



Guía del usuario de

AWS Ground Station



AWS Ground Station: Guía del usuario de

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

¿Qué es AWS Ground Station?	1
Casos de uso comunes	1
Pasos a seguir a continuación	2
Cómo AWS Ground Station funciona	3
Incorporación de satélites	3
Composición del perfil de la misión	3
Programación de contactos	5
Ejecución de contactos	6
Gemelo digital	9
Comprenda los componentes AWS Ground Station principales	9
Perfiles de misión	11
Configuraciones	14
Grupos de puntos finales de Dataflow	24
AWS Ground Station ¿Agente	32
Introducción	34
Inscríbese en un Cuenta de AWS	34
Creación de un usuario con acceso administrativo	34
Añada AWS Ground Station permisos a su cuenta AWS	36
Satélite a bordo	38
Descripción general del proceso de incorporación de clientes	38
(Opcional) Asignar nombres a los satélites	39
Satélites de radiodifusión pública	41
Planifique las rutas de comunicación de su flujo de datos	42
Entrega de datos asíncrona	42
Entrega de datos sincrónica	43
Planifique su telemetría	44
Crear configuraciones	45
Configuraciones de entrega de datos	45
Configuración de telemetría (opcional)	46
Configuraciones de satélite	46
Crear perfil de misión	46
Comprenda los próximos pasos	47
AWS Ground Station Ubicaciones	49
Búsqueda de la región de AWS para la ubicación de una estación terrestre	49

AWS Ground Station regiones de AWS compatibles	51
Disponibilidad de gemelos digitales	51
AWS Ground Station máscaras de sitio	51
Máscaras específicas para cada cliente	52
Impacto de las máscaras de sitio en los tiempos de contacto disponibles	52
AWS Ground Station Capacidades del sitio	53
Comprenda cómo AWS Ground Station usa las efemérides	57
Datos de efemérides predeterminados	58
Proporcione datos de efemérides personalizados	58
Descripción general de	58
Ejemplo: usar efemérides proporcionadas por el cliente con AWS Ground Station	59
Proporcione datos de efemérides de TLE	59
Proporcione datos de efemérides OEM	66
Proporcione datos de efemérides de elevación del acimut	74
Reserva contactos con efemérides personalizadas	86
Descripción general de	86
Flujos de trabajo para reservar contactos	86
Flujo de trabajo 1: Listar los contactos disponibles y luego reservar	87
Flujo de trabajo 2: reserva por contacto directo	91
Supervisión de los cambios de estado de los contactos	94
Prácticas recomendadas y consideraciones	97
Comprenda qué efemérides se utilizan	98
Efemérides TLE y OEM	98
Efemérides de elevación azimutal	99
Efecto de las nuevas efemérides en los contactos previamente programados	99
Obtén las efemérides actuales de un satélite	100
Ejemplo de retorno GetSatellite para un satélite que utiliza una efeméride predeterminada .	101
Ejemplo GetSatellite para un satélite que utiliza una efeméride predeterminada	101
Listado de efemérides de elevación azimutal	102
Vuelva a los datos de efemérides predeterminados	103
Reversión de efemérides TLE y OEM	103
Gestión de efemérides de elevación azimutal	103
Trabaje con flujos de datos	105
AWS Ground Station interfaces del plano de datos	105
Uso de la entrega de datos entre regiones	106
Instalación y configuración de Amazon S3	106

Instalación y configuración de Amazon VPC	106
Configuración de VPC con agente AWS Ground Station	108
Configuración de VPC con un punto final de flujo de datos	111
Configurar y configurar Amazon EC2	113
Software común suministrado	114
AWS Ground Station Imágenes de máquinas de Amazon (AMIs)	114
Trabaje con telemetría	115
Cómo funciona la telemetría	115
Tipos de telemetría disponibles	115
Disponibilidad regional	116
Configure la telemetría	116
Paso 1: Cree los recursos necesarios AWS	117
Paso 2: Crear un TelemetrySinkConfig	119
Paso 3: Añade la telemetría al perfil de tu misión	119
Paso 4: programar un contacto	119
Sigüientes pasos	120
Comprenda los datos de telemetría	120
Descripción general del formato de datos	120
Telemetría de puntería	121
Telemetría de seguimiento	123
Lectura de datos de la transmisión de Kinesis Data Streams	125
Evolución y control de versiones del esquema	126
Trabaja con contactos	127
Comprenda el ciclo de vida de	127
AWS Ground Station estados de contacto	130
Retención de datos de contacto	131
Comprenda la facturación por contacto	132
Definición de ancho de banda	132
Modos de programación	132
CancelContact	133
Escenario 1: contacto único	133
Escenario 2: contacto con una sola parada	134
Escenario 3: Duplicado único	134
Escenario 4: Duplicado corto	135
Escenario 5: Varios duplicados	136
Escenario 6: paradas múltiples	138

Escenario 7: estación terrestre con varias antenas sin duplicados	139
Escenario 8: estación terrestre con varias antenas con contactos duplicados	140
AWS Ground Station gemelo digital	142
Monitorización	143
Automatica con eventos	144
AWS Ground Station Tipos de eventos	145
Cronología del evento de contacto	145
Eventos de efemérides	148
Registra las llamadas a la API con CloudTrail	149
AWS Ground Station Información en CloudTrail	149
Descripción de las entradas de los archivos de AWS Ground Station registro	150
Consulta las métricas con Amazon CloudWatch	152
AWS Ground Station Métricas y dimensiones	152
Visualización de métricas	159
Seguridad	166
Gestión de identidad y acceso	166
Público	167
Autenticación con identidades	167
Administración del acceso con políticas	168
¿Cómo AWS Ground Station funciona con IAM	170
Ejemplos de políticas basadas en identidades	176
Resolución de problemas	179
AWS políticas gestionadas	181
AWSGroundStationAgentInstancePolicy	181
AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy	182
Actualizaciones de políticas	183
Uso de roles vinculados a servicios	184
Permisos de roles vinculados al servicio para la estación terrestre	184
Creación de un rol vinculado al servicio para Ground Station	185
Edición de un rol vinculado al servicio para Ground Station	185
Eliminación de un rol vinculado al servicio para Ground Station	186
Regiones compatibles con las funciones vinculadas al servicio de Ground Station	186
Resolución de problemas	187
Cifrado de datos en reposo para AWS Ground Station	187
Creación de una clave administrada por el cliente	189
Especificar una clave gestionada por el cliente para AWS Ground Station	190

AWS Ground Station contexto de cifrado	190
Cifrado en reposo para datos de efemérides TLE y OEM	190
Cifrado en reposo para efemérides de elevación de acimut	200
Cifrado de datos durante el tránsito para AWS Ground Station	209
AWS Ground Station Flujos de agentes	209
Flujos de puntos finales de flujo de datos	209
Ejemplos de configuraciones de perfil de misión	210
JPSS-1: Satélite de radiodifusión pública (PBS): evaluación	210
Satélite de transmisión pública que utiliza la entrega de datos de Amazon S3	211
Vías de comunicación	212
AWS Ground Station configuraciones	214
AWS Ground Station perfil de misión	215
Poniéndolo todo junto	216
Satélite de transmisión pública que utiliza un punto final de flujo de datos (banda estrecha)	217
Rutas de comunicación	217
AWS Ground Station configuraciones	224
AWS Ground Station perfil de la misión	225
Poniéndolo todo junto	226
Satélite de transmisión pública que utiliza un punto final de flujo de datos (demodulado y decodificado)	228
Vías de comunicación	228
AWS Ground Station configuraciones	235
AWS Ground Station perfil de la misión	238
Poniéndolo todo junto	239
Satélite de transmisión pública que utiliza AWS Ground Station Agent (banda ancha)	241
Rutas de comunicación	242
AWS Ground Station configuraciones	253
AWS Ground Station perfil de misión	254
Poniéndolo todo junto	255
Resolución de problemas	258
Solucionar problemas con los contactos que envían datos a Amazon EC2	258
Paso 1: Compruebe que la instancia EC2 se esté ejecutando	259
Paso 2: Determine el tipo de aplicación de flujo de datos utilizada	259
Paso 3: Compruebe que la aplicación de flujo de datos se esté ejecutando	259
Paso 4: Compruebe que el flujo de aplicaciones de flujo de datos esté configurado	261

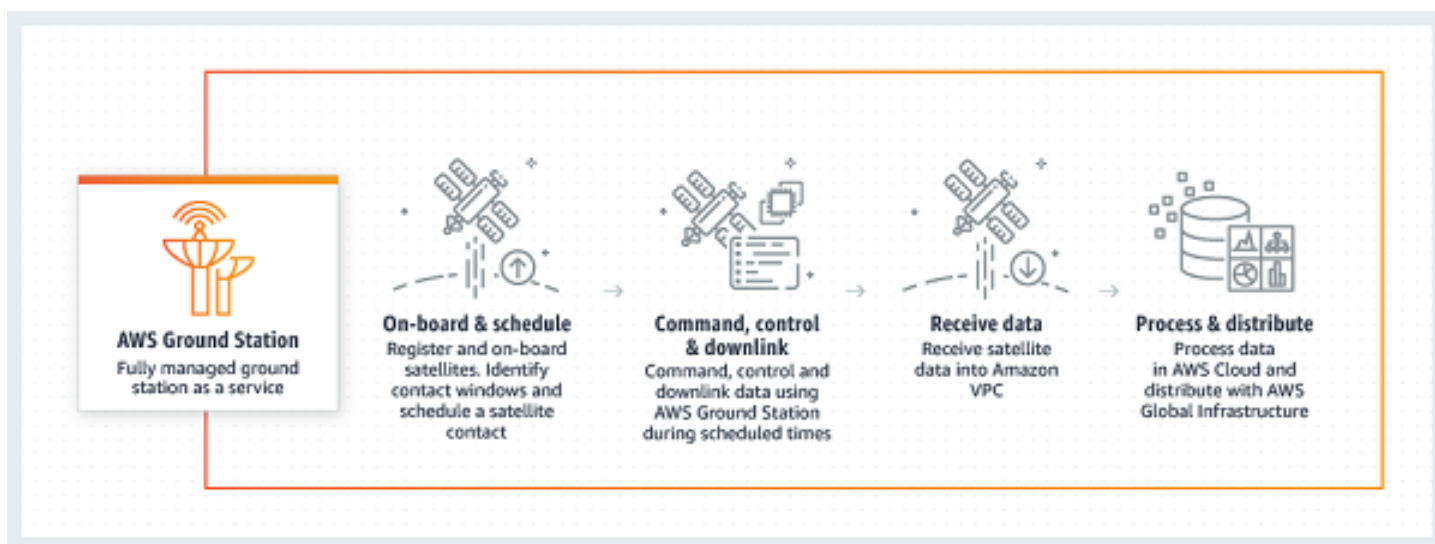
Paso 5: Asegúrese de tener suficientes direcciones IP disponibles en la subred de las instancias receptoras	263
Solucionar problemas de contactos fallidos	264
Casos de uso fallidos del punto final de Dataflow	264
AWS Ground Station Casos de uso fallidos del agente	265
Solucionar problemas de contactos de FAILED_TO_SCHEDULE	266
No se admiten los ajustes especificados en su Antenna Downlink Demod Decode Config. ..	267
Soluciones de problemas generales	267
Solucione el problema DataflowEndpointGroups si no se encuentra en un estado SALUDABLE	267
Solucionar problemas de efemérides no válidas	268
Descripción de los errores de validación de efemérides	268
Errores de validación comunes para las efemérides TLE	269
Errores de validación comunes en las efemérides OEM	269
Errores de validación comunes para las efemérides de elevación azimutal	270
Pasos para la solución de problemas	271
Referencia completa del código de error	272
Solucionar problemas de contactos que no recibieron datos	276
Configuración de enlace descendente incorrecta	276
Maniobra de satélite	277
AWS Ground Station interrupción	277
Solucionar problemas de telemetría	278
Problemas comunes de configuración	278
Problemas con la entrega de telemetría	280
Problemas de formato de datos	282
Obtener ayuda	283
Cuotas y límites	284
Términos del servicio	285
Historial de documentos	286
AWS Glosario	292
.....	ccxciii

¿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, consulte [Cómo AWS Ground Station funciona](#).
- Para obtener información sobre cómo configurar su cuenta y los recursos que puede utilizar AWS Ground Station, consulte [Introducción](#).
- 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 a través del [AWS Support Center Consoles](#) si su caso de uso requiere capacidades adicionales, ofertas de ubicación adicionales o ubicaciones de antena 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

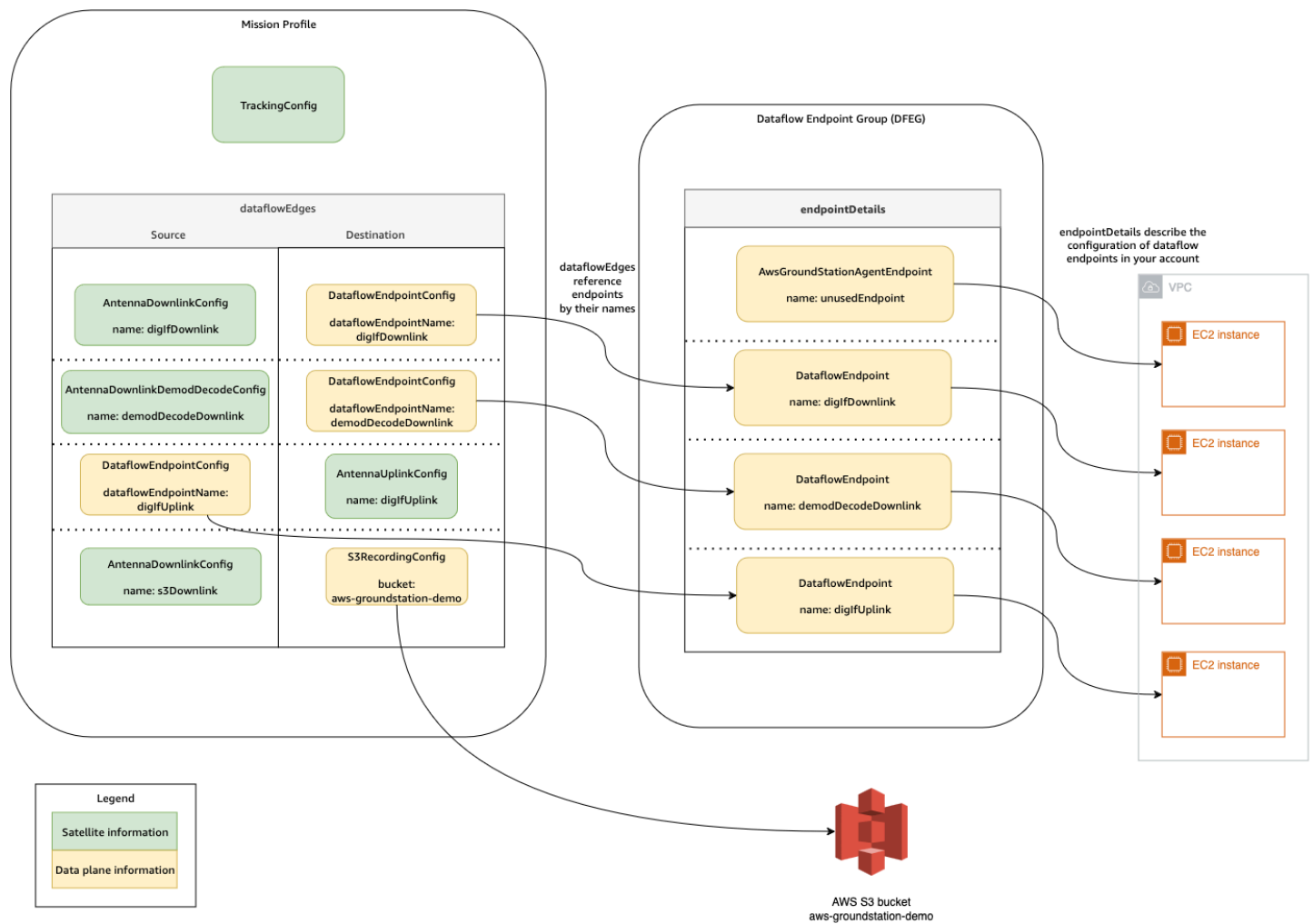
individuales, sino que solo contienen información sobre sus capacidades técnicas, varios satélites que tengan la misma configuración también pueden reutilizar los perfiles de misión.

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, consulte [Usa perfiles AWS Ground Station de misión](#).
- Para ver ejemplos sobre cómo se pueden crear varios perfiles de misión para respaldar su caso de uso, consulte [Ejemplos 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:

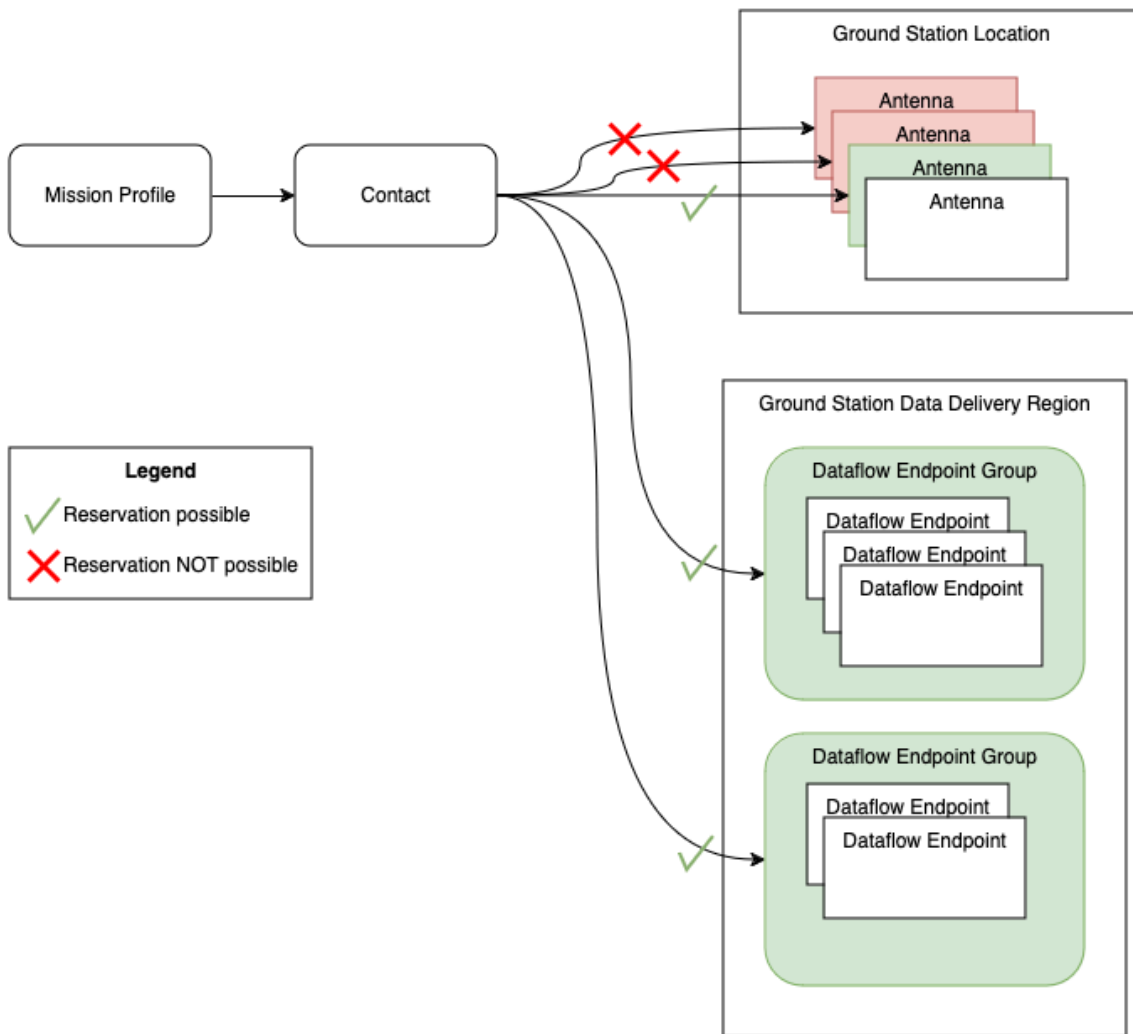
- Enlace descendente sincrónico de datos digitales de frecuencias intermedias a una EC2 instancia de Amazon que gestione. Denotado por el nombre. diglfDownlink
- Enlace descendente asíncrono de datos digitales de frecuencias intermedias a un bucket de Amazon S3. Se indica mediante el nombre del bucket. 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. diglfUplink



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 [Automatiza 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 a fin de reducir los costos. Consulte [Automatiza AWS Ground Station con eventos](#) para obtener más detalles.

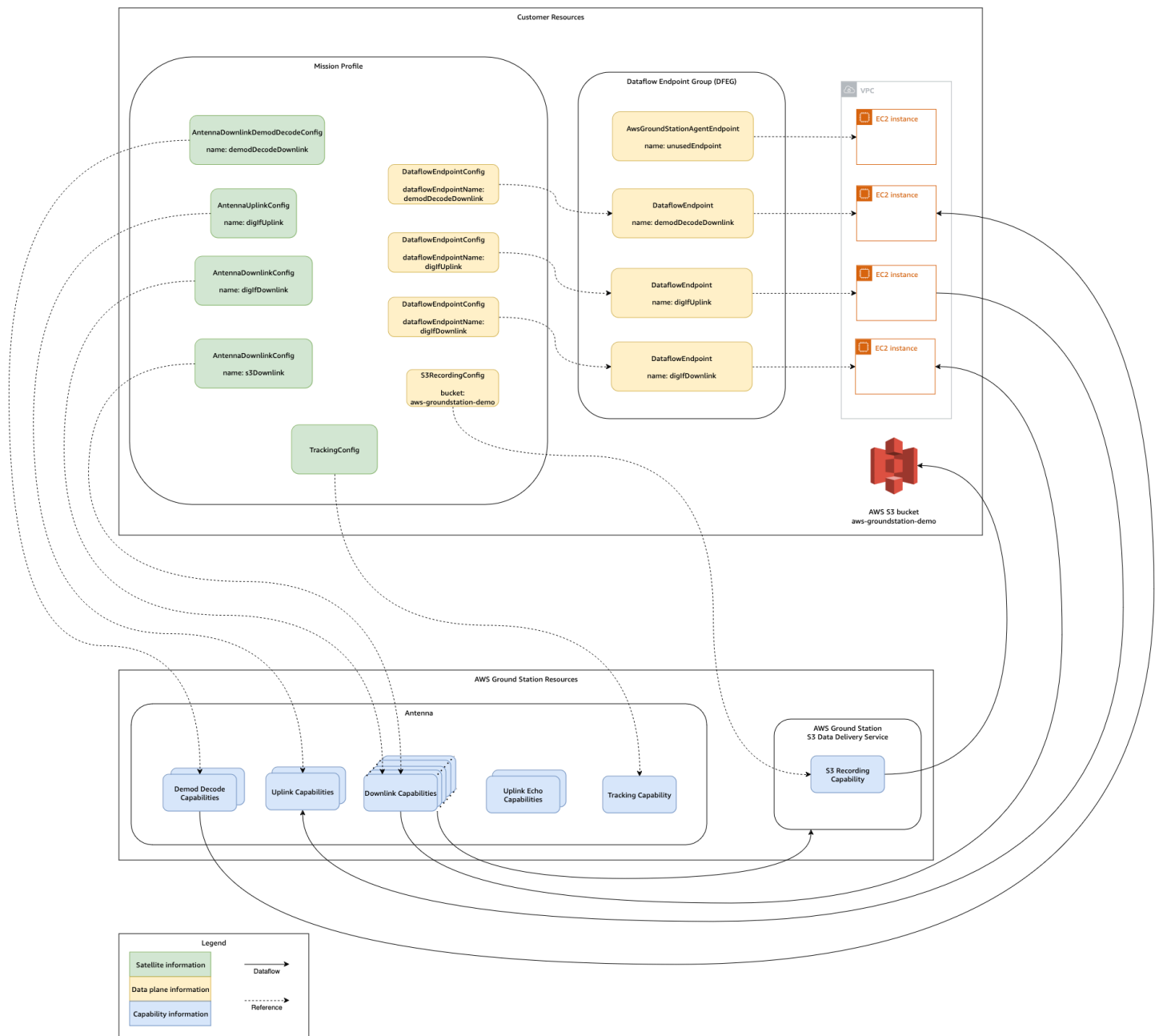
Durante el contacto, la telemetría sobre el rendimiento del contacto se envía a AWS. CloudWatch Para obtener información sobre cómo monitorear su contacto durante la ejecución, consulte.

[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_FAILED` estado. 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, consulte [Comprenda el ciclo de vida de](#).

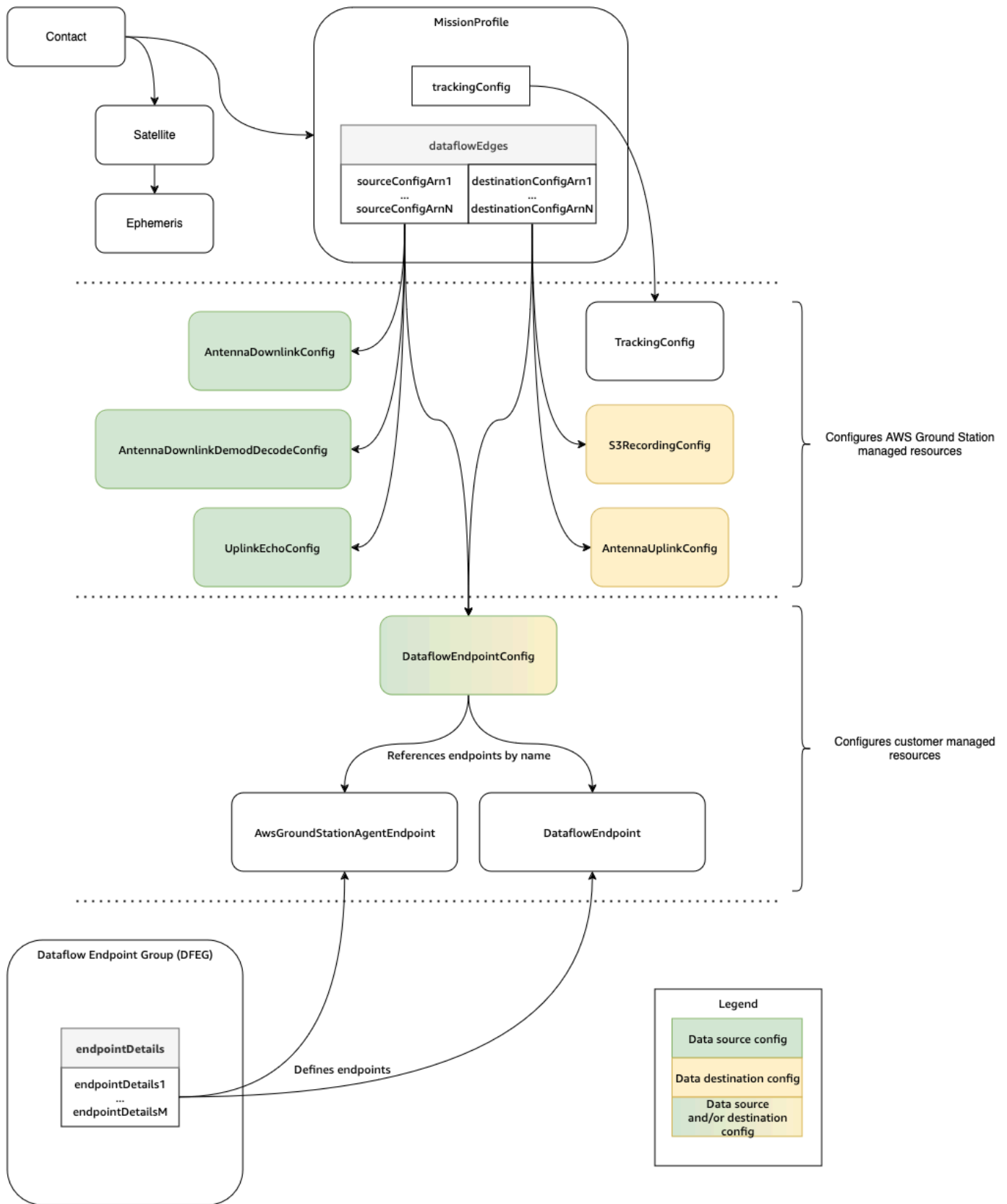
Gemelo digital

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.



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

Temas

- [Usa perfiles AWS Ground Station de misión](#)
- [Usa AWS Ground Station configuraciones](#)
- [Utilice grupos de AWS Ground Station puntos finales de Dataflow](#)
- [Usa AWS Ground Station un agente](#)

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](#).

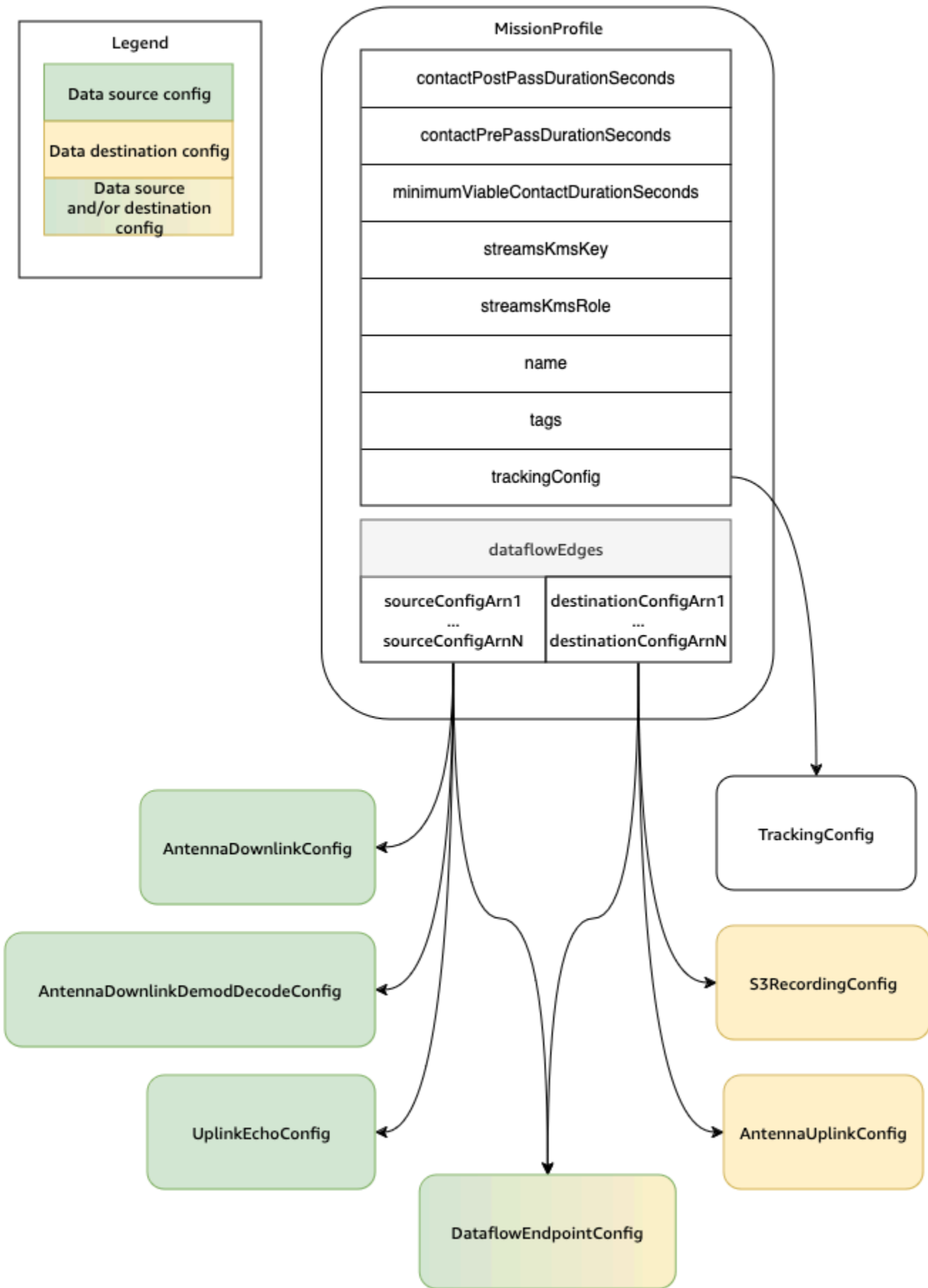
Las `contactPrePassDurationSeconds` y `contactPostPassDurationSeconds` permiten especificar las horas en relación con el contacto en el que recibirás una CloudWatch notificación de

evento. Para obtener una cronología de los eventos relacionados con su contacto, lea [Comprenda 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](#).

El telemetrySinkConfigArn campo es opcional y permite activar la AWS Ground Station telemetría durante los contactos. Cuando se especifica, AWS Ground Station transmite datos de telemetría prácticamente en tiempo real a tu cuenta durante la ejecución de tus contactos. Para obtener más información sobre la configuración y el uso de la telemetría, consulte. [Trabaje con telemetría](#)



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 tres categorías:

- Configuraciones de seguimiento
- Configuraciones de flujo de datos
- Configuraciones de telemetría

A TrackingConfig es 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 and/or destino

A TelemetrySinkConfig es el único tipo de configuración de telemetría. Se usa para configurar dónde se entregarán los datos de telemetría durante un contacto y es opcional en el perfil de una misión. Cuando se incluye, AWS Ground Station transmite la telemetría prácticamente en tiempo real a tu cuenta durante la ejecución de tus contactos.

Consulte la siguiente documentación para obtener más información sobre cómo realizar operaciones en configuraciones mediante CloudFormation la API o la AWS Command Line Interface API. AWS Ground Station 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 AWS Ground Station usa las efemérides](#) 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 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 señal Data/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 decodificación, consulte la [Configuración de decodificación 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 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 decodificación 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 decodificación por demodulación. and/or Si está interesado en ejecutar este tipo de contactos, abra un ticket a través del. AWS Support [AWS Support Center Console](#) 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 de datos/IP. Demodulated/Decoded

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 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 señal 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 enlace ascendente de la antena mediante 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 de señal. Data/IP 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 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 de conexión de Dataflow solo se utilizan para la entrega de datos a Amazon EC2 y no se utilizan para la entrega de datos a Amazon S3.

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

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "groundstation.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "999999999999"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:groundstation:us-east-1:999999999999: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.

JSON

```

{
  "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 usará al nombrar el 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 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](#)

Config del disipador de telemetría

Puede utilizar las configuraciones del receptor de telemetría para especificar dónde desea que se entreguen los datos de telemetría durante los contactos por satélite. La configuración de un receptor de telemetría es opcional y se añade al perfil de la misión para programar los contactos habilitados para telemetría. A continuación, se especifican las restricciones y los detalles sobre estos parámetros:

- 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.

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"
    }
  ]
}
```

- La función de IAM debe tener una política de IAM que le permita realizar las `kinesis:DescribeStream` operaciones `kinesis:PutRecord` y `kinesis:PutRecords` acciones en la transmisión. 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": [
        "kinesis:DescribeStream",
        "kinesis:PutRecord",
        "kinesis:PutRecords"
      ],
      "Resource": "arn:aws:kinesis:us-east-2:999999999999:stream/your-stream-name"
    }
  ]
}
```

Cuando incluyas una configuración de receptor de telemetría en tu perfil de misión, AWS Ground Station transmitirá los datos de telemetría a tu cuenta durante los contactos. Para obtener más

información sobre los tipos de telemetría, el formato de los datos y la configuración de los recursos necesarios, consulte. AWS [Trabaje con telemetría](#)

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

- [AWS::GroundStation::Config TelemetrySinkConfig CloudFormation propiedad](#)
- [Config AWS CLI reference](#) (consulte la `telemetrySinkConfig` -> `(structure)` sección)
- [TelemetrySinkConfig Referencia de API](#)

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.

Versiones de grupos de puntos finales de Dataflow

AWS Ground Station admite dos versiones de grupos de puntos finales de flujos de datos:

- `DataflowEndpointGroup`- [La implementación original que admite el enlace ascendente y el enlace descendente mediante un punto final de flujo de datos y solo el enlace descendente para un punto final de agente AWS Ground Station](#)
- `DataflowEndpointGroupV2`: versión actualizada que admite flujos de datos de enlace ascendente y descendente para los puntos finales del agente con mayor claridad y funcionalidad AWS Ground Station

Comparación de grupos de puntos finales de flujos de datos

Característica	DataflowEndpointGroup	DataflowEndpointGroupV2
Tipos de puntos finales compatibles	DataflowEndpoint, AwsGroundStationAgentEndpoint	DownlinkAwsGroundStationAgentEndpoint, UplinkAwsGroundStationAgentEndpoint
Puntos finales que admiten enlaces ascendentes	DataflowEndpoint	UplinkAwsGroundStationAgentEndpoint
Puntos finales que admiten el enlace descendente	DataflowEndpoint, AwsGroundStationAgentEndpoint	DownlinkAwsGroundStationAgentEndpoint

DataflowEndpointGroupLa V2 se creó para admitir flujos de datos de enlace ascendente y para aclarar el lenguaje que rodea a los grupos de puntos finales de los flujos de datos. Recomendamos utilizar [UplinkAwsGroundStationAgentEndpointDownlinkAwsGroundStationAgentEndpoint](#) puntos finales con una [DataflowEndpointGroupV2](#) para todos los casos de uso nuevos.

DataflowEndpointGroup sigue siendo compatible con versiones anteriores, pero la DataflowEndpointGroup V2 ofrece una funcionalidad mejorada y opciones de configuración más claras.

 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 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. Los tipos de puntos finales compatibles dependen de la versión del grupo de puntos finales del flujo de datos que utilice.

DataflowEndpointGroup puntos de conexión

DataflowEndpointGroup [admite el enlace ascendente y el enlace descendente mediante un punto final de flujo de datos y solo el enlace descendente para un punto final de agente.](#) [AWS Ground Station](#) Para ambos tipos de puntos de enlace, debe crear las estructuras de soporte (por ejemplo, las direcciones IP) antes de crear el grupo de puntos de enlace 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.

En el DataflowEndpointGroup caso de la versión 2, puede mezclar

[UplinkAwsGroundStationAgentEndpoint](#) y formar [DownlinkAwsGroundStationAgentEndpoint](#) el mismo grupo.

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. Para crear un punto final de AWS Ground Station agente, solo debe rellenar el `AwsGroundStationAgentEndpoint` campo del `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 la dirección del puerto utilizadas 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 vincular datos de señal digital por vía ascendente, enlace descendente de menos del 50% de los datos de señal digital o enlace descendente de datos MHz de señal. `Demodulated/Decoded` Para construir un punto final de flujo de datos, rellenará 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.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```

    "Principal": {
      "Service": "groundstation.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "999999999999"
      },
      "ArnLike": {
        "aws:SourceArn": "arn:aws:groundstation:us-
east-1:999999999999: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.

JSON

```

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

```

```
}
```

DataflowEndpointGroupPuntos finales V2

DataflowEndpointGroupLa versión 2 presenta tipos de terminales especializados que proporcionan una configuración más clara y una funcionalidad mejorada:

- [UplinkAwsGroundStationAgentEndpoint](#)- Optimizado para flujos de datos de enlace ascendente
- [DownlinkAwsGroundStationAgentEndpoint](#)- Optimizado para flujos de datos de enlace descendente

Estos puntos finales especializados sustituyen las configuraciones genéricas [AwsGroundStationAgentEndpoint](#) por configuraciones específicas para cada dirección, lo que facilita la configuración y la administración de los flujos de datos.

AWS Ground Station Punto final de Uplink Agent

[UplinkAwsGroundStationAgentEndpoint](#) Está diseñado específicamente para flujos de datos de enlace ascendente y ofrece opciones de configuración más claras. Utilice este tipo de punto final cuando necesite proporcionar datos para su enlace ascendente AWS Ground Station a su satélite.

`UplinkAwsGroundStationAgentEndpoint` 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.
- IngressAddressAndPort- Dirección IP y puerto únicos para la entrada de datos al agente
- AgentIpAndPortAddress- Rango de puertos para la comunicación con el agente

Punto final de Downlink AWS Ground Station Agent

[DownlinkAwsGroundStationAgentEndpoint](#) Está optimizado para los flujos de datos de enlace descendente, incluidos los escenarios de enlace descendente de banda estrecha, demodulación/decodificación de banda ancha y eco de enlace ascendente.

`DownlinkAwsGroundStationAgentEndpoint` 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.
- EgressAddressAndPort- Dirección IP y puerto únicos para la salida de datos del agente
- AgentIpAndPortAddress- Rango de puertos para la comunicación con el agente

Creación de grupos de puntos finales de flujos de datos

Puede crear grupos de puntos finales de flujo de datos con cualquiera de las versiones:

CreateDataflowEndpointGroup

Úselo [CreateDataflowEndpointGroup](#) para garantizar la compatibilidad con versiones anteriores o cuando necesite usar el genérico [AwsGroundStationAgentEndpoint](#) [DataflowEndpoint](#) los tipos.

CreateDataflowEndpointGroupV2

Utilice la [CreateDataflowEndpointGroupV2](#) para las nuevas implementaciones y aproveche los tipos de terminales especializados que admiten flujos de datos de enlace ascendente y descendente. Esta API solo admite y. [UplinkAwsGroundStationAgentEndpointDownlinkAwsGroundStationAgentEndpoint](#)

Consideraciones sobre la migración

Si la está utilizando actualmente `DataflowEndpointGroup`, puede seguir utilizando la configuración existente sin cambios. AWS Ground Station mantiene una total compatibilidad con versiones anteriores.

Si desea migrar para utilizar la nueva `DataflowEndpointGroup` versión 2 y actualmente utiliza una [DataflowEndpoint](#) aplicación de punto final de Dataflow para recibir sus datos, tendrá que migrar para utilizar el AWS Ground Station agente en su lugar. Si ya utiliza un AWS Ground Station agente para el enlace descendente, también puede utilizar la misma instancia de agente para el enlace superior; no se requieren instancias de agente adicionales.

Para migrar a la versión 2 `DataflowEndpointGroup`:

1. Si está migrando desde `DataflowEndpoint`, configure el AWS Ground Station agente siguiendo la Guía del [usuario del AWS Ground Station agente](#)
2. Identifique la dirección del flujo de datos y cree el tipo (o) de punto final adecuado [UplinkAwsGroundStationAgentEndpointDownlinkAwsGroundStationAgentEndpoint](#)

3. Cree la [DataflowEndpointGroupV2](#) que haga referencia a esos puntos finales
4. Cree una nueva [configuración de punto final de flujo de datos](#) que haga referencia a la nueva V2 por su nombre DataflowEndpointGroup
5. Cree un nuevo perfil de misión que haga referencia a la configuración del punto final del flujo de datos como borde del flujo de datos
6. Usa el nuevo perfil de misión para programar contactos
7. Pruebe la configuración antes de implementarla en producción

Para obtener más información sobre el flujo de trabajo completo, consulte [Comprenda los componentes AWS Ground Station principales](#) y [Crear configuraciones](#).

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.

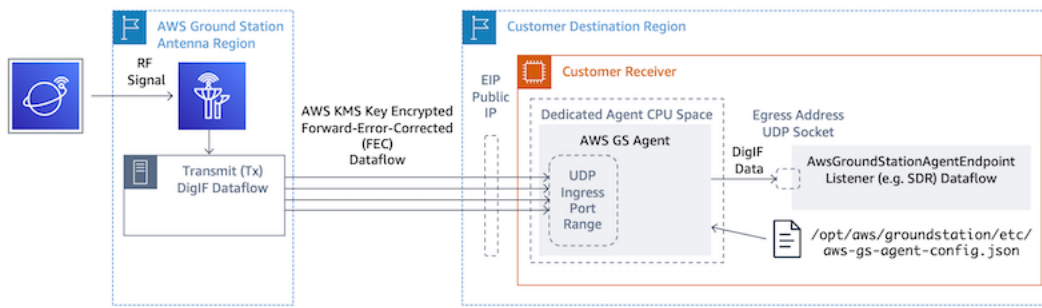
Funcionamiento

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.

Inscríbese en un Cuenta de AWS

Si no tiene una 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 AWS se 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 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 [Consola de administración de AWS](#) como 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 Consola de administración de AWS](#) y ábrala.
2. Cree una política nueva. Utilice los siguientes pasos:
 - a. En el panel de navegación, seleccione Políticas (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:

JSON

```
{
  "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:

JSON

```
{
  "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`

JSON

```
{
  "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 (NDA).

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 AWS Ground Station, envíe un cuestionario de incorporación de [satélites en la sección Satélites y recursos](#) de la página de la AWS Ground Station consola. Incluya un breve resumen de su misión y sus necesidades de satélites, incluyendo el nombre de su organización, las frecuencias requeridas, cuándo se lanzarán o se lanzarán los satélites, el tipo de órbita del satélite y si tiene previsto utilizarlos. [Utilice la función de gemelo AWS Ground Station digital](#)
3. Una vez que su solicitud haya sido revisada y aprobada, AWS Ground Station solicitará la licencia reglamentaria en las ubicaciones específicas que planea 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 de que la actualización se ha 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. 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 a través de la API [list-satellites](#) de la AWS CLI:

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

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

```
{
  "satellites": [
    {
      "groundStations": [
        "Ohio 1",
        "Oregon 1"
      ],
      "noradSatelliteID": 27424,
      "satelliteArn":
"arn:aws:groundstation::111111111111:satellite/11111111-2222-3333-4444-555555555555",
      "satelliteId": "11111111-2222-3333-4444-555555555555"
    }
  ]
}
```

Busque el satélite que desea etiquetar y anote su `satelliteArn`. [Una advertencia importante para el etiquetado es que la API 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 CloudFormation plantillas preconfiguradas para facilitar la puesta en marcha del servicio. Consulte [Ejemplos de configuraciones de perfil de misión](#) para ver ejemplos de cómo se AWS Ground Station puede 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](#).

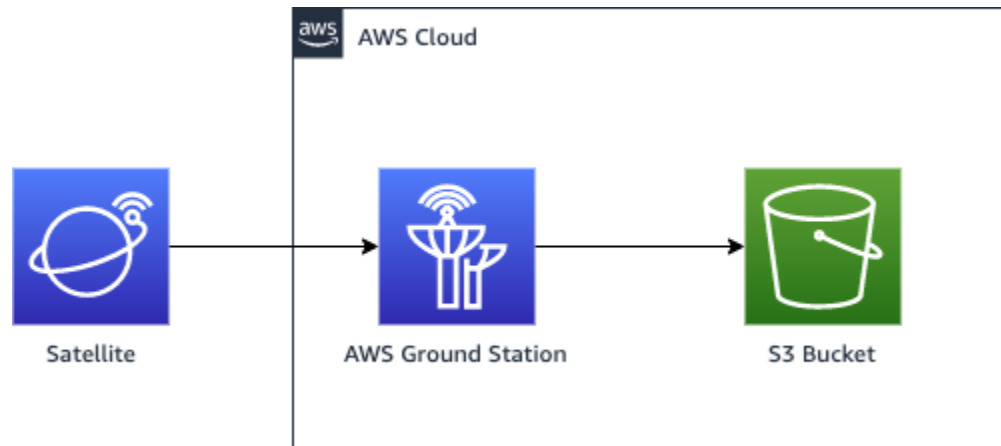
Planifique las rutas de comunicación de su flujo de datos

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.



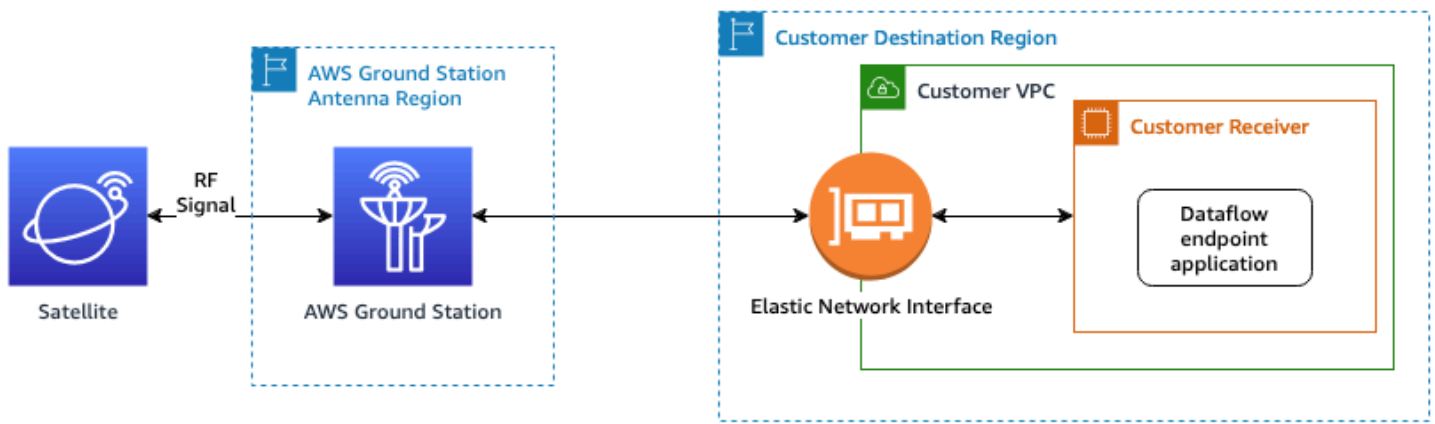
Para utilizar esta ruta, necesitará crear un bucket de Amazon S3 AWS Ground Station para entregar los datos. En el siguiente paso, también tendrás que crear una S3 Recording Config en el siguiente paso. Consulte las restricciones sobre [Config de grabación de Amazon S3](#) la denominación de los depósitos 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.

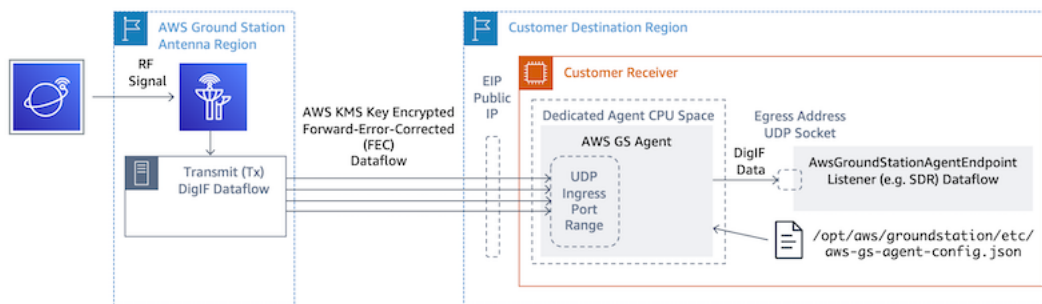
Para utilizar una ruta sincrónica, necesitará instalar y configurar sus EC2 instancias de Amazon y crear uno o más grupos de puntos de conexión de Dataflow. Para configurar tu EC2 instancia de Amazon, consulta el [Configurar y configurar Amazon EC2](#). Para crear su grupo de puntos de conexión de Dataflow, 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.



*End to end data connection is established and maintained only during the scheduled contact duration.

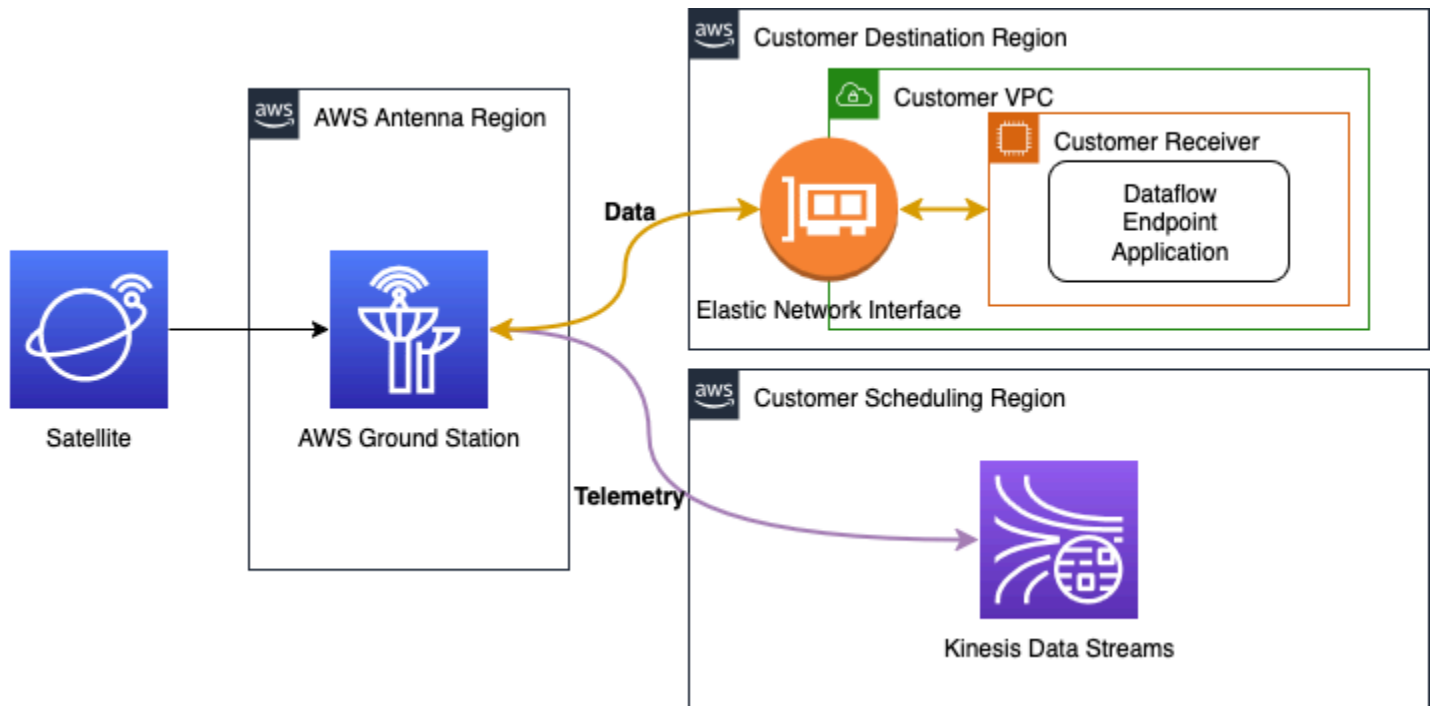
A continuación, se muestra la ruta de comunicación si utiliza la configuración del AWS Ground Station agente.



Planifique su telemetría

AWS Ground Station la telemetría es una función opcional que transmite las métricas de las AWS Ground Station antenas a tu AWS cuenta durante los contactos por satélite. Esto le permite monitorear el rendimiento de los contactos prácticamente en tiempo real y crear soluciones de monitoreo personalizadas.

Con la AWS Ground Station telemetría, las métricas de las AWS Ground Station antenas se transmiten directamente a su cuenta. Los datos de telemetría comienzan a transmitirse al inicio del contacto y continúan durante todo el tiempo que dura el contacto. Los datos de telemetría se envían a su cuenta prácticamente en tiempo real, ya que se toman muestras del hardware de la antena. Una vez recibidos, puede procesar los datos con su propio software de posprocesamiento o utilizar otros servicios de AWS, como Amazon Data AWS Lambda Firehose o.



En el siguiente paso, creará las configuraciones necesarias para el perfil de su misión. Si quieres habilitar la telemetría, crearás una configuración de receptor de telemetría además de la configuración de seguimiento y de flujo de datos. Para obtener instrucciones de configuración detalladas, consulte. [Configure la telemetría](#)

Para obtener más información al respecto TelemetrySinkConfig, consulte [Config del dissipador de telemetría](#).

Crear configuraciones

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

Configuración de telemetría (opcional)

Si desea recibir telemetría casi en tiempo real durante sus contactos, puede crear un TelemetrySinkConfig. Esta configuración es opcional y especifica dónde se AWS Ground Station entregará los datos de telemetría.

- [Config del disipador de telemetría](#)- Entregue los datos de telemetría a su cuenta.

Para obtener instrucciones de configuración detalladas, consulte [Configure la telemetría](#)

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, las posibles formas de comunicarse con su satélite y cómo habilitar la telemetría prácticamente en tiempo real durante la ejecución del contacto. En este paso, creará 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-operation` si 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 `streamsKmsKey` y `streamsKmsRole` que 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, consulte [Automatiza AWS Ground Station con eventos](#).
7. [Opcional] Configura tu `telemetrySinkConfigArn` para activar la telemetría durante los contactos. Esto le permite recibir telemetría prácticamente en tiempo real directamente en su cuenta para su supervisión y análisis. Para obtener más información, consulte [Trabaje con telemetría](#).
8. [Opcional] Puedes asociar etiquetas al perfil de tu misión. Se pueden usar para ayudar a diferenciar programáticamente los perfiles de sus misiones.

Puede consultarlos para ver solo algunas de las posibles configuraciones. [Ejemplos de configuraciones de perfil de misión](#)

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, consulte [Comprenda cómo AWS Ground Station usa las efemérides](#).

AWS Ground Station mantiene una serie de CloudFormation plantillas preconfiguradas para facilitar la puesta en marcha del servicio. [Ejemplos de configuraciones de perfil de misión](#) Consulte 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 [ListGroundStation](#) respuesta 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 digital](#) está 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 descenden te 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.
antena: enlace descendente	7750 - 8500 MHz	50 - 400 MHz	RHCP		El ancho de banda total no debe superar los 400 MHz por polarización en cada ubicación.
antena: enlace descendente	7750 - 8500 MHz	50 - 400 MHz	LHCP		Todos los rangos de frecuencia utilizados no deben superponerse.
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 polarizac ión 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 descenden te de banda estrecha de banda X	Solo se puede usar una polarizac ión 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 polarizac ión a la vez
antena- enlace ascendente	2025 - 2110 MHz	Hasta 40 MHz	LHCP		EIRP de 20 a 50 dBW
antenna-u plink-echo	2025 - 2110 MHz	2 MHz	RHCP	Eco de enlace ascendente	Coincide con las restricciones
antenna-u plink-echo	2025 - 2110 MHz	2 MHz	LHCP		de enlace ascendente entre antenas

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 AWS Ground Station usa las efemérides

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.

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

AWS Ground Station utiliza los datos de efemérides para determinar cuándo estarán disponibles los contactos en función de las efemérides proporcionadas y controlar correctamente las antenas de la red. AWS Ground Station [De forma predeterminada, no es necesario realizar ninguna acción para proporcionar AWS Ground Station efemérides si el satélite tiene un identificador de NORAD asignado.](#)

Al subir efemérides personalizadas, se puede 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

Como alternativa, AWS Ground Station admite un formato de elevación acimutal, que permite especificar directamente las direcciones de orientación de la antena sin proporcionar información sobre la órbita del satélite. Esto resulta útil en situaciones en las que se requiere una orientación precisa de la antena porque la información sobre la trayectoria del satélite es imprecisa o desconocida.

Temas

- [Datos de efemérides predeterminados](#)
- [Proporcione datos de efemérides personalizados](#)
- [Reserva contactos con efemérides personalizadas](#)
- [Comprenda qué efemérides se utilizan](#)
- [Obtén las efemérides actuales de un satélite](#)
- [Vuelva a los datos de efemérides predeterminados](#)

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. Por lo tanto, las efemérides personalizadas que no hayan caducado y se hayan subido a través de la API de efemérides, las cuales siempre deberán tener una prioridad igual o superior. 1

Los satélites que no cuenten con un ID de NORAD deberán subir datos de efemérides personalizadas a 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 de NORAD y deberían tener cargadas las efemérides personalizadas. [Para obtener más información sobre cómo proporcionar datos de efemérides personalizadas, consulte: Proporcionar datos de efemérides personalizadas.](#)

Proporcione 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 necesita poder cargar datos de efemérides personalizados, abra un AWS Support ticket a través del [AWS Support Center Console](#). Nuestro equipo trabajará con usted para habilitar esta capacidad para sus requisitos específicos.

Descripción general de

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

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.

La carga de efemérides personalizadas puede mejorar la calidad del seguimiento, gestionar operaciones en las que no haya efemérides de [Space-Track](#) disponibles y tener en cuenta las maniobras. AWS Ground Station

Para solucionar problemas relacionados con una efeméride no válida, consulta: [Solucionar problemas de efemérides no válidas](#)

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, consulte Uso de efemérides proporcionadas por el cliente con AWS Ground Station aws-samples/ y su repositorio asociado. AWS Ground Station GitHub aws-groundstation-cpe](#)

Proporcione datos de efemérides de TLE

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 necesita poder cargar datos de efemérides personalizados, abra un AWS Support ticket a través del [AWS Support Center Console](#). Nuestro equipo trabajará con usted para habilitar esta capacidad para sus requisitos específicos.

Descripción general de

Los conjuntos de elementos de dos líneas (TLE) son un formato estandarizado para describir las órbitas de los satélites. La API de efemérides permite cargar las efemérides del TLE para usarlas con un satélite. AWS Ground Station [Estas efemérides anulan las efemérides predeterminadas de Space-Track \(consulte:\). Datos de efemérides predeterminados](#)

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.

La carga de efemérides TLE personalizadas puede mejorar la calidad del seguimiento, gestionar las primeras operaciones en las que no haya efemérides de [Space-Track](#) disponibles 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 utilizarlas para el campo de números de catálogo de satélites de la TLE y 00000 para la parte del número de lanzamiento del campo designador internacional de la TLE (por ejemplo, 000 para un vehículo lanzado en 2024). 24000A

Para obtener más información sobre el formato de TLEs, consulte [Conjunto de elementos de dos líneas](#).

Crear una efeméride TLE

Se puede crear una efeméride de TLE mediante la [CreateEphemeris](#) acción de la API. 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 [DescribeEphemeris](#) para 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 [CreateEphemeris](#) llamada. Esta efeméride se utilizará en lugar de los datos de efemérides predeterminados de 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:

```
[
  {
    "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:

```
import boto3
from datetime import datetime, timedelta, timezone

# Create AWS Ground Station client
ground_station_client = boto3.client("groundstation")

# Create TLE ephemeris
tle_ephemeris = ground_station_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   .000000075   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),
                    },
                }
            ]
        }
    },
)

print(f"Created TLE ephemeris with ID: {tle_ephemeris['ephemerisId']}")

```

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:

```

import boto3
from datetime import datetime, timedelta, timezone
import time

# Create AWS Ground Station client
ground_station_client = boto3.client("groundstation")

# First, create a TLE ephemeris
print("Creating TLE ephemeris...")

tle_ephemeris = ground_station_client.create_ephemeris(
    name="Example TLE Ephemeris for Description",
    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),
            },
          }
        ]
      }
    },
  )

ephemeris_id = tle_ephemeris["ephemerisId"]
print(f"Created TLE ephemeris with ID: {ephemeris_id}")

# Describe the ephemeris immediately to check initial status
print("Describing ephemeris...")

response = ground_station_client.describe_ephemeris(ephemerisId=ephemeris_id)

print(f"Ephemeris ID: {response['ephemerisId']}")
print(f"Name: {response['name']}")
print(f"Status: {response['status']}")

```

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 [DescribeEphemeris](#) ruta 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 efemérides del TLE desde un depósito S3

También es posible cargar un archivo de efemérides TLE directamente desde un depósito de S3 apuntando al depósito y a la clave del objeto. AWS Ground Station recuperará el objeto en tu nombre. La información sobre el cifrado de los datos en reposo AWS Ground Station se detalla en: [Cifrado de datos en reposo para AWS Ground Station](#).

A continuación se muestra un ejemplo de cómo cargar un archivo de efemérides TLE desde un bucket de S3

```

import boto3
from datetime import datetime, timedelta, timezone
import json

# Create AWS clients
s3_client = boto3.client("s3")
ground_station_client = boto3.client("groundstation")

# Define S3 bucket and key
bucket_name = "ephemeris-bucket"
object_key = "test_data.tle"

# Create sample TLE set data
# Note: For actual satellites, use real TLE data from sources like Space-Track
tle_set_data = [
    {
        "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=3),
        },
    },
    {
        "tleLine1": "1 25994U 99068A 20321.54719794 .00000075 00000-0 26688-4 0
9998",
        "tleLine2": "2 25994 98.2007 33.6589 0001234 89.2782 18.9934
14.57114995112342",
        "validTimeRange": {
            "startTime": datetime.now(timezone.utc) + timedelta(days=3),
            "endTime": datetime.now(timezone.utc) + timedelta(days=7),
        },
    },
]

# Convert to JSON string for upload
tle_json = json.dumps(tle_set_data, indent=2)

# Upload sample TLE data to S3
print(f"Uploading TLE set data to s3://{bucket_name}/{object_key}")

s3_client.put_object(
    Bucket=bucket_name, Key=object_key, Body=tle_json, ContentType="application/json"
)
print("TLE set data uploaded successfully to S3")
print(f"Uploaded {len(tle_set_data)} TLE entries covering 7 days")

# Create TLE ephemeris from S3
print("Creating TLE ephemeris from S3...")

s3_tle_ephemeris = ground_station_client.create_ephemeris(
    name="2022-11-05 S3 TLE Upload",
    satelliteId="fde41049-14f7-413e-bd7b-EXAMPLE01",
    enabled=True,
    expirationTime=datetime.now(timezone.utc) + timedelta(days=5),
    priority=2,
    ephemeris={"tle": {"s3object": {"bucket": bucket_name, "key": object_key}}},
)

```

```
print(f"Created TLE ephemeris with ID: {s3_tle_ephemeris['ephemerisId']}")
```

Proporcione datos de efemérides OEM

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 necesita poder cargar datos de efemérides personalizados, abra un AWS Support ticket a través del [AWS Support Center Console](#). Nuestro equipo trabajará con usted para habilitar esta capacidad para sus requisitos específicos.

Descripción general de

El mensaje de efemérides en órbita (OEM) es un formato estandarizado para representar los datos de trayectoria de las naves espaciales. La API de efemérides permite cargar efemérides OEM para usarlas con un satélite. AWS Ground Station [Estas efemérides anulan las efemérides predeterminadas de Space-Track \(consulte:\)](#). [Datos de efemérides predeterminados](#)

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 resolución de problemas.

La carga de efemérides OEM personalizadas permite mejorar la calidad del seguimiento, gestionar las primeras operaciones en las que 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 al satélite, puede utilizarlas para la parte del OEM. `satelliteId OBJECT_ID`. Para obtener más información sobre el formato de OEMs, consulte [Formato 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
				:, EME2000 ITRF2000
	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:

- `CCSDS_OEM_VERSION` se requiere que sea `2.0`
- `REF_FRAME` se requiere que sea uno `EME2000` de los dos `ITRF2000`.
- `REF_FRAME_EPOCH` no es compatible con AWS Ground Station.
- `CENTER_NAME` se requiere que lo sea `Earth`.
- `TIME_SYSTEM` se requiere que lo sea `UTC`.
- `INTERPOLATION` y ambos `INTERPOLATION_DEGREE` son obligatorios para las efemérides proporcionadas por el AWS Ground Station cliente.

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

```

Creación de una efeméride OEM

Se puede crear una efeméride OEM mediante la [CreateEphemeris](#) acción de la API. 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 [DescribeEphemeris](#) para hacer 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: cargar datos de efemérides OEM desde un bucket de S3

También es posible cargar un archivo de efemérides OEM directamente desde un depósito de S3 apuntando al depósito y a la clave del objeto. AWS Ground Station recuperará el objeto en tu nombre. La información sobre el cifrado de los datos en reposo AWS Ground Station se detalla en: [Cifrado de datos en reposo para AWS Ground Station](#).

A continuación se muestra un ejemplo de cómo cargar un archivo de efemérides OEM desde un bucket de S3

```
import boto3
from datetime import datetime, timedelta, timezone

# Create AWS clients
s3_client = boto3.client("s3")
ground_station_client = boto3.client("groundstation")

# Define S3 bucket and key
bucket_name = "ephemeris-bucket"
object_key = "test_data.oem"

# Create sample OEM data in KVN format
oem_data = """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
""

# Upload sample OEM data to S3
print(f"Uploading OEM data to s3://{bucket_name}/{object_key}")

s3_client.put_object(
    Bucket=bucket_name, Key=object_key, Body=oem_data, ContentType="text/plain"
)

```

```
print("OEM data uploaded successfully to S3")

# Create OEM ephemeris from S3
print("Creating OEM ephemeris from S3...")

s3_oem_ephemeris = ground_station_client.create_ephemeris(
    name="2024-07-22 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": bucket_name, "key": object_key}}},
)

print(f"Created OEM ephemeris with ID: {s3_oem_ephemeris['ephemerisId']}")
```

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"
      }
    }
  }
}
```

Proporcione datos de efemérides de elevación del acimut

Important

La función de efemérides de elevación azimutal se encuentra actualmente en estado de vista previa y requiere una incorporación explícita.

La funcionalidad de efemérides de elevación azimutal está sujeta a un estricto control de acceso para un número limitado de casos de uso especializados y predeterminados. El acceso es considerablemente más restrictivo que el de las funciones de efemérides estándar proporcionadas por el cliente. Para obtener más información sobre los casos de uso aprobados y el proceso de solicitud de acceso, abra un AWS Support ticket a través del [AWS Support Center Console](#). Nuestro equipo lo guiará a través del proceso de aprobación de casos de uso especializados.

Descripción general de

Las efemérides de elevación azimutal permiten especificar directamente las direcciones de orientación de la antena sin proporcionar información sobre la órbita del satélite. En lugar de cargar datos de efemérides que describen la órbita de un satélite, se proporcionan ángulos de acimut y elevación marcados con el tiempo que indican a la antena exactamente hacia dónde debe apuntar un 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.

Este enfoque resulta especialmente útil en los siguientes escenarios:

- Apoyo a las primeras operaciones: durante la fase de lanzamiento y la fase de órbita temprana (LEOP), cuando no se dispone de datos orbitales precisos o los parámetros orbitales cambian rápidamente.
- Patrones de puntería personalizados: implementación de secuencias de puntería específicas para pruebas de antenas u operaciones no estándar.

Note

Cuando se utilizan efemérides de elevación de acimut, es posible que se omita el ARN del satélite en la solicitud de reserva de contacto. Si no se omite el ARN del satélite, se seguirá incluyendo como parte de los datos de contacto, pero las efemérides de elevación del acimut se utilizarán para apuntar la antena en lugar de realizar una resolución prioritaria de efemérides. La efeméride de elevación acimutal está asociada a una estación terrestre específica y define las direcciones de orientación de la antena para esa ubicación.

Formato de datos de efemérides de elevación azimutal

Los datos de efemérides de elevación azimutal se componen de valores de acimut y elevación etiquetados en función del tiempo y organizados en segmentos. Cada segmento contiene una serie de ángulos de acimut y elevación que cubren un intervalo de tiempo específico.

Los componentes clave de los datos de efemérides de elevación del acimut son:

- Ground Station: la estación terrestre específica en la que se utilizará esta efeméride de elevación acimutal.
- Unidad de ángulo: la unidad de medida de los ángulos (o). DEGREE_ANGLE RADIAN
- Segmentos: uno o más conjuntos de ángulos de acimut y elevación limitados en el tiempo.
- Ángulos etiquetados con el tiempo: valores individuales de acimut y elevación con marcas de tiempo asociadas.

Cada segmento requiere:

- Una época de referencia (el tiempo base del segmento)
- Un intervalo de tiempo válido (horas de inicio y finalización del segmento)
- Al menos 5 pares etiquetados con el tiempo azimuth/elevation

Restricciones de elevación del acimut:

- Acimut en grados: de -180° a 360°
- Acimut en radianes: de $-\pi$ a 2π
- Elevación en grados: de -90° a 90°
- Elevación en radianes: de $-\pi/2$ a $\pi/2$
- Los valores de tiempo deben estar en orden ascendente dentro de cada segmento
- Los segmentos no deben superponerse en el tiempo

Para obtener más información, consulta la documentación de la [CreateEphemeris](#) API y el tipo de [TimeAzEl](#) datos.

Crear efemérides de elevación de acimut

Las efemérides de elevación azimutal se crean mediante la misma acción de API, pero con el tipo de efemérides. [CreateEphemeris](#) azEl Las principales diferencias entre las efemérides TLE y OEM son:

- Debe especificar un parámetro `groundStation`
- El `satelliteId` parámetro debe omitirse de la solicitud
- No se aplica la configuración de prioridad (cada efeméride de elevación de acimut es específica de una estación terrestre)
- Cada segmento debe contener al menos 5 azimuth/elevation puntos para admitir la interpolación de Lagrange de cuarto orden
- Los límites y requisitos adicionales se detallan en la documentación de la API [CreateEphemeris](#)

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. Una efeméride solo se utilizará para los contactos una vez que haya superado este flujo de trabajo y su estado pase a ser `ENABLED` Deberías sondear el estado de las efemérides o usar `CloudWatch` eventos [DescribeEphemeris](#) para 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 efemérides de elevación de acimut mediante la API

El siguiente ejemplo muestra cómo crear una efeméride de elevación de acimut mediante el AWS SDK para Python (Boto3):

```
import boto3

# Create AWS Ground Station client
ground_station_client = boto3.client("groundstation")

# Create azimuth elevation ephemeris
azimuth_elevation_ephemeris = ground_station_client.create_ephemeris(
    name="Azimuth Elevation for Ohio Ground Station",
    ephemeris={
        "azEl": {
```

```

    "groundStation": "Ohio 1",
    "data": {
      "azElData": {
        "angleUnit": "DEGREE_ANGLE",
        "azElSegmentList": [
          {
            "referenceEpoch": "2024-03-15T10:00:00Z",
            "validTimeRange": {
              "startTime": "2024-03-15T10:00:00Z",
              "endTime": "2024-03-15T10:15:00Z",
            },
            "azElList": [
              {"dt": 0.0, "az": 45.0, "el": 10.0},
              {"dt": 180.0, "az": 50.0, "el": 15.0},
              {"dt": 360.0, "az": 55.0, "el": 20.0},
              {"dt": 540.0, "az": 60.0, "el": 25.0},
              {"dt": 720.0, "az": 65.0, "el": 30.0},
              {"dt": 900.0, "az": 70.0, "el": 35.0},
            ],
          },
        ],
      },
    },
  },
)

print(f"Created ephemeris with ID: {azimuth_elevation_ephemeris['ephemerisId']}")

```

En este ejemplo:

- Los datos de elevación acimutal están asociados a la estación terrestre «Ohio 1»
- Los ángulos se especifican en grados
- El segmento cubre un período de 15 minutos
- Los dt valores son segundos atómicos con respecto a la época de referencia
- Se proporcionan seis azimuth/elevation pares (el mínimo es 5)

Ejemplo: cargue datos de elevación de acimut desde S3

Para conjuntos de datos más grandes, puede cargar datos de elevación de acimut desde un depósito de S3:

```
import boto3
import json

# Create AWS clients
s3_client = boto3.client("s3")
ground_station_client = boto3.client("groundstation")

# Define S3 bucket and key
bucket_name = "azimuth-elevation-bucket"
object_key = "singapore-azimuth-elevation.json"

# Create sample azimuth elevation data
azimuth_elevation_data = {
    "angleUnit": "DEGREE_ANGLE",
    "azElSegmentList": [
        {
            "referenceEpoch": "2024-03-15T10:00:00Z",
            "validTimeRange": {
                "startTime": "2024-03-15T10:00:00Z",
                "endTime": "2024-03-15T10:15:00Z",
            },
            "azElList": [
                {"dt": 0.0, "az": 45.0, "el": 10.0},
                {"dt": 180.0, "az": 50.0, "el": 15.0},
                {"dt": 360.0, "az": 55.0, "el": 20.0},
                {"dt": 540.0, "az": 60.0, "el": 25.0},
                {"dt": 720.0, "az": 65.0, "el": 30.0},
                {"dt": 900.0, "az": 70.0, "el": 35.0},
            ],
        },
        {
            "referenceEpoch": "2024-03-15T10:15:00Z",
            "validTimeRange": {
                "startTime": "2024-03-15T10:15:00Z",
                "endTime": "2024-03-15T10:30:00Z",
            },
            "azElList": [
                {"dt": 0.0, "az": 70.0, "el": 35.0},
                {"dt": 180.0, "az": 75.0, "el": 40.0},
                {"dt": 360.0, "az": 80.0, "el": 45.0},
                {"dt": 540.0, "az": 85.0, "el": 50.0},
                {"dt": 720.0, "az": 90.0, "el": 55.0},
                {"dt": 900.0, "az": 95.0, "el": 50.0},
            ],
        },
    ],
}
```

```

        ],
    },
],
}

# Upload sample data to S3
print(f"Uploading azimuth elevation data to s3://{bucket_name}/{object_key}")

s3_client.put_object(
    Bucket=bucket_name,
    Key=object_key,
    Body=json.dumps(azimuth_elevation_data, indent=2),
    ContentType="application/json",
)
print("Sample data uploaded successfully to S3")

# Create azimuth elevation ephemeris from S3
print("Creating azimuth elevation ephemeris from S3...")

s3_azimuth_elevation_ephemeris = ground_station_client.create_ephemeris(
    name="Large Azimuth Elevation Dataset",
    ephemeris={
        "azEl": {
            "groundStation": "Singapore 1",
            "data": {"s3Object": {"bucket": bucket_name, "key": object_key}},
        }
    },
)

print(f"Created ephemeris with ID: {s3_azimuth_elevation_ephemeris['ephemerisId']}")

```

El objeto S3 debe contener una estructura JSON con los datos de elevación del acimut en el mismo formato que se muestra en el ejemplo de carga directa.

Reservar contactos con efemérides de elevación de acimut

Cuando se utiliza una efeméride de elevación de acimut para reservar un contacto, el proceso es diferente al de las efemérides TLE y OEM:

1. Cree las efemérides de elevación de acimut mediante [CreateEphemeris](#)
2. Espere a que las efemérides alcancen el estado ENABLED
3. Reserva el contacto utilizando las anulaciones de [ReserveContactseguimiento](#)

Ejemplo de reserva de un contacto con efemérides de elevación acimutal:

```

import boto3
from datetime import datetime
import time

# Create AWS Ground Station client
ground_station_client = boto3.client("groundstation")

# First, create an azimuth elevation ephemeris
print("Creating azimuth elevation ephemeris...")

create_ephemeris_response = ground_station_client.create_ephemeris(
    name="Azimuth Elevation for Contact Reservation",
    ephemeris={
        "azEl": {
            "groundStation": "Ohio 1",
            "data": {
                "azElData": {
                    "angleUnit": "DEGREE_ANGLE",
                    "azElSegmentList": [
                        {
                            "referenceEpoch": "2024-03-15T10:00:00Z",
                            "validTimeRange": {
                                "startTime": "2024-03-15T10:00:00Z",
                                "endTime": "2024-03-15T10:15:00Z",
                            },
                            "azElList": [
                                {"dt": 0.0, "az": 45.0, "el": 10.0},
                                {"dt": 180.0, "az": 50.0, "el": 15.0},
                                {"dt": 360.0, "az": 55.0, "el": 20.0},
                                {"dt": 540.0, "az": 60.0, "el": 25.0},
                                {"dt": 720.0, "az": 65.0, "el": 30.0},
                                {"dt": 900.0, "az": 70.0, "el": 35.0},
                            ],
                        },
                    ],
                },
            },
        },
    },
)

ephemeris_id = create_ephemeris_response["ephemerisId"]

```

```
print(f"Created ephemeris with ID: {ephemeris_id}")

# Wait for ephemeris to become ENABLED
print("Waiting for ephemeris to become ENABLED...")

while True:
    status = ground_station_client.describe_ephemeris(ephemerisId=ephemeris_id)[
        "status"
    ]
    if status == "ENABLED":
        print("Ephemeris is ENABLED")
        break
    elif status in ["INVALID", "ERROR"]:
        raise RuntimeError(f"Ephemeris failed: {status}")
    time.sleep(5)

# Reserve contact with azimuth elevation ephemeris
print("Reserving contact...")

contact = ground_station_client.reserve_contact(
    # Note: satelliteArn is omitted when using azimuth elevation ephemeris
    missionProfileArn="arn:aws:groundstation:us-east-2:111122223333:mission-profile/
example-mission-profile",
    groundStation="Ohio 1",
    startTime=datetime(2024, 3, 15, 10, 0, 0),
    endTime=datetime(2024, 3, 15, 10, 15, 0),
    trackingOverrides={"programTrackSettings": {"azEl": {"ephemerisId":
ephemeris_id}}},
)

print(f"Reserved contact with ID: {contact['contactId']}")
```

Note

El `satelliteArn` parámetro puede omitirse al reservar un contacto con efemérides de elevación de acimut. La antena seguirá los ángulos de acimut y elevación especificados durante el contacto.

Listado de contactos disponibles

Cuando se utilizan efemérides de elevación de acimut, la [ListContacts](#) API requiere parámetros específicos:

- Es posible que el `satelliteArn` parámetro se omita en la solicitud
- Debe proporcionar un `ephemeris` parámetro con el identificador de efemérides de elevación del acimut para especificar qué efemérides utilizar
- [Las ventanas de contacto disponibles se muestran cuando los ángulos de acimut y elevación proporcionados están por encima de la máscara de emplazamiento de la estación terrestre solicitada](#)
- Aún así, debe proporcionar y `groundStation missionProfileArn`

Ejemplo de cómo crear una efeméride de elevación acimutal y enumerar los contactos disponibles con ella:

```
import boto3
from datetime import datetime, timezone
import time

# Create AWS Ground Station client
ground_station_client = boto3.client("groundstation")

# Step 1: Create azimuth elevation ephemeris
print("Creating azimuth elevation ephemeris...")
ephemeris_response = ground_station_client.create_ephemeris(
    name="Stockholm AzEl Ephemeris",
    ephemeris={
        "azEl": {
            "groundStation": "Stockholm 1",
            "data": {
                "azElData": {
                    "angleUnit": "DEGREE_ANGLE",
                    "azElSegmentList": [
                        {
                            "referenceEpoch": "2024-04-01T12:00:00Z",
                            "validTimeRange": {
                                "startTime": "2024-04-01T12:00:00Z",
                                "endTime": "2024-04-01T12:30:00Z",
                            }
                        }
                    ]
                }
            }
        }
    }
)
```

```

        "azElList": [
            {"dt": 0.0, "az": 30.0, "el": 15.0},
            {"dt": 360.0, "az": 45.0, "el": 30.0},
            {"dt": 720.0, "az": 60.0, "el": 45.0},
            {"dt": 1080.0, "az": 75.0, "el": 35.0},
            {"dt": 1440.0, "az": 90.0, "el": 20.0},
            {"dt": 1800.0, "az": 105.0, "el": 10.0},
        ],
    ],
}
},
},
)

ephemeris_id = ephemeris_response["ephemerisId"]
print(f"Created ephemeris: {ephemeris_id}")

# Step 2: Wait for ephemeris to become ENABLED
print("Waiting for ephemeris to become ENABLED...")
while True:
    describe_response = ground_station_client.describe_ephemeris(
        ephemerisId=ephemeris_id
    )
    status = describe_response["status"]

    if status == "ENABLED":
        print("Ephemeris is ENABLED")
        break
    elif status in ["INVALID", "ERROR"]:
        # Check for validation errors
        if "invalidReason" in describe_response:
            print(f"Ephemeris validation failed: {describe_response['invalidReason']}")
            raise RuntimeError(f"Ephemeris failed with status: {status}")

    print(f"Current status: {status}, waiting...")
    time.sleep(5)

# Step 3: List available contacts using the azimuth elevation ephemeris
print("Listing available contacts with azimuth elevation ephemeris...")

# Convert epoch timestamps to datetime objects
start_time = datetime.fromtimestamp(1760710513, tz=timezone.utc)

```

```
end_time = datetime.fromtimestamp(1760883313, tz=timezone.utc)

contacts_response = ground_station_client.list_contacts(
    startTime=start_time,
    endTime=end_time,
    groundStation="Stockholm 1",
    statusList=["AVAILABLE"],
    ephemeris={"azEl": {"id": ephemeris_id}},
    # satelliteArn is optional
    satelliteArn="arn:aws:groundstation::111122223333:satellite/a88611b0-f755-404e-
b60d-57d8aEXAMPLE",
    missionProfileArn="arn:aws:groundstation:eu-north-1:111122223333:mission-
profile/966b72f6-6d82-4e7e-b072-f8240EXAMPLE",
)

# Process the results
if contacts_response["contactList"]:
    print(f"Found {len(contacts_response['contactList'])} available contacts:")
    for contact in contacts_response["contactList"]:
        print(f" - Contact from {contact['startTime']} to {contact['endTime']}")
        print(
            f"    Max elevation: {contact.get('maximumElevation', {}).get('value', 'N/
A')}°"
        )
    )
else:
    print("No available contacts found for the specified azimuth elevation ephemeris")
```

Note

Al enumerar los contactos, se debe proporcionar el ephemeris parámetro con el identificador de elevación de acimut para especificar qué efemérides de elevación de acimut se deben utilizar para determinar las ventanas de contacto. Si satelliteArn se incluye, se asociará a los datos de contacto, pero las efemérides de elevación acimutal se utilizarán para apuntar la antena en lugar de realizar una resolución prioritaria de efemérides.

Reserva contactos con efemérides personalizadas

Descripción general de

Al usar efemérides personalizadas (TLE, OEM o elevación de acimut), puedes reservar contactos mediante la API. [ReserveContact](#) En esta sección se describen dos flujos de trabajo comunes para reservar contactos y algunas consideraciones importantes para garantizar una programación de contactos correcta.

AWS Ground Station las antenas son recursos compartidos entre varios clientes. Esto significa que, aunque aparezca una ventana de contactos disponible al enumerar los contactos, es posible que otro cliente la reserve antes que tú. Por lo tanto, es fundamental comprobar que tu contacto llegue al SCHEDULED estado tras realizar la reserva e implementar un seguimiento adecuado de los cambios de estado del contacto.

Important

En el caso de las efemérides de elevación de acimut, es posible que se omita el `satelliteArn` parámetro en la `ReserveContact` solicitud y debes proporcionarnos el identificador de la efeméride. `trackingOverrides` En el caso de las efemérides TLE y OEM, aún debe proporcionar el. `satelliteArn`

Flujos de trabajo para reservar contactos

Existen dos flujos de trabajo principales para reservar contactos con efemérides personalizadas:

1. List-then-reserve flujo de trabajo: primero enumere las ventanas de contactos disponibles y [ListContacts](#), a continuación, seleccione y reserve una ventana específica. Este enfoque resulta útil si desea ver todas las oportunidades disponibles antes de realizar una selección.
2. Flujo de trabajo de reserva directa: reserve directamente un contacto para un período de tiempo específico sin enumerar primero los contactos disponibles. Este enfoque resulta útil cuando ya sabes la hora de contacto deseada o si trabajas con horarios predeterminados.

Ambos flujos de trabajo son válidos y la elección depende de sus requisitos operativos. En las siguientes secciones se proporcionan ejemplos de cada enfoque.

Flujo de trabajo 1: Listar los contactos disponibles y luego reservar

Este flujo de trabajo consulta primero las ventanas de contacto disponibles y, a continuación, reserva una ventana específica. Esto resulta útil si desea ver todas las oportunidades disponibles antes de realizar una selección.

Ejemplo: Listar y reservar con efemérides de elevación acimutal

```
import boto3
from datetime import datetime, timezone
import time

# Create AWS Ground Station client
ground_station_client = boto3.client("groundstation")

# Create azimuth elevation ephemeris
print("Creating azimuth elevation ephemeris...")
ephemeris_response = ground_station_client.create_ephemeris(
    name="AzEl Ephemeris for Contact",
    ephemeris={
        "azEl": {
            "groundStation": "Ohio 1",
            "data": {
                "azElData": {
                    "angleUnit": "DEGREE_ANGLE",
                    "azElSegmentList": [
                        {
                            "referenceEpoch": "2024-03-15T10:00:00Z",
                            "validTimeRange": {
                                "startTime": "2024-03-15T10:00:00Z",
                                "endTime": "2024-03-15T10:15:00Z",
                            },
                            "azElList": [
                                {"dt": 0.0, "az": 45.0, "el": 10.0},
                                {"dt": 180.0, "az": 50.0, "el": 15.0},
                                {"dt": 360.0, "az": 55.0, "el": 20.0},
                                {"dt": 540.0, "az": 60.0, "el": 25.0},
                                {"dt": 720.0, "az": 65.0, "el": 30.0},
                                {"dt": 900.0, "az": 70.0, "el": 35.0},
                            ],
                        },
                    ],
                },
            },
        },
    ],
}
```

```

        },
    }
},
)

ephemeris_id = ephemeris_response["ephemerisId"]
print(f"Created ephemeris: {ephemeris_id}")

# Wait for ephemeris to become ENABLED
while True:
    status = ground_station_client.describe_ephemeris(ephemerisId=ephemeris_id)[
        "status"
    ]
    if status == "ENABLED":
        print("Ephemeris is ENABLED")
        break
    elif status in ["INVALID", "ERROR"]:
        raise RuntimeError(f"Ephemeris failed: {status}")
    time.sleep(5)

# List available contacts
print("Listing available contacts...")
contacts = ground_station_client.list_contacts(
    # Note: satelliteArn is omitted for azimuth elevation ephemeris
    groundStation="Ohio 1",
    missionProfileArn="arn:aws:groundstation:us-east-2:111122223333:mission-profile/
example-profile",
    startTime=datetime(2024, 3, 15, 10, 0, 0, tzinfo=timezone.utc),
    endTime=datetime(2024, 3, 15, 10, 15, 0, tzinfo=timezone.utc),
    statusList=["AVAILABLE"],
    ephemeris={"azEl": {"id": ephemeris_id}},
)

if contacts["contactList"]:
    # Reserve the first available contact
    contact = contacts["contactList"][0]
    print(f"Reserving contact from {contact['startTime']} to {contact['endTime']}...")

    reservation = ground_station_client.reserve_contact(
        # Note: satelliteArn is omitted when using azimuth elevation ephemeris
        missionProfileArn="arn:aws:groundstation:us-east-2:111122223333:mission-
profile/example-profile",
        groundStation="Ohio 1",
        startTime=contact["startTime"],

```

```

        endTime=contact["endTime"],
        trackingOverrides={
            "programTrackSettings": {"azEl": {"ephemerisId": ephemeris_id}}
        },
    )

    print(f"Reserved contact: {reservation['contactId']}")
else:
    print("No available contacts found")

```

Ejemplo: Listar y reservar con efemérides TLE

```

import boto3
from datetime import datetime, timedelta, timezone
import time

# Create AWS Ground Station client
ground_station_client = boto3.client("groundstation")

satellite_id = "12345678-1234-1234-1234-123456789012"
satellite_arn = f"arn:aws:groundstation::111122223333:satellite/{satellite_id}"

# Create TLE ephemeris
print("Creating TLE ephemeris...")
ephemeris_response = ground_station_client.create_ephemeris(
    name="TLE Ephemeris for Contact",
    satelliteId=satellite_id,
    enabled=True,
    expirationTime=datetime.now(timezone.utc) + timedelta(days=7),
    priority=1, # Higher priority than default ephemeris
    ephemeris={
        "tle": {
            "tleData": [
                {
                    "tleLine1": "1 25994U 99068A 24075.54719794 .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),
                    },
                },
            ],
        }
    }
)

```

```

    ]
    }
},
)

ephemeris_id = ephemeris_response["ephemerisId"]
print(f"Created ephemeris: {ephemeris_id}")

# Wait for ephemeris to become ENABLED
while True:
    status = ground_station_client.describe_ephemeris(ephemerisId=ephemeris_id)[
        "status"
    ]
    if status == "ENABLED":
        print("Ephemeris is ENABLED")
        break
    elif status in ["INVALID", "ERROR"]:
        raise RuntimeError(f"Ephemeris failed: {status}")
    time.sleep(5)

# List available contacts
print("Listing available contacts...")
start_time = datetime.now(timezone.utc) + timedelta(hours=1)
end_time = start_time + timedelta(days=1)

contacts = ground_station_client.list_contacts(
    satelliteArn=satellite_arn, # Required for TLE/OEM ephemeris
    groundStation="Hawaii 1",
    missionProfileArn="arn:aws:groundstation:us-west-2:111122223333:mission-profile/
example-profile",
    startTime=start_time,
    endTime=end_time,
    statusList=["AVAILABLE"],
)

if contacts["contactList"]:
    # Reserve the first available contact
    contact = contacts["contactList"][0]
    print(f"Reserving contact from {contact['startTime']} to {contact['endTime']}...")

    reservation = ground_station_client.reserve_contact(
        satelliteArn=satellite_arn, # Required for TLE/OEM ephemeris
        missionProfileArn="arn:aws:groundstation:us-west-2:111122223333:mission-
profile/example-profile",

```

```

    groundStation="Hawaii 1",
    startTime=contact["startTime"],
    endTime=contact["endTime"],
    # Note: trackingOverrides is optional for TLE/OEM
    # The system will use the highest priority ephemeris automatically
)

print(f"Reserved contact: {reservation['contactId']}")
else:
    print("No available contacts found")

```

Flujo de trabajo 2: reserva por contacto directo

Este flujo de trabajo reserva directamente un contacto sin enumerar primero las ventanas disponibles. Este enfoque es útil cuando ya sabe la hora de contacto deseada o si está implementando una programación automatizada.

Ejemplo: reserva directa con efemérides de elevación acimutal

```

import boto3
from datetime import datetime, timezone
import time

# Create AWS Ground Station client
ground_station_client = boto3.client("groundstation")

# Define contact window
contact_start = datetime(2024, 3, 20, 14, 0, 0, tzinfo=timezone.utc)
contact_end = datetime(2024, 3, 20, 14, 15, 0, tzinfo=timezone.utc)

# Create azimuth elevation ephemeris for the specific contact time
print("Creating azimuth elevation ephemeris...")
ephemeris_response = ground_station_client.create_ephemeris(
    name="Direct Contact AzEl Ephemeris",
    ephemeris={
        "azEl": {
            "groundStation": "Ohio 1",
            "data": {
                "azElData": {
                    "angleUnit": "DEGREE_ANGLE",
                    "azElSegmentList": [
                        {
                            "referenceEpoch": contact_start.isoformat(),

```

```

        "validTimeRange": {
            "startTime": contact_start.isoformat(),
            "endTime": contact_end.isoformat(),
        },
        "azElList": [
            {"dt": 0.0, "az": 45.0, "el": 10.0},
            {"dt": 180.0, "az": 50.0, "el": 15.0},
            {"dt": 360.0, "az": 55.0, "el": 20.0},
            {"dt": 540.0, "az": 60.0, "el": 25.0},
            {"dt": 720.0, "az": 65.0, "el": 30.0},
            {"dt": 900.0, "az": 70.0, "el": 35.0},
        ],
    ],
}
},
),
)

ephemeris_id = ephemeris_response["ephemerisId"]
print(f"Created ephemeris: {ephemeris_id}")

# Wait for ephemeris to become ENABLED
while True:
    status = ground_station_client.describe_ephemeris(ephemerisId=ephemeris_id)[
        "status"
    ]
    if status == "ENABLED":
        print("Ephemeris is ENABLED")
        break
    elif status in ["INVALID", "ERROR"]:
        raise RuntimeError(f"Ephemeris failed: {status}")
    time.sleep(5)

# Directly reserve the contact
print(f"Reserving contact from {contact_start} to {contact_end}...")

reservation = ground_station_client.reserve_contact(
    # Note: satelliteArn is omitted for azimuth elevation
    missionProfileArn="arn:aws:groundstation:us-east-2:111122223333:mission-profile/
example-profile",
    groundStation="Ohio 1",
    startTime=contact_start,

```

```

    endTime=contact_end,
    trackingOverrides={"programTrackSettings": {"azEl": {"ephemerisId":
ephemeris_id}}},
)

print(f"Reserved contact: {reservation['contactId']}")

```

Ejemplo: reserva directa con efemérides TLE

```

import boto3
from datetime import datetime, timedelta, timezone
import time

# Create AWS Ground Station client
ground_station_client = boto3.client("groundstation")

satellite_id = "12345678-1234-1234-1234-123456789012"
satellite_arn = f"arn:aws:groundstation::111122223333:satellite/{satellite_id}"

# Define contact window (based on predicted pass)
contact_start = datetime(2024, 3, 21, 10, 30, 0, tzinfo=timezone.utc)
contact_end = datetime(2024, 3, 21, 10, 42, 0, tzinfo=timezone.utc)

# Create TLE ephemeris
print("Creating TLE ephemeris...")
ephemeris_response = ground_station_client.create_ephemeris(
    name="Direct Contact TLE Ephemeris",
    satelliteId=satellite_id,
    enabled=True,
    expirationTime=contact_end + timedelta(days=1),
    priority=1,
    ephemeris={
        "tle": {
            "tleData": [
                {
                    "tleLine1": "1 25994U 99068A 24080.50000000 .00000075 00000-0
26688-4 0 9999",
                    "tleLine2": "2 25994 98.2007 35.6589 0001234 89.2782 18.9934
14.57114995112000",
                    "validTimeRange": {
                        "startTime": (contact_start - timedelta(hours=1)).isoformat(),
                        "endTime": (contact_end + timedelta(hours=1)).isoformat(),
                    },
                },
            ],
        },
    },
)

```

```

        }
    ]
}
},
)

ephemeris_id = ephemeris_response["ephemerisId"]
print(f"Created ephemeris: {ephemeris_id}")

# Wait for ephemeris to become ENABLED
while True:
    status = ground_station_client.describe_ephemeris(ephemerisId=ephemeris_id)[
        "status"
    ]
    if status == "ENABLED":
        print("Ephemeris is ENABLED")
        break
    elif status in ["INVALID", "ERROR"]:
        raise RuntimeError(f"Ephemeris failed: {status}")
    time.sleep(5)

# Directly reserve the contact
print(f"Reserving contact from {contact_start} to {contact_end}...")

reservation = ground_station_client.reserve_contact(
    satelliteArn=satellite_arn, # Required for TLE ephemeris
    missionProfileArn="arn:aws:groundstation:us-west-2:111122223333:mission-profile/
example-profile",
    groundStation="Hawaii 1",
    startTime=contact_start,
    endTime=contact_end,
    # Note: trackingOverrides is optional for TLE
    # The system will use the highest priority ephemeris automatically
)

print(f"Reserved contact: {reservation['contactId']}")

```

Supervisión de los cambios de estado de los contactos

Tras reservar un contacto, es importante supervisar su estado para garantizar que la transición a un contacto se realice correctamente SCHEDULED y se le notifique cualquier problema. AWS Ground Station emite eventos a Amazon EventBridge para todos los cambios de estado de contacto.

Los estados de contacto siguen este ciclo de vida:

- SCHEDULING- El contacto se está procesando para su programación
- SCHEDULED- El contacto se programó correctamente y se ejecutará
- FAILED_TO_SCHEDULE- No se ha podido programar el contacto (estado terminal)

Para obtener más información sobre los estados y el ciclo de vida de los contactos, consulte [Comprenda el ciclo de vida de](#).

Implementar la supervisión del estado de los contactos con EventBridge

Para monitorizar los cambios de estado de los contactos en tiempo real, puedes configurar una EventBridge regla de Amazon que active una función Lambda cada vez que un contacto de Ground Station cambie de estado. Este enfoque es más eficiente y escalable que sondear el estado del contacto.

Pasos para la implementación

1. Cree una función Lambda para procesar eventos de cambio de estado de contacto
2. Cree una EventBridge regla que coincida con los eventos de cambio de estado de contacto de Ground Station
3. Agregue la función Lambda como objetivo de la regla

Ejemplo de controlador de funciones Lambda

Para ver un ejemplo completo de una función Lambda que procesa eventos de cambio de estado de contacto, consulte el `GroundStationCloudWatchEventHandlerLambda` recurso de la `AquaSnppJpssTerraDigIF.yml` CloudFormation plantilla. Esta plantilla está disponible en el bucket de Amazon S3 que se está incorporando AWS Ground Station al cliente. Para obtener instrucciones sobre cómo acceder a esta plantilla, consulte la [Poniéndolo todo junto](#) sección del ejemplo del punto final del flujo de datos.

EventBridge configuración de reglas

La EventBridge regla debe usar el siguiente patrón de eventos para que coincida con todos los cambios de estado de contacto de Ground Station:

```
{
```

```
"source": ["aws.groundstation"],
"detail-type": ["Ground Station Contact State Change"]
}
```

Para filtrar únicamente por estados específicos (por ejemplo, errores), puedes añadir un filtro detallado:

```
{
  "source": ["aws.groundstation"],
  "detail-type": ["Ground Station Contact State Change"],
  "detail": {
    "contactStatus": [
      "FAILED_TO_SCHEDULE",
      "FAILED",
      "AWS_FAILED",
      "AWS_CANCELLED"
    ]
  }
}
```

Para obtener instrucciones detalladas sobre la creación de EventBridge reglas con objetivos Lambda, consulte [Creación de reglas que reaccionen a los eventos](#) en la Guía EventBridge del usuario de Amazon.

Configuración de EventBridge reglas para la automatización

Puede crear EventBridge reglas para responder automáticamente a los cambios de estado de los contactos. Por ejemplo:

- Envía notificaciones cuando un contacto no pueda programar una cita
- Activa funciones Lambda para preparar los recursos cuando entra un contacto PREPASS
- Registre las terminaciones de los contactos con fines de auditoría

Para obtener información detallada sobre cómo configurar EventBridge las reglas para AWS Ground Station los eventos, consulte [Automatiza AWS Ground Station con eventos](#).

Prácticas recomendadas y consideraciones

Gestión de conflictos de programación

Como AWS Ground Station las antenas son recursos compartidos, es ListContacts posible que otro cliente reserve una ventana de contacto que aparece disponible en antes de que tú puedas reservarla. Para gestionar esto:

1. Compruebe siempre el estado de contacto después de la reserva
2. Implemente la lógica de reintento con ventanas de tiempo alternativas
3. Considere la posibilidad de reservar los contactos con bastante antelación siempre que sea posible
4. Utilice EventBridge los eventos para monitorear los estados FAILED_TO_SCHEDULE

Tiempo de validación de efemérides

Recuerda que las efemérides deben estar en ENABLED estado para poder usarlas para reservar contactos. El proceso de validación suele tardar entre unos segundos y unos minutos, según el tipo y el tamaño de las efemérides. Compruebe siempre el estado de las efemérides antes de intentar reservar los contactos.

Consideraciones sobre el tiempo de contacto

Al usar efemérides personalizadas:

- Asegúrate de que tus efemérides cubran toda la duración del contacto
- [En el caso de las efemérides de elevación acimutal, compruebe que los ángulos mantienen la antena por encima de la máscara de sitio durante todo el contacto](#)
- Tenga en cuenta los tiempos de caducidad de las efemérides al programar futuros contactos

Diferencias de API por tipo de efemérides

La ReserveContact API se comporta de forma diferente según el tipo de efemérides:

Tipo de efemérides	Se requiere un ARN satelital	Es obligatorio rastrear las anulaciones
TLE	Sí	No (opcional)
OEM	Sí	No (opcional)
Elevación del acimut	No (opcional)	Sí

Comprenda qué efemérides se utilizan

Las efemérides tienen una prioridad, un tiempo de caducidad y un indicador de activación. En conjunto, determinan qué efemérides se utilizan para el seguimiento durante un contacto.

Efemérides TLE y OEM

En el caso de las efemérides OEM y TLE, solo puede haber una efeméride activa para cada satélite. La efeméride que se utiliza es la que 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 [ListContacts](#) se 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.](#)

Efemérides de elevación azimutal

Las efemérides de elevación azimutal funcionan de manera diferente a las efemérides OEM y TLE. Cada efeméride de elevación acimutal está asociada a una estación terrestre específica y no tiene prioridad. Al reservar un contacto con efemérides de elevación de acimut, se especifica explícitamente qué efemérides de elevación de acimut se van a utilizar a través del parámetro `trackingOverrides`.

Diferencias clave entre las efemérides de elevación azimutal:

- Sin sistema de prioridad: se seleccionan de forma explícita las efemérides de cada contacto
- Estación terrestre específica: cada efeméride está asociada a una estación terrestre concreta
- Sin respaldo automático: si la efeméride especificada no está disponible, el contacto fallará

Note

Las efemérides de elevación de acimut no compiten con las efemérides OEM y TLE. Se seleccionan de forma explícita al reservar un contacto y solo se utilizan cuando se especifican las anulaciones de seguimiento.

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.

En el caso de las efemérides OEM y TLE, 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, es posible que se reduzca el tiempo de contacto del satélite con la antena debido a que la nave espacial opera fuera de la máscara de ubicación. `transmit/receive` 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 `transmit/receive` sitio comparando

su contacto `startTime` programado `endTime` con el devuelto `visibilityStartTime` y `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](#).

Para las efemérides de elevación acimutal, los contactos programados utilizarán las efemérides específicas que se seleccionaron al reservar el contacto. Si necesita actualizar los datos de elevación de acimut de un contacto programado, puede cancelar y reprogramar el contacto con una efeméride nueva.

Obtén 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

Note

Las efemérides de elevación acimutal no están asociadas a los satélites y, por lo tanto, no las devuelven ni. [GetSatelliteListSatellites](#) Para recuperar información sobre las efemérides de elevación del acimut, usa la [DescribeEphemeris](#) API con el ID de efemérides específico o úsala para ver todas las efemérides disponibles en tu cuenta. [ListEphemerides](#)

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-EXAMPLE",
  "satelliteArn": "arn:aws:groundstation::111122223333:satellite/e1cfe0c7-67f9-4d98-bad2-EXAMPLE",
  "noradSatelliteID": 25994,
  "groundStations": [
    "Ohio 1",
    "Oregon 1"
  ],
  "currentEphemeris": {
    "source": "SPACE_TRACK",
    "epoch": 1528245583.619
  }
}
```

Ejemplo [GetSatellite](#) para un satélite que utiliza una efeméride predeterminada

```
{
  "satelliteId": "e1cfe0c7-67f9-4d98-bad2-EXAMPLE",
  "satelliteArn": "arn:aws:groundstation::111122223333:satellite/e1cfe0c7-67f9-4d98-bad2-EXAMPLE",
  "noradSatelliteID": 25994,
  "groundStations": [
    "Ohio 1",
    "Oregon 1"
  ],
  "currentEphemeris": {
    "source": "CUSTOMER_PROVIDED",
    "ephemerisId": "e1cfe0c7-67f9-4d98-bad2-EXAMPLE",
    "name": "My Ephemeris"
  }
}
```

Listado de efemérides de elevación azimutal

Como las efemérides de elevación azimutal no están asociadas a los satélites, es necesario utilizar diferentes para descubrirlas y recuperar información sobre ellas: APIs

1. Utilízalo [ListEphemerides](#) para enumerar todas las efemérides de tu cuenta, incluidas las efemérides de elevación azimutal. Puedes filtrar por estado y tipo de efemérides.
2. [DescribeEphemeris](#) Utilízalo con un identificador de efemérides específico para obtener información detallada sobre una efeméride de elevación azimutal.
3. Úsalo [DescribeContact](#) con un ID de contacto específico para obtener información detallada sobre una efeméride utilizada para el contacto.

Ejemplo de [ListEphemerides](#) respuesta que incluye una efeméride de elevación acimutal:

```
{
  "ephemerides": [
    {
      "ephemerisId": "abc12345-6789-def0-1234-5678EXAMPLE",
      "ephemerisType": "AZ_EL",
      "name": "Azimuth Elevation for Ohio Ground Station",
      "status": "ENABLED",
      "creationTime": 1620254718.765
    },
    {
      "ephemerisId": "def45678-9012-abc3-4567-8901EXAMPLE",
      "ephemerisType": "TLE",
      "name": "TLE for Satellite 12345",
      "status": "ENABLED",
      "creationTime": 1620254700.123
    }
  ]
}
```

Note

En la [ListEphemerides](#) respuesta, las efemérides de elevación acimutal tendrán un campo en lugar de un `groundStation` campo, lo que facilitará su identificación. `satelliteId`

Vuelva 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.

Note

Las efemérides de elevación acimutal no tienen valores predeterminados y no anulan las efemérides de los satélites. Se seleccionan de forma explícita al reservar un contacto mediante el parámetro. `trackingOverrides` Si ya no desea utilizar las efemérides de elevación acimutal, simplemente reserve los contactos sin especificar las anulaciones de seguimiento y el sistema utilizará en su lugar las efemérides de satélite activas.

Reversión de efemérides TLE y OEM

Para volver a las efemérides [Space-Track](#) predeterminadas de un satélite, deberá realizar una de las siguientes acciones:

- Borrar (usando [DeleteEphemeris](#)) o deshabilitar (usando [UpdateEphemeris](#)) todas las efemérides proporcionadas por el cliente. Puede enumerar las efemérides proporcionadas por el cliente para un satélite usando [ListEphemerides](#).
- Esperar a que caduquen todas las efemérides proporcionadas por el cliente.

Puede confirmar que se están utilizando las efemérides predeterminadas llamando a [GetSatellite](#) y verificando que la `source` de las efemérides actuales para el satélite es `SPACE_TRACK`. Consulte para [Datos de efemérides predeterminados](#) obtener más información sobre las efemérides predeterminadas.

Gestión de efemérides de elevación azimutal

Dado que las efemérides de elevación del acimut se seleccionan de forma explícita para cada contacto y no están asociadas a los satélites, no existe la idea de «volver» a un valor

predeterminado. En su lugar, puede gestionar las efemérides de elevación azimutal de la siguiente manera:

- Para dejar de usar efemérides de elevación azimutal: basta con reservar nuevos contactos sin especificar ni especificar un `trackingOverrides.satelliteArn`. En su lugar, el contacto utilizará las efemérides activas para el satélite especificado.
- Para eliminar las efemérides de elevación de acimut no utilizadas: utilice esta opción [DeleteEphemeris](#) para eliminar las efemérides de elevación de acimut que ya no se necesitan. Tenga en cuenta que no puede eliminar una efeméride que esté siendo utilizada actualmente por un contacto programado.

Para ver todas las efemérides de elevación acimutal de tu cuenta, utiliza [ListEphemerides](#)

Las efemérides de elevación acimutal se pueden identificar mediante el campo `ephemerisType` o mediante la presencia de un `ephemerisType` campo en lugar de un campo `groundStationSatelliteId` en la respuesta.

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 según 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.

- `antenna`: enlace descendente
 - (Ancho de banda `less-than-or-equal`: hasta 40MHz) los datos se entregan como paquetes de datos de señal/formato IP [VITA-49](#).
 - (Ancho de banda superior a 40MHz) los datos se entregan como paquetes de clase 2. AWS Ground Station

- antenna-downlink-demod-decode
 - Los datos se entregan como paquetes de formato de Demodulated/Decoded datos/IP.
- 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 AWS región 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 Ubicaciones](#) que esté incorporado.

Cuando reciba sus datos de contacto en un Amazon S3 Bucket, AWS Ground Station gestionará todos los aspectos de la entrega por usted.

Para utilizar la entrega de datos entre regiones a una EC2 instancia de Amazon (mediante el AWS Ground Station agente o un punto de enlace de flujo de datos), el punto de enlace del flujo de datos debe crearse en su región de AWS actual y debe especificar la misma región. dataflow-endpoint-config AWS Ground Station se encargará de entregarle los datos entre regiones.

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.

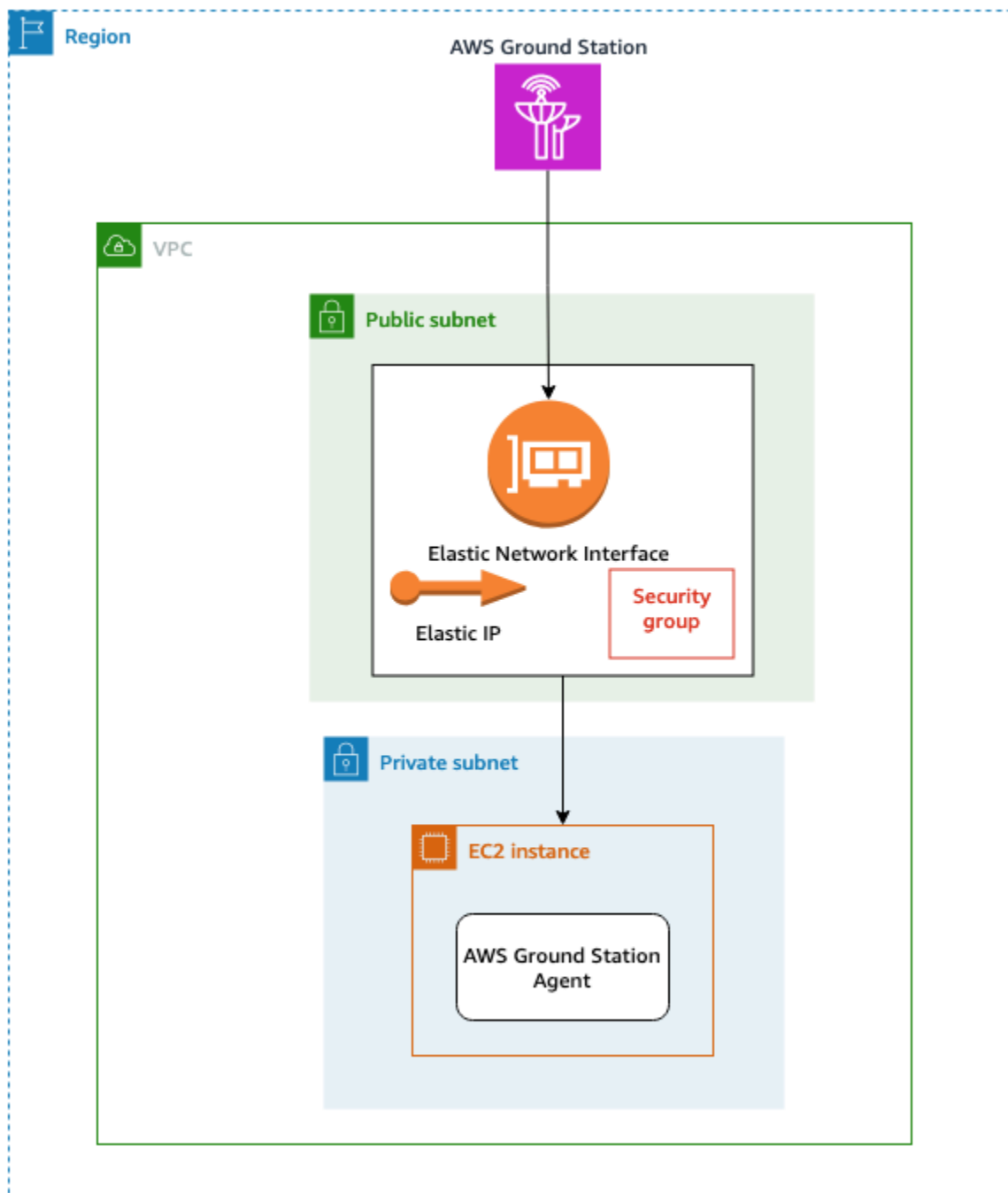
Consulte [Config de grabación de Amazon S3](#) las restricciones sobre el bucket de Amazon S3, el rol de IAM o la creación de AWS Ground Station configuraciones.

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 se espera de un solo 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 y, 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.

Note

La cuota predeterminada para el número de grupos de seguridad conectados por ENI es de 5. Se trata de un límite ajustable de hasta 16 (consulta las cuotas de [Amazon VPC](#)).

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:

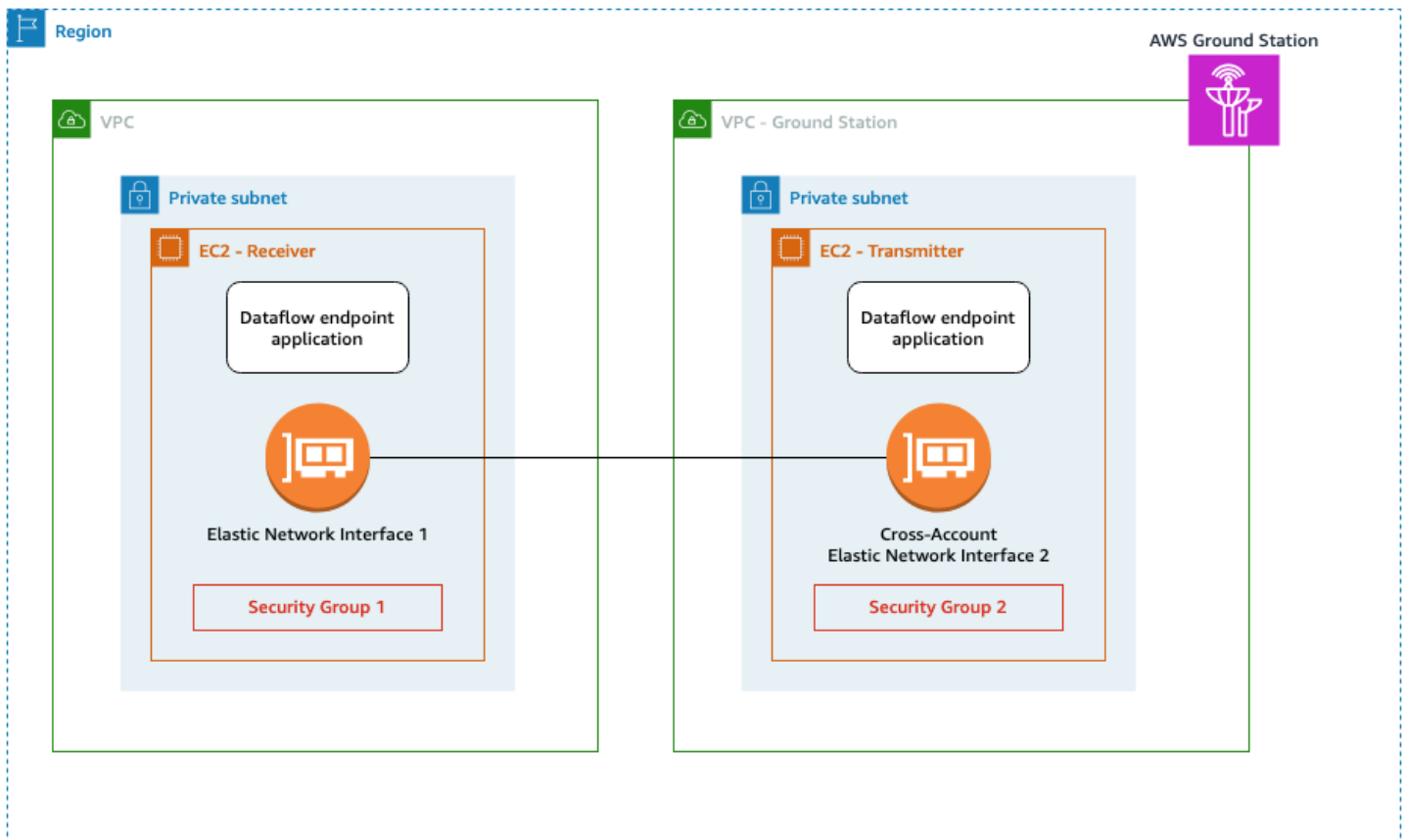
AllocationId:

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 que está 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.

Note

La cuota predeterminada para el número de grupos de seguridad adjuntos por ENI es de 5. Se trata de un límite ajustable de hasta 16 (consulta las cuotas de [Amazon VPC](#)).

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, consulte [Utilice 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 subnet 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, consulte [AWS 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 \(AMIs\)](#).

Trabaje con telemetría

AWS Ground Station La telemetría proporciona métricas casi en tiempo real de las AWS Ground Station antenas durante sus contactos por satélite. Puede utilizar los datos de telemetría para supervisar el rendimiento de los contactos, detectar anomalías y tomar decisiones informadas sobre sus comunicaciones por satélite.

Cómo funciona la telemetría

Para usar la telemetría, debe configurar una `TelemetrySinkConfig` que especifique dónde AWS Ground Station deben entregarse los datos de telemetría. A continuación, añada esta configuración al perfil de su misión mediante el campo `telemetrySinkConfigArn`. Durante los contactos que utilizan un perfil de misión con telemetría, transmiten los datos de AWS Ground Station telemetría a tu cuenta.

El proceso de entrega telemétrica funciona de la siguiente manera:

1. Cree una transmisión de Kinesis Data Streams en AWS su cuenta para recibir datos de telemetría. La transmisión debe crearse en la misma cuenta y región desde las que programa sus contactos.
2. Creas un rol de IAM que otorga AWS Ground Station permiso para escribir datos en tu transmisión.
3. Creas una `TelemetrySinkConfig` que haga referencia a tu transmisión y a tu función de IAM.
4. Lo añades `TelemetrySinkConfig` al perfil de tu misión.
5. Puede enumerar y reservar contactos mediante el nuevo perfil de misión con telemetría.
6. Durante los contactos que utilizan este perfil de misión, AWS Ground Station transmite los datos de telemetría a su transmisión de Kinesis Data Streams prácticamente en tiempo real.
7. Usted consume y procesa los datos de telemetría de su transmisión mediante AWS servicios o sus propias aplicaciones.

Tipos de telemetría disponibles

AWS Ground Station proporciona los siguientes tipos de telemetría durante los contactos:

Note

AWS Ground Station está trabajando para ampliar el número de tipos de telemetría compatibles

Telemetría de puntería

Proporciona información sobre la dirección de orientación de la antena durante los contactos con el satélite. Este tipo de telemetría se envía siempre durante un contacto e incluye los ángulos de elevación y acimut reales y controlados. Para obtener más información, consulte [Telemetría de puntería](#).

Telemetría de seguimiento

Proporciona información sobre el estado del rastreo de la antena y los errores de rastreo. Este tipo de telemetría se envía cuando el seguimiento automático está activado en la configuración de seguimiento. Para obtener más información, consulte [Telemetría de seguimiento](#).

Disponibilidad regional

La telemetría está disponible en todas las regiones en las AWS que opera. AWS Ground Station Durante la ejecución del contacto, la telemetría se enviará desde la AWS Ground Station antena a la región desde la que programó el contacto, lo que le proporcionará asistencia en todas las regiones.

Para obtener una lista completa de AWS Ground Station las regiones y ubicaciones de las estaciones terrestres, consulte. [AWS Ground Station Ubicaciones](#)

Temas

- [Configure la telemetría](#)
- [Comprenda los datos de telemetría](#)

Configure la telemetría

Sigue estos pasos para configurar la telemetría de tus contactos. AWS Ground Station Tras completar esta configuración, los datos de telemetría se enviarán a la transmisión de Kinesis Data Streams durante los contactos que utilicen un perfil de misión con telemetría habilitada. Para obtener

información detallada sobre Kinesis Data Streams, consulte la Guía [del usuario de Kinesis Data Streams](#).

Paso 1: Cree los recursos necesarios AWS

En el siguiente CloudFormation fragmento se muestra cómo crear los AWS recursos necesarios para la entrega de telemetría. Este fragmento crea una transmisión de Kinesis Data Streams y una función de IAM que concede AWS Ground Station permiso para escribir datos de telemetría en la transmisión.

TelemetryStream:

```
Type: AWS::Kinesis::Stream
Properties:
  Name: GroundStationTelemetryStream
  StreamModeDetails:
    StreamMode: ON_DEMAND
  RetentionPeriodHours: 24
```

TelemetryRole:

```
Type: AWS::IAM::Role
Properties:
  RoleName: GroundStationTelemetryRole
  AssumeRolePolicyDocument:
    Version: '2012-10-17'
    Statement:
      - Effect: Allow
        Principal:
          Service: groundstation.amazonaws.com
        Action: sts:AssumeRole
  Policies:
    - PolicyName: KinesisWritePolicy
      PolicyDocument:
        Version: '2012-10-17'
        Statement:
          - Effect: Allow
            Action:
              - kinesis:DescribeStream
              - kinesis:PutRecord
              - kinesis:PutRecords
            Resource: !GetAtt TelemetryStream.Arn
```

La siguiente lista incluye consideraciones de configuración específicas al configurar la entrega de telemetría para AWS Ground Station

Transmisión de Kinesis Data Streams: la transmisión utiliza el modo de capacidad bajo demanda, que se escala automáticamente en función del rendimiento. Esto se recomienda para la mayoría de los casos de uso. La transmisión está configurada para conservar los datos durante 24 horas. De forma predeterminada, la transmisión utiliza un cifrado AWS gestionado. Para utilizar el cifrado administrado por el cliente AWS Key Management Service, añada la `StreamEncryption` propiedad y actualice la política de funciones de IAM para incluir los permisos. `kms:GenerateDataKey` Para obtener más información, consulte [Protección de datos en Amazon Kinesis Data Streams](#).

Función de IAM: la función de IAM permite al director del `groundstation.amazonaws.com` servicio asumir la función y escribir datos de telemetría en la transmisión de Kinesis Data Streams. La política de roles otorga permisos y `kinesis:PutRecords` acciones `kinesis:DescribeStream` en la `kinesis:PutRecord` transmisión. Consulte [Config del disipador de telemetría](#) para obtener orientación sobre cómo configurar la política de confianza y la política de roles.

Configuración adicional: añada `iam:PassRole` permisos al usuario o rol de IAM que utilizas para las llamadas a la AWS Ground Station API. Esto le permite transferir la función de telemetría AWS Ground Station al crear un `TelemetrySinkConfig`

Ejemplo de política PassRole

Para obtener más información sobre cómo actualizar o adjuntar una política de funciones, consulte [Gestión de las políticas de IAM](#) en la Guía del usuario de IAM. Para obtener más información sobre el `iam:PassRole` permiso, consulte [Otorgar permisos a un usuario para transferir un rol a un servicio de AWS](#)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetRole",
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::999999999999:role/your-telemetry-delivery-role-name"
    }
  ]
}
```

```
]
}
```

Paso 2: Crear un TelemetrySinkConfig

Cree una `TelemetrySinkConfig` que defina cómo AWS Ground Station se entregarán los datos de telemetría a su transmisión de Kinesis Data Streams. Utilice el ARN de flujo y el ARN de rol de las salidas de la CloudFormation pila en el paso 1.

Note

Cuando cree una `TelemetrySinkConfig`, AWS Ground Station verificará el acceso a su transmisión de Kinesis Data Streams entregando un registro de prueba vacío con una clave `test` de partición de.

Para obtener más información sobre la creación de una `TelemetrySinkConfig`, consulte [Config del disipador de telemetría](#).

Paso 3: Añade la telemetría al perfil de tu misión

Crea un perfil de misión. Para obtener más información sobre la creación de perfiles de misión, consulte [Usa perfiles AWS Ground Station de misión](#). `telemetrySinkConfigArn` Añádalo al perfil de su misión para activar la telemetría durante los contactos. Utilice el ARN del `TelemetrySinkConfig` creado en el paso 2.

Paso 4: programar un contacto

Programa un contacto utilizando tu perfil de misión con telemetría. Durante el contacto, AWS Ground Station transmitirá los datos de telemetría a su transmisión de Kinesis Data Streams.

¿Qué esperar durante los contactos

- Inicio por telemetría: los datos comienzan a transmitirse a medida que se inicia el contacto.
- Entrega casi en tiempo real: la telemetría llega a su transmisión de Kinesis Data Streams prácticamente en tiempo real.
- Duración del contacto: los datos se conservan durante todo el contacto.

- Parada automática: la telemetría detiene la transmisión cuando finaliza el contacto.

Supervisión de la entrega

Puede monitorear la entrega de telemetría mediante:

- Métricas de transmisión de Kinesis Data Streams: compruebe los registros CloudWatch entrantes. Para obtener más información, consulte [Supervisión de Amazon Kinesis Data Streams](#).
- Registros de aplicaciones: compruebe el procesamiento de datos en las aplicaciones que consumen contenido de la transmisión.
- Visor de datos de Kinesis: utilice la consola de transmisiones de Kinesis Data Streams para ver los registros de muestra de su transmisión.

Siguientes pasos

Tras completar la configuración, puede:

- Obtenga información sobre el formato de datos de telemetría y los tipos de telemetría disponibles. Consulte [Comprenda los datos de telemetría](#).
- Cree aplicaciones para procesar los datos de telemetría de su transmisión de Kinesis Data Streams. Para obtener más información, consulte [Creación de consumidores para Amazon Kinesis Data Streams](#).
- Cree paneles y alertas mediante CloudWatch y otros AWS servicios.
- Consulte la guía de solución de problemas si encuentra algún problema. Consulte [Solucionar problemas de telemetría](#).

Comprenda los datos de telemetría

Los datos de telemetría se envían como registros JSON codificados en Base64 a su transmisión de Kinesis Data Streams. Cada registro contiene información recopilada durante el contacto con el satélite, incluidos los metadatos sobre el contacto y las mediciones telemétricas muestreadas.

Descripción general del formato de datos

Cada registro de telemetría contiene los siguientes componentes:

Tipo y versión de telemetría

Identifica el tipo específico de datos de telemetría y su versión de esquema. Esto le permite analizar diferentes tipos de telemetría de forma adecuada. Para obtener más información sobre el control de versiones de esquemas, consulte. [Evolución y control de versiones del esquema](#)

ID de ámbito

Un identificador único para el alcance de la telemetría. Esto le permite correlacionar los datos de telemetría con contactos específicos.

Metadatos

Información contextual sobre la telemetría.

Datos

Las medidas de telemetría muestreadas específicas del tipo de telemetría.

Clave de partición

Los registros de telemetría se envían a la transmisión de Kinesis Data Streams con una clave de partición en el formato:

```
SCOPE#scopeId#TELEMETRY_ID#telemetryId#TELEMETRY_VERSION#telemetryVersion
```

Esta clave de partición garantiza que toda la telemetría de un tipo determinado para un solo contacto se entregue a la misma partición dentro de la transmisión de Kinesis Data Streams, lo que permite ordenar al máximo la transmisión de telemetría de ese contacto.

Telemetría de puntería

La telemetría de puntería proporciona información sobre la dirección de apuntamiento de la antena durante los contactos con el satélite. Este tipo de telemetría siempre se envía durante un contacto.

Campos de datos

Ejemplo de marca de tiempo

Hora en que se muestrearon los datos de telemetría, en formato ISO-8601 en UTC con una precisión de milisegundos.

azimut

Ángulo acimutal real de la antena en grados.

elevación

Ángulo de elevación real de la antena en grados.

Comandó Azimuth

Ángulo acimutal controlado en grados. Este es el ángulo acimutal objetivo que la antena intenta alcanzar.

Elevación ordenada

Ángulo de elevación controlado en grados. Este es el ángulo de elevación objetivo que la antena intenta alcanzar.

Note

La posición real de la antena puede diferir de la posición ordenada debido a limitaciones físicas o retrasos mecánicos durante el contacto.

Campos de metadatos

Estación terrestre

Nombre de la estación terrestre (por ejemplo, «Ohio 1”).

ID del satélite

Identificador del recurso satelital en. AWS Ground Station

contactId

Identificador del contacto.

Ejemplo: JSON

```
{
  "telemetryTypeAndVersion": "POINTING#1.0.0",
  "telemetryType": "POINTING",
```

```
"telemetryVersion": "1.0.0",
"scopeId": "12345678-1234-1234-1234-123456789012",
"metadata": {
  "groundStation": "Ohio 1",
  "satelliteId": "87654321-4321-4321-4321-210987654321",
  "contactId": "12345678-1234-1234-1234-123456789012"
},
"data": {
  "sampleTimestamp": "2025-12-08T12:00:00.123Z",
  "azimuth": 180.5,
  "elevation": 45.2,
  "commandedAzimuth": 180.0,
  "commandedElevation": 45.0
}
}
```

Telemetría de seguimiento

La telemetría de seguimiento proporciona información sobre el estado del seguimiento de la antena y los errores de seguimiento. Este tipo de telemetría se envía cuando el seguimiento automático está activado en la configuración de seguimiento y cuando la antena utiliza activamente el seguimiento automático.

Note

Si tu autotrack parámetro TrackingConfig está establecido en, no se proporcionará ninguna REMOVED telemetría de rastreo. Para obtener más información sobre el seguimiento de las configuraciones, consulte. [Configuración de seguimiento](#)

Campos de datos

Ejemplo de marca de tiempo

Hora en que se muestrearon los datos de telemetría, en formato ISO-8601 en UTC con una precisión de milisegundos.

Estado de seguimiento

Estado de seguimiento actual de la antena. Entre los valores posibles se incluyen: TRACKING, ACQUIRING y MASKED.

trackingErrorAzimuth

Error de seguimiento en el eje acimutal, medido en grados.

trackingErrorElevation

Error de rastreo en el eje de elevación, medido en grados.

Note

Los valores de error de seguimiento representan ajustes del seguimiento del programa basado en efemérides que AWS Ground Station se aplica durante el seguimiento automático para maximizar la intensidad de la señal.

Campos de metadatos

La telemetría de seguimiento incluye los mismos campos de metadatos que la telemetría de puntería: `groundStation`, `y. satelliteId` `contactId`

Ejemplo: JSON

```
{
  "telemetryTypeAndVersion": "TRACKING#1.0.0",
  "telemetryType": "TRACKING",
  "telemetryVersion": "1.0.0",
  "scopeId": "12345678-1234-1234-1234-123456789012",
  "metadata": {
    "groundStation": "Ohio 1",
    "satelliteId": "87654321-4321-4321-4321-210987654321",
    "contactId": "12345678-1234-1234-1234-123456789012"
  },
  "data": {
    "sampleTimestamp": "2025-12-08T12:00:00.123Z",
    "trackingStatus": "TRACKING",
    "trackingErrorAzimuth": 0.2,
    "trackingErrorElevation": 0.1
  }
}
```

Lectura de datos de la transmisión de Kinesis Data Streams

Los datos de telemetría se envían a la transmisión de Kinesis Data Streams y se pueden consumir mediante patrones de consumo de transmisión estándar. Al leer los datos de la transmisión, tenga en cuenta las siguientes consideraciones.

Decodificación Base64

Los datos de la transmisión de Kinesis Data Streams están codificados en Base64. Debe decodificar los datos antes de analizarlos como JSON. Para obtener más información, consulte [Trabajar con Amazon Kinesis Data Streams](#).

Uso del visor de datos de Kinesis

Para acceder rápidamente a los datos de telemetría, la consola de streaming de Kinesis Data Streams ofrece una función de visor de datos. Al utilizar esta función:

- La transmisión por telemetría se puede realizar en cualquier fragmento de la transmisión.
- La posición inicial predeterminada se basa en los registros más recientes del fragmento.
- Es posible que necesite ajustar el fragmento seleccionado y utilizar la posición inicial «En la marca de tiempo» para ver los registros recibidos.

Uso de la biblioteca de clientes de Kinesis

La biblioteca de clientes de Kinesis (KCL) gestiona muchas de las complejidades asociadas al consumo de datos de la transmisión de Kinesis Data Streams, incluida la administración de fragmentos, los puntos de control y el equilibrio de carga. Recomendamos utilizar KCL para las aplicaciones de consumo de telemetría de producción.

Para obtener más información, consulte [Desarrollo de consumidores mediante la biblioteca de clientes de Kinesis](#).

Mejores prácticas de consumo

- Minimice la latencia: utilice un ventilador de salida mejorado para leer la transmisión de Kinesis Data Streams con un rendimiento dedicado y una latencia más baja en comparación con el sondeo. Para obtener más información, consulte [Cómo desarrollar consumidores con canales de distribución ampliados mejorados](#).

- **Transmisión dedicada:** utilice una transmisión dedicada de Kinesis Data Streams para la integración de AWS Ground Station telemetría. Compartir una transmisión con otras aplicaciones puede provocar una saturación del rendimiento de escritura y fallos en la entrega de la telemetría.
- **Capacidad bajo demanda:** Implemente su transmisión de Kinesis Data Streams en el modo de aprovisionamiento bajo demanda para permitir el escalado automático de los fragmentos en función del rendimiento.
- **Supervise el rendimiento:** supervise su transmisión para detectar posibles limitaciones mediante métricas. CloudWatch Para obtener más información, consulte [Supervisión de Amazon Kinesis Data Streams](#).

Evolución y control de versiones del esquema

Los esquemas de telemetría están versionados para adaptarse a la evolución a lo largo del tiempo. El `telemetryVersion` campo de cada registro indica la versión del esquema.

Gestionar los cambios de esquema

- Es posible que en el futuro se introduzcan nuevos tipos de telemetría.
- Es posible que los tipos de telemetría existentes reciban nuevas versiones con cambios importantes.
- Sus aplicaciones deben tolerar tipos y versiones de telemetría desconocidos.
- Analice los `telemetryVersion` campos `telemetryTypeAndVersion` y `telemetryType`, y para determinar cómo procesar cada registro.

Recomendamos implementar una serialización de cargas útil que tenga en cuenta las versiones y que permita gestionar varias versiones del esquema sin problemas, lo que permitirá que las aplicaciones sigan funcionando cuando se introduzcan nuevas versiones.

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, consulte [Introducción](#). Cuando [ReserveContact](#) se le llama, AWS Ground Station toma una instantánea del perfil de la misión y configura los recursos para utilizarlos durante todo el ciclo de vida del contacto. Los cambios que se realicen en estos recursos mediante [UpdateMissionProfile](#) 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

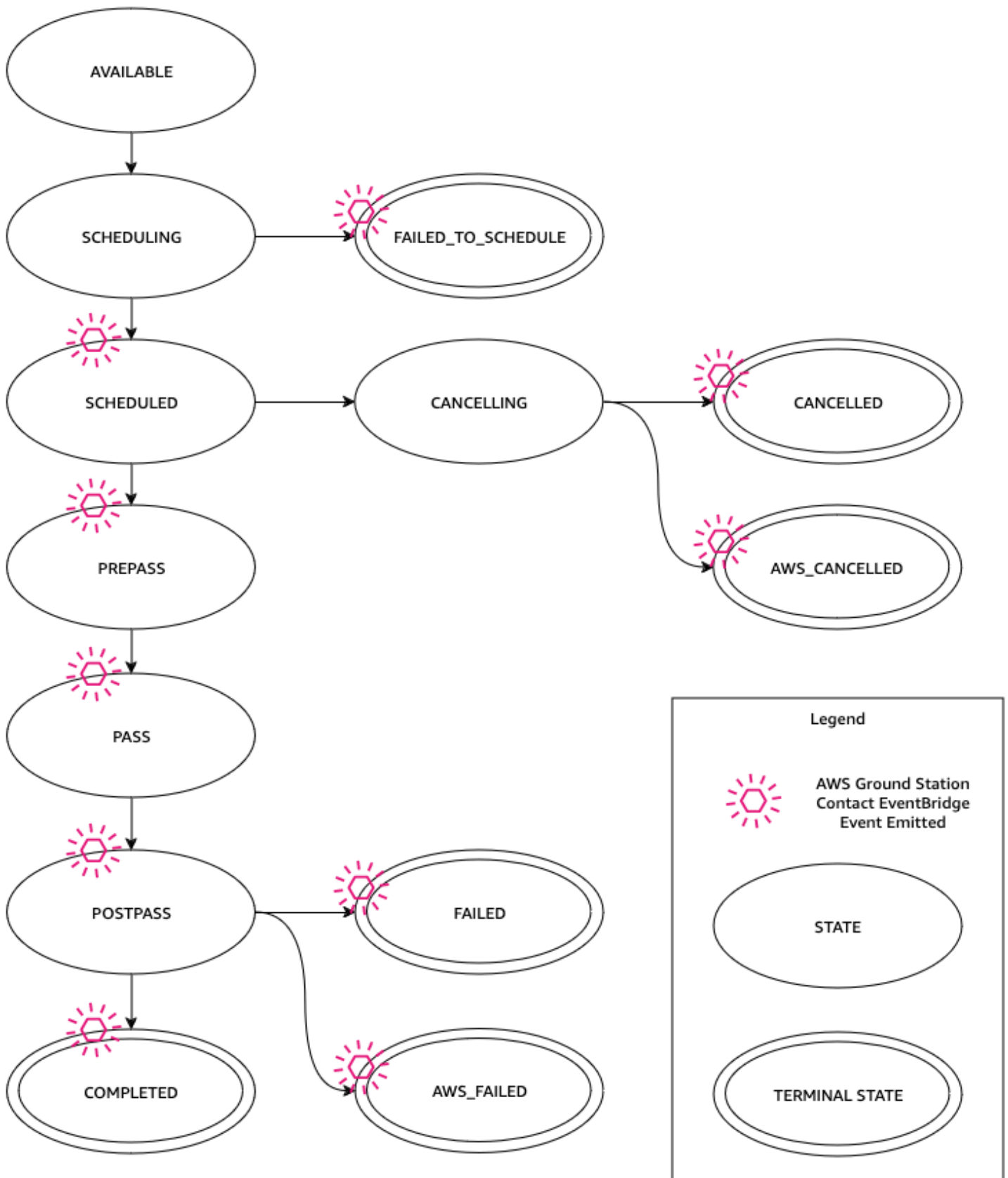
- [Comprenda el ciclo de vida de](#)
- [Comprenda la facturación por contacto](#)

Comprenda el ciclo de vida de

Comprender el ciclo de vida de los contactos puede ayudarte a automatizar y solucionar diversos problemas durante el uso AWS Ground Station. 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 [AWS Ground Station estados de contacto](#) para obtener más información sobre lo que indica cada estado y si se puede detener o cancelar su uso.

[CancelContact](#)



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

En la siguiente tabla se describen los estados que puede tener un contacto:

Status	Description (Descripción)	Terminal	Cancelable	Detenible
DISPONIBLE	El contacto está disponible para ser reservado.	No	N/A	N/A
PROGRAMACIÓN	El contacto está en proceso de programación.	No	Sí	No
SCHEDULED	El contacto se programó correctamente.	No	Sí	No
NO SE PUDO PROGRAMAR	El contacto no se pudo programar.	Sí	No	No
PASE PREVIO	El contacto comenzará pronto y se están preparando los recursos.	No	Sí	No
PASS	El contacto se está ejecutando actualmente y se está comunicando con el satélite.	No	No	Sí
POSTPASO	La comunicación se ha completado y se están limpiando los recursos utilizados.	No	No	No
COMPLETED	El contacto se completó sin errores.	Sí	No	No
ERROR	Se produjo un error en el contacto debido a un problema con la configuración de los recursos.	Sí	No	No

Status	Description (Descripción)	Terminal	Cancelable	Detenible
AWS_FAILED	Se produjo un error en el contacto debido a un problema en el AWS Ground Station servicio.	Sí	No	No
CANCELADO	El contacto está en proceso de ser cancelado.	No	No	No
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.	Sí	No	No
CANCELLED	Tú cancelaste el contacto.	Sí	No	No

Note

Para obtener información sobre las implicaciones de facturación de los contactos cancelados o interrumpidos, consulte [Comprenda la facturación por contacto](#).

Retención de datos de contacto

AWS Ground Station conserva los datos de contacto durante un año después de realizar una [ReserveContact](#) solicitud para reservar un contacto. Después del período de 1 año, los datos de contacto se eliminan.

Si necesita conservar los datos de contacto durante más de un año, se recomienda exportarlos antes de que venza el período de retención. Para obtener más información sobre cómo acceder a los datos de contacto y exportarlos, consulta:

- [AWS Ground Station Referencia de la API](#)
- [AWS Ground Station Referencia de los comandos de la CLI](#)

Comprenda la facturación por contacto

Con AWS Ground Station, solo paga por el tiempo que utilice la antena. AWS Ground Station el uso de los medidores se mide por minuto. Para cada contacto, el servicio calcula la duración del contacto desde el inicio hasta el final y lo redondea al minuto más cercano. Esta duración medida determina los cargos que se cobrarán por ese contacto.

Tu tarifa depende de dos factores principales:

- Ancho de banda: la cantidad de ancho de banda reservada para el contacto (banda estrecha o banda ancha)
- Ubicación de la estación terrestre: las tarifas varían según la ubicación de la estación terrestre

Definición de ancho de banda

AWS Ground Station clasifica los contactos en dos niveles de ancho de banda en función del ancho de banda instantáneo:

- Banda estrecha: cualquier contacto en el que el ancho de banda instantáneo sea inferior o igual a 40 MHz
- Banda ancha: cualquier contacto en el que el ancho de banda instantáneo sea superior a 40 MHz

Modos de programación

AWS Ground Station ofrece dos modos de programación:

- A pedido: pague por el acceso a la antena sin compromisos a largo plazo
- Reservado: ofrece una tarifa con descuento y una mejor programación en comparación con la opción bajo demanda, con un compromiso mensual. Los precios por minutos reservados están disponibles para los clientes que se comprometan a usarlos mensualmente durante un período de tiempo determinado.

Para obtener información específica sobre los precios de su cuenta o para obtener más información sobre el modo de programación reservada, póngase en contacto con su representante de AWS.

CancelContact

El uso de la [CancelContact](#) API varía en función del estado del contacto al llamarla:

- Antes del inicio del contacto: cancela el contacto por completo
- Tras el inicio del contacto y antes de su finalización: detiene el contacto en curso

Cuando cancelas un contacto, la facturación depende del modo de programación y del momento en que lo canceles. Para obtener más información, póngase en contacto con su representante de AWS.

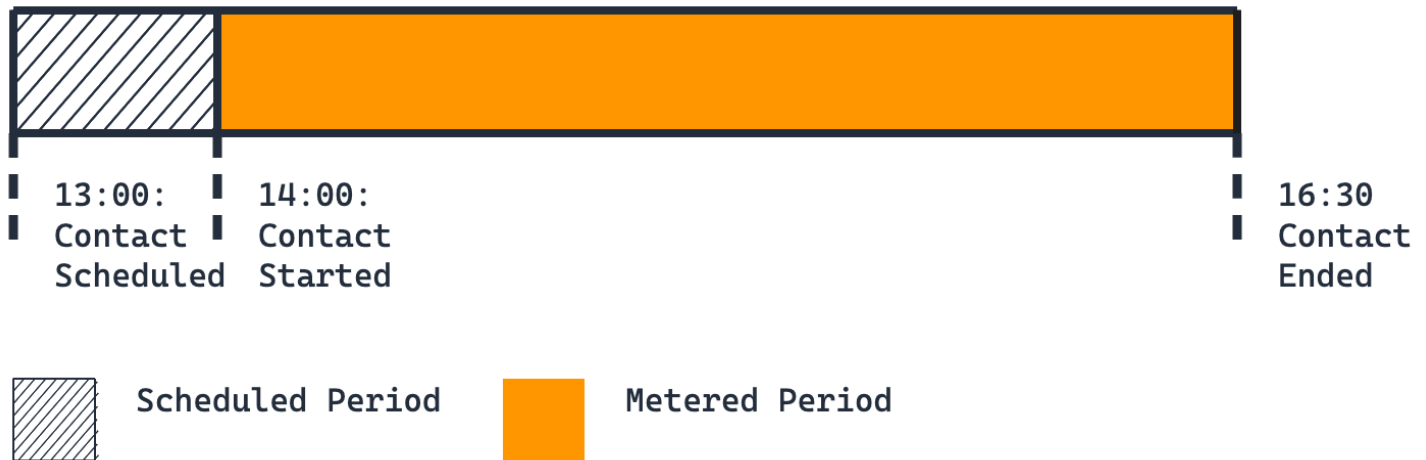
Cuando detiene a un contacto, se le facturará la parte del contacto ejecutada y el tiempo restante que no esté cubierto por contactos duplicados. Un contacto duplicado en este contexto ha sido:

- Programado en la misma estación terrestre que el contacto detenido original
- Programado con el mismo ID de cuenta de AWS que el contacto detenido original
- Reservado después de que se emitiera el comando para detener el contacto original

Los siguientes escenarios demuestran cómo funciona esta medición en la práctica.

Escenario 1: contacto único

Programa un contacto de 150 minutos en Ground Station Anytown 1 para que comience a las 14:00 y finalice a las 16:30.



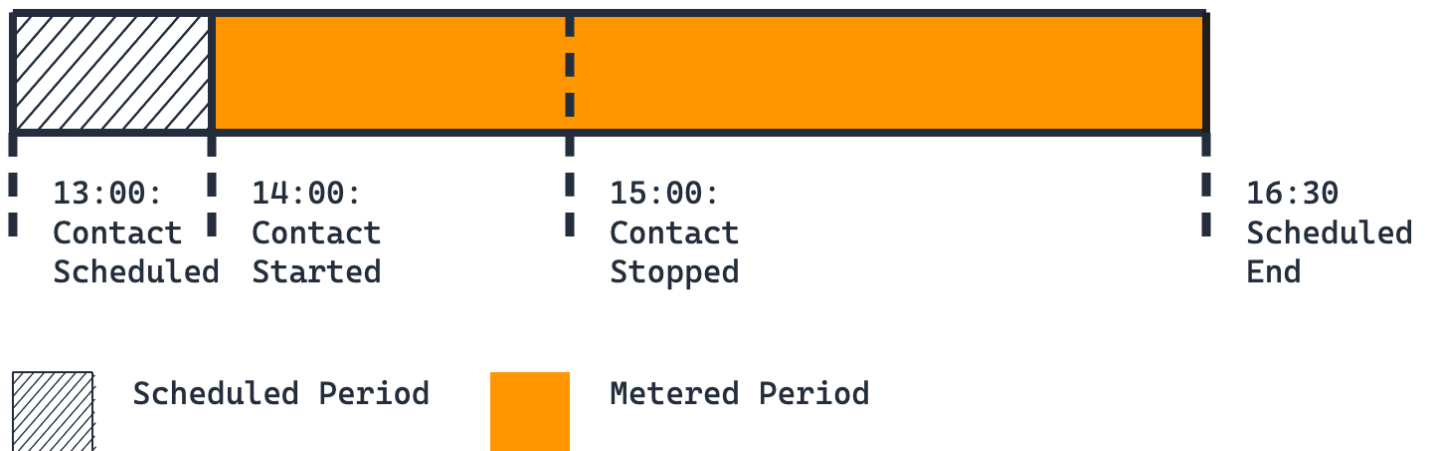
Desglose de facturación:

- Primer contacto: 150 minutos (duración completa)

Se te facturarán 150 minutos. Este es el escenario base en el que un contacto se ejecuta hasta su finalización programada sin paradas ni cancelaciones.

Escenario 2: contacto con una sola parada

Programe un contacto de 150 minutos en Ground Station Anytown 1 para que comience a las 14:00 y finalice a las 16:30. A las 15:00, llamas a la API para detener tu contacto `CancelContact`.



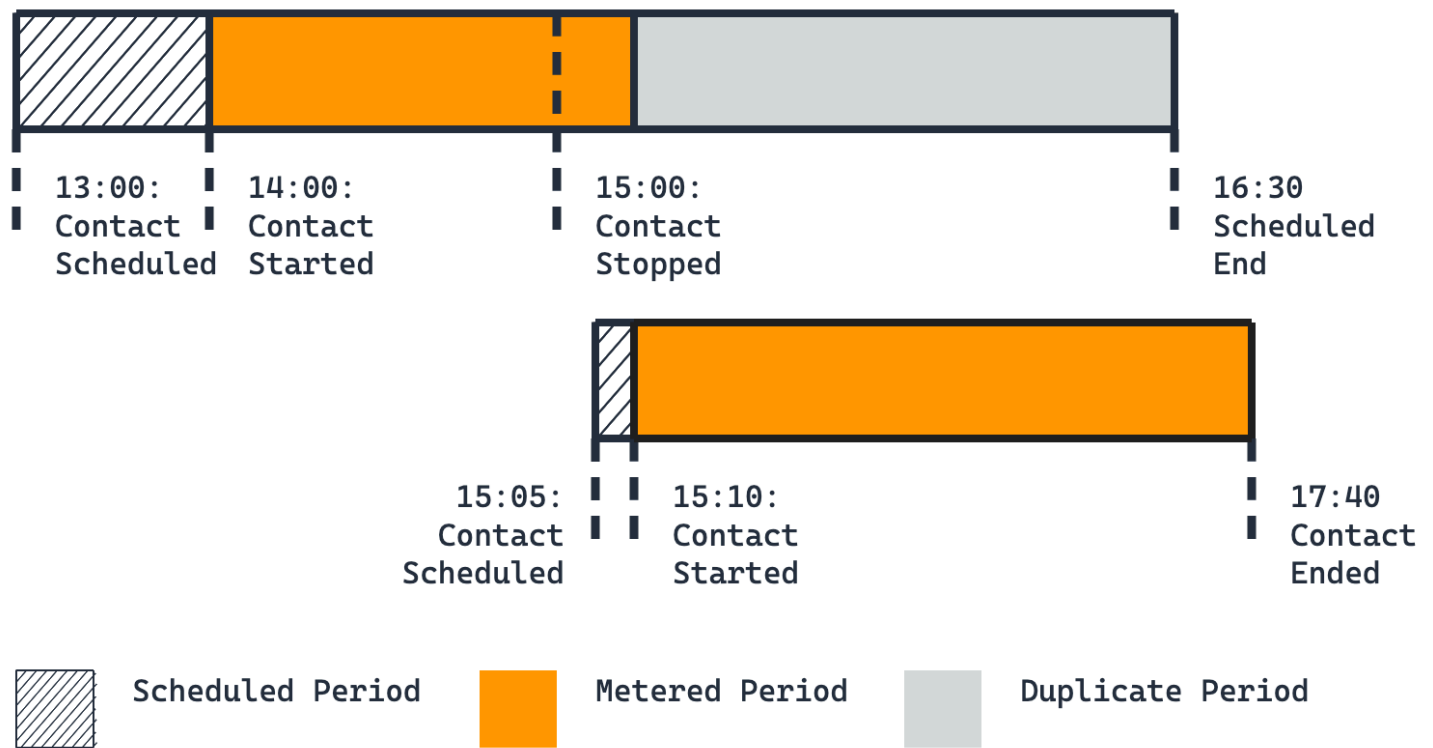
Desglose de facturación:

- Primer contacto: 150 minutos (duración original completa)

Se te facturarán los 150 minutos completos porque detuviste el contacto pero no programaste ningún contacto duplicado para cubrir el tiempo restante (15:00 a 16:30). Si detienes un contacto sin programar los duplicados, sigues siendo responsable de todo el tiempo programado originalmente.

Escenario 3: Duplicado único

Programe un contacto de 150 minutos en Ground Station Anytown 1 para que comience a las 14:00 y finalice a las 16:30. A las 15:00, llamas a la `CancelContact` API para detener tu primer contacto. Después de llamar `CancelContact`, programa otro contacto en la misma Ground Station a partir de las 15:10 durante 150 minutos.



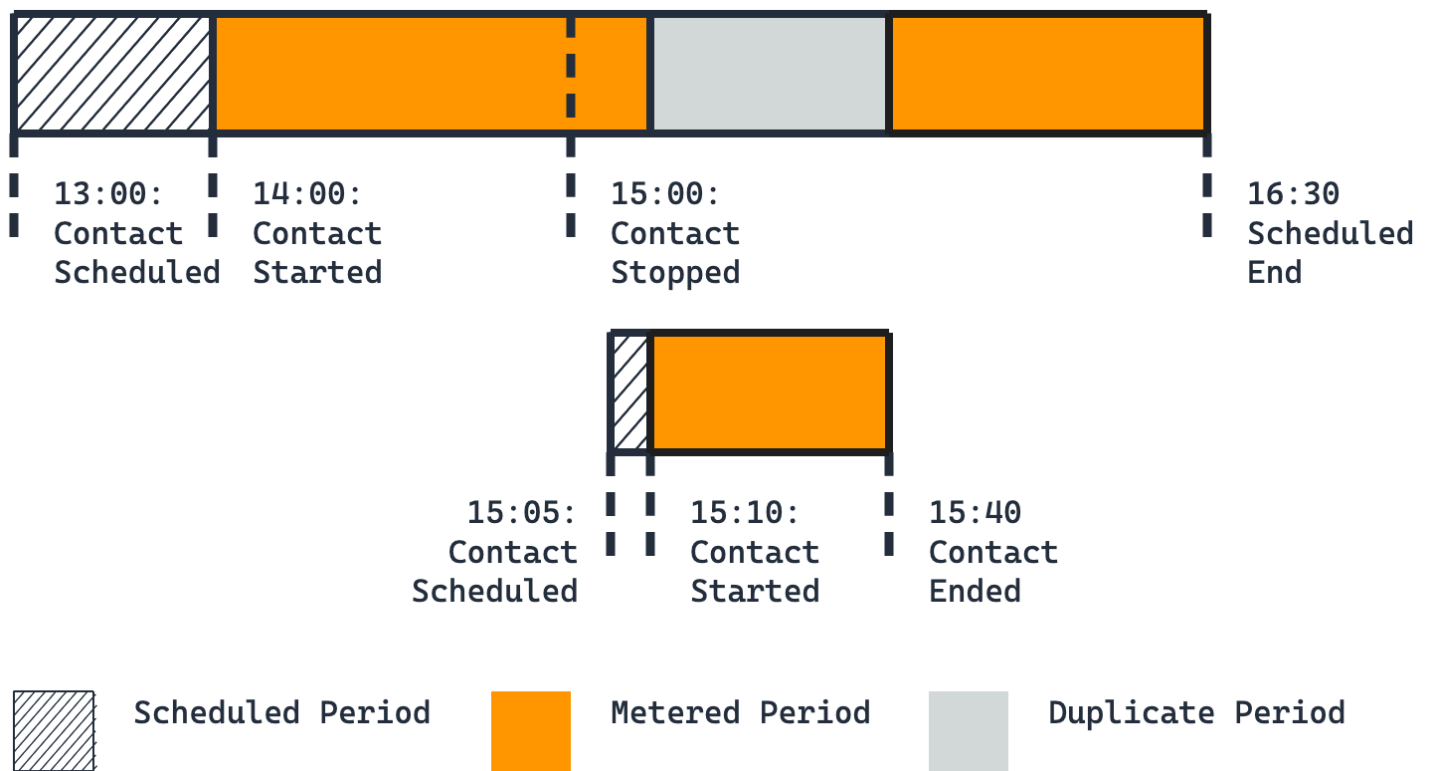
Desglose de facturación:

- Primer contacto: 70 minutos (60 minutos ejecutados más 10 minutos de inactividad antes de que comience el segundo contacto)
- Segundo contacto: 150 minutos (duración total)

El segundo contacto es un duplicado porque lo programaste después de detener el primer contacto. El duplicado cubre el tiempo restante, entre las 15:10 y las 16:30, por lo que solo se te facturará el tiempo que duró el primer contacto, más los 10 minutos que transcurren entre la parada y el reinicio.

Escenario 4: Duplicado corto

Programa un contacto de 150 minutos en Ground Station Anytown 1 para que comience a las 14:00 y finalice a las 16:30. A las 15:00, llamas a la CancelContact API para detener tu primer contacto. Después de llamar CancelContact, programa un contacto de 30 minutos en la misma Ground Station a partir de las 15:10.



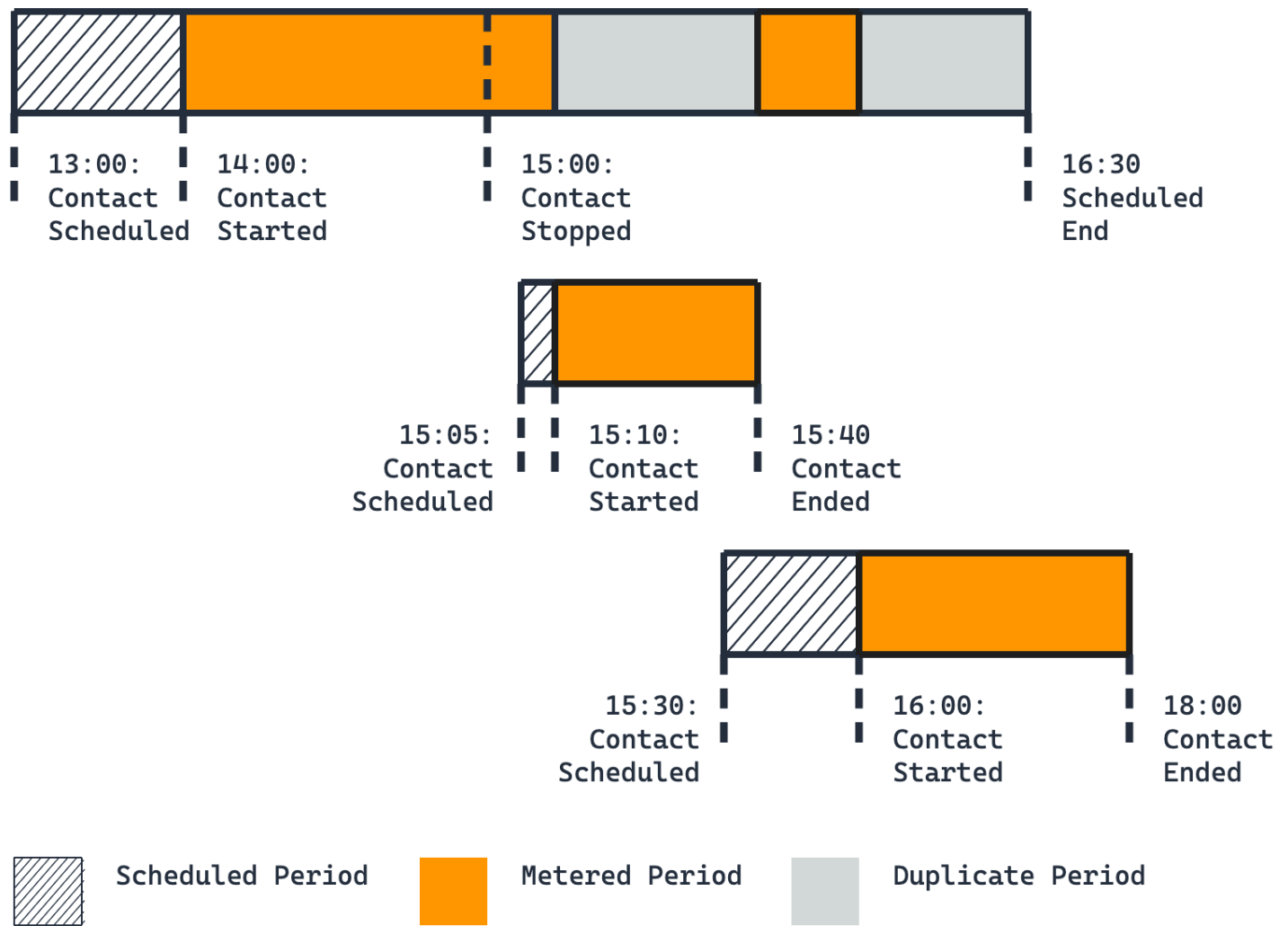
Desglose de facturación:

- Primer contacto: 120 minutos (60 minutos ejecutados más 10 minutos de inactividad antes de que comience el segundo contacto más 50 minutos de tiempo restante que el duplicado no cubrió)
- Segundo contacto: 30 minutos (duración total)

El contacto duplicado solo cubre 30 minutos (15:10-15:40) de los 90 minutos restantes después de detener el primer contacto. Se te facturará el intervalo de 10 minutos antes de que comience el duplicado y los 50 minutos sin cubrir después de que finalice el duplicado (15:40-16:30).

Escenario 5: Varios duplicados

Programe un contacto de 150 minutos en Ground Station Anytown 1 para que comience a las 14:00 y finalice a las 16:30. A las 15:00, llamas a la CancelContact API para detener tu primer contacto. Después de llamar CancelContact, programa un contacto de 30 minutos en la misma Ground Station a partir de las 15:10. Más tarde, a las 15:30, programa otro contacto a partir de las 16:00 durante 120 minutos.



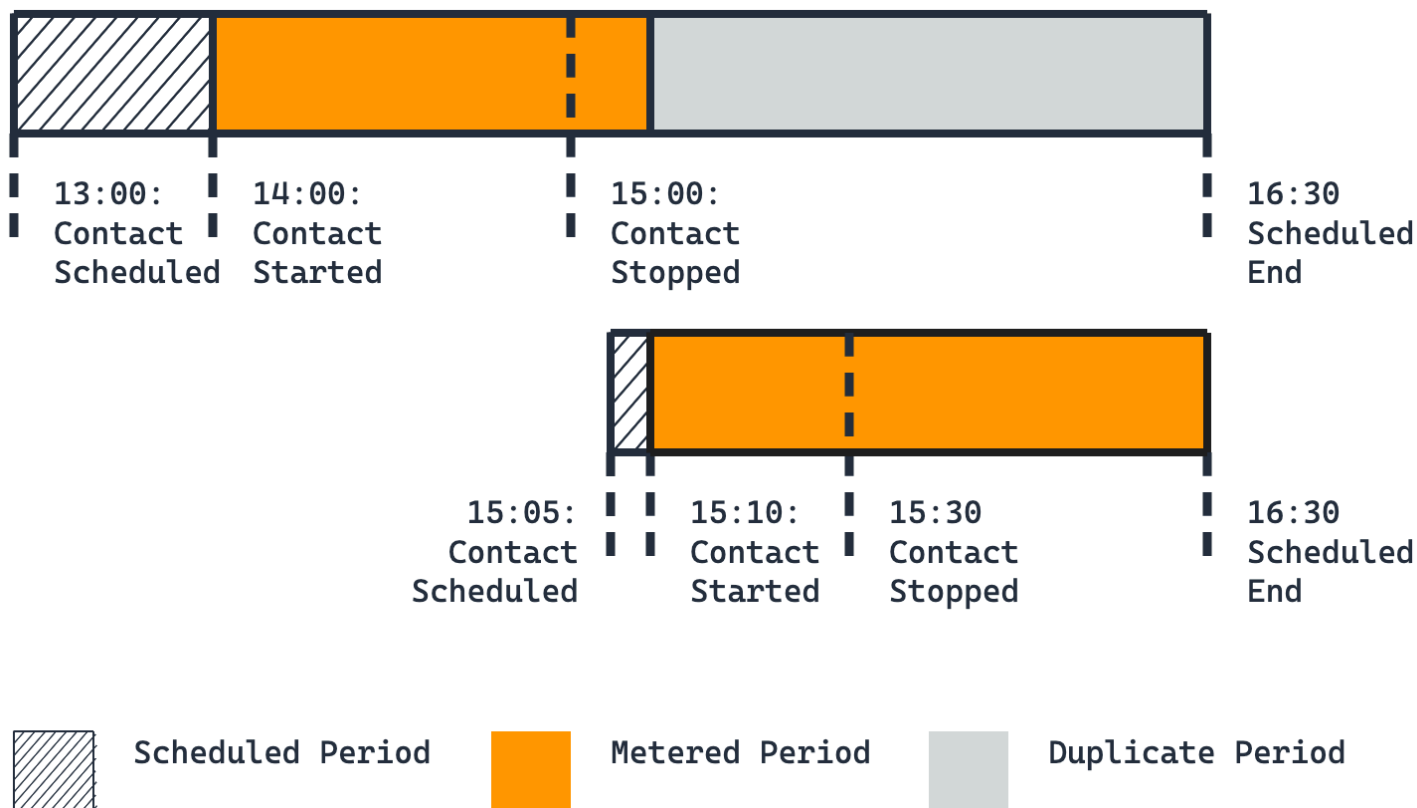
Desglose de facturación:

- Primer contacto: 90 minutos (60 minutos ejecutados más 10 minutos de inactividad antes del inicio del segundo contacto más 20 minutos de inactividad entre el segundo y el tercer contacto)
- Segundo contacto: 30 minutos (duración total)
- Tercer contacto: 120 minutos (duración completa)

Tanto el segundo como el tercer contacto cuentan como duplicados porque los programaste después de detener el primer contacto. Sin embargo, se seguirán facturando los intervalos entre los contactos: 10 minutos entre la primera parada (15:00) y la segunda salida (15:10), y 20 minutos entre la segunda parada (15:40) y la tercera salida (16:00).

Escenario 6: paradas múltiples

Programe un contacto de 150 minutos en Ground Station Anytown 1 para que comience a las 14:00 y finalice a las 16:30. A las 15:00, llamas a la CancelContact API para detener tu primer contacto. Después de llamar CancelContact, programa un contacto de 80 minutos en Ground Station Anytown 1 que comienza a las 15:10 y termina a las 16:30. A las 15:30, vuelves a llamar a la CancelContact API y detienes tu contacto duplicado.



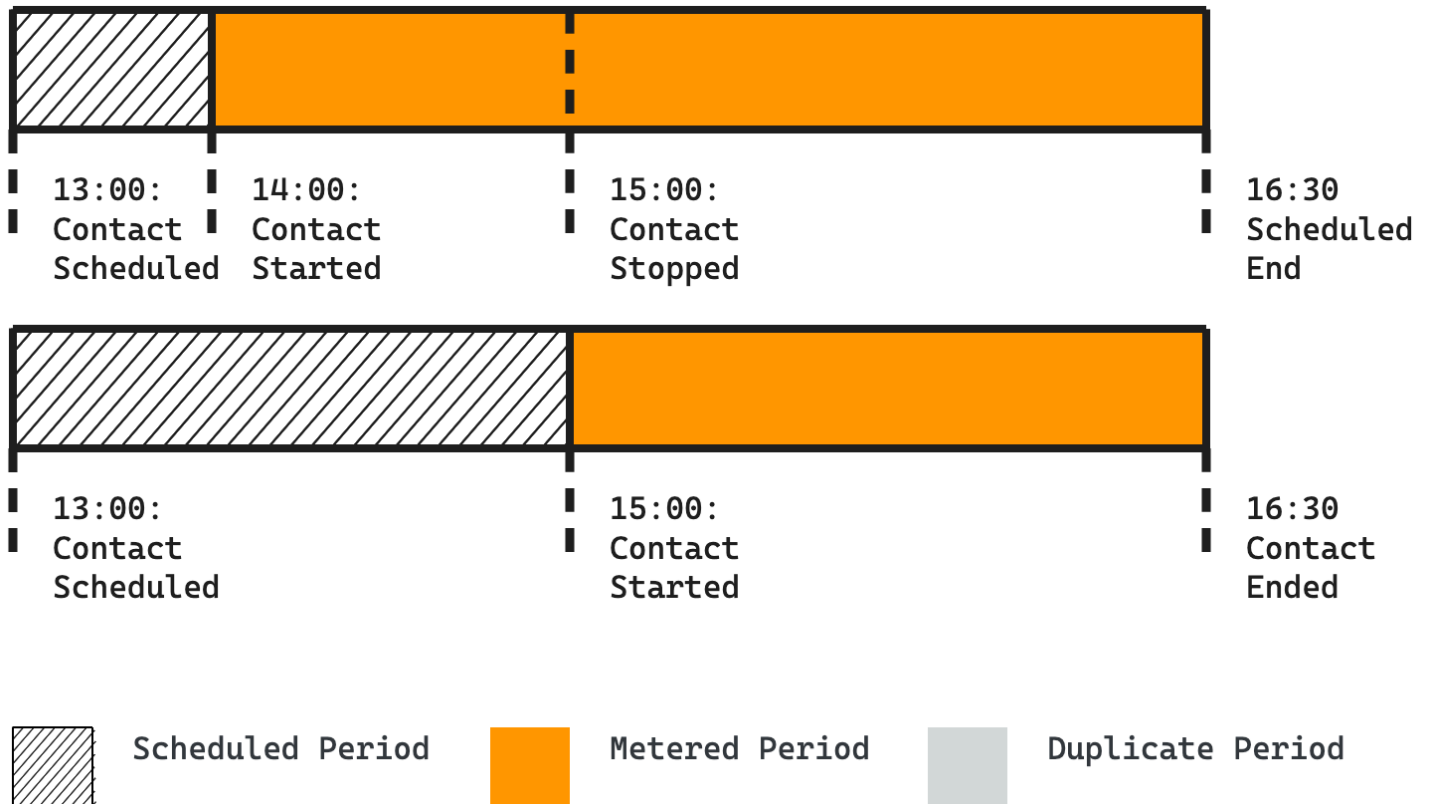
Desglose de facturación:

- Primer contacto: 70 minutos (60 minutos ejecutados más 10 minutos de inactividad antes de que comience el segundo contacto)
- Segundo contacto: 80 minutos (duración original completa)

El segundo contacto se factura por su duración total de 80 minutos, ya que lo interrumpiste a las 15:30 y dejaste sin cubrir 60 minutos del horario inicialmente programado (15:30 a 16:30). A menos que programes otro contacto duplicado para cubrir el tiempo restante, serás responsable de toda la duración de cualquier contacto interrumpido.

Escenario 7: estación terrestre con varias antenas sin duplicados

A las 13:00, programa dos contactos en la Ground Station Anytown 1. El primero es un contacto de 150 minutos que comienza a las 14:00 y termina a las 16:30. El segundo es un contacto de 90 minutos que comienza a las 15:00 y termina a las 16:30. A las 15:00, llamas a la CancelContact API para detener tu primer contacto. Ground Station Anytown 1 es una estación terrestre con múltiples antenas que permite que ambos contactos funcionen simultáneamente.



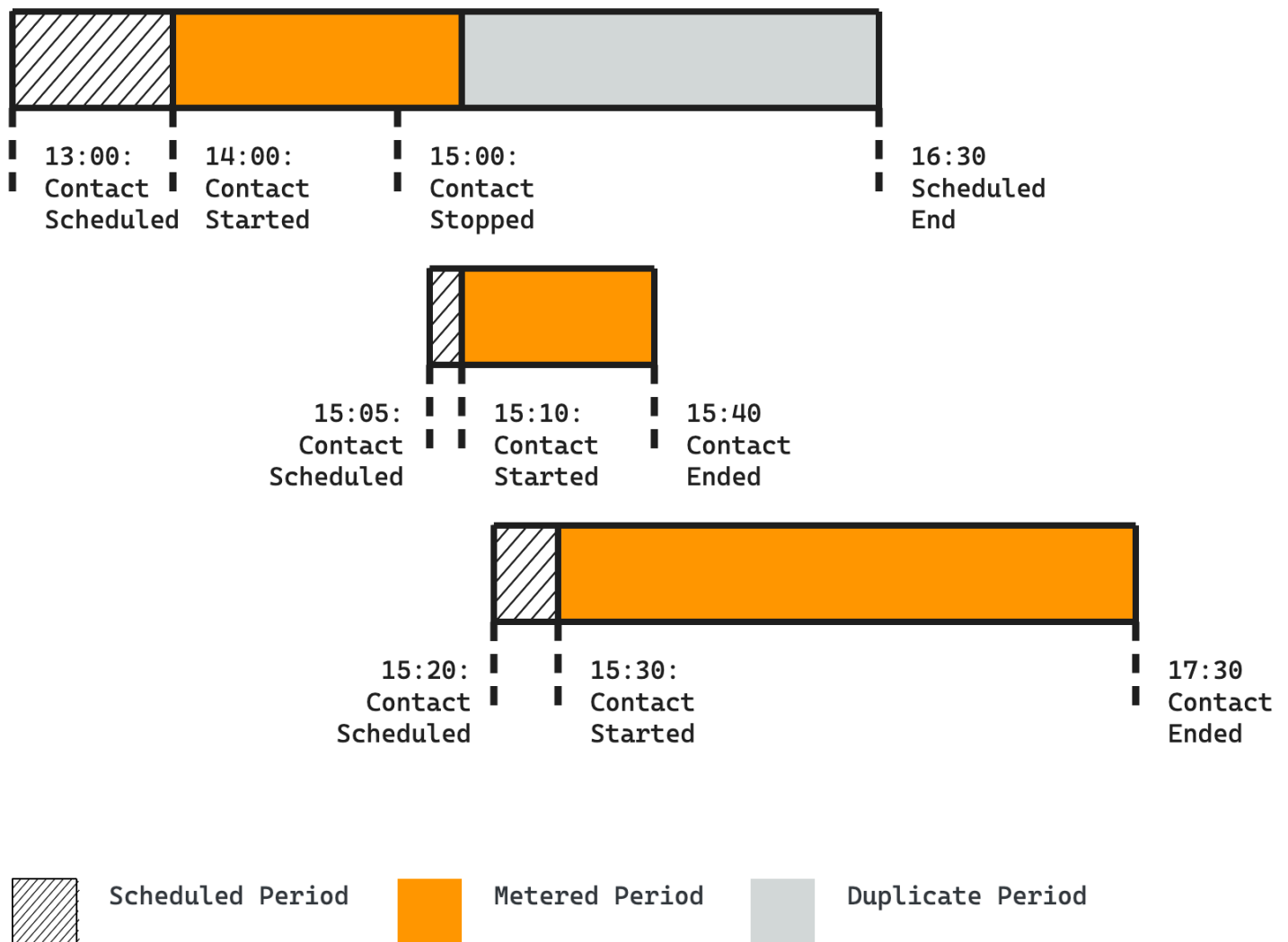
Desglose de facturación:

- Primer contacto: 150 minutos (duración original completa)
- Segundo contacto: 90 minutos (duración completa)

Aunque el segundo contacto se superponga con la parte detenida del primer contacto, no cuenta como duplicado. El segundo contacto no cumple el primer criterio para los duplicados: estaba programado para las 13:00, antes de detener el primer contacto a las 15:00. Como no se trata de un duplicado, se te facturará toda la duración original del primer contacto, independientemente de cuándo lo hayas detenido.

Escenario 8: estación terrestre con varias antenas con contactos duplicados

Programe un contacto de 150 minutos en Ground Station Anytown 1 para que comience a las 14:00 y finalice a las 16:30. A las 15:00, llamas a la CancelContact API para detener tu primer contacto. Después de llamar CancelContact, programa un contacto de 30 minutos en Ground Station Anytown 1 que comienza a las 15:10 y termina a las 15:40. Más tarde, programa otro contacto de 90 minutos en Ground Station Anytown 1 a partir de las 15:30 y finalizando a las 17:00. Ground Station Anytown 1 es una estación terrestre con varias antenas, que permite que ambos contactos duplicados se ejecuten simultáneamente con tiempos superpuestos.



Desglose de facturación:

- Primer contacto: 70 minutos (60 minutos ejecutados más 10 minutos de inactividad antes de que comience el segundo contacto)

- Segundo contacto: 30 minutos (duración completa)
- Tercer contacto: 90 minutos (duración completa)

Tanto el segundo como el tercer contacto cuentan como duplicados porque los programaste después de detener el primer contacto. El intervalo de 10 minutos entre la detención del primer contacto (15:00) y el inicio del segundo contacto (15:10) representa el tiempo de inactividad que se te factura con respecto al contacto original.

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 empezar [Satélite 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 [ListGroundStations](#) respuesta 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 en [Trabaje 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 [Automatiza 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 CloudTrail captura 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

- [Automatiza AWS Ground Station con eventos](#)
- [Registra las llamadas a la AWS Ground Station API con AWS CloudTrail](#)
- [Consulta las métricas con Amazon CloudWatch](#)

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

Para obtener más información, consulta la [Guía del usuario de Amazon EventBridge Events](#).

AWS Ground Station Tipos de eventos

Note

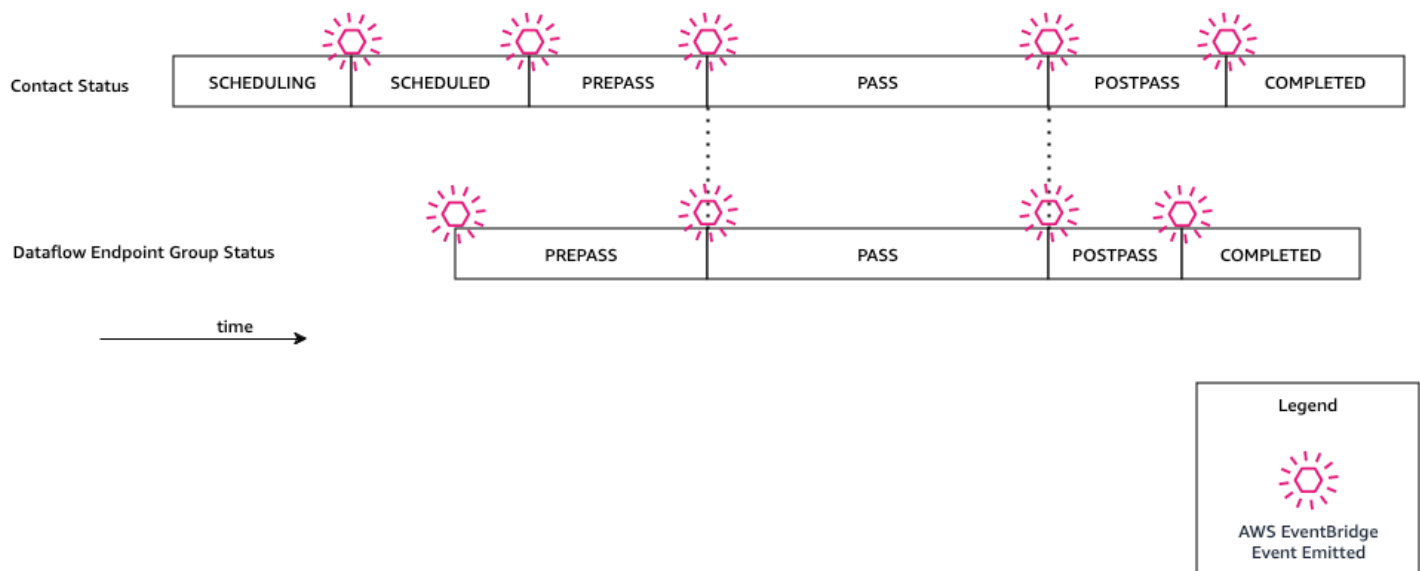
Todos los eventos generados por AWS Ground Station tienen "aws.groundstation" como valor de "source".

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, consulte [Comprenda 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 [contactPrePassDurationSeconds](#) y [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-
bccccca005000"
  ],
  "detail": {
    "ephemerisStatus": "ENABLED",
    "ephemerisId": "111111-cccc-bbbb-a555-bccccca005000",
    "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](#).

La función de AWS Ground Station telemetría también se puede utilizar para recibir métricas casi en tiempo real durante los contactos. CloudWatch las métricas no están disponibles casi en tiempo real y pueden provocar retrasos en la entrega. CloudWatch también agrega las métricas durante un período de un segundo, lo que podría reducir la granularidad de los datos. La función de telemetría proporciona las métricas individuales y las envía casi en tiempo real directamente a su cuenta. AWS Para obtener más información, consulte [Trabaje con telemetría](#).

Important

AWS Ground Station emite CloudWatch las métricas a la AWS región asociada a la ubicación de la estación terrestre del contacto, no a la AWS región desde la que se programó el contacto. Para ver las métricas de un contacto, debes acceder a la CloudWatch región de la estación terrestre. Para obtener información sobre qué AWS región está asociada a cada ubicación de la estación terrestre, consulte [Búsqueda de la AWS región para la ubicación de una estación terrestre](#). Para recibir datos de telemetría en la región desde la que programa sus contactos, puede utilizar la función de AWS Ground Station telemetría. Consulte [Trabaje con telemetría](#) para obtener más detalles.

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	Description (Descripción)
<code>AzimuthAngle</code>	<code>SatelliteId</code>	El ángulo azimut de la antena. El norte verdadero está a 0 grados y el este a 90 grados. Unidades: grados
<code>BitErrorRate</code>	Canal, polarización, <code>SatelliteId</code>	Tasa de error en bits en un número determinado de transmisiones de bits. El ruido, la distorsión o las interferencias causan los errores de bits. Unidades: errores de bits por unidad de tiempo
<code>BlockErrorRate</code>	Canal, polarización, <code>SatelliteId</code>	La tasa de errores de los

Métrica	Dimensiones de la métrica	Description (Descripción)
		<p>bloques en un número dado de bloques recibidos. Las interferencias causan los errores de bloque.</p> <p>Unidades: Bloques erróneos/ Número total de bloques</p>
CarrierFrequencyRecovery_Cn0	Categoría, Config, SatelliteId	<p>Relación portadora/densidad de ruido por unidad de ancho de banda.</p> <p>Unidades: decibelio-hercio (dB-HZ)</p>

Métrica	Dimensiones de la métrica	Description (Descripción)
CarrierFrequencyRecovery_Locked	Categoría, Config, SatelliteId	<p>Se establece en 1 cuando el bucle de recuperación de frecuencia portadora del desmodulador está bloqueado y en 0 cuando está desbloqueado.</p> <p>Unidades: sin unidades</p>
CarrierFrequencyRecovery_OffsetFrequency_Hz	Categoría, Config, SatelliteId	<p>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.</p> <p>Unidades: hercios (Hz)</p>

Métrica	Dimensiones de la métrica	Description (Descripción)
ElevationAngle	SatelliteId	<p>El ángulo de elevación de la antena. El horizonte está a 0 grados y el cenit a 90 grados.</p> <p>Unidades: grados</p>
Es/N0	Canal, polarización, SatelliteId	<p>Relación entre la energía por símbolo y la densidad espectral de potencia del ruido.</p> <p>Unidades: decibelios (dB)</p>
ReceivedPower	Polarización, SatelliteId	<p>La intensidad de la señal medida en el desmodulador/ descodificador.</p> <p>Unidades: decibelios relativos a milivatios (dBm)</p>

Métrica	Dimensiones de la métrica	Description (Descripción)
SymbolTimingRecovery_ErrorVectorMagnitude	Categoría, Config, SatelliteId	<p>La magnitud del vector de error entre los símbolos recibidos y los puntos de constelación ideales.</p> <p>Unidades: porcentaje</p>
SymbolTimingRecovery_Locked	Categoría, Config, SatelliteId	<p>Se establece en 1 cuando el bucle de recuperación de temporización de símbolos del desmodulador está bloqueado y en 0 cuando está desbloqueado.</p> <p>Unidades: sin unidades</p>

Métrica	Dimensiones de la métrica	Description (Descripción)
SymbolTimingRecovery_OffsetSymbolRate	Categoría, Config, SatelliteId	<p>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.</p> <p>Unidades: Símbolos/ segundo</p>

¿Para qué dimensiones se utilizan AWS Ground Station?

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

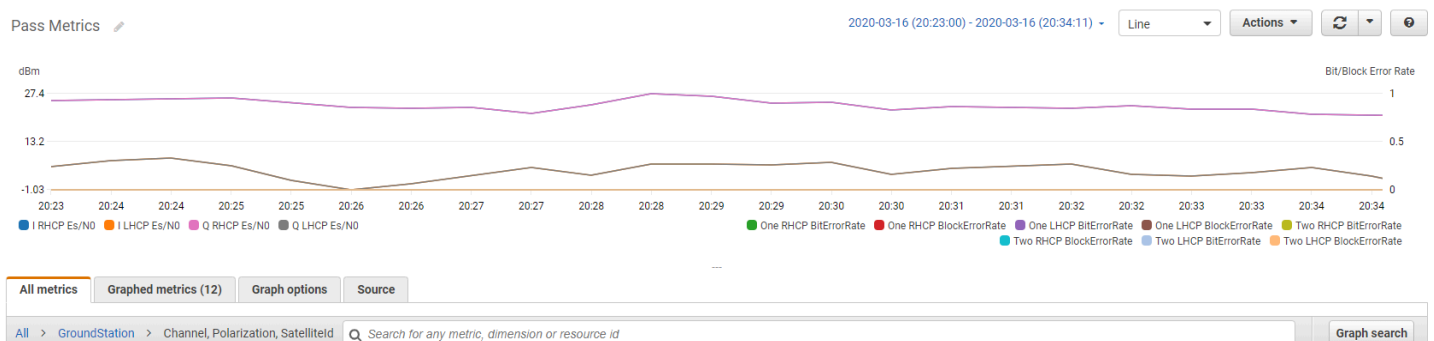
Dimensión	Description (Descripción)
Category	Demodulación o decodificación.
Channel	Los canales para cada contacto incluyen Uno, Dos, I (en fase) y Q (cuadratura).
Config	Un arn de configuración de decodificación de demodos de enlace descendente de antena.

Dimensión	Description (Descripción)
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. CloudWatchMetrics 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](#).

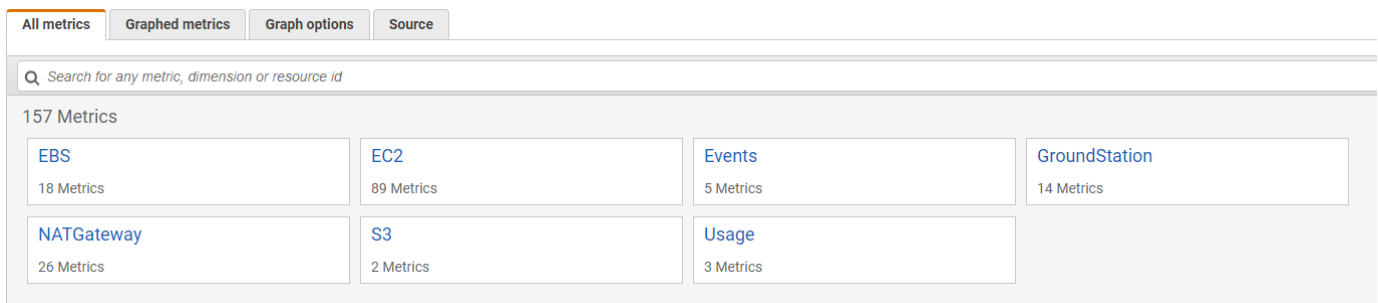
Además, los datos capturados en los primeros 60 segundos no contendrán suficiente información para producir métricas significativas y es probable que no se muestren. Para consultar las métricas significativas, se recomienda consultar los datos después de 60 segundos.



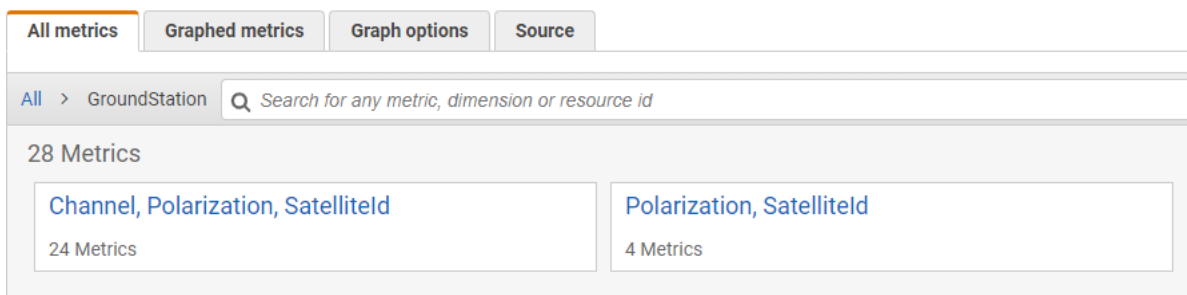
Para obtener más información sobre cómo graficar AWS Ground Station las métricas CloudWatch, consulte [Graficar las métricas](#).

Para consultar las métricas desde la consola de

1. Determine la AWS región asociada a la ubicación de su estación terrestre. AWS Ground Station emite CloudWatch métricas en la región asociada a la ubicación de la estación terrestre de tu contacto. Para ver la lista de ubicaciones de las estaciones terrestres y sus AWS regiones asociadas, consulte [Búsqueda de la AWS región para la ubicación de una estación terrestre](#).
2. Abra la [consola de CloudWatch](#).
3. En el panel de navegación, seleccione Métricas.
4. Seleccione el espacio de nombres de GroundStation.



5. Seleccione las dimensiones métricas que desee (por ejemplo, canal, polarización Satelliteld).



6. La pestaña All metrics muestra todas las métricas para dicha dimensión en el espacio de nombres. Se 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 situada 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

AWS Ground Station emite CloudWatch métricas en la región asociada a la ubicación de la estación terrestre de tu contacto. Para ver la lista de ubicaciones de estaciones terrestres y sus AWS regiones asociadas, [Búsqueda de la AWS región para la ubicación de una estación terrestre](#). `ground-station-region-code` Sustitúyalo por el código de AWS región de la ubicación de la estación terrestre (us-west-2 por ejemplo, en Oregón 1, Hawái 1 o Alaska 1). Todos los AWS CLI comandos siguientes de este procedimiento deben usar la misma región.

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. Identifique la AWS región asociada a la ubicación de su estación terrestre.
3. Utilice el `get-metric-data` método 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 --region ground-station-region-code --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": ""
    }
}

```

4. Enumere las CloudWatch métricas disponibles ejecutándolas `aws cloudwatch list-metrics --region ground-station-region-code`.

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

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 CloudWatch las limitaciones, consulta: [Ver las métricas disponibles](#)

5. 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-
                eeeeeeeeeee"
            },
            {
              "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.

- 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 --region ground-station-region-code --cli-input-json
file://<nameOfConfigurationFileCreatedInStep2>.json

```

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

```

{
  "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 políticas gestionadas para AWS Ground Station](#)
- [Utilice funciones vinculadas a servicios para Ground Station](#)
- [Cifrado de datos en reposo para AWS Ground Station](#)
- [Cifrado de datos durante el tránsito para AWS Ground Station](#)

Identity and Access Management para AWS Ground Station

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

Temas

- [Público](#)
- [Autenticación con identidades](#)
- [Administración del acceso con políticas](#)

- [¿Cómo AWS Ground Station funciona con IAM](#)
- [Ejemplos de políticas basadas en la identidad para AWS Ground Station](#)
- [Solución de problemas de AWS Ground Station identidad y acceso](#)

Público

La forma de usar AWS Identity and Access Management (IAM) varía según la función que desempeñes:

- Usuario del servicio: solicite permisos al administrador si no puede acceder a las características (consulte [Solución de problemas de AWS Ground Station identidad y acceso](#)).
- Administrador del servicio: determine el acceso de los usuarios y envíe las solicitudes de permiso (consulte [¿Cómo AWS Ground Station funciona con IAM](#)).
- Administrador de IAM: escribe las políticas para administrar el acceso (consulte [Ejemplos de políticas basadas en la identidad para AWS Ground Station](#)).

Autenticación con identidades

La autenticación es la forma en que inicias sesión AWS con tus credenciales de identidad. Debe autenticarse como usuario de Usuario raíz de la cuenta de AWS IAM o asumir una función de IAM.

Puede iniciar sesión como una identidad federada con las credenciales de una fuente de identidad, como AWS IAM Identity Center (IAM Identity Center), la autenticación de inicio de sesión único o las credenciales. Google/Facebook Para obtener más información sobre el inicio de sesión, consulte [Cómo iniciar sesión en la Cuenta de AWS](#) en la Guía del usuario de AWS Sign-In .

Para el acceso programático, AWS proporciona un SDK y una CLI para firmar criptográficamente las solicitudes. Para obtener más información, consulte [AWS Signature Version 4 para solicitudes de API](#) en la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear un Cuenta de AWS, se comienza con una identidad de inicio de sesión denominada usuario Cuenta de AWS raíz que tiene acceso completo a todos Servicios de AWS los recursos. Se recomienda encarecidamente que no utilice el usuario raíz para las tareas diarias. Para ver las tareas que requieren credenciales de usuario raíz, consulte [Tareas que requieren credenciales de usuario raíz](#) en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos 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 empresarial, del proveedor de identidades web o al Directory Service que se accede Servicios de AWS mediante credenciales de una fuente de identidad. Las identidades federadas asumen roles que proporcionan credenciales temporales.

Para una administración de acceso centralizada, se recomienda AWS IAM Identity Center. Para obtener más información, consulte [¿Qué es el Centro de identidades de IAM?](#) en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un [usuario de IAM](#) es una identidad con permisos específicos para una sola persona o aplicación. Recomendamos el uso de credenciales temporales en lugar de usuarios de IAM con credenciales de larga duración. Para obtener más información, consulte [Exigir a los usuarios humanos que utilicen la federación con un proveedor de identidad para acceder AWS mediante credenciales temporales](#) en la Guía del usuario de IAM.

Un [grupo de IAM](#) especifica un conjunto de usuarios de IAM y facilita la administración de los permisos para grupos grandes de usuarios. 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 con permisos específicos que proporciona credenciales temporales. Puede asumir un rol [cambiando de un rol de usuario a uno de IAM \(consola\)](#) o llamando a una AWS CLI operación de AWS API. Para obtener más información, consulte [Métodos para asumir un rol](#) en la Guía del usuario de IAM.

Los roles de IAM son útiles para el acceso de usuario federado, los permisos de usuario de IAM temporales, el acceso entre cuentas, el acceso entre servicios y las aplicaciones que se ejecutan en Amazon EC2. Para obtener más información, consulte [Acceso a recursos entre cuentas en IAM](#) en la Guía del usuario de IAM.

Administración del acceso con políticas

AWS Para controlar el acceso, puede crear políticas y adjuntarlas a AWS identidades o recursos. Una política define los permisos cuando están asociados a una identidad o un recurso. AWS evalúa

estas políticas cuando un director hace una solicitud. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre los documentos de políticas de JSON, consulte [Información general de políticas de JSON](#) en la Guía del usuario de IAM.

Mediante las políticas, los administradores especifican quién tiene acceso a qué, definiendo qué entidad principal puede realizar acciones sobre qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM crea políticas de IAM y las agrega a roles, que los usuarios pueden asumir posteriormente. Las políticas de IAM definen permisos independientemente del método que se utilice para realizar la operación.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de política de permisos JSON que asocia a una identidad (usuario, grupo o rol). Estas políticas controlan qué acciones pueden realizar las identidades, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte [Definición de permisos de IAM personalizados con políticas administradas por el cliente](#) en la Guía del usuario de IAM.

Las políticas basadas en identidad pueden ser políticas insertadas (incrustadas directamente en una sola identidad) o políticas administradas (políticas independientes asociadas a varias identidades). Para obtener información sobre cómo elegir entre políticas administradas e insertadas, consulte [Selección 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 políticas JSON que se asocian a un recurso. Los ejemplos incluyen las Políticas de confianza de roles de IAM y las Políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Debe [especificar una entidad principal](#) en una política basada en recursos.

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.

Otros tipos de políticas

AWS admite tipos de políticas adicionales que pueden establecer los permisos máximos que conceden los tipos de políticas más comunes:

- Límites de permisos: establecen los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM. Para obtener más información, consulte [Límites de permisos para las entidades de IAM](#) en la Guía del usuario de IAM.
- Políticas de control de servicios (SCPs): especifican los permisos máximos para una organización o unidad organizativa en AWS Organizations. Para obtener más información, consulte [Políticas de control de servicios](#) en la Guía del usuario de AWS Organizations .
- Políticas de control de recursos (RCPs): establece los permisos máximos disponibles para los recursos de tus cuentas. Para obtener más información, consulte [Políticas de control de recursos \(RCPs\)](#) en la Guía del AWS Organizations usuario.
- Políticas de sesión: políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal para un rol o un usuario federado. Para obtener más información, consulte [Políticas de sesión](#) en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo 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

Característica de IAM	AWS Ground Station soporte
Claves de condición de política (específicas del servicio)	Sí
ACLs	No
ABAC (etiquetas en políticas)	Sí
Credenciales temporales	Sí
Permisos de entidades principales	Sí
Roles de servicio	No
Roles vinculados al servicio	Sí

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

Políticas basadas en la identidad para AWS Ground Station

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte [Definición de permisos de IAM personalizados con políticas administradas por el cliente](#) 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. Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte [Referencia de los elementos de la política 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 incluidas 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 pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe [especificar una entidad principal](#) en una política basada en 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. Para obtener más información, consulte [Acceso a recursos entre cuentas en IAM](#) en la Guía del usuario de IAM.

Acciones políticas para AWS Ground Station

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 puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. 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, consulte [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 puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Como práctica recomendada, especifique un recurso utilizando el [Nombre de recurso de Amazon \(ARN\)](#). En el caso de las acciones que no admiten permisos por recurso, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

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

Para ver una lista de los tipos de AWS Ground Station recursos y sus 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 puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` especifica cuándo se ejecutan las instrucciones en función de criterios definidos. Puede 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. 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 denominados etiquetas. Puede adjuntar etiquetas a las entidades y AWS los recursos de IAM y, a continuación, diseñar políticas de ABAC para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso.

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, consulte [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

Las credenciales temporales proporcionan acceso a AWS los recursos a corto plazo y se crean automáticamente cuando se utiliza la federación o se cambia de rol. 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](#) y [Servicios de AWS que funcionan con IAM](#) en la Guía del usuario de IAM.

Permisos principales entre servicios para AWS Ground Station

Admite sesiones de acceso directo (FAS): sí

Las sesiones de acceso directo (FAS) utilizan los permisos de la persona principal que llama Servicio de AWS, junto con la solicitud, Servicio de AWS para realizar solicitudes a los servicios descendentes. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte [Sesiones de acceso directo](#).

Funciones 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 [Crear 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 podría interrumpir AWS Ground Station la funcionalidad. Edite las funciones de servicio solo cuando se AWS Ground Station proporcionen instrucciones para hacerlo.

Funciones vinculadas al servicio para AWS Ground Station

Compatible con roles vinculados al servicio: sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio

aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para más información sobre cómo crear o administrar roles vinculados a servicios, 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 . Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan.

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 por ellos AWS Ground Station, incluido el ARNs formato de cada uno de los tipos de recursos, consulte [las claves de acción, recursos y condición de la Referencia AWS Ground Station](#) de autorización de servicios.

Temas

- [Prácticas recomendadas sobre las políticas](#)
- [Uso de la consola AWS Ground Station](#)
- [Cómo permitir a los usuarios consultar sus propios permisos](#)

Prácticas recomendadas sobre las políticas

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

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están

disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las [políticas administradas por AWS](#) o las [políticas administradas por AWS para funciones de 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 pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte [Políticas y permisos en IAM](#) en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo CloudFormation. Para obtener más información, consulte [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.

Uso de la consola 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, permita 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 administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API AWS CLI o AWS .

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "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 administrador es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar tareas como: PassRole

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

Algunos 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 la función 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 AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

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

Se puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Se puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que respaldan las políticas basadas en recursos o las 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, consulte [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 por AWS](#) en la Guía del usuario de IAM.

AWS política gestionada: AWSGround StationAgentInstancePolicy

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

Esta política otorga permisos de AWS Ground Station agente a su instancia de Amazon EC2 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

Para ver la versión más reciente del documento de política de JSON, consulte

[AWSGroundStationAgentInstancePolicy](#) la Guía de referencia de políticas administradas de AWS.

AWS política gestionada: `AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy`

No puede adjuntarse `AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy` 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 permisos a EC2 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 en su nombre información sobre las interfaces de red asociadas a las instancias EC2.

Para ver la versión más reciente del documento de política de JSON, consulte [AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy](#) la Guía de referencia de políticas administradas de AWS.

AWS Ground Station actualizaciones de las políticas AWS administradas

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, suscríbese a la fuente RSS de la página del historial del AWS Ground Station documento.

Cambio	Descripción	Fecha
AWSGroundStationAgentInstancePolicy : actualización de una política actual	AWS Ground Station se agregaron nuevos permisos para permitir a los agentes recuperar la respuesta a las tareas URLs para mejorar las operaciones de la Ground Station.	13 de noviembre de 2025
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 permisos a EC2 para	2 de noviembre de 2022

Cambio	Descripción	Fecha
	poder encontrar direcciones IPv4 públicas asociadas AWS Ground Station a las EIP e interfaces de red asociadas a las instancias de EC2.	
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. Ground Station predefine las funciones vinculadas al servicio 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:

`AWSServiceRoleForGroundStationDataflowEndpointGroup` AWS Ground Station usa este rol vinculado al servicio para invocar EC2 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 `AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy` 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 instancias EC2

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte [Permisos de roles vinculados a servicios](#) en la Guía del usuario de IAM.

Creación de un rol vinculado al servicio para Ground Station

No necesita crear manualmente un rol vinculado a servicios. 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 puede utilizar la consola de IAM para crear un rol vinculado al servicio con el caso de uso Entrega de datos a Amazon EC2. En la AWS CLI o en la AWS API, crea un rol vinculado 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 `AWSServiceRoleForGroundStationDataflowEndpointGroup` 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](#).

Resolución 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.

- **AWS claves propias:** AWS Ground Station utiliza estas claves de forma predeterminada para cifrar automáticamente los datos personales y directamente identificables y las efemérides. No puede ver, administrar ni usar claves AWS propias, ni auditar su uso; sin embargo, no es necesario realizar ninguna acción o cambiar los programas para proteger las claves que cifran los datos. [Para obtener más información, consulte las claves AWS propias en la AWS Key Management Service Guía para desarrolladores.](#)

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 inactivos; 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 en lugar del cifrado que ya posee. 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
 - Adición de etiquetas de

- Crear alias de clave
- Programar la eliminación de claves

Para obtener más información, consulte las [claves administradas por el cliente](#) en 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:	AWS cifrado de clave propia	Cifrado de claves administradas por el cliente (opcional)
Datos de efemérides utilizados para calcular la trayectoria de un satélite	Habilitado	Habilitado
Efemérides de elevación azimutal utilizadas para controlar las antenas	Habilitado	Habilitado

Note

AWS Ground Station habilita automáticamente el cifrado en reposo y se utiliza Claves propiedad de AWS para proteger los datos de identificación personal sin coste alguno. Sin embargo, se aplican AWS KMS cargos por el uso de una clave gestionada por el cliente. Para obtener más información acerca de los precios, consulte [Precios de AWS Key Management Service](#).

Para obtener más información AWS KMS, consulte la [Guía para AWS Key Management Service desarrolladores](#).

Para obtener información específica sobre cada tipo de recurso, consulte:

- [Cifrado en reposo para datos de efemérides TLE y OEM](#)
- [Cifrado en reposo para efemérides de elevación de acimut](#)

Creación de una clave administrada por el cliente

Puede crear una clave simétrica gestionada por el cliente mediante el Consola de administración de AWS, o el AWS KMS 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 [AWS Key Management Service desarrolladores](#).

Descripción general de las políticas clave

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 AWS Key Management Service desarrolladores.

Para utilizar la clave gestionada por el cliente con AWS Ground Station los recursos, debe configurar la política de claves para conceder los permisos adecuados al AWS Ground Station servicio. Los permisos específicos y la configuración de la política dependen del tipo de recurso que se esté cifrando:

- Para obtener información sobre las efemérides de TLE y OEM, consulte los requisitos y [Cifrado en reposo para datos de efemérides TLE y OEM](#) ejemplos específicos de las políticas clave.
- Para obtener datos sobre las efemérides de elevación del acimut, consulte [Cifrado en reposo para efemérides de elevación de acimut](#) los requisitos y ejemplos específicos de las políticas clave.

Note

La configuración de políticas clave difiere según los tipos de efemérides. Los datos de efemérides TLE y OEM utilizan concesiones para el acceso a las claves, mientras que las efemérides de elevación acimutal utilizan permisos de política de clave directa. Asegúrese de configurar su política de claves de acuerdo con el tipo de recurso específico que esté cifrando.

Para obtener más información sobre la [especificación de los permisos en una política y la solución de problemas de acceso a las claves](#), consulta la Guía para AWS Key Management Service desarrolladores.

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 (TLE, OEM y elevación de acimut)

Al crear un recurso, puede especificar la clave de datos proporcionando una kmsKeyArn

- kmsKeyArn- Un [identificador clave](#) para una clave gestionada por el AWS KMS cliente

AWS Ground Station contexto de cifrado

Un [contexto de cifrado](#) es un conjunto opcional de pares clave-valor que contienen información contextual adicional sobre los datos. AWS KMS utiliza el contexto de cifrado como datos autenticados adicionales para respaldar 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 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.

Para obtener información sobre el contexto de cifrado específico del recurso, consulte:

- [Cifrado en reposo para datos de efemérides TLE y OEM](#)
- [Cifrado en reposo para efemérides de elevación de acimut](#)

Cifrado en reposo para datos de efemérides TLE y OEM

Requisitos políticos clave para las efemérides de TLE y OEM

Para utilizar una clave gestionada por el cliente con datos de efemérides, tu política de claves debe conceder los siguientes permisos al servicio: AWS Ground Station

- [kms:CreateGrant](#)- Crea una concesión de acceso a una clave gestionada por el cliente. Concede AWS Ground Station acceso para realizar [operaciones de concesión](#) con la clave gestionada por el cliente para leer y almacenar datos cifrados.
- [kms:DescribeKey](#)- Proporciona los detalles de la clave gestionada por el cliente AWS Ground Station para poder validarla antes de intentar utilizar la clave proporcionada.

Para obtener más información sobre el [uso de las subvenciones](#), consulta la Guía para AWS Key Management Service desarrolladores.

Permisos de usuario de IAM para crear efemérides con claves administradas por el cliente

Cuando AWS Ground Station utiliza una clave gestionada por el cliente en las operaciones criptográficas, actúa en nombre del usuario que está creando el recurso de efemérides.

Para crear un recurso de efemérides con una clave administrada por el cliente, el usuario debe tener permisos para realizar las siguientes operaciones en la clave administrada por el cliente:

- [kms:CreateGrant](#)- Permite al usuario crear subvenciones en la clave gestionada por el cliente en nombre de. AWS Ground Station
- [kms:DescribeKey](#)- Permite al usuario ver los detalles de la clave gestionada por el cliente para validarla.

Puede especificar estos permisos necesarios en una política de claves o en una política de IAM si lo permite la política de claves. Estos permisos garantizan que los usuarios puedan autorizar AWS Ground Station el uso de la clave gestionada por el cliente para las operaciones de cifrado en su nombre.

¿Cómo se AWS Ground Station utilizan las subvenciones AWS KMS para las efemérides

AWS Ground Station requiere una [concesión de clave](#) para utilizar la clave gestionada 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 solicitud a [CreateGrant](#) AWS KMS. Las subvenciones AWS KMS se utilizan para dar AWS Ground Station acceso a una AWS KMS clave de tu cuenta.

Esto permite AWS Ground Station 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.
- Llame a [Decrypt](#) para utilizar 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](#).

Puedes revocar el acceso a la subvención en cualquier momento. Si lo haces, AWS Ground Station no podrás acceder a ninguno de los datos cifrados por la clave gestionada 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.

Contexto de cifrado de efemérides

Las concesiones clave para cifrar los recursos de efemérides están vinculadas a un ARN de satélite específico.

```
"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"
}
```

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.

El siguiente ejemplo muestra una política clave para los datos de efemérides enlazados a un satélite:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow AWS Ground Station to Describe key",
      "Effect": "Allow",
      "Principal": {
        "Service": "groundstation.us-east-1.amazonaws.com"
      },
      "Action": "kms:DescribeKey",
      "Resource": "*"
    },
    {
      "Sid": "Allow AWS Ground Station to Create Grant on key",
      "Effect": "Allow",
      "Principal": {
        "Service": "groundstation.us-east-1.amazonaws.com"
      },
    },
  ]
}
```

```

    "Action": "kms:CreateGrant",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "kms:EncryptionContext:aws:groundstation:arn":
"arn:aws:groundstation::123456789012:satellite/satellite-id"
      }
    }
  ]
}

```

Supervisión de las claves de cifrado para detectar efemérides

Cuando utilizas una clave gestionada por el AWS Key Management Service cliente con tus recursos de efemérides, puedes utilizar los [CloudWatch registros de AWS CloudTrailAmazon](#) para realizar un seguimiento de las solicitudes que se AWS Ground Station envían a. AWS KMS Los siguientes ejemplos son CloudTrail eventos para [CreateGrantdescifrar](#) y monitorear AWS KMS las operaciones solicitadas para acceder [DescribeKey](#) AWS Ground Station a los datos cifrados por su clave administrada por el cliente. [GenerateDataKey](#)

CreateGrant

Cuando utilizas una clave gestionada por el AWS KMS cliente para cifrar tus recursos efemérides, AWS Ground Station envía una [CreateGrant](#)solicitud en tu nombre para acceder a la AWS KMS clave de tu cuenta. AWS La concesión que se AWS Ground Station crea es específica del recurso asociado a la clave gestionada por el AWS KMS cliente. Además, AWS Ground Station utiliza la [RetireGrant](#)operación para eliminar una concesión al eliminar un recurso.

El siguiente evento de ejemplo registra la [CreateGrant](#)operación de una efeméride:

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "ASIAIOSFODNN7EXAMPLE",
    "arn": "arn:aws:sts::111122223333:assumed-role/Admin/SampleUser01",
    "accountId": "111122223333",
    "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {

```

```

        "type": "Role",
        "principalId": "ASIAIOSFODNN7EXAMPLE",
        "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": "AWS Internal",
"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

Cuando utilizas una clave gestionada por el AWS KMS cliente para cifrar tus recursos de efemérides, AWS Ground Station envía una [DescribeKey](#) solicitud en tu nombre para validar que la clave solicitada existe en tu cuenta.

El siguiente evento de ejemplo registra la operación [DescribeKey](#):

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "ASIAIOSFODNN7EXAMPLE",
    "arn": "arn:aws:sts::111122223333:assumed-role/User/Role",
    "accountId": "111122223333",
    "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "ASIAIOSFODNN7EXAMPLE",
        "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

Cuando utilizas una clave gestionada por el AWS KMS cliente para cifrar tus recursos de efemérides, AWS Ground Station envía una [GenerateDataKey](#) solicitud a para generar una clave de datos con la que cifrar tus datos.

El siguiente evento de ejemplo registra la [GenerateDataKey](#) operación de una efeméride:

```

{
  "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

Cuando utiliza una clave gestionada por el AWS KMS cliente para cifrar los recursos de efemérides, AWS Ground Station utiliza la operación de descifrado 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 evento de ejemplo registra la operación de descifrado de una efeméride:](#)

```
{
  "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 en reposo para efemérides de elevación de acimut

Requisitos normativos clave para las efemérides de elevación del acimut

Para usar una clave administrada por el cliente con datos de efemérides de elevación del acimut, tu política de claves debe conceder los siguientes permisos al servicio. AWS Ground Station A diferencia de los datos de efemérides TLE y OEM, que utilizan concesiones, las efemérides de elevación azimutal utilizan permisos de política de clave directa para las operaciones de cifrado. Se trata de un método más sencillo para administrar los permisos y utilizar las claves.

- [kms:GenerateDataKey](#)- Genera claves de datos para cifrar los datos de efemérides de elevación del acimut.
- [kms:Decrypt](#)- Descifra las claves de datos cifradas al acceder a sus datos de efemérides de elevación azimutal.

Ejemplo de política de claves que concede AWS Ground Station acceso a una clave gestionada por el cliente

Note

Con las efemérides de elevación de acimut, debe configurar estos permisos directamente en la política clave. Al director del AWS Ground Station servicio regional (por ejemplo, `groundstation.region.amazonaws.com`) se le deben conceder estos permisos en sus declaraciones de política clave. Si no se añaden estas declaraciones a la política clave, no AWS Ground Station podrá almacenar ni acceder a sus efemérides de elevación de acimut personalizadas.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```

    "Sid": "Allow AWS Ground Station to Describe key",
    "Effect": "Allow",
    "Principal": {
      "Service": "groundstation.us-east-1.amazonaws.com"
    },
    "Action": "kms:DescribeKey",
    "Resource": "*"
  },
  {
    "Sid": "Allow AWS Ground Station to Encrypt and Decrypt with key",
    "Effect": "Allow",
    "Principal": {
      "Service": "groundstation.us-east-1.amazonaws.com"
    },
    "Action": [
      "kms:GenerateDataKey",
      "kms:Decrypt"
    ],
    "Resource": "*"
  }
]
}

```

Permisos de usuario de IAM para crear efemérides de elevación de acimut con claves administradas por el cliente

Cuando se AWS Ground Station utiliza una clave gestionada por el cliente en las operaciones criptográficas, actúa en nombre del usuario que está creando el recurso de efemérides de elevación de acimut.

Para crear un recurso de efemérides de elevación azimutal con una clave administrada por el cliente, el usuario debe tener permisos para realizar las siguientes operaciones en la clave administrada por el cliente:

- [kms:GenerateDataKey](#)- Permite al usuario generar claves de datos para cifrar los datos de las efemérides de elevación azimutal.
- [kms:Decrypt](#)- Permite al usuario descifrar las claves de datos al acceder a los datos de las efemérides de elevación azimutal.
- [kms:DescribeKey](#)- Permite al usuario ver los detalles de las claves gestionadas por el cliente para validar la clave.

Puede especificar estos permisos necesarios en una política de claves o en una política de IAM si lo permite la política de claves. Estos permisos garantizan que los usuarios puedan autorizar AWS Ground Station el uso de la clave gestionada por el cliente para las operaciones de cifrado en su nombre.

¿Cómo AWS Ground Station utiliza las políticas clave para las efemérides de elevación del acimut

Cuando proporciona datos de efemérides de elevación del acimut con una clave administrada por el cliente, utiliza políticas de claves para acceder a su clave de cifrado. AWS Ground Station Los permisos se otorgan directamente mediante declaraciones de políticas clave y no AWS Ground Station mediante subvenciones, como ocurre con los datos de efemérides de TLE o OEM.

Si AWS Ground Station eliminan el acceso a la clave gestionada por el cliente, AWS Ground Station no podrás acceder a ninguno de los datos cifrados por esa clave, lo que afectará a las operaciones que dependen de esos datos. Por ejemplo, si eliminan los permisos de política clave para las efemérides de elevación de acimut que actualmente se utilizan para un contacto, no AWS Ground Station podrá utilizar los datos de elevación de acimut proporcionados para controlar la antena durante el contacto. Esto provocará que el contacto finalice con un estado de FALLIDO.

Contexto de cifrado de efemérides de elevación azimutal

[Cuando AWS Ground Station utiliza su AWS KMS clave para cifrar los datos de efemérides de elevación del acimut, el servicio especifica un contexto de cifrado.](#) El contexto de cifrado son datos autenticados adicionales (AAD) que se utilizan para garantizar la integridad de los datos. AWS KMS Cuando se especifica un contexto de cifrado para una operación de cifrado, el servicio debe especificar el mismo contexto de cifrado para la operación de descifrado. De lo contrario, el descifrado produce un error. El contexto de cifrado también se escribe en sus CloudTrail registros para ayudarle a entender por qué se utilizó una AWS KMS clave determinada. Sus CloudTrail registros pueden contener muchas entradas que describen el uso de una AWS KMS clave, pero el contexto de cifrado de cada entrada de registro puede ayudarle a determinar el motivo de ese uso concreto.

AWS Ground Station especifica el siguiente contexto de cifrado cuando realiza operaciones criptográficas con la clave administrada por el cliente en una efeméride de elevación de acimut:

```
{
  "encryptionContext": {
    "aws:groundstation:ground-station-id": "Ohio 1",
```

```

    "aws:groundstation:arn": "arn:aws:groundstation:us-
east-2:111122223333:ephemeris/00a770b0-082d-45a4-80ed-SAMPLE",
    "aws:s3:arn": "arn:aws:s3:::customerephemerisbucket/00a770b0-082d-45a4-80ed-
SAMPLE/raw"
  }
}

```

El contexto de cifrado contiene:

`aws:groundstation:ground-station-id`

El nombre de la estación terrestre asociada a las efemérides de elevación del acimut.

`aws: estación terrestre: arn`

El ARN del recurso de efemérides.

`aws:s3:arn`

El ARN de las efemérides almacenadas en Amazon S3.

Utilizar el contexto de cifrado para controlar el acceso a la clave administrada por el cliente

Puede utilizar las declaraciones de condición de IAM para controlar el AWS Ground Station acceso a la clave gestionada por el cliente. Añadir una declaración de condición a `kms:Decrypt` las acciones `kms:GenerateDataKey` y restringe las estaciones terrestres para las que se AWS KMS puede utilizar a.

Los siguientes son ejemplos de declaraciones de políticas clave para conceder AWS Ground Station acceso a su clave gestionada por el cliente en una región específica para una estación terrestre específica. La condición de esta declaración de política exige que todos los accesos cifren y descifren a la clave que especifique un contexto de cifrado que coincida con la condición de la política de claves.

Ejemplo de política de claves que permite el AWS Ground Station acceso a una clave gestionada por el cliente para una estación terrestre específica

JSON

```
{
```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "Allow AWS Ground Station to Describe key",
    "Effect": "Allow",
    "Principal": {
      "Service": "groundstation.us-east-1.amazonaws.com"
    },
    "Action": "kms:DescribeKey",
    "Resource": "*"
  },
  {
    "Sid": "Allow AWS Ground Station to Encrypt and Decrypt with key",
    "Effect": "Allow",
    "Principal": {
      "Service": "groundstation.us-east-1.amazonaws.com"
    },
    "Action": [
      "kms:GenerateDataKey",
      "kms:Decrypt"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "kms:EncryptionContext:aws:groundstation:ground-station-id":
"specific-ground-station-name"
      }
    }
  }
]
}

```

Ejemplo de política clave que otorga AWS Ground Station acceso a una clave administrada por el cliente para varias estaciones terrestres

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {

```

```

    "Sid": "Allow AWS Ground Station to Describe key",
    "Effect": "Allow",
    "Principal": {
      "Service": "groundstation.us-east-1.amazonaws.com"
    },
    "Action": "kms:DescribeKey",
    "Resource": "*"
  },
  {
    "Sid": "Allow AWS Ground Station to Encrypt and Decrypt with key",
    "Effect": "Allow",
    "Principal": {
      "Service": "groundstation.us-east-1.amazonaws.com"
    },
    "Action": [
      "kms:GenerateDataKey",
      "kms:Decrypt"
    ],
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:EncryptionContext:aws:groundstation:ground-station-id":
        [
          "specific-ground-station-name-1",
          "specific-ground-station-name-2"
        ]
      }
    }
  }
]
}

```

Supervisión de las claves de cifrado para detectar efemérides de elevación del acimut

[Cuando utilizas una clave gestionada por el AWS KMS cliente con tus recursos de efemérides de elevación del acimut, puedes utilizarla o registrarla para hacer un seguimiento de las solicitudes que se envían a. CloudTrail CloudWatch](#) AWS Ground Station AWS KMS Los siguientes ejemplos son CloudTrail eventos de [Decrypt](#) para [GenerateDataKey](#)supervisar AWS KMS las operaciones solicitadas para acceder AWS Ground Station a los datos cifrados por la clave gestionada por el cliente.

GenerateDataKey

Cuando utiliza una clave gestionada por el AWS KMS cliente para cifrar sus recursos de efemérides de elevación del acimut, AWS Ground Station envía una [GenerateDataKey](#) solicitud a para AWS KMS generar una clave de datos con la que cifrar los datos.

El siguiente evento de ejemplo registra la operación de las efemérides de elevación acimutal:

[GenerateDataKey](#)

```
{
  "eventVersion": "1.11",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "ASIAIOSFODNN7EXAMPLE",
    "arn": "arn:aws:sts::111122223333:assumed-role/Admin/SampleUser01",
    "accountId": "111122223333",
    "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "ASIAIOSFODNN7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:role/Admin",
        "accountId": "111122223333",
        "userName": "Admin"
      },
      "attributes": {
        "creationDate": "2025-08-25T14:45:48Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "invokedBy": "AWS Internal"
},
"eventTime": "2025-08-25T14:52:02Z",
"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:us-west-2:111122223333:ephemeris/bb650670-7a4b-4152-bd60-SAMPLE",
```

```

        "aws:groundstation:ground-station-id": "Ohio 1",
        "aws:s3:arn": "arn:aws:s3:::customerephemerisbucket/bb650670-7a4b-4152-
bd60-SAMPLE/raw"
    },
    "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
},
"responseElements": null,
"requestID": "ef6f9a8f-8ef6-46a1-bdcb-123456SAMPLE",
"eventID": "952842d4-1389-3232-b885-123456SAMPLE",
"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": "8424f6b6-2280-4d1d-b9fd-0348b1546cba",
"eventCategory": "Management"
}

```

Decrypt

Cuando utiliza una clave administrada por el AWS KMS cliente para cifrar sus recursos de efemérides de elevación de acimut, AWS Ground Station utiliza la operación de descifrado para [descifrar](#) los datos de efemérides de elevación de acimut proporcionados si ya están cifrados con la misma clave administrada por el cliente.

[El siguiente evento de ejemplo registra la operación de descifrado para las efemérides de elevación azimutal:](#)

```

{
  "eventVersion": "1.11",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "ASIAIOSFODNN7EXAMPLE",
    "arn": "arn:aws:sts::111122223333:assumed-role/Admin/SampleUser01",
    "accountId": "111122223333",

```

```

    "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "ASIAIOSFODNN7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:role/Admin",
        "accountId": "111122223333",
        "userName": "Admin"
      }
    },
    "attributes": {
      "creationDate": "2025-08-25T14:45:48Z",
      "mfaAuthenticated": "false"
    }
  },
  "invokedBy": "AWS Internal",
  "eventTime": "2025-08-25T14:54:01Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "Decrypt",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "requestParameters": {
    "encryptionContext": {
      "aws:groundstation:arn": "arn:aws:groundstation:us-
west-2:111122223333:ephemeris/bb650670-7a4b-4152-bd60-SAMPLE",
      "aws:groundstation:ground-station-id": "Ohio 1",
      "aws:s3:arn": "arn:aws:s3:::customerephemerisbucket/bb650670-7a4b-4152-
bd60-SAMPLE/raw"
    },
    "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
  },
  "responseElements": null,
  "requestID": "a2f46066-49fb-461a-93cb-123456SAMPLE",
  "eventID": "e997b426-e3ad-31c7-a308-123456SAMPLE",
  "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": "477b568e-7f56-4f04-905c-623ff146f30d",
"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 instancias de Amazon EC2 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 su instancia de Amazon EC2 descifrá 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 conceden 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 ninguna 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](#)
- [Satélite de transmisión pública que utiliza la entrega de datos de Amazon S3](#)
- [Satélite de transmisión pública que utiliza un punto final de flujo de datos \(banda estrecha\)](#)
- [Satélite de transmisión pública que utiliza un punto final de flujo de datos \(demodulado y decodificado\)](#)
- [Satélite de transmisión pública que utiliza AWS Ground Station Agent \(banda ancha\)](#)

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

La 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 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 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 CloudFormation plantilla: las secciones de parámetros y recursos.

Note

Para obtener más información sobre el contenido de una 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 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 CloudFormation pila. Consulte [AWS Ground Station Imágenes de máquinas de Amazon \(AMIs\)](#).

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

```

```

SnpJPSSMissionProfile:

```

```

  Type: AWS::GroundStation::MissionProfile

```

```

  Properties:

```

```

    Name: "37849 SNPP And 43013 JPSS"

```

```

    ContactPrePassDurationSeconds: 120

```

```

    ContactPostPassDurationSeconds: 60

```

```

    MinimumViableContactDurationSeconds: 180

```

```

    TrackingConfigArn: !Ref TrackingConfig

```

```

    DataflowEdges:

```

```

      - Source: !Ref SnpJPSSDownlinkDigIfAntennaConfig

```

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

La 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 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 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 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 CloudFormation plantilla: las secciones de parámetros y recursos.

Note

Para obtener más información sobre el contenido de una 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 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 CloudFormation pila. Consulte [AWS Ground Station Imágenes de máquinas de Amazon \(AMIs\)](#).

Los fragmentos de plantilla restantes pertenecen a la sección Recursos de la 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":"Mpsps"
    },
    "range":{
        "value":0.75,
        "units":"kpsps"
    },
    "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"
      }
    },
    "NrzDecoder":{
      "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 CloudFormation plantilla completa que incluye todos los recursos descritos en esta sección combinados en una sola plantilla que se puede utilizar directamente. CloudFormation

La 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 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 `.yaml` 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.yaml .
```

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.yaml
```

Puede especificar la plantilla directamente en CloudFormation el siguiente enlace:

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

¿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 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 CloudFormation plantilla, consulta las secciones de [plantillas](#).

Empezará por configurar una sección de mapeos en la 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 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 CloudFormation pila. Consulte [AWS Ground Station Imágenes de máquinas de Amazon \(AMIs\)](#).

Los fragmentos de plantilla restantes pertenecen a la sección Recursos de la 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::VPCEGatewayAttachment
```

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

La 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 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 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 `.yaml` 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.yaml .
```

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.yaml
```

Puede especificar la plantilla directamente en CloudFormation el siguiente enlace:

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

¿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 `PublicSubnetId` si 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 `PublicSubnetId` se especifica. Esto requiere que haga `SubnetId` referencia 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 `PublicSubnetId` se 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?](#)

Resolución 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](#)
- [Solucionar problemas de contactos fallidos](#)
- [Solucionar problemas de contactos de FAILED_TO_SCHEDULE](#)
- [Solucione el problema DataflowEndpointGroups si no se encuentra en un estado SALUDABLE](#)
- [Solucionar problemas de efemérides no válidas](#)
- [Solucionar problemas de contactos que no recibieron datos](#)
- [Solucionar problemas de telemetría](#)

Solucionar problemas con los contactos que envían datos a Amazon EC2

Si no puede completar un AWS Ground Station contacto correctamente, tendrá que comprobar que su instancia de Amazon EC2 se está ejecutando, comprobar que la aplicación de punto final de flujo de datos se está ejecutando y comprobar que la transmisión de la aplicación de punto final de 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

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

Paso 1: Compruebe que la instancia EC2 se esté ejecutando

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

1. Busque la instancia de Amazon EC2 que se utilizó pcon el contacto cuyo problema está solucionando. Utilice los siguientes pasos:
 - a. En su CloudFormationpanel de control, seleccione la pila que contiene su instancia de Amazon EC2.
 - b. Seleccione la pestaña Recursos y localice su instancia de Amazon EC2 en la columna Logical ID. Asegúrese de que la instancia se ha creado en la columna Status (Estado).
 - c. En la columna ID física, seleccione el enlace de su instancia de Amazon EC2. Esto le llevará a la consola de administración de Amazon EC2.
2. En la consola de administración de Amazon EC2, asegúrese de que el estado de su instancia de Amazon EC2 se está ejecutando.
3. Si la instancia se está ejecutando, continúe en el paso siguiente. Si la instancia no está en ejecución, iníciela siguiendo este paso.
 - Con su instancia de Amazon EC2 seleccionada, seleccione Actions (Acciones) > Instance State (Estado de la instancia) > Start (Iniciar).

Paso 2: 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 se conecte a su 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. Abra un terminal o símbolo del sistema y conéctese a la instancia de Amazon EC2 mediante SSH. Reenvía el puerto 80 del host remoto para ver la interfaz de usuario DataDefender web. Los siguientes comandos indican cómo utilizar SSH para conectarse a una instancia de Amazon EC2 a través de un bastión con el reenvío de puertos habilitado.

 Note

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

Para Windows

```
ssh -L 8080:localhost:80 -o ProxyCommand="C:\Windows\System32\OpenSSH\ssh.exe -o
\"ForwardAgent yes\" -W %h:%p -i \"<SSH KEY>\" ec2-user@<BASTION HOST>" -i "<SSH
KEY>" ec2-user@<HOST>
```

Para Mac

```
ssh -L 8080:localhost:80 -o ProxyCommand="ssh -A -o 'ForwardAgent yes' -W %h:%p -i
<SSH KEY> ec2-user@<BASTION HOST>" -i <SSH KEY> ec2-user@<HOST>
```

2. Compruebe que DataDefender (también denominado DDX) se esté ejecutando agregando (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

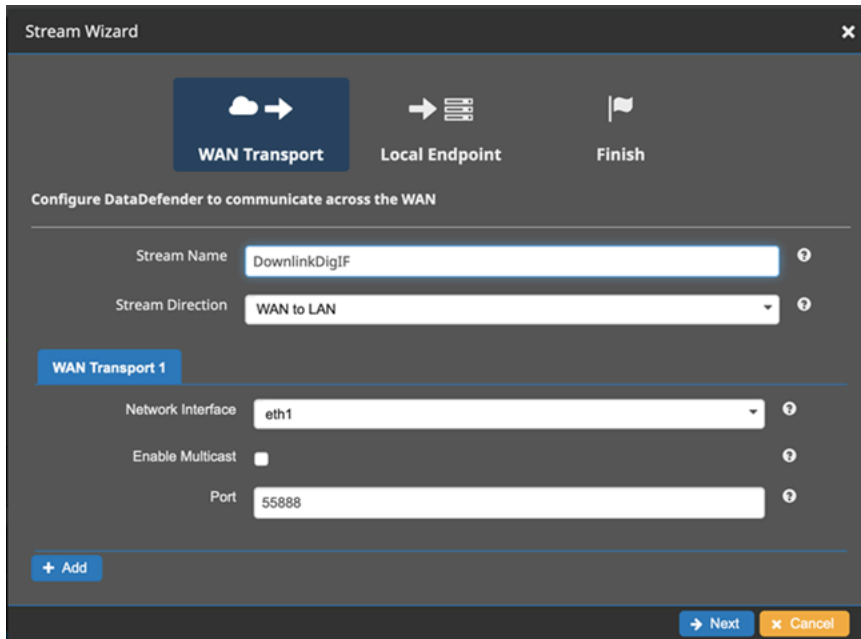
Un problema común detectado al inspeccionar estos archivos es que la Amazon VPC en la que se ejecuta la instancia de Amazon EC2 no tiene acceso a Amazon S3 para descargar los archivos de instalación. Si descubre en sus registros que este es el problema, compruebe la configuración de Amazon VPC y del grupo de seguridad de su instancia EC2 para asegurarse de que no están bloqueando el acceso a Amazon S3.

Si 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.

The screenshot shows the 'Stream Wizard' interface with three steps: 'WAN Transport', 'Local Endpoint', and 'Finish'. The 'Local Endpoint' step is active. Below the step indicators, the text reads 'Configure DataDefender to communicate with a local endpoint'. Under the 'Local Endpoint 1' section, the following fields are visible: 'Network Interface' (dropdown menu showing 'lo'), 'Protocol' (dropdown menu showing 'UDP'), 'Enable Multicast' (checkbox), 'Local Consumer' (text input showing '127.0.0.1'), and 'Port' (text input showing '50000'). At the bottom, there are navigation buttons: '+ Add', '< Previous', 'Next >', and 'Cancel'.

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

Ahora se ha asegurado de que su instancia de Amazon EC2 DataDefender se ejecutan y configuran correctamente para recibir datos desde ella. 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. Está solucionando el problema de cada instancia de receptor Amazon EC2 que se utilizó para el contacto. Utilice los siguientes pasos:
 - a. En su CloudFormation panel de control, seleccione la pila que contiene su instancia de Amazon EC2.
 - b. Seleccione la pestaña Recursos y localice su instancia de Amazon EC2 en la columna Logical ID. Asegúrese de que la instancia se ha creado en la columna Status (Estado).
 - c. En la columna ID física, seleccione el enlace de su instancia de Amazon EC2. Esto le llevará a la consola de administración de Amazon EC2.

2. En la consola de administración de Amazon EC2, busque y haga clic en el enlace del ID de subred del resumen de instancias de la instancia receptora Amazon EC2. 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 receptor Amazon EC2, haga lo siguiente:
 - a. Actualice la subred CidrBlock correspondiente de la CloudFormation plantilla para 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. 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 fallido y no está destinada a otros estados de error, como `AWS_FAILED`, `AWS_CANCELLED`, o `FAILED_TO_SCHEDULE`. Para obtener más información sobre los estados del contacto, consulte [the section called “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.
- La subred del punto final de Dataflow no es válida; su solución AWS Ground Station de entrega de datos no puede crear un ENI en su red privada porque no puede acceder a la subred proporcionada especificada en el grupo de puntos finales de Dataflow.

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

- Confirme que la instancia Amazon EC2 receptora se haya iniciado correctamente antes de la hora de inicio del contacto.
- Confirme que el software del 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.
- Asegúrese de que las subredes asociadas a su grupo de puntos finales de flujo de datos, a través de los flujos de datos configurados en, permanezcan activas y disponibles para él. [Instalación y configuración de Amazon VPC](#) 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.

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:

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

Consulte la sección en [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 la instancia EC2, que registrará el agente.enga en cuenta que debe tener un archivo de configuración del controlador válido para que esta llamada se realice correctamente. Consulte la [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 de conexión de Dataflow y, a continuación, utilice la `CreateDataflowEndpointGroup` API para volver a crear el grupo de puntos de conexión de Dataflow con las direcciones IP y los puertos asociados a la instancia de EC2.
- **UNVERIFIED_IP_OWNERSHIP**- La dirección IP aún no se ha validado. La validación se realiza periódicamente, por lo que debería resolverse por sí sola.
- **NOT_AUTHORIZED_TO_CREATE_SLR**- La cuenta no está autorizada para crear el rol vinculado al servicio necesario. Consulte los pasos de solución de problemas en [Utilice funciones vinculadas a servicios para Ground Station](#)

Solucionar problemas de efemérides no válidas

Al cargar datos de efemérides en, estos pasan por un flujo de trabajo de AWS Ground Station validación asíncrono. Si se produce un error en la validación, el estado de las efemérides cambiará a **INVALID** El mensaje de error de la [DescribeEphemeris](#) respuesta proporciona información detallada para ayudarle a identificar y resolver el problema.

Descripción de los errores de validación de efemérides

Cuando una efeméride no pasa la validación, la respuesta de la [DescribeEphemeris](#) API incluye dos campos para ayudar a diagnosticar el problema:

`errorCode`

Un código legible por máquina que identifica el error de validación específico. Se puede utilizar para la gestión de errores programáticos.

`errorMessage`

Una descripción legible para los humanos del error de validación con detalles específicos sobre lo que salió mal y orientación sobre cómo solucionarlo.

Ejemplo de [DescribeEphemeris](#) respuesta para una efeméride no válida:

```
{
  "ephemerisId": "abc12345-6789-def0-1234-567890abcdef",
  "name": "My Invalid Ephemeris",
  "status": "INVALID",
  "creationTime": 1620254718.765,
  "invalidReason": "METADATA_INVALID",
  "errorCode": "OBJECT_NAME_MISSING",
  "errorMessage": "Metadata field missing: OBJECT_NAME",
  "suppliedData": {
    "tle": {
      "ephemerisData": "[...]"
    }
  }
}
```

Errores de validación comunes para las efemérides TLE

Los siguientes son errores de validación comunes que se producen al cargar las efemérides de TLE:

El número de catálogo de satélites no coincide

Error: «El número de catálogo de satélites presente en las efemérides no coincide con el número de catálogo de satélites del satélite asociado»

Solución: compruebe que el número de ID/satellite catálogo del NORAD de las líneas TLE coincide con el número de catálogo de satélites del satélite. `00000` Utilícelo para satélites sin un número de catálogo asignado.

Movimiento medio no válido

Error: «El movimiento medio de las efemérides proporcionadas difiere demasiado del movimiento de las efemérides de referencia más recientes»

Solución: compruebe que los datos de TLE son correctos y representan una órbita válida. Ground Station utiliza las efemérides de Space-Track como referencia durante la validación.

Errores de validación comunes en las efemérides OEM

Los siguientes son errores de validación comunes que se producen al cargar efemérides OEM:

Marco de referencia no válido

Error: «El REF_FRAME no es compatible»

Solución: actualice el archivo OEM para utilizar uno de los marcos de referencia compatibles: EME2000 o. ITRF2000

Faltan campos obligatorios

Error: «Falta el campo de metadatos: INTERPOLACIÓN»

Solución: añada los campos INTERPOLATION e INTERPOLATION_DEGREE a la sección de metadatos OEM. Estos son necesarios para generar ángulos de orientación de antena AWS Ground Station precisos.

Sistema de tiempo no compatible

Error: «El TIME_SYSTEM no es compatible»

Solución: asegúrese de que su archivo OEM utilice UTC como sistema horario.

Versión OEM no compatible

Error: «El CCSDS_OEM_VERS no es compatible»

Solución: asegúrese de que su archivo OEM utilice la versión 2.0 del CCSDS OEM.

Errores de validación comunes para las efemérides de elevación azimutal

Los siguientes son errores de validación comunes que se producen al cargar efemérides de elevación azimutal:

Faltan datos azimuth/elevation

Error: «No había TimeAzEl campos en al menos uno AzElSegment»

Solución: asegúrese de que cada segmento de los datos de elevación del acimut contenga al menos un par marcado con el tiempo. azimuth/elevation

Rango de ángulos acimutales (grados) no válido

Error: «AzEl az debe ser mayor o igual a -180 y menor o igual a 360 grados»

Solución: compruebe que los ángulos acimutales estén dentro de [-180, 360] grados.

Rango de ángulos de elevación (grados) no válido

Error: «AzEl el debe ser mayor o igual a -90 y menor o igual a 90 grados»

Solución: compruebe que los ángulos de elevación estén dentro de [-90, 90] grados.

Rango de ángulos de acimut (radianes) no válido

Error: «AzEl az debe ser mayor o igual que -pi y menor o igual que 2pi radianes»

Solución: compruebe que los ángulos acimutales estén dentro de $[-\pi, 2\pi]$ radianes.

Rango de ángulos de elevación (radianes) no válido

Error: «AzEl el debe ser mayor o igual que $-\pi/2$ y menor o igual que $\pi/2$ radianes»

Solución: compruebe que los ángulos de elevación estén dentro de $[-\pi/2, \pi/2]$ radianes.

Valores de tiempo no monótonos

Error: «Los TimeAzEl artículos incluidos en a AzElSegment deben estar en orden temporalmente»

Solución: asegúrese de que los valores de tiempo de cada segmento aumenten estrictamente.

Segmentos fuera de orden

Error: «AzElSegments debe estar temporalmente en orden»

Solución: asegúrese de que los segmentos estén organizados en orden cronológico.

Segmentos superpuestos

Error: «El intervalo de tiempo de al menos un segmento se superpone con otros intervalos de tiempo del segmento»

Solución: asegúrese de que cada segmento tenga un rango de tiempo único que no se superponga. El endTime de un segmento no debe superar el startTime del siguiente segmento.

Pasos para la solución de problemas

Si tu efeméride no pasa la validación, sigue estos pasos para resolver el problema:

1. Llama [DescribeEphemeris](#) con tu identificador de efemérides para recuperar la y. `errorCode` `errorMessage`

2. Revisa el mensaje de error para obtener detalles específicos sobre qué comprobación de validación ha fallado.
3. Corrija los problemas identificados en los datos de efemérides.
4. Cargue una nueva efeméride con los datos corregidos utilizando [CreateEphemeris](#)
5. Supervisa el estado de la nueva efeméride hasta que alcance el estado. ENABLED
6. Elimine las efemérides no válidas utilizando [DeleteEphemeris](#) si ya no son necesarias.

Referencia completa del código de error

Las siguientes secciones proporcionan un mapeo completo de todos los `errorCode` valores que pueden devolverse cuando se produce un error en la validación de las efemérides, organizados por categoría de alto nivel `invalidReason`.

Motivo no válido: **METADATA_INVALID**

Estos errores se producen cuando faltan campos de metadatos obligatorios, tienen un formato incorrecto o contienen valores no admitidos en los datos de efemérides.

Código de error	Mensaje de error
<code>_SATCAT_ID NO COINCIDE</code>	El número de catálogo de satélites presente en las efemérides de la TLE no coincide con el número de catálogo de satélites del satélite asociado
<code>OEM_VERSION_UNSUPPORTED</code>	No se admiten las <code>CCSDS_OEM_VERS</code> efemérides del OEM. Valores admitidos: [] 2.0
<code>ORIGINATOR_MISSING</code>	Falta el campo de <code>ORIGINATOR</code> encabezado en las efemérides del OEM
<code>FALTA LA FECHA DE CREACIÓN</code>	Falta el campo de <code>CREATION_DATE</code> encabezado en las efemérides del OEM
<code>FALTA EL NOMBRE_OBJETO</code>	Falta el campo de <code>OBJECT_NAME</code> metadatos en las efemérides del OEM

Código de error	Mensaje de error
OBJECT_ID_MISSING	Falta el campo de OBJECT_ID metadatos en las efemérides del OEM
REF_FRAME_UNSUPPORTED	No se admiten las REF_FRAME efemérides del OEM. Valores admitidos: [,] EME2000 ITRF2000
REF_FRAME_EPOCH_UNSUPPORTED	No se admite el campo de REF_FRAME_EPOCH metadatos de las efemérides OEM. Elimine este campo de las efemérides
TIME_SYSTEM_UNSUPPORTED	No se admiten las TIME_SYSTEM efemérides del OEM. Valores admitidos: [] UTC
CENTER_BODY_UNSUPPORTED	No se admiten las CENTER_BODY efemérides del OEM. Valores admitidos: [] Earth
FALTA INTERPOLACIÓN_	Falta el campo de INTERPOLATION metadatos en las efemérides del OEM
GRADO DE INTERPOLACIÓN NO VÁLIDO	El grado de interpolación de las efemérides OEM debe ser superior a 0 para el método de interpolación
AZ_EL_SEGMENT_LIST_MISSING	Falta el campo azElSegmentList
INSUFICIENT_TIME_AZ_EL	No había ningún campo en al menos una TimeAzElazElSegmentList

Motivo no válido: **TIME_RANGE_INVALID**

Estos errores se producen cuando las efemérides contienen intervalos de tiempo no válidos, como problemas con los start/end tiempos, el orden de los segmentos, la superposición de segmentos o las incoherencias temporales.

Código de error	Mensaje de error
TIME_START_IN_FUTURE	La hora de inicio de las efemérides está en el futuro, pero debe estar en el pasado
END_TIME_IN_PAST	Efemérides: el fin del tiempo está en el pasado, pero debe estar en el futuro
CADUCIDAD DEMASIADO TEMPRANA	La hora de caducidad proporcionada es anterior a la hora de finalización de la efeméride
START_TIME_METADATA_TOO_EARLY	El valor de los START_TIME metadatos es anterior a la primera vez que aparece en los datos de efemérides del OEM
STOP_TIME_METADATA_TOO_LATE	El valor de los STOP_TIME metadatos es posterior a la última vez que aparece en los datos de efemérides del OEM
AZ_EL_SEGMENT_END_TIME_BEFORE_START_TIME	El de al menos un segmento de datos está antes del segmento endTimestartTime
AZ_EL_SEGMENT_TIMES_OVERLAP	El intervalo de tiempo de al menos un segmento se superpone con otros intervalos de tiempo del segmento
AZ_EL_SEGMENTS_OUT_OF_ORDER	Los segmentos no están ordenados temporalmente
TIME_AZ_EL_ITEMS_OUT_OF_ORDER	Los artículos incluidos en un deben estar ordenados temporalmente TimeAzElAzElSegment
AZ_EL_SEGMENT_REFERENCE_EPOCH_INVALID	La época de referencia de un segmento no es válida o tiene un formato incorrecto
AZ_EL_SEGMENT_START_TIME_INVALID	La hora de inicio en el intervalo de tiempo válido de un segmento no comienza después del primer segmento
AZ_EL_SEGMENT_END_TIME_INVALID	La hora de finalización en el intervalo de tiempo válido de un segmento no termina después del último segmento

Código de error	Mensaje de error
AZ_EL_SEGMENT_VALID_TIME_RANGE_INVALID	El intervalo de tiempo válido para un segmento no es válido
AZ_EL_SEGMENT_END_TIME_TOO_LATE	La hora de finalización de un segmento supera la duración máxima permitida a partir de la época de referencia
AZ_EL_TOTAL_DURATION_EXCEEDED	La duración total en todos los segmentos supera la duración máxima permitida del ángulo de puntería

Motivo no válido: **TRAJECTORY_INVALID**

Estos errores se producen cuando la efeméride contiene datos de trayectoria no válidos, incluidos problemas con los parámetros orbitales, los rangos de ángulos o las unidades.

Código de error	Mensaje de error
MEAN_MOTION_INVALID	El movimiento medio de las efemérides TLE proporcionadas difiere demasiado de las efemérides de referencia más recientes. Nota: Ground Station utiliza las efemérides de Space-Track como referencia durante la validación
TIME_AZ_EL_AZ_RADIAN_RANGE_INVALID	AzEl az debe ser mayor o igual a $-\pi$ y menor o igual a 2π radianes
TIME_AZ_EL_EL_RADIAN_RANGE_INVALID	AzEl el debe ser mayor o igual que $-\pi/2$ y menor o igual que $\pi/2$ radianes
TIME_AZ_EL_AZ_DEGREE_RANGE_INVALID	AzEl az debe ser mayor o igual a -180 y menor o igual a 360 grados
TIME_AZ_EL_EL_DEGREE_RANGE_INVALID	AzEl el debe ser mayor o igual a -90 grados y menor o igual a 90 grados
TIME_AZ_EL_ANGLE_UNITS_INVALID	Unidades de ángulo no válidas AzEl

Motivo no válido: **KMS_KEY_INVALID**

Estos errores se producen cuando hay problemas con la clave de AWS Key Management Service (KMS) utilizada para cifrar los datos de efemérides.

Código de error	Mensaje de error
KMS_PERMISSIONS_INSUFFICIENTES	Ground Station no tiene permisos suficientes para acceder a la clave KMS de esta efeméride

Motivo no válido: **VALIDATION_ERROR**

Estos errores se producen cuando hay problemas generales de validación con los datos de efemérides que no se incluyen en las otras categorías específicas.

Código de error	Mensaje de error
INTERNAL_ERROR	Se produjo un error interno durante la validación de las efemérides
FILE_FORMAT_INVALID	El formato del archivo de efemérides no es válido o está dañado. Compruebe que el archivo se ajusta al formato esperado para el tipo de efemérides

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 [Comprenda cómo AWS Ground Station usa las efemérides](#)

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, consulte [Comprenda 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_CANCELLED` estado `AWS_FAILED`. 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](#).

Solucionar problemas de telemetría

Utilice la siguiente información para solucionar problemas comunes relacionados con la telemetría.

Problemas comunes de configuración

Errores de permisos de IAM

Síntomas

Cuando llamas `CreateConfig` para crear un `TelemetrySinkConfig`, recibes un mensaje de error:

```
Unable to write to Kinesis Data Streams stream. Ensure that Ground Station has kinesis:PutRecord permissions for the given stream
```

Causas

- El rol de IAM especificado en el `TelemetrySinkConfig` no tiene los permisos necesarios para escribir en la transmisión de Kinesis Data Streams.
- La política de confianza del rol de IAM no permite AWS Ground Station asumir el rol.
- El ARN de la transmisión de Kinesis Data Streams que aparece en `TelemetrySinkConfig` es incorrecto o la transmisión no existe.

Soluciones

1. Compruebe que el rol de IAM existe y tiene los permisos correctos. Revise [Paso 2: Crear un TelemetrySinkConfig](#) y asegúrese de que se hayan seguido todos los pasos.
2. Compruebe si AWS Ground Station puede asumir su función de IAM:

```
aws iam get-role --role-name GroundStationTelemetryRole
```

Compruebe que la política de confianza `groundstation.amazonaws.com` se incluye como principio de servicio de confianza.

3. Compruebe que el rol de IAM tenga los permisos de Kinesis necesarios:

```
aws iam list-attached-role-policies --role-name GroundStationTelemetryRole
```

Asegúrese de que la política incluya `kinesis:DescribeStream` y `kinesis:PutRecord` los `kinesis:PutRecords` permisos para su transmisión.

4. Compruebe que la transmisión de Kinesis Data Streams existe y que el ARN es correcto:

```
aws kinesis describe-stream \  
  --stream-name your-stream-name \  
  --region us-east-2
```

5. Si utiliza un cifrado administrado por el cliente, compruebe que el rol de IAM tenga `kms:GenerateDataKey` permiso para su clave. AWS KMS

PassRole errores de permisos

Síntomas

Cuando llamas `CreateConfig`, recibes un mensaje de error que indica que no tienes permiso para pasar a la función de IAM.

Solución

Asegúrese de que su usuario o rol de IAM tenga `iam:PassRole` permiso para el rol de IAM de telemetría. Añada la siguiente política a su usuario o rol:

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "iam:GetRole",  
        "iam:PassRole"  
      ],  
      "Resource": "arn:aws:iam::9999999999:role/your-stream-name"  
    }  
  ]  
}
```

Problemas de configuración de transmisiones de Kinesis Data Streams

Síntomas

El suministro de telemetría falla o es intermitente.

Causas

- La transmisión de Kinesis Data Streams no tiene suficiente capacidad para el rendimiento de telemetría.
- Otras aplicaciones utilizan la transmisión, lo que provoca una ralentización de la escritura.

Soluciones

1. Compruebe el estado de la transmisión:

```
aws kinesis describe-stream \  
  --stream-name your-stream-name \  
  --region us-east-2
```

2. Supervisa la limitación de la escritura mediante CloudWatch métricas:

```
aws cloudwatch get-metric-statistics \  
  --namespace AWS/Kinesis \  
  --metric-name WriteProvisionedThroughputExceeded \  
  --dimensions Name=StreamName,Value=your-stream-name \  
  --start-time 2025-12-08T00:00:00Z \  
  --end-time 2025-12-08T23:59:59Z \  
  --period 60 \  
  --statistics Sum \  
  --region us-east-2
```

3. Si se detecta una limitación, tenga en cuenta lo siguiente:
 - Cambiar al modo de capacidad bajo demanda para el escalado automático.
 - Uso de una transmisión dedicada para AWS Ground Station telemetría.
 - Si utiliza el modo aprovisionado, aumentar la cantidad de fragmentos.

Problemas con la entrega de telemetría

No aparecen datos de telemetría

Síntomas

Tras programar un contacto con un perfil de misión habilitado para telemetría, no aparece ningún dato de telemetría en la transmisión de Kinesis Data Streams.

Posibles causas y soluciones

El perfil de la misión no tiene habilitada la telemetría

Comprueba que el perfil de misión utilizado para el contacto incluya:
`telemetrySinkConfigArn`

```
aws groundstation get-mission-profile \  
  --mission-profile-id 12345678-1234-1234-1234-123456789012 \  
  --region us-east-2
```

Compruebe el resultado del `telemetrySinkConfigArn` campo. Si no está presente, el perfil de la misión no tiene habilitada la telemetría.

Problema con los permisos de los roles de IAM

Consulte los pasos de solución de problemas de permisos de IAM que se indican en. [Errores de permisos de IAM](#)

La transmisión de Kinesis Data Streams no existe o se encuentra en una región equivocada

Compruebe que la transmisión existe en la región correcta:

```
aws kinesis describe-stream \  
  --stream-name your-stream-name \  
  --region us-east-2
```

El contacto aún no se ha iniciado

La entrega de telemetría comienza a la hora de inicio del contacto. Verifique que el contacto se haya iniciado comprobando el estado del contacto:

```
aws groundstation describe-contact \  
  --contact-id 12345678-1234-1234-1234-123456789012 \  
  --region us-east-2
```

Datos de telemetría intermitente

Síntomas

Los datos de telemetría se entregan de forma incoherente, con lagunas o registros faltantes.

Posibles causas

- Problemas o limitaciones en la capacidad de transmisión de Kinesis Data Streams. Consulte [Problemas de configuración de transmisiones de Kinesis Data Streams](#).
- Problemas de conectividad de red entre AWS Ground Station y su transmisión de Kinesis Data Streams.

Soluciones

- Supervise las métricas CloudWatch de transmisión de Kinesis Data Streams para detectar limitaciones o errores.
- Asegúrese de que su transmisión utilice el modo de capacidad bajo demanda o que tenga suficiente capacidad aprovisionada.
- Usa una transmisión dedicada a la AWS Ground Station telemetría para evitar problemas con otras aplicaciones.

Problemas de formato de datos

Errores de análisis de JSON

Síntomas

La aplicación detecta errores al analizar los registros de telemetría como JSON.

Soluciones

- Verifique la decodificación en Base64: los datos de la transmisión de Kinesis Data Streams están codificados en Base64. Asegúrese de decodificar los datos antes de analizarlos como JSON. Para obtener más información, consulte [Lectura de datos de la transmisión de Kinesis Data Streams](#).
- Compruebe si hay registros vacíos: es AWS Ground Station posible que se envíen registros de validación vacíos al crear un. TelemetrySinkConfig Su aplicación debe gestionar correctamente los registros vacíos o con formato incorrecto.
- Implemente un análisis que tenga en cuenta las versiones: analice primero los `telemetryVersion` campos y `telemetryTypeAndVersion` `telemetryType`, para determinar el esquema apropiado para cada registro.

Tipos o versiones de telemetría desconocidos

Síntomas

La aplicación encuentra tipos o versiones de telemetría que no reconoce.

Solución

Este es el comportamiento esperado, ya que es posible que con el tiempo se introduzcan nuevos tipos de telemetría y versiones de esquemas. Su solicitud debería:

- Registre los tipos y versiones desconocidos para su supervisión.
- Continúe procesando los tipos y versiones conocidos.
- Implemente un manejo correcto de los esquemas desconocidos.

Para obtener más información sobre el control de versiones de esquemas, consulte [Evolución y control de versiones del esquema](#)

Obtener ayuda

Si sigue teniendo problemas después de seguir los pasos de solución de problemas, póngase en contacto con AWS Support.

Información que debe proporcionar

Cuando te pongas en contacto con el servicio de asistencia, proporciona la siguiente información:

- El contacto IDs tiene problemas
- Se utilizó el identificador del perfil de la misión
- TelemetrySinkConfig ARN
- ARN de transmisión de Kinesis Data Streams
- Rol de IAM (ARN) y políticas asociadas
- Mensajes de error de los CloudWatch registros o de su aplicación
- Marcas de tiempo en las que se produjeron los problemas
- Ya se han tomado medidas de solución de problemas

Para obtener AWS Ground Station asistencia general, consulte la [Guía AWS Ground Station del usuario](#).

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 funcionalidad adicional a la CancelContact API e incluye información sobre dicha funcionalidad y las implicaciones de medición. Para obtener más información, consulte Cómo entender la medición de contactos .	10 de diciembre de 2025
Actualización de la documentación	Se aclaró que CloudWatch las métricas se emiten en la región asociada a la estación terrestre del contacto. Se corrigieron los enlaces que no funcionaban.	2 de diciembre de 2025
Política AWS gestionada actualizada	AWS Ground Station ha actualizado la política gestionada AWSGroundStationAgentInstancePolicy para incluir permisos adicionales para recuperar la respuesta URLs a las tareas. Para obtener más información, consulte AWS Ground Station las actualizaciones de las políticas AWS administradas .	13 de noviembre de 2025

Nueva característica	Se actualizó la guía del usuario para incluir las efemérides de elevación del acimut. Para obtener más información, consulte <u>Proporcionar datos de efemérides de elevación acimutal</u>	22 de octubre de 2025
Actualización de la documentación	La entrega de datos entre regiones ya no requiere configuraciones ni aprobaciones especiales. Para obtener más información, consulte Utilizar la entrega de datos entre regiones.	11 de septiembre de 2025
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 un 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 DescribeContact las respuestas.	26 de marzo de 2024
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 DirectBroadcastSatelliteWbd iglfEc 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 han añadido instrucciones para etiquetar satélites con un nombre que se mostrará en la consola de la estación terrestre de AWS Ground Station .	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 AWSGroundStationAgentInstancePolicy.	12 de abril de 2023
Nueva característica	Se ha actualizado la guía del usuario para el lanzamiento de CPE Preview.	9 de noviembre de 2022
Nueva política AWS gestionada	AWS Ground Station se agregó la AWSServiceRoleForGroundStationDataflowEndpointGroup service-linked-role (SLR) que incluye una nueva política denominada AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy.	2 de noviembre de 2022

Nueva característica	Se actualizó la guía del usuario para incluir la integración con AWS CLI.	17 de abril de 2020
Nueva característica	Se actualizó la guía del usuario para incluir la integración con CloudWatch Metrics.	24 de febrero de 2020
Nueva plantilla	Se 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 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 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 versión original de inglés, prevalecerá la versión en inglés.