Guía del usuario

AWS Ground Station

AWS Ground Station: Guía del usuario

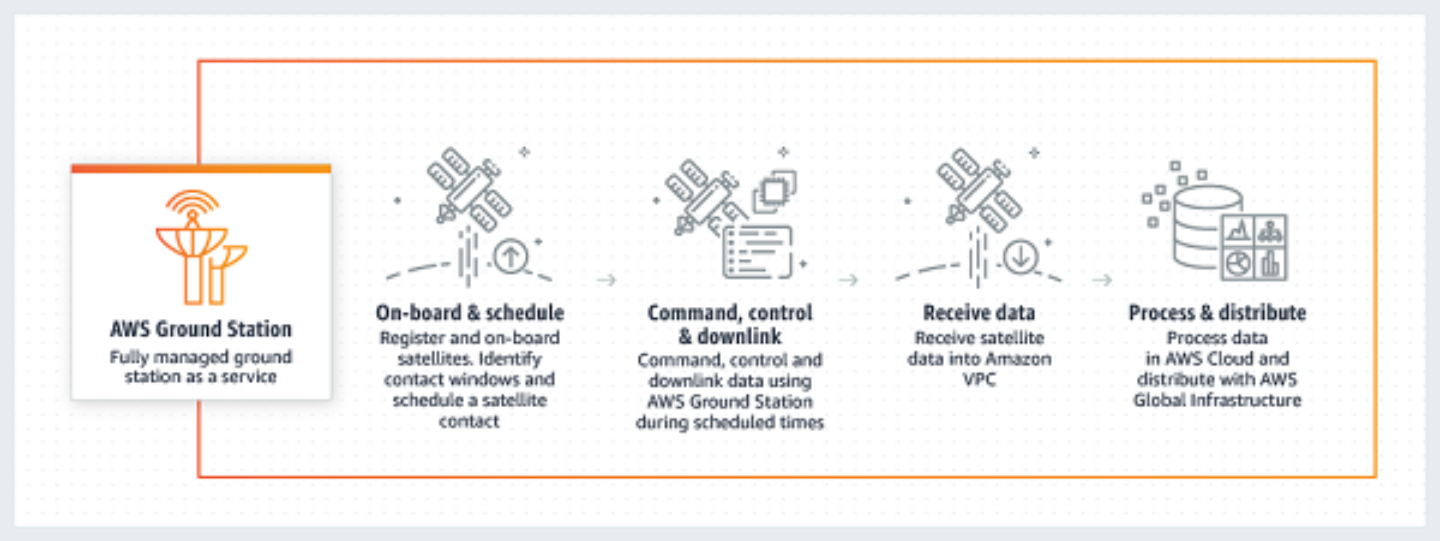
Table of Contents

¿Qué es AWS Ground Station?

AWS Ground Station es un servicio totalmente gestionado que proporciona comunicaciones por satélite seguras, rápidas y predecibles en una infraestructura global. Con AWS Ground Station ello, ya no tendrá que crear, gestionar ni escalar su propia infraestructura de estación terrestre. AWS Ground Station le permite centrarse en innovar y experimentar rápidamente con nuevas aplicaciones que ingieren datos satelitales, en lugar de gastar recursos en construir, operar y escalar sus propias estaciones terrestres.

Con la red de fibra global de baja latencia y gran ancho de banda de AWS, puede empezar a procesar sus datos satelitales en cuestión de segundos después de su recepción en el sistema de antenas. Esto le permite convertir los datos sin procesar en información procesada o conocimiento analizado en cuestión de segundos.

Casos de uso comunes



AWS Ground Station le permite comunicarse con sus satélites de forma bidireccional y es compatible con los siguientes casos de uso:

- Datos de enlace descendente: reciba datos de sus satélites, que transmiten frecuencias de banda X y banda S, y envíelos a una EC2 instancia de Amazon en tiempo real (formato VITA-49) o directamente a un bucket de Amazon S3 de su cuenta (formato PCAP). Además, en el caso de los satélites que utilizan un esquema de modulación y codificación compatible, puede elegir

entre recibir datos demodulados y decodificados o muestras digitales sin procesar de frecuencia intermedia (DigiF) (formato VITA-49).

- Datos de enlace ascendente: envíe datos y comandos a sus satélites, que reciben frecuencias de banda S, mediante el envío de datos DigiF (formato VITA-49) para su transmisión. AWS Ground Station
- Eco de enlace ascendente: valide los comandos enviados a su nave espacial y realice otras tareas avanzadas al recibir la señal transmitida en una antena ubicada físicamente en el mismo lugar.
- Radio definida por software (SDR) /procesador frontal (FEP): utilice su SDR existente, sus formas de onda existentes y and/or FEP, that's capable of running on an Amazon EC2 instance, to process your data in real-time to send/receive genere sus productos de datos.
- Telemetría, seguimiento y comando (TT&C): realice la TT&C utilizando una combinación de los casos de uso enumerados anteriormente para gestionar su flota de satélites.
- Entrega de datos entre regiones: gestione varios contactos simultáneos mediante AWS Ground Station la red de antenas global desde una sola región de AWS.
- Gemelo digital: programación de pruebas, verificación de las configuraciones y gestión adecuada de los errores a un costo reducido sin utilizar la capacidad de la antena de producción.

Pasos a seguir a continuación

Le recomendamos que comience leyendo las secciones siguientes:

- Para conocer AWS Ground Station los conceptos esenciales, consulteCómo AWS Ground Station funciona.
- Para obtener información sobre cómo configurar su cuenta y los recursos que puede utilizar AWS Ground Station, consulteIntroducción.
- Para utilizarlos mediante programación AWS Ground Station, consulta la referencia de la AWS Ground Station API. La referencia de la API describe en detalle todas las operaciones de la AWS Ground Station API. También proporciona ejemplos de solicitudes, respuestas y errores de los protocolos de servicios web compatibles. Puede usar la AWS CLI o un AWS SDK en el idioma que prefiera para escribir código con AWS Ground Station el que interactúe.

Cómo AWS Ground Station funciona

AWS Ground Station opera antenas terrestres para facilitar la comunicación con su satélite. Las características físicas de lo que pueden hacer las antenas se resumen y se denominan capacidades. En la AWS Ground Station Ubicaciones sección se puede consultar la ubicación física de la antena junto con sus capacidades actuales. Póngase en contacto con nosotros en <aws-groundstation@amazon.com> si su caso de uso requiere capacidades adicionales, ofertas de ubicación adicionales o ubicaciones de antenas más precisas.

Para usar una de las AWS Ground Station antenas, debe reservar una hora en una ubicación específica. Esta reserva se denomina contacto. Para programar correctamente un contacto, se AWS Ground Station requieren datos adicionales para garantizar su éxito.

- Su satélite debe estar embarcado en una o más ubicaciones, lo que garantiza que cuenta con la aprobación necesaria para operar las distintas capacidades en la ubicación solicitada.
- El satélite debe tener una efeméride válida: esto garantiza que las antenas tengan una línea de visión y puedan apuntar con precisión al satélite durante el contacto.
- Debe tener un perfil de misión válido: esto le permite personalizar el comportamiento de este contacto, incluida la forma en que recibirá y enviará los datos a su satélite. Puedes utilizar varios perfiles de misión para el mismo vehículo a fin de crear diferentes contactos que se adapten a las distintas posturas operativas o situaciones a las que te enfrentes.

Incorporación de satélites

La incorporación de un satélite AWS Ground Station es un proceso de varios pasos que incluye la recopilación de datos, la validación técnica, la concesión de licencias de espectro, además de la integración y las pruebas. La sección de incorporación de satélites de la guía le explicará este proceso.

Composición del perfil de la misión

La información sobre la frecuencia del satélite, la información del plano de datos y otros detalles se encapsulan en un perfil de misión. El perfil de la misión es un conjunto de componentes de configuración. Esto te permite reutilizar los componentes de configuración en diferentes perfiles de misión según tu caso de uso. Como los perfiles de misión no hacen referencia directa a los satélites

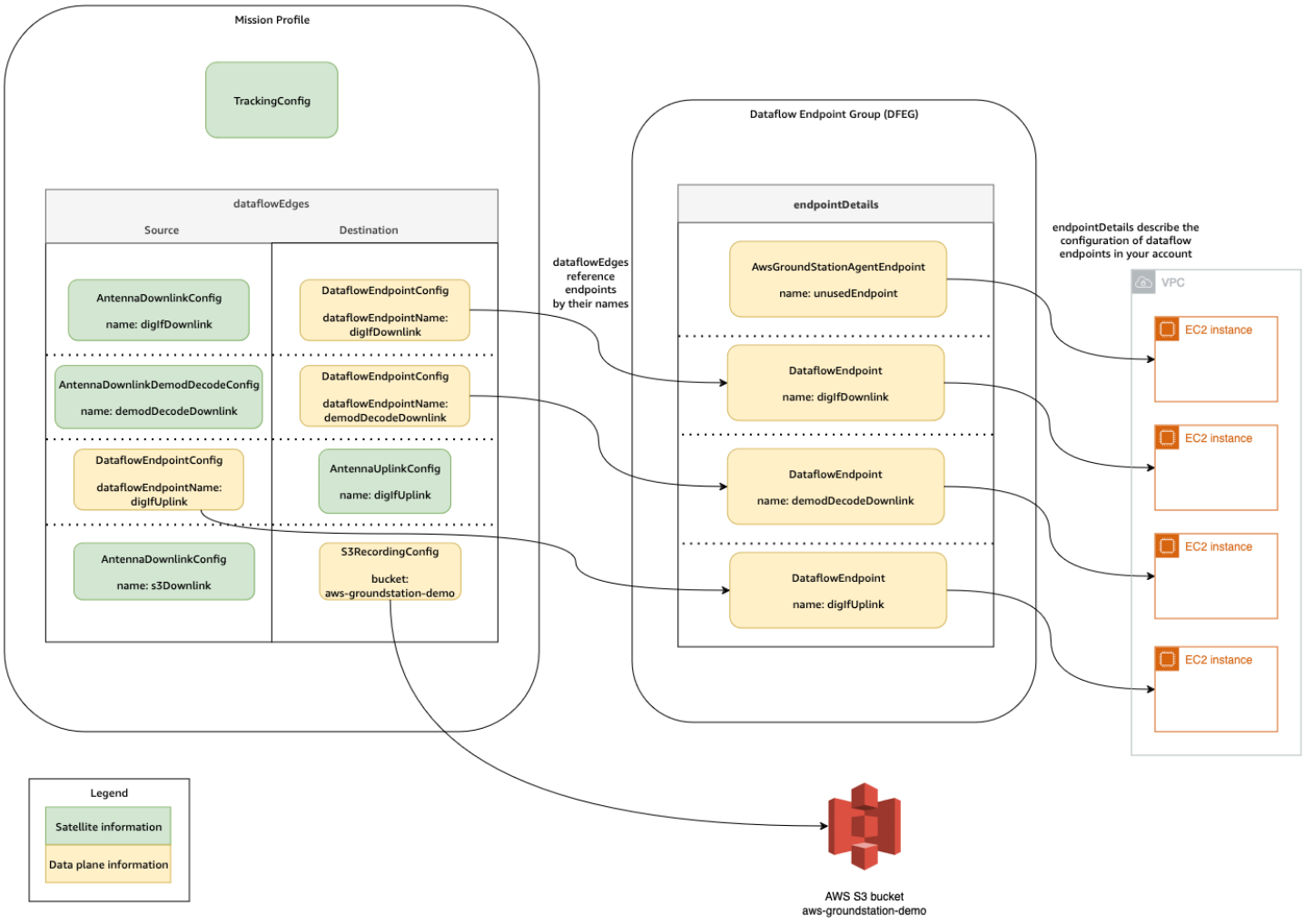
individuales, sino que solo contienen información sobre sus capacidades técnicas, varios satélites que tengan la misma configuración también pueden reutilizar los perfiles de misión.

Un perfil de misión válido tendrá una configuración de seguimiento y uno o más flujos de datos. La configuración de seguimiento especificará tu preferencia de seguimiento durante un contacto. Cada par de configuraciones de un flujo de datos establece un origen y un destino. Según el satélite y sus modos de funcionamiento, el número exacto de flujos de datos variará en un perfil de misión para representar las rutas de comunicación de enlace ascendente y descendente, así como cualquier aspecto del procesamiento de datos.

- Para obtener más información sobre la configuración de los EC2 recursos de Amazon VPC, Amazon S3 y Amazon que se utilizarán durante un contacto, consulte. Trabaje con flujos de datos
- Para obtener detalles sobre el comportamiento de cada configuración, consulte. Usa AWS Ground Station configuraciones
- Para obtener detalles específicos sobre todos los parámetros esperados, consulteUsa perfiles AWS Ground Station de misión.
- Para ver ejemplos sobre cómo se pueden crear varios perfiles de misión para respaldar su caso de uso, consulteEjemplos de configuraciones de perfil de misión.

El siguiente diagrama muestra un ejemplo del perfil de la misión y los recursos adicionales necesarios. Tenga en cuenta que el ejemplo muestra un punto final de flujo de datos que no es necesario para este perfil de misión, denominado UnuseEndpoint, para demostrar su flexibilidad. El ejemplo admite los siguientes flujos de datos:

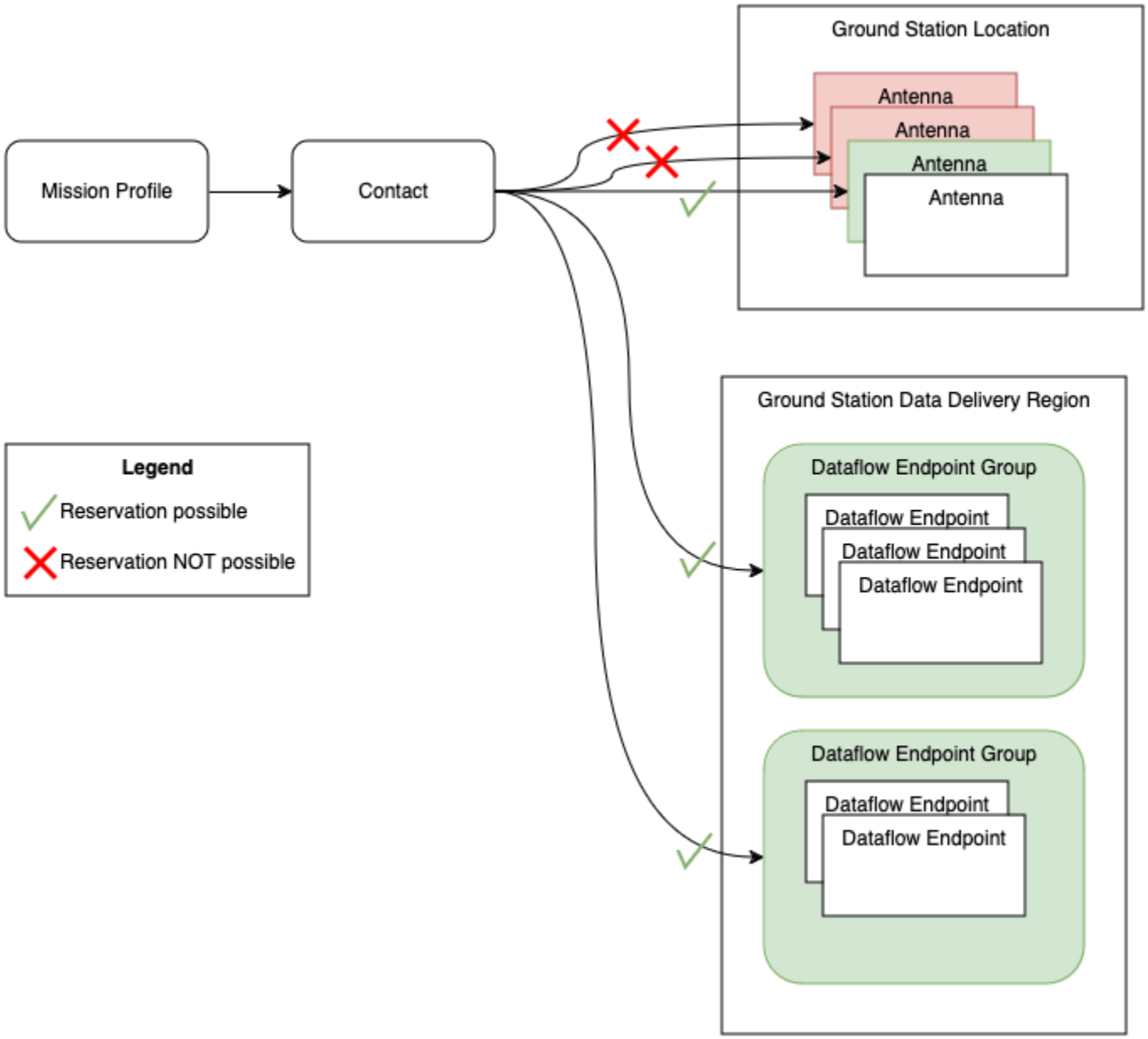
- Enlace descendente sincrónico de datos digitales de frecuencias intermedias a una EC2 instancia de Amazon que gestione. Denotado por el nombre. digIfDownlink
- Enlace descendente asíncrono de datos digitales de frecuencias intermedias a un bucket de Amazon S3. Se indica mediante el nombre del bucket. aws-groundstation-demo
- Enlace descendente sincrónico de datos desmodulados y decodificados a una instancia de Amazon EC2 que gestione. Denotado por el nombre. demodDecodeDownlink
- Enlace ascendente sincrónico de datos desde una EC2 instancia de Amazon que gestionas a una antena AWS Ground Station gestionada. Denotado por el nombre. digIfUplink



Programación de contactos

Con un perfil de misión válido, puede solicitar un contacto con los satélites a bordo. La solicitud de reserva de contactos es asincrónica para que el servicio de antenas global tenga tiempo de cumplir un horario uniforme en todas las regiones implicadas. AWS Durante este proceso, se evalúan varias antenas en la ubicación de la estación terrestre solicitada para determinar si están disponibles y son capaces de procesar el contacto. Durante este proceso, también se evalúan los puntos finales del flujo de datos configurados para determinar su disponibilidad. Mientras se lleva a cabo esta evaluación, el estado del contacto aparecerá en SCHEDULING.

Este proceso de programación asincrónica finalizará cinco minutos después de la solicitud, pero normalmente finaliza en un minuto. Compruebe la supervisión basada en eventos Automatice AWS Ground Station con eventos durante el horario de programación.



Los contactos que se pueden realizar y que tienen disponibilidad dan como resultado contactos PROGRAMADOS. Con un contacto programado, los recursos necesarios para realizar el contacto se han reservado en las regiones de AWS necesarias, tal como se define en el perfil de su misión. Los contactos que no se puedan realizar o que tengan partes no disponibles generarán contactos con FAILED_TO_SCHEDULE. Consulte para obtener detalles sobre la depuración. Solucionar problemas de contactos de FAILED_TO_SCHEDULE

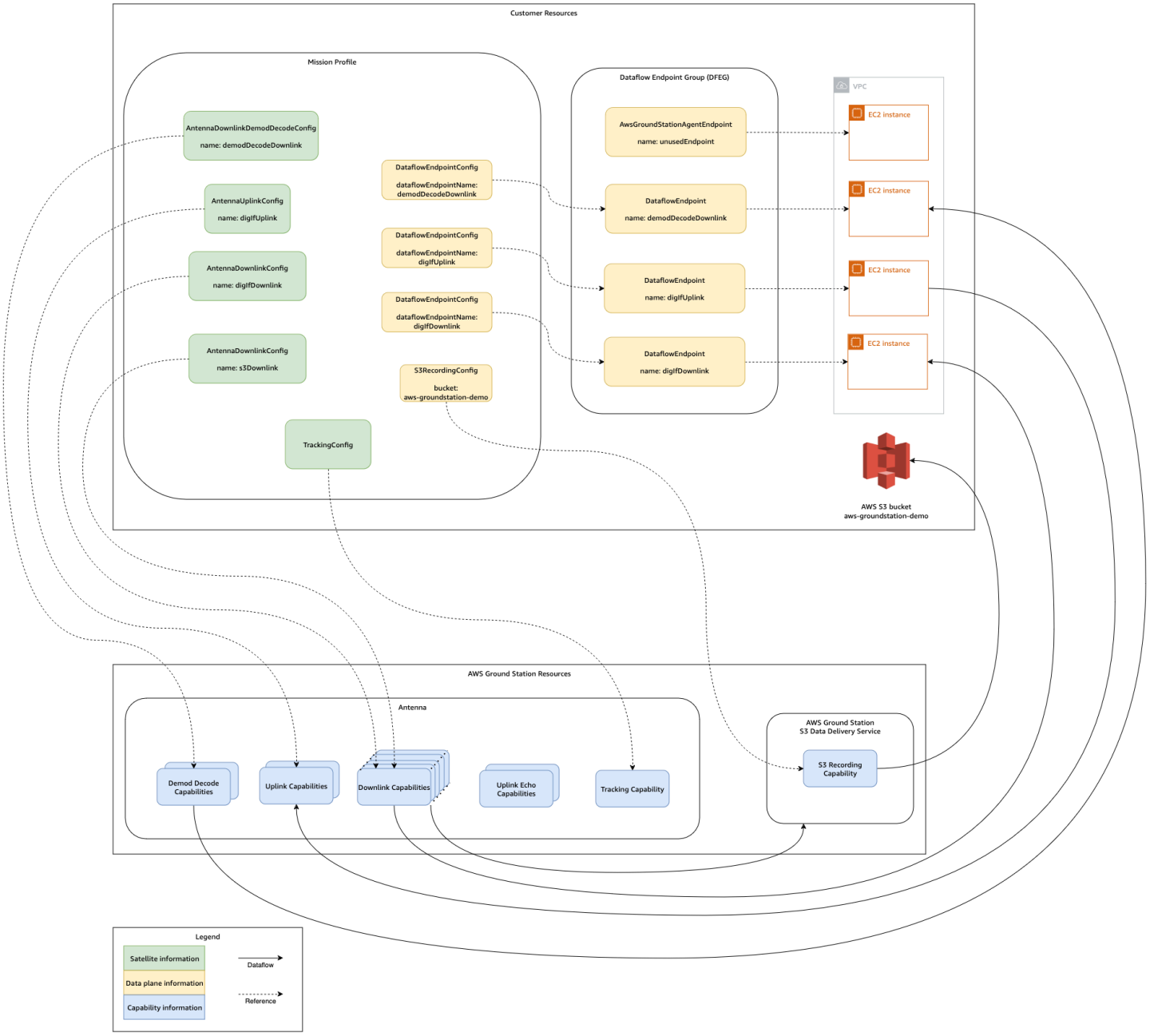
Ejecución de contactos

AWS Ground Station organizará automáticamente los recursos gestionados por AWS durante la reserva de contactos. Si corresponde, usted es responsable de organizar los EC2 recursos definidos en el perfil de su misión como puntos de enlace del flujo de datos. AWS Ground Station proporciona AWS EventBridge Events para automatizar la organización de sus recursos y reducir los costos. Consulte Automatice AWS Ground Station con eventos para obtener más detalles.

Durante el contacto, la telemetría sobre el rendimiento del contacto se envía a AWS. CloudWatch Para obtener información sobre cómo monitorear su contacto durante la ejecución, consulte. Comprenda la supervisión con AWS Ground Station

El siguiente diagrama continúa con el ejemplo anterior y muestra los mismos recursos orquestados durante el contacto.

> **Note**
>
> En este ejemplo, no se utilizaron todas las capacidades de la antena. Por ejemplo, hay más de una docena de capacidades de enlace descendente de antena disponibles en cada antena que admiten múltiples frecuencias y polarizaciones. Para obtener más información sobre la cantidad de cada tipo de capacidad disponible en AWS Ground Station las antenas y sus frecuencias y polarizaciones compatibles, consulte. AWS Ground Station Capacidades del sitio



Al final de su contacto, AWS Ground Station evaluará su rendimiento y determinará su estado final. Los contactos en los que no se detecten errores tendrán como resultado un estado de contacto COMPLETADO. Los contactos en los que los errores de servicio hayan provocado problemas en la entrega de datos durante el contacto generarán un AWS_FAILEDestado. Los contactos en los que los errores del cliente o usuario hayan provocado problemas en la entrega de datos durante el contacto tendrán un estado FALLIDO. Los errores fuera del horario de contacto, es decir, durante la fase previa o posterior a la transferencia, no se tienen en cuenta durante la adjudicación.

Para obtener más información, consulta Comprenda el ciclo de vida de.

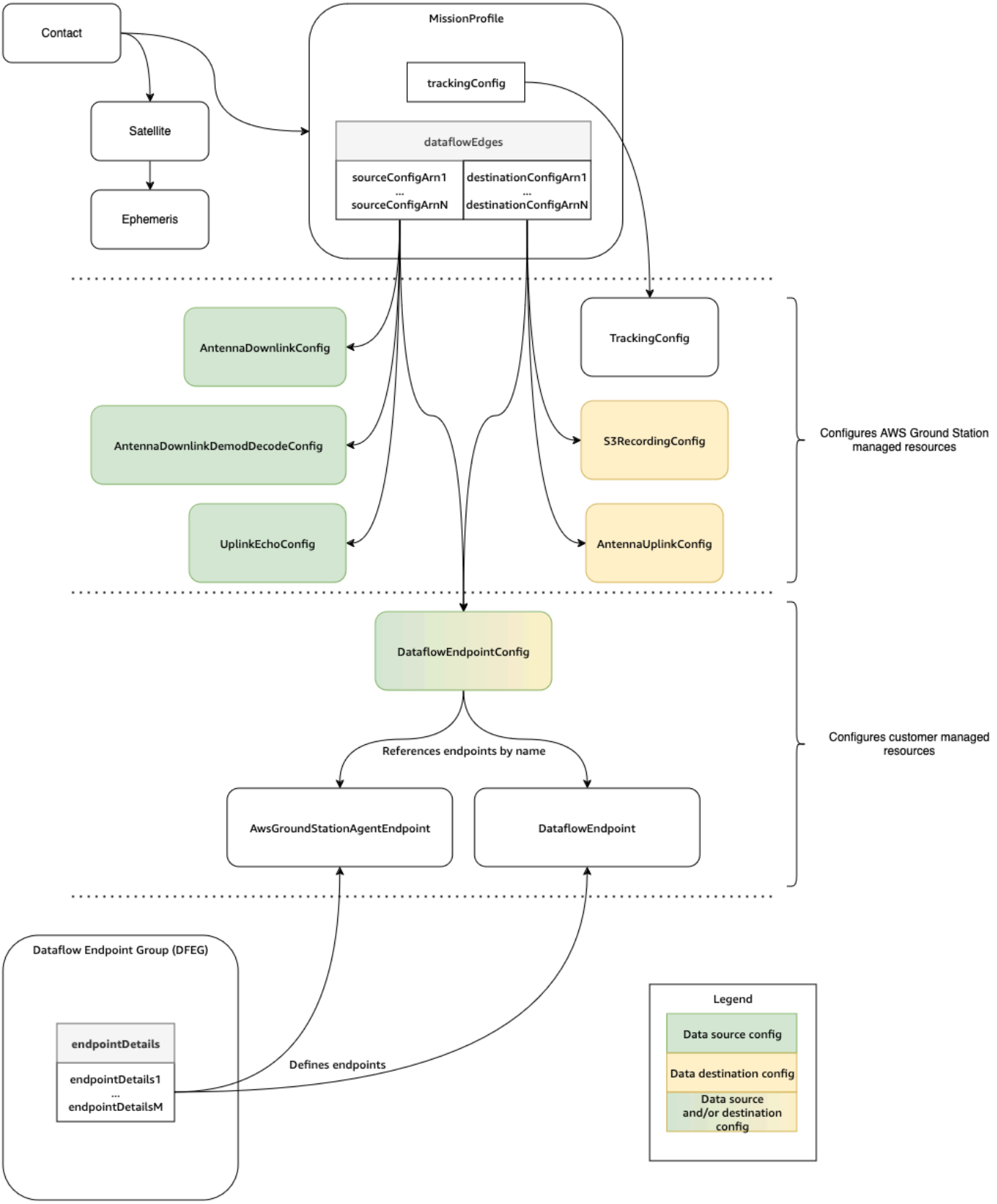
Gemelo digital

La función de gemelo digital AWS Ground Station le permite programar los contactos en función de las ubicaciones virtuales de las estaciones terrestres. Estas estaciones terrestres virtuales son réplicas exactas de las estaciones terrestres de producción, incluidas las capacidades de antena, las máscaras de sitio y las coordenadas GPS reales. La función de gemelo digital le permite probar su flujo de trabajo de orquestación de contactos por una fracción del costo en comparación con las estaciones terrestres de producción. Para obtener más información, consulte Utilice la función de gemelo AWS Ground Station digital.

Comprenda los componentes AWS Ground Station principales

En esta sección se proporcionan definiciones detalladas de los componentes principales de AWS Ground Station.

El siguiente diagrama muestra los componentes principales AWS Ground Station y cómo se relacionan entre sí. Las flechas indican la dirección de las dependencias entre los componentes, donde cada componente apunta a sus dependencias.


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

En los temas siguientes se describen los componentes AWS Ground Station principales en detalle.

Temas

Usa perfiles AWS Ground Station 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.

Los perfiles de misión se pueden compartir entre satélites que comparten las mismas características de radio. Puede crear grupos de puntos finales de flujo de datos adicionales para limitar el número máximo de contactos simultáneos que desee establecer para su constelación.

Las configuraciones de seguimiento se especifican como un campo único dentro del perfil de la misión. Las configuraciones de seguimiento se utilizan para especificar tu preferencia a la hora de utilizar el seguimiento por programas y el seguimiento automático durante el contacto. Para obtener más información, consulte Configuración de seguimiento.

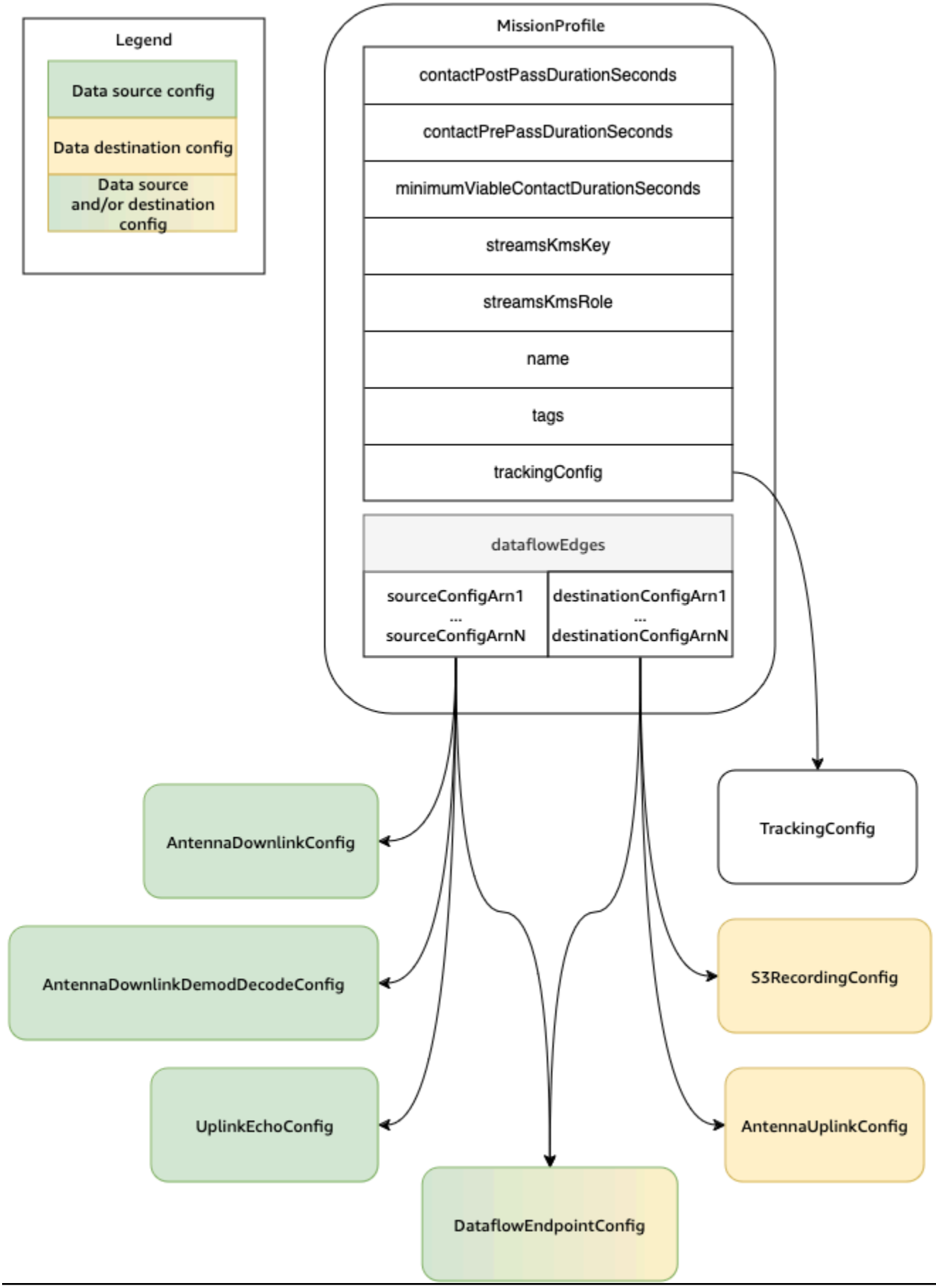
Todas las demás configuraciones se incluyen en el `dataflowEdges` campo del perfil de la misión. Estas configuraciones pueden considerarse nodos de flujo de datos, cada uno de los cuales representa un recurso AWS Ground Station administrado que puede enviar o recibir datos y su configuración asociada. El `dataflowEdges` campo define qué nodos de flujo de datos de origen y destino (configuraciones) se necesitan. Un único borde de flujo de datos es una lista de dos nombres de recursos de Amazon (ARNs) de configuración: 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. Para obtener más información, consulte Usa AWS Ground Station configuraciones.

Las `contactPrePassDurationSeconds` y te `contactPostPassDurationSeconds` permiten especificar las horas en relación con el contacto en el que recibirás una CloudWatch notificación de

evento. Para obtener una cronología de los eventos relacionados con su contacto, leaComprenda el ciclo de vida de.

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

`streamsKmsKeyLos` `streamsKmsRole` y se utilizan para definir el cifrado utilizado AWS Ground Station para la entrega de datos con AWS Ground Station Agent. Consulte Cifrado de datos durante el tránsito para AWS Ground Station.


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

En la siguiente documentación se incluye una lista completa de parámetros y ejemplos.

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

Usa AWS Ground Station 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. Las configuraciones se pueden agrupar en dos categorías:

- Configuraciones de seguimiento
- Configuraciones de flujo de datos

A TrackingConfiges el único tipo de configuración de seguimiento. Se utiliza para configurar el ajuste de seguimiento automático de la antena durante un contacto y es obligatorio en el perfil de una misión.

Las configuraciones que se pueden usar en un flujo de datos de un perfil de misión pueden considerarse nodos de flujo de datos, cada uno de los cuales representa un recurso AWS Ground Station administrado que puede enviar o recibir datos. Un perfil de misión requiere al menos un par de estas configuraciones, una que represente una fuente de datos y la otra que represente un destino. Estas configuraciones se resumen en la siguiente tabla.

Config name	Origen/destino del flujo de datos
AntennaDownlinkConfig	Origen
AntennaDownlinkDemodDecodeConfig	Origen
UplinkEchoConfig	Origen
S3 RecordingConfig	Destino
AntennaUplinkConfig	Destino
DataflowEndpointConfig	Origen y/o destino

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

AWS Ground Station utilizará un seguimiento programático que apuntará en función de tus efemérides cuando no se utilice el seguimiento automático. Consulte Comprenda cómo se AWS Ground Station utilizan los datos de efemérides satelitales para obtener detalles sobre cómo se construyen las efemérides.

Autotrack utilizará el seguimiento del programa hasta encontrar la señal esperada. Una vez que eso ocurra, seguirá rastreando en función de la intensidad de la señal.

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.

Esta configuración representa un nodo fuente en un flujo de datos. Es responsable de digitalizar los datos de radiofrecuencia. Los datos transmitidos desde este nodo seguirán el formato de datos de señal/IP. Para obtener información más detallada sobre cómo construir flujos de datos con esta configuración, consulte Trabaje con flujos de datos

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 configuraciones de enlace descendente de antenas mediante AWS CloudFormation la API o la API AWS Command Line Interface. AWS Ground Station

- 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 decodificación de demodo de enlace descendente de antena son un tipo de configuración más complejo y personalizable que se puede utilizar para ejecutar contactos de enlace descendente con demodulación y/o decodificación.
`<Si estás interesado en ejecutar este tipo de contactos, ponte en contacto con e`
Le ayudaremos a definir la configuración y el perfil de misión correctos según su caso de uso.

Esta configuración representa un nodo fuente en un flujo de datos. Es responsable de digitalizar los datos de radiofrecuencia y de realizar la demodulación y la decodificación según lo especificado. Los datos transmitidos desde este nodo seguirán el formato. Demodulated/Decoded Data/IP Para obtener información más detallada sobre cómo construir flujos de datos con esta configuración, consulte Trabaje con flujos de datos

Consulte la siguiente documentación para obtener más información sobre cómo realizar operaciones en las configuraciones de decodificación demod de enlace descendente de antena 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 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 repetición de enlace de subida de antena.

Esta configuración representa un nodo de destino en un flujo de datos. Convertirá la señal de datos de radiofrecuencia digitalizada proporcionada en una señal analógica y la emitirá para que la reciba el satélite. Se espera que los datos transmitidos a este nodo cumplan con el formato de datos de señal/IP. Para obtener información más detallada sobre cómo construir flujos de datos con esta configuración, consulte Trabaje con flujos de datos

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 o la API AWS Command Line Interface. AWS Ground Station

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

Configuración de repetición de enlace de subida de antena

Las configuraciones de repetición de enlace de subida indican a la antena cómo ejecutar una repetición de enlace de subida. Se puede utilizar un eco de enlace ascendente para validar los comandos enviados a la nave espacial y realizar otras tareas avanzadas. Esto se consigue registrando la señal real transmitida por la AWS Ground Station antena (es decir, el enlace

ascendente). Esto hace eco de la señal enviada por la antena al punto final del flujo de datos y debe coincidir con la señal transmitida. 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.

Esta configuración representa un nodo fuente en un flujo de datos. Los datos transmitidos desde este nodo cumplirán con el formato IP o datos de señal. Para obtener información más detallada sobre cómo construir flujos de datos con esta configuración, consulte Trabaje con flujos de datos

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

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

Configuración de punto de enlace de flujo de datos

> **Note**
>
> Las configuraciones de punto final 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 de enlace del flujo de datos en la AWS región que contenga todos los puntos de enlace del flujo de datos especificados en las configuraciones de puntos finales del flujo de datos incluidas en su perfil de misión. Si se encuentra un grupo de puntos finales de flujo de datos adecuado, el estado del contacto pasará a ser programado; de lo contrario, pasará a ser FAILED_TO_SCHEDULE. Para obtener más información sobre los posibles estados de un contacto, consulte. AWS Ground Station estados de contacto

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, AWS Ground Station busca un punto final del flujo de datos en la región especificada. 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 Trabaje con flujos de datos para obtener más información sobre los flujos de datos entre regiones.

Consulte Utilice grupos de AWS Ground Station puntos finales de Dataflow para obtener consejos sobre cómo los diferentes esquemas de nomenclatura para sus flujos de datos pueden beneficiar su caso de uso.

Para obtener información más detallada sobre cómo construir flujos de datos con esta configuración, consulta Trabaje con flujos de datos

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 API o la AWS CloudFormation 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

Config de grabación de Amazon S3

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

Esta configuración representa un nodo de destino en un flujo de datos. Este nodo encapsulará los datos entrantes del nodo de origen del flujo de datos en datos pcap. Para obtener información más

detallada sobre cómo construir flujos de datos con esta configuración, consulte Trabaje con flujos de datos

Puede usar las configuraciones de grabación de S3 para especificar un bucket de Amazon S3 al que desea que se entreguen los datos de enlace descendente junto con la convención de nomenclatura utilizada. A continuación, se especifican las restricciones y los detalles sobre estos parámetros:

- 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 puede actualizarse tras la creación con el identificador del recurso de configuración.

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"
        }
      }
    }
  ]
```

```
}
```

- 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 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/*"
      ]
    }
  ]
}
```

- El prefijo se utilizará al asignar un nombre al objeto de datos de S3. Puede especificar claves opcionales para la sustitución; estos valores se sustituirán por la información correspondiente de sus datos de contacto. Por ejemplo, se `{satellite_id}/{year}/{month}/{day}` sustituirá el prefijo de y el resultado será un resultado como `fake_satellite_id/2021/01/10`

  Teclas opcionales de sustitución: `{satellite_id}` | `{config-name}` | `{config-id}` | `{year}` | `{month}` | `{day}`

Consulte la siguiente documentación para obtener más información sobre cómo realizar operaciones en S3 grabando configuraciones mediante AWS CloudFormation la AWS Command Line Interface API o la 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

Utilice grupos de AWS Ground Station puntos finales de Dataflow

Los puntos finales del flujo de datos definen la ubicación desde o hacia la que desea que se transmitan los datos de forma sincrónica durante los contactos. 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.

> **Tip**
>
> Los puntos finales del flujo de datos se identifican con el nombre que elija al ejecutar los contactos. No es necesario que estos nombres sean únicos en la cuenta. Esto permite ejecutar múltiples contactos a través de diferentes satélites y antenas al mismo tiempo utilizando el mismo perfil de misión. Esto puede resultar útil si tiene una constelación de satélites que tienen las mismas características de funcionamiento. Puede aumentar el número de grupos de puntos finales del flujo de datos para ajustarlo al número máximo de contactos simultáneos que necesita su constelación de satélites.

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.

> **Important**
>
> Los grupos del punto de conexión de flujo de datos deben estar en un estado `HEALTHY` para programar que los contactos los utilicen. Para obtener información sobre cómo solucionar problemas de grupos de puntos finales de flujos de datos que no están en un estado, consulte. `HEALTHY` Solucione el problema DataflowEndpointGroups si no se encuentra en un estado SALUDABLE

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 AWS CloudFormation AWS Command Line Interface API. AWS Ground Station

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

Puntos de enlace de flujo de datos

Los miembros de un grupo de puntos finales de un flujo de datos son puntos finales de flujo de datos. Hay dos tipos de puntos finales de flujo de datos: puntos finales de agente y puntos finales de flujo de datos.AWS Ground Station Para ambos tipos de puntos finales, debe crear las estructuras de soporte (por ejemplo, direcciones IP) antes de crear el grupo de puntos finales del flujo de datos. Consulte Trabaje con flujos de datos las recomendaciones sobre el tipo de punto final del flujo de datos que debe utilizar y cómo configurar las estructuras de soporte.

En las siguientes secciones se describen los dos tipos de puntos finales compatibles.

> **Important**
>
> Todos los puntos finales del flujo de datos de un único grupo de puntos finales del flujo de datos deben ser del mismo tipo. No se pueden mezclar los puntos finales del AWS Ground Station agente con los puntos finales del flujo de datos en el mismo grupo. Si su caso de uso

requiere ambos tipos de puntos de enlace, debe crear grupos de puntos de enlace de flujo de datos independientes para cada tipo.

AWS Ground Station Punto final del agente

El punto final del AWS Ground Station agente utiliza el AWS Ground Station agente como un componente de software para finalizar las conexiones. Utilice un punto final de flujo de datos de AWS Ground Station agente cuando desee transferir más del 50% de los datos de señal digital. MHz Para crear un AWS Ground Station Agent Endpoint, solo debe rellenar el campo del. `AwsGroundStationAgentEndpoint` EndpointDetails Para obtener más información sobre el AWS Ground Station agente, consulte la Guía del usuario completa del AWS Ground Station agente.

`AwsGroundStationAgentEndpoint` consta de lo siguiente:

- `Name`- El nombre del punto final del flujo de datos. Para que el contacto utilice este punto final del flujo de datos, este nombre debe coincidir con el nombre utilizado en la configuración del punto final del flujo de datos.
- `EgressAddress`- La dirección IP y el puerto utilizados para extraer los datos del agente.
- `IngressAddress`- La dirección IP y el puerto utilizados para introducir los datos en el agente.

Punto final del flujo de datos

El punto final de Dataflow utiliza una aplicación de red como componente de software para finalizar las conexiones. Utilice Dataflow Endpoint cuando desee realizar un enlace ascendente de datos de señal digital, un enlace descendente de menos del 50% de los datos de señal digital o un enlace descendente de datos MHz de señal demodulados/decodificados. Para crear un punto final de flujo de datos, rellene los campos y del. `Endpoint` `Security Details` EndpointDetails

`Endpoint` consta de lo siguiente:

- `Name`- El nombre del punto final del flujo de datos. Para que el contacto utilice este punto final del flujo de datos, este nombre debe coincidir con el nombre utilizado en la configuración del punto final del flujo de datos.
- `Address`- La dirección IP y el puerto utilizados.

`SecurityDetails` consta de lo siguiente:

- `roleArn`- El nombre de recurso de Amazon (ARN) de un rol que AWS Ground Station asumirá la creación de interfaces de red elásticas (ENIs) en la VPC. ENIs Sirven como puntos de entrada y salida de los datos transmitidos durante un contacto.
- `securityGroupIds`: los grupos de seguridad que adjuntar a las interfaces de redes elásticas.
- `subnetIds`- Una lista de subredes en las que AWS Ground Station puede colocar interfaces de red elásticas para enviar transmisiones a sus instancias. Si se especifican varias subredes, deben poder enrutarse entre sí. Si las subredes se encuentran en zonas de disponibilidad diferentes (AZs), es posible que se le cobren cargos por la transferencia de datos entre zonas de disponibilidad.

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 de recurso del punto final no existe, por lo que la política de confianza debe usar un asterisco (*) en lugar de. *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 el. ENIs 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"
      ]
    }
  ]
}
```

Usa AWS Ground Station un agente

El AWS Ground Station agente le permite recibir flujos de datos de frecuencia intermedia digital de banda ancha (DigiF) síncronos (enlace descendente) durante los contactos con AWS Ground Station.

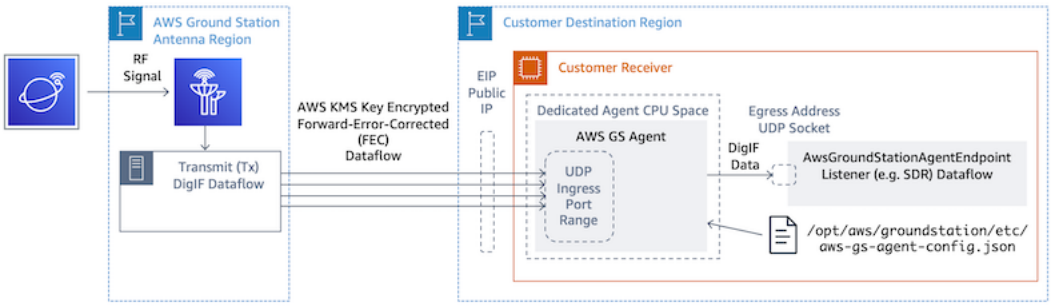
Funcionamiento

Puede seleccionar dos opciones para la entrega de datos:

1. Entrega de datos a una EC2 instancia: entrega de datos a una EC2 instancia de tu propiedad. Usted administra el AWS Ground Station agente. Esta opción puede ser la más adecuada si necesita un procesamiento de datos casi en tiempo real. Consulte la Trabaje con flujos de datos sección para obtener información sobre la entrega de EC2 datos.
2. Entrega de datos a un depósito de S3: la entrega de datos a su depósito de S3 de AWS se gestiona en su totalidad mediante AWS Ground Station. Consulte la guía de Introducción para obtener información sobre el envío de datos a S3.

Ambos modos de entrega de datos requieren la creación de un conjunto de recursos de AWS. Se recomienda encarecidamente el uso de CloudFormation para crear sus 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.

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



Información adicional

Para obtener información más detallada, consulte la Guía del usuario del agente completa.AWS Ground Station

Introducción

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

A continuación, se indican las prácticas recomendadas para AWS Identity and Access Management (IAM) y los permisos que necesitará. Tras configurar las funciones adecuadas, puede empezar a seguir el resto de los pasos.

Inscríbase en 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. Abrir https://portal.aws.amazon.com/billing/registro.
2. Siga las instrucciones que se le indiquen.

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

   Cuando te registras en un Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea un. 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. En cualquier momento, puede ver la actividad de su cuenta actual y administrarla accediendo a 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.

Inicio de sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, use 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 .

Añada AWS Ground Station permisos a su cuenta AWS

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.

Satélite a bordo

La incorporación de un satélite AWS Ground Station es un proceso de varios pasos que incluye la recopilación de datos, la validación técnica y la concesión de licencias de espectro, además de la integración y las pruebas. También se requieren acuerdos de confidencialidad ()NDAs.

Descripción general del proceso de incorporación de clientes

La incorporación de satélites es un proceso manual que se encuentra en la sección Satélites y recursos de la página de la AWS Ground Station consola. A continuación se describe el proceso general.

1. Revise la AWS Ground Station Ubicaciones sección para determinar si su satélite cumple con las características geográficas y de radiofrecuencia.
2. Para empezar a incorporar su satélite a AWS Ground Station, envíe un correo electrónico a `<aws-groundstation@amazon.com>` con un breve resumen de sus necesidades de misión y satélite, incluido el nombre de su organización, las frecuencias requeridas, cuándo se lanzarán o se lanzarán los satélites, el tipo de órbita del satélite y si planea Utilice la función de gemelo AWS Ground Station digital utilizarlos.
3. Una vez que su solicitud haya sido revisada y aprobada, AWS Ground Station solicitará la licencia reglamentaria en las ubicaciones específicas que vaya a utilizar. La duración de este paso variará en función de las ubicaciones y de las normativas vigentes.
4. Una vez obtenida esta aprobación, podrá ver su satélite para que lo utilice. AWS Ground Station le enviará una notificación cuando la actualización se haya realizado correctamente.

(Opcional) Asignar nombres a los satélites

Tras la incorporación, es posible que desee añadir un nombre al registro de satélites para reconocerlo más fácilmente. 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 los satélites de AWS Ground Station se puede realizar mediante la API tag-resource con la CLI de AWS o con una de las herramientas de AWS. SDKs 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 la configuración y los ajustes de credenciales, consulte Ajustes de configuración y 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 mediante 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 de recursos de etiquetas requiere un ARN regional, y el ARN devuelto por los satélites de listas 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 estamos utilizando las comillas, las comillas deben ir AWS CLI precedidas de una barra invertida. La etiqueta tendrá un aspecto similar a

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

A continuación, llamará 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, podrá ver el nombre que estableció para el satélite en la consola de AWS Ground Station .

Cambiar el nombre de un satélite

Si desea cambiar el nombre de un satélite, simplemente puede volver a llamar a tag-resource con el ARN del satélite con la misma "Name" clave, pero con un valor diferente 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 establecido para un satélite se puede eliminar 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
```

Satélites de radiodifusión pública

Además de incorporar sus propios satélites, puede solicitar la incorporación a satélites de transmisión pública compatibles que proporcionen una vía de comunicación de enlace descendente de acceso público. Esto le permite utilizar el enlace descendente AWS Ground Station de datos de estos satélites.

> **Note**
>
> No podrá establecer un enlace ascendente a estos satélites. Solo podrá utilizar las vías de comunicación de enlace descendente de acceso público.

AWS Ground Station admite la incorporación de los siguientes satélites para transferir datos de transmisión directa por enlace descendente:

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

Una vez embarcados, se puede 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. Ejemplos de configuraciones de perfil de misiónConsulte algunos ejemplos de cómo se AWS Ground Station pueden utilizar.

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.

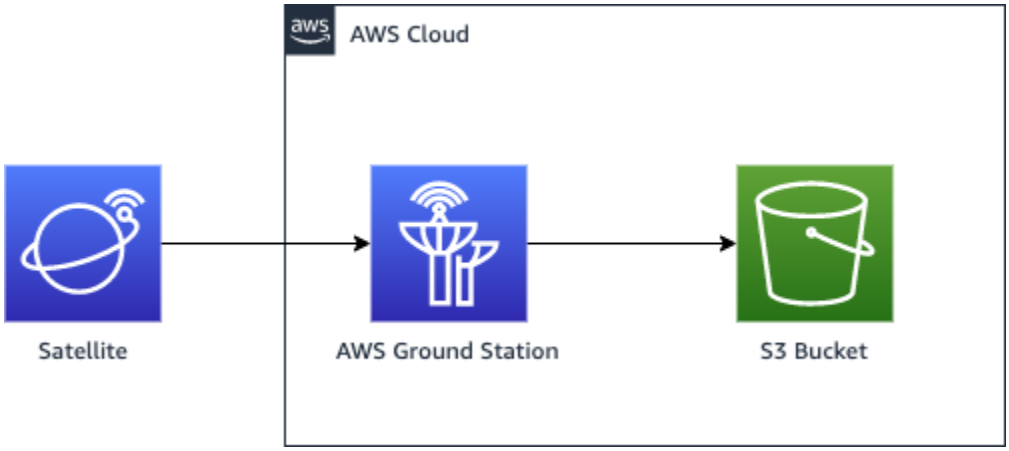
Planifique las rutas de comunicación de su flujo de datos

Puede elegir entre comunicación síncrona y asíncrona para cada ruta de comunicación de su satélite. Según el satélite y el caso de uso, es posible que necesite uno o ambos tipos. Las rutas de comunicación sincrónicas permiten realizar operaciones de enlace ascendente prácticamente en tiempo real, así como de enlace descendente de banda estrecha y ancha. Las rutas de comunicación asíncronas solo admiten operaciones de enlace descendente de banda estrecha y banda ancha.

Entrega de datos asíncrona

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 AI 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.



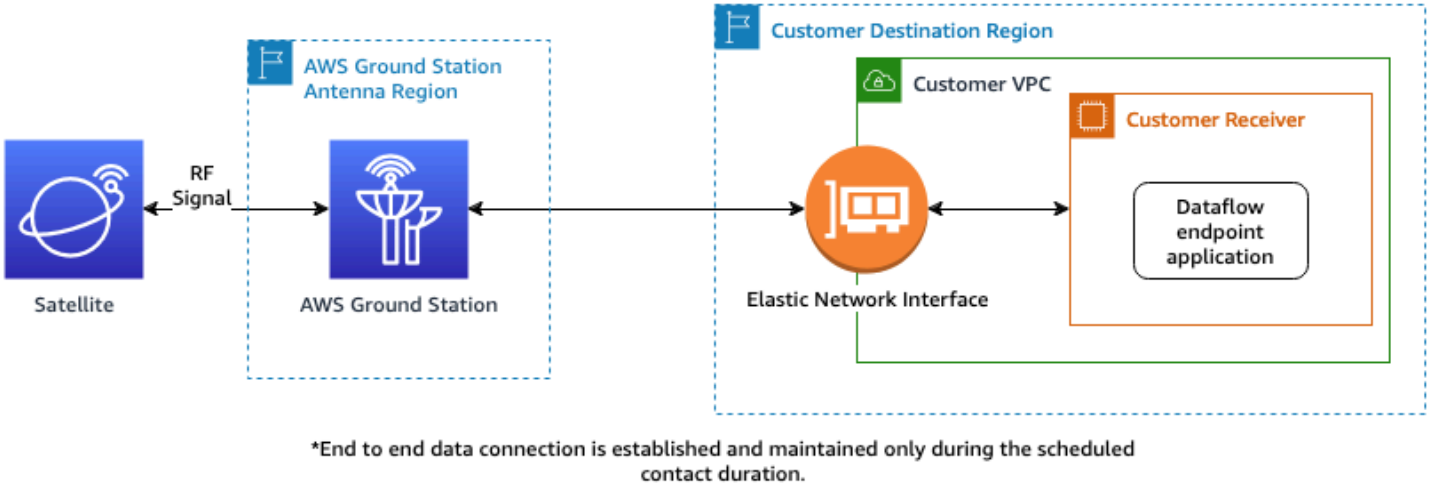
Para utilizar esta ruta, necesitará crear un bucket de Amazon S3 AWS Ground Station para entregar los datos. En el siguiente paso, también tendrás que crear una S3 Recording Config en el siguiente paso. Consulte las restricciones sobre Config de grabación de Amazon S3 la denominación de los depósitos y cómo especificar la convención de nomenclatura utilizada para sus archivos.

Entrega de datos sincrónica

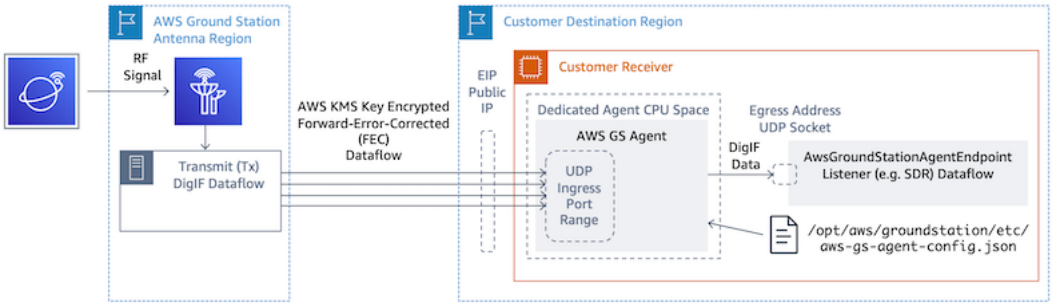
Con la entrega de datos a Amazon EC2, tus datos de contacto se transmiten desde y hacia tu EC2 instancia de Amazon. Puedes procesar tus datos en tiempo real en tu EC2 instancia de Amazon o reenviar los datos para su posterior procesamiento.

Para utilizar una ruta sincrónica, necesitará instalar y configurar sus EC2 instancias de Amazon y crear uno o más grupos de puntos de conexión de Dataflow. Para configurar tu EC2 instancia de Amazon, consulta elConfigurar y configurar Amazon EC2. Para crear su grupo de puntos de conexión de Dataflow, consulte el. Utilice grupos de AWS Ground Station puntos finales de Dataflow

A continuación, se muestra la ruta de comunicación si utiliza la configuración de punto final del flujo de datos.



A continuación, se muestra la ruta de comunicación si utiliza la configuración del AWS Ground Station agente.



Crear configuraciones

Con este paso, ha identificado el satélite, las rutas de comunicación y los recursos de IAM EC2, Amazon y Amazon S3 según sea necesario. En este paso, creará AWS Ground Station configuraciones que almacenarán sus parámetros respectivos.

Configuraciones de entrega de datos

Las primeras configuraciones que se deben crear se refieren a dónde y cómo desea que se entreguen los datos. Con la información del paso anterior, construirá muchos de los siguientes tipos de configuración.

- Config de grabación de Amazon S3- Entregue datos a su bucket de Amazon S3.
- Configuración de punto de enlace de flujo de datos- Entregue datos a su EC2 instancia de Amazon.

Configuraciones de satélite

Las configuraciones de satélite indican cómo se AWS Ground Station puede comunicar con su satélite. Hará referencia a la información que recopiló. Satélite a bordo

- Configuración de seguimiento- Establece las preferencias sobre cómo se rastrea físicamente tu vehículo durante un contacto. Esto es obligatorio para la construcción del perfil de la misión.
- Configuración de enlace de bajada de antena- Entregue datos de radiofrecuencia digitalizados.
- Configuración de descodificación y desmodulación de enlace de bajada de antena - Entregue datos de radiofrecuencia demodulados y decodificados.
- Configuración de enlace de subida de antena- Enlaza los datos a tu satélite.
- Configuración de repetición de enlace de subida de antena- Entregue un eco de los datos de su señal de enlace ascendente.

Crear perfil de misión

Con las configuraciones creadas en el paso anterior, ha identificado cómo rastrear su satélite y las posibles formas de comunicarse con su satélite. En este paso, construirá uno o más perfiles de misión. Un perfil de misión representa la agregación de las posibles configuraciones en un comportamiento esperado que luego se puede programar y ejecutar.

Para ver los parámetros más recientes, consulte el tipo de AWS::GroundStation::MissionProfile CloudFormation recurso

1. Pon un nombre al perfil de tu misión. Esto le permite comprender rápidamente su uso en su sistema. Por ejemplo, puede tener un operador satellite-wideband-narrowband-nominal-Operations y uno satellite-narrowband-emergency-operationssi tiene un operador de banda estrecha independiente para operaciones de emergencia.
2. Establece tu configuración de rastreo.
3. Establece tus duraciones de contacto mínimas viables. Esto le permite filtrar los posibles contactos para satisfacer las necesidades de su misión.
4. Configure sus streamsKmsKeyanuncios streamsKmsRoleque se utilizarán para cifrar sus datos durante el tránsito. Se usa para todos los flujos de datos de los AWS Ground Station agentes.
5. Configure sus flujos de datos. Cree sus flujos de datos para que coincidan con las señales de su operador utilizando las configuraciones que creó en el paso anterior.

6. [Opcional] Establece los segundos de duración del contacto antes y después del pase. Se utiliza para emitir eventos por contacto antes y después del contacto, respectivamente. Para obtener más información, consulta Automatice AWS Ground Station con eventos.
7. [Opcional] Puedes asociar etiquetas al perfil de tu misión. Se pueden usar para ayudar a diferenciar programáticamente los perfiles de sus misiones.

Puede hacer referencia a ellos Ejemplos de configuraciones de perfil de misión para ver solo algunas de las posibles configuraciones.

Comprenda los próximos pasos

Ahora que tiene un satélite incorporado y un perfil de misión válido, está listo para programar contactos y comunicarse con su satélite. AWS Ground Station

Puede programar un contacto de una de las siguientes maneras:

- La AWS Ground Station consola.
- El comando reserve-contact de la AWS CLI.
- El SDK. AWS ReserveContact API.

Para obtener información sobre cómo AWS Ground Station rastrea la trayectoria de su satélite y cómo se utiliza esa información, consulteComprenda cómo se AWS Ground Station utilizan los datos de efemérides satelitales.

AWS Ground Station mantiene una serie de AWS CloudFormation plantillas preconfiguradas para facilitar la puesta en marcha del servicio. Ejemplos de configuraciones de perfil de misiónConsulte algunos ejemplos de cómo se AWS Ground Station pueden utilizar.

El procesamiento de los datos digitales de frecuencia intermedia o de los datos desmodulados y decodificados que se le proporcionen AWS Ground Station dependerá de su caso de uso específico. Las siguientes publicaciones del blog pueden ayudarte a entender algunas de las opciones disponibles:

- Observación automatizada de la Tierra mediante la entrega de datos de AWS Ground Station Amazon S3 (y su GitHub repositorio asociado awslabs/ aws-groundstation-eos-pipeline)
- Virtualización del segmento terrestre del satélite con AWS
- Observación de la Tierra mediante AWS Ground Station: una guía práctica

- Creación de arquitecturas de enlace descendente de datos satelitales de alto rendimiento con AWS Ground Station WideBand DigiF y Amphinicy Blink SDR (y su repositorio asociado aws-samples/) GitHub aws-groundstation-wbdigif-snpp

AWS Ground Station Ubicaciones

AWS Ground Station proporciona una red global de estaciones terrestres muy cerca de nuestra red global de regiones de infraestructura de AWS. Puede configurar el uso de estas ubicaciones desde cualquier región de AWS compatible. Esto incluye la región de AWS en la que se entregan los datos.

Búsqueda de la AWS región para la ubicación de una estación terrestre

La red AWS Ground Station global incluye ubicaciones de estaciones terrestres que no están ubicadas físicamente en la región de AWS a la que están conectadas. La lista de estaciones terrestres a las que tiene acceso se puede recuperar mediante la ListGroundStationrespuesta del SDK de AWS. La lista completa de ubicaciones de las estaciones terrestres se presenta a continuación, y próximamente habrá más. Consulte la guía de incorporación para añadir o modificar las aprobaciones in situ de sus satélites.

Nombre de la estación terrestre	Ubicación de Ground Station	Nombre de la región de AWS	Código de región de AWS	Notas
Alaska 1	Alaska, EE. UU.	Oeste de EE. UU. (Oregón)	us-west-2	No se encuentra físicamente en una AWS región
Baréin 1	Bahréin	Medio Oriente (Baréin)	me-south-1	
Ciudad del Cabo 1	Ciudad del Cabo, Sudáfrica	África (Ciudad del Cabo)	af-south-1	
Dubbo 1	Dubbo, Australia	Asia-Pacífico (Sídney)	ap-southeast-2	No se encuentra físicamente en una región AWS
Hawái 1	Hawái, EE. UU.	Oeste de EE. UU. (Oregón)	us-west-2	No se encuentra físicamente en una AWS región
Irlanda 1	Irlanda	Europa (Irlanda)	eu-west-1	
Ohio 1	Ohio, EE. UU.	Este de EE. UU. (Ohio)	us-east-2	
Oregón 1	Oregon, EE. UU.	Oeste de EE. UU. (Oregón)	us-west-2	
Punta Arenas 1	Punta Arenas, Chile	América del Sur (São Paulo)	sa-east-1	No se encuentra físicamente en una AWS región
Seúl 1	Seoul, Corea del Sur	Asia-Pacífico (Seúl)	ap-northeast-2	

Nombre de la estación terrestre	Ubicación de Ground Station	Nombre de la región de AWS	Código de región de AWS	Notas
Singapur 1	Singapur	Asia-Pacífico (Singapur)	ap-southeast-1	
Estocolmo 1	Stockholm, Suecia	Europa (Estocolmo)	eu-north-1	

AWS Ground Station regiones de AWS compatibles

Puede enviar datos y configurar sus contactos mediante el SDK de AWS o la AWS Ground Station consola desde las regiones de AWS compatibles. Puede ver las regiones compatibles y sus puntos de enlace asociados en los puntos de AWS Ground Station enlace y las cuotas.

Disponibilidad de gemelos digitales

Utilice la función de gemelo AWS Ground Station digitalestá disponible en todas las regiones de AWS en las AWS Ground Station que esté disponible. Las estaciones terrestres gemelas digitales son copias exactas de las estaciones terrestres de producción con un prefijo modificativo del nombre de la estación terrestre de «Digital Twin». Por ejemplo, «Digital Twin Ohio 1" es una estación terrestre gemela digital que es una copia exacta de la estación terrestre de producción «Ohio 1".

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, esto incluye elementos como montañas o edificios, que podrían bloquear una señal de radiofrecuencia (RF) o impedir su transmisión.
- Interferencia de radiofrecuencia (RFI): esto afecta tanto a la capacidad de recibir (fuentes de RFI externas que impactan en una señal de enlace descendente en las antenas de AWS Ground

Station) como de transmitir (la señal de RF transmitida por las antenas de AWS Ground Station afecta negativamente a los receptores externos).

- Autorizaciones legales: las autorizaciones de sitios locales para operar AWS Ground Station en cada región pueden incluir restricciones específicas, como un ángulo de elevación mínimo para la transmisión.

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 a su disposición en virtud de un acuerdo de confidencialidad (NDA).

Máscaras específicas para cada cliente

Además de las máscaras de sitio de AWS Ground Station en cada sitio, es posible que tenga máscaras adicionales debido a restricciones en 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 de 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 no reserve tiempo cuando su satélite esté por debajo de la máscara del 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 le permite utilizar todo el tiempo de contacto disponible para el enlace descendente, incluso si es posible que el enlace ascendente no esté disponible durante parte de ese tiempo debido a la máscara de sitio del 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. Usted es responsable de tener en cuenta la máscara de enlace ascendente proporcionada 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 le facturará todo el tiempo de contacto, incluso si algunas partes del tiempo reservado no están disponibles para el enlace ascendente.

AWS Ground Station Capacidades del sitio

Para simplificar su experiencia, AWS Ground Station determina un conjunto común de capacidades para un tipo de antena y, a continuación, despliega varias antenas en la ubicación de una estación terrestre. Parte de los pasos de incorporación garantizan que su satélite sea compatible con los tipos de antenas de una ubicación específica. Al reservar un contacto, se determina indirectamente el tipo de antena que se utilizará. Esto garantiza que su experiencia en una ubicación determinada de la estación terrestre siga siendo la misma a lo largo del tiempo, independientemente de las antenas que utilice. El rendimiento específico de su contacto variará debido a una amplia variedad de problemas ambientales, como el clima en el sitio.

Actualmente, todos los sitios admiten las siguientes capacidades:

> **Note**
>
> Cada fila de la siguiente tabla indica una ruta de comunicación independiente, a menos que se indique lo contrario. Existen filas duplicadas para reflejar nuestras capacidades multicanal, que permiten utilizar múltiples rutas de comunicación de forma simultánea.

Tipo de capacidad	Rango de frecuencia	Rango de ancho de banda	Polarization	Common Name	Notas
antena: enlace descendente	7750 - 8500 MHz	50 - 400 MHz	RHCP	Enlace descendente de banda ancha de banda X	Esta capacidad requiere el uso del agente.AWS Ground Station
antena y enlace descendente	7750 - 8500 MHz	50 - 400 MHz	RHCP		
antena: enlace descendente	7750 - 8500 MHz	50 - 400 MHz	RHCP		Esta capacidad no es compatible con Alaska 1 ni Punta Arenas 1. El ancho de banda total no debe superar los 400 MHz por polarización en cada ubicación. Todos los rangos de frecuencia utilizados no deben superponerse.
antena: enlace descendente	7750 - 8500 MHz	50 - 400 MHz	RHCP		
antena: enlace descendente	7750 - 8500 MHz	50 - 400 MHz	RHCP		
antena: enlace descendente	7750 - 8500 MHz	50 - 400 MHz	LHCP		
antena: enlace descendente	7750 - 8500 MHz	50 - 400 MHz	LHCP		
antena: enlace descendente	7750 - 8500 MHz	50 - 400 MHz	LHCP		
antena: enlace descendente	7750 - 8500 MHz	50 - 400 MHz	LHCP		

Tipo de capacidad	Rango de frecuencia	Rango de ancho de banda	Polarization	Common Name	Notas
antena: enlace descendente	7750 - 8500 MHz	50 - 400 MHz	LHCP		
antena: enlace descendente	2200 - 290 MHz	Hasta 40 MHz	RHCP	Enlace descendente en banda S	Solo se puede usar una polarización a la vez
enlace descendente de antena	2200 - 290 MHz	Hasta 40 MHz	LHCP		
antena: enlace descendente	7750 - 8500 MHz	Hasta 40 MHz	RHCP	Enlace descendente de banda estrecha de banda X	Solo se puede usar una polarización a la vez
enlace descendente de antena	7750 - 8500 MHz	Hasta 40 MHz	LHCP		
antena-enlace ascendente	2025 - 2110 MHz	Hasta 40 MHz	RHCP	enlace ascendente de banda S	Solo se puede usar una polarización a la vez
antena-enlace ascendente	2025 - 2110 MHz	Hasta 40 MHz	LHCP		EIRP de 20 a 50 dBW
antenna-uplink-echo	2025 - 2110 MHz	2 MHz	RHCP	Eco de enlace ascendente	Coincide con las restricciones de enlace ascendente entre antenas
antenna-uplink-echo	2025 - 2110 MHz	2 MHz	LHCP		

Tipo de capacidad	Rango de frecuencia	Rango de ancho de banda	Polarization	Common Name	Notas
antenna-downlink-demod-decode	7750 - 8500 MHz	Hasta 500 MHz	RHCP	Enlace descendente desmodulado y decodificado en banda X	
antenna-downlink-demod-decode	7750 - 8500 MHz	Hasta 500 MHz	LHCP		
seguimiento	N/A	N/A	N/A	N/A	Support para el seguimiento automático y el seguimiento de programas

* RHCP = polarización circular para diestros y LHCP = polarización circular para zurdos. Para obtener más información sobre la polarización, consulte Polarización circular.

Comprenda cómo se AWS Ground Station utilizan los datos de efemérides satelitales

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 estarán 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 AWS Ground Station efemérides si el satélite tiene un identificador de NORAD asignado.

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 () TLEs asociados al ID NORAD del 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 sin un ID del NORAD deben cargar datos de efemérides personalizados en ellos. AWS Ground Station Por ejemplo, los satélites que se acaban de lanzar o que se han omitido intencionadamente del catálogo de Space-Track no tendrían un identificador del NORAD y deberían tener cargadas las efemérides personalizadas. Para obtener más información sobre

cómo proporcionar efemérides personalizadas, consulte: Proporcionar datos de efemérides personalizadas.

Proporcionar datos de efemérides personalizados

> **Important**
>
> 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.
<Si necesitas poder cargar datos de efemérides personalizados, ponte en contacto
AWS Ground Station trata las efemérides como datos de uso individualizados. Si utiliza esta función opcional, AWS utilizará sus datos de efemérides para proporcionar asistencia en la solución de problemas.

Descripción general

La API de efemérides permite cargar efemérides personalizadas para usarlas con un satélite. AWS Ground Station Estas efemérides anulan las efemérides predeterminadas de Space-Track (consulte:). Datos de efemérides predeterminados Admitimos la recepción de datos de efemérides en los formatos Orbit Ephemeris Message (OEM) y elementos de dos líneas (TLE).

La carga de efemérides personalizadas permite mejorar la calidad del rastreo, gestionar las primeras operaciones cuando no se dispone de efemérides de Space-Track y tener en cuenta las maniobras. AWS Ground Station

> **Note**
>
> Al proporcionar efemérides personalizadas antes de asignar un número de catálogo de satélites a su satélite, puede utilizar 00000 para el campo de número de catálogo de satélites de la TLE y 000 para la parte del número de lanzamiento del campo de designación internacional de los metadatos de la TLE o OEM (por ejemplo, 24000A para un vehículo lanzado en 2024).
> Para obtener más información sobre el formato de, consulte Conjunto de elementos de dos TLEs líneas. Para obtener más información sobre el formato de OEMs, consulteFormato de efemérides OEM.

Formato de efemérides OEM

AWS Ground Station procesa las efemérides OEM proporcionadas por el cliente de acuerdo con el estándar CCSDS con algunas restricciones adicionales. Los archivos OEM deben estar en formato KVN. La siguiente tabla describe los diferentes campos de un OEM y en qué AWS Ground Station se diferencian del estándar CCSDS.

Sección	Campo	Se requiere CCSDS	AWS Ground Station obligatorio	Notas
Encabezado	CCSDS_OEM_VERS	Sí	Sí	Valor requerido: 2.0
	COMMENT	No	No	
	CLASIFICACIÓN	No	No	
	FECHA DE CREACIÓN	Sí	Sí	
	INICIADOR	Sí	Sí	
	MESSAGE_ID	No	No	
Metadatos	META_START	Sí	Sí	
	COMMENT	No	No	
	NOMBRE_OBJETO	Sí	Sí	
	OBJECT_ID	Sí	Sí	
	NOMBRE_CENTRO	Sí	Sí	Valor obligatorio: Tierra
	REF_FRAME	Sí	Sí	Valores aceptados:

Sección	Campo	Se requiere CCSDS	AWS Ground Station obligatorio	Notas
				EME2 000, 000 ITRF2
	REF_FRAME_EPOCH	No	No compatible*	No es necesario porque los REF_ FRAMEs aceptados tienen una época implícita
	SISTEMA_TIEMPO	Sí	Sí	Valor obligatorio: UTC
	HORA_INICIO	Sí	Sí	
	HORA_INICIO UTILIZABLE	No	No	
	TIEMPO_DE_PARADA UTILIZABLE	No	No	
	STOP_TIME	Sí	Sí	
	INTERPOLACIÓN	No	Sí	Necesario para AWS Ground Station poder generar ángulos de puntería precisos para los contactos.

Sección	Campo	Se requiere CCSDS	AWS Ground Station obligatorio	Notas
	GRADO DE INTERPOLACIÓN	No	Sí	Necesario para AWS Ground Station poder generar ángulos de puntería precisos para los contactos.
	META_STOP	Sí	Sí	
Datos	X	Sí	Sí	Representado en `km`
	Y	Sí	Sí	Representado en `km`
	Z	Sí	Sí	Representado en `km`
	X_DOT	Sí	Sí	Representado en `km/s`
	Y_DOT	Sí	Sí	Representado en `km/s`
	Z_DOT	Sí	Sí	Representado en `km/s`
	X_DDOT	No	No	Representado en `km/s^2`
	Y_DDOT	No	No	Representado en `km/s^2`

Sección	Campo	Se requiere CCSDS	AWS Ground Station obligatorio	Notas
	Z_DDOT	No	No	Representado en `km/s^2`
Matriz de covarianzas	COVARIANCE_START	No	No	
	EPOCH	No	No	
	COV_REF_FRAME	No	No	
	COVARIANCE_STOP	No	No	

* Si en el OEM proporcionado AWS Ground Station se incluye alguna fila que no sea compatible, el OEM no pasará la validación.

Las desviaciones importantes con respecto al estándar de la CCSDS son las AWS Ground Station siguientes:

- Se requiere que CCSDS_OEM_VERS sea. `2.0`
- Se requiere que REF_FRAME sea o. `EME2000` `ITRF2000`
- REF_FRAME_EPOCH no es compatible con. AWS Ground Station
- Se requiere que CENTER_NAME lo sea. `Earth`
- Se requiere que TIME_SYSTEM lo sea. `UTC`
- Tanto INTERPOLATION como INTERPOLATION_DEGREE son necesarios para el CPE. AWS Ground Station

Ejemplo de efemérides OEM en formato KVN

A continuación se presenta un ejemplo truncado de una efeméride OEM en formato KVN para el satélite de radiodifusión pública JPSS-1.

```
CCSDS_OEM_VERS = 2.0

COMMENT Orbit data are consistent with planetary ephemeris DE-430

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

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

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

Crear 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`. Deberías sondear el estado de las efemérides o usar CloudWatch eventos DescribeEphemerispara realizar un seguimiento de los cambios de estado de las efemérides.

Para solucionar problemas relacionados con una efeméride no válida, consulta: Solucionar problemas de efemérides no válidas

Ejemplo: cree un conjunto de efemérides de elementos de dos líneas (TLE) mediante la API

La AWS SDKs CLI y la CLI se pueden usar para cargar un conjunto de efemérides de dos elementos de línea (TLE) AWS Ground Station mediante la CreateEphemerisllamada. Se utilizará esta efeméride en lugar de los datos de efemérides predeterminados para un satélite (consulte Datos de efemérides predeterminados). En este ejemplo se muestra cómo hacerlo con el AWS SDK para Python (Boto3).

Un conjunto TLE es un objeto con formato JSON que enlaza uno o más TLEs para construir una trayectoria continua. El del TLEs conjunto TLE debe formar un conjunto continuo que podamos usar para construir una trayectoria (es decir, no debe haber intervalos de tiempo intermedios TLEs 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 TLEs de un conjunto TLE deben coincidir exactamente para que sea una trayectoria continua y 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 EphemerisID que se puede usar para hacer referencia a las efemérides en el futuro. Por ejemplo, podemos usar el EphemerisID proporcionado en la llamada anterior para sondear el estado de las efemérides:

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

Se recomienda sondear la DescribeEphemerisruta o usar CloudWatch eventos para rastrear el estado de las efemérides subidas, ya que deben pasar por un flujo de trabajo de validación asíncrona antes de configurarse y poder utilizarse para programar y ejecutar contactos. `ENABLED`

Tenga en cuenta que el identificador de NORAD que aparece TLEs en todo el conjunto TLE, en los ejemplos anteriores, debe coincidir con el identificador de NORAD asignado a su satélite 25994 en la base de datos Space-Track.

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

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"
      }
    }
  }
}
```

Ejemplo: usar efemérides proporcionadas por el cliente con AWS Ground Station

Para obtener instrucciones más detalladas sobre el uso de efemérides proporcionadas por el cliente AWS Ground Station, consulte Uso de efemérides proporcionadas por el cliente con (y su repositorio asociado aws-samples/) AWS Ground Station GitHub aws-groundstation-cpe

Comprende 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. Un valor de prioridad más alto indica una prioridad más alta. 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 previamente programados

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 obtener más información sobre los contactos cancelados, consulte: Ground Station FAQs.

Obtenga las efemérides actuales de un satélite

Las efemérides actuales que utiliza un satélite específico se pueden recuperar llamando a las acciones o. AWS Ground Station GetSatelliteListSatellites 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 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 subida a través de la acción. AWS Ground Station 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"
      }
  }
```

Volver a los datos de efemérides predeterminados

Al cargar datos de efemérides personalizados, estos anularán los usos predeterminados de las efemérides AWS Ground Station para ese satélite en particular. 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 de Space-Track predeterminadas, tendrás que 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 para Datos de efemérides predeterminados obtener más información sobre las efemérides predeterminadas.

Trabaje con flujos de datos

AWS Ground Station utiliza una relación de nodo y borde para construir flujos de datos que permitan el procesamiento de los datos en flujo. Cada nodo está representado por una configuración que describe su procesamiento esperado. Para ilustrar este concepto, considere un flujo de datos de `antenna-downlink` a. `s3-recording` El `antenna-downlink` nodo representa la transformación analógica a digital del espectro de radiofrecuencias según los parámetros definidos en la configuración. `s3-recording`Representa un nodo de cómputo que recibirá los datos entrantes y los almacenará en su bucket de S3. El flujo de datos resultante es una entrega asíncrona de datos de RF digitalizados a un depósito de S3 en función de sus especificaciones.

Dentro del perfil de su misión, puede crear muchos flujos de datos para satisfacer sus necesidades. En las siguientes secciones se describe cómo configurar los demás recursos de AWS para usarlos con ellos AWS Ground Station y se ofrecen recomendaciones para crear flujos de datos. Para obtener información detallada sobre el comportamiento de cada nodo, incluso si se considera un nodo de origen o de destino, consulte. Usa AWS Ground Station configuraciones

Temas

- AWS Ground Station interfaces del plano de datos
- Utilice la entrega de datos entre regiones
- Instalación y configuración de Amazon S3
- Instalación y configuración de Amazon VPC
- Configurar y configurar Amazon EC2

AWS Ground Station interfaces del plano de datos

La estructura de datos resultante del flujo de datos elegido depende de la fuente del flujo de datos. Los detalles de estos formatos se le proporcionan durante la incorporación de sus satélites. A continuación se resumen los formatos utilizados para cada tipo de flujo de datos.

- antena: enlace descendente
  - (Ancho de banda inferior a 54MHz) los datos se envían como paquetes de datos de señal/formato IP VITA-49.
  - (Ancho de banda greater-than-or-equal: hasta 54MHz) los datos se entregan como paquetes de clase 2. AWS Ground Station

- antenna-downlink-demod-decode
  - Los datos se entregan como paquetes Demodulated/Decoded Data/IP de formato.
- antena-enlace ascendente
  - Los datos deben entregarse como paquetes de datos de señal VITA-49 en formato IP.
- antenna-uplink-echo
  - Los datos se envían como paquetes de datos de señal/formato IP VITA-49.

Utilice la 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 cualquier región de AWS AWS Ground Station compatible. Esto significa que puede mantener su infraestructura en una sola región de AWS y programar contactos en cualquier región en la AWS Ground Station AWS Ground Station Ubicaciones que esté incorporado.

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. AWS Ground Station gestionará todos los aspectos de la entrega por usted.

La entrega de datos entre regiones a Amazon EC2 con el AWS Ground Station agente está disponible en todas antenna-to-destination las regiones. No se requiere ninguna configuración ni aprobación únicas para esta configuración.

La entrega de datos entre regiones a Amazon EC2 mediante un punto final de flujo de datos está disponible de forma predeterminada* en las regiones que se describen a continuación. antenna-to-destination

- 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 a una EC2 instancia de Amazon, el punto de enlace del flujo de datos debe crearse en su región de AWS actual y dataflow-endpoint-configdebe especificar la misma región.

La información anterior, que detalla las regiones y los métodos de entrega compatibles para la entrega de datos entre regiones, se resume en la siguiente tabla.

Método de recepción	Región de antena	Región receptora
Entrega de datos de Amazon S3	¡Todo incorporado AWS Ground Station AWS Ground Station Ubicaciones	Todas las regiones AWS Ground Station
AWS Ground Station Agente en Amazon EC2	¡Todos a bordo AWS Ground Station AWS Ground Station Ubicaciones	Todas las regiones AWS Ground Station
Punto final de Dataflow en Amazon* EC2	Región Este de EE. UU. (Ohio) (us-east-2)	Región Oeste de EE. UU. (Oregón) (us-west-2)
	Región Oeste de EE. UU. (Oregón) (us-west-2)	Región Este de EE. UU. (Ohio) (us-east-2)

*Las antenna-to-destination regiones adicionales que no figuran en la lista requieren una configuración especial de Amazon EC2 y software. Ponte en contacto con nosotros en `<aws-groundstation@amazon.com>` para obtener instrucciones de incorporación.

Instalación y configuración de Amazon S3

Puede utilizar un bucket de Amazon S3 para recibir sus señales de enlace descendente mediante AWS Ground Station. Para crear el s3-recording-config de destino, debe poder especificar un bucket de Amazon S3 y un rol de IAM que autorice AWS Ground Station la escritura de archivos en el bucket.

Consulte Config de grabación de Amazon S3 las restricciones sobre el bucket de Amazon S3, el rol de IAM o la creación de AWS Ground Station configuraciones.

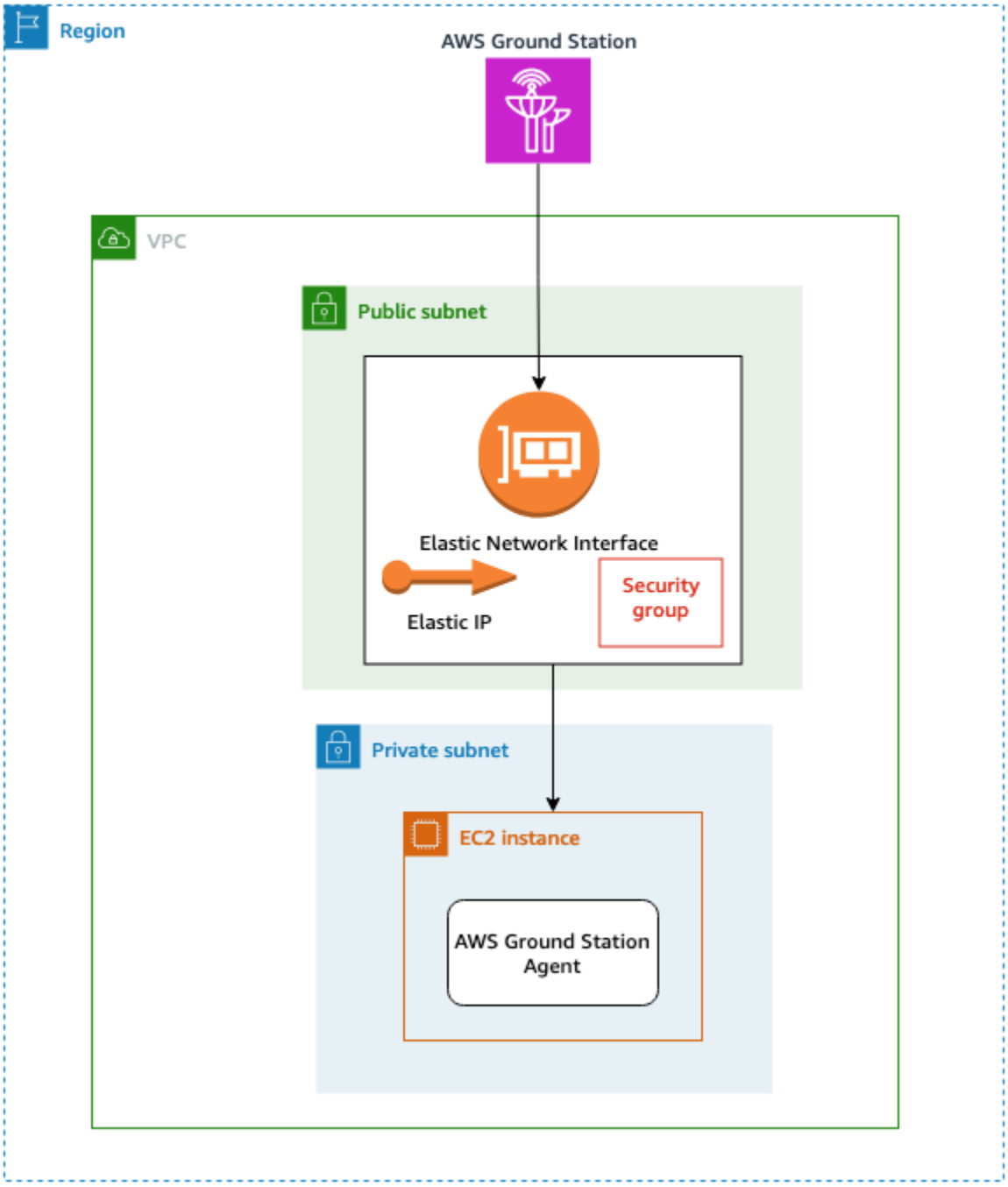
Instalación y configuración de Amazon VPC

Una guía completa para configurar una VPC va más allá del alcance de esta guía. Para obtener información detallada, consulte la Guía del usuario de Amazon VPC.

En esta sección, se describe cómo pueden existir su punto final de Amazon EC2 y de flujo de datos dentro de una VPC. AWS Ground Station no admite varios puntos de entrega para un flujo de datos determinado; se espera que cada flujo de datos termine en un solo receptor. EC2 Como esperamos

un único EC2 receptor, la configuración no es redundante en zonas de disponibilidad múltiples (Multi-AZ). Para ver ejemplos completos en los que se utilizará su VPC, consulte. Ejemplos de configuraciones de perfil de misión

Configuración de VPC con agente AWS Ground Station



Los datos de su satélite se proporcionan a una instancia de AWS Ground Station agente próxima a la antena. El AWS Ground Station agente separará sus datos y los cifrará con la AWS KMS clave

que usted proporcione. Cada banda se envía a su Amazon EC2 Elastic IP (EIP) desde la antena de origen a través de la red troncal de AWS. Los datos llegan a la EC2 instancia a través de la Amazon EC2 Elastic Network Interface (ENI) adjunta. Una vez en la EC2 instancia, el AWS Ground Station agente instalado descifrará los datos y realizará la corrección de errores de reenvío (FEC) para recuperar los datos perdidos. A continuación, los reenviará a la IP y al puerto que especificó en la configuración.

En la siguiente lista, se indican consideraciones de configuración específicas a la hora de configurar la VPC para la entrega de AWS Ground Station agentes.

Grupo de seguridad: se recomienda configurar un grupo de seguridad dedicado únicamente al AWS Ground Station tráfico. Este grupo de seguridad debe permitir el tráfico de entrada UDP en el mismo rango de puertos que especifique en su grupo de puntos finales de Dataflow. AWS Ground Station mantiene una lista de prefijos administrada por AWS para restringir sus permisos únicamente AWS Ground Station a las direcciones IP. Consulte las listas de prefijos gestionados por AWS para obtener más información sobre cómo sustituirlas PrefixListIden sus regiones de implementación.

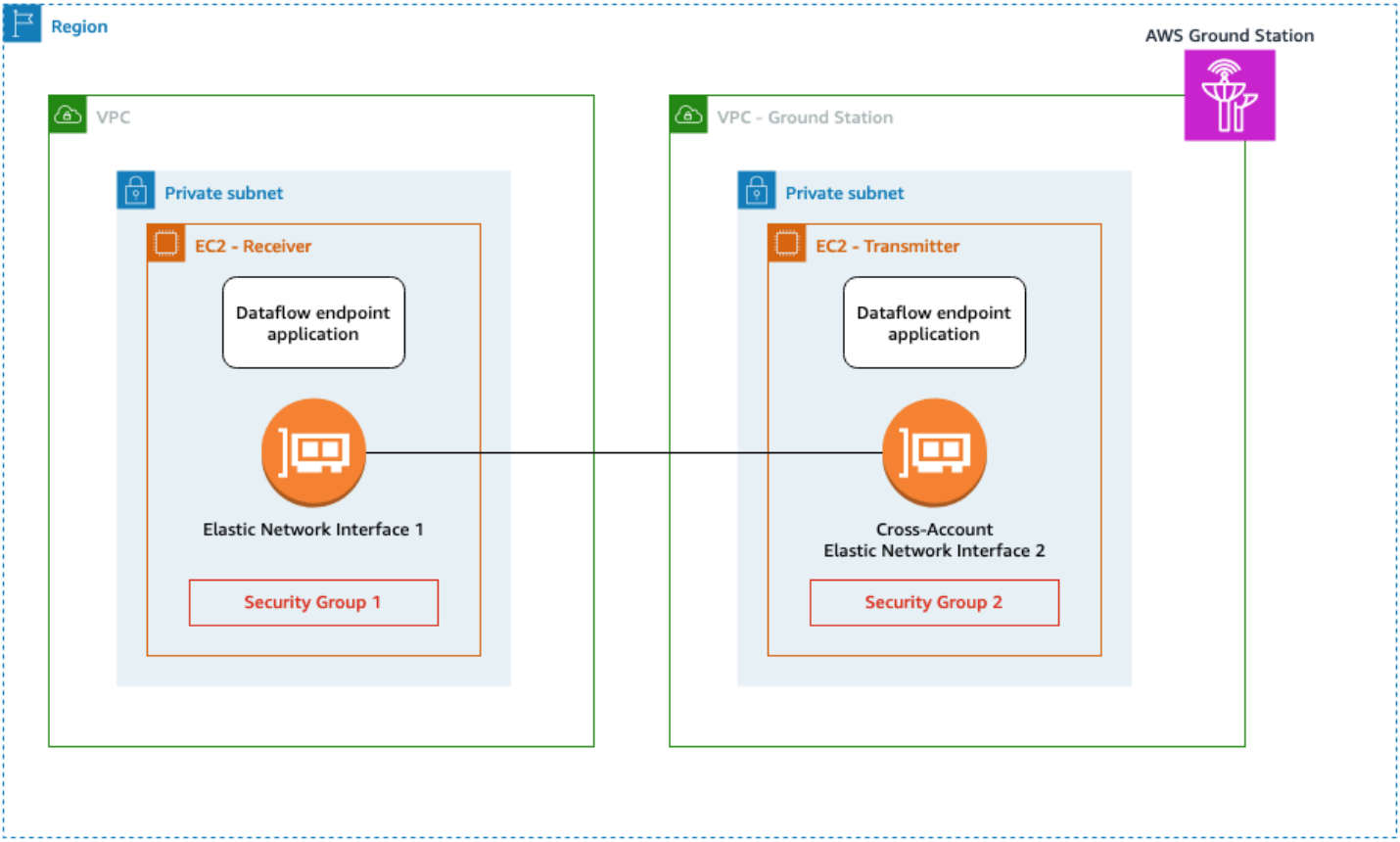
Interfaz de red elástica (ENI): deberá asociar el grupo de seguridad anterior a este ENI y colocarlo en su subred pública.

La siguiente CloudFormation plantilla muestra cómo crear la infraestructura descrita en esta sección.

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

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

InstanceNetworkInterface:
```

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

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

Configuración de VPC con un punto final de flujo de datos



Los datos de su satélite se proporcionan a una instancia de aplicación de punto final de flujo de datos próxima a la antena. Luego, los datos se envían a través de Amazon EC2 Elastic Network

Interface (ENI) multicuenta desde una VPC propiedad de. AWS Ground Station Luego, los datos llegan a su EC2 instancia a través del ENI adjunto a su EC2 instancia de Amazon. A continuación, la aplicación de punto final del flujo de datos instalada los reenviará a la IP y al puerto que especificó en la configuración. Lo contrario de este flujo ocurre en las conexiones de enlace ascendente.

En la siguiente lista, se indican consideraciones de configuración únicas al configurar su VPC para la entrega de puntos finales de flujos de datos.

Función de IAM: la función de IAM forma parte del punto final del flujo de datos y no se muestra en el diagrama. La función de IAM que se utiliza para crear y adjuntar el ENI multicuenta a la instancia de AWS Ground Station Amazon EC2.

Grupo de seguridad 1: este grupo de seguridad está asociado al ENI, que se asociará a la EC2 instancia de Amazon de su cuenta. Debe permitir el tráfico UDP del grupo de seguridad 2 en los puertos especificados en su dataflow-endpoint-group.

Interfaz de red elástica (ENI) 1: deberá asociar el grupo de seguridad 1 a este ENI y colocarlo en una subred.

Subred: tendrás que asegurarte de que haya al menos una dirección IP disponible por flujo de datos para la EC2 instancia de Amazon de tu cuenta. Para obtener más información sobre el tamaño de las subredes, consulte Bloques CIDR de subred

Grupo de seguridad 2: se hace referencia a este grupo de seguridad en el punto final de Dataflow. Este grupo de seguridad se adjuntará al ENI que AWS Ground Station se utilizará para colocar los datos en su cuenta.

Región: para obtener más información sobre las regiones compatibles para las conexiones entre regiones, consulteUtilice la entrega de datos entre regiones.

La siguiente CloudFormation plantilla muestra cómo crear la infraestructura descrita en esta sección.

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

AWSGroundStationSecurityGroupEgress:
```

```
  Type: AWS::EC2::SecurityGroupEgress
  Properties:
    GroupId: !Ref DataflowEndpointSecurityGroup
    IpProtocol: udp
    FromPort: 55555
    ToPort: 55555
    CidrIp: 10.0.0.0/8
    Description: "Allow AWS Ground Station to send UDP traffic on port 55555 to the
 10/8 range."

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

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

Configurar y configurar Amazon EC2

Es necesario configurar correctamente su EC2 instancia de Amazon para que la entrega sincrónica del VITA-49 se entregue Signal/IP data or VITA-49 Extension data/IP a través del AWS Ground

Station agente o de un punto final de flujo de datos. Según sus necesidades específicas, puede instalar el procesador front-end (FE) o la radio definida por software (SDR) directamente en la misma instancia, o puede que necesite utilizar instancias adicionales. EC2 La selección e instalación de su FE o SDR van más allá del ámbito de esta guía del usuario. Para obtener más información sobre los formatos de datos específicos, consulteAWS Ground Station interfaces del plano de datos.

Para obtener información sobre nuestras condiciones de servicio, consulte las condiciones AWS de servicio.

Software común suministrado

AWS Ground Station proporciona un software común para facilitar la configuración de su EC2 instancia de Amazon.

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 de alta velocidad y baja fluctuación a cualquier IP pública AWS (IP elástica) de la AWS red.
- Entrega de datos fiable mediante la corrección de errores de reenvío (FEC).
- Entrega segura de datos mediante una AWS KMS clave de cifrado gestionada por el cliente.

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

Aplicación de punto final Dataflow

Una aplicación de red que se utiliza AWS Ground Station para enviar y recibir datos entre las ubicaciones de las AWS Ground Station antenas y sus EC2 instancias de Amazon. Se puede utilizar para el enlace ascendente y descendente de datos.

Radio definida por software (SDR)

Una radio definida por software (SDR) que se puede utilizar para modular/demodular la señal utilizada para comunicarse con el satélite.

AWS Ground Station Imágenes de máquinas de Amazon (AMIs)

Para reducir los tiempos de construcción y configuración de estas instalaciones, AWS Ground Station también ofrece opciones AMIs preconfiguradas. La aplicación de red para puntos terminales AMIs con flujo de datos y una radio definida por software (SDR) estarán disponibles en su cuenta una vez completada la incorporación. Se pueden encontrar en la EC2 consola de Amazon buscando estación terrestre en Amazon Machine Images (AMIs) privado. Los AMIs with AWS Ground Station Agent son públicos y se pueden encontrar en la EC2 consola de Amazon buscando Groundstation en Amazon Machine Images (AMIs).

Trabaja con contactos

Puede introducir datos de satélites, identificar las ubicaciones de las antenas, comunicarse y programar la hora de antena de los satélites seleccionados mediante la AWS Ground Station consola o el AWS SDK en el idioma que prefiera. AWS CLI Puedes revisar, cancelar y reprogramar las reservas de contactos hasta 15 minutos antes del inicio del contacto*. Además, puedes ver los detalles de tu plan de precios de minutos reservados si utilizas 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 sobre el uso de la entrega de datos entre regiones, consulte. Utilice la entrega de datos entre regiones

Para programar contactos, los recursos deben estar configurados. Si no ha configurado los recursos, consulteIntroducción. Cuando ReserveContactse le llama, AWS Ground Station toma una instantánea del perfil de la misión y configura los recursos para usarlos durante el pase de contacto. Los cambios que se realicen en estos recursos mediante UpdateMissionProfiley no se UpdateConfig APIs reflejarán en los contactos reservados antes de las actualizaciones. Si necesita que los cambios de recursos se apliquen a un contacto ya programado, primero debe cancelar el contacto utilizando y CancelContact, a continuación, reprogramarlo utilizando. ReserveContact

* Los contactos cancelados pueden conllevar costes si se cancelan demasiado cerca de la hora del contacto. Para obtener más información sobre los contactos cancelados, consulte: Ground Station FAQs.

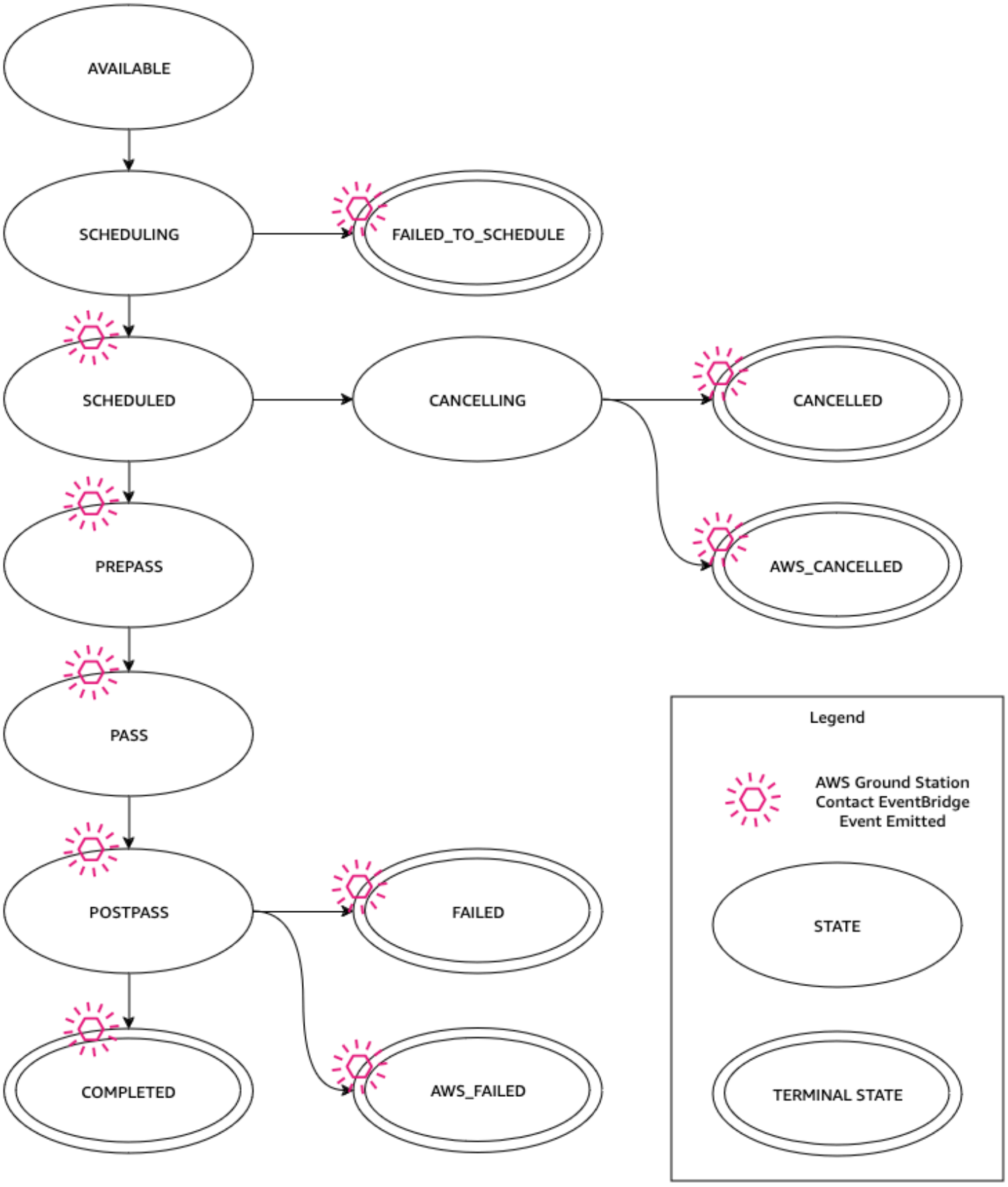
Temas

- Comprenda el ciclo de vida de

Comprenda el ciclo de vida de

Comprender el ciclo de vida de los contactos puede ayudar a determinar cómo configurar la automatización y a la hora de solucionar problemas. El siguiente diagrama muestra el ciclo de vida de los AWS Ground Station contactos, así como los eventos de Event Bridge emitidos durante el ciclo de vida. Es importante tener en cuenta que los estados COMPLETADO, FALLIDO, FALLIDO AL PROGRAMAR AWS_CANCELLED, CANCELADO y son estados terminales. AWS_FAILED Los

contactos no pasarán de un estado terminal. Consulte la AWS Ground Station estados de contacto para obtener más información sobre lo que indica cada estado.


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

AWS Ground Station estados de contacto

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

Los 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.
- COMPLETADO: el contacto se completó sin errores.
- ERROR: el contacto ha fallado debido a un problema con la configuración de los recursos.
- 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 AWS Ground Station servicio canceló el contacto. El mantenimiento de la antena o del sitio y la deriva de las efemérides son ejemplos de casos en los que esto podría ocurrir.
- CANCELADO: cancelaste el contacto por tu parte.

Utilice la función de gemelo AWS Ground Station digital

La función de gemelo digital le AWS Ground Station proporciona un entorno en el que puede probar e integrar su software de gestión de misiones satelitales y de mando y control. La función de gemelo digital le permite probar la programación, verificar las configuraciones y gestionar correctamente los errores sin utilizar la capacidad de la antena de producción. Probar la AWS Ground Station integración con la función de gemelo digital le permitirá confiar cada vez más en la capacidad del sistema para gestionar las operaciones de sus satélites sin problemas. También le permite realizar pruebas AWS Ground Station APIs sin utilizar la capacidad de producción ni requerir licencias de espectro.

Para empezarSatélite a bordo, síganos y solicite que se le incorpore a la función de gemelo digital. Una vez que el satélite esté incorporado a la función de gemelo digital, podrá programar los contactos en las estaciones terrestres gemelas digitales. La lista de estaciones terrestres a las que tiene acceso se puede recuperar mediante la ListGroundStationsrespuesta del SDK de AWS. Las estaciones terrestres gemelas digitales son copias exactas de las estaciones terrestres que figuran en la lista AWS Ground Station Ubicaciones con un prefijo modificativo del nombre de la estación terrestre de «Digital Twin». Esto incluye sus capacidades de antena y sus metadatos, que incluyen, entre otros, la máscara del sitio y las coordenadas GPS reales. En este momento, la función de gemelo digital no admite la entrega de datos, tal y como se describe enTrabaje con flujos de datos.

Una vez incorporada, la función de gemelo digital emite los mismos EventBridge eventos de Amazon y respuestas de API que el servicio de producción, tal y como se describe en. Automatice AWS Ground Station con eventos Estos eventos le permitirán ajustar las configuraciones y los grupos de puntos finales del flujo de datos.

Comprenda la supervisión con 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 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 la computación automatizada basada en eventos, ya que puede escribir reglas que vigilen ciertos eventos y activen acciones automatizadas en otros AWS servicios cuando estos eventos ocurren. 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. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. 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 CloudWatch las métricas de Amazon.
- 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 Amazon Q Developer en aplicaciones de chat o notificaciones push de AWS Console Mobile Application. También puede ver las notificaciones en el centro de notificaciones de la AWS consola. Notificaciones de usuario admiten la agregación, lo que puede reducir la cantidad de notificaciones que recibe durante eventos específicos.

Utilice los temas siguientes para monitorear AWS Ground Station.

Temas

- Automatice AWS Ground Station con eventos
- Registra las llamadas a la AWS Ground Station API con AWS CloudTrail
- Consulta las métricas con Amazon CloudWatch

Automatice 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. Algunas de las acciones que se pueden activar automáticamente son las siguientes:

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

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

- Invocar una función Lambda para automatizar el inicio y la parada de las instancias de EC2 Amazon 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, consulta la Guía del usuario de Amazon EventBridge Events.

AWS Ground Station Tipos de eventos

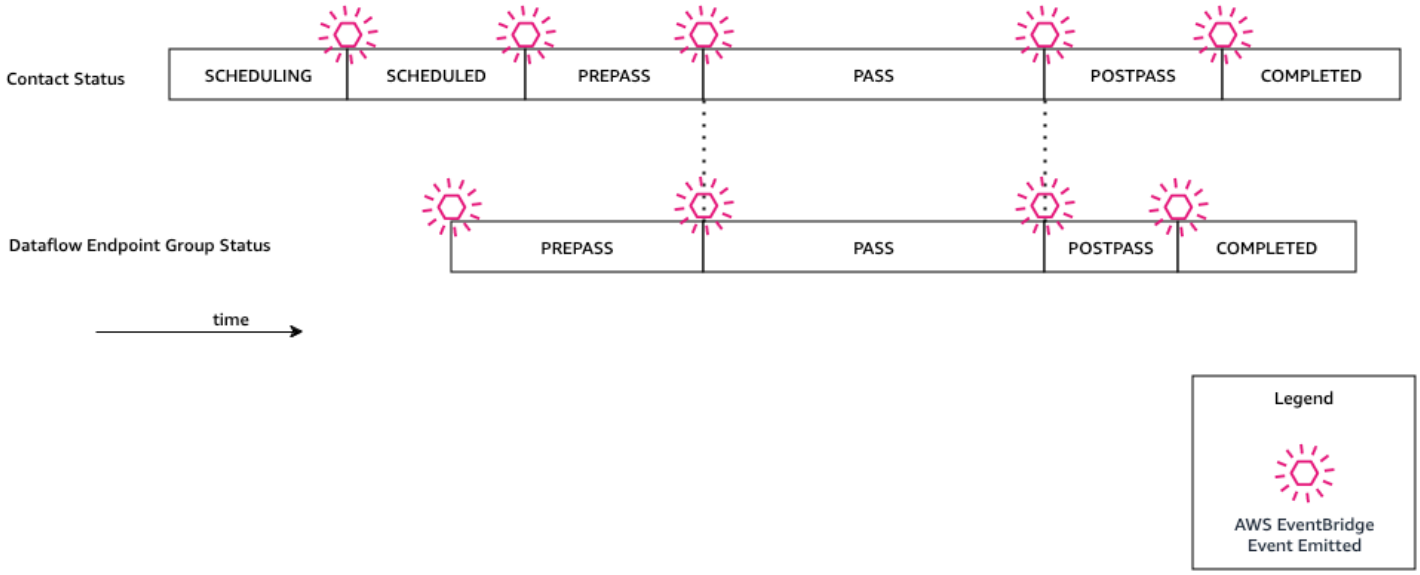
> **Note**
>
> Todos los eventos generados por AWS Ground Station tienen "aws.groundstation" como valor de "source".

AWS Ground Station emite eventos relacionados con los cambios de estado para respaldar tu capacidad de personalizar tu automatización. Actualmente, AWS Ground Station admite eventos de cambio de estado de contacto, eventos de cambio de grupo de puntos finales de flujo de datos y eventos de cambio de estado de efemérides. En las siguientes secciones se proporciona información detallada sobre cada tipo.

Cronología del evento de contacto

AWS Ground Station emite eventos cuando tu contacto cambia de estado. Para obtener más información sobre cuáles son esos cambios de estado y qué significan los estados en sí, consulteComprenda el ciclo de vida de. Todos los grupos de puntos finales de un flujo de datos que se utilicen en su contacto tienen un conjunto independiente de eventos que también se emiten. Durante ese mismo período, también emitimos eventos para su grupo de puntos finales de flujo de datos. Puede configurar la hora exacta de los eventos previos y posteriores a la transferencia al configurar el perfil de la misión y el grupo de puntos finales del flujo de datos.

El siguiente diagrama muestra los estados y eventos emitidos para un contacto nominal y su grupo de puntos finales de flujo de datos asociado.



Cambio de estado del contacto de Ground Station

Si desea realizar una acción específica cuando un próximo contacto cambie de estado, puede configurar una regla para automatizar esta acción. Esto es útil para cuando desee recibir notificaciones acerca de los cambios de estado del contacto. Si quieres cambiar el momento en que recibes 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 muestra un ejemplo de evento.

```
{
    "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"
    }
}
```

Los valores posibles para `contactStatus` se definen en the section called “AWS Ground Station estados de contacto”.

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"
    }
}
```

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

Eventos de efemérides

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`

Registra las 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 userIdentity de CloudTrail .

Descripción de las entradas de los archivos de AWS Ground Station 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_PRINCIPAL_ID",
        "arn": "arn:aws:sts::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2019-05-15T21:11:59Z"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EX_PRINCIPAL_ID",
                "arn": "arn:aws:iam::123456789012:role/Alice",
                "accountId": "123456789012",
                "userName": "Alice"
            }
        }
    },
    "eventTime": "2019-05-15T21:14:37Z",
    "eventSource": "groundstation.amazonaws.com",
    "eventName": "ReserveContact",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "127.0.0.1",
    "userAgent": "Mozilla/5.0 Gecko/20100101 Firefox/123.0",
    "requestParameters": {
        "satelliteArn":
 "arn:aws:groundstation::123456789012:satellite/11111111-2222-3333-4444-555555555555",
        "groundStation": "Ohio 1",
        "startTime": 1558356107,
        "missionProfileArn": "arn:aws:groundstation:us-east-2:123456789012:mission-
profile/11111111-2222-3333-4444-555555555555",
        "endTime": 1558356886
    },
    "responseElements": {
        "contactId": "11111111-2222-3333-4444-555555555555"
    },
    "requestID": "11111111-2222-3333-4444-555555555555",
    "eventID": "11111111-2222-3333-4444-555555555555",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "11111111-2222-3333-4444-555555555555"
```

```
}
```

Consulta las 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 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.

> **Note**
>
> Las métricas específicas emitidas dependen de las AWS Ground Station capacidades que se utilicen. Según la configuración, es posible que solo se emita un subconjunto de las siguientes métricas.

Métrica	Dimensiones de la métrica	Descripción
`AzimuthAngle`	SatelliteId	El ángulo azimut de la antena. El norte verdadero está a 0 grados y el este a 90 grados. Unidades: grados
`BitErrorRate`	Canal, polarización, SatelliteId	Tasa de error en bits en un número determinado de

Métrica	Dimensiones de la métrica	Descripción
		transmisiones de bits. El ruido, la distorsión o las interfere ncias causan los errores de bits. Unidades: errores de bits por unidad de tiempo
`BlockErrorRate`	Canal, polarización, SatelliteId	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	Dimensiones de la métrica	Descripción
`CarrierFrequencyRecovery_Cn0`	Categoría, Config, SatelliteId	Relación portadora/densidad de ruido por unidad de ancho de banda. Unidades: decibelio-hercio (dB-HZ)
`CarrierFrequencyRecovery_Locked`	Categoría, Config, SatelliteId	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

Métrica	Dimensiones de la métrica	Descripción
`CarrierFrequencyRecovery_OffsetFrequency_Hz`	Categoría, Config, SatelliteId	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`	SatelliteId	El ángulo de elevación de la antena. El horizonte está a 0 grados y el cenit a 90 grados. Unidades: grados

Métrica	Dimensiones de la métrica	Descripción
`Es/N0`	Canal, polarización, SatelliteId	Relación entre la energía por símbolo y la densidad espectral de potencia del ruido. Unidades: decibelios (dB)
`ReceivedPower`	Polarización, SatelliteId	La intensidad de la señal medida en el desmodulador/descodificador. Unidades: decibelios relativos a milivatios (dBm)
`SymbolTimingRecovery_ErrorVectorMagnitude`	Categoría, Config, SatelliteId	La magnitud del vector de error entre los símbolos recibidos y los puntos de constelación ideales. Unidades: porcentaje

Métrica	Dimensiones de la métrica	Descripción
`SymbolTimingRecovery_Locked`	Categoría, Config, SatelliteId	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_OffsetSymbolRate`	Categoría, Config, SatelliteId	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?

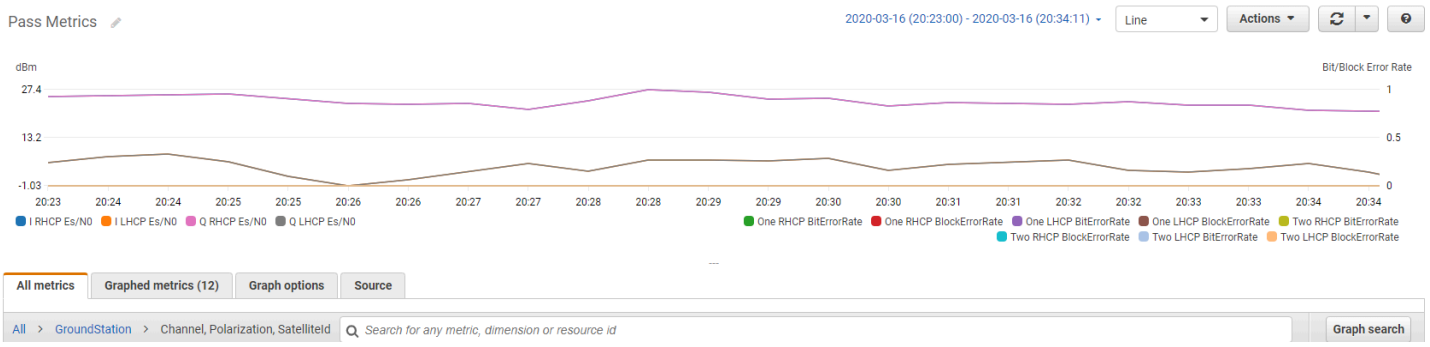
Puede filtrar AWS Ground Station los datos mediante las siguientes dimensiones.

Dimensión	Descripción
`Category`	Demodulación o decodificación.
`Channel`	Los canales para cada contacto incluyen Uno, Dos, I (en fase) y Q (cuadratura).
`Config`	Un arn de configuración de decodificación de demodos de enlace descendente de antena.
`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 dentro del período de 3 horas tras su recepción o que los mantengas fuera de Metrics. CloudWatch Para obtener más información sobre la CloudWatch retención, consulta CloudWatch Conceptos de Amazon: Retención métrica.

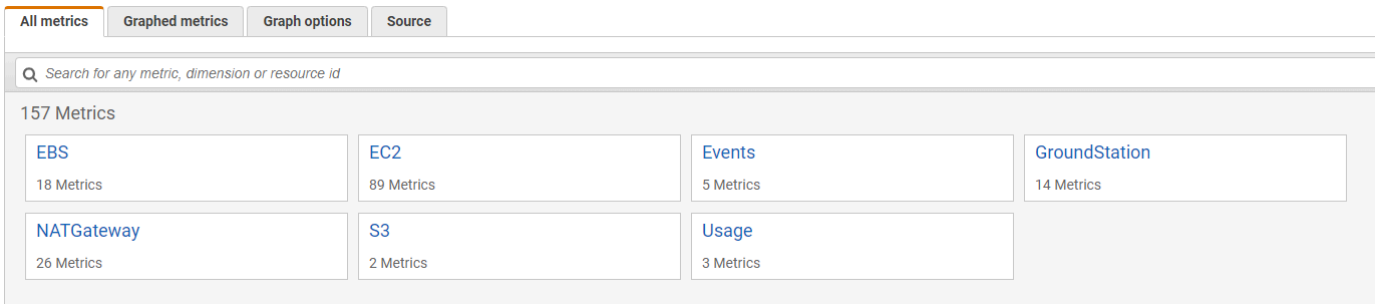
Además, los datos capturados en los primeros 60 segundos no contendrán suficiente información para producir métricas significativas y es probable que no se muestren. Para consultar las métricas significativas, se recomienda consultar los datos después de 60 segundos.



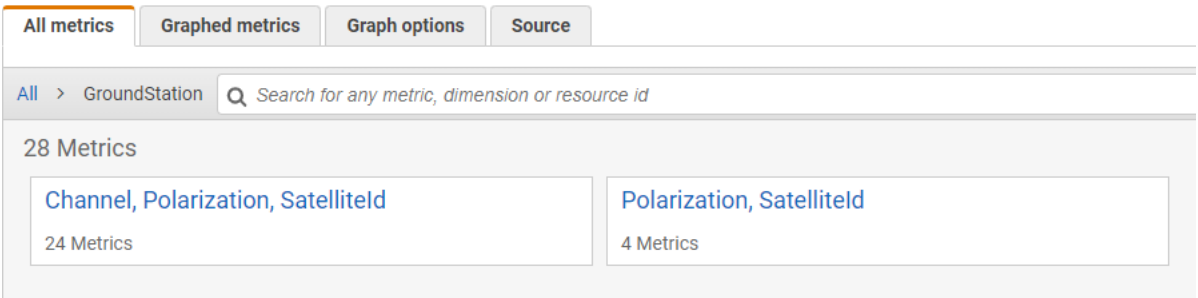
Para obtener más información sobre cómo graficar AWS Ground Station las métricas CloudWatch, consulte Graficar las métricas.

Para consultar las métricas desde la consola de

1. Abra la consola de CloudWatch .
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 graficar 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 encabezados 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 versión 2 de la AWS CLI.
2. Utilice el get-metric-datamétodo de la CloudWatch CLI para generar un archivo que se pueda modificar para especificar las métricas que le interesan y, a continuación, se utilice para consultarlas.

   Para ello, ejecute lo siguiente:`aws cloudwatch get-metric-data --generate-cli-skeleton`. Esto generará un resultado similar a:

```
{
   "MetricDataQueries": [
      {
         "Id": "",
         "MetricStat": {
            "Metric": {
               "Namespace": "",
               "MetricName": "",
               "Dimensions": [
                  {
                     "Name": "",
                     "Value": ""
                  }
               ]
            },
            "Period": 0,
            "Stat": "",
            "Unit": "Seconds"
         },
```

```
                "Expression": "",
                "Label": "",
                "ReturnData": true,
                "Period": 0,
                "AccountId": ""
             } ],
          "StartTime": "1970-01-01T00:00:00",
          "EndTime": "1970-01-01T00:00:00",
          "NextToken": "",
          "ScanBy": "TimestampDescending",
          "MaxDatapoints": 0,
          "LabelOptions": {
             "Timezone": ""
          }
       }
```

3. Enumere las CloudWatch métricas disponibles ejecutándolas`aws cloudwatch list-metrics`.

   Si lo has utilizado recientemente AWS Ground Station, el método debería devolver un resultado que contenga entradas como las siguientes:

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

> **Note**
>
> Debido a una limitación CloudWatch, si han pasado más de 2 semanas desde la última vez que lo usaste AWS Ground Station, tendrás que inspeccionar manualmente la tabla de métricas disponibles para encontrar los nombres y las dimensiones de las métricas en el espacio de nombres de las `AWS/GroundStation` métricas. Para obtener más información sobre la CloudWatch limitación, consulta: Ver las métricas disponibles

4. Modifique el archivo JSON que creó en el paso 2 para que coincida con los valores requeridos del paso 3, por ejemplo`SatelliteId`, y con los `Polarization` de sus métricas. Asegúrate también de actualizar los `StartTime` `EndTime` valores y para que coincidan con tu contacto. Por ejemplo:

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

```
            }
         ],
         "StartTime": "2024-02-08T00:00:00",
         "EndTime": "2024-04-09T00:00:00"
      }
```

> **Note**
>
> AWS Ground Station publica las métricas cada 1 a 60 segundos, según la métrica. Las métricas no se devolverán si el `Period` campo tiene un valor inferior al período de publicación de la métrica.

5. Ejecute `aws cloudwatch get-metric-data` con el archivo de configuración creado en los pasos anteriores. A continuación, se proporciona un ejemplo.

```
aws cloudwatch get-metric-data --cli-input-json file://
<nameOfConfigurationFileCreatedInStep2>.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": "receivedPowerExample",
         "Label": "ReceivedPowerExample",
         "Timestamps": [
            "2024-04-08T18:35:00+00:00",
            "2024-04-08T18:30:00+00:00",
            "2024-04-08T18:25:00+00:00"
         ],
         "Values": [
            -33.30191555023193,
            -31.46100273132324,
            -32.13915576934814
         ],
         "StatusCode": "Complete"
      }
```

```
    ],
    "Messages": []
}
```

Seguridad en AWS Ground Station

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, se beneficiará de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad. 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.

Cuando lo utilice AWS Ground Station, le recomendamos que siga las mejores prácticas del sector e implemente end-to-end el cifrado. AWS le permite APIs integrar el cifrado y la protección de datos. Para obtener más información sobre AWS la seguridad, 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

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

- ¿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 ayudarle 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 gestionador 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 Ground Station. 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 (IAM Identity Center), 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 gestionador 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 la firma de solicitudes, consulte AWS Signature Versión 4 para solicitudes 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 Autenticación multifactor AWS en IAM en 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 utiliza 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, consulta 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 de su empresa, 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 utiliza 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, consulta ¿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, consulta 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 puedes iniciar sesión como grupo. Puedes usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos para grandes conjuntos de usuarios. Por ejemplo, puede asignar un nombre a un grupo IAMAdminsy concederle permisos 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 de larga duración permanentes; no obstante, los roles proporcionan credenciales temporales. Para obtener más información, consulte Casos de uso para usuarios de IAM 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 persona determinada. Para asumir temporalmente un rol de IAM en el AWS Management Console, puede cambiar de un rol de usuario a uno de IAM (consola). Puedes asumir un rol llamando a una operación de AWS API AWS CLI o usando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulta Métodos para asumir un rol 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, puedes 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 de federación, consulte Crear un rol para un proveedor de identidad de terceros (federación) en la Guía de usuario de IAM. Si utiliza el 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 puedes acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulta Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .
- Permisos de usuario de IAM temporales: un usuario de IAM puedes asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puedes 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, consulta 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 realizas una llamada en un servicio, es habitual 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 AWS ellas, se te considera principal. 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, consulta 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 puedes 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 puedes ver, pero no editar, los permisos de los roles vinculados a servicios.

- Aplicaciones que se ejecutan en Amazon EC2: puedes usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una EC2 instancia y realizan AWS CLI solicitudes a la AWS API. Esto es preferible a almacenar las claves de acceso en la EC2 instancia. Para asignar un AWS rol a una EC2 instancia 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 que los programas que se ejecutan en la EC2 instancia obtengan credenciales temporales. Para obtener más información, consulte Usar un rol de IAM para conceder permisos a las aplicaciones que se ejecutan en EC2 instancias de Amazon 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, consulta 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 puedes crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puedes añadir las políticas de IAM a roles y los usuarios puedes asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utiliza 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 puedes 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 puedes 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 obtener 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. Los 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 puedes utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puedes 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 () ACLs

Las listas de control de acceso (ACLs) controlan qué responsables (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs 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 compatibles. AWS WAF ACLs Para obtener más información ACLs, consulte la descripción general de la 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 puedes 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 puedes conceder a una entidad de IAM (usuario o rol de IAM). Puedes 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, consulta Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCPs): SCPs 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 administrar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilitas todas las funciones de una organización, puedes aplicar políticas de control de servicios (SCPs) a una o a todas tus 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 sobre Organizations SCPs, consulte las políticas de control de servicios en la Guía del AWS Organizations usuario.
- Políticas de control de recursos (RCPs): RCPs son políticas de JSON que puedes usar para establecer los permisos máximos disponibles para los recursos de tus cuentas sin actualizar las políticas de IAM asociadas a cada recurso que poseas. El RCP limita los permisos de los recursos en las cuentas de los miembros y puede afectar a los permisos efectivos de las identidades, incluidos los permisos Usuario raíz de la cuenta de AWS, independientemente de si pertenecen a su organización. Para obtener más información sobre Organizations e RCPs incluir una lista de Servicios de AWS ese apoyo RCPs, consulte Políticas de control de recursos (RCPs) en la Guía del AWS Organizations usuario.
- 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 puedes proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulta 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 se AWS determina 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
ACLs	No
ABAC (etiquetas en políticas)	Sí
Credenciales temporales	Sí
Permisos de entidades principales	Sí

Característica de IAM	AWS Ground Station soporte
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 asociada. Para obtener 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

Admite políticas basadas en recursos: no

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los 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 puedes utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puedes 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 basada en recursos concede acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte Cross account resource access in IAM en la Guía del usuario de IAM.

Acciones políticas para AWS Ground Station

Compatibilidad con las acciones de políticas: sí

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

El elemento `Action` de una política JSON describe las acciones que puedes 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

Compatibilidad con los 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 puedes 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). Puedes 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, utiliza 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 tipos ARNs, 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

Compatibilidad con 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 puedes 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. Puedes crear expresiones condicionales que utilizan 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 puedes utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puedes 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, consulta 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

ACLs in AWS Ground Station

Soporta ACLs: No

Las listas de control de acceso (ACLs) controlan qué directores (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs 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 Definición de permisos con la autorización de ABAC en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulta Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Utilizar credenciales temporales con AWS Ground Station

Compatibilidad con 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 obtener más

información sobre el cambio de roles, consulte Cambio de un usuario a un rol de IAM (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 obtener más información, consulte Credenciales de seguridad temporales en IAM.

Permisos principales entre servicios para AWS Ground Station

Admite sesiones de acceso directo (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 sobre las políticas a la hora de realizar solicitudes de FAS, consulta Reenviar sesiones de acceso.

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

Admite roles vinculados a servicios: sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puedes 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 puedes ver, pero no editar, los permisos de los roles vinculados a servicios.

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulta 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 puedes crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puedes añadir las políticas de IAM a roles y los usuarios puedes 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 (consola) 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 ARNs de cada uno de los tipos de recursos, consulte las claves de condición, recursos y acciones de AWS Ground Station la Referencia de autorización de servicios.

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, consulta las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea 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 puedes 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, consulta Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utiliza condiciones en las políticas de IAM para restringir aún más el acceso: puedes agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puedes 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, consulta Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utiliza 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 Validación de políticas con el Analizador de acceso de IAM en la Guía del 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 exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte 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 el 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, adjunte también la política *ReadOnly* AWS gestionada AWS Ground Station *ConsoleAccess* o la política gestionada a las entidades. Para obtener 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 gestionadas 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
- No estoy autorizado a realizar tareas como: PassRole
- Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis AWS Ground Station recursos

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 gestionador 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 gestionador 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

Puedes crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puedes especificar una persona de confianza para que asuma el rol. En el caso de los servicios que respaldan políticas basadas en recursos o listas de control de acceso (ACLs), puedes usar esas políticas para permitir que las personas accedan a tus recursos.

Para obtener 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, consulta Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

AWS políticas gestionadas para AWS Ground Station

Una política AWS administrada es una política independiente creada y administrada por AWS. AWS Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte Políticas administradas de AWS en la Guía del usuario de IAM.

AWS política gestionada: AWSGround StationAgentInstancePolicy

Puede adjuntar la política `AWSGroundStationAgentInstancePolicy` a las identidades de IAM.

Esta política otorga permisos de AWS Ground Station agente a tu EC2 instancia de Amazon que permiten 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 de los permisos

Esta política incluye los siguientes permisos.

- `groundstation`— Permite que las instancias de punto final del flujo de datos llamen al Ground Station Agent. APIs

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

AWS política gestionada: AWSService RoleForGroundStationDataflowEndpointGroupPolicy

No puede adjuntarse AWSService RoleForGroundStationDataflowEndpointGroupPolicy a sus entidades de IAM. Esta política está asociada a un rol vinculado al servicio que le permite AWS Ground Station realizar acciones en su nombre. Para más información, consulte el Uso de roles vinculados a servicios.

Esta política otorga EC2 permisos que permiten AWS Ground Station encontrar direcciones públicas IPv4 .

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `ec2:DescribeAddresses`— Permite AWS Ground Station enumerar todas las IPs entidades asociadas EIPs en su nombre.
- `ec2:DescribeNetworkInterfaces`— Permite AWS Ground Station obtener información en su nombre sobre las interfaces de red asociadas a EC2 las instancias.

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

AWS Ground Station actualizaciones de las políticas AWS gestionadas

Consulte los detalles sobre las actualizaciones de las políticas AWS administradas AWS Ground Station desde que este servicio comenzó a rastrear estos cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbase a la fuente RSS de la página del historial del AWS Ground Station documento.

Cambio	Descripción	Fecha
AWSGroundStationAgentInstancePolicy: política nueva	AWS Ground Station se agregó una nueva política para proporcionar a la instancia de punto final del flujo de datos permisos para usar AWS Ground Station Agent.	12 de abril de 2023
AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy: política nueva	AWS Ground Station se agregó una nueva política que otorga EC2 permisos que permiten encontrar IPv4 las direcciones públicas asociadas AWS Ground Station a las instancias EIPs y las interfaces de red asociadas EC2 a ellas.	2 de noviembre de 2022
AWS Ground Station comenzó a rastrear los cambios	AWS Ground Station comenzó a rastrear los cambios de las políticas AWS gestionadas.	1 de marzo de 2021

Utilice funciones vinculadas a servicios para Ground Station

AWS Ground Station usa roles vinculados al AWS Identity and Access Management servicio (IAM). Un rol vinculado al servicio es un tipo único de rol de IAM que está vinculado directamente a Ground Station. Las funciones vinculadas al servicio están predefinidas por Ground Station e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios 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 asociar a ninguna otra entidad de IAM.

Para obtener información sobre otros servicios que admiten funciones vinculadas a servicios, consulte los AWS servicios que funcionan con IAM y busque los servicios con la palabra Sí en la columna Funciones vinculadas a servicios. Elija 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 usa el rol vinculado al servicio denominado: AWSServiceRoleForGroundStationDataflowEndpointGroupAWS GroundStation usa este rol vinculado al servicio para EC2 invocar y buscar direcciones públicas. IPv4

El rol AWSService RoleForGroundStationDataflowEndpointGroup vinculado al servicio confía en los siguientes servicios para asumir el rol:

- `groundstation.amazonaws.com`

La política de permisos de roles denominada AWSService RoleForGroundStationDataflowEndpointGroupPolicy permite a Ground Station completar las siguientes acciones en los recursos especificados:

- Acción: `ec2:DescribeAddresses` en `all AWS resources (*)`

  La acción permite a Ground Station enumerar todos los IPs elementos asociados a EIPs.

- Acción: `ec2:DescribeNetworkInterfaces` en `all AWS resources (*)`

  La acción permite a Ground Station obtener información sobre las interfaces de red asociadas a las EC2 instancias

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. Al crear una DataflowEndpointGroup en la API AWS CLI o en la AWS API, Ground Station crea automáticamente la función vinculada al servicio.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Al crear una DataflowEndpointGroup, Ground Station vuelve a crear la función vinculada al servicio para usted.

También puedes usar la consola de IAM para crear un rol vinculado a un servicio con el caso de uso de Data Delivery to Amazon EC2. En la API AWS CLI o en la AWS API, crea una función vinculada al servicio con el nombre del servicio. `groundstation.amazonaws.com` Para obtener más información, consulte Crear 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 permite editar el rol AWSService RoleForGroundStationDataflowEndpointGroup vinculado al servicio. Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con 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 usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. Así no tendrá una entidad no utilizada que no se supervise ni mantenga de forma activa.

Puede eliminar un rol vinculado al servicio solo después de eliminarlo por primera vez DataflowEndpointGroups mediante el rol vinculado al servicio. Esto lo protege de la revocación inadvertida de sus permisos. DataflowEndpointGroups Si un rol vinculado a un servicio se usa con varios DataflowEndpointGroups, debe eliminar todos los DataflowEndpointGroups que usen 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 el AWSService RoleForGroundStationDataflowEndpointGroup

- Elimine DataflowEndpointGroups mediante la AWS CLI o la API de AWS.

Para eliminar manualmente el rol vinculado a servicios mediante IAM

Utilice la consola de IAM AWS CLI, la o la AWS API para eliminar la función vinculada al AWSService RoleForGroundStationDataflowEndpointGroup servicio. Para obtener más información, consulte Eliminación de un rol vinculado a servicios 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 tu cuenta que se utiliza para llamar a la CreateDataflowEndpointGroup API no tiene el permiso. `iam:CreateServiceLinkedRole` Un administrador con el permiso `iam:CreateServiceLinkedRole` debe crear manualmente el rol vinculado al servicio para su cuenta.

Cifrado de datos en reposo para AWS Ground Station

AWS Ground Station proporciona cifrado de forma predeterminada para proteger sus datos confidenciales 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 de su cuenta.

AWS Ground Station requiere la concesión para utilizar la clave gestionada por el cliente en las siguientes operaciones internas:

- Envíe GenerateDataKeysolicitudes a AWS KMS para generar claves de datos cifradas por su clave administrada por el cliente.
- Envíe solicitudes de descifrado a AWS KMS para descifrar las claves de datos cifradas, de modo que puedan usarse para cifrar sus datos.
- Envíe solicitudes de cifrado 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.

Creación de una clave administrada por el cliente

Puede crear una clave simétrica gestionada por el cliente mediante la consola de AWS administración o el KMS. AWS APIs

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.

- Llama a Decrypt para usar la clave de datos cifrados almacenada para acceder a los datos cifrados.
- Llame a Encrypt para usar 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 de la clave gestionada 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 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"
}
```

Cifrado de datos durante el tránsito para AWS Ground Station

AWS Ground Station proporciona cifrado de forma predeterminada para proteger sus datos confidenciales durante el tránsito. Los datos se pueden transmitir entre las ubicaciones de las AWS Ground Station antenas y las EC2 instancias de Amazon de dos maneras, según la configuración del perfil de la misión.

- AWS Ground Station Agente
- Punto final del flujo de datos

Cada método de transmisión de datos gestiona el cifrado de los datos en tránsito de forma diferente. En las secciones siguientes se describe cada método.

AWS Ground Station Flujos de agentes

AWS Ground Station El agente cifra sus transmisiones mediante claves administradas AWS KMS por el cliente. El AWS Ground Station agente que se ejecuta en tu EC2 instancia de Amazon descifrará automáticamente la transmisión para proporcionar datos descifrados.

La AWS KMS clave utilizada para cifrar una transmisión se especifica al crear una `MissionProfile` en el parámetro. streamsKmsKey Todos los permisos que otorgan AWS Ground Station acceso a las claves se gestionan mediante la política de AWS KMS claves adjunta. `streamsKmsKey`

Flujos de puntos finales de flujo de datos

Los flujos de puntos finales de Dataflow se cifran mediante Datagram Transport Layer Security (DTLS). Esto se hace mediante certificados autofirmados y no requiere configuración adicional.

Ejemplos de configuraciones de perfil de misión

Los ejemplos proporcionados muestran cómo tomar un satélite de transmisión pública y crear un perfil de misión que lo respalde. Las plantillas resultantes se proporcionan para ayudarle a ponerse en contacto con un satélite de radiodifusión pública y a tomar decisiones sobre sus satélites.

Temas

JPSS-1: Satélite de radiodifusión pública (PBS): evaluación

Esta sección de ejemplo coincide con. Descripción general del proceso de incorporación de clientes Proporciona un breve análisis de compatibilidad AWS Ground Station y sienta las bases para los ejemplos específicos que siguen.

Como se menciona en la Satélites de radiodifusión pública sección, puede utilizar algunos satélites o rutas de comunicación de un satélite que estén disponibles públicamente. En esta sección describimos el JPSS-1 en los siguientes términos. AWS Ground Station Como referencia, utilizamos los datos de alta velocidad (HRD) de las naves espaciales del Joint Polar Satellite System 1 (JPSS-1) para dirigir el documento de control de la interfaz de radiofrecuencia (RF) (ICD) de las estaciones de transmisión (DBS) para completar el ejemplo. Además, cabe destacar que el JPSS-1 está asociado al ID 43013 del NORAD.

El satélite JPSS-1 ofrece una ruta de comunicación de enlace ascendente y tres de enlace descendente directo, como se ve en la figura 1-1 del ICD. De estas cuatro rutas de comunicación, solo la única ruta de comunicación de enlace descendente de datos de alta velocidad (HRD) está disponible para el consumo público. En función de esto, verá que esta ruta también tendrá datos mucho más específicos asociados. Las cuatro rutas son las siguientes:

- Ruta de comando (enlace ascendente) a una frecuencia MHz central de 2067,27 con una velocidad de datos de 2 a 128 kbps. Esta ruta no es de acceso público.

- Ruta de telemetría (enlace descendente) a una frecuencia MHz central de 2247,5 con una velocidad de datos de 1 a 524 kbps. Esta ruta no es de acceso público.
- Ruta SMD (enlace descendente) a una frecuencia GHz central de 26,7034 con una velocidad de datos de 150 a 300 Mbps. Esta ruta no es de acceso público.
- La RF de la ruta HRD (enlace descendente) a una frecuencia MHz central de 7812 con una velocidad de datos de 15 Mbps. Tiene un ancho de MHz banda de 30, y es. right-hand-circular-polarized Cuando incorporas el JPSS-1 con AWS Ground Station, esta es la ruta de comunicación a la que tienes acceso. Esta ruta de comunicación contiene datos científicos de los instrumentos, datos de ingeniería de los instrumentos, datos de telemetría de los instrumentos y datos de mantenimiento de las naves espaciales en tiempo real.

Al comparar las posibles rutas de datos, vemos que las rutas de comando (enlace ascendente), telemetría (enlace descendente) y HRD (enlace descendente) cumplen con las capacidades de frecuencia, ancho de banda y uso simultáneo multicanal de las mismas. AWS Ground Station La ruta SMD no es compatible porque la frecuencia central está fuera del alcance de los receptores existentes. Para obtener más información sobre las capacidades compatibles, consulte. AWS Ground Station Capacidades del sitio

> **Note**
>
> Como la ruta SMD no es compatible AWS Ground Station , no se representará en las configuraciones de ejemplo.

> **Note**
>
> Como las rutas de comando (enlace ascendente) y telemetría (enlace descendente) no están definidas en el ICD ni están disponibles para uso público, los valores proporcionados cuando se utilizan son teóricos.

Satélite de transmisión pública que utiliza la entrega de datos de Amazon S3

Este ejemplo se basa en el análisis realizado en la JPSS-1: Satélite de radiodifusión pública (PBS): evaluación sección de la guía del usuario.

Para este ejemplo, tendrá que asumir un escenario: desea capturar la ruta de comunicación del HRD como frecuencia intermedia digital y almacenarla para su futuro procesamiento por lotes. Esto ahorra las muestras en cuadratura infásica (I/Q) de radiofrecuencia (RF) sin procesar una vez digitalizadas. Una vez que los datos estén en su bucket de Amazon S3, podrá demodular y decodificar los datos con el software que desee. Consulte el MathWorks tutorial para ver un ejemplo detallado del procesamiento. Tras usar este ejemplo, puedes considerar añadir componentes de precios al EC2 contado de Amazon para procesar los datos y reducir los costes generales de procesamiento.

Vías de comunicación

Esta sección representa Planifique las rutas de comunicación de su flujo de datos los primeros pasos.

Todos los siguientes fragmentos de plantilla pertenecen a la sección Recursos de la AWS CloudFormation plantilla.

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

> **Note**
>
> Para obtener más información sobre el contenido de una AWS CloudFormation plantilla, consulte las secciones de plantillas.

Dado nuestro escenario de ofrecer una única ruta de comunicación a Amazon S3, sabe que tendrá una única ruta de entrega asíncrona. Según la Entrega de datos asíncrona sección, debe definir un bucket de Amazon S3.

```
  # The S3 bucket where AWS Ground Station will deliver the downlinked data.
  GroundStationS3DataDeliveryBucket:
    Type: AWS::S3::Bucket
    DeletionPolicy: Retain
    UpdateReplacePolicy: Retain
    Properties:
```

```
      # Results in a bucket name formatted like: aws-groundstation-data-{account id}-
{region}-{random 8 character string}
      BucketName: !Join ["-", ["aws-groundstation-data", !Ref AWS::AccountId, !Ref
 AWS::Region, !Select [0, !Split ["-", !Select [2, !Split ["/", !Ref AWS::StackId]]]]]]
```

Además, tendrá que crear las funciones y políticas adecuadas para poder AWS Ground Station utilizar el bucket.

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

  # The S3 bucket policy that defines what actions AWS Ground Station can perform on
 your S3 bucket.
  GroundStationS3DataDeliveryBucketPolicy:
    Type: AWS::IAM::Policy
    Properties:
      PolicyDocument:
        Statement:
          - Action:
              - 's3:GetBucketLocation'
            Effect: Allow
            Resource:
              - !GetAtt GroundStationS3DataDeliveryBucket.Arn
          - Action:
```

```
            - 's3:PutObject'
          Effect: Allow
          Resource:
            - !Join [ "/", [ !GetAtt GroundStationS3DataDeliveryBucket.Arn, "*" ] ]
    PolicyName: GroundStationS3DataDeliveryPolicy
    Roles:
      - !Ref GroundStationS3DataDeliveryRole
```

AWS Ground Station configuraciones

Esta sección representa Crear configuraciones los primeros pasos.

Necesitarás una configuración de seguimiento para establecer tus preferencias sobre el uso del autotrack. Si se selecciona PREFERRED como pista automática, se puede mejorar la calidad de la señal, pero no es obligatorio para cumplir con la calidad de la señal, ya que la calidad de las efemérides del JPSS-1 es suficiente.

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

Según la ruta de comunicación, tendrá que definir una configuración de antena y enlace descendente para representar la parte del satélite, así como una grabación s3 para hacer referencia al bucket de Amazon S3 que acaba de crear.

```
 # The AWS Ground Station Antenna Downlink Config that defines the frequency spectrum
used to
 # downlink data from your satellite.
 JpssDownlinkDigIfAntennaConfig:
   Type: AWS::GroundStation::Config
   Properties:
     Name: "JPSS Downlink DigIF Antenna Config"
     ConfigData:
       AntennaDownlinkConfig:
```

```
          SpectrumConfig:
            Bandwidth:
              Units: "MHz"
              Value: 30
            CenterFrequency:
              Units: "MHz"
              Value: 7812
            Polarization: "RIGHT_HAND"

  # The AWS Ground Station S3 Recording Config that defines the S3 bucket and IAM role
to use
  # when AWS Ground Station delivers the downlink data.
  S3RecordingConfig:
    Type: AWS::GroundStation::Config
    DependsOn: GroundStationS3DataDeliveryBucketPolicy
    Properties:
      Name: "JPSS S3 Recording Config"
      ConfigData:
        S3RecordingConfig:
          BucketArn: !GetAtt GroundStationS3DataDeliveryBucket.Arn
          RoleArn: !GetAtt GroundStationS3DataDeliveryRole.Arn
```

AWS Ground Station perfil de misión

Esta sección representa Crear perfil de misión cómo empezar.

Ahora que tiene las configuraciones asociadas, puede usarlas para construir el flujo de datos. Utilizará los valores predeterminados para el resto de los parámetros.

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

Poniéndolo todo junto

Con los recursos anteriores, ahora puede programar los contactos del JPSS-1 para la entrega asíncrona de datos desde cualquiera de sus dispositivos integrados. AWS Ground Station [AWS Ground Station Ubicaciones]

La siguiente es una AWS CloudFormation plantilla completa que incluye todos los recursos descritos en esta sección combinados en una sola plantilla que se puede utilizar directamente. AWS CloudFormation

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.

Si Aqua, SNPP, JPSS-1/NOAA-20 y Terra no están integrados en su cuenta, consulte. [Satélite a bordo]

> **Note**
>
> Puede acceder a la plantilla accediendo al bucket de Amazon S3 del cliente con AWS credenciales válidas. Los enlaces que aparecen a continuación utilizan un bucket regional de Amazon S3. Cambie el código de `us-west-2` región para que represente la región correspondiente en la que desea crear la AWS CloudFormation pila.
> Además, en las siguientes instrucciones se utiliza YAML. Sin embargo, las plantillas están disponibles en formato YAML y JSON. Para usar JSON, reemplaza la extensión del `.yml` archivo por la extensión `.json` al descargar la plantilla.

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
```

Satélite de transmisión pública que utiliza un punto final de flujo de datos (banda estrecha)

Este ejemplo se basa en el análisis realizado en la JPSS-1: Satélite de radiodifusión pública (PBS): evaluación sección de la guía del usuario.

Para completar este ejemplo, tendrá que asumir un escenario: desea capturar la ruta de comunicación del HRD como frecuencia intermedia digital (DigiF) y procesarla tal como la recibe una aplicación de punto final de flujo de datos en una instancia de EC2 Amazon mediante un SDR.

Rutas de comunicación

Esta sección representa Planifique las rutas de comunicación de su flujo de datos los primeros pasos. Para este ejemplo, creará dos secciones en la AWS CloudFormation plantilla: las secciones de parámetros y recursos.

> **Note**
>
> Para obtener más información sobre el contenido de una AWS CloudFormation plantilla, consulte las secciones de plantillas.

Para la sección de parámetros, va a añadir los siguientes parámetros. Especificará sus valores al crear la pila a través de la AWS CloudFormation consola.

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

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

> **Note**
>
> Debe crear un key pair y proporcionar el nombre del EC2 `EC2Key` parámetro Amazon. Consulta Crear un key pair para tu EC2 instancia de Amazon.
> Además, tendrás que proporcionar el ID de AMI específico de la región correcto al crear la AWS CloudFormation pila. Consulte AWS Ground Station Imágenes de máquinas de Amazon (AMIs).

Los fragmentos de plantilla restantes pertenecen a la sección Recursos de la AWS CloudFormation plantilla.

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

Dado nuestro escenario de entregar una única ruta de comunicación a una EC2 instancia, tendrás una única ruta de entrega sincrónica. Según la Entrega de datos sincrónica sección, debe instalar y configurar una EC2 instancia de Amazon con una aplicación de punto final de flujo de datos y crear uno o más grupos de puntos de enlace de flujo de datos.

```
  # The EC2 instance that will send/receive data to/from your satellite using AWS
 Ground Station.
  ReceiverInstance:
    Type: AWS::EC2::Instance
    Properties:
      DisableApiTermination: false
      IamInstanceProfile: !Ref GeneralInstanceProfile
      ImageId: !Ref ReceiverAMI
      InstanceType: m5.4xlarge
      KeyName: !Ref EC2Key
```

```
      Monitoring: true
      PlacementGroupName: !Ref ClusterPlacementGroup
      SecurityGroupIds:
        - Ref: InstanceSecurityGroup
      SubnetId: !Ref ReceiverSubnet
      BlockDeviceMappings:
        - DeviceName: /dev/xvda
          Ebs:
            VolumeType: gp2
            VolumeSize: 40
      Tags:
        - Key: Name
          Value: !Join [ "-" , [ "Receiver" , !Ref "AWS::StackName" ] ]
      UserData:
        Fn::Base64:
          |
          #!/bin/bash
          exec > >(tee /var/log/user-data.log|logger -t user-data -s 2>/dev/console)
2>&1
          echo `date +'%F %R:%S'` "INFO: Logging Setup" >&2

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

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

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

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

          exit 0

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

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

```
          Description: "AWS Ground Station Downlink Stream"

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

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

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

  ReceiverSubnet:
    Type: AWS::EC2::Subnet
```

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

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

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

Además, también tendrá que crear las políticas y funciones adecuadas para poder crear una interfaz de red elástica (ENI) en su cuenta. AWS Ground Station

```
  # AWS Ground Station assumes this role to create/delete ENIs in your account in order
to stream data.
  DataDeliveryServiceRole:
    Type: AWS::IAM::Role
    Properties:
      Policies:
```

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

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

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

AWS Ground Station configuraciones

Esta sección representa Crear configuraciones los primeros pasos.

Necesitarás una configuración de seguimiento para establecer tus preferencias sobre el uso del autotrack. Si se selecciona PREFERRED como pista automática, se puede mejorar la calidad de la señal, pero no es obligatorio para cumplir con la calidad de la señal, ya que la calidad de las efemérides del JPSS-1 es suficiente.

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

En función de la ruta de comunicación, tendrá que definir una configuración de antena y enlace descendente que represente la parte del satélite, así como una configuración de punto final del flujo de datos que haga referencia al grupo de puntos finales del flujo de datos que define los detalles del punto final.

```
  # The AWS Ground Station Antenna Downlink Config that defines the frequency spectrum
  used to
  # downlink data from your satellite.
  SnppJpssDownlinkDigIfAntennaConfig:
    Type: AWS::GroundStation::Config
    Properties:
      Name: "SNPP JPSS Downlink DigIF Antenna Config"
      ConfigData:
        AntennaDownlinkConfig:
```

```
          SpectrumConfig:
            Bandwidth:
              Units: "MHz"
              Value: 30
            CenterFrequency:
              Units: "MHz"
              Value: 7812
            Polarization: "RIGHT_HAND"

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

AWS Ground Station perfil de la misión

Esta sección representa Crear perfil de misión los primeros pasos.

Ahora que tiene las configuraciones asociadas, puede usarlas para construir el flujo de datos. Utilizará los valores predeterminados para el resto de los parámetros.

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

```
          Destination: !Ref DownlinkDigIfEndpointConfig
```

Poniéndolo todo junto

Con los recursos anteriores, ahora puede programar los contactos del JPSS-1 para la entrega sincrónica de datos desde cualquiera de sus dispositivos integrados. AWS Ground Station [AWS Ground Station Ubicaciones]

La siguiente es una AWS CloudFormation plantilla completa que incluye todos los recursos descritos en esta sección combinados en una sola plantilla que se puede utilizar directamente. AWS CloudFormation

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 EC2 instancia de Amazon y los AWS CloudFormation recursos necesarios para recibir datos de transmisión directa de DigiF sin procesar.

Si Aqua, SNPP, JPSS-1/NOAA-20 y Terra no están integrados en su cuenta, consulte. [Satélite a bordo]

> **Note**
>
> Puede acceder a la plantilla accediendo al bucket de Amazon S3 del cliente con AWS credenciales válidas. Los enlaces que aparecen a continuación utilizan un bucket regional de Amazon S3. Cambie el código de `us-west-2` región para que represente la región correspondiente en la que desea crear la AWS CloudFormation pila.
> Además, en las siguientes instrucciones se utiliza YAML. Sin embargo, las plantillas están disponibles en formato YAML y JSON. Para usar JSON, reemplaza la extensión del `.yml` archivo por la extensión `.json` al descargar la plantilla.

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 adicionales define la plantilla?

La `AquaSnppJpssTerraDigIF` plantilla incluye los siguientes recursos adicionales:

- (Opcional) Activadores de CloudWatch eventos: 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.
- EC2 Verificación de contactos (opcional): la opción de usar Lambda para configurar un sistema de verificación de las EC2 instancias de Amazon para los contactos con notificaciones de SNS. Es importante tener en cuenta que esto puede conllevar gastos en función del uso actual.
- 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.
- Perfiles de misión adicionales: perfiles de misión para otros satélites de transmisión pública (Aqua, SNPP y Terra).
- Configuraciones adicionales de enlace descendente de antena: configuraciones de enlace descendente de antena para otros satélites de transmisión pública (Aqua, SNPP y Terra).

Los valores y parámetros de los satélites de esta plantilla ya se han rellenado. Estos parámetros facilitan su uso inmediato con estos satélites. AWS Ground Station 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 utiliza una aplicación de punto final del flujo de datos para recibir el flujo de datos desde el puerto definido por AWS

Ground Station 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. AWS::GroundStation::DataflowEndpointGroup

Satélite de transmisión pública que utiliza un punto final de flujo de datos (demodulado y decodificado)

Este ejemplo se basa en el análisis realizado en la JPSS-1: Satélite de radiodifusión pública (PBS): evaluación sección de la guía del usuario.

Para completar este ejemplo, tendrá que asumir un escenario: desea capturar la ruta de comunicación del HRD como datos de transmisión directa desmodulados y decodificados mediante un punto final de flujo de datos. Este ejemplo es un buen punto de partida si planea procesar los datos con el software Direct Readout Labs de la NASA (RT-STPS e IPOPP).

Vías de comunicación

Esta sección representa Planifique las rutas de comunicación de su flujo de datos los primeros pasos. Para este ejemplo, creará dos secciones en la AWS CloudFormation plantilla: las secciones de parámetros y recursos.

> **Note**
>
> Para obtener más información sobre el contenido de una AWS CloudFormation plantilla, consulte las secciones de plantillas.

Para la sección de parámetros, va a añadir los siguientes parámetros. Especificará sus valores al crear la pila a través de la AWS CloudFormation consola.

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

```
    ConstraintDescription: must be the name of an existing EC2 KeyPair.

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

> **Note**
>
> Debe crear un key pair y proporcionar el nombre del EC2 `EC2Key` parámetro Amazon. Consulta Crear un key pair para tu EC2 instancia de Amazon.
> Además, tendrás que proporcionar el ID de AMI específico de la región correcto al crear la AWS CloudFormation pila. Consulte AWS Ground Station Imágenes de máquinas de Amazon (AMIs).

Los fragmentos de plantilla restantes pertenecen a la sección Recursos de la AWS CloudFormation plantilla.

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

Dado nuestro escenario de entregar una única ruta de comunicación a una EC2 instancia, tendrás una única ruta de entrega sincrónica. Según la Entrega de datos sincrónica sección, debe instalar y configurar una EC2 instancia de Amazon con una aplicación de punto final de flujo de datos y crear uno o más grupos de puntos de enlace de flujo de datos.

```
  # The EC2 instance that will send/receive data to/from your satellite using AWS
 Ground Station.
  ReceiverInstance:
    Type: AWS::EC2::Instance
    Properties:
      DisableApiTermination: false
      IamInstanceProfile: !Ref GeneralInstanceProfile
```

```
      ImageId: !Ref ReceiverAMI
      InstanceType: m5.4xlarge
      KeyName: !Ref EC2Key
      Monitoring: true
      PlacementGroupName: !Ref ClusterPlacementGroup
      SecurityGroupIds:
        - Ref: InstanceSecurityGroup
      SubnetId: !Ref ReceiverSubnet
      BlockDeviceMappings:
        - DeviceName: /dev/xvda
          Ebs:
            VolumeType: gp2
            VolumeSize: 40
      Tags:
        - Key: Name
          Value: !Join [ "-" , [ "Receiver" , !Ref "AWS::StackName" ] ]
      UserData:
        Fn::Base64:
          |
          #!/bin/bash
          exec > >(tee /var/log/user-data.log|logger -t user-data -s 2>/dev/console)
2>&1
          echo `date +'%F %R:%S'` "INFO: Logging Setup" >&2

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

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

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

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

        exit 0
```

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

 # The security group that the ENI created by AWS Ground Station belongs to.
 DataflowEndpointSecurityGroup:
   Type: AWS::EC2::SecurityGroup
   Properties:
     GroupDescription: Security Group for AWS Ground Station registration of Dataflow
Endpoint Groups
     VpcId: !Ref ReceiverVPC
     SecurityGroupEgress:
```

```
        - IpProtocol: udp
          FromPort: 55888
          ToPort: 55888
          CidrIp: 10.0.0.0/8
          Description: "AWS Ground Station Downlink Stream To 10/8"
        - IpProtocol: udp
          FromPort: 55888
          ToPort: 55888
          CidrIp: 172.16.0.0/12
          Description: "AWS Ground Station Downlink Stream To 172.16/12"
        - IpProtocol: udp
          FromPort: 55888
          ToPort: 55888
          CidrIp: 192.168.0.0/16
          Description: "AWS Ground Station Downlink Stream To 192.168/16"

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

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

  ReceiverVPC:
    Type: AWS::EC2::VPC
    Properties:
      CidrBlock: "10.0.0.0/16"
      Tags:
        - Key: "Name"
```

```
          Value: "AWS Ground Station - PBS to dataflow endpoint Demod Decode Example
VPC"
        - Key: "Description"
          Value: "VPC for EC2 instance receiving AWS Ground Station data"

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

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

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

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

También necesitará las políticas, las funciones y los perfiles adecuados para poder crear AWS Ground Station una interfaz de red elástica (ENI) en su cuenta.

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

 # The EC2 instance assumes this role.
 InstanceRole:
   Type: AWS::IAM::Role
   Properties:
     AssumeRolePolicyDocument:
       Version: "2012-10-17"
       Statement:
         - Effect: "Allow"
           Principal:
```

```
            Service:
              - "ec2.amazonaws.com"
          Action:
            - "sts:AssumeRole"
    Path: "/"
    ManagedPolicyArns:
      - arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess
      - arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceforEC2Role
      - arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy
      - arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforSSM
```

AWS Ground Station configuraciones

Esta sección representa Crear configuraciones la guía del usuario.

Necesitarás una configuración de seguimiento para establecer tus preferencias sobre el uso del autotrack. Si se selecciona PREFERRED como pista automática, se puede mejorar la calidad de la señal, pero no es obligatorio para cumplir con la calidad de la señal, ya que la calidad de las efemérides del JPSS-1 es suficiente.

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

En función de la ruta de comunicación, tendrá que definir una antenna-downlink-demod-decodeconfiguración que represente la parte del satélite, así como una configuración de puntos finales del flujo de datos que haga referencia al grupo de puntos finales del flujo de datos que define los detalles de los puntos finales.

> **Note**
>
> Para obtener más información sobre cómo configurar los valores de yDemodulationConfig, consulte. DecodeConfig Configuración de descodificación y desmodulación de enlace de bajada de antena

```
 # The AWS Ground Station Antenna Downlink Config that defines the frequency spectrum
used to
 # downlink data from your satellite.
 JpssDownlinkDemodDecodeAntennaConfig:
   Type: AWS::GroundStation::Config
   Properties:
     Name: "JPSS Downlink Demod Decode Antenna Config"
     ConfigData:
       AntennaDownlinkDemodDecodeConfig:
         SpectrumConfig:
           CenterFrequency:
             Value: 7812
             Units: "MHz"
           Polarization: "RIGHT_HAND"
           Bandwidth:
             Value: 30
             Units: "MHz"
         DemodulationConfig:
           UnvalidatedJSON: '{
             "type":"QPSK",
             "qpsk":{
               "carrierFrequencyRecovery":{
                 "centerFrequency":{
                   "value":7812,
                   "units":"MHz"
                 },
                 "range":{
                   "value":250,
                   "units":"kHz"
                 }
               },
               "symbolTimingRecovery":{
                 "symbolRate":{
                   "value":15,
```

```
                "units":"Msps"
              },
              "range":{
                "value":0.75,
                "units":"ksps"
              },
              "matchedFilter":{
                "type":"ROOT_RAISED_COSINE",
                "rolloffFactor":0.5
              }
            }
          }
        }'
      DecodeConfig:
        UnvalidatedJSON: '{
          "edges":[
            {
              "from":"I-Ingress",
              "to":"IQ-Recombiner"
            },
            {
              "from":"Q-Ingress",
              "to":"IQ-Recombiner"
            },
            {
              "from":"IQ-Recombiner",
              "to":"CcsdsViterbiDecoder"
            },
            {
              "from":"CcsdsViterbiDecoder",
              "to":"NrzmDecoder"
            },
            {
              "from":"NrzmDecoder",
              "to":"UncodedFramesEgress"
            }
          ],
          "nodeConfigs":{
            "I-Ingress":{
              "type":"CODED_SYMBOLS_INGRESS",
              "codedSymbolsIngress":{
                "source":"I"
              }
            },
```

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

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

AWS Ground Station perfil de la misión

Esta sección representa Crear perfil de misión la guía del usuario.

Ahora que tiene las configuraciones asociadas, puede usarlas para construir el flujo de datos. Utilizará los valores predeterminados para el resto de los parámetros.

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

Poniéndolo todo junto

Con los recursos anteriores, ahora puede programar los contactos del JPSS-1 para la entrega sincrónica de datos desde cualquiera de sus dispositivos integrados. AWS Ground Station [AWS Ground Station Ubicaciones]

La siguiente es una AWS CloudFormation plantilla completa que incluye todos los recursos descritos en esta sección combinados en una sola plantilla que se puede utilizar directamente. AWS CloudFormation

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 EC2 instancia de Amazon y los AWS Ground Station recursos necesarios para programar contactos y recibir datos de transmisión directa desmodulados y decodificados.

Si Aqua, SNPP, JPSS-1/NOAA-20 y Terra no están integrados en su cuenta, consulte. [Satélite a bordo]

> **Note**
>
> Puede acceder a la plantilla accediendo al bucket de Amazon S3 del cliente con AWS credenciales válidas. Los enlaces que aparecen a continuación utilizan un bucket regional de Amazon S3. Cambie el código de `us-west-2` región para que represente la región correspondiente en la que desea crear la AWS CloudFormation pila.
> Además, en las siguientes instrucciones se utiliza YAML. Sin embargo, las plantillas están disponibles en formato YAML y JSON. Para usar JSON, reemplaza la extensión del `.yml` archivo por la extensión `.json` al descargar la plantilla.

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 adicionales define la plantilla?

La `AquaSnppJpss` plantilla incluye los siguientes recursos adicionales:

- (Opcional) Activadores de CloudWatch eventos: 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.
- EC2 Verificación de contactos (opcional): la opción de usar Lambda para configurar un sistema de verificación de las EC2 instancias de Amazon para los contactos con notificaciones de SNS. Es importante tener en cuenta que esto puede conllevar gastos en función del uso actual.
- 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, consulte. Satélite de transmisión pública que utiliza AWS Ground Station Agent (banda ancha) Estas opciones seguirán ampliándose a medida que se publiquen actualizaciones y características adicionales del software.

- Perfiles de misión adicionales: perfiles de misión para otros satélites de transmisión pública (Aqua, SNPP y Terra).
- Configuraciones adicionales de enlace descendente de antena: configuraciones de enlace descendente de antena para otros satélites de transmisión pública (Aqua, SNPP y Terra).

Los valores y parámetros de los satélites de esta plantilla ya se han rellenado. Estos parámetros facilitan su uso inmediato con estos satélites. AWS Ground Station 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 utiliza una aplicación de punto final del flujo de datos para recibir el flujo de datos desde el puerto definido por AWS Ground Station 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. AWS::GroundStation::DataflowEndpointGroup

Satélite de transmisión pública que utiliza AWS Ground Station Agent (banda ancha)

Este ejemplo se basa en el análisis realizado en la JPSS-1: Satélite de radiodifusión pública (PBS): evaluación sección de la guía del usuario.

Para completar este ejemplo, tendrá que asumir un escenario: desea capturar la ruta de comunicación del HRD como frecuencia intermedia digital de banda ancha (DigiF) y procesarla tal como la recibe el agente AWS Ground Station en una instancia de Amazon EC2 mediante un SDR.

> **Note**
>
> La señal de la ruta de comunicación JPSS HRD real tiene un ancho de banda de 30 MHz, pero configurará la configuración antena-enlace descendente para tratarla como una señal

con un MHz ancho de banda del 100, de modo que pueda fluir por la ruta correcta para que la reciba el AWS Ground Station agente en este ejemplo.

Rutas de comunicación

Esta sección representa Planifique las rutas de comunicación de su flujo de datos los primeros pasos. Para este ejemplo, necesitarás una sección adicional en la AWS CloudFormation plantilla que no se haya utilizado en los otros ejemplos, la sección de mapeos.

> **Note**
>
> Para obtener más información sobre el contenido de una AWS CloudFormation plantilla, consulta las secciones de plantillas.

Empezará por configurar una sección de mapeos en la AWS CloudFormation plantilla para las listas de AWS Ground Station prefijos por región. Esto permite que el grupo de seguridad de EC2 instancias de Amazon pueda hacer referencia fácilmente a las listas de prefijos. Para obtener más información sobre el uso de una lista de prefijos, consulte. Configuración de VPC con agente AWS Ground Station

```
Mappings:
  PrefixListId:
    us-east-2:
      groundstation: pl-087f83ba4f34e3bea
    us-west-2:
      groundstation: pl-0cc36273da754ebdc
    us-east-1:
      groundstation: pl-0e5696d987d033653
    eu-central-1:
      groundstation: pl-03743f81267c0a85e
    sa-east-1:
      groundstation: pl-098248765e9effc20
    ap-northeast-2:
      groundstation: pl-059b3e0b02af70e4d
    ap-southeast-1:
      groundstation: pl-0d9b804fe014a6a99
    ap-southeast-2:
```

```
      groundstation: pl-08d24302b8c4d2b73
    me-south-1:
      groundstation: pl-02781422c4c792145
    eu-west-1:
      groundstation: pl-03fa6b266557b0d4f
    eu-north-1:
      groundstation: pl-033e44023025215c0
    af-south-1:
      groundstation: pl-0382d923a9d555425
```

Para la sección Parámetros, va a añadir los siguientes parámetros. Especificará sus valores al crear la pila a través de la AWS CloudFormation consola.

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

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

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

> **Note**
>
> Debe crear un key pair y proporcionar el nombre del EC2 `EC2Key` parámetro Amazon. Consulta Crear un key pair para tu EC2 instancia de Amazon.

Además, tendrás que proporcionar el ID de AMI específico de la región correcto al crear la AWS CloudFormation pila. Consulte AWS Ground Station Imágenes de máquinas de Amazon (AMIs).

Los fragmentos de plantilla restantes pertenecen a la sección Recursos de la AWS CloudFormation plantilla.

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

Dado nuestro escenario de entregar una única ruta de comunicación a una EC2 instancia de Amazon, sabes que tendrás una única ruta de entrega sincrónica. Según la Entrega de datos sincrónica sección, debe configurar una EC2 instancia de Amazon con AWS Ground Station Agent y crear uno o más grupos de puntos de enlace de flujo de datos. En primer lugar, debe configurar la Amazon VPC para el AWS Ground Station agente.

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

  PublicSubnet:
    Type: AWS::EC2::Subnet
    Properties:
      VpcId: !Ref ReceiverVPC
      MapPublicIpOnLaunch: 'true'
      AvailabilityZone: !Ref AZ
      CidrBlock: 10.0.0.0/20
      Tags:
      - Key: "Name"
```

```
        Value: "AWS Ground Station Example - PBS to AWS Ground Station Agent Public
Subnet"
      - Key: "Description"
        Value: "Subnet for EC2 instance receiving AWS Ground Station data"

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

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

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

  InternetGateway:
    Type: AWS::EC2::InternetGateway
    Properties:
      Tags:
        - Key: Name
          Value: AWS Ground Station Example - Internet Gateway

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

> **Note**
>
> Para obtener más información sobre las configuraciones de VPC compatibles con el AWS Ground Station agente, consulte Requisitos del agente:AWS Ground Station diagramas de VPC.

A continuación, configurará la EC2 instancia de Amazon de Receiver.

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

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

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

 # Attach the ENI to the EC2 instance if using a separate public subnet.
 # Requires the receiver instance to be in a public subnet (SubnetId should be the id
of a public subnet)
 ReceiverNetworkInterfaceAttachment:
   Type: AWS::EC2::NetworkInterfaceAttachment
   Properties:
```

```
      DeleteOnTermination: false
      DeviceIndex: 1
      InstanceId: !Ref ReceiverInstance
      NetworkInterfaceId: !Ref ReceiverInstanceNetworkInterface

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

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

              AGENT_CONFIG_PATH="/opt/aws/groundstation/etc/aws-gs-agent-config.json"
              cat << AGENT_CONFIG > "$AGENT_CONFIG_PATH"
```

```
              {
                "capabilities": [
                  "arn:aws:groundstation:${AWS::Region}:${AWS::AccountId}:dataflow-
endpoint-group/${DataflowEndpointGroupId}"
                ],
                "device": {
                  "privateIps": [
                    "127.0.0.1"
                  ],
                  "publicIps": [
                    "${EIP}"
                  ],
                  "agentCpuCores": [

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

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

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

              # Set IRQ affinity with list of CPU cores and Receive Side Scaling mask
              # Core list should be the first two cores (and hyperthreads) on each
 socket
              # Mask set to everything currently
              # https://github.com/torvalds/linux/blob/v4.11/Documentation/networking/
scaling.txt#L80-L96
              echo "@reboot sudo /opt/aws/groundstation/bin/set_irq_affinity.sh '0 1 48
 49' 'ffffffff,ffffffff,ffffffff' >>/var/log/user-data.log 2>&1" >>/var/spool/cron/root

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

              # </Tuning Section End>
```

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

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

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

También necesitará las políticas, funciones y perfiles adecuados para poder crear AWS Ground Station la elastic network interface (ENI) en su cuenta.

```
 # The security group for your EC2 instance.
 InstanceSecurityGroup:
   Type: AWS::EC2::SecurityGroup
   Properties:
     GroupDescription: AWS Ground Station receiver instance security group.
     VpcId: !Ref ReceiverVPC
     SecurityGroupEgress:
```

```
        - CidrIp: 0.0.0.0/0
          Description: Allow all outbound traffic by default
          IpProtocol: "-1"
      SecurityGroupIngress:
        # To allow SSH access to the instance, add another rule allowing tcp port 22
from your CidrIp
        - IpProtocol: udp
          Description: Allow AWS Ground Station Incoming Dataflows
          ToPort: 50000
          FromPort: 42000
          SourcePrefixListId:
            Fn::FindInMap:
              - PrefixListId
              - Ref: AWS::Region
              - groundstation

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

```
          PolicyName: InstanceGroundStationApiAccessPolicy

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

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

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

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

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

AWS Ground Station configuraciones

Esta sección representa Crear configuraciones los primeros pasos.

Necesitarás una configuración de seguimiento para establecer tus preferencias de uso del autotrack. Si se selecciona PREFERRED como pista automática, se puede mejorar la calidad de la señal, pero no es obligatorio para cumplir con la calidad de la señal, ya que la calidad de las efemérides del JPSS-1 es suficiente.

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

En función de la ruta de comunicación, tendrá que definir una configuración de antena y enlace descendente que represente la parte del satélite, así como una configuración de punto final del flujo de datos que haga referencia al grupo de puntos finales del flujo de datos que define los detalles del punto final.

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

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

AWS Ground Station perfil de misión

Esta sección representa Crear perfil de misión cómo empezar.

Ahora que tiene las configuraciones asociadas, puede usarlas para construir el flujo de datos. Utilizará los valores predeterminados para el resto de los parámetros.

```
 # The AWS Ground Station Mission Profile that groups the above configurations to
define how to
```

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

Poniéndolo todo junto

Con los recursos anteriores, ahora puede programar los contactos del JPSS-1 para la entrega sincrónica de datos desde cualquiera de sus dispositivos integrados. AWS Ground Station AWS Ground Station Ubicaciones

La siguiente es una AWS CloudFormation plantilla completa que incluye todos los recursos descritos en esta sección combinados en una sola plantilla que se puede utilizar directamente. AWS CloudFormation

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 EC2 instancia de Amazon y los AWS CloudFormation recursos necesarios para recibir datos de transmisión directa de DigiF sin procesar mediante AWS Ground Station Agent.

Si Aqua, SNPP, JPSS-1/NOAA-20 y Terra no están integrados en su cuenta, consulte. Satélite a bordo

> **Note**
>
> Puede acceder a la plantilla accediendo al bucket de Amazon S3 del cliente con AWS credenciales válidas. Los enlaces que aparecen a continuación utilizan un bucket regional

de Amazon S3. Cambie el código de `us-west-2` región para que represente la región correspondiente en la que desea crear la AWS CloudFormation pila.
Además, en las siguientes instrucciones se utiliza YAML. Sin embargo, las plantillas están disponibles en formato YAML y JSON. Para usar JSON, reemplaza la extensión del `.yml` archivo por la extensión `.json` al descargar la plantilla.

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 adicionales define la plantilla?

La `DirectBroadcastSatelliteWbDigIfEc2DataDelivery` plantilla incluye los siguientes recursos adicionales:

- 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.
- (Opcional) Amazon EC2 Verification for Contacts: la opción de usar Lambda para configurar un sistema de verificación de las EC2 instancias de Amazon para los contactos con notificaciones de SNS. Es importante tener en cuenta que esto puede conllevar gastos en función del uso actual.
- Perfiles de misión adicionales: perfiles de misión para otros satélites de transmisión pública (Aqua, SNPP y Terra).
- Configuraciones adicionales de enlace descendente de antena: configuraciones de enlace descendente de antena para otros satélites de transmisión pública (Aqua, SNPP y Terra).

Los valores y parámetros de los satélites de esta plantilla ya se han rellenado. Estos parámetros facilitan su uso inmediato con estos satélites. AWS Ground Station 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. AWS::GroundStation::DataflowEndpointGroup Para obtener más información sobre el AWS Ground Station agente, consulte ¿Qué es el AWS Ground Station agente?

Solución de problemas

La siguiente documentación puede ayudarle a solucionar los problemas que puedan producirse durante el uso. AWS Ground Station

Temas

Solucionar problemas con los contactos que envían datos a Amazon EC2

Si no puedes completar un AWS Ground Station contacto correctamente, tendrás que comprobar que tu EC2 instancia de Amazon se está ejecutando, comprobar que la aplicación de punto final del flujo de datos se está ejecutando y comprobar que la transmisión de la aplicación de punto final del flujo de datos está configurada correctamente.

> **Note**
>
> DataDefender (DDX) es un ejemplo de una aplicación de punto final de flujo de datos compatible actualmente con AWS Ground Station

Requisito previo

En los siguientes procedimientos se presupone que una EC2 instancia de Amazon ya está configurada. Para configurar una EC2 instancia de Amazon en AWS Ground Station, consulta Cómo empezar.

Paso 1: Comprueba que la EC2 instancia se esté ejecutando

El siguiente procedimiento muestra cómo encontrar tu EC2 instancia de Amazon en la consola e iniciarla si no se está ejecutando.

1. Busca la EC2 instancia de Amazon que se usó para el contacto que estás solucionando. Utilice los siguientes pasos:

   a. En tu AWS CloudFormationpanel de control, selecciona la pila que contiene tu EC2 instancia de Amazon.

   b. Selecciona la pestaña Resources y localiza tu EC2 instancia de Amazon en la columna Logical ID. Asegúrese de que la instancia se ha creado en la columna Status (Estado).

   c. En la columna ID física, elige el enlace de tu EC2 instancia de Amazon. Esto lo llevará a la consola de EC2 administración de Amazon.

2. En la consola EC2 de administración de Amazon, asegúrese de que el estado de su EC2 instancia de Amazon esté en ejecución.
3. Si la instancia se está ejecutando, continúe en el paso siguiente. Si la instancia no está en ejecución, iníciela siguiendo este paso.

   - Con tu EC2 instancia de Amazon seleccionada, selecciona Acciones > Estado de la instancia > Iniciar.

Paso 2: Determine 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 Agente de solución de problemas AWS Ground Station. De lo contrario, si está utilizando la aplicación DataDefender (DDX), continúe the section called “Paso 3: Compruebe que la aplicación de flujo de datos se esté ejecutando” utilizándola.

Paso 3: Compruebe que la aplicación de flujo de datos se esté ejecutando

La verificación del estado de DataDefender requiere que te conectes a tu instancia en Amazon EC2. Para obtener más información sobre la conexión a tu instancia, consulta Conéctate a tu instancia de Linux.

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

1. Abre un terminal o una línea de comandos y conéctate a tu EC2 instancia de Amazon mediante SSH. Reenvía el puerto 80 del host remoto para ver la interfaz de usuario DataDefender web. Los siguientes comandos muestran cómo usar SSH para conectarse a una EC2 instancia de Amazon a través de un bastión con el reenvío de puertos habilitado.

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

   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. Verifica que DataDefender (también denominado DDX) se esté ejecutando suprimiendo (comprobando) un proceso en ejecución denominado ddx en el resultado. 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 DataDefender se está ejecutando, vaya a Si no es the section called “Paso 4: Compruebe que el flujo de aplicaciones de flujo de datos esté configurado” así, continúe con el paso siguiente.

3. Comience a DataDefender usar el comando que se muestra a continuación.

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

Si DataDefender se está ejecutando después de usar el comando, vaya a the section called “Paso 4: Compruebe que el flujo de aplicaciones de flujo de datos esté configurado” En caso contrario, continúe con el paso siguiente.

4. Inspeccione los siguientes archivos mediante los siguientes comandos para comprobar si hubo algún error durante la instalación y la configuración DataDefender.

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

> **Note**
>
> Un problema habitual que se descubre al inspeccionar estos archivos es que la VPC de Amazon en la que se ejecuta la instancia de EC2 Amazon no tiene acceso a Amazon S3 para descargar los archivos de instalación. Si descubres en tus registros que este es el problema, comprueba la configuración de Amazon VPC y del grupo de seguridad de tu EC2 instancia para asegurarte de que no bloqueen el acceso a Amazon S3.

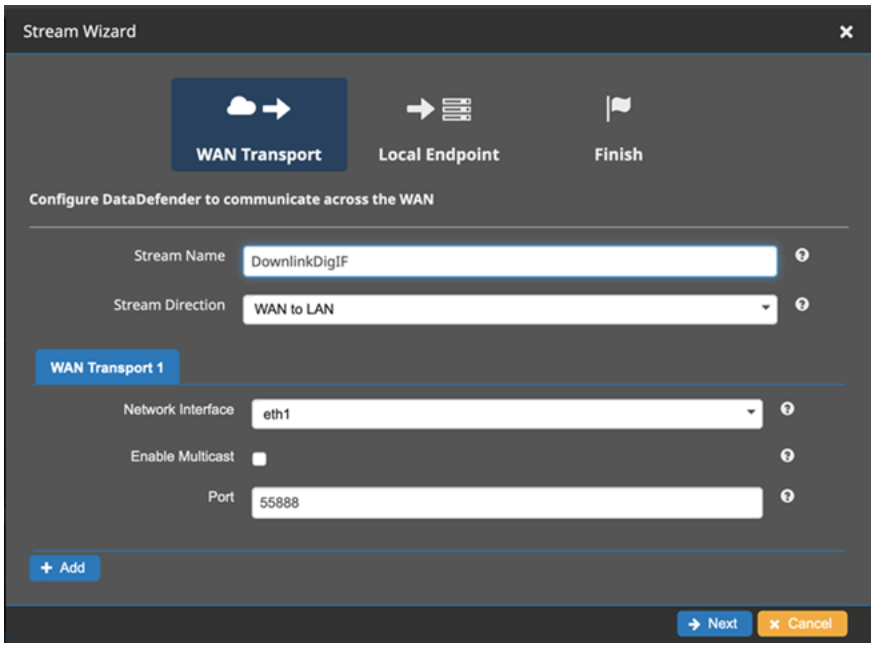
Si DataDefender se está ejecutando después de comprobar la configuración de Amazon VPC, continúe. the section called “Paso 4: Compruebe que el flujo de aplicaciones de flujo de datos esté configurado” Si el problema persiste, póngase en contacto con AWS Support y envíe los archivos de registro con una descripción del problema.

Paso 4: Compruebe que el flujo de aplicaciones de flujo de datos esté configurado

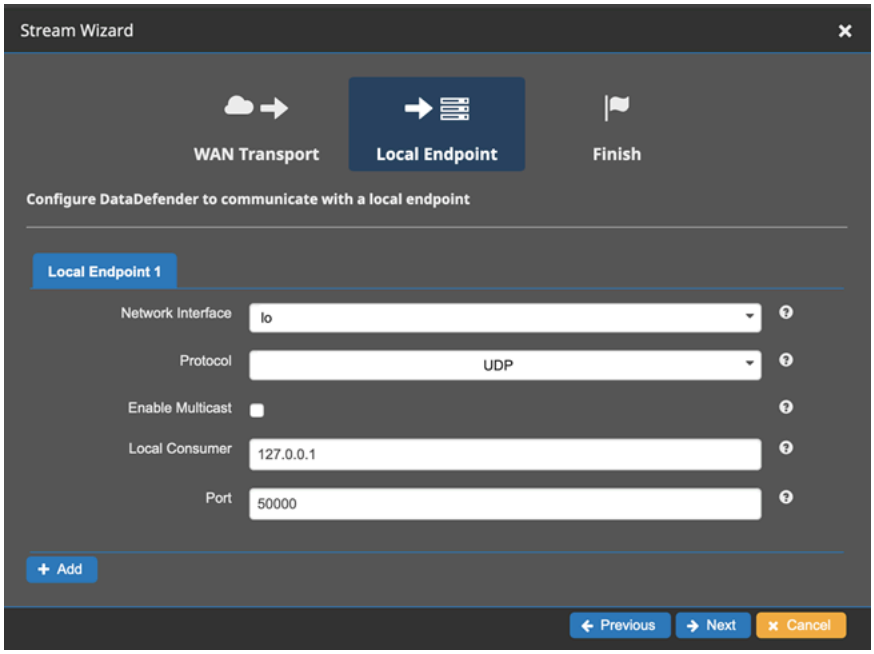
1. En un navegador web, acceda a la interfaz de usuario DataDefender web introduciendo la siguiente dirección en la barra de direcciones: localhost:8080. A continuación, pulse Intro.
2. En el DataDefenderpanel de control, selecciona Ir a detalles.
3. Seleccione una secuencia en la lista de secuencias 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 recibirás tus datos una vez que los hayas DataDefender 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 te has asegurado de que tanto tu EC2 instancia de Amazon como tu instancia DataDefender están ejecutándose y configuradas correctamente para recibir datos AWS Ground Station. Siga en the section called “Paso 5: Asegúrese de tener suficientes direcciones IP disponibles en la subred de las instancias receptoras”.

Paso 5: Asegúrese de tener suficientes direcciones IP disponibles en la subred de las instancias receptoras

El siguiente procedimiento muestra cómo encontrar el número de direcciones IP disponibles en una instancia de Amazon EC2 Receiver en la consola.

1. Estás solucionando el problema de cada instancia de Amazon EC2 Receiver que se utilizó para el contacto. Utilice los siguientes pasos:

   a. En tu AWS CloudFormationpanel de control, selecciona la pila que contiene tu EC2 instancia de Amazon.

   b. Selecciona la pestaña Resources y localiza tu EC2 instancia de Amazon en la columna Logical ID. Asegúrese de que la instancia se ha creado en la columna Status (Estado).

c. En la columna ID física, elige el enlace de tu EC2 instancia de Amazon. Esto lo llevará a la consola de EC2 administración de Amazon.

2. En la consola EC2 de administración de Amazon, busca y haz clic en el enlace del ID de subred en el resumen de instancias de tu instancia de Amazon EC2 Receiver. Esto lo llevará a la consola de administración de Amazon VPC correspondiente.
3. Seleccione la subred correspondiente en la consola de administración de Amazon VPC y compruebe las direcciones disponibles en los detalles de la subred. IPv4 Si este número no es igual al de los puntos de enlace del flujo de datos que utilizan esta instancia de Amazon EC2 Receiver, haga lo siguiente:

   a. Actualiza la subred correspondiente de tu AWS CloudFormation plantilla CidrBlockpara que tenga el tamaño correcto. Para obtener más información sobre el tamaño de las subredes, consulte Bloques CIDR de subred.

   b. Vuelva a implementar su pila con la plantilla actualizada. AWS CloudFormation

Si sigue teniendo problemas, póngase en contacto con AWS Support.

Solucionar problemas de contactos fallidos

Un contacto tendrá el estado de contacto de terminal FALLIDO cuando AWS Ground Station detecte un problema con la configuración de sus recursos. 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 es específica para el estado de contacto con error y no para otros estados de error, como AWS_FAILED, o AWS_CANCELLEDFAILED_TO_SCHEDULE. Para obtener más información sobre los estados del contacto, consulte the section called “AWS Ground Station estados de contacto”

Casos de uso fallidos del punto final de Dataflow

La siguiente es la lista de casos de uso comunes que pueden provocar un estado de contacto FALLIDO para los flujos de datos basados en puntos finales de flujo de datos:

- El punto final del flujo de datos nunca se conecta: nunca se estableció la conexión entre AWS Ground Station Antenna y su grupo de puntos finales de Dataflow para uno o más flujos de datos.
- El punto final de Dataflow se conecta tarde: la conexión entre AWS Ground Station Antenna y su grupo de puntos finales de Dataflow para uno o más flujos de datos se estableció después de la hora de inicio del contacto.
- La subred del punto final de Dataflow no tiene direcciones IP disponibles; la solución de entrega AWS Ground Station de datos no puede crear un ENI en su red privada porque no tiene ninguna dirección IP disponible en la subred de la instancia receptora.

Para cualquier caso de fallo en el punto final del flujo de datos, se recomienda tener en cuenta lo siguiente:

- Confirma que la EC2 instancia de Amazon receptora se haya iniciado correctamente antes de la hora de inicio del contacto.
- Confirme que el software de punto final del flujo de datos estaba funcionando durante el contacto.
- Asegúrese de tener al menos una dirección IP disponible por punto final del flujo de datos por subred de la instancia receptora.

Consulte la sección en Solucionar problemas con los 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:

- AWS Ground Station Estado del agente que nunca informó: el agente responsable de organizar la entrega de datos en su grupo de puntos finales de Dataflow para uno o más flujos de datos a los 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.
- AWS Ground Station El agente comenzó tarde: el agente responsable de organizar la entrega de datos en su grupo de endpoints de Dataflow para uno o más flujos de datos comenzó tarde, después de la hora de inicio del contacto.

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

- Confirma que la EC2 instancia de Amazon 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.
- Confirma que la aplicación Agent y la EC2 instancia de Amazon 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 Solucionar problemas con los contactos que envían datos a Amazon EC2 para ver los pasos de solución de problemas más específicos.

Solucionar problemas de contactos de FAILED_TO_SCHEDULE

Un contacto terminará en el estado FAILED_TO_SCHEDULE cuando AWS Ground Station detecte un problema en la configuración de los recursos 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, consulta la API. DescribeContact

A continuación, se indican los casos de uso más comunes que pueden provocar la aparición de errores en los contactos, junto con los pasos que pueden ayudar a solucionar los problemas.

> **Note**
>
> Esta guía es específica para el estado de contacto FAILED_TO_SCHEDULE y no está destinada a otros estados de error, como, o FALLIDO. AWS_FAILEDAWS_CANCELLED Para obtener más información sobre los estados del contacto, consulte the section called "AWS Ground Station estados de contacto"

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. Para obtener información sobre cómo reservar un contacto, consulte ReserveContact.
- Si sigue recibiendo el estado FAILED_TO_SCHEDULE para este perfil de misión, póngase en contacto con AWS Support

Solucione el problema DataflowEndpointGroups si no se encuentra en un estado SALUDABLE

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 su EC2 instancia, que registrará al agente. enga en cuenta que debe tener un archivo de configuración del controlador válido para que esta llamada se realice correctamente. Consulte la Usa AWS Ground Station un agente para obtener más información sobre la configuración de ese archivo.
- `INVALID_IP_OWNERSHIP`- Utilice la DeleteDataflowEndpointGroup API para eliminar el grupo de puntos finales de Dataflow y, a continuación, utilice la CreateDataflowEndpointGroup API para volver a crear el grupo de puntos finales de Dataflow con las direcciones IP y los puertos asociados a la instancia. 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 Utilice funciones vinculadas a servicios para Ground Station

Solucionar problemas de efemérides no válidas

Cuando se carga una efeméride personalizada, pasa por un flujo de trabajo de validación asíncrona AWS Ground Station antes de convertirse en efemérides. `ENABLED` Este flujo de trabajo garantiza que los identificadores del satélite, los metadatos y la trayectoria son válidos.

Cuando una efeméride no pasa la validación, `DescribeEphemeris` devolverá un EphemerisInvalidReason, que proporciona información sobre por qué la efeméride no se validó. Los valores potenciales de son los EphemerisInvalidReasonsiguientes:

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

Valor	Descripción	Acción para la solución de problemas
		y corresponde al satélite correcto.
VALIDATION_ERROR	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"
      }
    }
  },
}
```

> **Note**
>
> Si el estado de una efeméride es`ERROR`, la efeméride no se `ENABLED` debe a un problema con el servicio. AWS Ground Station Deberías intentar volver a proporcionar las efemérides a través de. `CreateEphemeris` Las nuevas efemérides podrían convertirse `ENABLED` si el problema fuera transitorio.

> **Note**
>
> AWS Ground Station trata las efemérides como datos de uso individualizados. Si utiliza esta función opcional, AWS utilizará sus datos de efemérides para proporcionar asistencia en la solución de problemas.

Solucionar problemas de contactos que no recibieron datos

Es posible que un contacto parezca correcto, pero aun así no haya recibido ningún dato. Esto puede significar que recibe archivos PCAP vacíos o que no recibe ningún archivo PCAP si utiliza la entrega de datos de S3. Esto puede suceder por varias razones. A continuación, se analizan algunas de las causas y cómo abordarlas.

Configuración de enlace descendente incorrecta

Cada contacto que reciba datos de un satélite tendrá un Configuración de enlace de bajada de antena o Configuración de descodificación y desmodulación de enlace de bajada de antena asociado. Si la configuración especificada no está de acuerdo con la señal que transmite un satélite, no AWS Ground Station podrá recibir la señal transmitida. Esto provocará que no reciba ningún dato AWS Ground Station.

Para solucionar este problema, compruebe que las configuraciones que está utilizando coinciden con la señal que transmite su satélite. Por ejemplo, compruebe que ha establecido la frecuencia central, el ancho de banda, la polarización y, si es necesario, los parámetros de demodulación y decodificación correctos.

Maniobra de satélite

Hay ocasiones en las que un satélite puede realizar una maniobra que desactiva temporalmente algunos de sus sistemas de comunicación. La maniobra también puede cambiar significativamente la ubicación del satélite en el cielo. AWS Ground Station no podrá recibir una señal de un satélite que no esté transmitiendo ninguna señal, o si las efemérides utilizadas hacen que la AWS Ground Station antena apunte a un lugar del cielo en el que el satélite no esté presente.

Si está intentando comunicarse con un satélite de transmisión pública operado por la NOAA, es posible que encuentre un mensaje que describa una interrupción o una maniobra en la página de mensajes de alerta por satélite de la NOAA. El mensaje puede incluir una cronología de cuándo se espera que se reanude la transmisión de datos o puede publicarse en un mensaje posterior.

Si te estás comunicando con tus propios satélites, es tu responsabilidad entender las operaciones de los satélites y cómo esto puede afectar a la comunicación con ellos AWS Ground Station. Si vas a realizar una maniobra que afectará a la trayectoria del satélite, esto puede incluir proporcionar datos de efemérides personalizados y actualizados. Para obtener más información sobre cómo proporcionar datos de efemérides personalizados, consulte. Proporcionar datos de efemérides personalizados

AWS Ground Station interrupción

Si AWS Ground Station provoca un error en un contacto o lo cancela, AWS Ground Station configurará el estado del contacto en AWS_FAILED, o. AWS_CANCELLED Para obtener más información sobre el ciclo de vida de los contactos, consulteComprenda el ciclo de vida de. En algunos casos, es AWS Ground Station posible que se produzca un error que impida que los datos se envíen a tu cuenta, pero que no provoque que el contacto esté en AWS_CANCELLEDestado AWS_FAILEDo. Cuando esto suceda, AWS Ground Station debes publicar un evento específico de la cuenta en tu panel de AWS Salud. Para obtener más información sobre el panel de AWS Salud, consulte AWS la Guía del usuario de Salud.

Cuotas y límites

Puede ver las regiones compatibles, sus puntos de enlace asociados y las cuotas en los puntos de enlace y en las cuotas AWS Ground Station .

Puede utilizar la consola de Service Quotas, la API de AWS y la CLI de AWS para solicitar aumentos de cuotas cuando sea necesario.

Términos del servicio

Para conocer las condiciones del AWS Ground Station servicio, consulte las condiciones del servicio de AWS.

Historial de documentos de la Guía AWS Ground Station del usuario

En la siguiente tabla se describen los cambios importantes de cada versión de la Guía del AWS Ground Station usuario.

Cambio	Descripción	Fecha
Actualización de la documentación	Se agregó una aclaración sobre la utilización por parte de los contactos de los recursos configurados.	4 de abril de 2025
Nueva característica	Se actualizó la guía del usuario para incluir el gemelo AWS Ground Station digital.	6 de agosto de 2024
Actualización de la documentación	Se actualizaron muchas secciones de la guía del usuario, incluidos nuevos diagramas, ejemplos y mucho más.	18 de julio de 2024
Actualización de la documentación	Se agregó una fuente RSS a la Guía del usuario.	18 de julio de 2024
Actualización de la documentación	Divida la Guía del usuario del AWS Ground Station agente en una guía de usuario independiente.	18 de julio de 2024
Nueva característica	Los contactos ahora se pueden programar hasta 30 segundos fuera de los intervalos de tiempo de visibilidad. Los tiempos de visibilidad se incluyen en	26 de marzo de 2024

	DescribeContact las respuestas.	
Actualización de la documentación	Se mejoró la organización y se agregó la sección «Selección de EC2 instancias y planificación de la CPU».	6 de marzo de 2024
Actualización de la documentación	Se han añadido 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 la 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 la documentación	Se agregó la referencia a AWS Notificaciones de usuario en la documentación de monitoreo.	6 de agosto de 2023
Actualización de la documentación	Se agregaron instrucciones para etiquetar satélites con un nombre que se muestre en la AWS Ground Station consola.	26 de julio de 2023

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
Nueva política gestionada AWS	AWS Ground Station se agregó una nueva política denominada AWSGround StationAgentInstancePolicy.	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
Nueva política AWS gestionada	AWS Ground Station se agregó la AWSService RoleForGroundStationDataflowEndpointGroup 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 han añadido satélites de radiodifusión 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 la documentación	Ejemplos y descripciones actualizados para la supervisión AWS Ground Station con CloudWatch eventos.	4 de febrero de 2020
Actualización de la 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 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

AWS Glosario

Para obtener la AWS terminología más reciente, consulte el AWS glosario de la Glosario de AWS Referencia.

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.