Station, consulte Solución de problemas de AWS Ground Station identidad y acceso.

Administrador de servicios: si estás a cargo de AWS Ground Station los recursos de tu empresa, probablemente tengas acceso total a ellos AWS Ground Station. Su trabajo consiste en determinar a qué AWS Ground Station funciones y recursos deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar la IAM AWS Ground Station, consulte¿Cómo AWS Ground Station funciona con IAM.

Administrador de IAM: si es un administrador de IAM, es posible que quiera conocer más detalles sobre cómo escribir políticas para administrar el acceso a AWS. Para ver ejemplos de políticas AWS Ground Station basadas en la identidad que puede utilizar en IAM, consulte. Ejemplos de políticas basadas en la identidad para AWS Ground Station

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (Centro de identidades de IAM), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su

administrador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, asumes un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte Cómo iniciar sesión Cuenta de AWS en su Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte Firmar las solicitudes de la AWS API en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la Guía del usuario de AWS IAM Identity Center y Uso de la autenticación multifactor (MFA) en AWSen la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos, incluidos los que requieren acceso de administrador, que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios empresarial, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de

identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utilice AWS IAM Identity Center. Puede crear usuarios y grupos en el Centro de identidades de IAM o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus Cuentas de AWS aplicaciones. Para obtener más información, consulte ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales permanentes a largo plazo y los roles proporcionan credenciales temporales. Para más información, consulte Cuándo crear un usuario de IAM (en lugar de un rol) en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente una función de IAM en el AWS Management Console cambiando de función. Puede asumir un rol llamando a una operación de AWS API AWS CLI o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulte Uso de roles de IAM en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles para federación, consulte Creación de un rol para un proveedor de identidades de terceros en la Guía del usuario de IAM. Si utiliza IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .
- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.
- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
  - Sesiones de acceso directo (FAS): cuando utilizas un usuario o un rol de IAM para realizar acciones en ellas AWS, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.
  - Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio

desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

- Función vinculada al servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

- Aplicaciones que se ejecutan en Amazon EC2: puede usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una instancia EC2 y realizan AWS CLI solicitudes a la API. AWS Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia de EC2. Para asignar un AWS rol a una instancia EC2 y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia de EC2 obtener credenciales temporales. Para más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2 en la Guía del usuario de IAM.

Para obtener información sobre el uso de los roles de IAM, consulte Cuándo crear un rol de IAM (en lugar de un usuario) en la Guía del usuario de IAM.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de políticas JSON en la Guía del usuario de IAM.

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Listas de control de acceso (ACL)

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3 y Amazon VPC son ejemplos de servicios que admiten las ACL. AWS WAF Para obtener más información sobre las ACL, consulte Información general de Lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCP): las SCP son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations AWS Organizations es un servicio para agrupar y gestionar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilita todas las características en una organización, entonces podrá aplicar políticas de control de servicio (SCP) a una o a todas sus cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una. Usuario raíz de la cuenta de AWS Para obtener más información acerca de Organizations y las SCP, consulte Funcionamiento de las SCP en la Guía del usuario de AWS Organizations .
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo AWS determinar si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

¿Cómo AWS Ground Station funciona con IAM

Antes de utilizar IAM para gestionar el acceso AWS Ground Station, infórmese sobre las funciones de IAM disponibles para su uso. AWS Ground Station

Funciones de IAM que puede utilizar con AWS Ground Station

Característica de IAM	AWS Ground Station soporte
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política (específicas del servicio)	Sí
ACL	No
ABAC (etiquetas en políticas)	Sí
Credenciales temporales	Sí
Permisos de entidades principales	Sí
Roles de servicio	No
Roles vinculados al servicio	Sí

Para obtener una visión general de cómo AWS Ground Station funcionan otros AWS servicios con la mayoría de las funciones de IAM, consulte AWS los servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas basadas en la identidad para AWS Ground Station

Compatibilidad con las políticas basadas en identidad	Sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está adjunto. Para más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Ejemplos de políticas basadas en la identidad para AWS Ground Station

Para ver ejemplos de políticas AWS Ground Station basadas en la identidad, consulte. Ejemplos de políticas basadas en la identidad para AWS Ground Station

Políticas basadas en recursos dentro de AWS Ground Station

Compatibilidad con las políticas basadas en recursos	No

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico.

Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política en función de recursos concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Acciones políticas para AWS Ground Station

Admite acciones de política	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de AWS Ground Station acciones, consulta las acciones definidas AWS Ground Station en la Referencia de autorización del servicio.

Las acciones políticas AWS Ground Station utilizan el siguiente prefijo antes de la acción:

```
groundstation
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

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

Para ver ejemplos de políticas AWS Ground Station basadas en la identidad, consulte. Ejemplos de políticas basadas en la identidad para AWS Ground Station

Recursos de políticas para AWS Ground Station

Admite recursos de políticas	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

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

Para ver una lista de los tipos de AWS Ground Station recursos y sus ARN, consulte los recursos definidos AWS Ground Station en la Referencia de autorización de servicios. Para obtener información sobre las acciones con las que puede especificar el ARN de cada recurso, consulte Acciones definidas por AWS Ground Station.

Para ver ejemplos de políticas AWS Ground Station basadas en la identidad, consulte. Ejemplos de políticas basadas en la identidad para AWS Ground Station

Claves de condición de la política para AWS Ground Station

Admite claves de condición de políticas específicas del servicio	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones condicionales que utilicen operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulte Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Para ver una lista de claves de AWS Ground Station condición, consulte las claves de condición AWS Ground Station en la Referencia de autorización de servicio. Para saber con qué acciones y recursos puede utilizar una clave de condición, consulte Acciones definidas por AWS Ground Station.

Para ver ejemplos de políticas AWS Ground Station basadas en la identidad, consulte. Ejemplos de políticas basadas en la identidad para AWS Ground Station

ACL en AWS Ground Station

Admite las ACL	No

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

ABAC con AWS Ground Station

Admite ABAC (etiquetas en las políticas)	Sí

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte ¿Qué es ABAC? en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Utilizar credenciales temporales con AWS Ground Station

Compatible con el uso de credenciales temporales	Sí

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluida información sobre cuáles Servicios de AWS funcionan con

credenciales temporales, consulta Cómo Servicios de AWS funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para más información sobre el cambio de roles, consulte Cambio a un rol (consola) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para más información, consulte Credenciales de seguridad temporales en IAM.

Permisos principales entre servicios para AWS Ground Station

Admite Forward access sessions (FAS)	Sí

Cuando utilizas un usuario o un rol de IAM para realizar acciones en él AWS, se te considera principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama y los que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información detallada sobre las políticas a la hora de realizar solicitudes de FAS, consulte Forward access sessions.

Roles de servicio para AWS Ground Station

Compatible con roles de servicio	No

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener

más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio puede interrumpir AWS Ground Station la funcionalidad. Edite las funciones de servicio solo cuando se AWS Ground Station proporcionen instrucciones para hacerlo.

Funciones vinculadas al servicio para AWS Ground Station

Compatible con roles vinculados al servicio	Sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM. Busque un servicio en la tabla que incluya `Yes` en la columna Rol vinculado a un servicio. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

Ejemplos de políticas basadas en la identidad para AWS Ground Station

De forma predeterminada, los usuarios y roles no tienen permiso para crear, ver ni modificar recursos de AWS Ground Station . Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS la API. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos AWS Ground Station, incluido el formato de los ARN para cada uno de los tipos de recursos, consulte las claves de condición, recursos y acciones de la Referencia de autorización de servicios. AWS Ground Station

Temas

- Prácticas recomendadas sobre las políticas
- Mediante la consola de AWS Ground Station
- Cómo permitir a los usuarios consultar sus propios permisos

Prácticas recomendadas sobre las políticas

Las políticas basadas en la identidad determinan si alguien puede crear AWS Ground Station recursos de tu cuenta, acceder a ellos o eliminarlos. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de trabajo en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.

- Utilice el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Política de validación de Analizador de acceso de IAM en la Guía de usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para más información, consulte Configuración del acceso a una API protegido por MFA en la Guía de usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte las Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Mediante la consola de AWS Ground Station

Para acceder a la AWS Ground Station consola, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los AWS Ground Station recursos de su cuenta Cuenta de AWS. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que concedas permisos mínimos de consola a los usuarios que solo realicen llamadas a la API AWS CLI o a la AWS API. En su lugar, permite acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para garantizar que los usuarios y los roles puedan seguir utilizando la AWS Ground Station consola, asocie también la AWS Ground Station `ConsoleAccess` política `ReadOnly` AWS gestionada a las entidades. Para más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM:

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política

incluye permisos para completar esta acción en la consola o mediante programación mediante la API AWS CLI o AWS .

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

Solución de problemas de AWS Ground Station identidad y acceso

Utilice la siguiente información como ayuda para diagnosticar y solucionar los problemas habituales que pueden surgir al trabajar con un AWS Ground Station IAM.

Temas

No estoy autorizado a realizar ninguna acción en AWS Ground Station

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `groundstation:`*`GetWidget`*.

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

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `groundstation:`*`GetWidget`*.

Si necesita ayuda, póngase en contacto con su AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar tareas como: PassRole

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, las políticas deben actualizarse a fin de permitirle pasar un rol a AWS Ground Station.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en AWS Ground Station. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

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

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su administrador. AWS El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis AWS Ground Station recursos

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para más información, consulte lo siguiente:

- Para saber si AWS Ground Station es compatible con estas funciones, consulte¿Cómo AWS Ground Station funciona con IAM.
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a un usuario de IAM en otro usuario de su propiedad Cuenta de AWS en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para obtener información acerca del uso de roles y políticas basadas en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Uso de funciones vinculadas a servicios para la estación terrestre

AWS Ground Station utiliza roles vinculados a servicios de AWS Identity and Access Management (IAM). Un rol vinculado al servicio es un tipo único de rol de IAM que está vinculado directamente a Ground Station. Los roles vinculados al servicio están predefinidos por Ground Station e incluyen todos los permisos que el servicio requiere para llamar a otros servicios de AWS en su nombre.

Un rol vinculado a un servicio facilita la configuración de Ground Station porque no tiene que añadir manualmente los permisos necesarios. Ground Station define los permisos de sus roles vinculados al servicio, y a menos que se defina lo contrario, solo Ground Station puede asumir sus roles. Los permisos definidos incluyen las políticas de confianza y de permisos y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM.

Para obtener información sobre otros servicios que admiten roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Yes (Sí) en la columna Service-linked roles (Roles vinculados a servicios). Seleccione una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

Permisos de roles vinculados al servicio para la estación terrestre

Ground Station utiliza el rol vinculado al servicio denominado AWSServiceRoleForGroundStationDataflowEndpointGroup – AWS GroundStation utiliza este rol vinculado al servicio para llamar a EC2 para encontrar direcciones IPv4 públicas.

El rol vinculado al servicio AWSServiceRoleForGroundStationDataflowEndpointGroup confía en los siguientes servicios para asumir el rol:

- `groundstation.amazonaws.com`

La política de permisos de rol denominada AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy permite a Ground Station realizar las siguientes acciones en los recursos especificados:

- Acción: `ec2:DescribeAddresses` en `all AWS resources (*)`

  La acción permite que la estación terrestre enumere todas las IP asociadas a los EIP.

- Acción: `ec2:DescribeNetworkInterfaces` en `all AWS resources (*)`

La acción permite a Ground Station obtener información sobre las interfaces de red asociadas a las instancias EC2

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Creación de un rol vinculado al servicio para Ground Station

No necesita crear manualmente un rol vinculado a servicios. Cuando crea un DataflowEndpointGroup en la AWS CLI o en la API de AWS, Ground Station crea el rol vinculado al servicio por usted.

Si elimina este rol vinculado al servicio y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Cuando crea un DataflowEndpointGroup, Ground Station vuelve a crear el rol vinculado al servicio por usted.

También puede utilizar la consola de IAM para crear un rol vinculado al servicio con el caso de uso Entrega de datos a Amazon EC2. En la AWS CLI o la API de AWS, cree un rol vinculado al servicio con el nombre de servicio `groundstation.amazonaws.com`. Para obtener más información, consulte Creación de un rol vinculado a un servicio en la Guía del usuario de IAM. Si elimina este rol vinculado al servicio, puede utilizar este mismo proceso para volver a crear el rol.

Edición de un rol vinculado al servicio para Ground Station

Ground Station no le permite editar el rol vinculado al servicio AWSServiceRoleForGroundStationDataflowEndpointGroup. Después de crear un rol vinculado a servicios, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia al mismo. Sin embargo, puede editar la descripción del rol mediante IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminación de un rol vinculado al servicio para Ground Station

Si ya no necesita utilizar una característica o servicio que requiere un rol vinculado a un servicio, recomendamos que elimine dicho rol. De esta forma no tiene una entidad no utilizada que no se monitoree ni mantenga de forma activa.

Solo se puede eliminar una función vinculada a un servicio después de eliminar primero los DataflowEndpointGroups que utilizan la función vinculada al servicio. De esta forma se evita revocar

accidentalmente los permisos de los DataflowEndpointGroups. Si un rol vinculado al servicio se utiliza con varios DataflowEndpointGroups, deberá eliminar todos los DataflowEndpointGroups que utilicen el rol vinculado al servicio antes de poder eliminarlo.

> **Note**
>
> Si el servicio Ground Station está utilizando el rol cuando intente eliminar los recursos, la eliminación puede fallar. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar los recursos de Ground Station utilizados por AWSServiceRoleForGroundStationDataflowEndpointGroup

- Elimine DataflowEndpointGroups mediante AWS CLI o la API de AWS.

Para eliminar manualmente el rol vinculado a servicios mediante IAM

Utilice la consola de IAM, la AWS CLI o la API de AWS para eliminar el rol vinculado a servicio WSServiceRoleForGroundStationDataflowEndpointGroup. Para obtener más información, consulte Eliminar un rol vinculado a un servicio en la Guía del usuario de IAM.

Regiones compatibles con las funciones vinculadas al servicio de Ground Station

Ground Station admite el uso de roles vinculados al servicio en todas las regiones en las que el servicio esté disponible. Para obtener más información, consulte la tabla de regiones.

Solución de problemas

`NOT_AUTHORIZED_TO_CREATE_SLR` - Esto indica que el rol de la cuenta que se está utilizando para llamar a la API CreateDataflowEndpointGroup no tiene el permiso `iam:CreateServiceLinkedRole`. Un administrador con el permiso `iam:CreateServiceLinkedRole` debe crear manualmente el rol vinculado al servicio para su cuenta.

Políticas administradas de AWS para AWS Ground Station

Una política administrada de AWS es una política independiente que AWS crea y administra. Las políticas administradas de AWS se diseñan para ofrecer permisos para muchos casos de uso comunes, por lo que puede empezar a asignar permisos a los usuarios, grupos y roles.

Tenga presente que es posible que las políticas administradas de AWS no concedan permisos de privilegio mínimo para los casos de uso concretos, ya que están disponibles para que las utilicen todos los clientes de AWS. Se recomienda definir políticas administradas por el cliente para los casos de uso a fin de reducir aún más los permisos.

No puede cambiar los permisos definidos en las políticas administradas por AWS. Si AWS actualiza los permisos definidos en un política administrada de AWS, la actualización afecta a todas las identidades de entidades principales (usuarios, grupos y roles) a las que está adjunta la política. Lo más probable es que AWS actualice una política administrada de AWS cuando se lance un nuevo Servicio de AWS o las operaciones de la API nuevas estén disponibles para los servicios existentes.

Para obtener más información, consulte Políticas administradas de AWS en la Guía del usuario de IAM.

Política administrada por AWS: AWS GroundStationAgentInstancePolicy

Puede adjuntar la política `AWSGroundStationAgentInstancePolicy` a las identidades de IAM.

Esta política concede permisos de agente de AWS Ground Station a una instancia de cliente que permite a la instancia enviar y recibir datos durante los contactos de Ground Station. Todos los permisos de esta política son del servicio Ground Station.

Detalles sobre los permisos

Esta política incluye los siguientes permisos.

- `groundstation` – Permite que las instancias de punto de conexión de flujo de datos llamen a las API del agente de Ground Station Agent.

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

Política administrada por AWS: AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy

No se puede asociar AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy a las entidades de IAM. Esta política está adjunta a un rol vinculado a servicios que permite a AWS Ground Station realizar acciones en su nombre. Para más información, consulte el Uso de roles vinculados a servicios.

Esta política concede permisos EC2 que permiten a AWS Ground Station encontrar direcciones IPv4 públicas.

Detalles sobre los permisos

Esta política incluye los siguientes permisos.

- `ec2:DescribeAddresses` – Permite a AWS Ground Station enumerar todas las IPs asociadas con EIPs en su nombre.

- `ec2:DescribeNetworkInterfaces` – Permite a AWS Ground Station obtener información sobre las interfaces de red asociadas con instancias EC2 en su nombre.

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

Actualizaciones de AWS Ground Station en las políticas administradas de AWS

Es posible consultar los detalles sobre las actualizaciones de las políticas administradas de AWS para AWS Ground Station debido a que este servicio comenzó a realizar el seguimiento de estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la página de historial de documentos AWS Ground Station.

Cambio	Descripción	Fecha
Nueva política AWSGroundStationAgentInstancePolicy	AWS Ground Station ha añadido una nueva política para proporcionar permisos a la la instancia de punto de conexión de flujo de datos	12 de abril de 2023

Cambio	Descripción	Fecha
	para utilizar el agente de AWS Ground Station.	
Nueva política AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy	AWS Ground Station ha añadido una nueva política que concede permisos a EC2 para permitir a AWS Ground Station encontrar direcciones IPv4 públicas asociadas a EIP e interfaces de red asociadas a instancias EC2.	2 de noviembre de 2022
AWS Ground Station comenzó el seguimiento de los cambios.	AWS Ground Station comenzó el seguimiento de los cambios de las políticas administradas de AWS.	1 de marzo de 2021

Cifrado de datos en reposo para AWS Ground Station

AWS Ground Station proporciona cifrado de forma predeterminada para proteger los datos confidenciales de los clientes en reposo mediante claves AWS de cifrado propias.

- Claves propiedad de AWS: AWS Ground Station utiliza estas claves de forma predeterminada para cifrar automáticamente los datos personales y de identificación directa y las efemérides. No es posible ver, administrar o utilizar las claves propiedad de AWS, ni auditar su uso; sin embargo, no es necesario realizar ninguna acción ni cambiar los programas para proteger las claves que cifran los datos. Para obtener más información, consulte Claves propiedad de AWS en la Guía para desarrolladores de AWS Key Management Service.

El cifrado de datos en reposo de forma predeterminada ayuda a reducir la sobrecarga operativa y la complejidad que conlleva la protección de datos confidenciales. Al mismo tiempo, permite crear aplicaciones seguras que cumplen estrictos requisitos de encriptación, así como requisitos normativos.

AWS Ground Station aplica el cifrado de todos los datos confidenciales en reposo; sin embargo, en el caso de algunos AWS Ground Station recursos, como las efemérides, puede optar por utilizar una clave gestionada por el cliente en lugar de las claves gestionadas por defecto. AWS

- Claves administradas por el cliente: AWS Ground Station admite el uso de una clave simétrica administrada por el cliente, que usted crea, posee y administra para agregar una segunda capa de cifrado sobre la encriptación propia existente. AWS Como usted tiene el control total de este cifrado, puede realizar dichas tareas como:
  - Establecer y mantener políticas de claves
  - Establecer y mantener concesiones y políticas de IAM
  - Habilitar y deshabilitar políticas de claves
  - Rotar el material criptográfico
  - Agregar etiquetas.
  - Crear alias de clave
  - Programar la eliminación de claves

  Para obtener más información, consulte clave administrada por el cliente ien la Guía para desarrolladores de AWS Key Management Service..

En la siguiente tabla se resumen los recursos para los que se AWS Ground Station admite el uso de claves administradas por el cliente

Tipo de datos	Cifrado de claves propiedad de AWS	Cifrado de claves administradas por el cliente (opcional)
Datos de efemérides utilizados para calcular la trayectoria de un satélite	Habilitado	Habilitado

> **Note**
>
> AWS Ground Station habilita automáticamente el cifrado en reposo mediante claves AWS propias para proteger los datos de identificación personal sin coste alguno. Sin embargo, se aplican cargos de AWS KMS por el uso de una clave administrada por el cliente. Para obtener más información sobre precios, consulte los precios de AWS Key Management Service.
> Para obtener más información sobre AWS KMS, consulte la Guía para desarrolladores de AWS KMS.

¿Cómo se AWS Ground Station utilizan las subvenciones en AWS KMS?

AWS Ground Station requiere una concesión de clave para usar la clave administrada por el cliente.

Cuando subes una efeméride cifrada con una clave gestionada por el cliente, AWS Ground Station crea una concesión de claves en tu nombre enviando una CreateGrant solicitud a KMS. AWS Las concesiones en AWS KMS se utilizan para dar AWS Ground Station acceso a una clave de KMS en una cuenta de cliente.

AWS Ground Station requiere la concesión para utilizar la clave gestionada por el cliente en las siguientes operaciones internas:

- Envíe `GenerateDataKey` solicitudes a AWS KMS para generar claves de datos cifradas por su clave administrada por el cliente.

- Envíe `Decrypt` solicitudes a AWS KMS para descifrar las claves de datos cifradas para que puedan usarse para cifrar sus datos.
- Envíe `Encrypt` solicitudes a AWS KMS para cifrar los datos proporcionados.

Puede revocar el acceso a la concesión o eliminar el acceso del servicio a la clave administrada por el cliente en cualquier momento. Si lo hace, AWS Ground Station no podrá acceder a ninguno de los datos cifrados por la clave administrada por el cliente, lo que afectará a las operaciones que dependen de esos datos. Por ejemplo, si eliminas la concesión de una clave de una efeméride actualmente en uso para un contacto, no AWS Ground Station podrás utilizar los datos de efemérides proporcionados para apuntar la antena durante el contacto. Esto provocará que el contacto finalice con un estado de FALLIDO.

Crear una clave administrada por el cliente

Puede crear una clave simétrica administrada por el cliente mediante la consola de AWS administración o las API de KMS. AWS

Para crear una clave simétrica administrada por el cliente

Siga los pasos para crear una clave simétrica gestionada por el cliente que se indican en la Guía para desarrolladores del servicio de administración de AWS claves.

Política de claves

Las políticas de clave controlan el acceso a la clave administrada por el cliente. Cada clave administrada por el cliente debe tener exactamente una política de clave, que contiene instrucciones que determinan quién puede usar la clave y cómo puede utilizarla. Cuando crea la clave administrada por el cliente, puede especificar una política de clave. Para obtener más información, consulte Administrar el acceso a las claves administradas por el cliente en la Guía para desarrolladores del Servicio de administración de AWS claves.

Para utilizar la clave gestionada por el cliente con AWS Ground Station los recursos, la política de claves debe permitir las siguientes operaciones de API:

`kms:CreateGrant` - Añade una subvención a una clave administrada por el cliente. Otorga el acceso de control a una clave de KMS específica, que permite el acceso a las operaciones de concesión AWS Ground Station necesarias. Para obtener más información sobre el uso de las subvenciones, consulte la Guía para desarrolladores del servicio de administración de AWS claves.

Esto permite AWS a Amazon hacer lo siguiente:

- Llamar a `GenerateDataKey` para generar una clave de datos cifrada y almacenarla, ya que la clave de datos no se utiliza inmediatamente para cifrar.
- Llamar a `Decrypt` para usar la clave de datos cifrados almacenada para acceder a los datos cifrados.
- Llame a `Encrypt` para utilizar la clave de datos para cifrar los datos.
- Configurar una entidad principal que se retire para permitir que el servicio `RetireGrant`.

`kms:DescribeKey`- Proporciona los detalles clave gestionados por el cliente AWS Ground Station para poder validarla antes de intentar crear una concesión para la clave proporcionada.

Los siguientes son ejemplos de declaraciones de políticas de IAM que puede añadir 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 obtener más información sobre cómo especificar los permisos en una política, consulta la Guía para desarrolladores de AWS Key Management Service.

Para obtener más información sobre la solución de problemas de acceso a las claves, consulte la Guía AWS para desarrolladores del Servicio de administración de claves.

Especificar una clave gestionada por el cliente para AWS Ground Station

Puede especificar una clave administrada por el cliente para cifrar los siguientes recursos:

- Efemérides

Al crear un recurso, puede especificar la clave de datos proporcionando una kmsKeyArn

- kmsKeyArn- Un identificador clave para una clave de AWS KMS administrada por el cliente

AWS Ground Station contexto de cifrado

Un contexto de cifrado es un conjunto opcional de pares clave-valor que pueden contener información contextual adicional sobre los datos. AWS KMS utiliza el contexto de cifrado como datos autenticados adicionales para admitir el cifrado autenticado. Al incluir un contexto de cifrado en una

solicitud de cifrado de datos, AWS KMS vincula el contexto de cifrado a los datos cifrados. Para descifrar los datos, debe incluir el mismo contexto de cifrado en la solicitud.

AWS Ground Station contexto de cifrado

AWS Ground Station utiliza un contexto de cifrado diferente en función del recurso que se esté cifrando y especifica un contexto de cifrado específico para cada concesión de clave creada.

Contexto de cifrado de efemérides:

La concesión de claves para cifrar recursos de efemérides está vinculada a un ARN de satélite específico

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

> **Note**
>
> Las concesiones de claves se reutilizan para el mismo par clave-satélite.

Uso del contexto de cifrado para la supervisión

Si utiliza una clave simétrica administrada por el cliente para cifrar sus efemérides, también puede utilizar el contexto de cifrado en los registros y registros de auditoría para identificar cómo se está utilizando la clave administrada por el cliente. El contexto de cifrado también aparece en los registros generados por AWS CloudTrail Amazon CloudWatch Logs.

Utilizar el contexto de cifrado para controlar el acceso a la clave administrada por el cliente

Puede utilizar el contexto de cifrado en las políticas de claves y las políticas de IAM como `conditions` para controlar el acceso a la clave simétrica administrada por el cliente. Puede usar también una restricción de contexto de cifrado en una concesión.

AWS Ground Station utiliza una restricción de contexto de cifrado en las concesiones para controlar el acceso a la clave gestionada por el cliente en su cuenta o región. La restricción de concesión requiere que las operaciones que permite la concesión utilicen el contexto de cifrado especificado.

Los siguientes son ejemplos de declaraciones de política de claves para conceder acceso a una clave administrada por el cliente para un contexto de cifrado específico. La condición de esta declaración de política exige que las concesiones tengan una restricción de contexto de cifrado que especifique el contexto de cifrado.

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

Supervisa tus claves de cifrado para AWS Ground Station

Cuando utilizas una clave gestionada por el cliente de AWS KMS con tus AWS Ground Station recursos, puedes utilizar AWS CloudTrailnuestros CloudWatch registros de Amazon para realizar un seguimiento de las solicitudes que se AWS Ground Station envían a AWS KMS. Los siguientes ejemplos son AWS CloudTrail eventos para `CreateGrant` `GenerateDataKeyDecrypt`, `Encrypt` y `DescribeKey` para monitorear las operaciones de KMS llamadas por AWS Ground Station para acceder a los datos cifrados por su clave administrada por el cliente.

`CreateGrant` (CloudTrail)

Cuando utilizas una clave de AWS KMS gestionada por el cliente para cifrar tus recursos efemérides, AWS Ground Station envía una `CreateGrant` solicitud en tu nombre para acceder a la clave de KMS de tu cuenta. AWS La concesión que se AWS Ground Station crea es específica del recurso asociado a la clave gestionada por el cliente de AWS KMS. Además, AWS Ground Station utiliza la `RetireGrant` operación para eliminar una concesión al eliminar un recurso.

El siguiente ejemplo de evento registra la operación `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)

Cuando utilizas una clave de AWS KMS gestionada por el cliente para cifrar tus recursos efemérides, AWS Ground Station envía una `DescribeKey` solicitud en tu nombre para validar que la clave solicitada existe en tu cuenta.

El siguiente ejemplo de evento registra la operación `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)

Cuando utilizas una clave gestionada por el cliente de AWS KMS para cifrar tus recursos de efemérides, AWS Ground Station envía una `GenerateDataKey` solicitud a KMS para generar una clave de datos con la que cifrar tus datos.

El siguiente ejemplo de evento registra la operación `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)

Cuando utiliza una clave de AWS KMS gestionada por el cliente para cifrar los recursos de efemérides, AWS Ground Station utiliza la `Decrypt` operación para descifrar las efemérides proporcionadas si ya están cifradas con la misma clave gestionada por el cliente. Por ejemplo si se está cargando una efeméride desde un bucket de S3 y se cifra en ese bucket con una clave determinada.

El siguiente ejemplo de evento registra la operación `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"
}
```

Datos de efemérides de satélite

Una efeméride, en plural efemérides, es un archivo o estructura de datos que proporciona la trayectoria de objetos astronómicos. Históricamente, este archivo solo hacía referencia a datos tabulares pero, poco a poco, ha ido dirigiéndose a una amplia variedad de archivos de datos que indican la trayectoria de una nave espacial.

AWS Ground Station utiliza los datos de efemérides para determinar cuándo están disponibles los contactos para el satélite y ordenar correctamente a las antenas de la AWS Ground Station red que apunten al satélite. De forma predeterminada, no es necesario realizar ninguna acción para proporcionar efemérides AWS Ground Station .

Temas

Datos de efemérides predeterminados

De forma predeterminada, AWS Ground Station utiliza datos disponibles públicamente de Space-Track y no es necesario realizar ninguna acción para proporcionar AWS Ground Station estas efemérides predeterminadas. Estas efemérides son conjuntos de elementos de dos líneas asociados al ID NORAD de su satélite. Todas las efemérides predeterminadas tienen una prioridad de 0. Como resultado, se anularán siempre por cualquier efeméride personalizada no caducada cargada a través de la API de efemérides, que siempre debe tener una prioridad de 1 o superior.

Los satélites que no cuenten con un ID de NORAD deben cargar datos de efemérides personalizados a. AWS Ground Station Por ejemplo, los satélites que se acaban de lanzar o que se han omitido intencionadamente del catálogo Space-Track no tienen ID NORAD y necesitarán que se carguen efemérides personalizadas. Para obtener más información sobre cómo proporcionar efemérides personalizadas, consulte: Proporcionar datos de efemérides personalizadas.

¿Qué efemérides se utilizan?

Las efemérides tienen una prioridad,, un tiempo de caducidad y un indicador de activación. Juntos, determinan qué efemérides se utiliza para un satélite. Solo se puede activar una efeméride para cada satélite.

La efeméride que se utiliza es la que tiene la tiene la prioridad de activación más alta y cuyo tiempo de expiración es futuro. Los tiempos de contacto disponibles devueltos por ListContactsse basan en esta efeméride. Si hay varias efemérides `ENABLED` con la misma prioridad, se utilizará la efeméride creada o actualizada más recientemente.

> **Note**
>
> AWS Ground Station tiene una cuota de servicio en función del número de efemérides `ENABLED` proporcionadas por el cliente por satélite (consulte: Service Quotas). Para cargar datos de efemérides después de alcanzar esta cuota, elimine (mediante `DeleteEphemeris`) o desactive (mediante `UpdateEphemeris`) las efemérides de menor prioridad o las que se crearon más temprano y que proporcionó el cliente.

Si no se ha creado ninguna efeméride o si ninguna efeméride tiene `ENABLED` estado, AWS Ground Station utilizará una efeméride predeterminada para el satélite (de Space Track), si está disponible. Esta efeméride predeterminada tiene prioridad 0.

Efecto de las nuevas efemérides en los contactos programados previamente

Usa la DescribeContact API para ver los efectos de las nuevas efemérides en los contactos previamente programados devolviendo los tiempos de visibilidad activos.

Los contactos programados antes de subir una nueva efeméride conservarán la hora de contacto programada originalmente, mientras que el seguimiento por antena utilizará las efemérides activas. Si la posición de la nave espacial, basada en las efemérides activas, difiere considerablemente de las efemérides anteriores, esto puede reducir el tiempo de contacto del satélite con la antena, ya que la nave espacial opera fuera de la máscara del sitio de transmisión/recepción. Por lo tanto, te recomendamos que canceles y reprogrames tus futuros contactos después de subir una nueva efeméride que difiera mucho de las efemérides anteriores. Con la DescribeContact API, puede

determinar la parte de su futuro contacto que no se puede utilizar debido a que la nave espacial opera fuera de la máscara del sitio de transmisión/recepción comparando su contacto programado `startTime` y `endTime` con el devuelto y. `visibilityStartTime` `visibilityEndTime` Si decide cancelar y reprogramar sus futuros contactos, el intervalo de tiempo de contacto no debe estar fuera del intervalo de tiempo de visibilidad en más de 30 segundos. Los contactos cancelados pueden conllevar costes si se cancelan demasiado cerca de la hora del contacto. Para más información sobre contactos cancelados, consulte: Preguntas frecuentes sobre Ground Station.

Indica cómo obtener las efemérides actuales de un satélite

Las efemérides actuales utilizadas AWS Ground Station por un satélite específico se pueden recuperar llamando a las acciones `GetSatellite` o`ListSatellites`. Ambos métodos proporcionan los metadatos de las efemérides actualmente en uso. Estos metadatos de efemérides son diferentes para las efemérides personalizadas cargadas y para las efemérides predeterminadas. AWS Ground Station

Las Efemérides predeterminadas solo incluyen los campos `source` y `epoch` fields. `epoch`Es la época del conjunto de elementos de dos líneas que se extrajo de Space Track y actualmente se utiliza para AWS Ground Station calcular la trayectoria del satélite.

Una efeméride personalizada tendrá un valor de origen `source` valor de `"CUSTOMER_PROVIDED"` e incluirá un identificador único en el campo `ephemerisId`. Este identificador único puede utilizarse para consultar las efemérides utilizando la acción `DescribeEphemeris`. Se devolverá un `name` campo opcional si se asignó un nombre a la efeméride durante la carga a AWS Ground Station través de la acción. `CreateEphemeris`

Es importante tener en cuenta que las efemérides se actualizan de forma dinámica, por AWS Ground Station lo que los datos devueltos son solo una instantánea de las efemérides que se estaban utilizando en el momento de la llamada a la API.

Ejemplo de retorno **`GetSatellite`** para un satélite que utiliza una efeméride predeterminada

```
{
    "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
    }
}
```

Ejemplo **`GetSatellite`** para un satélite que utiliza una efeméride predeterminada

```
{
      "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"
      }
  }
```

Proporcionar datos de efemérides personalizados

> **Warning**
>
> La API de efemérides se encuentra actualmente en estado de previsualización.

El acceso a la API de Efemérides solo se proporciona en función de las necesidades. Los clientes que necesiten cargar datos de efemérides personalizados deben ponerse en contacto con la dirección aws-groundstation@amazon.com.

Información general

La API de Ephemeris permite cargar efemérides personalizadas para usarlas con AWS Ground Station un satélite. Estas efemérides anulan las efemérides predeterminadas de Space Track (consulte: Datos de efemérides predeterminados).

Al subir las efemérides de los clientes, se puede mejorar la calidad del seguimiento, gestionar las primeras operaciones cuando no se dispone de las efemérides de Space Track y contabilizar las maniobras. AWS Ground Station

Creación de una efeméride personalizada

Se puede crear una efeméride personalizada mediante la acción `CreateEphemeris` de la API de AWS Ground Station . Esta acción cargará una efeméride utilizando los datos del cuerpo de la solicitud o de un bucket de S3 específico.

Es importante tener en cuenta que al cargar una efeméride ésta se establece en `VALIDATING` e inicia un flujo de trabajo asíncrono que validará y generará contactos potenciales a partir de la efeméride. Solo se podrá utilizar para contactos cuando la efeméride haya superado este flujo de trabajo y esté `ENABLED`. Debe consultar el estado de las efemérides en `DescribeEphemeris` o utilizar los eventos de Cloudwatch para realizar un seguimiento de los cambios de estado de las efemérides.

Para solucionar problemas de efemérides no válidas, consulte: Solución de problemas de efemérides no válidas

Creación de un conjunto de efemérides TLE a través de la API

El cliente AWS Ground Station boto3 se puede utilizar para cargar un conjunto de efemérides de dos líneas (TLE) mediante una llamada. AWS Ground Station `CreateEphemeris` Se utilizará esta efeméride en lugar de los datos de efemérides predeterminados para un satélite (consulte Datos de efemérides predeterminados).

Un conjunto de TLE es un objeto con formato JSON que une una o más TLE para construir una trayectoria continua. Los TLE en el conjunto TLE deben formar un conjunto continuo que podamos utilizar para construir una trayectoria (es decir, sin espacios en el tiempo entre TLE en un conjunto TLE). A continuación se muestra un ejemplo de conjunto TLE:

```
# 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**
>
> Los intervalos de tiempo de los TLE de un conjunto de TLE deben coincidir exactamente para ser una trayectoria continua válida.

Se puede cargar un conjunto de TLE a través del cliente AWS Ground Station boto3 de la siguiente manera:

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

Esta llamada devolverá un identificador de efemérides que se puede utilizar para hacer referencia a la efeméride en el futuro. Por ejemplo, podemos usar el identificador de efemérides proporcionado en la llamada anterior para consultar el estado de la efeméride:

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

A continuación se muestra un ejemplo de respuesta de la acción `DescribeEphemeris`

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

Es recomendable consultar la ruta `DescribeEphemeris` o utilizar los eventos de Cloudwatch para seguir el estado de la efeméride cargada, ya que debe pasar por un flujo de trabajo de validación asíncrono antes de que se establezca como `ENABLED` y ejecutar contactos.

Tenga en cuenta que el ID NORAD en todos los TLEs del conjunto de TLE, `25994` en los ejemplos anteriores, debe coincidir con el ID NORAD que su satélite tiene asignado en la base de datos Space Track.

Cargar datos de efemérides desde un bucket S3

También es posible cargar un archivo de efemérides directamente desde un depósito de S3 apuntando al depósito y a la clave del objeto. AWS Ground Station recuperará el objeto en tu nombre. La información sobre el cifrado de los datos en reposo AWS Ground Station se detalla en: Cifrado de datos en reposo para AWS Ground Station

A continuación se muestra un ejemplo de cómo cargar un archivo de efemérides OEM desde un bucket de 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",
            }
        }
    })
```

A continuación se muestra un ejemplo de los datos devueltos por la acción `DescribeEphemeris` a la que se llama para las efemérides OEM cargadas en el bloque anterior de código de ejemplo.

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

Solución de problemas de efemérides no válidas

Cuando se carga una efeméride personalizada en AWS Ground Station, pasa por un flujo de trabajo de validación asíncrono antes de quedar `ENABLED`. Este flujo de trabajo garantiza que los identificadores del satélite, los metadatos y la trayectoria son válidos.

Cuando una efeméride falla en la validación, `DescribeEphemeris` devolverá un EphemerisInvalidReason, que proporciona información sobre por qué falló la validación de la efeméride. Los valores potenciales de EphemerisInvalidReason son los siguientes:

Valor	Descripción	Acción para la solución de problemas
METADATA_INVALID	Tanto los identificadores de las naves espaciales como el ID del satélite no son válidos.	Compruebe el ID NORAD u otros identificadores proporcionados en los datos de las efemérides
TIME_RANGE_INVÁLIDO	Las horas de inicio, fin o expiración no son válidas para las efemérides proporcionadas.	Asegúrese de que la hora de inicio es anterior a "ahora" (se recomienda fijar la hora de inicio unos minutos antes), que la hora de finalización es posterior a la hora de inicio y que la hora de finalización es posterior a la hora de expiración.
TRAJECTORY_INVALID	Las efemérides proporcionadas definen una trayectoria no válida de la nave espacial	Confirme que la trayectoria proporcionada es continua y corresponde al satélite correcto.
ERROR DE VALIDACIÓN	Se ha producido un error interno de servicio al procesar las efemérides para la validación	Volver a cargar

A continuación se muestra un ejemplo de respuesta `DescribeEphemeris` para una efeméride `INVALID`:

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

Volver a los datos de efemérides predeterminados

Al cargar datos de efemérides personalizados, anularán los usos predeterminados de efemérides para ese satélite en particular AWS Ground Station . AWS Ground Station no volverá a utilizar las efemérides predeterminadas hasta que no haya ninguna efeméride proporcionada por el cliente que esté habilitada y no haya caducado y esté disponible para su uso. AWS Ground Station tampoco muestra los contactos que hayan pasado la fecha de caducidad de las efemérides actuales proporcionadas por el cliente, incluso si hay una efeméride predeterminada disponible después de esa fecha de caducidad.

Para volver a las efemérides predeterminadas de Space Track, deberá realizar una de las siguientes acciones:

- Borrar (usando `DeleteEphemeris`) o deshabilitar (usando `UpdateEphemeris`) todas las efemérides proporcionadas por el cliente. Puede enumerar las efemérides proporcionadas por el cliente para un satélite usando `ListEphemerides`.
- Esperar a que caduquen todas las efemérides proporcionadas por el cliente.

Puede confirmar que se están utilizando las efemérides predeterminadas llamando a `GetSatellite` y verificando que la `source` de las efemérides actuales para el satélite es `SPACE_TRACK`. Consulte Datos de efemérides predeterminadas para obtener más información sobre las efemérides predeterminadas.

AWS Ground Station Máscaras de sitio

Cada ubicación de AWS Ground Station antena tiene máscaras de sitio asociadas. Estas máscaras impiden que las antenas de esa ubicación transmitan o reciban cuando apuntan hacia determinadas direcciones, normalmente cerca del horizonte. Las máscaras deben tener en cuenta:

- Características del terreno geográfico que rodea la antena. Por ejemplo, montañas o edificios que podrían bloquear una señal de radiofrecuencia (RF) o impedir la transmisión.
- Interferencias de radiofrecuencia (RFI): afectan tanto a la capacidad de recepción (fuentes externas de RFI que afectan al enlace descendente de la señal en las antenas de AWS Ground Station) como a la de transmisión (la señal de RF transmitida por las antenas de AWS Ground Station afecta negativamente a los receptores externos).
- Autorizaciones legales Las autorizaciones locales para que opere AWS Ground Station en cada región pueden incluir restricciones específicas, como un ángulo de elevación mínimo para transmitir.

Estas máscaras de sitio pueden cambiar con el tiempo. Por ejemplo, pueden construirse nuevos edificios cerca de la ubicación de una antena, pueden cambiar las fuentes de RFI o puede renovarse la autorización legal con restricciones diferentes. Las máscaras de sitio de AWS Ground Station están disponibles para los clientes en virtud de un acuerdo de confidencialidad (NDA).

Máscaras específicas del cliente

Además de las máscaras de sitio de AWS Ground Station en cada sitio, cada cliente puede tener máscaras adicionales debido a restricciones de su propia autorización legal para comunicarse con sus satélites en una región determinada. Estas máscaras se pueden configurar en AWS Ground Station para case-by-case garantizar la conformidad al utilizar AWS Ground Station para comunicarse con estos satélites. Póngase en contacto con el equipo de AWS Ground Station para obtener más información.

Impacto de las máscaras del sitio en los tiempos de contacto disponibles

Hay dos tipos de máscaras de sitio: máscaras de sitio de enlace ascendente (transmisión) y máscaras de sitio de enlace descendente (recepción).

Al enumerar los tiempos de contacto disponibles mediante la ListContacts operación, AWS Ground Station devolverá los tiempos de visibilidad en función del momento en que el satélite se eleve por encima y se coloque por debajo de la máscara del enlace descendente. Los horarios de contacto disponibles se basan en esta ventana de visibilidad oculta en el enlace descendente. Esto garantiza que los clientes no reserven o paguen por un tiempo cuando su satélite está bajo la máscara de enlace descendente.

Las máscaras de sitios de enlace ascendente no afectan a los tiempos de contacto disponibles, incluso si el perfil de la misión incluye un enlace de subida de antena en la periferia de un flujo de datos. Esto permite a los clientes utilizar todo el tiempo de contacto disponible para el enlace descendente, incluso si el enlace ascendente no está disponible durante parte de ese tiempo debido a la máscara de sitio de enlace ascendente. Sin embargo, es posible que la señal de enlace ascendente no se transmita durante parte o la totalidad del tiempo reservado para un contacto por satélite. Los clientes son responsables de tener en cuenta la máscara de enlace ascendente que se proporciona al programar las transmisiones de enlace ascendente.

La parte de un contacto que no está disponible para el enlace ascendente varía en función de la trayectoria del satélite durante el contacto, en relación con la máscara del sitio de enlace ascendente en la ubicación de la antena. En las regiones en las que las máscaras de sitio de enlace ascendente y enlace descendente son similares, esta duración suele ser corta. En otras regiones, donde la máscara del enlace ascendente es considerablemente más alta que la máscara del enlace descendente, esto puede provocar que una parte significativa, o incluso toda, la duración del contacto no esté disponible para el enlace ascendente. Se factura al cliente el tiempo de contacto completo, aunque parte del tiempo reservado no esté disponible para el enlace ascendente.

Historial de documentos de la Guía AWS Ground Station del usuario

En la siguiente tabla se describen los cambios importantes en la documentación desde la última versión de AWS Ground Station.

Cambio	Descripción	Fecha de lanzamiento
Nueva característica	Los contactos ahora se pueden programar hasta 30 segundos fuera de los rangos de tiempo de visibilidad. Los tiempos de visibilidad se incluyen en DescribeContact las respuestas.	26 de marzo de 2024
Actualización de documentación	Se mejoró la organización y se agregó la sección «Selección de instancias de EC2 y planificación de la CPU».	6 de marzo de 2024
Actualización de documentación	Se agregaron nuevas prácticas recomendadas a la Guía del usuario del AWS Ground Station agente para ejecutar servicios y procesos junto con el AWS Ground Station agente.	23 de febrero de 2024
Actualización de documentación	Se agregó la página de notas de lanzamiento del agente.	21 de febrero de 2024
Actualización de plantilla	Se agregó soporte para una subred pública independiente en la DataDelivery plantilla DirectBroadcastSatelliteWbDigIfEc 2.	14 de febrero de 2024
Actualización de documentación	Se agregó la referencia a AWS Notificaciones de usuario en la documentación de monitoreo.	6 de agosto de 2023
Actualización de documentación	Se agregaron instrucciones para etiquetar los satélites con un nombre que se muestre en la AWS Ground Station consola.	26 de julio de 2023

Cambio	Descripción	Fecha de lanzamiento
Nueva característica	Se agregó la guía del usuario del AWS Ground Station agente para el lanzamiento de Wideband DigiF Data Delivery	12 de abril de 2023
Actualizaciones de la política gestionada por AWS: nueva política AWS gestionada	AWS Ground Station agregó una nueva política llamada AWSGroundStationAgentInstancePolicy.	12 de abril de 2023
Nueva característica	Se ha actualizado la guía del usuario para el lanzamiento de CPE Preview.	9 de noviembre de 2022
Actualizaciones de la política gestionada por AWS: nueva política AWS gestionada	AWS Ground Station se agregó la AWSServiceRoleForGroundStationDataflowEndpointGroup service-linked-role (SLR) que incluye una nueva política denominada AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy.	2 de noviembre de 2022
Nueva característica	Se actualizó la guía del usuario para incluir la integración con AWS CLI.	17 de abril de 2020
Nueva característica	Se actualizó la guía del usuario para incluir la integración con CloudWatch Metrics.	24 de febrero de 2020
Nueva plantilla	Se agregaron satélites de transmisión pública (AquaSnppJpss plantilla) a la guía del AWS Ground Station usuario.	19 de febrero de 2020
Nueva característica	Se ha actualizado la guía del usuario para incluir la entrega de datos entre regiones.	5 de febrero de 2020
Actualización de documentación	Se han actualizado los ejemplos y las descripciones para la monitorización AWS Ground Station con CloudWatch eventos.	4 de febrero de 2020

Cambio	Descripción	Fecha de lanzamiento
Actualización de documentación	Se han actualizado las ubicaciones de las plantillas y se han revisado las secciones Introducción y Solución de problemas.	19 de diciembre de 2019
Nueva sección de solución de problemas	Se ha añadido una sección de resolución de problemas a la la Guía del usuario de AWS Ground Station .	7 de noviembre de 2019
Nuevo tema de introducción	Se ha actualizado el tema de introducción, que incluye las AWS CloudFormation plantillas más actuales.	1 de julio de 2019
Versión para Kindle	Publicada la versión Kindle de la Guía del usuario de AWS Ground Station .	20 de junio de 2019
Nuevo servicio y guía	Esta es la versión inicial AWS Ground Station y la Guía AWS Ground Station del usuario.	23 de mayo de 2019

Glosario de AWS

Para ver la terminología más reciente de AWS, consulte el Glosario de AWS en la Referencia de Glosario de AWS.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.