aws

Guida per l'utente

AWS Ground Station

AWS Ground Station: Guida per l’utente

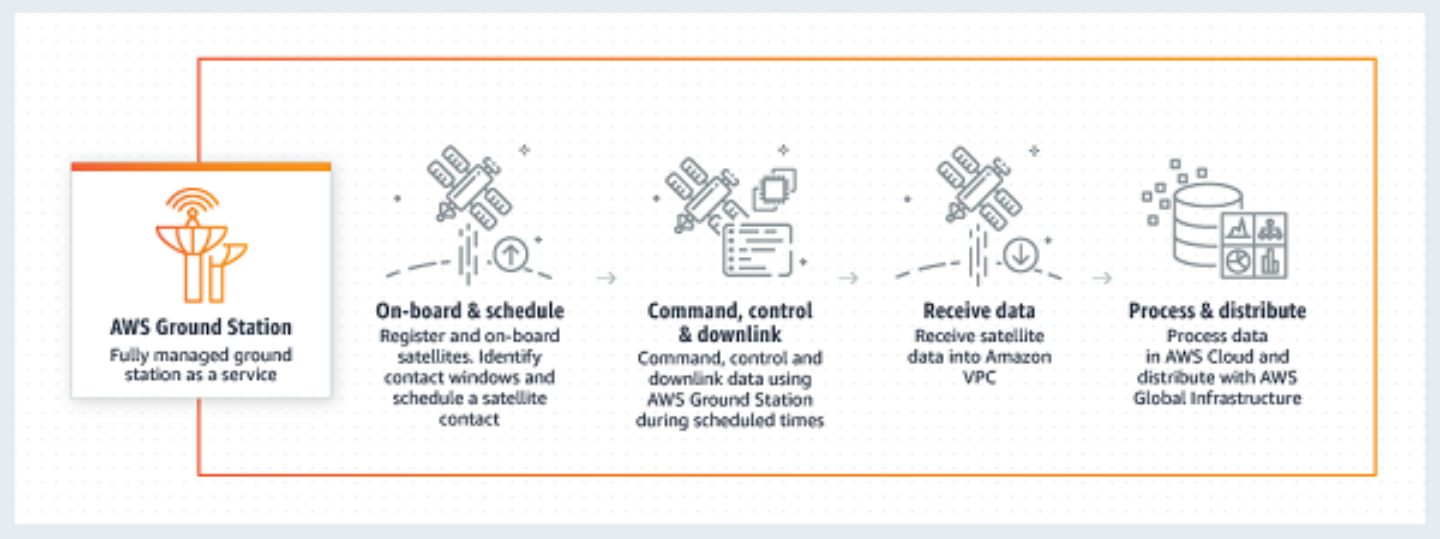
Table of Contents

Che cos'è AWS Ground Station?

AWS Ground Station è un servizio completamente gestito che fornisce comunicazioni satellitari sicure, veloci e prevedibili attraverso un'infrastruttura globale. Con AWS Ground Station, non è più necessario costruire, gestire o scalare la propria infrastruttura di stazione di terra. AWS Ground Station vi consente di concentrarvi sull'innovazione e sulla rapida sperimentazione di nuove applicazioni che acquisiscono dati satellitari, anziché spendere risorse per costruire, gestire e scalare le vostre stazioni terrestri.

Utilizzando la rete globale in fibra di AWS a bassa latenza e larghezza di banda elevata, puoi iniziare a elaborare i dati satellitari entro pochi secondi dalla ricezione sul sistema di antenne. Ciò consente di trasformare i dati grezzi in informazioni elaborate o conoscenze analizzate in pochi secondi.

Casi di utilizzo comune



AWS Ground Station consente di comunicare con i satelliti in modo bidirezionale e supporta i seguenti casi d'uso:

- Dati in downlink: ricevi dati dai tuoi satelliti, trasmettendo frequenze in banda X e in banda S, distribuiti a un' EC2 istanza Amazon in tempo reale (formato VITA-49) o direttamente a un bucket Amazon S3 nel tuo account (formato PCAP). Inoltre, per i satelliti che utilizzano uno schema di modulazione e codifica supportato, è possibile scegliere tra la ricezione di dati demodulati e decodificati o i campioni a frequenza intermedia digitale grezza (DiGIF) (formato VITA-49).

- Dati di uplink: invia dati e comandi ai tuoi satelliti, che ricevono frequenze in banda S, inviando dati DigiF (formato VITA-49) da trasmettere. AWS Ground Station
- Uplink echo: convalida i comandi inviati al veicolo spaziale ed esegui altre attività avanzate ricevendo il segnale trasmesso su un'antenna fisicamente collocata.
- Software Defined Radio (SDR) /Front End Processor (FEP): utilizza l'SDR and/or FEP, that's capable of running on an Amazon EC2 instance, to process your data in real-time to send/receive esistente, le forme d'onda esistenti e genera i tuoi prodotti di dati.
- Telemetry, Tracking, and Command (TT&C): esegui TT&C utilizzando una combinazione dei casi d'uso elencati in precedenza per gestire la tua flotta di satelliti.
- Distribuzione di dati tra regioni: gestisci più contatti simultanei utilizzando AWS Ground Station la rete di antenne globale da un'unica regione AWS.
- Digital twin: pianificazione dei test, verifica delle configurazioni e corretta gestione degli errori a un costo ridotto senza utilizzare la capacità dell'antenna di produzione.

Passaggi successivi

Consigliamo di iniziare leggendo le seguenti sezioni:

- Per apprendere i AWS Ground Station concetti essenziali, consulta. Come AWS Ground Station funziona
- Per informazioni su come configurare l'account e le risorse da utilizzare AWS Ground Station, consultaNozioni di base.
- Per utilizzarlo a livello di codice AWS Ground Station, consulta l'AWS Ground Station API Reference. L'API Reference descrive AWS Ground Station in dettaglio tutte le operazioni API. Fornisce inoltre esempi di richieste, risposte ed errori per i protocolli di servizi Web supportati. Puoi usare la AWS CLI o un AWS SDK, nella lingua che preferisci, per scrivere codice che interagisce con. AWS Ground Station

Come AWS Ground Station funziona

AWS Ground Station utilizza antenne terrestri per facilitare la comunicazione con il satellite. Le caratteristiche fisiche di ciò che le antenne possono fare sono astratte e vengono chiamate capacità. Nella sezione è possibile fare riferimento alla posizione fisica dell'antenna e alle sue capacità attuali. AWS Ground Station Sedi Contattateci tramite il seguente link AWS Support Center Consolese il vostro caso d'uso richiede funzionalità aggiuntive, offerte di localizzazione aggiuntive o posizioni più precise delle antenne.

Per utilizzare una delle AWS Ground Station antenne è necessario prenotare un orario in un luogo specifico. Questa prenotazione viene definita contatto. Per pianificare correttamente un contatto, sono AWS Ground Station necessari dati aggiuntivi per garantirne l'esito positivo.

- Il satellite deve essere imbarcato in una o più località: ciò garantisce l'approvazione per utilizzare le varie funzionalità nella posizione richiesta.
- Il satellite deve avere un'effemeride valida: ciò garantisce che le antenne abbiano una linea di vista e possano puntare con precisione verso il satellite durante il contatto.
- Devi avere un profilo di missione valido: ciò ti consente di personalizzare il comportamento di questo contatto, incluso il modo in cui riceverai e invierai dati al tuo satellite. Potete utilizzare più profili di missione per lo stesso veicolo per creare contatti diversi in base alle diverse posture operative o agli scenari che incontrate.

Onboarding via satellite

L'onboarding di un satellite AWS Ground Station è un processo in più fasi che prevede la raccolta dei dati, la convalida tecnica, la concessione di licenze per lo spettro radio, l'integrazione e il test. La sezione dedicata all'onboarding via satellite della guida ti illustrerà questo processo.

Composizione del profilo della missione

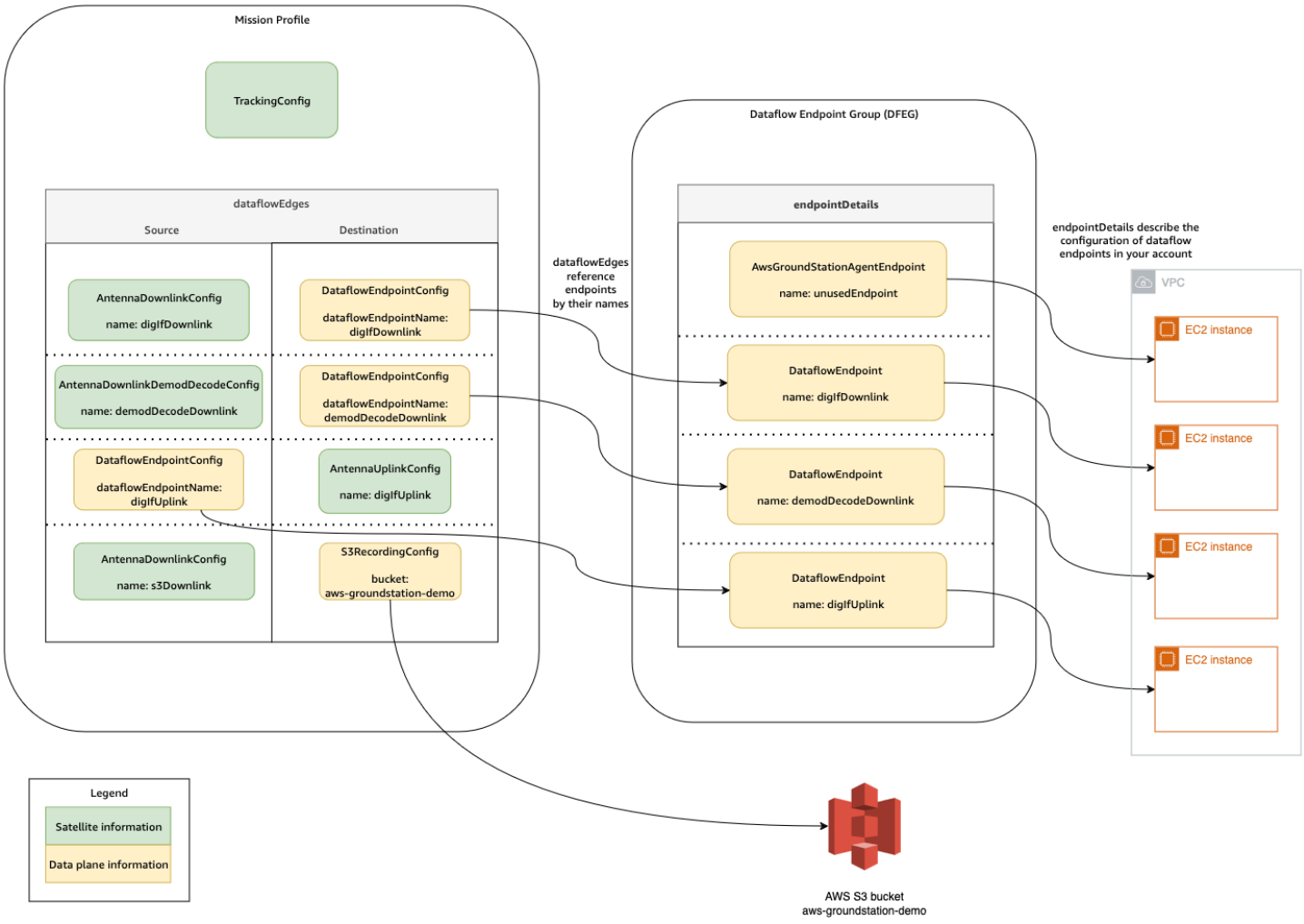
Le informazioni sulla frequenza satellitare, le informazioni sul piano dati e altri dettagli sono incapsulati in un profilo di missione. Il profilo di missione è una raccolta di componenti di configurazione. Ciò consente di riutilizzare i componenti di configurazione in diversi profili di missione in base al proprio caso d'uso. Poiché i profili di missione non fanno riferimento direttamente ai singoli satelliti, ma contengono solo informazioni sulle loro capacità tecniche, i profili di missione possono essere riutilizzati anche da più satelliti con la stessa configurazione.

Un profilo di missione valido avrà una configurazione di tracciamento e uno o più flussi di dati. La configurazione di tracciamento specificherà la tua preferenza per il tracciamento durante un contatto. Ogni coppia di configurazione all'interno di un flusso di dati stabilisce un'origine e una destinazione. A seconda del satellite e delle sue modalità operative, il numero esatto di flussi di dati varierà nel profilo di missione per rappresentare i percorsi di comunicazione in uplink e downlink e qualsiasi aspetto dell'elaborazione dei dati.

- Per ulteriori informazioni sulla configurazione delle risorse Amazon VPC, Amazon S3 e EC2 Amazon che verranno utilizzate durante un contatto, consulta. Lavora con i flussi di dati
- Per i dettagli sul comportamento di ciascuna configurazione, consulta. Usa AWS Ground Station configurazioni
- Per dettagli specifici su tutti i parametri previsti, vedere. Usa i profili di AWS Ground Station missione
- Per esempi su come è possibile creare vari profili di missione per supportare i diversi casi d'uso, consultaEsempi di configurazioni del profilo di missione.

Il diagramma seguente mostra un esempio di profilo di missione e le risorse aggiuntive necessarie. Nota che l'esempio mostra un endpoint di flusso di dati che non è necessario per questo profilo di missione, denominato UnusedEndpoint, per dimostrare la flessibilità. L'esempio supporta i seguenti flussi di dati:

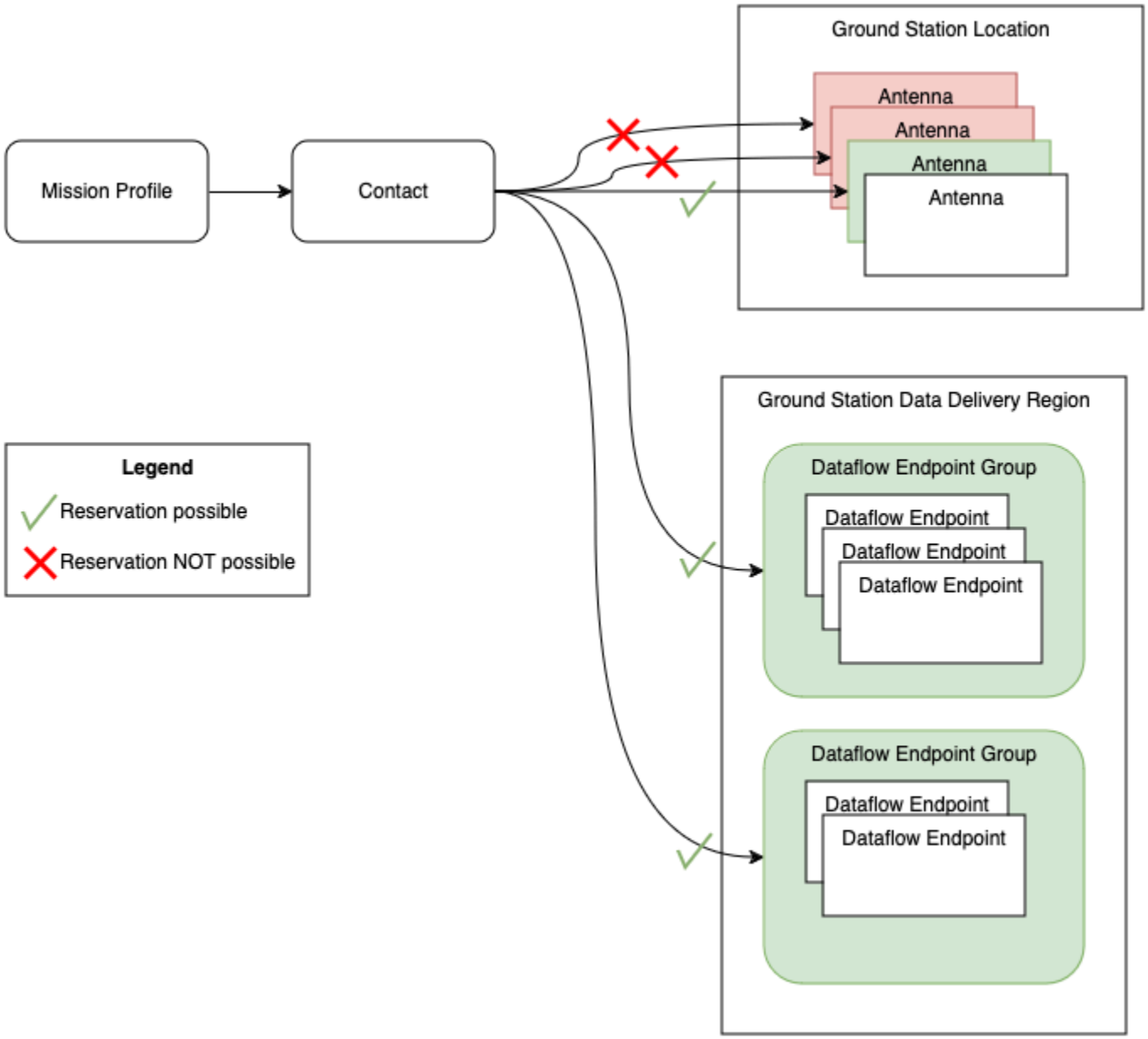
- Downlink sincrono di dati digitali a frequenza intermedia verso un' EC2istanza Amazon gestita da te. Denotato dal nome. digIfDownlink
- Downlink asincrono di dati digitali a frequenza intermedia verso un bucket Amazon S3. Denotato dal aws-groundstation-demonome del bucket.
- Downlink sincrono di dati demodulati e decodificati verso un'istanza Amazon EC2 gestita da te. Denotato dal nome. demodDecodeDownlink
- Uplink sincrono di dati da un' EC2 istanza Amazon che gestisci verso un' AWS Ground Station antenna gestita. Denotato dal nome. digIfUplink



Pianificazione dei contatti

Con un profilo di missione valido, puoi richiedere un contatto con i tuoi satelliti a bordo. La richiesta di prenotazione dei contatti è asincrona per consentire al servizio di antenna globale di raggiungere una pianificazione coerente in tutte le regioni coinvolte. AWS Durante questo processo, vengono valutate diverse antenne nella posizione richiesta della stazione di terra per determinare se sono disponibili e in grado di elaborare il contatto. Durante questo processo, gli endpoint del flusso di dati configurati vengono inoltre valutati per determinarne la disponibilità. Durante questa valutazione, lo stato del contatto sarà in SCHEDULING.

Questo processo di pianificazione asincrono termina entro cinque minuti dalla richiesta, ma in genere termina entro un minuto. Consulta la pagina Automatizza AWS Ground Station con gli eventi per il monitoraggio basato sugli eventi durante la pianificazione.



I contatti che possono essere eseguiti e che hanno disponibilità danno come risultato contatti PIANIFICATI. Con un contatto pianificato, le risorse necessarie per eseguire il contatto sono state riservate nelle regioni AWS necessarie, come definito dal profilo della missione. I contatti che non possono essere eseguiti o che hanno parti non disponibili produrranno contatti FAILED_TO_SCHEDULE. Vedi per i dettagli sul debug. Risoluzione dei problemi relativi ai contatti FAILED_TO_SCHEDULE

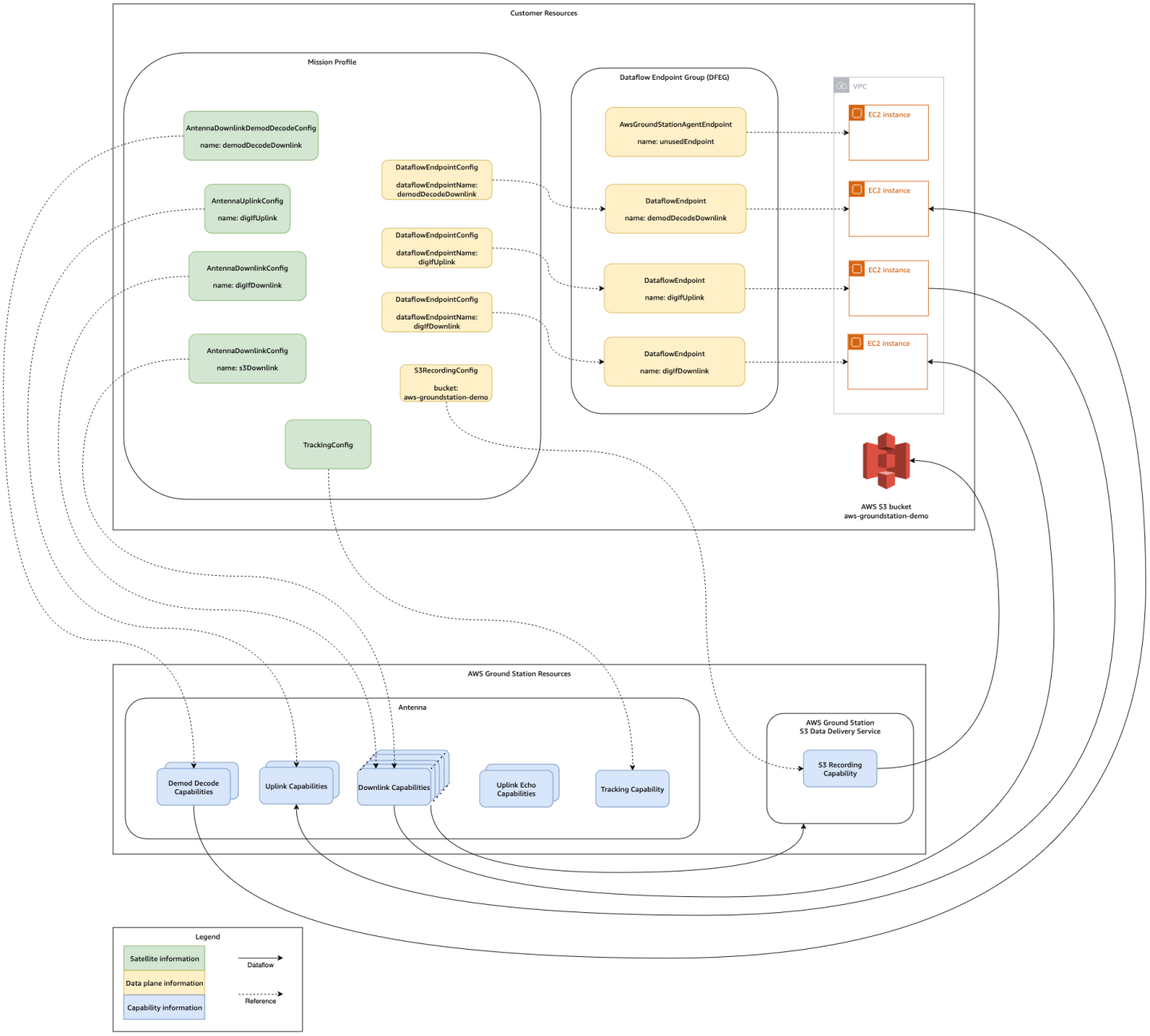
Esecuzione dei contatti

AWS Ground Station orchestrerà automaticamente le risorse gestite da AWS durante la prenotazione dei contatti. Se applicabile, sei responsabile dell'orchestrazione delle EC2 risorse definite dal tuo profilo di missione come endpoint del flusso di dati. AWS Ground Station fornisce AWS EventBridge Events per automatizzare l'orchestrazione delle risorse per ridurre i costi. Per ulteriori dettagli, consulta Automatizza AWS Ground Station con gli eventi.

Durante il contatto, la telemetria sulle prestazioni dei contatti viene fornita ad AWS. CloudWatch Per informazioni su come monitorare i contatti durante l'esecuzione, consulta. Comprendi il monitoraggio con AWS Ground Station

Il diagramma seguente continua l'esempio precedente mostrando le stesse risorse orchestrate durante il contatto.

> **Note**
>
> In questo esempio non sono state utilizzate tutte le funzionalità dell'antenna. Ad esempio, su ogni antenna sono disponibili più di una dozzina di funzionalità di downlink per antenna che supportano frequenze e polarizzazioni multiple. Per ulteriori dettagli sul numero di ciascun tipo di funzionalità disponibili dalle AWS Ground Station antenne e sulle frequenze e polarizzazioni supportate, vedere. AWS Ground Station Funzionalità del sito



Al termine del contatto, AWS Ground Station valuterà le prestazioni del contatto e determinerà lo stato del contatto finale. I contatti in cui non vengono rilevati errori restituiranno lo stato di contatto COMPLETATO. I contatti in cui gli errori di servizio hanno causato problemi di consegna dei dati durante il contatto restituiranno uno AWS_FAILEDstato. Lo stato dei contatti per i quali errori del cliente o dell'utente hanno causato problemi di consegna dei dati durante il contatto risulterà NON RIUSCITO. Gli errori al di fuori di un orario di contatto, ovvero durante il pre-pass o il post-pass, non vengono presi in considerazione durante l'aggiudicazione.

Per ulteriori informazioni, consulta Comprendi il ciclo di vita dei contatti.

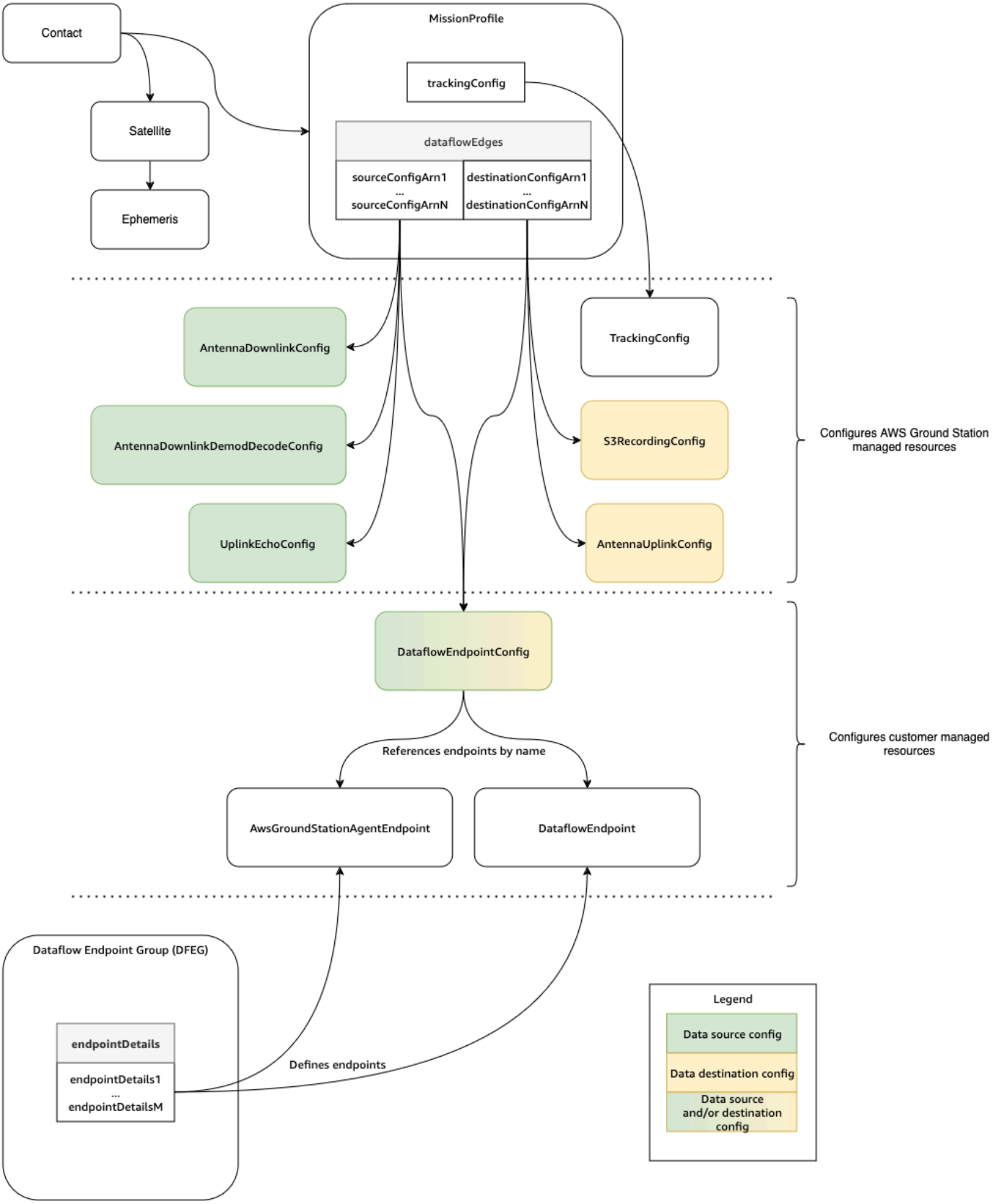
Gemello digitale

La funzione digital twin AWS Ground Station consente di programmare i contatti in base alle postazioni terrestri virtuali. Queste stazioni terrestri virtuali sono repliche esatte delle stazioni terrestri di produzione, tra cui funzionalità di antenna, maschere da cantiere e coordinate GPS effettive. La funzionalità digital twin consente di testare il flusso di lavoro di orchestrazione dei contatti a una frazione del costo rispetto alle stazioni terrestri di produzione. Per ulteriori informazioni, consulta Usa la funzione AWS Ground Station digital twin.

Comprendi i componenti AWS Ground Station principali

Questa sezione fornisce definizioni dettagliate per i componenti principali di AWS Ground Station.

Il diagramma seguente mostra i componenti principali AWS Ground Station e il modo in cui si relazionano tra loro. Le frecce indicano la direzione delle dipendenze tra i componenti, dove ogni componente punta alle proprie dipendenze.


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

I seguenti argomenti descrivono in dettaglio i componenti AWS Ground Station principali.

Argomenti

Usa i profili di AWS Ground Station missione

I profili di missione contengono config e parametri per la modalità di esecuzione dei contatti. Quando prenoti un contatto o cerchi contatti disponibili, fornisci il profilo di missione che intendi utilizzare. I profili di missione riuniscono tutte le configurazioni e definiscono come verrà configurata l'antenna e dove andranno i dati durante il contatto.

I profili di missione possono essere condivisi tra satelliti che condividono le stesse caratteristiche radio. Puoi creare gruppi di endpoint di dataflow aggiuntivi per associare il numero massimo di contatti simultanei che desideri eseguire per la tua costellazione.

Le configurazioni di tracciamento sono specificate come campo unico all'interno del profilo di missione. Le configurazioni di tracciamento vengono utilizzate per specificare la preferenza per l'utilizzo del tracciamento del programma e del tracciamento automatico durante il contatto. Per ulteriori informazioni, consulta Config di monitoraggio.

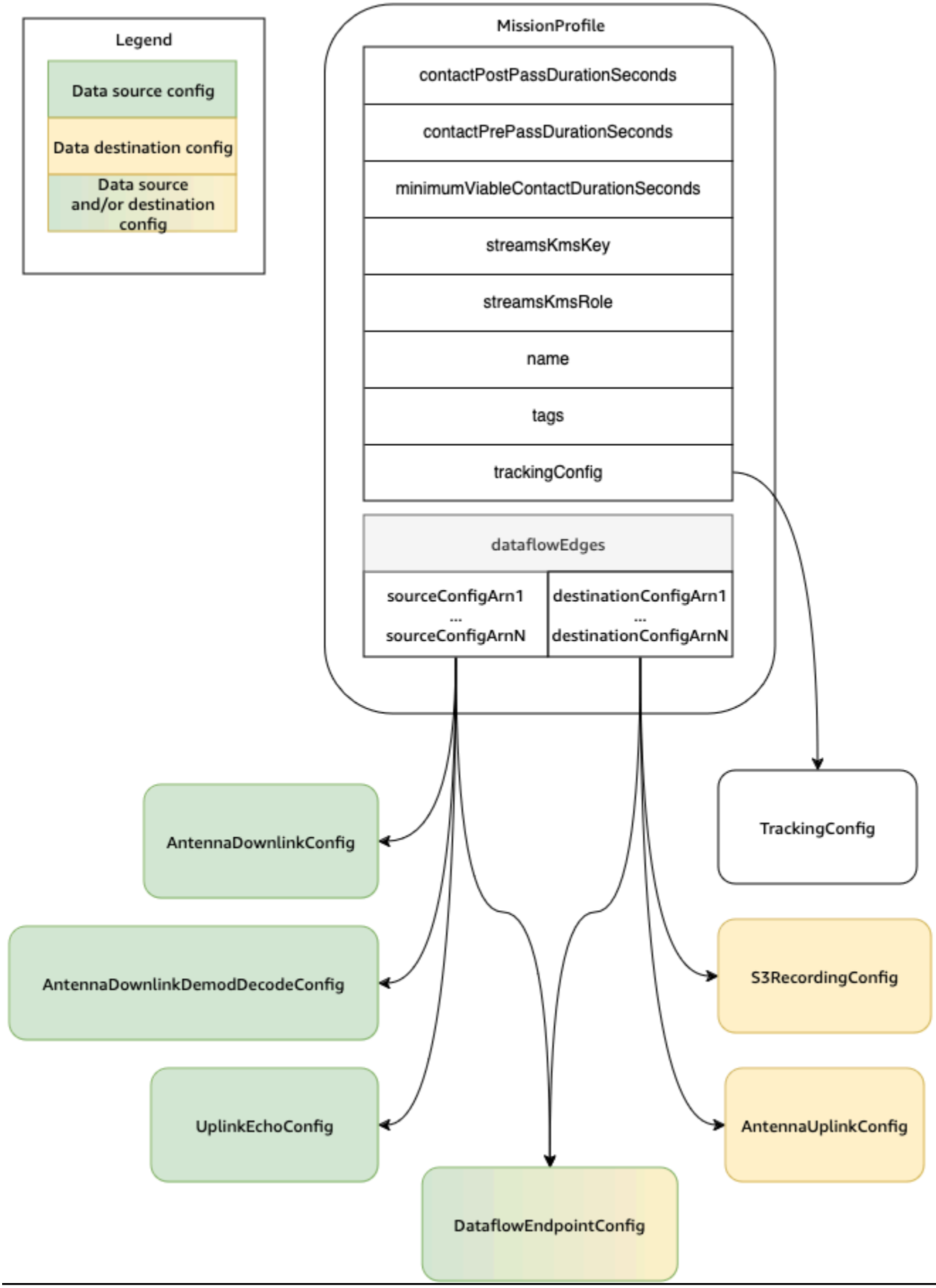
Tutte le altre configurazioni sono contenute nel `dataflowEdges` campo del profilo di missione. Queste configurazioni possono essere considerate come nodi di flusso di dati, ciascuno dei quali rappresenta una risorsa AWS Ground Station gestita in grado di inviare o ricevere dati e la configurazione associata. Il `dataflowEdges` campo definisce quali nodi (configurazioni) del flusso di dati di origine e destinazione sono necessari. Un singolo dataflow edge è un elenco di due configurazioni Amazon Resource Names ARNs (): la prima è la configurazione di origine e la seconda è la configurazione di destinazione. Specificando un dataflow edge tra due configurazioni, si indica AWS Ground Station da dove e verso dove devono fluire i dati durante un contatto. Per ulteriori informazioni, consulta Usa AWS Ground Station configurazioni.

La `contactPrePassDurationSeconds` e ti `contactPostPassDurationSeconds` consente di specificare gli orari relativi al contatto in cui riceverai una notifica dell'evento. CloudWatch Per una cronologia degli eventi relativi al tuo contatto, leggiComprendi il ciclo di vita dei contatti.

Il campo `name` del profilo di missione consente di distinguere tra i profili di missione creati.

Gli `streamsKmsRole` e `streamsKmsKey` vengono utilizzati per definire la crittografia utilizzata da AWS Ground Station per la consegna dei dati con AWS Ground Station Agent. Consulta Crittografia dei dati durante il transito per AWS Ground Station.

Il `telemetrySinkConfigArn` campo è facoltativo e consente di abilitare la AWS Ground Station telemetria durante i contatti. Quando specificato, AWS Ground Station trasmette i dati di telemetria quasi in tempo reale all'account durante l'esecuzione dei contatti. Per ulteriori informazioni sulla configurazione e l'utilizzo della telemetria, consulta. Lavora con la telemetria


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

Un elenco completo di parametri ed esempi è incluso nella documentazione seguente.

- AWS::GroundStation::MissionProfile CloudFormation tipo di risorsa

Usa AWS Ground Station configurazioni

Le configurazioni sono risorse che vengono AWS Ground Station utilizzate per definire i parametri per ogni aspetto del contatto. Se aggiungi i config desiderati a un profilo di missione, questo verrà utilizzato durante l'esecuzione del contatto. Puoi definire diversi tipi di config. Le configurazioni possono essere raggruppate in tre categorie:

- Configurazioni di tracciamento
- Configurazioni Dataflow
- Configurazioni di telemetria

A TrackingConfigè l'unico tipo di configurazione di tracciamento. Viene utilizzato per configurare l'impostazione dell'autotrack dell'antenna durante un contatto ed è richiesto in un profilo di missione.

Le configurazioni che possono essere utilizzate in un flusso di dati del profilo di missione possono essere considerate come nodi di flusso di dati, ciascuno dei quali rappresenta una risorsa AWS Ground Station gestita in grado di inviare o ricevere dati. Un profilo di missione richiede almeno una coppia di queste configurazioni, una che rappresenta una fonte di dati e una che rappresenta una destinazione. Queste configurazioni sono riepilogate nella tabella seguente.

Nome Config	Sorgente/destinazione del flusso di dati
AntennaDownlinkConfig	Origine
AntennaDownlinkDemodDecodeConfig	Origine
UplinkEchoConfig	Origine
S3 RecordingConfig	Destinazione
AntennaUplinkConfig	Destinazione
DataflowEndpointConfig	Destinazione di origine and/or

A TelemetrySinkConfigè l'unico tipo di configurazione di telemetria. Viene utilizzato per configurare dove verranno consegnati i dati di telemetria durante un contatto ed è facoltativo in un profilo di missione. Se incluso, AWS Ground Station trasmette dati di telemetria quasi in tempo reale all'account durante l'esecuzione dei contatti.

Consulta la seguente documentazione per ulteriori informazioni su come eseguire operazioni sulle configurazioni utilizzando CloudFormation, o l' AWS Command Line Interface API. AWS Ground Station Di seguito vengono forniti anche collegamenti alla documentazione per tipi di configurazione specifici.

- AWS::GroundStation::Config CloudFormation tipo di risorsa
- Riferimento alla configurazione AWS CLI
- Riferimento all'API Config

Config di monitoraggio

Puoi utilizzare config di monitoraggio nel profilo di missione per determinare se occorre abilitare il monitoraggio automatico durante i contatti. Questo config dispone di un singolo parametro: `autotrack`. Il parametro `autotrack` può avere i seguenti valori:

- `REQUIRED` - Il monitoraggio automatico è obbligatorio per i contatti.
- `PREFERRED` - Il monitoraggio automatico è preferito per contatti, ma i contatti possono comunque essere eseguiti senza monitoraggio automatico.
- `REMOVED` - Nessun monitoraggio automatico deve essere utilizzato per i contatti.

AWS Ground Station utilizzerà il tracciamento programmatico che indicherà in base alle tue effemeridi quando non viene utilizzato l'autotrack. Si prega di fare riferimento Comprendi come AWS Ground Station utilizza le effemeridi per i dettagli su come sono costruite le effemeridi.

Autotrack utilizzerà il tracciamento del programma fino a quando non verrà trovato il segnale previsto. Una volta che ciò si verifica, continuerà a tracciare in base alla potenza del segnale.

Consulta la seguente documentazione per ulteriori informazioni su come eseguire operazioni di tracciamento delle configurazioni utilizzando CloudFormation AWS Command Line Interface, o l' AWS Ground Station API.

- AWS::GroundStation::Config TrackingConfig CloudFormation proprietà

- AWS CLI Riferimento alla configurazione (vedi la `trackingConfig -> (structure)` sezione)
- TrackingConfig Documentazione di riferimento dell'API

Config di downlink antenna

È possibile utilizzare le configurazioni di downlink dell'antenna per configurare l'antenna per il downlink durante il contatto. Sono costituite da una configurazione dello spettro che specifica la frequenza, la larghezza di banda e la polarizzazione da utilizzare durante il contatto in downlink.

Questa configurazione rappresenta un nodo sorgente in un flusso di dati. È responsabile della digitalizzazione dei dati a radiofrequenza. I dati trasmessi da questo nodo seguiranno il formato del segnale Data/IP . Per informazioni più dettagliate su come costruire flussi di dati con questa configurazione, vedi Lavora con i flussi di dati

Se il tuo caso d'uso del downlink richiede la demodulazione o la decodifica, consulta il. Config di decodifica demodulazione downlink antenna

Consulta la seguente documentazione per ulteriori informazioni su come eseguire operazioni sulle configurazioni di antenna in downlink utilizzando CloudFormation, o l'API. AWS Command Line Interface AWS Ground Station

- AWS::GroundStation::Config AntennaDownlinkConfig CloudFormation proprietà
- AWS CLI Riferimento alla configurazione (vedi la `antennaDownlinkConfig -> (structure)` sezione)
- AntennaDownlinkConfig Documentazione di riferimento dell'API

Config di decodifica demodulazione downlink antenna

Le configurazioni di decodifica demod di Antenna downlink sono un tipo di configurazione più complesso e personalizzabile che è possibile utilizzare per eseguire contatti in downlink con decodifica di demodulazione. and/or Se sei interessato a eseguire questi tipi di contatti, apri un ticket tramite. Supporto AWS AWS Support Center Console Ti aiuteranno a definire il config e il profilo di missione corretti per il tuo caso d'uso.

Questa configurazione rappresenta un nodo sorgente in un flusso di dati. È responsabile della digitalizzazione dei dati a radiofrequenza e dell'esecuzione della demodulazione e della decodifica come specificato. I dati trasmessi da questo nodo seguiranno il formato Data/IP. Demodulated/

Decoded Per informazioni più dettagliate su come costruire flussi di dati con questa configurazione, vedi Lavora con i flussi di dati

Consulta la seguente documentazione per ulteriori informazioni su come eseguire operazioni sulle configurazioni di decodifica demod di antenna downlink utilizzando, o l'API. CloudFormation AWS Command Line Interface AWS Ground Station

- AWS::GroundStation::Config AntennaDownlinkDemodDecodeConfig CloudFormation proprietà
- AWS CLI Riferimento alla configurazione (vedi la `antennaDownlinkDemodDecodeConfig -> (structure)` sezione)
- AntennaDownlinkDemodDecodeConfig Riferimento all'API

Config di uplink antenna

È possibile utilizzare le configurazioni di uplink dell'antenna per configurare l'antenna per l'uplink durante il contatto. Sono costituite da una configurazione dello spettro con frequenza, polarizzazione e potenza irradiata isotropa effettiva (EIRP). Per informazioni su come configurare un contatto per il loopback in uplink, vedere. Config di uplink echo antenna

Questa configurazione rappresenta un nodo di destinazione in un flusso di dati. Convertirà il segnale di dati a radiofrequenza digitalizzato fornito in un segnale analogico e lo emetterà per essere ricevuto dal satellite. Si prevede che i dati trasmessi a questo nodo soddisfino il Signal Format. Data/IP Per informazioni più dettagliate su come costruire flussi di dati con questa configurazione, vedi Lavora con i flussi di dati

Consulta la seguente documentazione per ulteriori informazioni su come eseguire operazioni sulle configurazioni di uplink dell'antenna utilizzando CloudFormation, l'o l'API. AWS Command Line Interface AWS Ground Station

- AWS::GroundStation::Config AntennaUplinkConfig CloudFormation proprietà
- AWS CLI Riferimento alla configurazione (vedi la `antennaUplinkConfig -> (structure)` sezione)
- AntennaUplinkConfig Documentazione di riferimento dell'API

Config di uplink echo antenna

I config di uplink echo indicano all'antenna come eseguire un uplink echo. Un uplink echo può essere usato per convalidare i comandi inviati alla navicella spaziale ed eseguire altre attività avanzate. Ciò

si ottiene registrando il segnale effettivo trasmesso dall' AWS Ground Station antenna (cioè l'uplink). Ciò riproduce il segnale inviato dall'antenna all'endpoint del flusso di dati e dovrebbe corrispondere al segnale trasmesso. Un config di uplink echo contiene l'ARN di un config uplink. L'antenna utilizza i parametri del config di uplink a cui fa riferimento l'ARN durante l'esecuzione di un uplink echo.

Questa configurazione rappresenta un nodo sorgente in un flusso di dati. I dati trasmessi da questo nodo soddisferanno il Signal Format. Data/IP Per informazioni più dettagliate su come costruire flussi di dati con questa configurazione, vedi Lavora con i flussi di dati

Consulta la seguente documentazione per ulteriori informazioni su come eseguire operazioni sulle configurazioni di uplink echo utilizzando, o l'API. CloudFormation AWS Command Line Interface AWS Ground Station

- AWS::GroundStation::Config UplinkEchoConfig CloudFormation proprietà
- AWS CLI Riferimento alla configurazione (vedi la `uplinkEchoConfig -> (structure)` sezione)
- UplinkEchoConfig Documentazione di riferimento dell'API

Config di endpoint del flusso di dati

> **Note**
>
> Le configurazioni degli endpoint Dataflow vengono utilizzate solo per la consegna dei dati ad Amazon EC2 e non vengono utilizzate per la consegna dei dati ad Amazon S3.

Puoi utilizzare le configurazioni degli endpoint dataflow per specificare quale endpoint di flusso di dati in un gruppo di endpoint dataflow da cui o verso il quale desideri che i dati fluiscano durante un contatto. I due parametri di una configurazione endpoint del flusso di dati specificano il nome e la regione dell'endpoint del flusso di dati. Quando prenoti un contatto, AWS Ground Station analizza il profilo di missione specificato e tenta di trovare un gruppo di endpoint dataflow all'interno della AWS Regione che contenga tutti gli endpoint del flusso di dati specificati dalle configurazioni degli endpoint dataflow contenute nel tuo profilo di missione. Se viene trovato un gruppo di endpoint di dataflow adatto, lo stato del contatto diventerà SCHEDULED, altrimenti diventerà FAILED_TO_SCHEDULE. Per ulteriori informazioni sui possibili stati di un contatto, vedere. AWS Ground Station stati dei contatti

La `dataflowEndpointName` proprietà di una configurazione di endpoint dataflow specifica quale endpoint di dataflow in un gruppo di endpoint dataflow verso quali o da quali dati fluiranno durante un contatto.

La proprietà specifica in quale regione risiede l'endpoint del flusso di dati. `dataflowEndpointRegion` Se una regione è specificata nella configurazione dell'endpoint del flusso di dati, AWS Ground Station cerca un endpoint del flusso di dati nella regione specificata. Se non viene specificata alcuna regione, AWS Ground Station verrà utilizzata per impostazione predefinita la regione della stazione di terra del contatto. Un contatto è considerato un contatto interregionale per la fornitura di dati se la regione dell'endpoint dataflow non è la stessa della regione della stazione di terra del contatto. Lavora con i flussi di datiPer ulteriori informazioni sui flussi di dati interregionali, consulta.

Consulta Usa i gruppi AWS Ground Station di endpoint Dataflow i suggerimenti su come diversi schemi di denominazione per i flussi di dati possono essere utili per il tuo caso d'uso.

Per informazioni più dettagliate su come costruire flussi di dati con questa configurazione, vedi Lavora con i flussi di dati

Consulta la seguente documentazione per ulteriori informazioni su come eseguire operazioni sulle configurazioni degli endpoint di dataflow utilizzando, o l'API. CloudFormation AWS Command Line Interface AWS Ground Station

- AWS::GroundStation::Config DataflowEndpointConfig CloudFormation proprietà
- AWS CLI Riferimento alla configurazione (vedi la `dataflowEndpointConfig -> (structure)` sezione)
- DataflowEndpointConfig Documentazione di riferimento dell'API

Config di registrazione Amazon S3

> **Note**
>
> Le configurazioni di registrazione di Amazon S3 vengono utilizzate solo per la consegna dei dati ad Amazon S3 e non vengono utilizzate per la consegna dei dati ad Amazon EC2.

Questa configurazione rappresenta un nodo di destinazione in un flusso di dati. Questo nodo incapsulerà i dati in entrata dal nodo di origine del flusso di dati in dati pcap. Per informazioni più dettagliate su come costruire flussi di dati con questa configurazione, vedi Lavora con i flussi di dati

Puoi utilizzare le configurazioni di registrazione S3 per specificare un bucket Amazon S3 a cui desideri che vengano forniti i dati in downlink insieme alla convenzione di denominazione utilizzata. Di seguito vengono specificate le restrizioni e i dettagli relativi a questi parametri:

- Il nome del bucket Amazon S3 deve iniziare con. `aws-groundstation`
- Il ruolo IAM deve avere una politica di fiducia che consenta al responsabile del `groundstation.amazonaws.com` servizio di assumere il ruolo. Per un esempio, consulta la sezione Example Trust Policy di seguito. Durante la creazione della configurazione l'id della risorsa di configurazione non esiste, la policy di fiducia deve utilizzare un asterisco (*) al posto di *your-config-id* e può essere aggiornata dopo la creazione con l'id della risorsa di configurazione.

Esempio di politica di fiducia

Per ulteriori informazioni su come aggiornare la policy di fiducia di un ruolo, consulta Managing IAM roles nella IAM User Guide.

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"
                }
            }
```

```
        }
    ]
}
```

- Il ruolo IAM deve avere una policy IAM che consenta al ruolo di eseguire l'`s3:GetBucketLocation`azione sul bucket e l'`s3:PutObject`azione sugli oggetti del bucket. Se il bucket Amazon S3 dispone di una bucket policy, la bucket policy deve consentire anche al ruolo IAM di eseguire queste azioni. Per un esempio, consulta la sezione Example Role Policy di seguito.

Esempio di politica relativa al ruolo

Per ulteriori informazioni su come aggiornare o allegare una policy relativa ai ruoli, consulta Managing IAM policy nella IAM User Guide.

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/*"
      ]
    }
  ]
```

```
}
```

- Il prefisso verrà utilizzato per denominare l'oggetto dati S3. Puoi specificare chiavi opzionali per la sostituzione, questi valori verranno sostituiti con le informazioni corrispondenti dai tuoi dati di contatto. Ad esempio, il prefisso di `{satellite_id}/{year}/{month}/{day}` verrà sostituito e risulterà con un output simile `fake_satellite_id/2021/01/10`

  Tasti opzionali per la sostituzione: `{satellite_id}` | | | `{config-name}` | `{config-id}` | `{year}` `{month}` `{day}`

Consulta la seguente documentazione per ulteriori informazioni su come eseguire operazioni sulle configurazioni di registrazione di S3 utilizzando CloudFormation, o l'API AWS Command Line Interface. AWS Ground Station

- AWS::GroundStation::Config Proprietà S3 RecordingConfig CloudFormation
- AWS CLI Riferimento alla configurazione (vedi la `s3RecordingConfig -> (structure)` sezione)
- Riferimento all'API S3 RecordingConfig

Config del sink di telemetria

È possibile utilizzare le configurazioni dei sink di telemetria per specificare dove si desidera che i dati di telemetria vengano trasmessi durante i contatti satellitari. La configurazione del sink di telemetria è facoltativa e viene aggiunta al profilo di missione per pianificare i contatti abilitati alla telemetria. Di seguito vengono specificate le restrizioni e i dettagli relativi a questi parametri:

- Il ruolo IAM deve avere una politica di fiducia che consenta al responsabile del `groundstation.amazonaws.com` servizio di assumere il ruolo. Per un esempio, consulta la sezione Example Trust Policy di seguito.

Esempio di politica di fiducia

Per ulteriori informazioni su come aggiornare la policy di fiducia di un ruolo, consulta Managing IAM roles nella IAM User Guide.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "groundstation.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

- Il ruolo IAM deve avere una policy IAM che consenta al ruolo di eseguire `kinesis:PutRecords` azioni `kinesis:PutRecord` e sullo stream. `kinesis:DescribeStream` Per un esempio, consulta la sezione Example Role Policy di seguito.

Esempio di politica relativa al ruolo

Per ulteriori informazioni su come aggiornare o allegare una policy relativa ai ruoli, consulta Managing IAM policy nella IAM User Guide.

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

Quando includi una configurazione del sink di telemetria nel tuo profilo di missione, AWS Ground Station trasmetterà i dati di telemetria al tuo account durante i contatti. Per ulteriori informazioni sui tipi di telemetria, sul formato dei dati e sulla configurazione delle risorse necessarie, consulta. AWS Lavora con la telemetria

Consulta la seguente documentazione per ulteriori informazioni su come eseguire operazioni sulle configurazioni dei sink di telemetria utilizzando CloudFormation, o l'API. AWS Command Line Interface AWS Ground Station

- AWS::GroundStation::Config TelemetrySinkConfig CloudFormation proprietà
- AWS CLI Riferimento alla configurazione (vedi la `telemetrySinkConfig -> (structure)` sezione)
- TelemetrySinkConfig Riferimento all'API

Usa i gruppi AWS Ground Station di endpoint Dataflow

Gli endpoint Dataflow definiscono la posizione da cui desiderate che i dati vengano trasmessi in streaming sincrono da o verso durante i contatti. Gli endpoint del flusso di dati vengono sempre creati come parte di un gruppo di endpoint del flusso di dati. Includendo più endpoint del flusso di dati in un gruppo, si afferma che gli endpoint specificati possono tutti essere utilizzati insieme durante un singolo contatto. Ad esempio, se un contatto deve inviare dati a tre endpoint del flusso di dati separati, sono necessari tre endpoint in un singolo gruppo di endpoint del flusso di dati che soddisfano i config dell'endpoint del flusso di dati nel profilo di missione.

Versioni del gruppo di endpoint Dataflow

AWS Ground Station supporta due versioni di gruppi di endpoint dataflow:

- DataflowEndpointGroup- L'implementazione originale che supporta l'uplink e il downlink utilizzando un endpoint di flusso di dati e il solo downlink per un endpoint AgentAWS Ground Station
- DataflowEndpointGroupV2 - Versione aggiornata che supporta i flussi di dati in uplink e downlink per gli endpoint Agent con maggiore chiarezza e funzionalità AWS Ground Station

Confronto tra gruppi di endpoint Dataflow

Funzionalità	DataflowEndpointGroup	DataflowEndpointGroupV2
Tipi di endpoint supportati	DataflowEndpoint, AwsGroundStationAgentEndpoint	DownlinkAwsGroundStationAgentEndpoint, UplinkAwsGroundStationAgentEndpoint

Funzionalità	DataflowEndpointGroup	DataflowEndpointGroupV2
Endpoint che supportano l'uplink	DataflowEndpoint	UplinkAwsGroundStationAgentEndpoint
Endpoint che supportano il downlink	DataflowEndpoint, AwsGroundStationAgentEndpoint	DownlinkAwsGroundStationAgentEndpoint

DataflowEndpointGroupLa V2 è stata creata per supportare i flussi di dati in uplink e per rendere più chiaro il linguaggio che circonda i gruppi di endpoint di dataflow. Consigliamo di utilizzare DownlinkAwsGroundStationAgentEndpointendpoint con una versione V2 per tutti UplinkAwsGroundStationAgentEndpointi nuovi casi d'uso. DataflowEndpointGroup DataflowEndpointGroup rimane supportato per la compatibilità con le versioni precedenti, ma la DataflowEndpointGroup V2 offre funzionalità avanzate e opzioni di configurazione più chiare.

> **Tip**
>
> Gli endpoint del flusso di dati sono identificati da un nome a scelta durante l'esecuzione dei contatti. Non è necessario che questi nomi siano univoci in tutto l'account. Ciò consente di eseguire più contatti su diversi satelliti e antenne contemporaneamente utilizzando lo stesso profilo di missione. Ciò può essere utile se si dispone di una costellazione di satelliti con le stesse caratteristiche operative. Puoi scalare il numero di gruppi di endpoint di dataflow fino a raggiungere il numero massimo di contatti simultanei richiesti dalla tua costellazione di satelliti.

Quando una o più risorse in un gruppo di endpoint del flusso di dati è in uso per un contatto, l'intero gruppo viene prenotato per la durata del contatto. È possibile eseguire più contatti contemporaneamente, ma tali contatti devono essere eseguiti su diversi gruppi di endpoint di dataflow.

> **Important**
>
> I gruppi di endpoint Dataflow devono essere in grado di pianificare i contatti che li utilizzano. HEALTHY Per informazioni su come risolvere i problemi relativi ai gruppi di

endpoint Dataflow che non si trovano in uno stato, consulta. HEALTHY Risolvi i problemi DataflowEndpointGroups non in uno stato SANO

Consulta la seguente documentazione per ulteriori informazioni su come eseguire operazioni sui gruppi di endpoint di dataflow utilizzando, o l'API. CloudFormation AWS Command Line Interface AWS Ground Station

- AWS::GroundStation::DataflowEndpointGroup CloudFormation tipo di risorsa
- Riferimento al Dataflow Endpoint Group AWS CLI
- Riferimento all'API Dataflow Endpoint Group

Endpoint del flusso di dati

I membri di un gruppo di endpoint dataflow sono endpoint dataflow. I tipi di endpoint supportati dipendono dalla versione del gruppo di endpoint dataflow utilizzata.

DataflowEndpointGroup endpoint

DataflowEndpointGroup supporta l'uplink e il downlink utilizzando un endpoint di flusso di dati e il downlink solo per un endpoint Agent.AWS Ground Station Per entrambi i tipi di endpoint, creerai i costrutti di supporto (ad esempio gli indirizzi IP) prima di creare il gruppo di endpoint dataflow. Consulta Lavora con i flussi di dati i consigli su quale tipo di endpoint dataflow utilizzare e su come configurare i costrutti di supporto.

Le sezioni seguenti descrivono entrambi i tipi di endpoint supportati.

> **Important**
>
> Tutti gli endpoint del flusso di dati all'interno di un singolo gruppo di endpoint di flussi di dati devono essere dello stesso tipo. Non è possibile combinare gli endpoint AWS Ground Station Agent con gli endpoint Dataflow nello stesso gruppo. Se il tuo caso d'uso richiede entrambi i tipi di endpoint, devi creare gruppi di endpoint Dataflow separati per ogni tipo.
> Per la versione DataflowEndpointGroup V2, puoi mescolarli UplinkAwsGroundStationAgentEndpointe DownlinkAwsGroundStationAgentEndpointinserirli nello stesso gruppo.

AWS Ground Station Endpoint dell'agente

L' AWS Ground Station Agent Endpoint utilizza l' AWS Ground Station agente come componente software per interrompere le connessioni. Per costruire un AWS Ground Station Agent Endpoint, dovrai solo compilare il campo di. `AwsGroundStationAgentEndpoint` EndpointDetails Per ulteriori informazioni sull' AWS Ground Station agente, consulta la Guida utente completa dell'AWS Ground Station agente.

`AwsGroundStationAgentEndpoint` (Editor IU) include i seguenti elementi:

- `Name`- Il nome dell'endpoint del flusso di dati. Affinché il contatto possa utilizzare questo endpoint di flusso di dati, questo nome deve corrispondere al nome utilizzato nella configurazione dell'endpoint del flusso di dati.
- `EgressAddress`- L'indirizzo IP e la porta utilizzati per l'uscita dei dati dall'agente.
- `IngressAddress`- L'indirizzo IP e la porta utilizzati per immettere i dati nell'agente.

Endpoint Dataflow

L'endpoint Dataflow utilizza un'applicazione di rete come componente software per terminare le connessioni. Usa Dataflow Endpoint quando desideri collegare in uplink i dati dei segnali digitali, il downlink di meno del 50% dei dati dei segnali digitali o il downlink dei dati dei segnali. MHz Demodulated/Decoded Per costruire un Dataflow Endpoint, compilerai i campi e di. `Endpoint` `Security Details` EndpointDetails

`Endpoint` (Editor IU) include i seguenti elementi:

- `Name`- Il nome dell'endpoint del flusso di dati. Affinché il contatto possa utilizzare questo endpoint di flusso di dati, questo nome deve corrispondere al nome utilizzato nella configurazione dell'endpoint del flusso di dati.
- `Address`- L'indirizzo IP e la porta utilizzati.

`SecurityDetails` (Editor IU) include i seguenti elementi:

- `roleArn`- L'Amazon Resource Name (ARN) di un ruolo che AWS Ground Station assumerà la creazione di Elastic Network Interfaces (ENIs) nel tuo VPC. Questi ENIs fungono da punti di ingresso e uscita dei dati trasmessi durante un contatto.
- `securityGroupIds` - I gruppi di sicurezza da collegare alle interfacce di rete elastiche.

- `subnetIds`- Un elenco di sottoreti in cui è AWS Ground Station possibile inserire interfacce di rete elastiche per inviare flussi alle istanze. Se vengono specificate più sottoreti, queste devono essere instradabili l'una verso l'altra. Se le sottoreti si trovano in zone di disponibilità diverse (AZs), potrebbero essere applicati costi di trasferimento dati Cross-AZ.

Il ruolo IAM trasferito `roleArn` deve avere una politica di fiducia che consenta al responsabile del `groundstation.amazonaws.com` servizio di assumerlo. Per un esempio, consulta la sezione Example Trust Policy di seguito. Durante la creazione dell'endpoint l'id della risorsa dell'endpoint non esiste, quindi la policy di fiducia deve utilizzare un asterisco (*) al posto di. *your-endpoint-id* Questo può essere aggiornato dopo la creazione per utilizzare l'id della risorsa dell'endpoint al fine di estendere la policy di fiducia a quello specifico gruppo di endpoint del flusso di dati.

Il ruolo IAM deve avere una policy IAM che AWS Ground Station consenta di configurare. ENIs Per un esempio, consulta la sezione Example Role Policy di seguito.

Esempio di politica di fiducia

Per ulteriori informazioni su come aggiornare la policy di fiducia di un ruolo, consulta Managing IAM roles nella IAM User Guide.

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"
                }
            }
```

```
        }
    ]
}
```

Esempio di politica relativa ai ruoli

Per ulteriori informazioni su come aggiornare o allegare una policy relativa ai ruoli, consulta Managing IAM policy nella IAM User Guide.

JSON

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

DataflowEndpointGroupEndpoint V2

DataflowEndpointGroupLa V2 introduce tipi di endpoint specializzati che forniscono una configurazione più chiara e funzionalità avanzate:

- UplinkAwsGroundStationAgentEndpoint- Ottimizzato per i flussi di dati in uplink
- DownlinkAwsGroundStationAgentEndpoint- Ottimizzato per i flussi di dati in downlink

Questi endpoint specializzati sostituiscono le configurazioni generiche AwsGroundStationAgentEndpointcon configurazioni specifiche per la direzione che semplificano la configurazione e la gestione dei flussi di dati.

AWS Ground Station Endpoint Uplink Agent

UplinkAwsGroundStationAgentEndpointÈ progettato specificamente per i flussi di dati in uplink e offre opzioni di configurazione più chiare. Usa questo tipo di endpoint quando devi fornire dati da collegare AWS Ground Station al tuo satellite.

`UplinkAwsGroundStationAgentEndpoint` (Editor IU) include i seguenti elementi:

- `Name`- Il nome dell'endpoint del flusso di dati. Affinché il contatto possa utilizzare questo endpoint di flusso di dati, questo nome deve corrispondere al nome utilizzato nella configurazione dell'endpoint del flusso di dati.
- `IngressAddressAndPort`- Indirizzo IP e porta singoli per l'immissione dei dati all'agente
- `AgentIpAndPortAddress`- Intervallo di porte per la comunicazione tra agenti

Endpoint Downlink AWS Ground Station Agent

DownlinkAwsGroundStationAgentEndpointÈ ottimizzato per i flussi di dati in downlink, inclusi gli scenari di downlink a banda stretta, demodulazione/decodifica a banda larga e uplink echo.

`DownlinkAwsGroundStationAgentEndpoint` (Editor IU) include i seguenti elementi:

- `Name`- Il nome dell'endpoint del flusso di dati. Affinché il contatto possa utilizzare questo endpoint di flusso di dati, questo nome deve corrispondere al nome utilizzato nella configurazione dell'endpoint del flusso di dati.
- `EgressAddressAndPort`- Indirizzo IP e porta singoli per l'output dei dati dall'agente
- `AgentIpAndPortAddress`- Intervallo di porte per la comunicazione tra agenti

Creazione di gruppi di endpoint di dataflow

Puoi creare gruppi di endpoint dataflow utilizzando entrambe le versioni:

CreateDataflowEndpointGroup

Utilizzali CreateDataflowEndpointGroupper la compatibilità con le versioni precedenti o quando è necessario utilizzare i generici o i tipi. AwsGroundStationAgentEndpointDataflowEndpoint

CreateDataflowEndpointGroupV2

Usa CreateDataflowEndpointGroupV2 per nuove implementazioni per sfruttare i tipi di endpoint specializzati che supportano flussi di dati sia in uplink che in downlink. Questa API supporta solo e. UplinkAwsGroundStationAgentEndpointDownlinkAwsGroundStationAgentEndpoint

Considerazioni sulla migrazione

Se stai attualmente utilizzando DataflowEndpointGroup, puoi continuare a utilizzare la configurazione esistente senza modifiche. AWS Ground Station mantiene la piena compatibilità con le versioni precedenti.

Se desideri migrare per utilizzare la nuova DataflowEndpointGroup V2 e al momento stai utilizzando un'DataflowEndpointapplicazione Dataflow Endpoint per ricevere i tuoi dati, dovrai invece migrare per utilizzare l'agente. AWS Ground Station Se utilizzi già un AWS Ground Station agente per il downlink, puoi utilizzare la stessa istanza dell'agente anche per l'uplink: non sono necessarie istanze di agente aggiuntive.

Per migrare alla versione 2: DataflowEndpointGroup

1. In caso di migrazione da DataflowEndpoint, configura l' AWS Ground Station agente seguendo la Guida per l'utente dell'AWS Ground Station agente
2. Identifica la direzione del flusso di dati e crea il tipo di endpoint appropriato (o) UplinkAwsGroundStationAgentEndpointDownlinkAwsGroundStationAgentEndpoint
3. Crea la DataflowEndpointGroupV2 facendo riferimento a tali endpoint
4. Crea una nuova configurazione dell'endpoint del flusso di dati che faccia riferimento alla nuova V2 per nome DataflowEndpointGroup
5. Crea un nuovo profilo di missione che faccia riferimento alla configurazione dell'endpoint dataflow come dataflow edge
6. Usa il nuovo profilo di missione per pianificare i contatti
7. Testa la tua configurazione prima di passare alla produzione

Per ulteriori informazioni sul flusso di lavoro completo, consulta Comprendi i componenti AWS Ground Station principali eCrea configurazioni.

Usa AWS Ground Station agente

L' AWS Ground Station agente consente di ricevere (downlink) flussi di dati sincroni Wideband Digital Intermediate Frequency (DigiF) durante i contatti con AWS Ground Station.

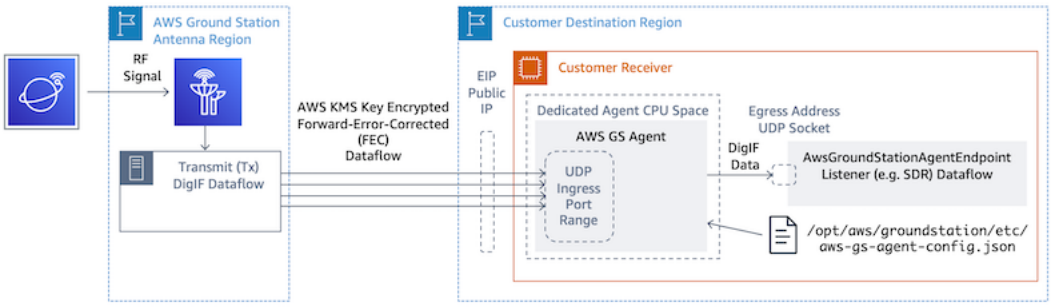
Come funziona

Puoi selezionare due opzioni per la consegna dei dati:

1. Consegna dei dati a un' EC2 istanza: consegna dei dati a un' EC2 istanza di tua proprietà. Sei tu a gestire l' AWS Ground Station agente. Questa opzione può essere la soluzione migliore se è necessaria un'elaborazione dei dati quasi in tempo reale. Consulta la Lavora con i flussi di dati sezione per informazioni sulla consegna EC2 dei dati.
2. Distribuzione dei dati in un bucket S3 - La consegna dei dati al bucket AWS S3 è completamente gestita da. AWS Ground Station Consulta la Nozioni di base guida per informazioni sulla distribuzione dei dati S3.

Entrambe le modalità di distribuzione dei dati richiedono la creazione di un set di risorse AWS. L'uso di CloudFormation per creare le tue risorse AWS è altamente consigliato per garantire affidabilità, precisione e supportabilità. Ogni contatto può fornire dati solo a EC2 o a S3 ma non a entrambi contemporaneamente.

Il diagramma seguente mostra un flusso di dati DigiF da AWS Ground Station una regione di antenna all'istanza con EC2 il Software-Defined Radio (SDR) o un ascoltatore simile.



Informazioni aggiuntive

Per informazioni più dettagliate, consultate la Guida per l'utente completa dell'agente.AWS Ground Station

Nozioni di base

Prima di iniziare, è necessario acquisire familiarità con i concetti di base di. AWS Ground Station Per ulteriori informazioni, consulta Come AWS Ground Station funziona.

Di seguito sono riportate le best practice per AWS Identity and Access Management (IAM) e le autorizzazioni necessarie. Dopo aver impostato i ruoli appropriati, puoi iniziare a seguire il resto dei passaggi.

Registrati per un Account AWS

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la https://portal.aws.amazon.com/billing/registrazione.
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata o un messaggio di testo e ti verrà chiesto di inserire un codice di verifica attraverso la tastiera del telefono.

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente e utilizza solo l'utente root per eseguire attività che richiedono l'accesso di un utente root.

AWS ti invia un'email di conferma dopo il completamento della procedura di registrazione. In qualsiasi momento, puoi visualizzare l'attività corrente del tuo account e gestirlo accedendo a https://aws.amazon.com/e scegliendo Il mio account.

Crea un utente con accesso amministrativo

Dopo esserti registrato Account AWS, proteggi Utente root dell'account AWS AWS IAM Identity Center, abilita e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Proteggi i tuoi Utente root dell'account AWS

1. Accedi Console di gestione AWScome proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

   Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Accedere come utente root nella Guida per l'utente di Accedi ad AWS .
2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

   Per istruzioni, consulta Abilitare un dispositivo MFA virtuale per l'utente Account AWS root (console) nella Guida per l'utente IAM.

Crea un utente con accesso amministrativo

1. Abilita il Centro identità IAM.

   Per istruzioni, consulta Abilitazione del AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center .
2. Nel Centro identità IAM, assegna l'accesso amministrativo a un utente.

   Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, consulta Configurare l'accesso utente con l'impostazione predefinita IAM Identity Center directory nella Guida per l'AWS IAM Identity Center utente.

Accesso come utente amministratore

- Per accedere come utente del Centro identità IAM, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente del Centro identità IAM.

  Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta AWS Accedere al portale di accesso nella Guida per l'Accedi ad AWS utente.

Assegnazione dell'accesso ad altri utenti

1. Nel Centro identità IAM, crea un set di autorizzazioni conforme alla best practice per l'applicazione di autorizzazioni con il privilegio minimo.

Segui le istruzioni riportate nella pagina Creazione di un set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .

2. Assegna al gruppo prima gli utenti e poi l'accesso con autenticazione unica (Single Sign-On).

   Per istruzioni, consulta Aggiungere gruppi nella Guida per l'utente di AWS IAM Identity Center .

Aggiungi AWS Ground Station le autorizzazioni al tuo account AWS

Per utilizzarla AWS Ground Station senza richiedere un utente amministrativo, devi creare una nuova politica e allegarla al tuo AWS account.

1. Accedi Console di gestione AWS e apri la console IAM.
2. Creare una nuova policy. Utilizza le fasi seguenti:

   a. Nel riquadro di navigazione, seleziona Policy e Crea policy.

   b. Nella scheda JSON, modificare il JSON con uno dei seguenti valori. Utilizzare il JSON più adatto alla propria applicazione.

   - Per i privilegi amministrativi di Ground Station, imposta Action su groundstation: * come segue:

     JSON

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

- Per la sola lettura, impostare Action (Operazione) su groundstation:Get*, groundstation:List* e groundstation:Describe* nel modo seguente:

  JSON

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

- Per una maggiore sicurezza tramite l'autenticazione a più fattori, imposta Action su groundstation: * e Condition/Bool su aws ::true come segue: MultiFactorAuthPresent

  JSON

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

3. Nella console IAM, collega la policy che hai creato all'utente desiderato.

Per ulteriori informazioni sulla creazione di utenti IAM e sull'associazione delle policy, consulta la Guida per l'utente di IAM.

Satellite a bordo

L'onboarding di un satellite AWS Ground Station è un processo in più fasi che prevede la raccolta dei dati, la convalida tecnica, la concessione di licenze per lo spettro radio, l'integrazione e il test. Sono inoltre richiesti accordi di non divulgazione (). NDAs

Panoramica del processo di onboarding dei clienti

L'onboarding via satellite è un processo manuale che può essere consultato nella sezione Satelliti e risorse della pagina della console. AWS Ground Station Di seguito viene descritto il processo complessivo.

1. Consultate la AWS Ground Station Sedi sezione per determinare se il vostro satellite soddisfa le caratteristiche geografiche e di radiofrequenza.
2. Per iniziare a effettuare l'onboarding del satellite AWS Ground Station, invia un questionario sull'onboarding satellitare nella sezione Satelliti e risorse della pagina della console. AWS Ground Station Includi un breve riepilogo della tua missione e delle tue esigenze satellitari, incluso il nome dell'organizzazione, le frequenze richieste, quando i satelliti saranno o sono stati lanciati, il tipo di orbita del satellite e se intendi utilizzarlo. Usa la funzione AWS Ground Station digital twin
3. Una volta esaminata e approvata la richiesta, AWS Ground Station richiederai le licenze normative nelle località specifiche che intendi utilizzare. La durata di questa fase varierà a seconda delle località e delle normative esistenti.
4. Dopo aver ottenuto questa approvazione, il satellite sarà visibile e potrà essere utilizzato. AWS Ground Station ti invierà una notifica dell'avvenuto aggiornamento.

(Facoltativo) Denominazione dei satelliti

Dopo l'onboarding, potresti voler aggiungere un nome al tuo record satellitare per riconoscerlo più facilmente. La AWS Ground Station console ha la capacità di visualizzare un nome definito dall'utente

per un satellite insieme al Norad ID quando si utilizza la pagina Contatti. La visualizzazione del nome del satellite semplifica notevolmente la selezione del satellite corretto durante la programmazione. Per fare ciò, è possibile utilizzare i tag.

L'etichettatura di AWS Ground Station Satellites può essere effettuata tramite l'API tag-resource con l'AWS CLI o uno degli AWS. SDKs Questa guida tratterà l'uso della AWS Ground Station CLI per etichettare il satellite di trasmissione pubblica Aqua (Norad ID 27424). `us-west-2`

AWS Ground Station CLI

Possono essere usati per AWS CLI interagire con. AWS Ground Station Prima di utilizzare AWS CLI per etichettare i satelliti, devono essere soddisfatti i seguenti AWS CLI prerequisiti:

- Assicuratevi che sia installato AWS CLI . Per informazioni sull'installazione AWS CLI, consulta Installazione della versione 2 dell'interfaccia a riga di comando di AWS.
- Assicurati che AWS CLI sia configurato. Per informazioni sulla configurazione AWS CLI, consulta Configurazione della versione 2 dell'interfaccia a riga di comando di AWS.
- Puoi salvare le impostazioni di configurazione e le credenziali utilizzate più di frequente nei file gestiti dall' AWS CLI. Hai bisogno di queste impostazioni e credenziali per prenotare e gestire i tuoi contatti. AWS Ground Station AWS CLI Per ulteriori informazioni sul salvataggio delle impostazioni di configurazione e delle credenziali, vedi Configurazione e impostazioni dei file di credenziali.

Una volta AWS CLI configurato e pronto per l'uso, consulta la pagina di riferimento dei comandi della CLI di AWS Ground Station per acquisire familiarità con i comandi disponibili. Segui la struttura dei AWS CLI comandi quando usi questo servizio e inserisci come prefisso i comandi `groundstation` per specificarli AWS Ground Station come servizio che desideri utilizzare. Per ulteriori informazioni sulla struttura dei AWS CLI comandi, consulta Command Structure nella pagina AWS CLI. Di seguito viene fornita una struttura di comando di esempio.

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

Assegna un nome a un satellite

Per prima cosa devi procurarti l'ARN del satellite o dei satelliti che desideri taggare. Ciò può essere fatto tramite l'API list-satellites nella CLI di AWS:

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

L'esecuzione del comando CLI precedente restituirà un output simile a questo:

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

Trova il satellite che desideri etichettare e annota il`satelliteArn`. Un avvertimento importante per il tagging è che l'API tag-resource richiede un ARN regionale e l'ARN restituito da list-satellites è globale. Per il passaggio successivo, dovresti aumentare l'ARN con la regione in cui desideri visualizzare il tag (probabilmente la regione in cui effettui la programmazione). Per questo esempio, stiamo usando. `us-west-2` Con questa modifica, l'ARN passerà da:

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

to:

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

Per mostrare il nome del satellite nella console, il satellite deve avere un tag `“Name"` come chiave. Inoltre, poiché stiamo usando il AWS CLI, le virgolette devono essere eliminate con una barra rovesciata. Il tag avrà un aspetto simile a:

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

Successivamente, chiamerai l'API tag-resource per taggare il satellite. Questo può essere fatto in questo AWS CLI modo:

```
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"}'
```

Dopo averlo fatto, potrai vedere il nome che hai impostato per il satellite nella AWS Ground Station console.

Cambia il nome di un satellite

Se vuoi cambiare il nome di un satellite, puoi semplicemente richiamare nuovamente tag-resource con l'ARN del satellite con la stessa "Name" chiave, ma con un valore diverso nel tag. Questo aggiornerà il tag esistente e mostrerà il nuovo nome nella console. Un esempio di chiamata per questo è il seguente:

```
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"}'
```

Rimuovi il nome di un satellite

Il nome impostato per un satellite può essere rimosso con l'API untag-resource. Questa API richiede l'ARN satellitare con la regione in cui si trova il tag e un elenco di chiavi di tag. Per il nome, la chiave del tag è"Name". Un esempio di chiamata a questa API utilizzando la CLI di AWS è il seguente:

```
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
```

Satelliti di trasmissione pubblici

Oltre all'onboarding dei tuoi satelliti, puoi richiedere di effettuare l'onboarding con satelliti di trasmissione pubblici supportati che forniscono un percorso di comunicazione in downlink accessibile al pubblico. Ciò consente di effettuare il downlink dei dati provenienti da questi satelliti AWS Ground Station .

> **Note**
>
> Non sarà possibile effettuare l'uplink verso questi satelliti. Potrai utilizzare solo i percorsi di comunicazione in downlink accessibili al pubblico.

AWS Ground Station supporta l'onboarding dei seguenti satelliti per il downlink dei dati di trasmissione diretta:

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

Una volta a bordo, è possibile accedere a questi satelliti per un uso immediato. AWS Ground Station mantiene una serie di CloudFormation modelli preconfigurati per facilitare l'avvio del servizio. Vedi Esempi di configurazioni del profilo di missione alcuni esempi di come AWS Ground Station può essere utilizzato.

Per ulteriori informazioni su questi satelliti e sul tipo di dati che trasmettono, consulta Aqua, JPSS-1/NOAA-20 e SNPP e Terra.

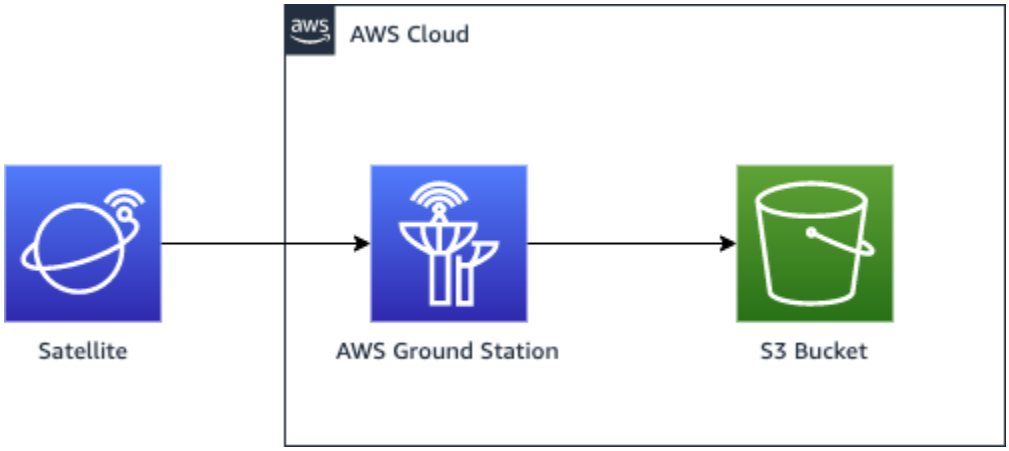
Pianifica i percorsi di comunicazione del flusso di dati

Puoi scegliere tra comunicazione sincrona e asincrona per ogni percorso di comunicazione sul tuo satellite. A seconda del satellite e del caso d'uso, potrebbero essere necessari uno o entrambi i tipi. I percorsi di comunicazione sincroni consentono operazioni di uplink quasi in tempo reale e di downlink a banda stretta e larga. I percorsi di comunicazione asincroni supportano solo operazioni di downlink a banda stretta e larga.

Distribuzione asincrona dei dati

Con la consegna dei dati ad Amazon S3, i dati di contatto vengono inviati in modo asincrono a un bucket Amazon S3 del tuo account. I dati di contatto vengono forniti come file di acquisizione dei pacchetti (pcap) per consentire la riproduzione dei dati di contatto in una Software Defined Radio (SDR) o per estrarre i dati del payload dai file pcap per l'elaborazione. I file pcap vengono consegnati

al tuo bucket Amazon S3 ogni 30 secondi quando i dati di contatto vengono ricevuti dall'hardware dell'antenna per consentire l'elaborazione dei dati di contatto durante il contatto, se lo desideri. Una volta ricevuti, puoi elaborare i dati utilizzando il tuo software di post-elaborazione o utilizzare altri servizi AWS come Amazon SageMaker AI o Amazon Rekognition. La consegna dei dati ad Amazon S3 è disponibile solo per il downlink dei dati dal satellite; non è possibile collegare i dati al satellite da Amazon S3.



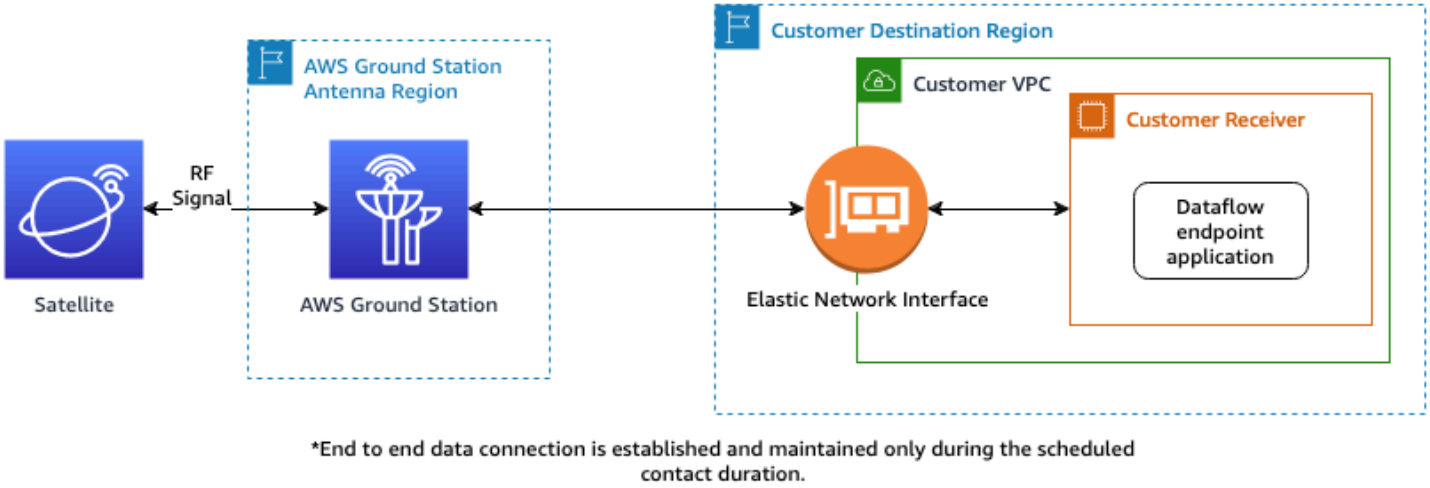
Per utilizzare questo percorso, dovrai creare un bucket Amazon S3 in cui distribuire AWS Ground Station i dati. Nel passaggio successivo, dovrai anche creare un Config di registrazione S3 nel passaggio successivo. Fai riferimento alle restrizioni sulla denominazione dei Config di registrazione Amazon S3 bucket e a come specificare la convenzione di denominazione utilizzata per i tuoi file.

Distribuzione sincrona dei dati

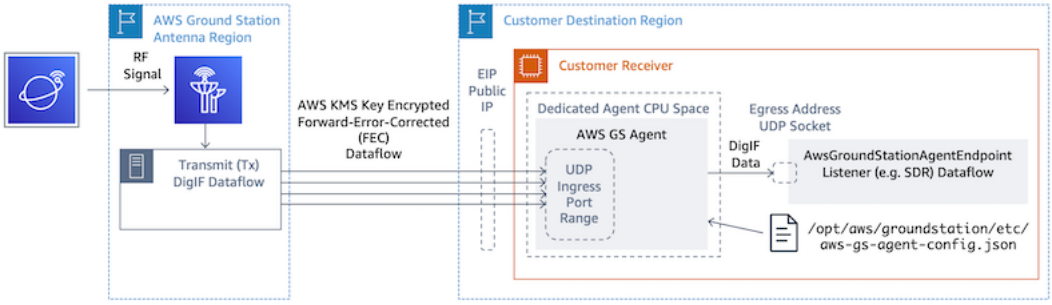
Con la consegna dei dati ad Amazon EC2, i dati di contatto vengono trasmessi in streaming da e verso l' EC2 istanza Amazon. Puoi elaborare i dati in tempo reale sulla tua EC2 istanza Amazon o inoltrarli per la post-elaborazione.

Per utilizzare un percorso sincrono, dovrai impostare e configurare le tue EC2 istanze Amazon e creare uno o più gruppi di endpoint Dataflow. Per configurare la tua EC2 istanza Amazon, fai riferimento aConfigura e configura Amazon EC2. Per creare il tuo Dataflow Endpoint Group, fai riferimento a. Usa i gruppi AWS Ground Station di endpoint Dataflow

Di seguito viene mostrato il percorso di comunicazione se si utilizza la configurazione degli endpoint dataflow.



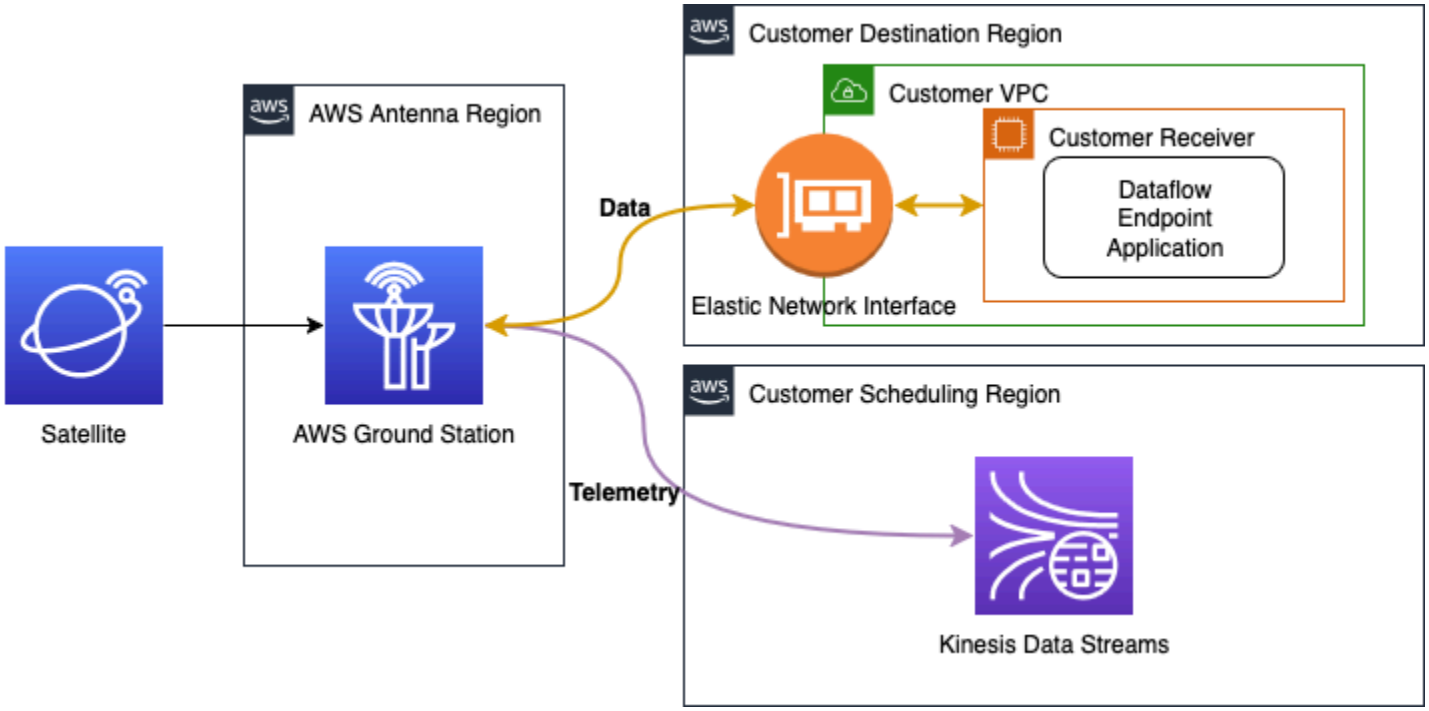
Di seguito viene illustrato il percorso di comunicazione se si utilizza la configurazione dell' AWS Ground Station agente.



Pianifica la tua telemetria

AWS Ground Station la telemetria è una funzionalità opzionale che trasmette le metriche dalle AWS Ground Station antenne all'account durante i contatti via satellite. AWS Ciò consente di monitorare le prestazioni dei contatti quasi in tempo reale e di creare soluzioni di monitoraggio personalizzate.

Con la AWS Ground Station telemetria, le metriche delle AWS Ground Station antenne vengono trasmesse in streaming direttamente al tuo account. Lo streaming dei dati di telemetria inizia all'inizio del contatto e continua per tutta la durata del contatto. I dati di telemetria vengono trasmessi al tuo account quasi in tempo reale mentre vengono campionati dall'hardware dell'antenna. Una volta ricevuti, puoi elaborare i dati utilizzando il tuo software di post-elaborazione o utilizzare altri servizi AWS come Amazon Data AWS Lambda Firehose o.



Nella fase successiva, creerai le configurazioni necessarie per il tuo profilo di missione. Se desideri abilitare la telemetria, creerai un Telemetry Sink Config oltre alla configurazione di tracciamento e alle configurazioni del flusso di dati. Per istruzioni Configurare la telemetria dettagliate sulla configurazione, consulta.

Per ulteriori informazioni su TelemetrySinkConfig, vedereConfig del sink di telemetria.

Crea configurazioni

In questa fase hai identificato il satellite, i percorsi di comunicazione e le risorse IAM, Amazon EC2 e Amazon S3 necessarie. In questo passaggio creerai AWS Ground Station configurazioni che memorizzano i rispettivi parametri.

Configurazioni di consegna dei dati

Le prime configurazioni da creare riguardano dove e come desideri che i dati vengano consegnati. Utilizzando le informazioni del passaggio precedente, costruirete molti dei seguenti tipi di configurazione.

- Config di registrazione Amazon S3- Fornisci dati al tuo bucket Amazon S3.
- Config di endpoint del flusso di dati- Fornisci dati alla tua istanza Amazon EC2.

Configurazione della telemetria (opzionale)

Se desideri ricevere telemetria quasi in tempo reale durante i tuoi contatti, puoi creare un. TelemetrySinkConfig Questa configurazione è facoltativa e specifica dove AWS Ground Station verranno forniti i dati di telemetria.

- Config del sink di telemetria- Fornisci dati di telemetria al tuo account.

Per istruzioni dettagliate sulla configurazione, consulta. Configurare la telemetria

Configurazioni satellitari

Le configurazioni satellitari riguardano il modo in cui AWS Ground Station è possibile comunicare con il satellite. Farai riferimento alle informazioni raccolte inSatellite a bordo.

- Config di monitoraggio- Imposta la preferenza per il tracciamento fisico del veicolo durante un contatto. Ciò è necessario per la costruzione del profilo di missione.
- Config di downlink antenna- Fornisci dati digitalizzati in radiofrequenza.
- Config di decodifica demodulazione downlink antenna- Fornisce dati a radiofrequenza demodulati e decodificati.
- Config di uplink antenna- Trasmetti i dati al tuo satellite.
- Config di uplink echo antenna- Fornisci un'eco dei dati del segnale di uplink.

Crea un profilo di missione

Con le configurazioni create nel passaggio precedente, avete identificato come tracciare il satellite, i possibili modi per comunicare con il satellite e come abilitare la telemetria quasi in tempo reale durante l'esecuzione dei contatti. In questa fase costruirete uno o più profili di missione. Un profilo di missione rappresenta l'aggregazione delle possibili configurazioni in un comportamento previsto che può essere quindi pianificato e utilizzato.

Per i parametri più recenti, fai riferimento al tipo di risorsa AWS::GroundStation::MissionProfile CloudFormation

1. Assegna un nome al tuo profilo di missione. Ciò consente di comprenderne rapidamente l'utilizzo all'interno del sistema. Ad esempio, potresti avere un operatore satellite-wideband-narrowband-

nominal-operations e un satellite-narrowband-emergency-operationsse disponi di un operatore a banda stretta separato per le operazioni di emergenza.

2. Imposta la configurazione di tracciamento.
3. Imposta la durata minima dei contatti. Ciò ti consente di filtrare i potenziali contatti per soddisfare le esigenze della tua missione.
4. Imposta i tuoi streamsKmsKeye streamsKmsRoleche vengono utilizzati per crittografare i tuoi dati durante il transito. Viene utilizzato per tutti i flussi di dati degli AWS Ground Station agenti.
5. Imposta i tuoi flussi di dati. Crea i flussi di dati in modo che corrispondano ai segnali dell'operatore utilizzando le configurazioni create nel passaggio precedente.
6. [Facoltativo] Imposta la durata del contatto prima e dopo il passaggio. Viene utilizzato per emettere eventi per contatto rispettivamente prima e dopo il contatto. Per ulteriori informazioni, consulta Automatizza AWS Ground Station con gli eventi.
7. [Opzionale] Imposta il tuo telemetrySinkConfigArn per abilitare la telemetria durante i contatti. Ciò ti consente di ricevere telemetria quasi in tempo reale direttamente nel tuo account per il monitoraggio e l'analisi. Per ulteriori informazioni, consulta Lavora con la telemetria.
8. [Facoltativo] Puoi associare i tag al tuo profilo di missione. Questi possono essere usati per aiutarti a differenziare programmaticamente i tuoi profili di missione.

Puoi fare riferimento aEsempi di configurazioni del profilo di missione, per vedere solo alcune delle possibili configurazioni.

Comprendi i passaggi successivi

Ora che hai un satellite a bordo e un profilo di missione valido, sei pronto per programmare i contatti e comunicare con il tuo satellite. AWS Ground Station

Puoi programmare un contatto in uno dei seguenti modi:

- La AWS Ground Station console.
- Il comando AWS CLI reserve-contact.
- L'SDK. AWS ReserveContact API.

Per informazioni su come AWS Ground Station traccia la traiettoria del satellite e su come tali informazioni vengono utilizzate, si prega di fare riferimento. Comprendi come AWS Ground Station utilizza le effemeridi

AWS Ground Station mantiene una serie di CloudFormation modelli preconfigurati per semplificare l'utilizzo del servizio. Vedi Esempi di configurazioni del profilo di missione alcuni esempi di come AWS Ground Station può essere utilizzato.

L'elaborazione dei dati digitali a frequenza intermedia o dei dati demodulati e decodificati forniti all'utente AWS Ground Station dipenderà dal caso d'uso specifico. I seguenti post del blog possono aiutarti a comprendere alcune delle opzioni disponibili:

- Osservazione automatica della Terra tramite la distribuzione dei dati di AWS Ground Station Amazon S3 (e il GitHub repository associato awslabs/) aws-groundstation-eos-pipeline
- Virtualizzazione del segmento terrestre satellitare con AWS
- Osservazione della Terra utilizzando AWS Ground Station: Una guida pratica
- Creazione di architetture di downlink di dati satellitari ad alto rendimento con AWS Ground Station WideBand DigiF e Amphinicy Blink SDR (e il repository associato aws-samples/) GitHub aws-groundstation-wbdigif-snpp

AWS Ground Station Sedi

AWS Ground Station fornisce una rete globale di stazioni terrestri in prossimità della nostra rete globale di regioni infrastrutturali AWS. Puoi configurare l'uso di queste sedi da qualsiasi regione AWS supportata. Ciò include la regione AWS in cui vengono distribuiti i dati.

Individuazione della AWS regione in cui localizzare una stazione di terra

La rete AWS Ground Station globale include stazioni di terra che non si trovano fisicamente nella regione AWS a cui sono connesse. L'elenco delle stazioni terrestri a cui hai accesso può essere recuperato tramite la risposta dell'SDK ListGroundStationAWS. L'elenco completo delle ubicazioni delle stazioni di terra è presentato di seguito, e altre saranno presto disponibili. Consultate la guida all'onboarding per aggiungere o modificare le approvazioni dei siti per i vostri satelliti.

Nome Ground Station	Ubicazione della Ground Station	Nome regione AWS	Codice regionale AWS	Note
Alaska 1	Alaska, Stati Uniti	US West (Oregon)	us-west-2	Non si trova fisicamente in una regione AWS
Bahrein 1	Bahrein	Medio Oriente (Bahrein)	me-south-1	
Città del Capo 1	Città del Capo, Sudafrica	Africa (Cape Town)	af-south-1	
Dubbo 1	Dubbo, Australia	Asia Pacific (Sydney)	ap-southeast-2	Non si trova fisicamente in una regione AWS
Hawaii 1	Hawaii, Stati Uniti	US West (Oregon)	us-west-2	Non si trova fisicamente in una regione AWS
Irlanda 1	Irlanda	Europa (Irlanda)	eu-west-1	
Ohio 1	Ohio, Stati Uniti	Stati Uniti orientali (Ohio)	us-east-2	
Oregon 1	Oregon, Stati Uniti	US West (Oregon)	us-west-2	
Punta Arenas 1	Punta Arenas, Cile	Sud America (São Paulo)	sa-east-1	Non si trova fisicamente in una regione AWS
Seoul 1	Seoul, Corea del Sud	Asia Pacifico (Seul)	ap-northeast-2	

Nome Ground Station	Ubicazione della Ground Station	Nome regione AWS	Codice regionale AWS	Note
Singapore 1	Singapore	Asia Pacific (Singapore)	ap-southeast-1	
Stoccolma 1	Stoccolma, Svezia	Europa (Stoccolma)	eu-north-1	

AWS Ground Station regioni AWS supportate

Puoi fornire dati e configurare i tuoi contatti tramite l'SDK AWS o la AWS Ground Station console delle regioni AWS supportate. Puoi visualizzare le regioni supportate e gli endpoint associati negli endpoint e nelle AWS Ground Station quote.

Disponibilità dei gemelli digitali

Usa la funzione AWS Ground Station digital twinè disponibile in tutte le regioni AWS in cui AWS Ground Station è disponibile. Le stazioni di terra gemelle digitali sono copie esatte delle stazioni di terra di produzione con un prefisso modificabile in Ground Station Nome di «Digital Twin». Ad esempio, «Digital Twin Ohio 1" è una stazione di terra doppia digitale che è una copia esatta della stazione di base di produzione «Ohio 1".

AWS Ground Station maschere del sito

A ogni posizione AWS Ground Station dell'antenna sono associate delle maschere di sito. Queste maschere impediscono alle antenne presenti in quella posizione di trasmettere o ricevere quando puntano in alcune direzioni, in genere vicino all'orizzonte. Le maschere possono tenere conto di:

- Caratteristiche del terreno geografico che circonda l'antenna: ad esempio, ciò include elementi come montagne o edifici che bloccherebbero un segnale a radiofrequenza (RF) o impedirebbero la trasmissione.
- Interferenza a radiofrequenza (RFI): ciò influisce sia sulla capacità di ricezione (sorgenti RFI esterne che influiscono su un segnale di downlink nelle antenne AWS Ground Station) sia sulla capacità di trasmissione (il segnale RF trasmesso dalle antenne di AWS Ground Station con un impatto negativo sui ricevitori esterni).

- Autorizzazioni legali: le autorizzazioni dei siti locali per utilizzare AWS Ground Station in ciascuna regione possono includere restrizioni specifiche, come un angolo di elevazione minimo per la trasmissione.

Queste maschere del sito possono cambiare nel tempo. Ad esempio, è possibile costruire nuovi edifici vicino a un'antenna, le sorgenti RFI potrebbero cambiare o l'autorizzazione legale potrebbe essere rinnovata con diverse restrizioni. Le maschere del sito AWS Ground Station sono disponibili in base a un accordo di non divulgazione (NDA).

Maschere specifiche per cliente

Oltre alle maschere del sito AWS Ground Station in ogni sito, potresti avere maschere aggiuntive a causa delle restrizioni sulla tua autorizzazione legale a comunicare con i tuoi satelliti in una determinata regione. Tali maschere possono essere configurate in AWS Ground Station per case-by-case garantire la conformità quando si utilizza AWS Ground Station per comunicare con questi satelliti. Contatta il team di AWS Ground Station per ulteriori dettagli.

Impatto delle maschere del sito sugli orari di contatto disponibili

Esistono due tipi di maschere del sito: le maschere del sito in uplink (trasmissione) e le maschere del sito in downlink (ricezione).

Quando elenca gli orari di contatto disponibili utilizzando l' ListContacts operazione, AWS Ground Station restituirà gli orari di visibilità in base a quando il satellite salirà al di sopra e si posizionerà al di sotto della maschera di downlink. Gli orari di contatto disponibili si basano su questa finestra di visibilità della maschera di downlink. In questo modo si evita di riservare del tempo quando il satellite si trova al di sotto della maschera di downlink.

Le maschere del sito Uplink non vengono applicate agli orari di contatto disponibili, anche se il Mission Profile include un Antenna Uplink Config in un dataflow edge. Ciò consente di utilizzare tutto il tempo di contatto disponibile per il downlink, anche se l'uplink potrebbe non essere disponibile per alcuni periodi di tempo a causa della maschera del sito uplink. Tuttavia, il segnale di uplink potrebbe non essere trasmesso per una parte o per tutto il tempo riservato a un contatto satellitare. L'utente è responsabile della contabilizzazione della maschera di uplink fornita durante la pianificazione delle trasmissioni in uplink.

La parte di contatto non disponibile per l'uplink varia a seconda della traiettoria del satellite durante il contatto, rispetto alla maschera del sito di uplink nella posizione dell'antenna. Nelle regioni in cui

le maschere del sito in uplink e in downlink sono simili, la durata è in genere breve. In altre regioni, in cui la maschera di uplink può essere notevolmente superiore a quella della maschera del sito in downlink, ciò potrebbe comportare che parti significative, o addirittura tutta, della durata del contatto non siano disponibili per l'uplink. L'intero tempo di contatto viene fatturato all'utente, anche se una parte del tempo riservato non è disponibile per l'uplink.

AWS Ground Station Funzionalità del sito

Per semplificare l'esperienza, AWS Ground Station determina un insieme comune di funzionalità per un tipo di antenna e quindi distribuisce più antenne in una stazione di terra. Parte delle fasi di onboarding garantisce la compatibilità del satellite con i tipi di antenna presenti in una posizione specifica. Quando si prenota un contatto, si determina indirettamente il tipo di antenna utilizzato. Ciò garantisce che l'esperienza in una particolare stazione di terra rimanga la stessa nel tempo, indipendentemente dalle antenne utilizzate. Le prestazioni specifiche del contatto varieranno a causa di un'ampia varietà di fattori ambientali, come le condizioni meteorologiche del sito.

Attualmente, tutti i siti supportano le seguenti funzionalità:

> **Note**
>
> Ogni riga della tabella seguente indica un percorso di comunicazione indipendente, salvo diversa indicazione. Esistono righe duplicate per riflettere le nostre funzionalità multicanale che consentono l'utilizzo simultaneo di più percorsi di comunicazione.

Tipo di capacità	Intervallo di frequenza	Intervallo di larghezza di banda	Polarization	Common Name (Nome comune)	Note
antenna - downlink	7750 - 8500 MHz	50 - 400 MHz	RHCP	Downlink a banda larga in banda X	Questa funzionalità richiede l'uso dell'agente.AWS Ground Station
antenna - downlink	7750 - 8500 MHz	50 - 400 MHz	RHCP		
antenna - downlink	7750 - 8500 MHz	50 - 400 MHz	RHCP		

Tipo di capacità	Intervallo di frequenza	Intervallo di larghezza di banda	Polarization	Common Name (Nome comune)	Note
antenna - downlink	7750 - 8500 MHz	50 - 400 MHz	RHCP		Questa funzionalità non è supportata in Alaska 1 o Punta Arenas 1. La larghezza di banda aggregata non deve superare 400 MHz per polarizzazione in ogni posizione. Tutte le gamme di frequenza utilizzate non devono sovrapporsi.
antenna - downlink	7750 - 8500 MHz	50 - 400 MHz	RHCP		
antenna - downlink	7750 - 8500 MHz	50 - 400 MHz	LHCP		
antenna - downlink	7750 - 8500 MHz	50 - 400 MHz	LHCP		
antenna - downlink	7750 - 8500 MHz	50 - 400 MHz	LHCP		
antenna - downlink	7750 - 8500 MHz	50 - 400 MHz	LHCP		
antenna - downlink	7750 - 8500 MHz	50 - 400 MHz	LHCP		
antenna - downlink	2200 - 2290 MHz	Fino a 40 MHz	RHCP	Downlink in banda S	È possibile utilizzare una sola polarizzazione alla volta
antenna - downlink	2200 - 2290 MHz	Fino a 40 MHz	LHCP		

Tipo di capacità	Intervallo di frequenza	Intervallo di larghezza di banda	Polarization	Common Name (Nome comune)	Note
antenna - downlink	7750 - 8500 MHz	Fino a 40 MHz	RHCP	Downlink a banda stretta in banda X	È possibile utilizzare una sola polarizzazione alla volta
antenna - downlink	7750 - 8500 MHz	Fino a 40 MHz	LHCP		
antenna - uplink	2025 - 2110 MHz	Fino a 40 MHz	RHCP	uplink in banda S	È possibile utilizzare una sola polarizzazione alla volta EIRP 20-50 dBW
antenna-uplink	2025 - 2110 MHz	Fino a 40 MHz	LHCP		
antenna-uplink-echo	2025 - 2110 MHz	2 MHz	RHCP	Eco in uplink	Rispetta le restrizioni relative all'antenna e all'uplink
antenna-uplink-echo	2025 - 2110 MHz	2 MHz	LHCP		
antenna-downlink-demod-decode	750 - 850 MHz	Fino a 500 MHz	RHCP	Downlink demodulato e decodificato in banda X	
antenna-downlink-demod-decode	7750 - 8500 MHz	Fino a 500 MHz	LHCP		

Tipo di capacità	Intervallo di frequenza	Intervallo di larghezza di banda	Polarization	Common Name (Nome comune)	Note
tracking	N/D	N/D	N/D	N/D	Support per il tracciamento automatico e il tracciamento dei programmi

* RHCP = polarizzazione circolare destra e LHCP = polarizzazione circolare sinistra. Per ulteriori informazioni sulla polarizzazione, vedere Polarizzazione circolare.

Comprendi come AWS Ground Station utilizza le effemeridi

Un'effemeride, plurale effemeridi, è un file o una struttura di dati che fornisce la traiettoria degli oggetti astronomici. Storicamente, questo file si riferiva solo a dati tabulari ma, gradualmente, è passato a indirizzarsi a un'ampia varietà di file di dati che indicavano la traiettoria di un veicolo spaziale.

L'API Ephemeris consente di caricare effemeridi personalizzate da utilizzare con un satellite. AWS Ground Station Queste effemeridi sostituiscono le effemeridi predefinite di Space-Track (vedi:). Dati predefiniti sulle effemeridi Supportiamo la ricezione di dati sulle effemeridi nei formati Orbit Ephemeris Message (OEM), Two Line Element (TLE) e elevazione azimutale.

AWS Ground Station utilizza i dati sulle effemeridi per determinare quando i contatti diventano disponibili in base alle effemeridi fornite e comanda correttamente le antenne nella rete. AWS Ground Station Per impostazione predefinita, non è richiesta alcuna azione per fornire effemeridi se al satellite è AWS Ground Station assegnato un ID NORAD.

Il caricamento di effemeridi personalizzate può migliorare la qualità del tracciamento, gestire le operazioni iniziali laddove non sono disponibili effemeridi Space-Track e tenere conto delle manovre. AWS Ground Station

In alternativa, AWS Ground Station supporta un formato di elevazione azimutale, che consente di specificare direttamente le direzioni di puntamento dell'antenna senza fornire informazioni orbitali satellitari. Ciò è utile negli scenari in cui è necessario un puntamento preciso dell'antenna perché le informazioni sulla traiettoria satellitare sono imprecise o sconosciute.

Argomenti

Dati predefiniti sulle effemeridi

Per impostazione predefinita, AWS Ground Station utilizza i dati disponibili pubblicamente da Space-Track e non è richiesta alcuna azione per fornire AWS Ground Station queste effemeridi predefinite. Queste effemeridi sono set di elementi a due righe () associati all'ID NORAD del satellite. TLEs Tutte le effemeridi predefinite hanno una priorità di. `0` Di conseguenza, verranno sostituite, sempre, da tutte le effemeridi personalizzate non scadute caricate tramite l'API ephemeris, che devono sempre avere una priorità pari o superiore. 1

I satelliti senza un NORAD ID devono caricare dati sulle effemeridi personalizzati su. AWS Ground Station Ad esempio, i satelliti appena lanciati o che sono stati intenzionalmente omessi dal catalogo Space-Track non avrebbero un ID NORAD e avrebbero bisogno del caricamento di effemeridi personalizzate. Per ulteriori informazioni sulla fornitura di dati sulle effemeridi personalizzati, vedere: Fornitura di dati sulle effemeridi personalizzati.

Fornisci dati sulle effemeridi personalizzati

> **Important**
>
> L'API ephemeris è attualmente in uno stato di anteprima

L'accesso all'API Ephemeris viene fornito solo in base alle necessità. Se hai bisogno della possibilità di caricare dati sulle effemeridi personalizzati, apri un ticket tramite. Supporto AWS AWS Support Center Console Il nostro team collaborerà con voi per abilitare questa funzionalità in base alle vostre esigenze specifiche.

Panoramica di

L'API Ephemeris consente di caricare effemeridi personalizzate da utilizzare con un satellite. AWS Ground Station Queste effemeridi sostituiscono le effemeridi predefinite di Space-Track (vedi:). Dati predefiniti sulle effemeridi Supportiamo la ricezione di dati sulle effemeridi nei formati Orbit Ephemeris Message (OEM), Two Line Element (TLE) e elevazione azimutale.

AWS Ground Station tratta le effemeridi come dati di utilizzo personalizzati. Se utilizzi questa funzionalità opzionale, AWS utilizzerà i tuoi dati sulle effemeridi per fornire supporto per la risoluzione dei problemi.

Il caricamento di effemeridi personalizzate può migliorare la qualità del tracciamento, gestire operazioni in cui non sono disponibili effemeridi Space-Track e tenere conto delle manovre. AWS Ground Station

Per risolvere un problema con un'effemeride non valida, consulta: Risoluzione dei problemi relativi alle effemeridi non valide

Esempio: utilizzo di effemeridi fornite dal cliente con AWS Ground Station

Per istruzioni più dettagliate sull'utilizzo delle effemeridi fornite dal cliente con, consulta Utilizzo delle effemeridi fornite dal cliente con e il repository associato AWS Ground Station aws-samples/. AWS Ground Station GitHub aws-groundstation-cpe

Fornisci dati sulle effemeridi TLE

> **Important**
>
> L'API delle effemeridi è attualmente in uno stato di anteprima

L'accesso all'API Ephemeris viene fornito solo in base alle necessità. Se hai bisogno della possibilità di caricare dati sulle effemeridi personalizzati, apri un ticket tramite. Supporto AWS AWS Support Center Console Il nostro team collaborerà con voi per abilitare questa funzionalità in base alle vostre esigenze specifiche.

Panoramica di

I set di elementi a due linee (TLE) sono un formato standardizzato per descrivere le orbite dei satelliti. L'API Ephemeris consente di caricare effemeridi TLE per utilizzarle con un satellite. AWS Ground Station Queste effemeridi sostituiscono le effemeridi predefinite di Space-Track (vedi:). Dati predefiniti sulle effemeridi

AWS Ground Station tratta le effemeridi come dati di utilizzo personalizzati. Se utilizzi questa funzionalità opzionale, AWS utilizzerà i tuoi dati sulle effemeridi per fornire supporto per la risoluzione dei problemi.

Il caricamento di effemeridi TLE personalizzate può migliorare la qualità del tracciamento, gestire le operazioni iniziali laddove non sono disponibili effemeridi Space-Track e tenere conto delle manovre. AWS Ground Station

> **Note**
>
> Quando si forniscono effemeridi personalizzate prima che venga assegnato un numero di catalogo satellitare al satellite, è possibile utilizzarlo `00000` per il campo del numero di catalogo satellitare del TLE e `000` per la parte relativa al numero di lancio del campo di designazione internazionale del TLE (ad esempio `24000A` per un veicolo lanciato nel 2024). Per ulteriori informazioni sul formato di, vedere Set di TLEs elementi a due righe.

Creazione di effemeridi TLE

È possibile creare un'effemeride TLE utilizzando l'azione nell'API. CreateEphemeris AWS Ground Station Questa azione caricherà un'effemeride utilizzando i dati nel corpo della richiesta o da un bucket S3 specificato.

È importante notare che il caricamento di un'effemeride imposta le effemeridi e avvia un flusso di lavoro asincrono che convaliderà `VALIDATING` e genererà potenziali contatti a partire dalle effemeridi. Solo dopo che un'effemeride avrà superato questo flusso di lavoro e sarà diventata tale, verrà utilizzata per i contatti. `ENABLED` È necessario eseguire un sondaggio DescribeEphemerisper verificare lo stato delle effemeridi o utilizzare CloudWatch gli eventi per tenere traccia delle modifiche allo stato delle effemeridi.

Per risolvere un problema di effemeridi non valido, consulta: Risoluzione dei problemi relativi alle effemeridi non valide

Esempio: crea un set di effemeridi a due righe (TLE) tramite API

È possibile utilizzare la AWS SDKs CLI e per caricare un set di effemeridi a due elementi di riga (TLE) tramite la chiamata. AWS Ground Station CreateEphemeris Queste effemeridi verranno utilizzate al posto dei dati sulle effemeridi predefiniti per un satellite (vedi). Dati predefiniti sulle effemeridi Questo esempio mostra come eseguire questa operazione utilizzando l'AWS SDK for Python (Boto3).

Un set TLE è un oggetto in formato JSON che mette insieme uno o più TLEs oggetti per costruire una traiettoria continua. Il TLEs set TLE deve formare un insieme continuo che possiamo usare per costruire una traiettoria (cioè nessun intervallo di tempo tra un set TLE e l'altro). TLEs Di seguito è riportato un esempio di set 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**
>
> Gli intervalli di tempo di un set TLE devono corrispondere esattamente per essere una traiettoria valida e continua. TLEs

Un set TLE può essere caricato tramite il client AWS Ground Station boto3 nel modo seguente:

```
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  .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),
                    },
                }
            ]
        }
    },
)

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

Questa chiamata restituirà un ephemerisID che può essere utilizzato per fare riferimento alle effemeridi in futuro. Ad esempio, possiamo utilizzare l'ephemerisID fornito dalla chiamata precedente per verificare lo stato delle effemeridi:

```
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']}")
```

Di seguito viene fornito un esempio di risposta derivante dall'azione 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}}]"
```

```
    }
  }
}
```

Si consiglia di eseguire il polling del DescribeEphemerispercorso o utilizzare CloudWatch gli eventi per tenere traccia dello stato delle effemeridi caricate, poiché deve passare attraverso un flusso di lavoro di convalida asincrono prima che venga impostato e diventi utilizzabile per la pianificazione ENABLED e l'esecuzione dei contatti.

Notate che l'ID NORAD in tutto il set TLE, TLEs negli esempi precedenti, deve corrispondere all'ID NORAD assegnato al vostro satellite 25994 nel database Space-Track.

Esempio: caricamento di dati sulle effemeridi TLE da un bucket S3

È anche possibile caricare un file di effemeridi TLE direttamente da un bucket S3 puntando al bucket e alla chiave dell'oggetto. AWS Ground Station recupererà l'oggetto per tuo conto. Le informazioni sulla crittografia dei dati archiviati AWS Ground Station sono dettagliate in:Crittografia dei dati a riposo per AWS Ground Station.

Di seguito è riportato un esempio di caricamento di un file di effemeridi TLE da un bucket 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']}")
```

Fornisci dati sulle effemeridi OEM

> **Important**
>
> L'API ephemeris è attualmente in uno stato di anteprima

L'accesso all'API Ephemeris viene fornito solo in base alle necessità. Se hai bisogno della possibilità di caricare dati sulle effemeridi personalizzati, apri un ticket tramite. Supporto AWS AWS Support Center Console Il nostro team collaborerà con voi per abilitare questa funzionalità in base alle vostre esigenze specifiche.

Panoramica di

Orbit Ephemeris Message (OEM) è un formato standardizzato per la rappresentazione dei dati di traiettoria dei veicoli spaziali. L'API Ephemeris consente di caricare effemeridi OEM per utilizzarle con un satellite. AWS Ground Station Queste effemeridi sostituiscono le effemeridi predefinite di Space-Track (vedi:). Dati predefiniti sulle effemeridi

AWS Ground Station tratta le effemeridi come dati di utilizzo personalizzati. Se utilizzi questa funzionalità opzionale, AWS utilizzerà i tuoi dati sulle effemeridi per fornire supporto per la risoluzione dei problemi.

Il caricamento di effemeridi OEM personalizzate può migliorare la qualità del tracciamento, gestire le operazioni iniziali laddove non sono disponibili effemeridi Space-Track e tenere conto delle manovre. AWS Ground Station

> **Note**
>
> Quando si forniscono effemeridi personalizzate prima che venga assegnato un numero di catalogo satellitare al satellite, è possibile utilizzarle per la parte dell'OEM. `satelliteId` `OBJECT_ID`
> Per ulteriori informazioni sul formato di, vedere. OEMs Formato delle effemeridi OEM

Formato delle effemeridi OEM

AWS Ground Station elabora le effemeridi fornite dal cliente OEM secondo lo standard CCSDS con alcune restrizioni aggiuntive. I file OEM devono essere in formato KVN. La tabella seguente illustra i diversi campi di un OEM e le AWS Ground Station differenze rispetto allo standard CCSDS.

Sezione	Campo	CCSDS richiesto	AWS Ground Station richiesto	Note
Header	CCSDS_OEM_VERS	Sì	Sì	Valore richiesto: 2.0
	COMMENT	No	No	
	CLASSIFICAZIONE	No	No	
	DATA_CREAZIONE	Sì	Sì	
	ARTEFICE	Sì	Sì	
	ID_MESSAGGIO	No	No	
Metadati	META_START	Sì	Sì	
	COMMENT	No	No	
	NOME_OGGETTO	Sì	Sì	
	ID_OGGETTO	Sì	Sì	
	NOME_CENTRO	Sì	Sì	Valore richiesto: Terra
	REF_FRAME	Sì	Sì	Valori accettati :, EME2000 ITRF2000

Sezione	Campo	CCSDS richiesto	AWS Ground Station richiesto	Note
	REF_FRAME _EPOCH	No	Non supportato*	Non necessari o perché i REF_ accettati FRAMEs hanno un'epoca implicita
	SISTEMA_O RARIO	Sì	Sì	Valore richiesto: UTC
	ORA DI INIZIO	Sì	Sì	
	ORA_DI_IN IZIO_UTIL IZZABILE	No	No	
	TEMPO_STO P_UTILIZZABILE	No	No	
	STOP_TIME	Sì	Sì	
	INTERPOLA ZIONE	No	Sì	Necessario in modo da AWS Ground Station poter generare angoli di puntament o accurati per i contatti.

Sezione	Campo	CCSDS richiesto	AWS Ground Station richiesto	Note
	GRADO_INTERPOLAZIONE	No	Sì	Necessario in modo da AWS Ground Station poter generare angoli di puntamento accurati per i contatti.
	META_STOP	Sì	Sì	
Dati	X	Sì	Sì	Rappresentato in `km`
	Y	Sì	Sì	Rappresentato in `km`
	Z	Sì	Sì	Rappresentato in `km`
	X_DOT	Sì	Sì	Rappresentato in `km/s`
	Y_DOT	Sì	Sì	Rappresentato in `km/s`
	Z_DOT	Sì	Sì	Rappresentato in `km/s`
	X_DDOT	No	No	Rappresentato in `km/s^2`
	Y_DDOT	No	No	Rappresentato in `km/s^2`

Sezione	Campo	CCSDS richiesto	AWS Ground Station richiesto	Note
	Z_DDOT	No	No	Rappresentato in `km/s^2`
Matrice di covarianza	COVARIANZA_INIZIO	No	No	
	EPOCA	No	No	
	COV_REF_FRAME	No	No	
	COVARIANZA_STOP	No	No	

* Se nell'OEM fornito AWS Ground Station sono incluse righe non supportate da, l'OEM non procederà alla convalida.

Le deviazioni importanti dallo standard CCSDS per sono: AWS Ground Station

- `CCSDS_OEM_VERS`deve esserlo. `2.0`
- `REF_FRAME`deve essere uno dei due `EME2000 ITRF2000`.
- `REF_FRAME_EPOCH`non è supportato da AWS Ground Station.
- `CENTER_NAME`deve esserlo`Earth`.
- `TIME_SYSTEM`deve esserlo`UTC`.
- `INTERPOLATION`e `INTERPOLATION_DEGREE` sono entrambi obbligatori per le effemeridi fornite dal AWS Ground Station cliente.

Esempio di effemeridi OEM in formato KVN

Di seguito è riportato un esempio troncato di effemeridi OEM in formato KVN per l'emittente satellitare pubblica 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
```

Creazione di un'effemeride OEM

È possibile creare un'effemeride OEM utilizzando l'azione nell'API. CreateEphemeris AWS Ground Station Questa azione caricherà un'effemeride utilizzando i dati nel corpo della richiesta o da un bucket S3 specificato.

È importante notare che il caricamento di un'effemeride imposta le effemeridi e avvia un flusso di lavoro asincrono che convaliderà `VALIDATING` e genererà potenziali contatti a partire dalle effemeridi. Solo dopo che un'effemeride avrà superato questo flusso di lavoro e sarà diventata tale, verrà utilizzata per i contatti. `ENABLED` È necessario eseguire un sondaggio DescribeEphemerisper verificare lo stato delle effemeridi o utilizzare CloudWatch gli eventi per tenere traccia delle modifiche allo stato delle effemeridi.

Per risolvere un problema di effemeridi non valido, consulta: Risoluzione dei problemi relativi alle effemeridi non valide

Esempio: caricamento di dati sulle effemeridi OEM da un bucket S3

È anche possibile caricare un file di effemeridi OEM direttamente da un bucket S3 puntando al bucket e alla chiave dell'oggetto. AWS Ground Station recupererà l'oggetto per tuo conto. Le informazioni sulla crittografia dei dati archiviati AWS Ground Station sono dettagliate in:Crittografia dei dati a riposo per AWS Ground Station.

Di seguito è riportato un esempio di caricamento di un file di effemeridi OEM da un bucket 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']}")
```

Di seguito è riportato un esempio di dati restituiti dall'DescribeEphemerisazione richiesta per le effemeridi OEM caricate nel precedente blocco di codice di esempio.

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

Fornisci dati sulle effemeridi di elevazione dell'azimut

> **Important**
>
> La funzionalità delle effemeridi di elevazione azimutale è attualmente in uno stato di anteprima e richiede un onboarding esplicito.

La funzionalità delle effemeridi di elevazione di Azimuth è sottoposta a un rigoroso controllo degli accessi per un numero limitato di casi d'uso predeterminati e specializzati. L'accesso è notevolmente più restrittivo rispetto alle funzionalità di effemeridi standard fornite dal cliente. Per ulteriori informazioni sui casi d'uso approvati e sulla procedura di richiesta di accesso, apri un ticket tramite il. Supporto AWS AWS Support Center Console Il nostro team ti guiderà attraverso il processo di approvazione per casi d'uso specializzati.

Panoramica di

Le effemeridi di elevazione azimutale forniscono un modo per specificare direttamente le direzioni di puntamento dell'antenna senza fornire informazioni orbitali satellitari. Invece di caricare dati sulle effemeridi che descrivono l'orbita di un satellite, è possibile fornire angoli di azimut e di elevazione con marcatura temporale che indicano all'antenna esattamente dove puntare durante il contatto.

AWS Ground Station tratta le effemeridi come dati di utilizzo personalizzati. Se utilizzi questa funzionalità opzionale, AWS utilizzerà i tuoi dati sulle effemeridi per fornire supporto per la risoluzione dei problemi.

Questo approccio è particolarmente utile per i seguenti scenari:

- Supporto operativo precoce: durante la fase di lancio e la fase iniziale di orbita (LEOP) quando non sono disponibili dati orbitali precisi o i parametri orbitali cambiano rapidamente.
- Schemi di puntamento personalizzati: implementazione di sequenze di puntamento specifiche per testare le antenne o operazioni non standard.

Note

Quando si utilizzano effemeridi di elevazione azimutale, l'ARN satellitare può essere omesso dalla richiesta di prenotazione del contatto. Se l'ARN satellitare non viene omesso, verrà comunque incluso come parte dei dati di contatto, ma le effemeridi di elevazione azimutale verranno utilizzate per il puntamento dell'antenna anziché per eseguire la risoluzione prioritaria delle effemeridi. Le effemeridi di elevazione azimutale sono associate a una stazione terrestre specifica e definiscono le direzioni di puntamento dell'antenna per quella posizione.

Formato dei dati sulle effemeridi di elevazione azimutale

I dati sulle effemeridi di elevazione azimutale sono costituiti da valori di azimut ed elevazione con marcatura temporale organizzati in segmenti. Ogni segmento contiene una serie di angoli di azimut e di elevazione che coprono un intervallo di tempo specifico.

I componenti chiave dei dati sulle effemeridi di elevazione dell'azimut sono:

- Ground Station: La stazione terrestre specifica in cui verranno utilizzate queste effemeridi di elevazione azimutale.
- Unità angolare: L'unità di misura degli angoli (o). `DEGREE_ANGLE` `RADIAN`
- Segmenti: una o più raccolte di angoli di azimut e di elevazione limitate nel tempo.
- Angoli con marcatura temporale: valori individuali di azimut ed elevazione con timestamp associati.

Ogni segmento richiede:

- Un'epoca di riferimento (l'ora base del segmento)
- Un intervallo di tempo valido (ora di inizio e fine del segmento)
- Almeno 5 coppie con data e ora azimuth/elevation

Vincoli di elevazione azimutale:

- Azimut in gradi: da -180° a 360°
- Azimut in radianti: da -π a 2π
- Elevazione in gradi: da -90° a 90°
- Elevazione in radianti: da -π /2 a π /2
- I valori temporali devono essere in ordine crescente all'interno di ogni segmento
- I segmenti non devono sovrapporsi nel tempo

Per ulteriori informazioni, consulta la documentazione dell'CreateEphemerisAPI e il tipo di TimeAzEldati.

Creazione di effemeridi di elevazione azimutale

Le effemeridi di elevazione azimutale vengono create utilizzando la stessa azione API, ma con il tipo di effemeridi. CreateEphemeris`azEl` Le differenze principali rispetto alle effemeridi TLE e OEM sono:

- È necessario specificare un parametro `groundStation`
- Il `satelliteId` parametro deve essere omesso dalla richiesta
- Le impostazioni di priorità non si applicano (ogni effemeride di elevazione azimutale è specifica di una stazione terrestre)
- Ogni segmento deve contenere almeno 5 azimuth/elevation punti per supportare l'interpolazione di Lagrange di 4° ordine
- I limiti e i requisiti aggiuntivi sono descritti in dettaglio nella documentazione dell'API CreateEphemeris

È importante notare che il caricamento di un'effemeride imposta le effemeridi `VALIDATING` e avvia un flusso di lavoro asincrono che convaliderà e genererà potenziali contatti a partire dalle effemeridi. Un'effemeride verrà utilizzata per i contatti solo dopo che avrà superato questo flusso di lavoro e il suo stato sarà diventato. `ENABLED` È necessario eseguire un sondaggio DescribeEphemerisper verificare lo stato delle effemeridi o utilizzare CloudWatch gli eventi per tenere traccia delle modifiche allo stato delle effemeridi.

Per risolvere un problema di effemeridi non valido, consulta: Risoluzione dei problemi relativi alle effemeridi non valide

Esempio: creazione di effemeridi di elevazione dell'azimut tramite API

L'esempio seguente mostra come creare effemeridi di elevazione azimutale utilizzando l' AWS SDK for 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']}")
```

In questo esempio:

- I dati di elevazione azimutale sono associati alla stazione terrestre «Ohio 1"
- Gli angoli sono specificati in gradi
- Il segmento copre un periodo di 15 minuti
- I `dt` valori sono secondi atomici scostati dall'epoca di riferimento
- Vengono fornite sei azimuth/elevation coppie (il minimo è 5)

Esempio: carica i dati di elevazione azimutale da S3

Per set di dati più grandi, puoi caricare i dati di elevazione azimutale da un bucket 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']}")
```

L'oggetto S3 deve contenere una struttura JSON con i dati di elevazione azimutale nello stesso formato mostrato nell'esempio di caricamento diretto.

Prenotazione dei contatti con effemeridi di elevazione azimutale

Quando si utilizza un'effemeride di elevazione azimutale per riservare un contatto, il processo è diverso da quello delle effemeridi TLE e OEM:

1. Crea le effemeridi di elevazione dell'azimut usando CreateEphemeris
2. Attendi che le effemeridi raggiungano lo stato `ENABLED`
3. Prenota il contatto utilizzando le opzioni di ReserveContacttracciamento

Esempio di prenotazione di un contatto con effemeridi di elevazione dell'azimut:

```
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**
>
> Il `satelliteArn` parametro può essere omesso quando si riserva un contatto con le effemeridi di elevazione dell'azimut. L'antenna seguirà gli angoli di azimut e di elevazione specificati durante il contatto.

Elenco dei contatti disponibili

Quando si utilizzano le effemeridi di elevazione azimutale, l'ListContactsAPI richiede parametri specifici:

- Il `satelliteArn` parametro può essere omesso dalla richiesta

- È necessario fornire un `ephemeris` parametro con l'ID delle effemeridi di elevazione dell'azimut per specificare quali effemeridi utilizzare
- Le finestre di contatto disponibili mostrano quando gli angoli di azimut e di elevazione forniti si trovano al di sopra della maschera del sito della stazione terrestre richiesta
- Devi comunque fornire e `groundStation` `missionProfileArn`

Esempio di creazione di effemeridi di elevazione azimutale e di elenco dei contatti disponibili con essa:

```
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**
>
> Il `ephemeris` parametro con l'ID di elevazione azimutale deve essere fornito quando si elencano i contatti per specificare quali effemeridi di elevazione azimutale devono essere utilizzate per determinare le finestre di contatto. Se `satelliteArn` è incluso, verrà associato ai dati di contatto, ma le effemeridi di elevazione azimutale verranno utilizzate per il puntamento dell'antenna anziché per eseguire la risoluzione prioritaria delle effemeridi.

Riserva i contatti con effemeridi personalizzate

Panoramica di

Quando si utilizzano effemeridi personalizzate (TLE, OEM o elevazione azimutale), è possibile prenotare i contatti utilizzando l'API. ReserveContact Questa sezione descrive due flussi di lavoro comuni per la prenotazione dei contatti e considerazioni importanti per garantire una corretta pianificazione dei contatti.

AWS Ground Station le antenne sono risorse condivise tra più clienti. Ciò significa che anche se una finestra di contatto appare disponibile quando si elencano i contatti, un altro cliente potrebbe prenotarla prima di te. Pertanto, è fondamentale verificare che il contatto raggiunga `SCHEDULED` lo

stato dopo la prenotazione e implementare un monitoraggio adeguato delle modifiche allo stato del contatto.

> **Important**
>
> Per le effemeridi di elevazione azimutale, il `satelliteArn` parametro può essere omesso dalla `ReserveContact` richiesta ed è necessario fornire l'ID delle effemeridi. `trackingOverrides` Per le effemeridi TLE e OEM, è comunque necessario fornire il. `satelliteArn`

Contatta i flussi di lavoro di prenotazione

Esistono due flussi di lavoro principali per la prenotazione di contatti con effemeridi personalizzate:

1. List-then-reserve flusso di lavoro: prima elenca le finestre di contatto disponibili utilizzando ListContacts, quindi seleziona e prenota una finestra specifica. Questo approccio è utile quando si desidera visualizzare tutte le opportunità disponibili prima di effettuare una selezione.
2. Flusso di lavoro di prenotazione diretta: prenota direttamente un contatto per una finestra temporale specifica senza prima elencare i contatti disponibili. Questo approccio è utile quando conosci già l'orario di contatto desiderato o lavori con orari predeterminati.

Entrambi i flussi di lavoro sono validi e la scelta dipende dai requisiti operativi. Le sezioni seguenti forniscono esempi di ciascun approccio.

Flusso di lavoro 1: Elenca i contatti disponibili e poi prenota

Questo flusso di lavoro richiede innanzitutto le finestre di contatto disponibili, quindi riserva una finestra specifica. Ciò è utile quando si desidera visualizzare tutte le opportunità disponibili prima di effettuare una selezione.

Esempio: elenca e prenota con effemeridi di elevazione azimutale

```
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")
```

Esempio: elenca e prenota con effemeridi 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")
```

Flusso di lavoro 2: prenotazione con contatto diretto

Questo flusso di lavoro prenota direttamente un contatto senza prima elencare le finestre disponibili. Questo approccio è utile quando si conosce già l'orario di contatto desiderato o si sta implementando una pianificazione automatizzata.

Esempio: prenotazione diretta con effemeridi di elevazione azimutale

```
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']}")
```

Esempio: prenotazione diretta con effemeridi 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']}")
```

Monitoraggio delle modifiche allo stato dei contatti

Dopo aver prenotato un contatto, è importante monitorarne lo stato per assicurarsi che passi correttamente `SCHEDULED` e che venga informato di eventuali problemi. AWS Ground Station invia eventi ad Amazon EventBridge per tutte le modifiche allo stato dei contatti.

Gli stati di contatto seguono questo ciclo di vita:

- `SCHEDULING`- Il contatto è in fase di elaborazione per la pianificazione
- `SCHEDULED`- Il contatto è stato pianificato con successo e verrà eseguito
- `FAILED_TO_SCHEDULE`- Il contatto non può essere pianificato (stato del terminale)

Per ulteriori informazioni sugli stati e sul ciclo di vita dei contatti, vedere. Comprendi il ciclo di vita dei contatti

Implementazione del monitoraggio dello stato di contatto con EventBridge

Per monitorare i cambiamenti dello stato dei contatti in tempo reale, puoi impostare una EventBridge regola Amazon che attiva una funzione Lambda ogni volta che un contatto Ground Station cambia stato. Questo approccio è più efficiente e scalabile rispetto al sondaggio dello stato del contatto.

Passaggi dell'implementazione

1. Crea una funzione Lambda per elaborare gli eventi di modifica dello stato dei contatti
2. Crea una EventBridge regola che corrisponda agli eventi di modifica dello stato dei contatti di Ground Station
3. Aggiungere la funzione Lambda come obiettivo per la regola

Esempio di gestore di funzioni Lambda

Per un esempio completo di una funzione Lambda che elabora gli eventi di modifica dello stato dei contatti, consulta la `GroundStationCloudWatchEventHandlerLambda` risorsa nel modello. `AquaSnppJpssTerraDigIF.yml` CloudFormation Questo modello è disponibile nel bucket Amazon S3 per l'onboarding dei AWS Ground Station clienti. Per istruzioni sull'accesso a questo modello, consulta la Mettendolo insieme sezione relativa all'esempio dell'endpoint dataflow.

EventBridge configurazione delle regole

La EventBridge regola deve utilizzare il seguente schema di eventi per corrispondere a tutte le modifiche dello stato dei contatti di Ground Station:

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

Per filtrare solo in base a stati specifici (ad esempio, guasti), puoi aggiungere un filtro di dettaglio:

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

```
      "AWS_FAILED",
      "AWS_CANCELLED"
    ]
  }
}
```

Per istruzioni dettagliate sulla creazione di EventBridge regole con obiettivi Lambda, consulta Creazione di regole che reagiscono agli eventi nella Amazon EventBridge User Guide.

Impostazione EventBridge delle regole per l'automazione

È possibile creare EventBridge regole per rispondere automaticamente alle modifiche dello stato dei contatti. Esempio:

- Invia notifiche quando un contatto non riesce a pianificare
- Attiva le funzioni Lambda per preparare le risorse quando entra un contatto `PREPASS`
- Registra i completamenti dei contatti a scopo di controllo

Per informazioni dettagliate sull'impostazione delle EventBridge regole per AWS Ground Station gli eventi, vedere. Automatizza AWS Ground Station con gli eventi

Best practice e considerazioni

Gestione dei conflitti di pianificazione

Poiché le AWS Ground Station antenne sono risorse condivise, una finestra di contatto che appare disponibile in `ListContacts` potrebbe essere prenotata da un altro cliente prima che tu possa prenotarla. Per gestire questo problema:

1. Controlla sempre lo stato del contatto dopo la prenotazione
2. Implementa la logica dei tentativi con finestre temporali alternative
3. Prendi in considerazione la possibilità di prenotare i contatti con largo anticipo, quando possibile
4. Usa EventBridge gli eventi per `FAILED_TO_SCHEDULE` monitorare gli stati

Tempi di convalida delle effemeridi

Ricorda che le effemeridi devono essere attive prima di poterle utilizzare per prenotare i `ENABLED` contatti. Il processo di convalida richiede in genere da pochi secondi a qualche minuto a seconda del

tipo e della dimensione delle effemeridi. Verifica sempre lo stato delle effemeridi prima di tentare di prenotare i contatti.

Considerazioni sulla tempistica dei contatti

Quando si utilizzano effemeridi personalizzate:

- Assicurati che le effemeridi coprano l'intera durata del contatto
- Per le effemeridi di elevazione azimutale, verifica che gli angoli mantengano l'antenna sopra la maschera del sito per tutta la durata del contatto
- Prendi in considerazione i tempi di scadenza delle effemeridi quando pianifichi contatti futuri

Differenze tra le API per tipo di effemeridi

L'`ReserveContact`API si comporta in modo diverso a seconda del tipo di effemeridi:

Tipo di effemeridi	È richiesto SatelliteArn	TrackingOverrides obbligatorio
TEL	Sì	No (opzionale)
OEM	Sì	No (opzionale)
Elevazione azimutale	No (opzionale)	Sì

Comprendi quali effemeridi vengono utilizzate

Le effemeridi hanno una priorità, una data di scadenza e un flag abilitato. Insieme, determinano quali effemeridi vengono utilizzate per il tracciamento durante un contatto.

Effemeridi TLE e OEM

Per le effemeridi OEM e TLE, può essere attiva una sola effemeridi per ogni satellite. Le effemeridi che verranno utilizzate sono le effemeridi abilitate con la massima priorità la cui scadenza è nelle future. Un valore di priorità maggiore indica una priorità più alta. Gli orari di contatto disponibili restituiti da si ListContactsbasano su queste effemeridi. Se più `ENABLED` effemeridi hanno la stessa priorità, verranno utilizzate le effemeridi create o aggiornate più di recente.

> **Note**
>
> AWS Ground Station dispone di una quota di servizio sul numero di effemeridi ENABLED fornite dal cliente per satellite (vedi: Service Quotas). Per caricare i dati sulle effemeridi dopo aver raggiunto questa quota, elimina (utilizzando DeleteEphemeris) o disabilita (utilizzando) le effemeridi fornite dal cliente con la priorità più bassa/la prima creata. UpdateEphemeris

Se non è stata creata alcuna effemeride, o se nessuna effemeride ha lo status, utilizzerà un'effemeride predefinita per il satellite (da Space-Track), se disponibile. ENABLEDAWS Ground Station Questa effemeride predefinita ha priorità 0.

Effemeridi di elevazione azimutale

Le effemeridi ad elevazione azimutale funzionano in modo diverso dalle effemeridi OEM e TLE. Ogni effemeride di elevazione azimutale è associata a una stazione terrestre specifica e non ha una priorità. Quando si prenota un contatto con le effemeridi di elevazione azimutale, si specifica esplicitamente quali effemeridi di elevazione azimutale utilizzare tramite il parametro. `tracking0verrides`

Principali differenze per le effemeridi di elevazione dell'azimut:

- Nessun sistema di priorità: selezioni esplicitamente le effemeridi per ogni contatto
- Specifico della stazione terrestre: ogni effemeride è associata a una particolare stazione terrestre
- Nessun fallback automatico: se le effemeridi specificate non sono disponibili, il contatto fallirà

> **Note**
>
> Le effemeridi di elevazione azimutale non competono con le effemeridi OEM e TLE. Vengono selezionati esplicitamente al momento della prenotazione di un contatto e vengono utilizzati solo quando vengono specificate le eccezioni di tracciamento.

Effetto delle nuove effemeridi sui contatti pianificati in precedenza

Utilizza l'DescribeContact API per visualizzare gli effetti delle nuove effemeridi sui contatti pianificati in precedenza restituendo i tempi di visibilità attivi.

Per le effemeridi OEM e TLE, i contatti programmati prima del caricamento di una nuova effemeridi manterranno l'orario di contatto originariamente pianificato, mentre il tracciamento dell'antenna utilizzerà le effemeridi attive. Se la posizione del veicolo spaziale, in base alle effemeridi attive, differisce notevolmente dalle effemeridi precedenti, ciò potrebbe comportare una riduzione del tempo di contatto del satellite con l'antenna, dovuto al fatto che la navicella spaziale opera al di fuori della maschera del sito. transmit/receive Pertanto, ti consigliamo di annullare e riprogrammare i tuoi contatti futuri dopo aver caricato una nuova effemeride che differisce notevolmente dalle precedenti.

Con l'DescribeContact API, puoi determinare la parte dei tuoi contatti futuri che è inutilizzabile a causa del veicolo spaziale che opera al di fuori della maschera del transmit/receive sito confrontando il contatto `startTime` programmato `endTime` con quello restituito`visibilityStartTime`. `visibilityEndTime` Se scegli di annullare e riprogrammare i tuoi contatti futuri, l'intervallo di tempo del contatto non deve superare l'intervallo di tempo di visibilità di più di 30 secondi. I contatti annullati possono comportare costi se annullati troppo vicino all'ora del contatto. Per ulteriori informazioni sui contatti annullati, vedere: Ground Station FAQs.

Per le effemeridi di elevazione azimutale, i contatti programmati utilizzeranno le effemeridi specifiche selezionate al momento della prenotazione del contatto. Se è necessario aggiornare i dati di elevazione azimutale per un contatto pianificato, è possibile annullare e riprogrammare il contatto con una nuova effemeride.

Ottieni le effemeridi attuali per un satellite

Le effemeridi attualmente utilizzate da AWS Ground Station un satellite specifico possono essere recuperate chiamando le azioni o. GetSatelliteListSatellites Entrambi questi metodi restituiranno i metadati per le effemeridi attualmente in uso. Questi metadati sulle effemeridi sono diversi per le effemeridi personalizzate caricate su e per le effemeridi predefinite. AWS Ground Station

> **Note**
>
> Le effemeridi di elevazione azimutale non sono associate ai satelliti e pertanto non vengono restituite da o. GetSatelliteListSatellites Per recuperare informazioni sulle effemeridi di elevazione azimutale, usa l'DescribeEphemerisAPI con l'ID specifico delle effemeridi o usala per visualizzare tutte le effemeridi disponibili per il tuo account. ListEphemerides

Le `epoch` effemeridi predefinite includeranno solo i campi e. `source` `epoch`Questa è l'epoca del set di elementi a due linee estratto da Space-Track e attualmente viene utilizzato per calcolare la traiettoria del satellite.

Un'effemeride personalizzata avrà un `source` valore di e includerà un identificatore univoco nel campo. `CUSTOMER_PROVIDED` `ephemerisId` Questo identificatore univoco può essere utilizzato per ricercare le effemeridi tramite l'azione. DescribeEphemeris Verrà restituito un `name` campo opzionale se alle effemeridi è stato assegnato un nome durante il caricamento tramite l'azione. AWS Ground Station CreateEphemeris

È importante notare che le effemeridi vengono aggiornate dinamicamente, AWS Ground Station quindi i dati restituiti sono solo un'istantanea delle effemeridi utilizzate al momento della chiamata all'API.

Esempio di restituzione di un satellite che utilizza un'effemeride predefinita GetSatellite

```
{
    "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
    }
}
```

Esempio GetSatellitedi un satellite che utilizza un'effemeride personalizzata

```
{
      "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"
        }
    }
```

Elenco delle effemeridi di elevazione azimutale

Poiché le effemeridi di elevazione azimutale non sono associate ai satelliti, è necessario utilizzare different per scoprire e recuperare informazioni su di esse: APIs

1. Utilizzalo ListEphemeridesper elencare tutte le effemeridi presenti nel tuo account, incluse le effemeridi di elevazione dell'azimut. Puoi filtrare per stato e tipo di effemeridi.
2. Utilizzalo DescribeEphemeriscon un ID di effemeride specifico per ottenere informazioni dettagliate su un'effemeride di elevazione dell'azimut.
3. Utilizzalo DescribeContactcon un ID di contatto specifico per ottenere informazioni dettagliate su un'effemeride utilizzata per il contatto.

Esempio di ListEphemeridesrisposta che include un'effemeride di elevazione dell'azimut:

```
{
    "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**
>
> Nella ListEphemeridesrisposta, le effemeridi di elevazione dell'azimut avranno un campo anziché un `groundStation` campo, il che le renderà facili da identificare. `satelliteId`

Ripristina i dati predefiniti sulle effemeridi

Quando carichi dati sulle effemeridi personalizzati, questi sostituiranno gli effemeridi predefiniti utilizzati per quel particolare satellite. AWS Ground Station AWS Ground Station non utilizza nuovamente le effemeridi predefinite finché non sono disponibili effemeridi attualmente abilitate e non scadute fornite dal cliente. AWS Ground Station inoltre non elenca i contatti che hanno superato la data di scadenza delle effemeridi attualmente fornite dal cliente, anche se è disponibile un'effemeridi predefinita dopo tale data di scadenza.

> **Note**
>
> Le effemeridi di elevazione azimutale non hanno valori predefiniti e non sostituiscono le effemeridi satellitari. Vengono selezionati in modo esplicito quando si prenota un contatto utilizzando il parametro. `trackingOverrides` Se non desideri più utilizzare le effemeridi di elevazione azimutali, è sufficiente prenotare i contatti senza specificare le interruzioni di tracciamento e il sistema utilizzerà invece le effemeridi satellitari attive.

Ripristino delle effemeridi TLE e OEM

Per ripristinare le effemeridi Space-Track predefinite per un satellite, dovrai effettuare una delle seguenti operazioni:

- Eliminare (utilizzare DeleteEphemeris) o disabilitare (utilizzare) tutte le effemeridi abilitate fornite dal cliente. UpdateEphemeris È possibile elencare le effemeridi fornite dal cliente per un satellite utilizzando. ListEphemerides
- Attendi la scadenza di tutte le effemeridi esistenti fornite dal cliente.

Puoi confermare che vengono utilizzate le effemeridi predefinite chiamando GetSatellitee verificando che quella delle effemeridi correnti per il satellite sia. `source` `SPACE_TRACK` Per ulteriori informazioni sulle effemeridi predefinite, vedereDati predefiniti sulle effemeridi.

Gestione delle effemeridi di elevazione dell'azimut

Poiché le effemeridi di elevazione dell'azimut sono selezionate esplicitamente per ogni contatto e non sono associate ai satelliti, non esiste il concetto di «ripristino» di un valore predefinito. È invece possibile gestire le effemeridi di elevazione dell'azimut come segue:

- Per smettere di usare le effemeridi di elevazione azimutale: è sufficiente prenotare nuovi contatti senza specificare e specificare a. `trackingOverrides` `satelliteArn` Il contatto utilizzerà invece le effemeridi attive per il satellite specificato.
- Per rimuovere le effemeridi di elevazione dell'azimut non utilizzate: utilizzare per eliminare le effemeridi di elevazione dell'azimut che non sono DeleteEphemerispiù necessarie. Tieni presente che non puoi eliminare un'effemeride attualmente utilizzata da un contatto pianificato.

Per elencare tutte le effemeridi di elevazione azimutale presenti nel tuo account, usa. ListEphemerides Le effemeridi di elevazione azimutale possono essere identificate dal campo o dalla presenza di un `ephemerisType` campo anziché di un campo nella risposta. `groundStation` `satelliteId`

Lavora con i flussi di dati

AWS Ground Station utilizza una relazione tra nodo e perimetro per costruire flussi di dati che consentano l'elaborazione in streaming dei dati. Ogni nodo è rappresentato da una configurazione che descrive l'elaborazione prevista. Per illustrare questo concetto, considera un flusso di dati di to a. `antenna-downlink` `s3-recording` Il `antenna-downlink` nodo rappresenta la trasformazione da analogico a digitale dello spettro delle radiofrequenze secondo i parametri definiti nella configurazione. `s3-recording`Rappresenta un nodo di elaborazione che riceverà i dati in entrata e li memorizzerà nel bucket S3. Il flusso di dati risultante è una consegna asincrona di dati RF digitalizzati a un bucket S3 in base alle specifiche dell'utente.

All'interno del tuo profilo di missione, puoi creare molti flussi di dati per soddisfare le tue esigenze. Le seguenti sezioni descrivono come configurare le altre risorse AWS da utilizzare AWS Ground Station e offrono consigli per la creazione di flussi di dati. Per informazioni dettagliate sul comportamento di ciascun nodo, incluso se è considerato un nodo di origine o di destinazione, consulta. Usa AWS Ground Station configurazioni

Argomenti

- AWS Ground Station interfacce del piano dati
- Usa la distribuzione di dati tra regioni
- Configurare e configurare Amazon S3
- Configurare e configurare Amazon VPC
- Configura e configura Amazon EC2

AWS Ground Station interfacce del piano dati

La struttura dati risultante del flusso di dati scelto dipende dall'origine del flusso di dati. I dettagli di questi formati ti vengono forniti durante l'onboarding dei tuoi satelliti. Di seguito sono riepilogati i formati utilizzati per ogni tipo di flusso di dati.

- antenna - downlink
  - (Larghezza di banda da less-than-or-equal -a 40MHz) i dati vengono forniti come pacchetti in formato VITA-49 Signal Data/IP.
  - (Larghezza di banda superiore a 40) i dati vengono forniti come pacchetti di Classe 2. MHz AWS Ground Station

- antenna-downlink-demod-decode
  - I dati vengono forniti come pacchetti in formato data/IP. Demodulated/Decoded
- antenna-uplink
  - I dati devono essere consegnati come pacchetti in formato VITA-49 Signal Data/IP.
- antenna-uplink-echo
  - I dati vengono forniti come pacchetti VITA-49 Signal Data/IP Format.

Usa la distribuzione di dati tra regioni

La AWS Ground Station funzionalità di trasmissione dati tra regioni offre la flessibilità necessaria per inviare i dati da un'antenna a qualsiasi AWS regione AWS Ground Station supportata. Ciò significa che puoi mantenere la tua infrastruttura in un'unica regione AWS e pianificare i contatti in qualsiasi regione in AWS Ground Station Sedi cui sei registrato.

Quando riceverai i tuoi dati di contatto in un bucket Amazon S3, AWS Ground Station gestirà tutti gli aspetti della consegna per te.

Per utilizzare la distribuzione di dati tra regioni a un' EC2 istanza Amazon (utilizzando l' AWS Ground Station agente o un endpoint dataflow), l'endpoint dataflow-endpoint deve essere creato nella regione AWS corrente e specificare la stessa regione. dataflow-endpoint-config AWS Ground Station gestirà la distribuzione dei dati tra le regioni per te.

Configurare e configurare Amazon S3

Puoi utilizzare un bucket Amazon S3 per ricevere i segnali di downlink. AWS Ground Station Per creare la destinazione s3-recording-config, devi essere in grado di specificare un bucket Amazon S3 e un ruolo IAM che autorizzi a scrivere file nel bucket. AWS Ground Station

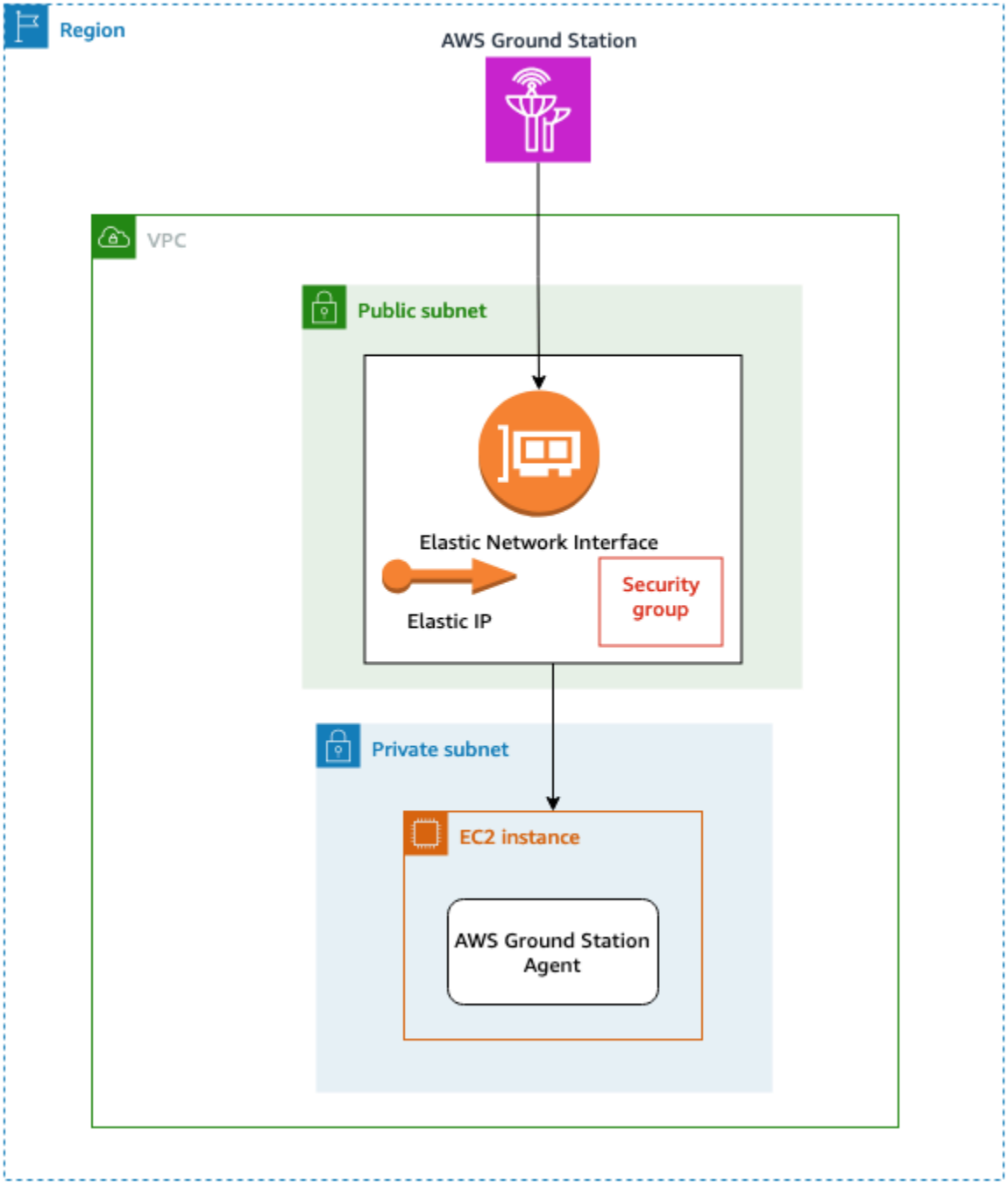
Consulta Config di registrazione Amazon S3 le restrizioni sul bucket Amazon S3, sul ruolo IAM o AWS Ground Station sulla creazione di configurazioni.

Configurare e configurare Amazon VPC

Una guida completa per configurare un VPC non rientra nell'ambito di questa guida. Per una comprensione approfondita, consulta la Amazon VPC User Guide.

In questa sezione, viene descritto come Amazon EC2 e l'endpoint dataflow possono esistere all'interno di un VPC. AWS Ground Station non supporta più punti di consegna per un determinato flusso di dati: si prevede che ogni flusso di dati termini verso un singolo ricevitore. EC2 Poiché prevediamo un singolo EC2 ricevitore, la configurazione non è ridondante Multi-AZ. Per esempi completi di utilizzo del tuo VPC, consulta. Esempi di configurazioni del profilo di missione

Configurazione VPC con agente AWS Ground Station



I dati satellitari vengono forniti a un'istanza AWS Ground Station dell'agente che si trova in prossimità dell'antenna. L' AWS Ground Station agente eseguirà lo striping e quindi crittograferà i dati utilizzando la AWS KMS chiave fornita dall'utente. Ogni striscia viene inviata al tuo Amazon EC2 Elastic IP (EIP) dall'antenna sorgente attraverso la dorsale della rete AWS. I dati arrivano alla tua EC2 istanza tramite l'Amazon EC2 Elastic Network Interface (ENI) allegata. Una volta sull' EC2istanza, l' AWS Ground Station agente installato decripterà i dati ed eseguirà la correzione degli errori di inoltro (FEC) per recuperare i dati persi, quindi li inoltrerà all'IP e alla porta specificati nella configurazione.

L'elenco seguente riporta considerazioni di configurazione uniche durante la configurazione del VPC AWS Ground Station per la consegna degli agenti.

Gruppo di sicurezza: si consiglia di configurare un gruppo di sicurezza dedicato solo AWS Ground Station al traffico. Questo gruppo di sicurezza dovrebbe consentire il traffico in ingresso UDP sullo stesso intervallo di porte specificato nel Dataflow Endpoint Group. AWS Ground Station mantiene un elenco di prefissi gestito da AWS per limitare le autorizzazioni ai soli indirizzi IP. AWS Ground Station Consulta AWS Managed Prefix Lists per dettagli su come sostituirli PrefixListIdper le tue regioni di distribuzione.

Elastic Network Interface (ENI): dovrai associare il gruppo di sicurezza di cui sopra a questo ENI e inserirlo nella tua sottorete pubblica.

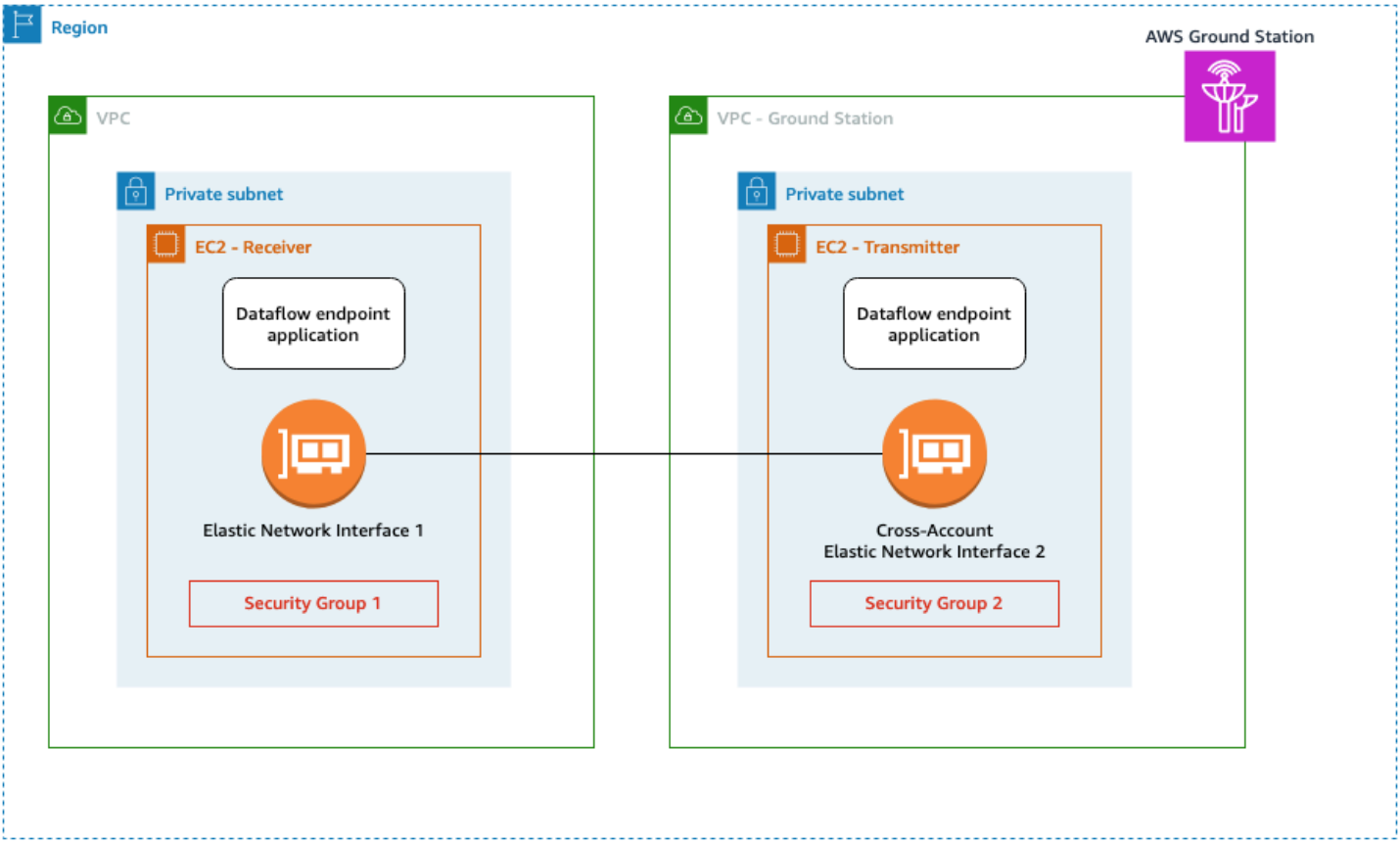
> **Note**
>
> La quota predefinita per il numero di gruppi di sicurezza collegati per ENI è 5. Si tratta di un limite regolabile fino a 16, vedi Amazon VPC Quotas.

Il CloudFormation modello seguente mostra come creare l'infrastruttura descritta in questa sezione.

```
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
```

Configurazione VPC con un endpoint dataflow



I dati satellitari vengono forniti a un'istanza dell'applicazione dataflow endpoint in prossimità dell'antenna. I dati vengono quindi inviati tramite Amazon EC2 Elastic Network Interface (ENI) tra account diversi da un VPC di proprietà di. AWS Ground Station I dati arrivano quindi alla tua EC2 istanza tramite l'ENI collegato alla tua EC2 istanza Amazon. L'applicazione dataflow endpoint installata li inoltrerà quindi all'IP e alla porta specificati nella configurazione. Per le connessioni uplink si verifica l'inverso di questo flusso.

L'elenco seguente riporta considerazioni di configurazione uniche quando si configura il VPC per la consegna degli endpoint con flusso di dati.

> **Note**
>
> La quota predefinita per il numero di gruppi di sicurezza collegati per ENI è 5. Si tratta di un limite regolabile fino a 16, vedi Amazon VPC Quotas.

Ruolo IAM: il ruolo IAM fa parte del Dataflow Endpoint e non è mostrato nel diagramma. Il ruolo IAM utilizzato per creare e collegare l'ENI tra account all' EC2istanza AWS Ground Station Amazon.

Gruppo di sicurezza 1: questo gruppo di sicurezza è collegato all'ENI che verrà associato all' EC2 istanza Amazon nel tuo account. Deve consentire il traffico UDP proveniente dal Security Group 2 sulle porte specificate nel tuo dataflow-endpoint-group.

Elastic Network Interface (ENI) 1 - Dovrai associare il Security Group 1 a questo ENI e inserirlo in una sottorete.

Subnet: dovrai assicurarti che ci sia almeno un indirizzo IP disponibile per flusso di dati per l' EC2 istanza Amazon nel tuo account. Per maggiori dettagli sul dimensionamento delle sottoreti, consulta Subnet CIDR blocks

Gruppo di sicurezza 2: questo gruppo di sicurezza è referenziato nel Dataflow Endpoint. Questo gruppo di sicurezza sarà collegato all'ENI che AWS Ground Station utilizzerà per inserire i dati nell'account dell'utente.

Regione: per ulteriori informazioni sulle regioni supportate per le connessioni interregionali, consultaUsa la distribuzione di dati tra regioni.

Il CloudFormation modello seguente mostra come creare l'infrastruttura descritta in questa sezione.

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

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

InstanceSecurityGroup:
```

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

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

Configura e configura Amazon EC2

La configurazione corretta dell' EC2 istanza Amazon è necessaria per la consegna Signal/IP data or VITA-49 Extension data/IP sincrona di VITA-49 tramite l' AWS Ground Station agente o un endpoint di flusso di dati. A seconda delle esigenze specifiche, è possibile eseguire il processore Front End (FE) o Software Defined Radio (SDR) direttamente sulla stessa istanza, oppure potrebbe essere necessario utilizzare istanze aggiuntive. EC2 La selezione e l'installazione del vostro FE o SDR non rientrano nell'ambito di questa guida per l'utente. Per ulteriori informazioni sui formati di dati specifici, vedereAWS Ground Station interfacce del piano dati.

Per informazioni sui nostri termini di servizio, consulta i Termini AWS di servizio.

Software comune fornito

AWS Ground Station fornisce un software comune per semplificare la configurazione dell' EC2 istanza Amazon.

AWS Ground Station Agente

L' AWS Ground Station agente riceve dati di downlink Digital Intermediate Frequency (DigiF) ed esce dai dati decrittografati che consentono quanto segue:

- Capacità di downlink DigiF da 40 MHz a 400 MHz di larghezza di banda.
- Distribuzione di dati DigiF ad alta velocità e basso jitter a qualsiasi IP pubblico AWS (Elastic IP) sulla AWS rete.
- Distribuzione affidabile dei dati tramite Forward Error Correction (FEC).
- Distribuzione sicura dei dati utilizzando una AWS KMS chiave di crittografia gestita dal cliente.

Per ulteriori informazioni, consulta la Guida per l'utente dell'AWS Ground Station agente.

Applicazione per endpoint Dataflow

Un'applicazione di rete utilizzata da AWS Ground Station per inviare e ricevere dati tra le posizioni delle AWS Ground Station antenne e le EC2 istanze Amazon. Può essere utilizzato per l'uplink e il downlink dei dati.

Software Defined Radio (SDR)

Una radio definita dal software (SDR) che può essere utilizzata per modulare/demodulare il segnale utilizzato per comunicare con il satellite.

AWS Ground Station Immagini di macchine Amazon (AMIs)

Per ridurre i tempi di compilazione e configurazione di queste installazioni, sono disponibili AWS Ground Station anche offerte AMIs preconfigurate. L'applicazione AMIs di rete per endpoint dataflow e una radio definita dal software (SDR) vengono rese disponibili per l'account dopo il completamento dell'onboarding. Possono essere trovati nella EC2 console Amazon cercando groundstation in Amazon Machine Images private (AMIs). I AMIs with AWS Ground Station Agent sono pubblici e possono essere trovati nella EC2 console Amazon cercando groundstation nelle Amazon Machine Images pubbliche (AMIs).

Lavora con la telemetria

AWS Ground Station la telemetria fornisce metriche quasi in tempo reale provenienti dalle AWS Ground Station antenne durante i contatti satellitari. È possibile utilizzare i dati di telemetria per monitorare le prestazioni dei contatti, rilevare anomalie e prendere decisioni informate sulle comunicazioni satellitari.

Come funziona la telemetria

Per utilizzare la telemetria, si configura un comando TelemetrySinkConfigche specifica dove devono essere forniti i dati di telemetria. AWS Ground Station Quindi aggiungi questa configurazione al tuo profilo di missione utilizzando il campo. `telemetrySinkConfigArn` Durante i contatti che utilizzano un profilo di missione abilitato alla telemetria, AWS Ground Station trasmette i dati di telemetria al tuo account.

Il processo di consegna della telemetria funziona come segue:

1. Crei uno stream Kinesis Data Streams AWS nel tuo account per ricevere dati di telemetria. Lo stream deve essere creato nello stesso account e nella stessa regione da cui pianifichi i contatti.
2. Crei un ruolo IAM che concede AWS Ground Station l'autorizzazione a scrivere dati nel tuo stream.
3. Ne crei un TelemetrySinkConfig che fa riferimento al tuo stream e al tuo ruolo IAM.
4. Lo aggiungi TelemetrySinkConfig al tuo profilo di missione.
5. Elenchi e prenoti i contatti utilizzando il nuovo profilo di missione abilitato alla telemetria.
6. Durante i contatti che utilizzano questo profilo di missione, AWS Ground Station trasmette i dati di telemetria allo stream Kinesis Data Streams quasi in tempo reale.
7. Consumi ed elabori i dati di telemetria del tuo stream utilizzando servizi o le tue applicazioni. AWS

Tipi di telemetria disponibili

AWS Ground Station fornisce i seguenti tipi di telemetria durante i contatti:

> **Note**
>
> AWS Ground Station sta lavorando all'espansione del numero di tipi di telemetria supportati

Puntamento della telemetria

Fornisce informazioni sulla direzione di puntamento dell'antenna durante i contatti satellitari. Questo tipo di telemetria viene sempre inviato durante un contatto e include gli angoli di azimut e di elevazione effettivi e comandati. Per ulteriori informazioni, consulta Telemetria di puntamento.

Telemetria di tracciamento

Fornisce informazioni sullo stato di tracciamento dell'antenna e sugli errori di tracciamento. Questo tipo di telemetria viene inviato quando il tracciamento automatico è abilitato nella configurazione di tracciamento. Per ulteriori informazioni, consulta Monitoraggio della telemetria.

Disponibilità regionale

La telemetria è disponibile in tutte le regioni in cui opera. AWS AWS Ground Station Durante l'esecuzione del contatto, la telemetria verrà trasmessa dall' AWS Ground Station antenna alla regione da cui è stato pianificato il contatto, fornendo supporto interregionale.

Per un elenco completo delle AWS Ground Station regioni e delle sedi delle stazioni terrestri, consulta. AWS Ground Station Sedi

Argomenti

- Configurare la telemetria
- Comprendi i dati di telemetria

Configurare la telemetria

Segui questi passaggi per configurare la telemetria per i tuoi contatti. AWS Ground Station Dopo aver completato questa configurazione, i dati di telemetria verranno inviati allo stream Kinesis Data Streams durante i contatti che utilizzano un profilo di missione abilitato alla telemetria. Per una comprensione approfondita di Kinesis Data Streams, consulta la Guida per l'utente di Kinesis Data Streams.

Fase 1: Creare le risorse indispensabili AWS

Il seguente CloudFormation frammento dimostra come creare le risorse AWS prerequisite per la distribuzione della telemetria. Questo frammento crea un flusso Kinesis Data Streams e un ruolo IAM che AWS Ground Station concede l'autorizzazione a scrivere dati di telemetria nello stream.

```
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
```

L'elenco seguente riporta considerazioni di configurazione uniche durante la configurazione della consegna della telemetria per. AWS Ground Station

Flusso Kinesis Data Streams: lo stream utilizza la modalità di capacità su richiesta, che si ridimensiona automaticamente in base alla velocità effettiva. Questa opzione è consigliata per la maggior parte dei casi d'uso. Lo stream è configurato per conservare i dati per 24 ore. Per impostazione predefinita, lo stream utilizza la crittografia AWS gestita. Per utilizzare la crittografia gestita dal cliente con AWS Key Management Service, aggiungi la `StreamEncryption` proprietà e aggiorna la policy del ruolo IAM per includere `kms:GenerateDataKey` l'autorizzazione. Per ulteriori informazioni, consulta la sezione Protezione dei dati in Amazon Kinesis Data Streams.

Ruolo IAM: il ruolo IAM consente al responsabile del `groundstation.amazonaws.com` servizio di assumere il ruolo e scrivere dati di telemetria nel flusso Kinesis Data Streams. La policy relativa al ruolo concede autorizzazioni e azioni sullo `kinesis:DescribeStream` stream. `kinesis:PutRecord` `kinesis:PutRecords` Consulta Config del sink di telemetria le linee guida sulla configurazione della politica di fiducia e della politica dei ruoli.

Configurazione aggiuntiva: aggiungi `iam:PassRole` le autorizzazioni all'utente o al ruolo IAM che utilizzi per le chiamate AWS Ground Station API. Ciò consente di passare il ruolo di telemetria a AWS Ground Station quando si crea un. TelemetrySinkConfig

Politica di esempio PassRole

Per ulteriori informazioni su come aggiornare o allegare una policy relativa ai ruoli, consulta Managing IAM policy nella IAM User Guide. Per ulteriori informazioni sull'`iam:PassRole`autorizzazione, consulta Concedere a un utente le autorizzazioni per passare un ruolo a un servizio AWS

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

Fase 2: Creare un TelemetrySinkConfig

Crea uno TelemetrySinkConfigche definisca come AWS Ground Station verranno forniti i dati di telemetria al tuo flusso Kinesis Data Streams. Usa lo stream ARN e il role ARN dagli output CloudFormation dello stack nel passaggio 1.

> **Note**
>
> Quando crei un TelemetrySinkConfig, AWS Ground Station verificherà l'accesso al tuo stream Kinesis Data Streams fornendo un record di test vuoto con una chiave di partizione di. `test`

Per ulteriori informazioni sulla creazione di un TelemetrySinkConfig, consulta. Config del sink di telemetria

Passaggio 3: aggiungi la telemetria al tuo profilo di missione

Crea un profilo di missione. Per ulteriori informazioni sulla creazione di profili di missione, consultaUsa i profili di AWS Ground Station missione. Aggiungilo `telemetrySinkConfigArn` al tuo profilo di missione per abilitare la consegna della telemetria durante i contatti. Usa l'ARN del file TelemetrySinkConfigcreato nel passaggio 2.

Fase 4: Pianifica un contatto

Pianifica un contatto utilizzando il tuo profilo di missione abilitato alla telemetria. Durante il contatto, AWS Ground Station trasmetterà i dati di telemetria allo stream Kinesis Data Streams.

Cosa aspettarsi durante i contatti

- Avvio della telemetria: lo streaming dei dati inizia all'avvio del contatto.
- Consegna quasi in tempo reale: la telemetria arriva nel flusso Kinesis Data Streams quasi in tempo reale.
- Durata del contatto: i dati continuano per l'intero contatto.
- Arresto automatico: la telemetria interrompe lo streaming al termine del contatto.

Monitoraggio della consegna

Puoi monitorare la consegna della telemetria utilizzando:

- Metriche del flusso di Kinesis Data Streams: archivia i record in entrata. CloudWatch Per ulteriori informazioni, consulta Monitoraggio di Amazon Kinesis Data Streams.
- Log delle applicazioni: verifica l'elaborazione dei dati nelle applicazioni che utilizzano lo stream.

- Kinesis Data Viewer: utilizza la console di streaming Kinesis Data Streams per visualizzare i record di esempio del tuo stream.

Fasi successive

Dopo aver completato la configurazione, puoi:

- Scopri il formato dei dati di telemetria e i tipi di telemetria disponibili. Per informazioni, consulta Comprendi i dati di telemetria.
- Crea applicazioni per elaborare i dati di telemetria dal tuo flusso Kinesis Data Streams. Per ulteriori informazioni, consulta Building Consumers for Amazon Kinesis Data Streams.
- Crea dashboard e avvisi utilizzando CloudWatch altri servizi. AWS
- Se riscontri problemi, consulta le linee guida per la risoluzione dei problemi. Per informazioni, consulta Risolvere i problemi di telemetria.

Comprendi i dati di telemetria

I dati di telemetria vengono forniti come record JSON con codifica Base64 al flusso Kinesis Data Streams. Ogni record contiene informazioni raccolte durante il contatto satellitare, inclusi i metadati sul contatto e le misurazioni telemetriche campionate.

Panoramica del formato dei dati

Ogni record di telemetria contiene i seguenti componenti:

Tipo e versione di telemetria

: Identifica il tipo specifico di dati di telemetria e la relativa versione dello schema. Ciò consente di analizzare i diversi tipi di telemetria in modo appropriato. Per ulteriori informazioni sul controllo delle versioni dello schema, vedere. Versionamento ed evoluzione dello schema

ID dell'ambito

: Un identificatore univoco per l'ambito della telemetria. Ciò consente di correlare i dati di telemetria con contatti specifici.

Metadati

: Informazioni contestuali sulla telemetria.

Dati

Le misurazioni telemetriche campionate specifiche per il tipo di telemetria.

Chiave di partizione

I record di telemetria vengono inviati al flusso Kinesis Data Streams con una chiave di partizione nel formato:

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

Questa chiave di partizione assicura che tutta la telemetria di un determinato tipo per un singolo contatto venga inviata allo stesso shard all'interno del flusso Kinesis Data Streams, permettendo di ordinare al meglio il flusso di telemetria di quel contatto.

Telemetria di puntamento

La telemetria di puntamento fornisce informazioni sulla direzione di puntamento dell'antenna durante i contatti satellitari. Questo tipo di telemetria viene sempre inviato durante un contatto.

Campi dati

Timestamp di esempio

Ora in cui i dati di telemetria sono stati campionati, in formato ISO-8601 in UTC con precisione al millisecondo.

azimut

Angolo di azimut effettivo dell'antenna in gradi.

elevazione

Angolo di elevazione effettivo dell'antenna in gradi.

Azimut comandato

Angolo azimutale comandato in gradi. Questo è l'angolo azimutale target che l'antenna sta cercando di raggiungere.

Elevazione comandata

Angolo di elevazione comandato in gradi. Questo è l'angolo di elevazione target che l'antenna sta cercando di raggiungere.

> **Note**
>
> La posizione effettiva dell'antenna può differire dalla posizione comandata a causa di limitazioni fisiche o ritardi meccanici durante il contatto.

Campi di metadati

Stazione terrestre

Nome della stazione di terra (ad esempio, «Ohio 1").

ID satellitare

Identificatore della risorsa satellitare in. AWS Ground Station

contactId

Identificatore del contatto.

Esempio 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
  }
}
```

Monitoraggio della telemetria

La telemetria di tracciamento fornisce informazioni sullo stato di tracciamento dell'antenna e sugli errori di tracciamento. Questo tipo di telemetria viene inviato quando il tracciamento automatico è abilitato nella configurazione di tracciamento e quando l'antenna utilizza attivamente l'autotrack.

> **Note**
>
> Se il `autotrack` parametro inserito TrackingConfig è impostato su, non verrà fornita alcuna telemetria di `REMOVED` tracciamento. Per ulteriori informazioni sul monitoraggio delle configurazioni, consulta. Config di monitoraggio

Campi dati

Timestamp di esempio

Ora in cui i dati di telemetria sono stati campionati, in formato ISO-8601 in UTC con precisione al millisecondo.

Stato del tracciamento

Stato di tracciamento attuale dell'antenna. I valori possibili sono `TRACKING`, `ACQUIRING` e `MASKED`.

trackingErrorAzimuth

Errore di tracciamento nell'asse azimutale, misurato in gradi.

trackingErrorElevation

Errore di tracciamento nell'asse di elevazione, misurato in gradi.

> **Note**
>
> I valori degli errori di tracciamento rappresentano le regolazioni della traccia del programma basata sulle effemeridi che AWS Ground Station si applica durante il tracciamento automatico per massimizzare la potenza del segnale.

Campi di metadati

La telemetria di tracciamento include gli stessi campi di metadati della telemetria di puntamento:, , e. `groundStation` `satelliteId` `contactId`

Esempio 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
  }
}
```

Lettura dei dati dal flusso Kinesis Data Streams

I dati di telemetria vengono forniti al flusso Kinesis Data Streams e possono essere utilizzati utilizzando modelli di consumo standard dei flussi. Quando leggi i dati del tuo stream, tieni a mente le seguenti considerazioni.

Decodifica Base64

I dati nello stream Kinesis Data Streams sono codificati in Base64. È necessario decodificare i dati prima di analizzarli come JSON. Per ulteriori informazioni, consulta Working with Amazon Kinesis Data Streams.

Utilizzo di Kinesis Data Viewer

Per un accesso rapido ai dati di telemetria, la console di streaming Kinesis Data Streams offre una funzionalità Data Viewer. Quando si utilizza questa funzionalità:

- La consegna della telemetria può avvenire su qualsiasi shard all'interno dello stream.
- La posizione iniziale predefinita viene letta dai record più recenti nello shard.

- Potrebbe essere necessario regolare lo shard selezionato e utilizzare la posizione iniziale «Al timestamp» per visualizzare i record ricevuti.

Utilizzo della libreria Kinesis Client

La Kinesis Client Library (KCL) gestisce molte delle complessità associate al consumo di dati dal flusso Kinesis Data Streams, tra cui la gestione degli shard, il checkpoint e il bilanciamento del carico. Consigliamo di utilizzare KCL per le applicazioni di consumo telemetrico di produzione.

Per ulteriori informazioni, consulta Sviluppo dei consumatori utilizzando la libreria client Kinesis.

Le migliori pratiche per il consumo

- Minimizza la latenza: utilizza Enhanced Fan-Out per leggere dal flusso Kinesis Data Streams con throughput dedicato e latenza inferiore rispetto al polling. Per ulteriori informazioni, consulta Developing Enhanced Fan-Out Consumers.
- Stream dedicato: utilizza un flusso Kinesis Data Streams dedicato AWS Ground Station per l'integrazione della telemetria. La condivisione di uno stream con altre applicazioni può causare la saturazione della velocità di scrittura e errori nell'erogazione della telemetria.
- Capacità su richiesta: implementa il tuo flusso Kinesis Data Streams in modalità di provisioning su richiesta per consentire il ridimensionamento automatico degli shard in base alla velocità effettiva.
- Monitora la velocità effettiva: monitora lo stream per verificare eventuali limitazioni utilizzando le metriche. CloudWatch Per ulteriori informazioni, consulta Monitoraggio di Amazon Kinesis Data Streams.

Versionamento ed evoluzione dello schema

Le versioni degli schemi di telemetria sono adattate per supportare l'evoluzione nel tempo. Il `telemetryVersion` campo in ogni record indica la versione dello schema.

Gestione delle modifiche allo schema

- In futuro potrebbero essere introdotti nuovi tipi di telemetria.
- I tipi di telemetria esistenti potrebbero ricevere nuove versioni con modifiche sostanziali.
- Le applicazioni devono tollerare tipi e versioni di telemetria sconosciuti.
- Analizza i `telemetryVersion` campi `telemetryTypeAndVersiontelemetryType`, e per determinare come elaborare ogni record.

Consigliamo di implementare una serializzazione del payload sensibile alla versione in grado di gestire più versioni dello schema in modo corretto, permettendo alle applicazioni di continuare a funzionare quando vengono introdotte nuove versioni.

Lavora con i contatti

Puoi inserire dati satellitari, identificare le posizioni delle antenne, comunicare e programmare l'ora dell'antenna per satelliti selezionati utilizzando la AWS Ground Station console o l' AWS SDK nella lingua che preferisci. AWS CLI Puoi rivedere, annullare e riprogrammare le prenotazioni dei contatti fino a 15 minuti prima dell'inizio del contatto*. Inoltre, puoi visualizzare i dettagli del tuo piano tariffario per i minuti riservati se utilizzi il modello tariffario dei minuti AWS Ground Station riservati.

AWS Ground Station supporta la consegna di dati tra regioni diverse. Le configurazioni endpoint del flusso di dati che fanno parte del profilo missione selezionato determinano a quale regione vengono consegnati i dati. Per ulteriori informazioni sull'utilizzo della distribuzione di dati tra regioni diverse, vedere. Usa la distribuzione di dati tra regioni

Per pianificare i contatti, è necessario configurare le risorse. Se non hai configurato le tue risorse, vediNozioni di base. Quando ReserveContactviene chiamato, AWS Ground Station scatta un'istantanea del profilo di missione e delle risorse di configurazione da utilizzare durante l'intero ciclo di vita del contatto. Le modifiche apportate a queste risorse tramite UpdateMissionProfilee non si UpdateConfig APIs rifletteranno nei contatti riservati prima degli aggiornamenti. Se è necessario applicare le modifiche alle risorse a un contatto già pianificato, è necessario innanzitutto annullare l'utilizzo CancelContactdel contatto e quindi riprogrammarlo. ReserveContact

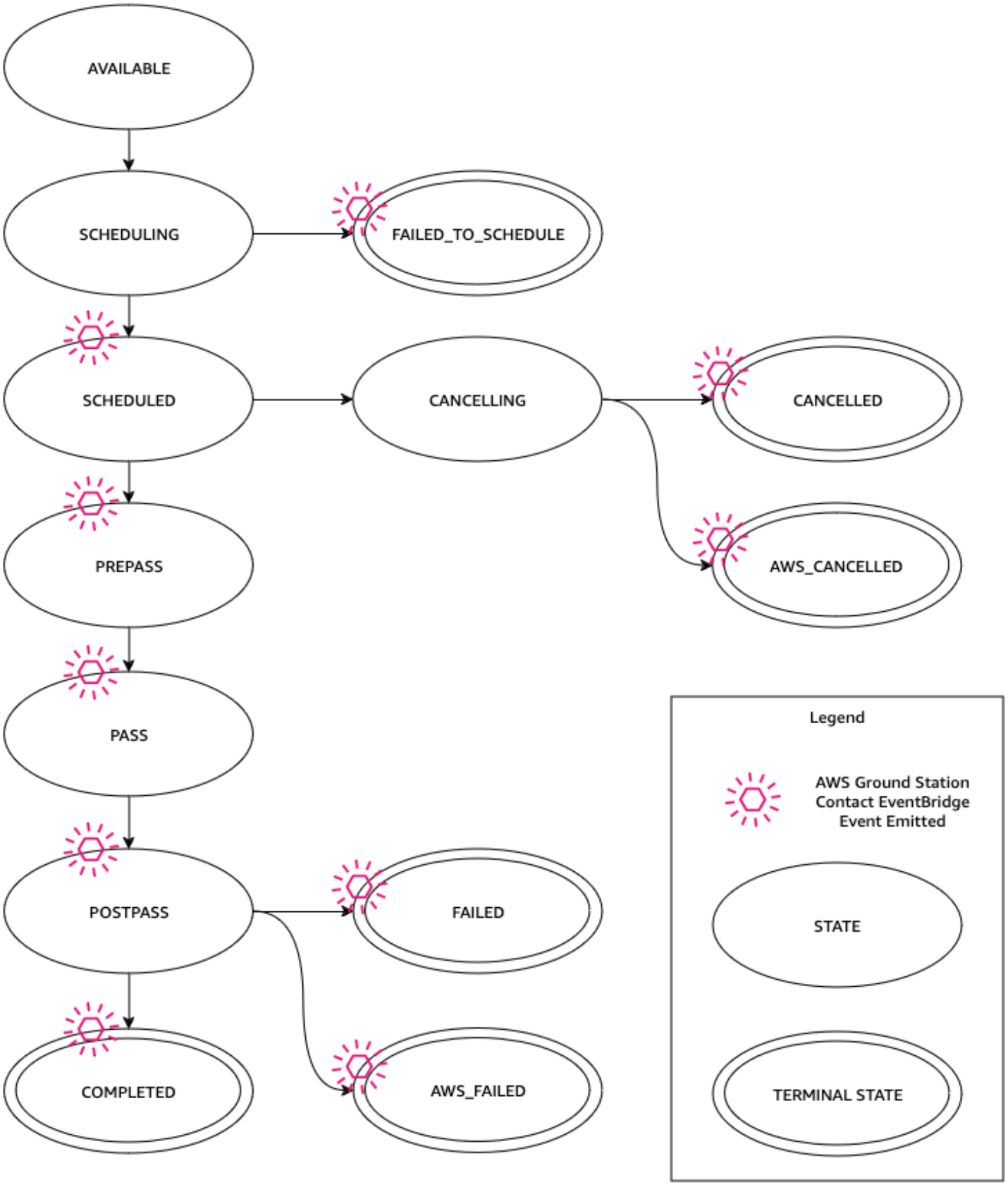
* I contatti annullati possono comportare costi se annullati troppo vicino al momento del contatto. Per ulteriori informazioni sui contatti annullati, vedere: Ground Station FAQs.

Argomenti

- Comprendi il ciclo di vita dei contatti
- Comprendi la fatturazione dei contatti

Comprendi il ciclo di vita dei contatti

Comprendere il ciclo di vita dei contatti può aiutarti ad automatizzare e risolvere vari problemi durante l'utilizzo. AWS Ground Station Il diagramma seguente mostra il ciclo di vita dei AWS Ground Station contatti e gli eventi Event Bridge emessi durante il ciclo di vita. È importante notare che gli stati COMPLETED, FAILED, FAILED_TO_SCHEDULE, CANCELLED e sono terminali. AWS_CANCELLED AWS_FAILED I contatti non passeranno da uno stato terminale. Vedi AWS Ground Station stati dei contatti i dettagli su cosa indica ogni stato e se è possibile interromperlo o annullarlo. CancelContact


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

AWS Ground Station stati dei contatti

Lo stato di un AWS Ground Station contatto fornisce informazioni su ciò che accade a quel contatto in un determinato momento.

Stati dei contatti

La tabella seguente descrive gli stati che un contatto può avere:

Status	Description	Terminale	Annullabile	Arrestabile
DISPONIBILE	Il contatto è disponibile per essere prenotato.	No	N/D	N/D
PROGRAMMARE	Il contatto è in fase di pianificazione.	No	Sì	No
SCHEDULED	Il contatto è stato pianificato con successo.	No	Sì	No
FAILED_TO_SCHEDULE	Il contatto non è riuscito a pianificare.	Sì	No	No
PREPASS	Il contatto inizierà presto e le risorse sono in fase di preparazione.	No	Sì	No
PASSARE	Il contatto è attualmente in esecuzione e con il satellite è in corso la comunicazione.	No	No	Sì
POSTICIPARE	La comunicazione è stata completata e le risorse utilizzate vengono ripulite.	No	No	No
COMPLETED	Il contatto è stato completato senza errori.	Sì	No	No

Status	Description	Terminale	Annullabile	Arrestabile
NON RIUSCITO	Il contatto non è riuscito a causa di un problema con la configurazione delle risorse.	Sì	No	No
AWS_FAILED	Il contatto non è riuscito a causa di un problema nel AWS Ground Station servizio.	Sì	No	No
IN CORSO DI ANNULLAMENTO	Il contatto è in fase di annullamento.	No	No	No
AWS_CANCELLED	Il contatto è stato annullato dal AWS Ground Station servizio. La manutenzione dell'antenna o del sito e la deriva delle effemeridi sono esempi di quando ciò potrebbe accadere.	Sì	No	No
ANNULLATO	Il contatto è stato annullato da te.	Sì	No	No

> **Note**
>
> Per informazioni sulle implicazioni di fatturazione dei contatti annullati o interrotti, consulta. Comprendi la fatturazione dei contatti

Conservazione dei dati di contatto

AWS Ground Station conserva i dati di contatto per 1 anno dopo la ReserveContactrichiesta di prenotazione di un contatto. Dopo il periodo di 1 anno, i dati di contatto vengono eliminati.

Se è necessario conservare i dati di contatto per più di un anno, si consiglia di esportare i dati prima della scadenza del periodo di conservazione. Per ulteriori informazioni su come accedere ed esportare i dati di contatto, consulta:

- AWS Ground Station Documentazione di riferimento delle API
- AWS Ground Station Riferimento ai comandi CLI

Comprendi la fatturazione dei contatti

Con AWS Ground Station, paghi solo per il tempo di antenna che utilizzi. AWS Ground Station contatori di utilizzo dei contatti al minuto. Per ogni contatto, il servizio calcola la durata del contatto dall'ora di inizio a quella di fine e lo arrotonda al minuto più vicino. Questa durata misurata determina i costi per quel contatto.

La tua tariffa dipende da due fattori principali:

- Larghezza di banda: la quantità di larghezza di banda riservata al contatto (banda stretta o banda larga)
- Ubicazione della stazione di terra: le tariffe variano in base alla posizione della stazione di terra

Definizioni della larghezza di banda

AWS Ground Station classifica i contatti in due livelli di larghezza di banda in base alla larghezza di banda istantanea:

- Banda stretta: qualsiasi contatto in cui la larghezza di banda istantanea è inferiore o uguale a 40 MHz
- Banda larga: qualsiasi contatto in cui la larghezza di banda istantanea è superiore a 40 MHz

Modalità di pianificazione

AWS Ground Station offre due modalità di pianificazione:

- On-Demand: paga l'accesso all'antenna senza impegni a lungo termine
- Riservato: offre una tariffa scontata e una pianificazione migliorata rispetto a On-Demand, con un impegno mensile. La tariffa riservata ai minuti è disponibile per i clienti che si impegnano a utilizzare mensilmente per un determinato periodo di tempo.

Per informazioni specifiche sui prezzi del tuo account o per saperne di più sulla modalità di pianificazione riservata, contatta il tuo rappresentante AWS.

CancelContact

L'uso dell' CancelContactAPI varia in base allo stato del contatto al momento della chiamata:

- Prima dell'inizio del contatto: annulla completamente il contatto
- Dopo l'inizio del contatto e prima della fine del contatto: interrompe il contatto in corso

Quando annulli un contatto, la fatturazione dipende dalla modalità di pianificazione e dal momento dell'annullamento. Per ulteriori informazioni, contatta il tuo rappresentante AWS.

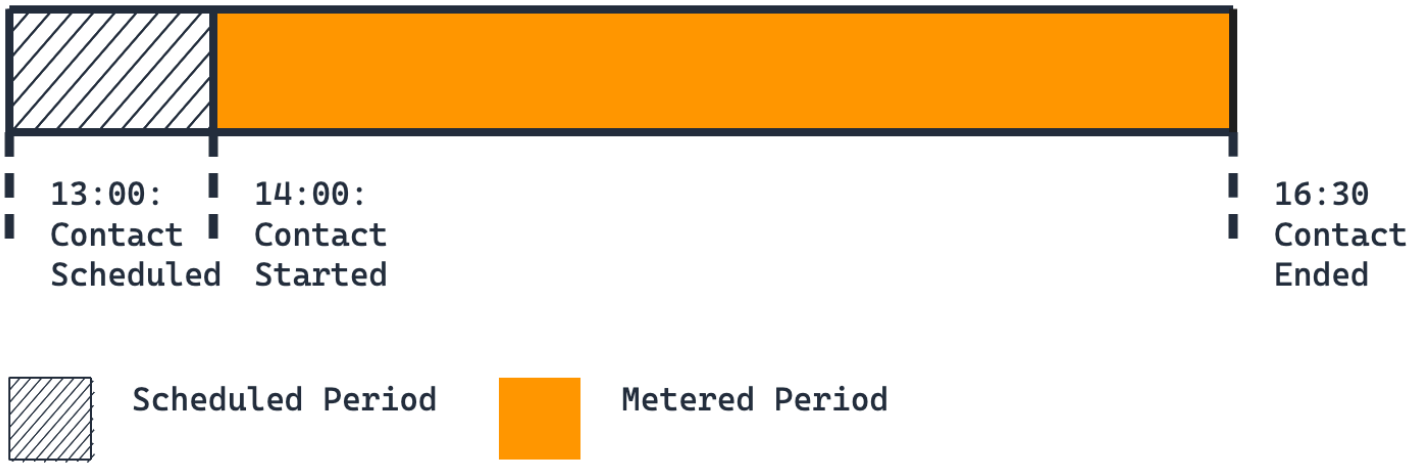
Quando interrompi un contatto, ti viene fatturata la parte del contatto che è stata eseguita e il tempo rimanente non coperto da contatti duplicati. Un contatto duplicato in questo contesto è stato:

- Pianificato sulla stessa stazione di terra del contatto interrotto originale
- Pianificato con lo stesso ID account AWS del contatto interrotto originale
- Riservato dopo l'emissione del comando per interrompere il contatto originale

Gli scenari seguenti mostrano come funziona in pratica questa misurazione.

Scenario 1: contatto singolo

Pianifica un contatto di 150 minuti su Ground Station Anytown 1 con inizio alle 14:00 e termine alle 16:30.



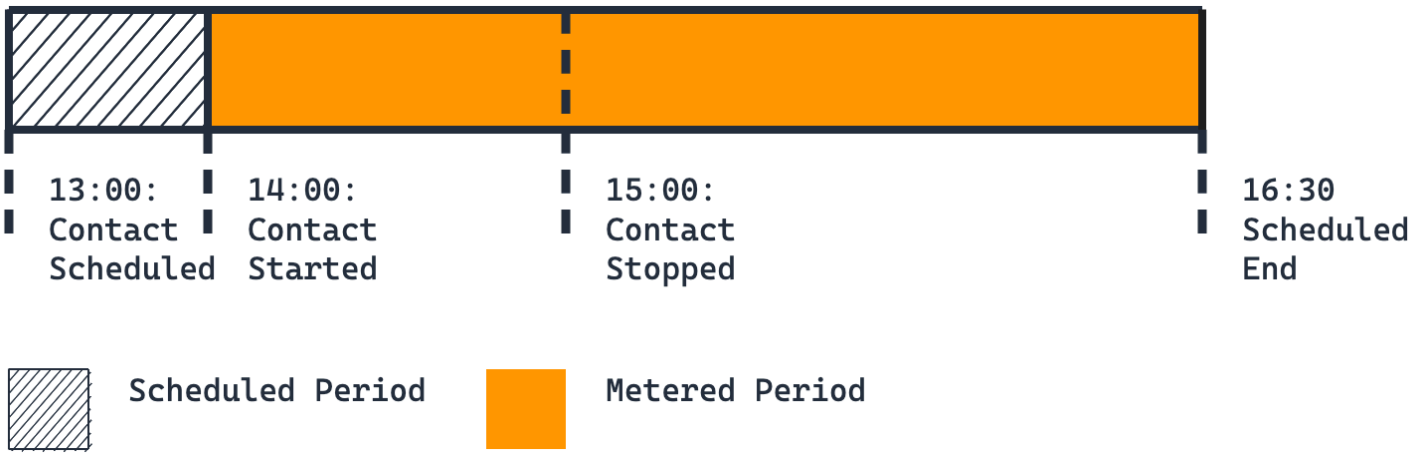
Suddivisione della fatturazione:

- Primo contatto: 150 minuti (durata completa)

Ti verranno fatturati 150 minuti. Questo è lo scenario di base in cui un contatto raggiunge il completamento pianificato senza interruzioni o annullamenti.

Scenario 2: singolo contatto interrotto

Pianifica un contatto di 150 minuti su Ground Station Anytown 1 con inizio alle 14:00 e termine alle 16:30. Alle 15:00, chiami l'API per interrompere il contatto. CancelContact



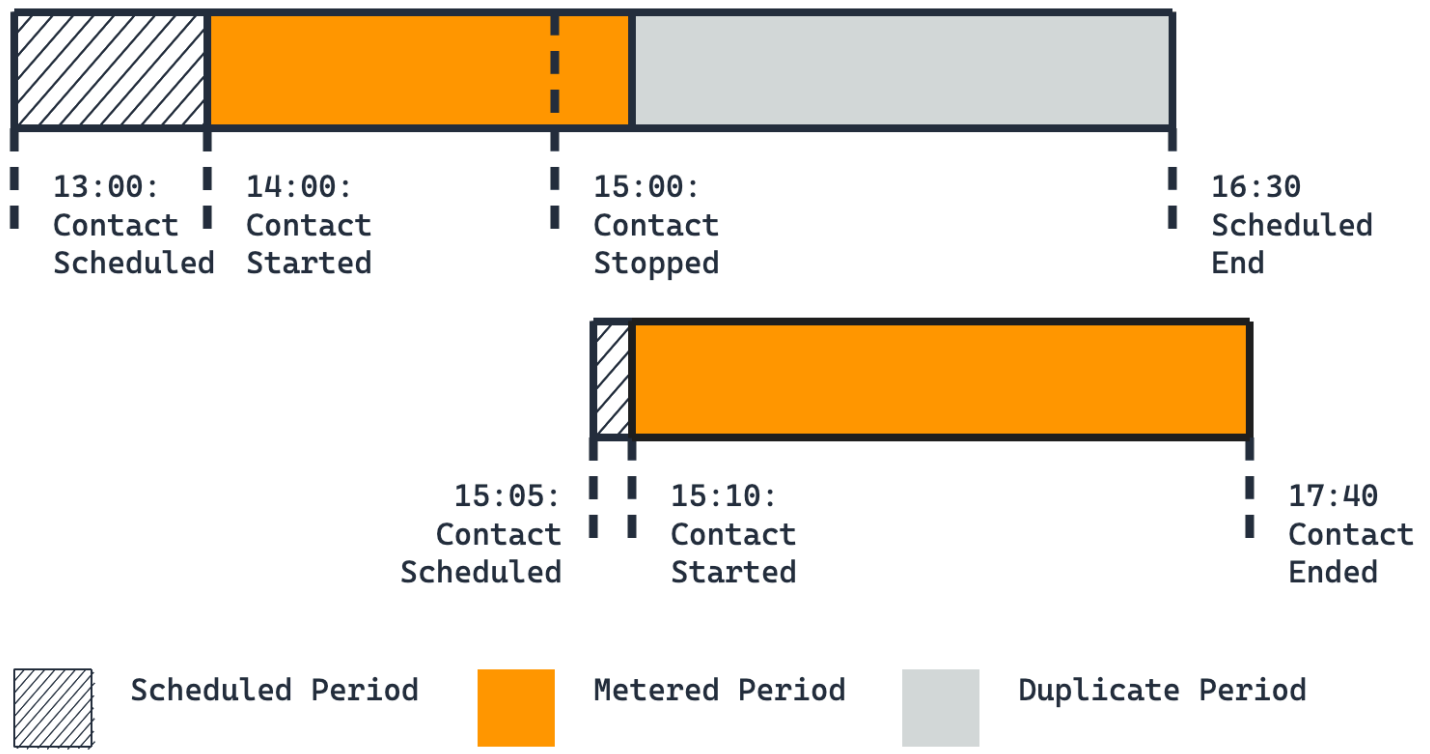
Suddivisione della fatturazione:

- Primo contatto: 150 minuti (durata originale completa)

Ti vengono addebitati i 150 minuti completi perché hai interrotto il contatto ma non hai pianificato contatti duplicati per coprire il tempo rimanente (15:00-16:30). Quando interrompi un contatto senza pianificare i duplicati, rimani responsabile per l'intera durata originariamente pianificata.

Scenario 3: Duplicato singolo

Pianifica un contatto di 150 minuti su Ground Station Anytown 1 con inizio alle 14:00 e termine alle 16:30. Alle 15:00, chiami l'API per interrompere il tuo primo contatto CancelContact . Dopo la chiamata CancelContact, pianifichi un altro contatto sulla stessa Ground Station a partire dalle 15:10 per 150 minuti.



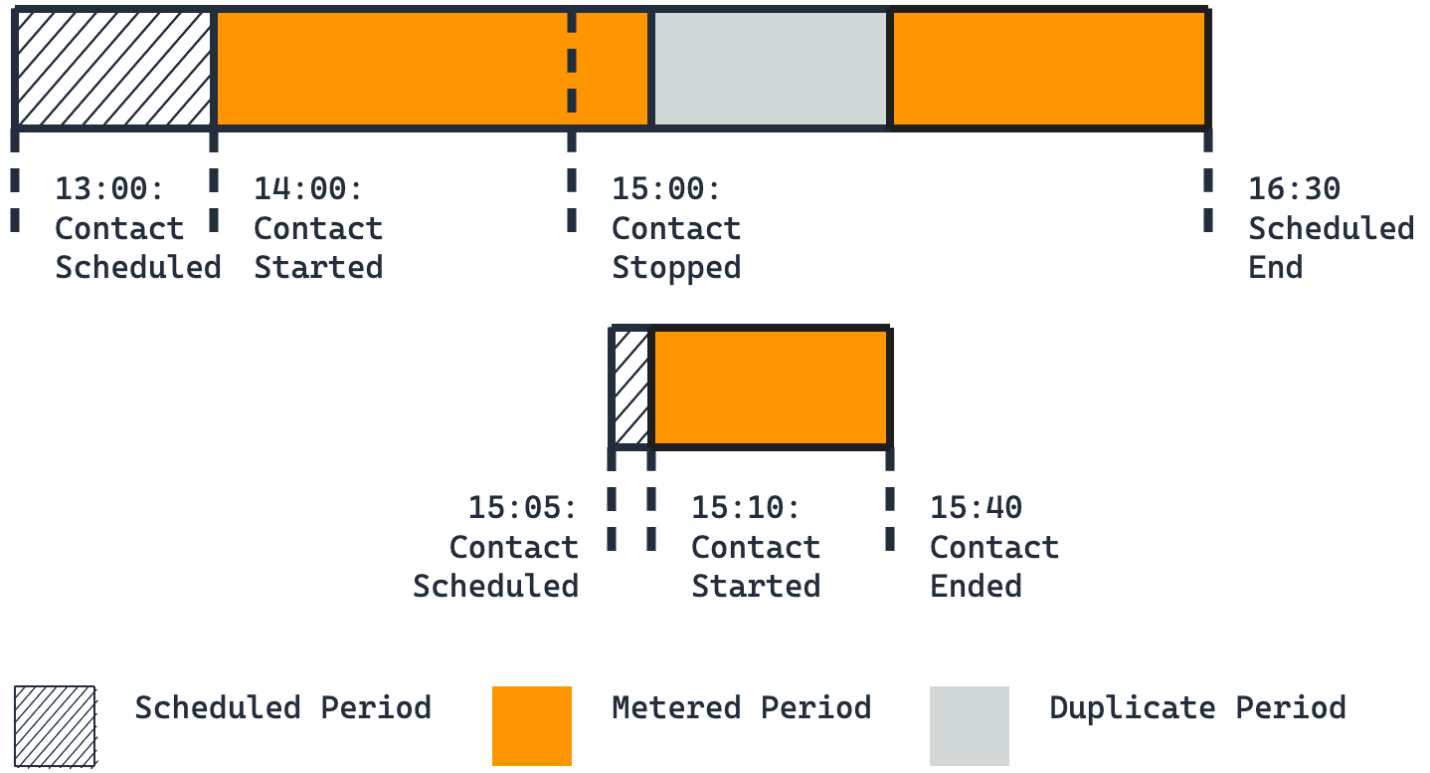
Suddivisione della fatturazione:

- Primo contatto: 70 minuti (60 minuti eseguiti più 10 minuti di inattività prima dell'inizio del secondo contatto)
- Secondo contatto: 150 minuti (durata completa)

Il secondo contatto è duplicato perché è stato pianificato dopo aver interrotto il primo contatto. Il duplicato copre il tempo rimanente dalle 15:10 alle 16:30, quindi ti verrà addebitato solo l'orario in cui è stato effettivamente eseguito il primo contatto più l'intervallo di 10 minuti tra l'interruzione e il riavvio.

Scenario 4: Duplicato breve

Pianifica un contatto di 150 minuti su Ground Station Anytown 1 con inizio alle 14:00 e termine alle 16:30. Alle 15:00, chiami l'API per interrompere il tuo primo contatto CancelContact . Dopo la chiamata CancelContact, pianifichi un contatto di 30 minuti sulla stessa Ground Station a partire dalle 15:10.



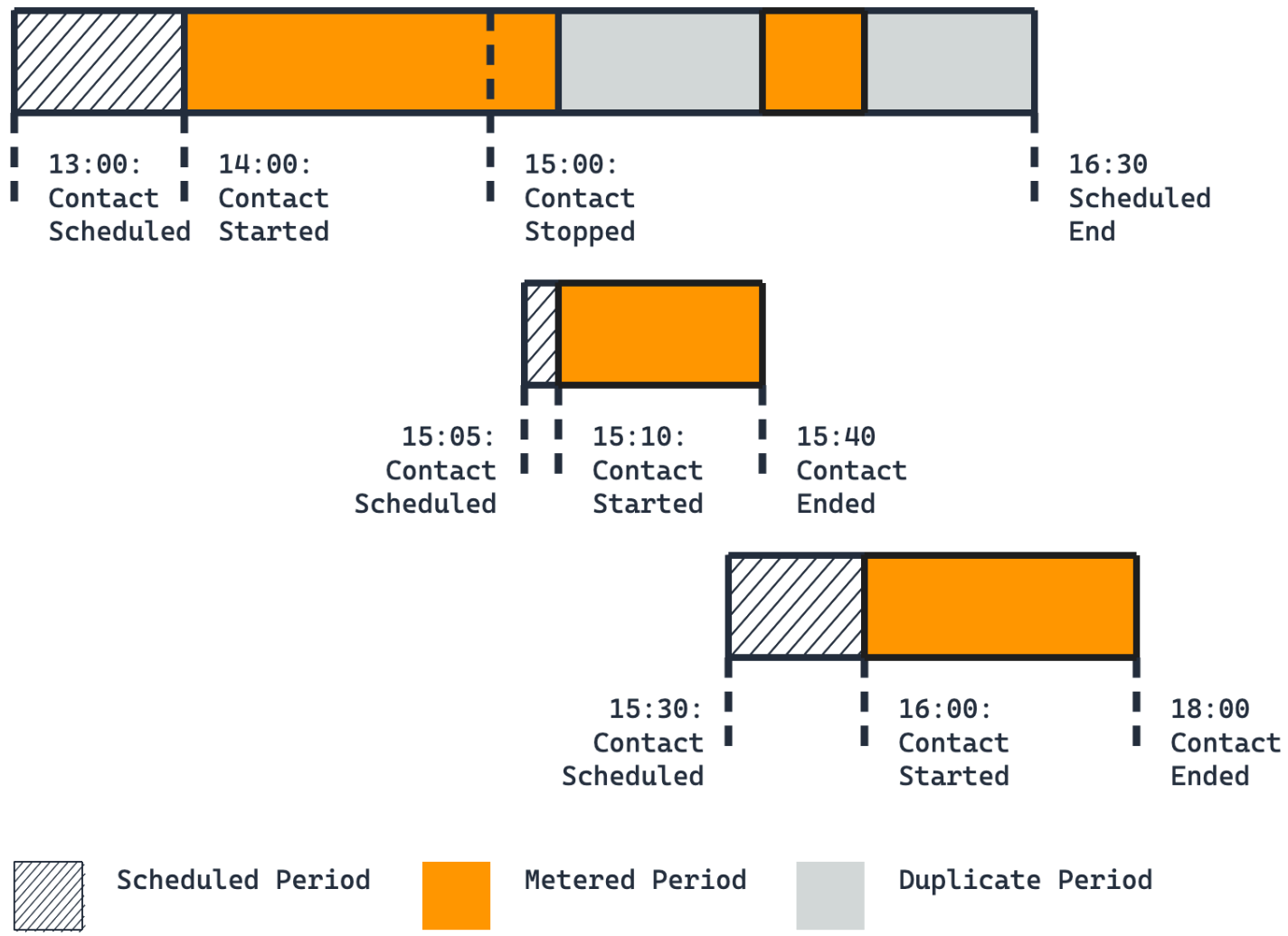
Suddivisione della fatturazione:

- Primo contatto: 120 minuti (60 minuti eseguiti più 10 minuti di inattività prima dell'inizio del secondo contatto + 50 minuti di tempo residuo non coperto dal duplicato)
- Secondo contatto: 30 minuti (durata completa)

Il contatto duplicato copre solo 30 minuti (15:10-15:40) dei 90 minuti rimanenti dopo l'interruzione del primo contatto. Ti verranno fatturati sia l'intervallo di 10 minuti prima dell'inizio del duplicato sia i 50 minuti di tempo scoperto dopo la fine del duplicato (15:40-16:30).

Scenario 5: duplicati multipli

Pianifica un contatto di 150 minuti su Ground Station Anytown 1 con inizio alle 14:00 e termine alle 16:30. Alle 15:00, chiami l'API per interrompere il tuo primo contatto CancelContact . Dopo la chiamata CancelContact, pianifichi un contatto di 30 minuti sulla stessa Ground Station a partire dalle 15:10. Successivamente, alle 15:30, pianifichi un altro contatto a partire dalle 16:00 per 120 minuti.



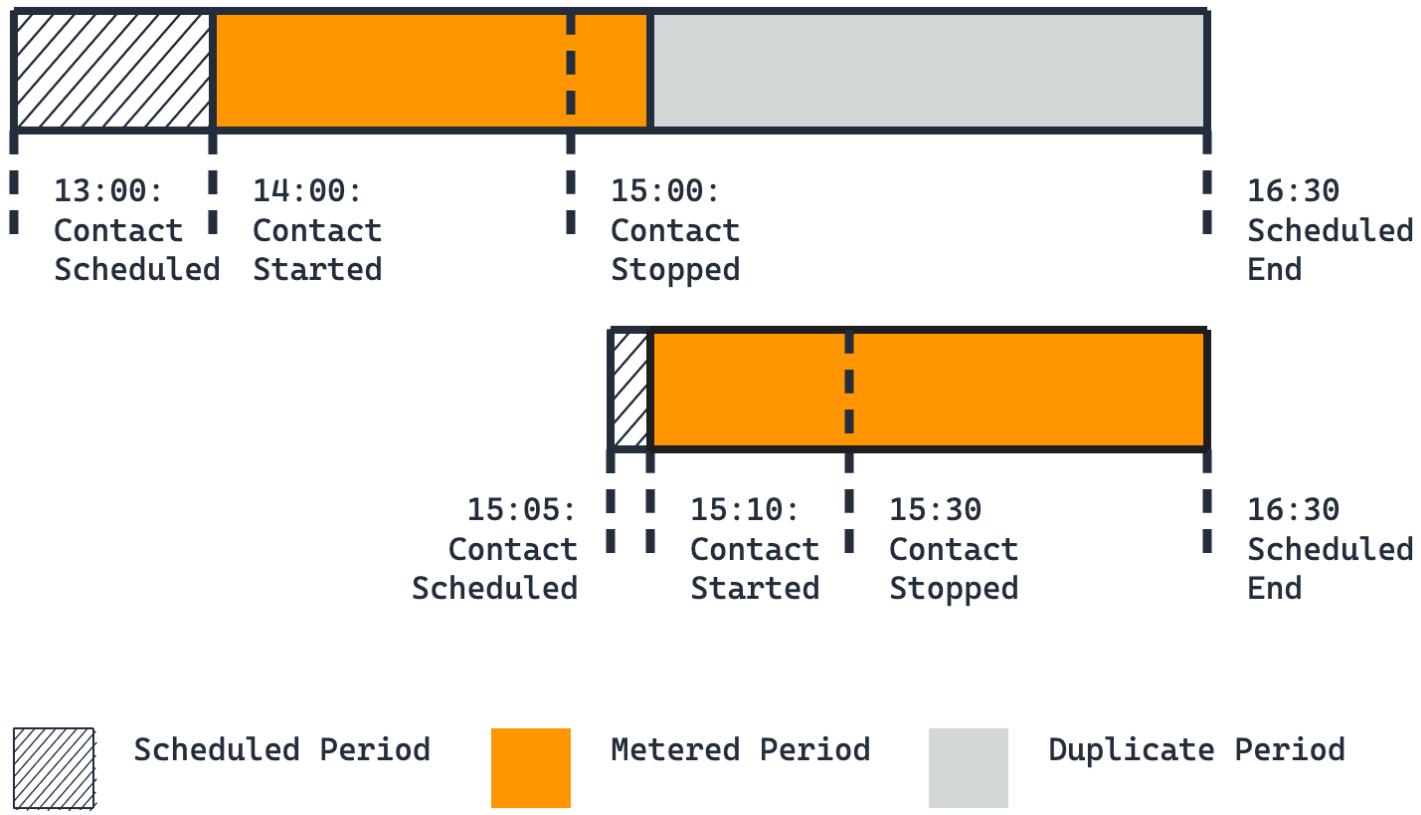
Suddivisione della fatturazione:

- Primo contatto: 90 minuti (60 minuti eseguiti+ 10 minuti di inattività prima dell'inizio del secondo contatto+ 20 minuti di inattività tra il secondo e il terzo contatto)
- Secondo contatto: 30 minuti (durata completa)
- Terzo contatto: 120 minuti (durata completa)

Sia il secondo che il terzo contatto vengono contati come duplicati perché li hai programmati dopo l'interruzione del primo contatto. Tuttavia, ti verranno comunque addebitati gli intervalli tra i contatti: 10 minuti tra la prima sosta (15:00) e il secondo inizio (15:10) e 20 minuti tra la seconda fine (15:40) e la terza (16:00).

Scenario 6: fermate multiple

Pianifica un contatto di 150 minuti su Ground Station Anytown 1 con inizio alle 14:00 e termine alle 16:30. Alle 15:00, chiami l'API per interrompere il tuo primo contatto CancelContact . Dopo la chiamata CancelContact, pianifichi un contatto di 80 minuti su Ground Station Anytown 1 che inizia alle 15:10 e termina alle 16:30. Alle 15:30, richiami nuovamente l' CancelContact API, interrompendo il contatto duplicato.



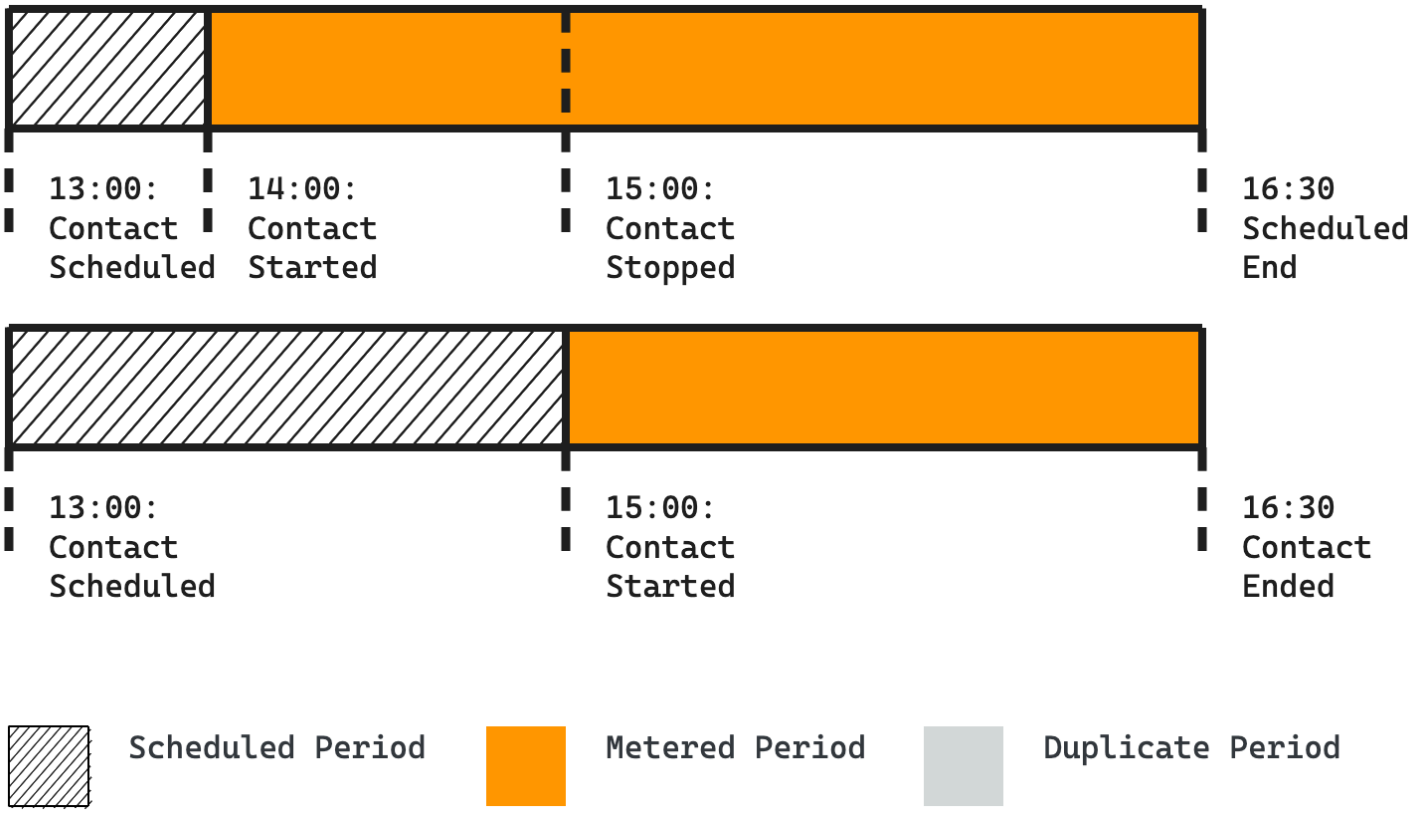
Suddivisione della fatturazione:

- Primo contatto: 70 minuti (60 minuti eseguiti più 10 minuti di inattività prima dell'inizio del secondo contatto)
- Secondo contatto: 80 minuti (durata originale completa)

Al secondo contatto viene fatturata l'intera durata di 80 minuti perché l'hai interrotto alle 15:30, lasciando vuoti 60 minuti dell'orario originariamente previsto (15:30-16:30). A meno che non pianifichi un altro contatto duplicato per coprire il tempo rimanente, sei responsabile per l'intera durata di ogni contatto interrotto.

Scenario 7: stazione terrestre con più antenne senza duplicati

Alle 13:00, pianifichi due contatti su Ground Station Anytown 1. Il primo è un contatto di 150 minuti che inizia alle 14:00 e termina alle 16:30. Il secondo è un contatto di 90 minuti che inizia alle 15:00 e termina alle 16:30. Alle 15:00, chiami l' CancelContact API per interrompere il primo contatto. Ground Station Anytown 1 è una stazione di terra multiantenna, che consente a entrambi i contatti di funzionare contemporaneamente.



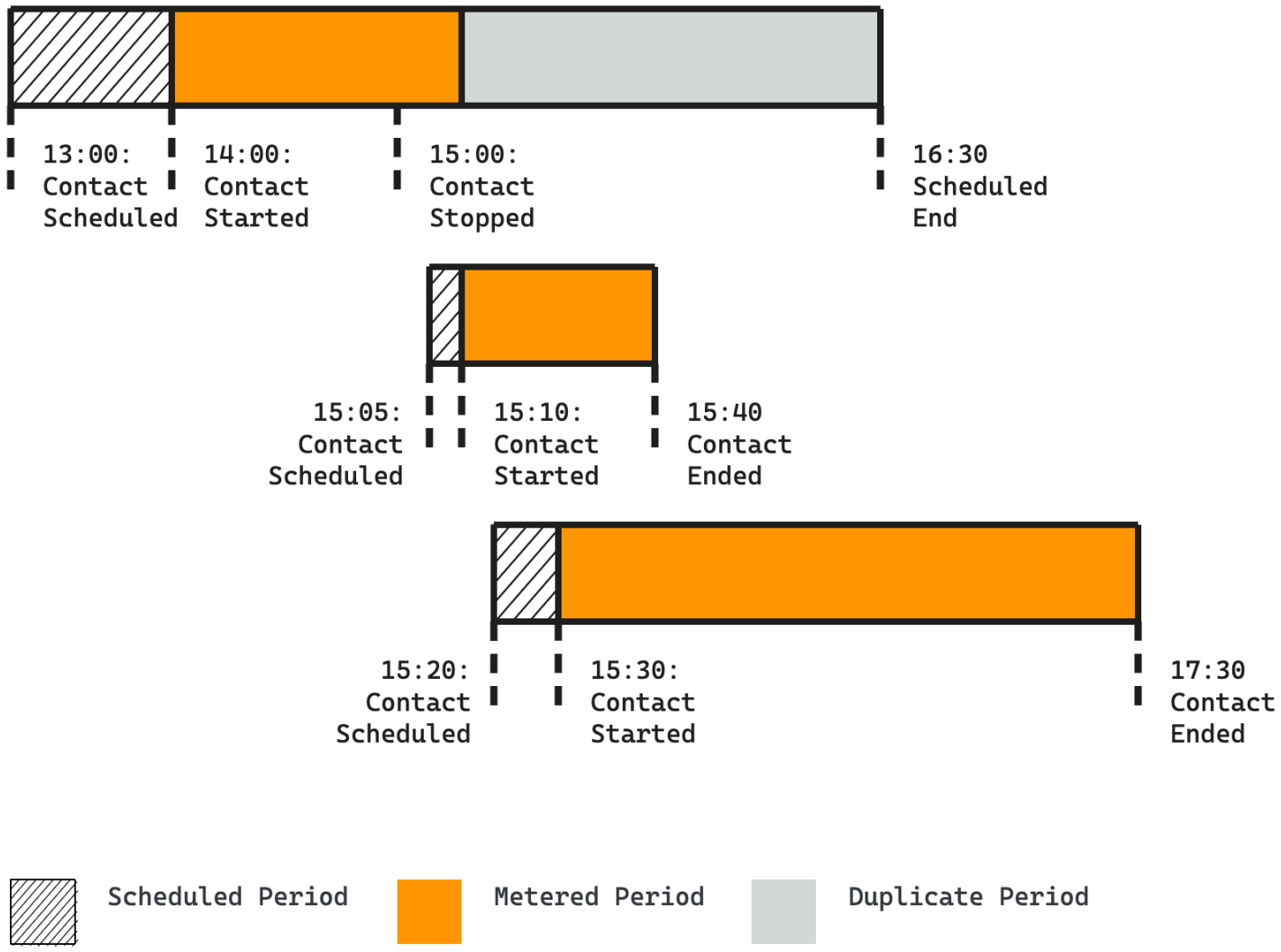
Suddivisione della fatturazione:

- Primo contatto: 150 minuti (durata originale completa)
- Secondo contatto: 90 minuti (durata completa)

Sebbene il secondo contatto si sovrapponga alla parte interrotta del primo contatto, non viene considerato un duplicato. Il secondo contatto non soddisfa il primo criterio per i duplicati: era programmato alle 13:00, prima di interrompere il primo contatto alle 15:00. Poiché non si tratta di un duplicato, ti verrà addebitata l'intera durata originale del primo contatto, indipendentemente da quando lo hai interrotto.

Scenario 8: stazione terrestre multiantenna con contatti duplicati

Pianifica un contatto di 150 minuti su Ground Station Anytown 1 con inizio alle 14:00 e termine alle 16:30. Alle 15:00, chiami l'API per interrompere il tuo primo contatto CancelContact . Dopo la chiamata CancelContact, pianifichi un contatto di 30 minuti su Ground Station Anytown 1 con inizio alle 15:10 e termine alle 15:40. Successivamente, pianifichi un altro contatto di 90 minuti su Ground Station Anytown 1 a partire dalle 15:30 e terminando alle 17:00. Ground Station Anytown 1 è una stazione di terra multiantenna, che consente a entrambi i contatti duplicati di funzionare contemporaneamente con tempi di sovrapposizione.



Suddivisione della fatturazione:

- Primo contatto: 70 minuti (60 minuti eseguiti più 10 minuti di inattività prima dell'inizio del secondo contatto)

- Secondo contatto: 30 minuti (durata completa)
- Terzo contatto: 90 minuti (durata completa)

Sia il secondo che il terzo contatto vengono contati come duplicati perché li hai programmati dopo l'interruzione del primo contatto. L'intervallo di 10 minuti tra l'interruzione del primo contatto (15:00) e l'avvio del secondo contatto (15:10) rappresenta i tempi di inattività addebitati rispetto al contatto originale.

Usa la funzione AWS Ground Station digital twin

La funzionalità digital twin AWS Ground Station fornisce un ambiente in cui è possibile testare e integrare il software di gestione e comando e controllo delle missioni satellitari. La funzione digital twin consente di testare la pianificazione, la verifica delle configurazioni e la corretta gestione degli errori senza utilizzare la capacità dell'antenna di produzione. Il test dell' AWS Ground Station integrazione con la funzionalità digital twin consente di avere maggiore fiducia nella capacità del sistema di gestire senza problemi le operazioni satellitari. Consente inoltre di eseguire i test AWS Ground Station APIs senza utilizzare la capacità di produzione o richiedere licenze per lo spettro.

Per iniziareSatellite a bordo, segui la pagina con la richiesta di accesso alla funzionalità digital twin. Una volta che il satellite è stato integrato nella funzione digital twin, puoi programmare i contatti tra le stazioni terrestri gemelle digitali. L'elenco delle stazioni terrestri a cui hai accesso può essere recuperato tramite la risposta dell'SDK ListGroundStationsAWS. Le stazioni di terra gemelle digitali sono copie esatte delle stazioni di terra elencate AWS Ground Station Sedi con un prefisso modificabile in Ground Station Nome di «Digital Twin». Ciò include le funzionalità delle antenne e i metadati, inclusi, a titolo esemplificativo, la maschera del sito e le coordinate GPS effettive. Al momento, la funzionalità digital twin non supporta la consegna dei dati come descritto inLavora con i flussi di dati.

Una volta integrata, la funzionalità digital twin emette gli stessi EventBridge eventi Amazon e le stesse risposte API del servizio di produzione, come descritto in. Automatizza AWS Ground Station con gli eventi Questi eventi ti consentiranno di ottimizzare le configurazioni e i gruppi di endpoint di dataflow.

Comprendi il monitoraggio con AWS Ground Station

Il monitoraggio è una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni di AWS Ground Station. AWS fornisce i seguenti strumenti di monitoraggio per osservare AWS Ground Station, segnalare quando qualcosa non va e intraprendere azioni automatiche quando necessario.

- Amazon EventBridge Events offre un flusso quasi in tempo reale di eventi di sistema che descrivono i cambiamenti nelle AWS risorse. EventBridge Events consente l'elaborazione automatizzata basata sugli eventi, poiché puoi scrivere regole che controllano determinati eventi e attivano azioni automatizzate in altri AWS servizi quando si verificano tali eventi. Per ulteriori informazioni sugli EventBridge eventi, consulta la Amazon EventBridge Events User Guide.
- AWS CloudTrailacquisisce le chiamate API e gli eventi correlati effettuati da o per conto del tuo AWS account e invia i file di log a un bucket Amazon S3 da te specificato. Puoi identificare quali utenti e account hanno chiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. Per ulteriori informazioni in merito AWS CloudTrail, consulta la Guida AWS CloudTrail per l'utente.
- Amazon CloudWatch Metrics acquisisce i parametri per i contatti pianificati durante l'utilizzo. AWS Ground Station CloudWatch Metrics ti consente di analizzare i dati in base al canale, alla polarizzazione e all'ID satellitare per identificare la potenza del segnale e gli errori nei tuoi contatti. Per ulteriori informazioni, consulta Usare i CloudWatch parametri di Amazon.
- AWS Notifiche all'utente può essere utilizzato per configurare canali di distribuzione per ricevere notifiche sugli AWS Ground Station eventi. L'utente riceverà una notifica quando un evento corrisponde a una regola specificata. Puoi ricevere notifiche relative agli eventi attraverso più canali, tra cui e-mail, Amazon Q Developer in applicazioni di chat, notifiche chat o notifiche AWS Console Mobile Applicationpush. Puoi anche visualizzare le notifiche nel centro di notifica della AWS console. Notifiche all'utente aggregazione dei supporti, che può ridurre il numero di notifiche ricevute durante eventi specifici.

Utilizza gli argomenti seguenti per monitorare AWS Ground Station.

Argomenti

- Automatizza AWS Ground Station con gli eventi
- Registra le chiamate AWS Ground Station API con AWS CloudTrail
- Visualizza le metriche con Amazon CloudWatch

Automatizza AWS Ground Station con gli eventi

> **Note**
>
> In questo documento viene utilizzato ovunque il termine «evento». CloudWatch Events e EventBridge sono lo stesso servizio e API sottostanti. Le regole per abbinare gli eventi in arrivo e indirizzarli verso le destinazioni per l'elaborazione possono essere create utilizzando entrambi i servizi.

Gli eventi consentono di automatizzare i AWS servizi e rispondere automaticamente a eventi di sistema come problemi di disponibilità delle applicazioni o modifiche delle risorse. Gli eventi dei AWS servizi vengono forniti quasi in tempo reale. Puoi compilare regole semplici che indichino quali eventi sono considerati di interesse per te e quali azioni automatizzate intraprendere quando un evento corrisponde a una regola. Alcune delle azioni che possono essere attivate automaticamente sono le seguenti:

- Invocare una funzione AWS Lambda
- Richiamo del comando di esecuzione di Amazon EC2
- Inoltro dell'evento a Amazon Kinesis Data Streams
- Attivazione di una macchina a stati AWS Step Functions
- Notifica di un argomento Amazon SNS o di una coda Amazon SQS

Alcuni esempi di utilizzo di eventi con AWS Ground Station includono:

- Richiamo di una funzione Lambda per automatizzare l'avvio e l'arresto delle istanze Amazon EC2 in base allo stato dell'evento.
- Pubblicazione su un argomento di Amazon SNS ogni volta che un contatto cambia stato. Questi argomenti possono essere impostati per inviare avvisi e-mail all'inizio o alla fine dei contatti.

Per ulteriori informazioni, consulta la Amazon EventBridge Events User Guide.

AWS Ground Station Tipi di eventi

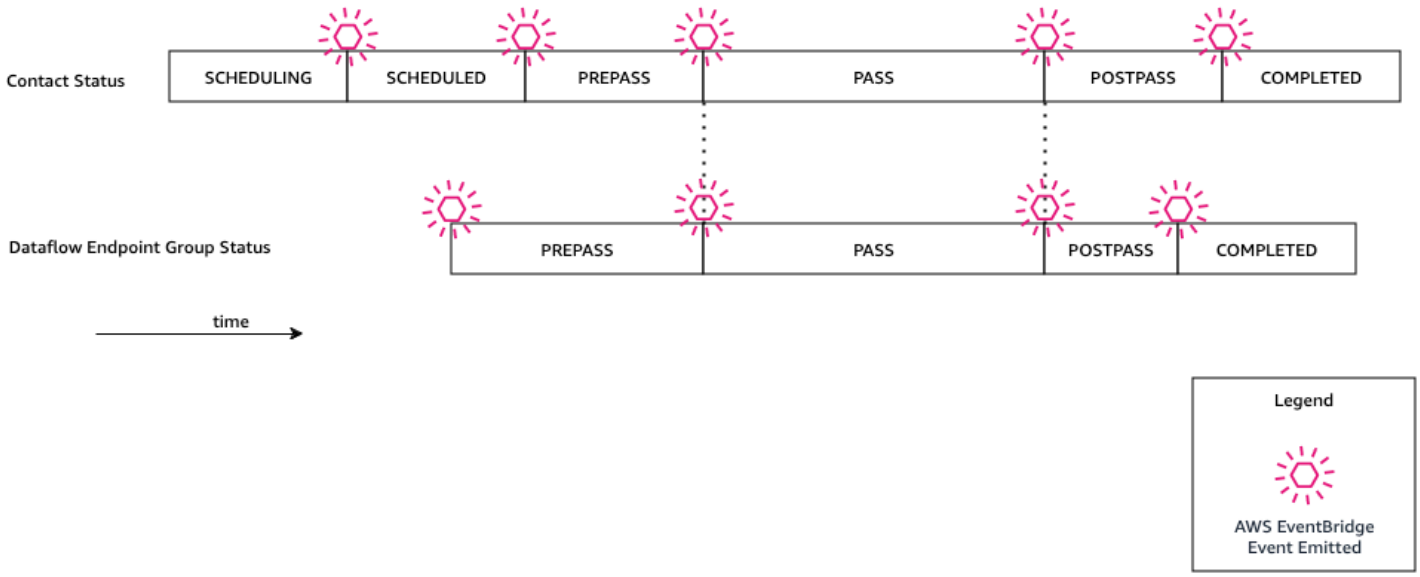
> **Note**
>
> Tutti gli eventi generati da AWS Ground Station hanno «aws.groundstation» come valore per «source».

AWS Ground Station emette eventi relativi ai cambiamenti di stato per supportare la capacità di personalizzare l'automazione. Attualmente, AWS Ground Station supporta gli eventi di modifica dello stato dei contatti, gli eventi di modifica del gruppo degli endpoint di dataflow e gli eventi di modifica dello stato delle effemeridi. Le seguenti sezioni forniscono informazioni dettagliate su ciascun tipo.

Cronologia degli eventi di contatto

AWS Ground Station emette eventi quando il contatto cambia stato. Per ulteriori informazioni su cosa sono questi cambiamenti di stato e sul significato degli stati stessi, vediComprendi il ciclo di vita dei contatti. Tutti i gruppi di endpoint di dataflow utilizzati nel tuo contatto hanno anche un set indipendente di eventi che vengono emessi. Nello stesso periodo di tempo, emettiamo anche eventi per il tuo gruppo di endpoint dataflow. L'ora precisa degli eventi pre-pass e post-pass è configurabile da te durante la configurazione del profilo di missione e del gruppo di endpoint del flusso di dati.

Il diagramma seguente mostra gli stati e gli eventi emessi per un contatto nominale e il gruppo di endpoint del flusso di dati associato.



Modifica dello stato di contatto della Ground Station

Se desideri eseguire un'azione specifica quando un contatto imminente cambia stato, puoi impostare una regola per automatizzare questa azione. Questo è utile per quando si desidera ricevere notifiche sulle modifiche di stato del contatto. Se desideri modificare la data di ricezione di questi eventi, puoi modificare il profilo contactPrePassDurationSecondse contactPostPassDurationSecondsdel tuo profilo di missione. Gli eventi vengono inviati alla regione da cui è stato pianificato il contatto.

Di seguito viene fornito un esempio di 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"
    }
}
```

I valori possibili per `contactStatus` sono definiti inthe section called "AWS Ground Station stati dei contatti".

Modifica dello stato del gruppo endpoint flusso dati della Ground Station

Se si desidera eseguire un'operazione quando il gruppo endpoint del flusso di dati viene utilizzato per ricevere i dati, è possibile impostare una regola per automatizzare questa operazione. Ciò consentirà di eseguire diverse operazioni in risposta agli stati di

modifica dello stato del gruppo endpoint del flusso di dati. Se desideri modificare la data di ricezione di questi eventi, utilizza un gruppo di endpoint dataflow con un and diverso. contactPrePassDurationSecondscontactPostPassDurationSeconds Questo evento verrà inviato alla regione del gruppo endpoint del flusso di dati.

Un esempio è fornito di seguito.

```
{
    "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"
    }
}
```

Possibili stati per `dataflowEndpointGroupState` includono `PREPASS`, `PASS`, `POSTPASS` e `COMPLETED`.

Eventi Ephemeris

Cambio di stato delle effemeridi di Ground Station

Se desideri eseguire un'azione quando un'effemeride cambia stato, puoi impostare una regola per automatizzare questa azione. Ciò consente di eseguire diverse azioni in risposta al cambiamento dello stato di un'effemeride. Ad esempio, è possibile eseguire un'azione quando un'effemeride ha completato la convalida, e lo è ora. `ENABLED` La notifica per questo evento verrà inviata alla regione in cui sono state caricate le effemeridi.

Un esempio è fornito di seguito.

```
{
    "id": "7bf73129-1428-4cd3-a780-95db273d1602",
    "detail-type": "Ground Station Ephemeris State Change",
    "source": "aws.groundstation",
    "account": "123456789012",
    "time": "2019-12-03T21:29:54Z",
    "region": "us-west-2",
    "resources": [
        "arn:aws:groundstation::123456789012:satellite/10313191-c9d9-4ecb-a5f2-
bc55cab050ec",
        "arn:aws:groundstation::123456789012:ephemeris/111111-cccc-bbbb-a555-
bcccca005000"
    ],
    "detail": {
        "ephemerisStatus": "ENABLED",
        "ephemerisId": "111111-cccc-bbbb-a555-bcccca005000",
        "satelliteId": "10313191-c9d9-4ecb-a5f2-bc55cab050ec"
    }
}
```

I possibili stati per l'opzione `ephemerisStatus` includono`ENABLED`,,,`VALIDATING`, `INVALID` `ERROR` `DISABLED` `EXPIRED`

Registra le chiamate AWS Ground Station API con AWS CloudTrail

AWS Ground Station è integrato con AWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, un ruolo o un AWS servizio in AWS Ground Station. CloudTrail acquisisce tutte le chiamate API AWS Ground Station come eventi. Le chiamate acquisite includono chiamate dalla AWS Ground Station console e chiamate di codice alle operazioni AWS Ground Station API. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per. AWS Ground Station Se non configuri un percorso, puoi comunque

visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare a quale richiesta è stata inviata AWS Ground Station, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Per ulteriori informazioni CloudTrail, consulta la Guida AWS CloudTrail per l'utente.

AWS Ground Station Informazioni in CloudTrail

CloudTrail è abilitato sul tuo AWS account al momento della creazione dell'account. Quando si verifica un'attività in AWS Ground Station, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi AWS di servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti nel tuo AWS account. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi nel tuo AWS account, inclusi gli eventi di AWS Ground Station, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un trail nella console, il trail sarà valido in tutte le regioni AWS. Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un trail
- CloudTrail Servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

Tutte AWS Ground Station le azioni vengono registrate CloudTrail e documentate nell'AWS Ground Station API Reference. Ad esempio, le chiamate a `CancelContact` e `ReserveContact` le `ListConfigs` azioni generano voci nei file di CloudTrail registro.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).

- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Comprensione delle AWS Ground Station voci dei file di registro

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'`ReserveContact`azione.

Esempio 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"
}
```

Visualizza le metriche con Amazon CloudWatch

Durante un contatto, acquisisce e invia AWS Ground Station automaticamente i dati CloudWatch per l'analisi. I tuoi dati possono essere visualizzati nella CloudWatch console Amazon. Per ulteriori informazioni sull'accesso e sui CloudWatch parametri, consulta Using Amazon CloudWatch Metrics.

La funzione di AWS Ground Station telemetria può essere utilizzata anche per ricevere metriche quasi in tempo reale durante i contatti. CloudWatch le metriche non sono disponibili quasi in tempo reale e potrebbero subire ritardi nella consegna. CloudWatch inoltre aggrega le metriche per un periodo di un secondo, riducendo potenzialmente la granularità dei dati. La funzionalità di telemetria fornisce le singole metriche e le trasmette quasi in tempo reale direttamente al tuo account. AWS Per ulteriori informazioni, consulta Lavora con la telemetria.

Important

AWS Ground Station emette le CloudWatch metriche relative alla AWS regione associata alla posizione della stazione di terra del contatto, non alla AWS regione da cui è stato programmato il contatto. Per visualizzare le metriche relative a un contatto, è necessario accedere alla regione della CloudWatch stazione di terra. Per informazioni sulla AWS regione associata a ciascuna stazione di terra, vedereIndividuazione della AWS regione in cui localizzare una stazione di terra. Per ricevere dati di telemetria nella regione da cui pianifichi i contatti, puoi utilizzare la funzione di telemetria. AWS Ground Station Per ulteriori dettagli, consulta Lavora con la telemetria.

AWS Ground Station Metriche e dimensioni

Quali parametri sono disponibili?

Le seguenti metriche sono disponibili presso. AWS Ground Station

Note

Le metriche specifiche emesse dipendono dalle AWS Ground Station funzionalità utilizzate. A seconda della configurazione, può essere emesso solo un sottoinsieme delle metriche seguenti.

Metrica	Dimensioni parametro	Description
`AzimuthAngle`	SatelliteId	L'angolo azimutale dell'antenna. Il vero nord è 0 gradi e l'est è 90 gradi. Unità: gradi
`BitErrorRate`	Canale, polarizzazione, SatelliteId	Il tasso di errore sui bit in un

Metrica	Dimensioni parametro	Description
		determina to numero di trasmissioni di bit. Gli errori di bit sono causati da rumore, distorsione o interferenza Unità: errori di bit per unità di tempo
`BlockErrorRate`	Canale, polarizzazione, SatelliteId	Il tasso di errore dei blocchi in un determina to numero di blocchi ricevuti. Gli errori dei blocchi sono causati da interferenze. Unità: Blocchi errati/Numero totale di blocchi
`CarrierFrequencyRecovery_Cn0`	Categoria, Config, SatelliteId	Rapporto tra densità portante e rumore per unità di larghezza di banda. Unità: Decibel-Hertz (dB-Hz)

Metrica	Dimensioni parametro	Description
`CarrierFrequencyRecovery_Locked`	Categoria, Config, SatelliteId	Impostato su 1 quando il circuito di recupero della frequenza portante del demodulatore è bloccato e 0 quando è sbloccato. Unità: senza unità
`CarrierFrequencyRecovery_OffsetFrequency_Hz`	Categoria, Config, SatelliteId	L'offset tra il centro del segnale stimato e la frequenza centrale ideale. Ciò è causato dallo spostamento Doppler e dall'offset dell'oscillatore locale tra il veicolo spaziale e il sistema di antenna. Unità: hertz (Hz)

Metrica	Dimensioni parametro	Description
`ElevationAngle`	SatelliteId	L'angolo di elevazione dell'antenna. L'orizzonte è di 0 gradi e lo zenit è di 90 gradi. Unità: gradi
`Es/N0`	Canale, polarizzazione, SatelliteId	Il rapporto tra l'energia per simbolo e la densità spettrale della potenza del rumore. Unità: decibel (dB)
`ReceivedPower`	Polarizzazione, SatelliteId	La potenza del segnale misurata nel demodulatore/decodificatore. Unità: decibel rispetto ai milliwatt (dBm)

Metrica	Dimensioni parametro	Description
`SymbolTimingRecovery_ErrorVectorMagnitude`	Categoria, Config, SatelliteId	La grandezza del vettore di errore tra i simboli ricevuti e i punti ideali della costellazione. Unità: percentuale
`SymbolTimingRecovery_Locked`	Categoria, Config, SatelliteId	Impostato su 1 quando il ciclo di ripristino del simbolo del demodulatore è bloccato e 0 quando è sbloccato Unità: senza unità

Metrica	Dimensioni parametro	Description
`SymbolTimingRecovery_OffsetSymbolRate`	Categoria, Config, SatelliteId	L'offset tra la frequenza simbolica stimata e la frequenza simbolica del segnale ideale. Ciò è causato dallo spostamento Doppler e dall'offset dell'oscillatore locale tra il veicolo spaziale e il sistema di antenna. Unità: simboli/secondo

Per quali dimensioni vengono utilizzate? AWS Ground Station

È possibile filtrare AWS Ground Station i dati utilizzando le seguenti dimensioni.

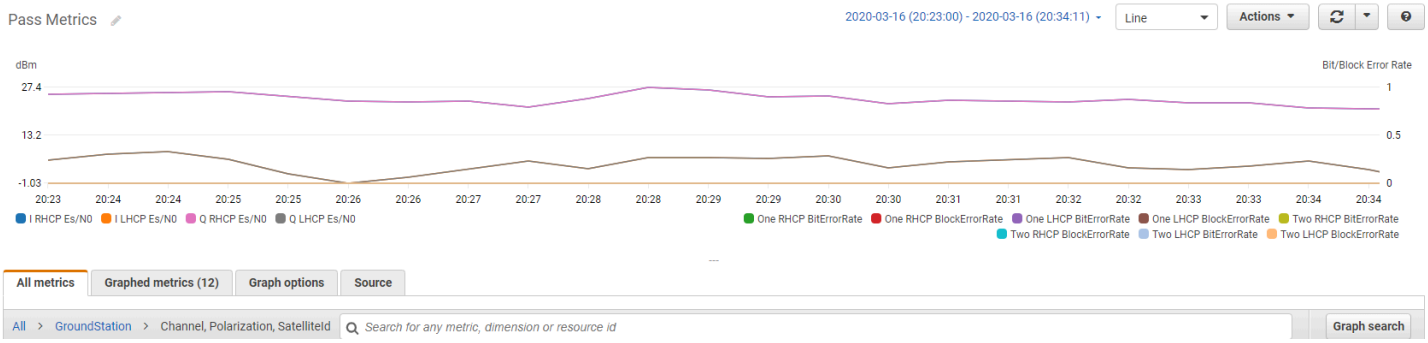
Dimensione	Description
`Category`	Demodulazione o decodifica.
`Channel`	I canali per ogni contatto includono Uno, Due, I (in fase) e Q (quadratura).
`Config`	Un'antenna downlink demod decode config arn.
`Polarization`	La polarizzazione per ogni contatto include LHCP (Left Hand Circular Polarized) o RHCP (Right Hand Circular Polarized).

Dimensione	Description
`SatelliteId`	L'ID satellitare contiene l'ARN del satellite per i tuoi contatti.

Visualizzazione dei parametri

Quando si visualizzano i parametri grafici, è importante notare che la finestra di aggregazione determina la modalità di visualizzazione dei parametri. Ogni parametro in un contatto può essere visualizzata come dati al secondo per 3 ore dopo la ricezione dei dati. I tuoi dati verranno aggregati da CloudWatch Metrics come dati al minuto dopo che sarà trascorso quel periodo di 3 ore. Se devi visualizzare le metriche su una misurazione di dati al secondo, ti consigliamo di visualizzarli entro il periodo di 3 ore dalla ricezione dei dati o di conservarli al di fuori delle Metriche. CloudWatch Per ulteriori informazioni sulla CloudWatch conservazione, consulta Amazon CloudWatch concepts - Metric retention.

Inoltre, i dati acquisiti entro i primi 60 secondi non conterranno informazioni sufficienti per produrre parametri significativi e probabilmente non verranno visualizzati. Per visualizzare metriche significative, si consiglia di visualizzare i dati dopo 60 secondi.

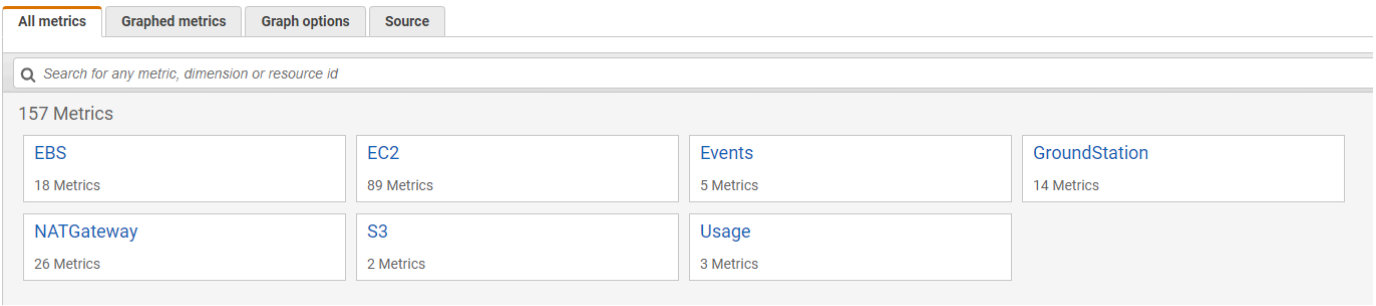


Per ulteriori informazioni sulla rappresentazione grafica delle AWS Ground Station metriche in CloudWatch, consulta Graphing Metrics.

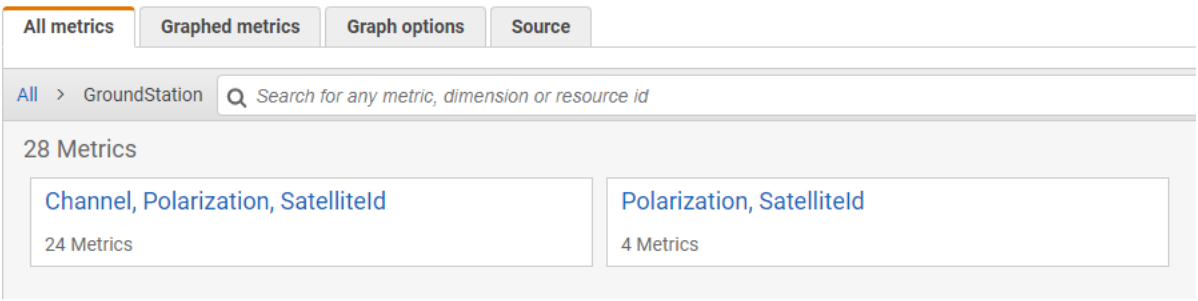
Per visualizzare i parametri tramite la console

1. Determina la AWS regione associata alla posizione della tua stazione di terra. AWS Ground Station emette CloudWatch metriche nella regione associata alla posizione della stazione di terra del contatto. Per l'elenco delle sedi delle stazioni terrestri e AWS delle regioni associate, vedi. Individuazione della AWS regione in cui localizzare una stazione di terra

2. Apri la CloudWatch console.
3. Nel riquadro di navigazione, seleziona Parametri.
4. Selezionare lo spazio dei nomi GroundStation.



5. Selezionate le dimensioni metriche desiderate (ad esempio, Canale, Polarizzazione, SatelliteId).



6. La scheda All metrics (Tutti i parametri) visualizza tutti i parametri per tale dimensione nello spazio dei nomi. Puoi fare quanto segue:

   a. Per ordinare la tabella, utilizza l'intestazione della colonna.
   b. Per rappresentare graficamente una metrica, seleziona la casella di controllo associata alla metrica. Per selezionare tutte le metriche, seleziona la casella di controllo nella riga del titolo della tabella.
   c. Per filtrare per risorsa, scegli l'ID della risorsa e quindi Add to search (Aggiungi alla ricerca).
   d. Per filtrare in base a un parametro, scegli il nome del parametro e quindi Add to search (Aggiungi alla ricerca).

Per visualizzare le metriche utilizzando AWS CLI

AWS Ground Station emette CloudWatch metriche nella regione associata alla posizione della stazione di terra del contatto. Per l'elenco delle ubicazioni delle stazioni terrestri e delle AWS regioni associate,. Individuazione della AWS regione in cui localizzare una stazione di terra Sostituiscilo *`ground-station-region-code`* con il codice AWS regionale della tua stazione di terra (ad

esempio, `us-west-2` per Oregon 1, Hawaii 1 o Alaska 1). Tutti i AWS CLI comandi successivi di questa procedura devono utilizzare la stessa regione.

1. Assicuratevi che AWS CLI sia installato. Per informazioni sull'installazione AWS CLI, consulta Installazione della versione 2 dell'interfaccia a riga di comando di AWS.
2. Identifica la AWS regione associata alla posizione della tua stazione di terra.
3. Utilizza il get-metric-datametodo della CloudWatch CLI per generare un file che può essere modificato per specificare le metriche che ti interessano e quindi essere utilizzato per eseguire query su tali metriche.

   Per fare ciò, esegui quanto segue:. `aws cloudwatch get-metric-data --region` *`ground-station-region-code`* `--generate-cli-skeleton` Questo genererà un output simile 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. Elenca le CloudWatch metriche disponibili `aws cloudwatch list-metrics --region` *`ground-station-region-code`* eseguendo.

   Se l'hai usato di recente AWS Ground Station, il metodo dovrebbe restituire un output contenente voci come:

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

> **Note**
>
> Se sono trascorse più di 2 settimane dall'ultimo utilizzo AWS Ground Station, dovrai controllare manualmente la tabella delle metriche disponibili per trovare i nomi e le dimensioni delle metriche nello spazio dei nomi delle `AWS/GroundStation` metriche.

Per ulteriori informazioni sulle limitazioni, consulta: Visualizza le metriche CloudWatch disponibili

5. Modifica il file JSON creato nel passaggio 2 in modo che corrisponda ai valori richiesti del passaggio 3, ad esempio`SatelliteId`, e delle tue `Polarization` metriche. Assicurati inoltre di aggiornare i `StartTime` `EndTime` valori e in modo che corrispondano al tuo contatto. Esempio:

```
        {
           "MetricDataQueries": [
              {
                 "Id": "receivedPowerExample",
                 "MetricStat": {
                    "Metric": {
                       "Namespace": "AWS/GroundStation",
                       "MetricName": "ReceivedPower",
                       "Dimensions": [
                          {
                             "Name": "SatelliteId",
                             "Value":
 "arn:aws:groundstation::111111111111:satellite/aaaaaaaa-bbbb-cccc-dddd-
eeeeeeeeeeee"
                          },
                          {
                             "Name": "Polarization",
                             "Value": "RHCP"
                          }
                       ]
                    },
                    "Period": 300,
                    "Stat": "Maximum",
                    "Unit": "None"
                 },
                 "Label": "ReceivedPowerExample",
                 "ReturnData": true
              }
           ],
           "StartTime": "2024-02-08T00:00:00",
           "EndTime": "2024-04-09T00:00:00"
        }
```

> **Note**
>
> AWS Ground Station pubblica le metriche ogni 1-60 secondi, a seconda della metrica. Le metriche non verranno restituite se il `Period` campo ha un valore inferiore al periodo di pubblicazione della metrica.

6. Esegui `aws cloudwatch get-metric-data` con il file di configurazione creato nei passaggi precedenti. Un esempio è fornito di seguito.

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

I parametri verranno fornite con i timestamp del tuo contatto. Di seguito viene fornito un esempio di output dei parametri 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": []
}
```

Sicurezza in AWS Ground Station

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, trarrai vantaggio da un data center e da un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza. AWS fornisce strumenti e caratteristiche specifici per la sicurezza per aiutare a raggiungere gli obiettivi di sicurezza. Questi strumenti e caratteristiche includono sicurezza di rete, gestione della configurazione, controllo degli accessi e protezione dei dati.

Durante l'utilizzo AWS Ground Station, ti consigliamo di seguire le migliori pratiche del settore e di implementare la crittografia. end-to-end AWS consente APIs di integrare crittografia e protezione dei dati. Per ulteriori informazioni sulla AWS sicurezza, consulta il white paper Introduzione alla sicurezza di AWS.

Utilizza i seguenti argomenti per scoprire come proteggere le risorse di .

Argomenti

Identity and Access Management per AWS Ground Station

AWS Identity and Access Management (IAM) è un software Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse. AWS Ground Station IAM è uno Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

Argomenti

- Gestione dell'accesso tramite policy
- Come AWS Ground Station funziona con IAM
- Esempi di policy basate sull'identità per AWS Ground Station
- Risoluzione dei problemi AWS Ground Station di identità e accesso

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia in base al tuo ruolo:

- Utente del servizio: richiedi le autorizzazioni all'amministratore se non riesci ad accedere alle funzionalità (consulta Risoluzione dei problemi AWS Ground Station di identità e accesso)
- Amministratore del servizio: determina l'accesso degli utenti e invia le richieste di autorizzazione (consulta Come AWS Ground Station funziona con IAM)
- Amministratore IAM: scrivi policy per gestire l'accesso (consulta Esempi di policy basate sull'identità per AWS Ground Station)

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi autenticarti come utente IAM o assumendo un ruolo IAM. Utente root dell'account AWS

Puoi accedere come identità federata utilizzando credenziali provenienti da una fonte di identità come AWS IAM Identity Center (IAM Identity Center), autenticazione Single Sign-On o credenziali. Google/ Facebook Per ulteriori informazioni sull'accesso, consulta Come accedere all' Account AWS nella Guida per l'utente di Accedi ad AWS .

Per l'accesso programmatico, AWS fornisce un SDK e una CLI per firmare crittograficamente le richieste. Per ulteriori informazioni, consulta AWS Signature Version 4 per le richieste API nella Guida per l'utente di IAM.

Account AWS utente root

Quando si crea un Account AWS, si inizia con un'identità di accesso denominata utente Account AWS root che ha accesso completo a tutte Servizi AWS le risorse. Consigliamo vivamente di non utilizzare l'utente root per le attività quotidiane. Per le attività che richiedono le credenziali dell'utente root, consulta Attività che richiedono le credenziali dell'utente root nella Guida per l'utente IAM.

Identità federata

Come procedura ottimale, richiedi agli utenti umani di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente della directory aziendale, del provider di identità Web o Directory Service che accede Servizi AWS utilizzando le credenziali di una fonte di identità. Le identità federate assumono ruoli che forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, si consiglia di utilizzare AWS IAM Identity Center. Per ulteriori informazioni, consulta Che cos'è il Centro identità IAM? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un utente IAM è una identità che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ti consigliamo di utilizzare credenziali temporanee invece di utenti IAM con credenziali a lungo termine. Per ulteriori informazioni, consulta Richiedere agli utenti umani di utilizzare la federazione con un provider di identità per accedere AWS utilizzando credenziali temporanee nella Guida per l'utente IAM.

Un gruppo IAM specifica una raccolta di utenti IAM e semplifica la gestione delle autorizzazioni per gestire gruppi di utenti di grandi dimensioni. Per ulteriori informazioni, consulta Casi d'uso per utenti IAM nella Guida per l'utente di IAM.

Ruoli IAM

Un ruolo IAM è un'identità con autorizzazioni specifiche che fornisce credenziali temporanee. Puoi assumere un ruolo passando da un ruolo utente a un ruolo IAM (console) o chiamando un'operazione AWS CLI o AWS API. Per ulteriori informazioni, consulta Metodi per assumere un ruolo nella Guida per l'utente di IAM.

I ruoli IAM sono utili per l'accesso degli utenti federati, le autorizzazioni utente IAM temporanee, l'accesso multi-account, l'accesso multi-servizio e le applicazioni in esecuzione su Amazon EC2. Per maggiori informazioni, consultare Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Gestione dell'accesso tramite policy

Puoi controllare l'accesso AWS creando policy e associandole a AWS identità o risorse. Una policy definisce le autorizzazioni quando è associata a un'identità o a una risorsa. AWS valuta queste

politiche quando un preside effettua una richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per maggiori informazioni sui documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente IAM.

Utilizzando le policy, gli amministratori specificano chi ha accesso a cosa definendo quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Un amministratore IAM crea le policy IAM e le aggiunge ai ruoli, che gli utenti possono quindi assumere. Le policy IAM definiscono le autorizzazioni indipendentemente dal metodo utilizzato per eseguirle.

Policy basate sull'identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile collegare a un'identità (utente, gruppo o ruolo). Tali policy controllano le operazioni autorizzate per l'identità, nonché le risorse e le condizioni in cui possono essere eseguite. Per informazioni su come creare una policy basata su identità, consultare Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente IAM.

Le policy basate su identità possono essere policy in linea (con embedding direttamente in una singola identità) o policy gestite (policy autonome collegate a più identità). Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scegliere tra policy gestite e policy in linea nella Guida per l'utente di IAM.

Policy basate sulle risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi includono le policy di trust dei ruoli IAM e le policy dei bucket di Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. In una policy basata sulle risorse è obbligatorio specificare un'entità principale.

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non è possibile utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi che possono impostare le autorizzazioni massime concesse dai tipi di policy più comuni:

- Limiti delle autorizzazioni: imposta il numero massimo di autorizzazioni che una policy basata su identità ha la possibilità di concedere a un'entità IAM. Per ulteriori informazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente di IAM.
- Politiche di controllo del servizio (SCPs): specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa in. AWS Organizations Per ulteriori informazioni, consultare Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .
- Politiche di controllo delle risorse (RCPs): imposta le autorizzazioni massime disponibili per le risorse nei tuoi account. Per ulteriori informazioni, consulta Politiche di controllo delle risorse (RCPs) nella Guida per l'AWS Organizations utente.
- Policy di sessione: policy avanzate passate come parametro quando si crea una sessione temporanea per un ruolo o un utente federato. Per maggiori informazioni, consultare Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

Quando a una richiesta si applicano più tipi di policy, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire o meno una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella IAM User Guide.

Come AWS Ground Station funziona con IAM

Prima di utilizzare IAM per gestire l'accesso a AWS Ground Station, scopri con quali funzionalità IAM è disponibile l'uso AWS Ground Station.

Funzionalità IAM che puoi utilizzare con AWS Ground Station

Funzionalità IAM	AWS Ground Station supporto
Policy basate sull'identità	Sì
Policy basate su risorse	No
Operazioni di policy	Sì
Risorse relative alle policy	Sì

Funzionalità IAM	AWS Ground Station supporto
Chiavi di condizione della policy (specifica del servizio)	Sì
ACLs	No
ABAC (tag nelle policy)	Sì
Credenziali temporanee	Sì
Autorizzazioni del principale	Sì
Ruoli di servizio	No
Ruoli collegati al servizio	Sì

Per avere una panoramica di alto livello su come AWS Ground Station e altri AWS servizi funzionano con la maggior parte delle funzionalità IAM, consulta AWS i servizi che funzionano con IAM nella IAM User Guide.

Politiche basate sull'identità per AWS Ground Station

Supporta le policy basate sull'identità: sì

Le policy basate sull'identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente di IAM.

Con le policy basate sull'identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente IAM.

Esempi di politiche basate sull'identità per AWS Ground Station

Per visualizzare esempi di politiche basate sull' AWS Ground Station identità, vedere. Esempi di policy basate sull'identità per AWS Ground Station

Politiche basate sulle risorse all'interno AWS Ground Station

Supporta le policy basate su risorse: no

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy di bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. In una policy basata sulle risorse è obbligatorio specificare un'entità principale. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, è possibile specificare un intero account o entità IAM in un altro account come entità principale in una policy basata sulle risorse. Per ulteriori informazioni, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Azioni politiche per AWS Ground Station

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso in una policy. Includere le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco di AWS Ground Station azioni, vedere Azioni definite da AWS Ground Station nel Service Authorization Reference.

Le azioni politiche in AWS Ground Station uso utilizzano il seguente prefisso prima dell'azione:

```
groundstation
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

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

```
        ]
```

Per visualizzare esempi di politiche AWS Ground Station basate sull'identità, vedere. Esempi di policy basate sull'identità per AWS Ground Station

Risorse politiche per AWS Ground Station

Supporta le risorse relative alle policy: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Per le azioni che non supportano le autorizzazioni a livello di risorsa, si utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

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

Per visualizzare un elenco dei tipi di AWS Ground Station risorse e relativi ARNs, vedere Resources defined by AWS Ground Station nel Service Authorization Reference. Per informazioni sulle operazioni con cui è possibile specificare l'ARN di ogni risorsa, consulta la sezione Operazioni definite da AWS Ground Station.

Per visualizzare esempi di politiche AWS Ground Station basate sull'identità, vedere. Esempi di policy basate sull'identità per AWS Ground Station

Chiavi relative alle condizioni delle politiche per AWS Ground Station

Supporta le chiavi di condizione delle policy specifiche del servizio: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Condition` specifica quando le istruzioni vengono eseguite in base a criteri definiti. È possibile compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio

uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Per visualizzare un elenco di chiavi di AWS Ground Station condizione, consulta Condition keys for AWS Ground Station nel Service Authorization Reference. Per sapere con quali azioni e risorse puoi utilizzare una chiave di condizione, vedi Azioni definite da AWS Ground Station.

Per visualizzare esempi di politiche AWS Ground Station basate sull'identità, vedere. Esempi di policy basate sull'identità per AWS Ground Station

ACLs in AWS Ground Station

Supporti: No ACLs

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

ABAC con AWS Ground Station

Supporta ABAC (tag nelle policy): sì

Il controllo degli accessi basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base ad attributi chiamati tag. Puoi allegare tag a entità e AWS risorse IAM, quindi progettare politiche ABAC per consentire operazioni quando il tag del principale corrisponde al tag sulla risorsa.

Per controllare l'accesso basato su tag, fornire informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Sì. Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per maggiori informazioni su ABAC, consulta Definizione delle autorizzazioni con autorizzazione ABAC nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

Utilizzo di credenziali temporanee con AWS Ground Station

Supporta le credenziali temporanee: sì

Le credenziali temporanee forniscono l'accesso a breve termine alle AWS risorse e vengono create automaticamente quando si utilizza la federazione o si cambia ruolo. AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza temporanee in IAM e Servizi AWS compatibili con IAM nella Guida per l'utente IAM.

Autorizzazioni principali multiservizio per AWS Ground Station

Supporta l'inoltro delle sessioni di accesso (FAS): sì

Le sessioni di accesso inoltrato (FAS) utilizzano le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta di effettuare richieste Servizio AWS ai servizi downstream. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.

Ruoli di servizio per AWS Ground Station

Supporta i ruoli di servizio: no

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta Create a role to delegate permissions to an Servizio AWS nella Guida per l'utente IAM.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe compromettere AWS Ground Station la funzionalità. Modifica i ruoli di servizio solo quando viene AWS Ground Station fornita una guida in tal senso.

Ruoli collegati ai servizi per AWS Ground Station

Supporta i ruoli collegati ai servizi: sì

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'operazione per tuo conto. I ruoli collegati al servizio vengono

visualizzati in Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati al servizio, ma non modificarle.

Per ulteriori informazioni su come creare e gestire i ruoli collegati ai servizi, consulta Servizi AWS supportati da IAM. Trova un servizio nella tabella che include un `Yes` nella colonna Service-linked role (Ruolo collegato ai servizi). Scegli il collegamento Sì per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Esempi di policy basate sull'identità per AWS Ground Station

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse AWS Ground Station . Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy IAM (console) nella Guida per l'utente di IAM.

Per informazioni dettagliate sulle azioni e sui tipi di risorse definiti da AWS Ground Station, incluso il formato di ARNs per ogni tipo di risorsa, vedere Azioni, risorse e chiavi di condizione AWS Ground Station nel Service Authorization Reference.

Argomenti

- Best practice per le policy
- Utilizzo della console AWS Ground Station
- Consentire agli utenti di visualizzare le loro autorizzazioni

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare AWS Ground Station risorse nel tuo account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando si creano o modificano policy basate sull'identità, seguire queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti

specifiche per i tuoi casi d'uso. Per maggiori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente di IAM.

- Applicazione delle autorizzazioni con privilegio minimo - Quando si impostano le autorizzazioni con le policy IAM, concedere solo le autorizzazioni richieste per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegio minimo. Per maggiori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso - Per limitare l'accesso ad azioni e risorse è possibile aggiungere una condizione alle policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio CloudFormation. Per maggiori informazioni, consultare la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.
- Utilizzo dello strumento di analisi degli accessi IAM per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali - Lo strumento di analisi degli accessi IAM convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio (JSON) della policy IAM e alle best practice di IAM. Lo strumento di analisi degli accessi IAM offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per maggiori informazioni, consultare Convalida delle policy per il Sistema di analisi degli accessi IAM nella Guida per l'utente di IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungere le condizioni MFA alle policy. Per maggiori informazioni, consultare Protezione dell'accesso API con MFA nella Guida per l'utente di IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Utilizzo della console AWS Ground Station

Per accedere alla AWS Ground Station console, è necessario disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle AWS Ground Station risorse del tuo. Account AWS Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario consentire autorizzazioni minime per la console agli utenti che effettuano chiamate solo verso AWS CLI o l' AWS API. Al contrario, è opportuno concedere l'accesso solo alle azioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che utenti e ruoli possano ancora utilizzare la AWS Ground Station console, allega anche la policy AWS Ground Station *ConsoleAccess* o la policy *ReadOnly* AWS gestita alle entità. Per maggiori informazioni, consulta Aggiunta di autorizzazioni a un utente nella Guida per l'utente di IAM.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono collegate alla relativa identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando l'API o a livello di codice. AWS CLI AWS

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

```
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Risoluzione dei problemi AWS Ground Station di identità e accesso

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con un AWS Ground Station IAM.

Argomenti

- Non sono autorizzato a eseguire alcuna azione in AWS Ground Station
- Non sono autorizzato a eseguire iam: PassRole
- Voglio consentire a persone esterne a me di accedere Account AWS alle mie AWS Ground Station risorse

Non sono autorizzato a eseguire alcuna azione in AWS Ground Station

Se ricevi un errore che indica che non sei autorizzato a eseguire un'operazione, le tue policy devono essere aggiornate per poter eseguire l'operazione.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa *`my-example-widget`* fittizia ma non dispone di autorizzazioni `groundstation:`*`GetWidget`* fittizie.

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

In questo caso, la policy per l'utente `mateojackson` deve essere aggiornata per consentire l'accesso alla risorsa *`my-example-widget`* utilizzando l'azione `groundstation:`*`GetWidget`*.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un errore che indica che non sei autorizzato a eseguire l'operazione `iam:PassRole`, le tue policy devono essere aggiornate per poter passare un ruolo a AWS Ground Station.

Alcuni Servizi AWS consentono di passare un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

L'errore di esempio seguente si verifica quando un utente IAM denominato `marymajor` cerca di utilizzare la console per eseguire un'operazione in AWS Ground Station. Tuttavia, l'operazione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per trasmettere il ruolo al servizio.

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

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne a me di accedere Account AWS alle mie AWS Ground Station risorse

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per i servizi che supportano politiche basate sulle risorse o liste di controllo degli accessi (ACLs), puoi utilizzare tali politiche per concedere alle persone l'accesso alle tue risorse.

Per maggiori informazioni, consulta gli argomenti seguenti:

- Per sapere se AWS Ground Station supporta queste funzionalità, consulta. Come AWS Ground Station funziona con IAM
- Per scoprire come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.

- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (federazione delle identità) nella Guida per l'utente IAM.
- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

AWS politiche gestite per AWS Ground Station

Una politica AWS gestita è una politica autonoma creata e amministrata da AWS. AWS le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni, in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Si consiglia pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i propri casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando ne Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consultare Policy gestite da AWS nella Guida per l'utente di IAM.

AWS politica gestita: AWSGround StationAgentInstancePolicy

È possibile allegare la policy `AWSGroundStationAgentInstancePolicy` alle identità IAM.

Questa politica concede le autorizzazioni di AWS Ground Station agente alla tua istanza Amazon EC2 che consente all'istanza di inviare e ricevere dati durante i contatti con Ground Station. Tutte le autorizzazioni in questa politica provengono dal servizio Ground Station.

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `groundstation`— Consente alle istanze degli endpoint Dataflow di chiamare Ground Station Agent. APIs

Per visualizzare la versione più recente del documento sulla policy JSON, consulta AWSGroundStationAgentInstancePolicyla AWS Managed Policy Reference Guide.

AWS politica gestita: AWSService RoleForGroundStationDataflowEndpointGroupPolicy

Non puoi collegarti AWSService RoleForGroundStationDataflowEndpointGroupPolicy alle tue entità IAM. Questa policy è associata a un ruolo collegato al servizio che consente di eseguire azioni AWS Ground Station per conto dell'utente. Per ulteriori informazioni, vedere Utilizzo dei ruoli collegati al servizio.

Questa politica concede le autorizzazioni EC2 che consentono di AWS Ground Station trovare indirizzi pubblici. IPv4

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `ec2:DescribeAddresses`— Consente di AWS Ground Station elencare tutti gli IPs associati per tuo EIPs conto.
- `ec2:DescribeNetworkInterfaces`— Consente di AWS Ground Station ottenere informazioni sulle interfacce di rete associate alle istanze EC2 per tuo conto.

Per visualizzare la versione più recente del documento sulla policy JSON, consulta AWSServiceRoleForGroundStationDataflowEndpointGroupPolicyla AWS Managed Policy Reference Guide.

AWS Ground Station aggiornamenti alle policy AWS gestite

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite AWS Ground Station da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS nella pagina della cronologia dei AWS Ground Station documenti.

Modifica	Descrizione	Data
AWSGroundStationAgentInstancePolicy: aggiornamento a una policy esistente	AWS Ground Station ha aggiunto nuove autorizzazioni per consentire agli agenti di recuperare la risposta alle attività URLs per operazioni avanzate di Ground Station.	13 novembre 2025
AWSGroundStationAgentInstancePolicy: nuova policy	AWS Ground Station ha aggiunto una nuova policy per fornire all'istanza dataflow endpoint le autorizzazioni per utilizzare AWS Ground Station Agent.	12 aprile 2023
AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy: nuova policy	AWS Ground Station ha aggiunto una nuova policy che concede le autorizzazioni EC2 per consentire di trovare indirizzi IPv4 pubblici associati agli EIP e AWS Ground Station alle interfacce di rete associate alle istanze EC2.	02 novembre 2022
AWS Ground Station ha iniziato a tenere traccia delle modifiche	AWS Ground Station ha iniziato a tenere traccia delle	01 marzo 2021

Modifica	Descrizione	Data
	modifiche per le politiche AWS gestite.	

Usa ruoli collegati ai servizi per Ground Station

AWS Ground Station utilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM collegato direttamente a Ground Station. I ruoli collegati ai servizi sono predefiniti da Ground Station e includono tutte le autorizzazioni richieste dal servizio per chiamare altri AWS servizi per conto dell'utente.

Un ruolo collegato al servizio semplifica la configurazione di Ground Station perché non è necessario aggiungere manualmente le autorizzazioni necessarie. Ground Station definisce le autorizzazioni dei suoi ruoli collegati al servizio e, se non diversamente definito, solo Ground Station può assumere i suoi ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni. Una policy delle autorizzazioni specifica non può essere collegata a un'altra entità IAM.

Per informazioni su altri servizi che supportano i ruoli collegati ai servizi, consulta i AWS servizi che funzionano con IAM e cerca i servizi con Sì nella colonna Ruoli collegati ai servizi. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato al servizio per tale servizio.

Autorizzazioni di ruolo collegate al servizio per Ground Station

Ground Station utilizza il ruolo collegato ai servizi denominato: AWSServiceRoleForGroundStationDataflowEndpointGroupAWS GroundStation utilizza questo ruolo collegato ai servizi per richiamare EC2 per trovare indirizzi pubblici. IPv4

Il ruolo AWSService RoleForGroundStationDataflowEndpointGroup collegato al servizio prevede che i seguenti servizi assumano il ruolo:

- `groundstation.amazonaws.com`

La politica di autorizzazione dei ruoli denominata AWSService RoleForGroundStationDataflowEndpointGroupPolicy consente a Ground Station di completare le seguenti azioni sulle risorse specificate:

- Operazione: `ec2:DescribeAddresses` su `all AWS resources (*)`

  L'azione consente a Ground Station di elencare tutti gli IPs associati a EIPs.

- Operazione: `ec2:DescribeNetworkInterfaces` su `all AWS resources (*)`

  Action consente a Ground Station di ottenere informazioni sulle interfacce di rete associate alle istanze EC2

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato al servizio è necessario configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente IAM.

Creazione di un ruolo collegato ai servizi per Ground Station

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando crei un DataflowEndpointGroup in AWS CLI o l' AWS API, Ground Station crea automaticamente il ruolo collegato al servizio.

Se elimini questo ruolo collegato al servizio, è possibile ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando crei un DataflowEndpointGroup, Ground Station crea nuovamente il ruolo collegato al servizio per te.

Puoi anche utilizzare la console IAM per creare un ruolo collegato al servizio con lo use case Data Delivery to Amazon EC2. Nella AWS CLI o nell' AWS API, crea un ruolo collegato al servizio con il nome del servizio. `groundstation.amazonaws.com` Per ulteriori informazioni, consulta Creazione di un ruolo collegato ai servizi nella Guida per l'utente IAM. Se elimini il ruolo collegato ai servizi, è possibile utilizzare lo stesso processo per crearlo nuovamente.

Modifica di un ruolo collegato al servizio per Ground Station

Ground Station non consente di modificare il ruolo AWSService RoleForGroundStationDataflowEndpointGroup collegato al servizio. Dopo avere creato un ruolo collegato al servizio, non sarà possibile modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato al servizio nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato al servizio per Ground Station

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato al servizio, ti consigliamo di eliminare il ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente.

È possibile eliminare un ruolo collegato al servizio solo dopo aver eliminato per la prima volta il ruolo utilizzando il ruolo collegato al servizio. DataflowEndpointGroups Questo ti protegge dalla revoca inavvertitamente delle autorizzazioni al tuo. DataflowEndpointGroups Se un ruolo collegato al servizio viene utilizzato con più ruoli DataflowEndpointGroups, è necessario eliminare tutti quelli DataflowEndpointGroups che utilizzano il ruolo collegato al servizio prima di poterlo eliminare.

> **Note**
>
> Se il servizio Ground Station utilizza il ruolo quando si tenta di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare le risorse Ground Station utilizzate da AWSService RoleForGroundStationDataflowEndpointGroup

- Elimina DataflowEndpointGroups tramite l'AWS CLI o l'API AWS.

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAM AWS CLI, l'o l' AWS API per eliminare il ruolo collegato al AWSService RoleForGroundStationDataflowEndpointGroup servizio. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente IAM.

Regioni supportate per i ruoli collegati al servizio Ground Station

Ground Station supporta l'utilizzo di ruoli collegati al servizio in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta la Tabella delle regioni.

Risoluzione dei problemi

`NOT_AUTHORIZED_TO_CREATE_SLR`- Ciò indica che il ruolo nel tuo account utilizzato per chiamare l' CreateDataflowEndpointGroup API non dispone

dell'`iam:CreateServiceLinkedRole`autorizzazione. Un amministratore con l'`iam:CreateServiceLinkedRole`autorizzazione deve creare manualmente il ruolo collegato ai servizi per il tuo account.

Crittografia dei dati a riposo per AWS Ground Station

AWS Ground Station fornisce la crittografia di default per proteggere i dati sensibili archiviati utilizzando chiavi AWS di crittografia proprietarie.

- AWS chiavi di proprietà: AWS Ground Station utilizza queste chiavi per impostazione predefinita per crittografare automaticamente dati ed effemeridi personali e direttamente identificabili. Non è possibile visualizzare, gestire o utilizzare chiavi di AWS proprietà o controllarne l'utilizzo; tuttavia, non è necessario intraprendere alcuna azione o modificare i programmi per proteggere le chiavi che crittografano i dati. Per ulteriori informazioni, consulta AWS-owned keys nella Developer Guide.AWS Key Management Service

La crittografia predefinita dei dati inattivi aiuta a ridurre il sovraccarico operativo e la complessità associati alla protezione dei dati sensibili. Allo stesso tempo, consente di creare applicazioni sicure che soddisfano la rigorosa conformità alla crittografia e i requisiti normativi.

AWS Ground Station applica la crittografia a tutti i dati sensibili archiviati, tuttavia, per alcune AWS Ground Station risorse, come le effemeridi, puoi scegliere di utilizzare una chiave gestita dal cliente al posto delle chiavi gestite predefinite. AWS

- Chiavi gestite dal cliente: AWS Ground Station supporta l'uso di una chiave simmetrica gestita dal cliente che è possibile creare, possedere e gestire al posto della crittografia di proprietà esistente. AWS Avendo il pieno controllo di questo livello di crittografia, è possibile eseguire operazioni quali:
  - Stabilire e mantenere le policy delle chiavi
  - Stabilire e mantenere le policy e le sovvenzioni IAM
  - Abilitare e disabilitare le policy delle chiavi
  - Ruotare i materiali crittografici delle chiavi
  - Aggiungere tag
  - Creare alias delle chiavi
  - Pianificare l'eliminazione delle chiavi

Per ulteriori informazioni, consulta la chiave gestita dal cliente nella Guida per gli AWS Key Management Service sviluppatori.

La tabella seguente riepiloga le risorse per le quali è AWS Ground Station supportato l'uso di Customer Managed Keys

Tipo di dati	AWS crittografia a chiave proprietaria	Crittografia con chiavi gestite dal cliente (opzionale)
Dati sulle effemeridi utilizzati per calcolare la traiettoria di un satellite	Abilitato	Abilitato
Effemeridi di elevazion e azimutale utilizzate per comandare le antenne	Abilitato	Abilitato

> **Note**
>
> AWS Ground Station abilita automaticamente la crittografia dei dati archiviati Chiavi di proprietà di AWS per proteggere gratuitamente i dati di identificazione personale. Tuttavia, l'utilizzo di una chiave gestita dal cliente comporta dei AWS KMS costi. Per ulteriori informazioni sui prezzi, consulta i AWS Key Management Service prezzi.
> Per ulteriori informazioni su AWS KMS, consulta la Guida per AWS Key Management Service gli sviluppatori.

Per informazioni specifiche su ciascun tipo di risorsa, consulta:

- Crittografia a riposo per dati effemeridi TLE e OEM
- Crittografia a riposo per effemeridi di elevazione dell'azimut

Creazione di una chiave gestita dal cliente

È possibile creare una chiave simmetrica gestita dal cliente utilizzando Console di gestione AWS, o il. AWS KMS APIs

Per creare una chiave simmetrica gestita dal cliente

Segui i passaggi per creare una chiave simmetrica gestita dal cliente nella Guida per gli sviluppatori.AWS Key Management Service

Panoramica delle politiche chiave

Le policy della chiave controllano l'accesso alla chiave gestita dal cliente. Ogni chiave gestita dal cliente deve avere esattamente una policy della chiave, che contiene istruzioni che determinano chi può usare la chiave e come la possono usare. Quando crei la chiave gestita dal cliente, è possibile specificare una policy della chiave. Per ulteriori informazioni, consulta Gestire l'accesso alle chiavi gestite dal cliente nella Guida per gli AWS Key Management Service sviluppatori.

Per utilizzare la chiave gestita dal cliente con AWS Ground Station le risorse, è necessario configurare la politica chiave per concedere le autorizzazioni appropriate al AWS Ground Station servizio. Le autorizzazioni specifiche e la configurazione delle policy dipendono dal tipo di risorsa che stai crittografando:

- Per i dati sulle effemeridi TLE e OEM, consulta la sezione dedicata ai requisiti ed esempi Crittografia a riposo per dati effemeridi TLE e OEM di policy chiave specifici.
- Per i dati sulle effemeridi di elevazione azimutale, consulta la sezione dedicata ai requisiti ed esempi specifici relativi alle politiche chiave. Crittografia a riposo per effemeridi di elevazione dell'azimut

> **Note**
>
> La configurazione delle politiche chiave differisce tra i tipi di effemeridi. I dati sulle effemeridi TLE e OEM utilizzano le concessioni per l'accesso con chiave, mentre le effemeridi di elevazione azimutale utilizzano le autorizzazioni delle policy chiave dirette. Assicurati di configurare la politica delle chiavi in base al tipo di risorsa specifico che stai crittografando.

Per ulteriori informazioni sulla specificazione delle autorizzazioni in una politica e sulla risoluzione dei problemi di accesso tramite chiave, consulta la Guida per gli AWS Key Management Service sviluppatori.

Specificazione di una chiave gestita dal cliente per AWS Ground Station

È possibile specificare una chiave gestita dal cliente per crittografare le seguenti risorse:

- Effemeridi (TLE, OEM e elevazione azimutale)

Quando si crea una risorsa, è possibile specificare la chiave dati fornendo un kmsKeyArn

- kmsKeyArn- Un identificatore chiave per una chiave gestita AWS KMS dal cliente

AWS Ground Station contesto di crittografia

Un contesto di crittografia è un insieme opzionale di coppie chiave-valore che contengono informazioni contestuali aggiuntive sui dati. AWS KMS utilizza il contesto di crittografia come dati autenticati aggiuntivi per supportare la crittografia autenticata. Quando includi un contesto di crittografia in una richiesta di crittografia dei dati, AWS KMS associa il contesto di crittografia ai dati crittografati. Per decrittografare i dati, nella richiesta deve essere incluso lo stesso contesto di crittografia.

AWS Ground Station utilizza un contesto di crittografia diverso a seconda della risorsa da crittografare e specifica un contesto di crittografia specifico per ogni concessione di chiave creata.

Per i dettagli del contesto di crittografia specifico della risorsa, consulta:

- Crittografia a riposo per dati effemeridi TLE e OEM
- Crittografia a riposo per effemeridi di elevazione dell'azimut

Crittografia a riposo per dati effemeridi TLE e OEM

Requisiti politici chiave per le effemeridi TLE e OEM

Per utilizzare una chiave gestita dal cliente con dati sulle effemeridi, la policy chiave deve concedere le seguenti autorizzazioni al servizio: AWS Ground Station

- `kms:CreateGrant`- Crea una concessione di accesso su una chiave gestita dal cliente. Concede AWS Ground Station l'accesso per eseguire operazioni di concessione sulla chiave gestita dal cliente per la lettura e l'archiviazione di dati crittografati.
- `kms:DescribeKey`- Fornisce i dettagli della chiave gestita dal cliente AWS Ground Station per consentire la convalida della chiave prima di tentare di utilizzare la chiave fornita.

Per ulteriori informazioni sull'utilizzo di Grants, consulta la AWS Key Management Service Guida per gli sviluppatori.

Autorizzazioni utente IAM per la creazione di effemeridi con chiavi gestite dal cliente

Quando AWS Ground Station utilizza una chiave gestita dal cliente nelle operazioni crittografiche, agisce per conto dell'utente che crea la risorsa effemeridi.

Per creare una risorsa effemeridi utilizzando una chiave gestita dal cliente, un utente deve disporre delle autorizzazioni per eseguire le seguenti operazioni sulla chiave gestita dal cliente:

- `kms:CreateGrant`- Consente all'utente di creare concessioni sulla chiave gestita dal cliente per conto di. AWS Ground Station
- `kms:DescribeKey`- Consente all'utente di visualizzare i dettagli della chiave gestita dal cliente per convalidare la chiave.

Puoi specificare queste autorizzazioni necessarie in una policy chiave o in una policy IAM se la policy chiave lo consente. Queste autorizzazioni garantiscono che gli utenti possano autorizzarsi AWS Ground Station a utilizzare la chiave gestita dal cliente per le operazioni di crittografia per loro conto.

Come AWS Ground Station utilizza le sovvenzioni per le effemeridi AWS KMS

AWS Ground Station richiede una concessione chiave per utilizzare la chiave gestita dal cliente.

Quando carichi un'effemeride crittografata con una chiave gestita dal cliente, AWS Ground Station crea una concessione di chiave per tuo conto inviando una richiesta a. CreateGrant AWS KMS Le sovvenzioni AWS KMS vengono utilizzate per AWS Ground Station consentire l'accesso a una AWS KMS chiave nel tuo account.

Questo permette di AWS Ground Station fare quanto segue:

- Chiama GenerateDataKey per generare una chiave dati crittografata e archiviarla, poiché la chiave dati non viene utilizzata immediatamente per crittografare.

- Chiama Decrypt per utilizzare la chiave dati crittografata memorizzata per accedere ai dati crittografati.
- Chiama Encrypt per utilizzare la chiave dati per crittografare i dati.
- Configurare un principale ritirato per consentire al servizio di RetireGrant.

Puoi revocare l'accesso alla concessione in qualsiasi momento. Se lo fai, non AWS Ground Station sarai in grado di accedere a nessuno dei dati crittografati dalla chiave gestita dal cliente, il che influirà sulle operazioni che dipendono da tali dati. Ad esempio, se rimuovi una chiave concessa da un'effemeride attualmente in uso per un contatto, non AWS Ground Station sarà possibile utilizzare i dati sulle effemeridi forniti per puntare l'antenna durante il contatto. Ciò farà sì che il contatto finisca in uno stato NON RIUSCITO.

Contesto di crittografia Ephemeris

Le principali concessioni per la crittografia delle risorse effemeridi sono vincolate a un ARN satellitare specifico.

```
"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**
>
> Le concessioni chiave vengono riutilizzate per la stessa coppia chiave-satellite.

Utilizzo del contesto di crittografia per il monitoraggio

Quando si utilizza una chiave simmetrica gestita dal cliente per crittografare le effemeridi, è inoltre possibile utilizzare il contesto di crittografia nei record e nei registri di controllo per identificare come viene utilizzata la chiave gestita dal cliente. Il contesto di crittografia appare anche nei log generati da AWS CloudTrail o Amazon CloudWatch Logs.

Utilizzo del contesto di crittografia per controllare l'accesso alla chiave gestita dal cliente

È possibile utilizzare il contesto di crittografia nelle policy delle chiavi e nelle policy IAM come `conditions` per controllare l'accesso alla chiave simmetrica gestita dal cliente. È possibile utilizzare i vincoli del contesto di crittografia in una concessione.

AWS Ground Station utilizza un vincolo di contesto di crittografia nelle concessioni per controllare l'accesso alla chiave gestita dal cliente nel tuo account o nella tua regione. Il vincolo della concessione richiede che le operazioni consentite dalla concessione utilizzino il contesto di crittografia specificato.

Di seguito sono riportati alcuni esempi di istruzioni delle policy della chiave per concedere l'accesso a una chiave gestita dal cliente per un contesto di crittografia specifico. Questa istruzione della policy impone come condizione che le concessioni abbiano un vincolo che specifica il contesto di crittografia.

L'esempio seguente mostra una politica chiave per i dati sulle effemeridi associati a un satellite:

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"
                }
            }
        }
    ]
}
```

Monitoraggio delle chiavi di crittografia per verificare la presenza di effemeridi

Quando utilizzi una chiave gestita AWS Key Management Service dal cliente con le tue risorse effemeridi, puoi utilizzare CloudWatch i log di AWS CloudTrailAmazon per tenere traccia delle richieste inviate a. AWS Ground Station AWS KMS Gli esempi seguenti sono CloudTrail eventi per CreateGrantGenerateDataKey, Decrypt e per monitorare AWS KMS le operazioni richieste per accedere DescribeKey AWS Ground Station ai dati crittografati dalla chiave gestita dal cliente.

CreateGrant

Quando utilizzi una chiave gestita AWS KMS dal cliente per crittografare le tue risorse effemeridi, AWS Ground Station invia una CreateGrantrichiesta per tuo conto per accedere alla chiave del tuo account. AWS KMS AWS La concessione che AWS Ground Station crea è specifica per la risorsa associata alla chiave gestita dal AWS KMS cliente. Inoltre, AWS Ground Station utilizza l'RetireGrantoperazione per rimuovere una concessione quando si elimina una risorsa.

L'evento di esempio seguente registra l'CreateGrantoperazione per un'effemeride:

```
{
    "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

Quando utilizzi una chiave gestita AWS KMS dal cliente per crittografare le tue risorse di effemeridi, AWS Ground Station invia una DescribeKeyrichiesta per tuo conto per verificare che la chiave richiesta esista nel tuo account.

L'evento di esempio seguente registra l'operazione 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

Quando utilizzi una chiave gestita AWS KMS dal cliente per crittografare le tue risorse di effemeridi, AWS Ground Station invia una GenerateDataKeyrichiesta a per generare una chiave dati con cui crittografare i tuoi dati.

L'evento di esempio seguente registra l'operazione per un'effemeride GenerateDataKey:


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2022-02-22T22:22:22Z",
```

```
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keySpec": "AES_256",
        "encryptionContext": {
            "aws:groundstation:arn":
 "arn:aws:groundstation::111122223333:satellite/00a770b0-082d-45a4-80ed-SAMPLE",
            "aws:s3:arn":
 "arn:aws:s3:::customerephemerisbucket/0034abcd-12ab-34cd-56ef-123456SAMPLE"
        },
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "sharedEventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventCategory": "Management"
}
```


Decrypt

Quando si utilizza una chiave gestita AWS KMS dal cliente per crittografare le risorse di effemeridi, AWS Ground Station utilizza l'operazione Decrypt per decrittografare le effemeridi fornite se sono già crittografate con la stessa chiave gestita dal cliente. Ad esempio, se un'effemeride viene caricata da un bucket S3 e viene crittografata in quel bucket con una determinata chiave.

L'evento di esempio seguente registra l'operazione Decrypt per un'effemeride:


```
{
    "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"
}
```

Crittografia a riposo per effemeridi di elevazione dell'azimut

Requisiti politici chiave per le effemeridi di elevazione dell'azimut

Per utilizzare una chiave gestita dal cliente con dati sulle effemeridi di elevazione dell'azimut, la politica chiave deve concedere le seguenti autorizzazioni al servizio. AWS Ground Station A differenza dei dati sulle effemeridi TLE e OEM che utilizzano concessioni, le effemeridi di elevazione azimutale utilizzano autorizzazioni basate su criteri a chiave diretta per le operazioni di crittografia. Si tratta di un metodo più semplice per gestire le autorizzazioni e utilizzare le chiavi.

- `kms:GenerateDataKey`- Genera chiavi di dati per crittografare i dati sulle effemeridi di elevazione azimutale.
- `kms:Decrypt`- Decripta le chiavi dati crittografate quando si accede ai dati sulle effemeridi di elevazione dell'azimut.

Esempio di politica chiave che concede l'accesso a una chiave gestita dal cliente AWS Ground Station

> **Note**
>
> Con le effemeridi di elevazione azimutale, è necessario configurare queste autorizzazioni direttamente nella policy chiave. Al responsabile del AWS Ground Station servizio regionale (ad esempio`groundstation.`*`region`*`.amazonaws.com`) devono essere concesse queste autorizzazioni nelle dichiarazioni politiche chiave. Senza queste istruzioni aggiunte alla policy chiave non AWS Ground Station sarà possibile memorizzare o accedere alle effemeridi di elevazione azimutale personalizzate.

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": "*"
        }
    ]
}
```

Autorizzazioni utente IAM per la creazione di effemeridi di elevazione azimutale con chiavi gestite dal cliente

Quando AWS Ground Station utilizza una chiave gestita dal cliente nelle operazioni crittografiche, agisce per conto dell'utente che sta creando la risorsa sulle effemeridi di elevazione dell'azimut.

Per creare una risorsa di effemeridi di elevazione azimutale utilizzando una chiave gestita dal cliente, un utente deve disporre delle autorizzazioni per eseguire le seguenti operazioni sulla chiave gestita dal cliente:

- `kms:GenerateDataKey`- Consente all'utente di generare chiavi di dati per crittografare i dati sulle effemeridi di elevazione azimutale.
- `kms:Decrypt`- Consente all'utente di decrittografare le chiavi di dati quando accede ai dati delle effemeridi di elevazione dell'azimut.
- `kms:DescribeKey`- Consente all'utente di visualizzare i dettagli delle chiavi gestite dal cliente per convalidare la chiave.

Puoi specificare queste autorizzazioni necessarie in una policy chiave o in una policy IAM se la policy chiave lo consente. Queste autorizzazioni garantiscono che gli utenti possano autorizzarsi AWS Ground Station a utilizzare la chiave gestita dal cliente per le operazioni di crittografia per loro conto.

Come AWS Ground Station utilizza le politiche chiave per le effemeridi di elevazione dell'azimut

Quando fornisci dati sulle effemeridi di elevazione dell'azimut con una chiave gestita dal cliente, utilizza politiche chiave per accedere alla tua chiave di crittografia. AWS Ground Station Le autorizzazioni vengono concesse direttamente tramite dichiarazioni politiche chiave anziché AWS Ground Station tramite concessioni come nel caso dei dati sulle effemeridi TLE o OEM.

Se rimuovi AWS Ground Station l'accesso alla chiave gestita dal cliente, non AWS Ground Station sarai in grado di accedere a nessuno dei dati crittografati da quella chiave, il che influirà sulle operazioni che dipendono da quei dati. Ad esempio, se rimuovi le autorizzazioni chiave relative alle effemeridi di elevazione azimutale attualmente utilizzate per un contatto, non AWS Ground Station sarà possibile utilizzare i dati di elevazione azimutale forniti per comandare l'antenna durante il contatto. Ciò farà sì che il contatto finisca in uno stato NON RIUSCITO.

Contesto di crittografia delle effemeridi di elevazione azimutale

Quando AWS Ground Station utilizza la AWS KMS chiave per crittografare i dati sulle effemeridi di elevazione azimutale, il servizio specifica un contesto di crittografia. Il contesto di crittografia è costituito da dati autenticati aggiuntivi (AAD) utilizzati per garantire l'integrità dei dati. AWS KMS Quando viene specificato un contesto di crittografia per un'operazione di crittografia, il servizio deve specificare lo stesso contesto di crittografia per l'operazione di decrittografia. In caso contrario, la decrittografia ha esito negativo. Il contesto di crittografia viene inoltre scritto CloudTrail nei log per aiutarti a capire perché è stata utilizzata una determinata AWS KMS chiave. CloudTrail I registri possono contenere molte voci che descrivono l'uso di una AWS KMS chiave, ma il contesto di crittografia in ogni voce di registro può aiutarti a determinare il motivo di quel particolare utilizzo.

AWS Ground Station specifica il seguente contesto di crittografia quando esegue operazioni crittografiche con la chiave gestita dal cliente su un'effemeride di elevazione azimutale:

```
{
    "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"
    }
}
```

Il contesto di crittografia contiene:

`aws:groundstation:ground-station-id`

Il nome della stazione terrestre associata alle effemeridi di elevazione azimutale.

aws: stazione di terra: arn

L'ARN della risorsa effemeridi.

aws: s3: arn

L'ARN delle effemeridi archiviato in Amazon S3.

Utilizzo del contesto di crittografia per controllare l'accesso alla chiave gestita dal cliente

Puoi utilizzare le istruzioni condizionali IAM per controllare l' AWS Ground Station accesso alla chiave gestita dal cliente. L'aggiunta di una dichiarazione di condizione `kms:Decrypt` alle azioni `kms:GenerateDataKey` and limita le stazioni di terra a che AWS KMS possono essere utilizzate.

Di seguito sono riportati alcuni esempi di dichiarazioni politiche chiave per concedere AWS Ground Station l'accesso alla chiave gestita dal cliente in una regione specifica per una stazione di terra specifica. La condizione contenuta in questa dichiarazione di politica richiede che tutti crittografino e decrittografino l'accesso alla chiave che specifica un contesto di crittografia che corrisponda alla condizione della politica di chiave.

Esempio di politica chiave che concede AWS Ground Station l'accesso a una chiave gestita dal cliente per una stazione di terra specifica

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"
                }
            }
        }
    ]
}
```

Esempio di politica chiave che garantisce AWS Ground Station l'accesso a una chiave gestita dal cliente per più stazioni terrestri

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"
                    ]
                }
            }
        }
    ]
}
```

Monitoraggio delle chiavi di crittografia per le effemeridi di elevazione azimutale

Quando utilizzi una chiave gestita AWS KMS dal cliente con le tue risorse sulle effemeridi di elevazione azimutale, puoi utilizzare o i log per tenere traccia delle richieste inviate a. CloudTrail CloudWatch AWS Ground Station AWS KMS Gli esempi seguenti sono CloudTrail Events for GenerateDataKeyand Decrypt per monitorare AWS KMS le operazioni richiamate per accedere AWS Ground Station ai dati crittografati dalla chiave gestita dal cliente.

GenerateDataKey

Quando si utilizza una chiave gestita AWS KMS dal cliente per crittografare le risorse relative alle effemeridi di elevazione azimutale, AWS Ground Station invia una GenerateDataKeyrichiesta AWS KMS a per generare una chiave dati con cui crittografare i dati.

L'evento di esempio seguente registra l'operazione per le effemeridi di elevazione dell'azimut: 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

Quando si utilizza una chiave gestita AWS KMS dal cliente per crittografare le risorse di effemeridi di elevazione azimutale, AWS Ground Station utilizza l'operazione Decrypt per decrittografare i dati sulle effemeridi di elevazione azimutale forniti se sono già crittografati con la stessa chiave gestita dal cliente.

L'evento di esempio seguente registra l'operazione Decrypt per le effemeridi di elevazione azimutale:

```
{
    "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"
}
```

Crittografia dei dati durante il transito per AWS Ground Station

AWS Ground Station fornisce la crittografia per impostazione predefinita per proteggere i dati sensibili durante il transito. I dati possono essere trasmessi tra le postazioni delle AWS Ground Station antenne e le istanze Amazon EC2 in due modi, a seconda della configurazione del profilo di missione.

- AWS Ground Station Agente
- Endpoint del flusso di dati

Ogni metodo di streaming dei dati gestisce la crittografia dei dati in transito in modo diverso. Le sezioni seguenti descrivono questi tre metodi.

AWS Ground Station Stream degli agenti

AWS Ground Station L'agente crittografa i propri flussi utilizzando chiavi gestite dal cliente. AWS KMS L' AWS Ground Station agente in esecuzione sulla tua istanza Amazon EC2 decrittograferà automaticamente il flusso per fornire dati decrittografati.

La AWS KMS chiave utilizzata per crittografare uno stream viene specificata durante la creazione di un parametro. `MissionProfile` streamsKmsKey Tutte le autorizzazioni che garantiscono AWS Ground Station l'accesso alle chiavi vengono gestite tramite la politica delle AWS KMS chiavi allegata a. `streamsKmsKey`

Stream degli endpoint Dataflow

I flussi degli endpoint Dataflow sono crittografati utilizzando Datagram Transport Layer Security (DTLS). Questa operazione viene eseguita utilizzando certificati autofirmati e non richiede una configurazione aggiuntiva.

Esempi di configurazioni del profilo di missione

Gli esempi forniti mostrano come prendere un satellite di trasmissione pubblica e creare un profilo di missione che lo supporti. I modelli risultanti vengono forniti per aiutarvi a stabilire un contatto via satellite per le trasmissioni pubbliche e per aiutarvi a prendere decisioni sui vostri satelliti.

Argomenti

JPSS-1 - Trasmissione pubblica via satellite (PBS) - Valutazione

Questa sezione di esempio corrisponde a. Panoramica del processo di onboarding dei clienti Fornisce una breve analisi di compatibilità con AWS Ground Station e pone le basi per gli esempi specifici che seguono.

Come indicato nella Satelliti di trasmissione pubblici sezione, è possibile utilizzare satelliti selezionati, o percorsi di comunicazione di un satellite, disponibili al pubblico. In questa sezione descriviamo JPSS-1 nei termini. AWS Ground Station Come riferimento, utilizziamo lo Spacecraft High Rate Data (HRD) del Joint Polar Satellite System 1 (JPSS-1) to Direct Broadcast Stations (DBS) Radio Frequency (RF) Interface Control Document (ICD) per completare l'esempio. Inoltre, vale la pena notare che JPSS-1 è associato al NORAD ID 43013.

Il satellite JPSS-1 offre un percorso di comunicazione in uplink e tre percorsi di comunicazione diretti in downlink, come illustrato nella Figura 1-1 dell'ICD. Di questi quattro percorsi di comunicazione, solo il percorso di comunicazione downlink High Rate Data (HRD) è disponibile per il consumo pubblico. In base a ciò, vedrai che a questo percorso saranno associati anche dati molto più specifici. I quattro percorsi sono i seguenti:

- Percorso di comando (uplink) a una frequenza MHz centrale di 2067,27 con una velocità dati di 2-128 kbps. Questo percorso non è accessibile pubblicamente.

- Percorso di telemetria (downlink) a una frequenza MHz centrale di 2247,5 con una velocità dati di 1-524 kbps. Questo percorso non è accessibile al pubblico.
- Percorso SMD (downlink) alla frequenza GHz centrale 26,7034 con una velocità dati di 150-300 Mbps. Questo percorso non è accessibile al pubblico.
- La RF per il percorso HRD (downlink) alla frequenza MHz centrale 7812 con una velocità dati di 15 Mbps. Ha una larghezza di banda di 30 MHz e lo è. right-hand-circular-polarized Quando si effettua l'accesso a JPSS-1 con AWS Ground Station, questo è il percorso di comunicazione a cui si ha accesso. Questo percorso di comunicazione contiene dati scientifici sugli strumenti, dati di ingegneria degli strumenti, dati di telemetria degli strumenti e dati di pulizia dei veicoli spaziali in tempo reale.

Confrontando i potenziali percorsi di dati, vediamo che i percorsi di comando (uplink), telemetria (downlink) e HRD (downlink) soddisfano le capacità di frequenza, larghezza di banda e utilizzo simultaneo multicanale di. AWS Ground Station Il percorso SMD non è compatibile in quanto la frequenza centrale non è compresa nell'intervallo dei ricevitori esistenti. Per ulteriori informazioni sulle funzionalità supportate, vedere. AWS Ground Station Funzionalità del sito

> **Note**
>
> Poiché il percorso SMD non è compatibile con AWS Ground Station esso, non verrà rappresentato nelle configurazioni di esempio.

> **Note**
>
> Poiché i percorsi di comando (uplink) e telemetria (downlink) non sono definiti nell'ICD, né sono disponibili per l'uso pubblico, i valori forniti quando vengono utilizzati sono fittizi.

Trasmissione satellitare pubblica che utilizza la distribuzione di dati Amazon S3

Questo esempio si basa sull'analisi effettuata nella JPSS-1 - Trasmissione pubblica via satellite (PBS) - Valutazione sezione della guida per l'utente.

Per questo esempio, è necessario ipotizzare uno scenario: si desidera acquisire il percorso di comunicazione HRD come frequenza intermedia digitale e memorizzarlo per future elaborazioni in batch. Ciò consente di salvare i campioni grezzi in quadratura (I/Q) in radiofrequenza (RF) in fase dopo la digitalizzazione. Una volta che i dati sono nel tuo bucket Amazon S3, puoi demodularli e decodificarli utilizzando qualsiasi software desideri. Consulta il MathWorks tutorial per un esempio dettagliato di elaborazione. Dopo aver utilizzato questo esempio, potresti prendere in considerazione l'aggiunta di componenti di Amazon EC2 Spot Pricing per elaborare i dati e ridurre i costi complessivi di elaborazione.

Percorsi di comunicazione

Questa sezione rappresenta una Pianifica i percorsi di comunicazione del flusso di dati guida introduttiva.

Tutti i seguenti frammenti di modello appartengono alla sezione Risorse del CloudFormation modello.

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

> **Note**
>
> Per ulteriori informazioni sul contenuto di un CloudFormation modello, consulta le sezioni relative ai modelli.

Considerando il nostro scenario di fornitura di un unico percorso di comunicazione ad Amazon S3, sai che disporrai di un unico percorso di distribuzione asincrono. Distribuzione asincrona dei datiIn base alla sezione, è necessario definire un bucket 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]]]]]]
```

Inoltre, dovrai creare i ruoli e le politiche appropriati per consentire l'utilizzo del AWS Ground Station 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 configurazioni

Questa sezione rappresenta Crea configurazioni come iniziare.

Avrai bisogno di un tracking-config per impostare le tue preferenze sull'uso dell'autotrack. La selezione di PREFERRED come autotrack può migliorare la qualità del segnale, ma non è necessario soddisfare la qualità del segnale perché la qualità delle effemeridi JPSS-1 è sufficiente.

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

In base al percorso di comunicazione, dovrai definire una configurazione antenna-downlink per rappresentare la parte satellitare e una registrazione s3 per fare riferimento al bucket Amazon S3 che hai appena creato.

```
 # 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 profilo della missione

Questa sezione rappresenta una Crea un profilo di missione guida introduttiva.

Ora che hai le configurazioni associate, puoi usarle per costruire il flusso di dati. Utilizzerai le impostazioni predefinite per i parametri rimanenti.

```
 # 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
```

Mettendolo insieme

Con le risorse di cui sopra, ora avete la possibilità di pianificare i contatti JPSS-1 per la consegna asincrona dei dati da qualsiasi dispositivo integrato. AWS Ground Station AWS Ground Station Sedi

Di seguito è riportato un CloudFormation modello completo che include tutte le risorse descritte in questa sezione combinate in un unico modello che può essere utilizzato direttamente. CloudFormation

Il CloudFormation modello denominato `AquaSnppJpss-1TerraDigIfS3DataDelivery.yml` contiene un bucket Amazon S3 e AWS Ground Station le risorse necessarie per pianificare i contatti e ricevere dati di trasmissione diretta di segnale/IP VITA-49.

Se Aqua, SNPP, JPSS-1/NOAA-20 e Terra non sono integrati nel tuo account, vedi. Satellite a bordo

> **Note**
>
> Puoi accedere al modello accedendo al bucket Amazon S3 per l'onboarding del cliente utilizzando credenziali valide. AWS I collegamenti seguenti utilizzano un bucket Amazon S3 regionale. Modifica il codice `us-west-2` regionale per rappresentare la regione corrispondente in cui desideri creare lo CloudFormation stack.
> Inoltre, le seguenti istruzioni utilizzano YAML. Tuttavia, i modelli sono disponibili sia in formato YAML che JSON. Per usare JSON, sostituisci l'estensione del `.yml` file con `.json` quando scarichi il modello.

Per scaricare il modello utilizzando AWS CLI, usa il seguente comando:

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

È possibile scaricare e visualizzare il modello nella console spostandosi all'URL seguente nel browser:

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

È possibile specificare il modello direttamente CloudFormation utilizzando il seguente link:

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

Trasmissione satellitare pubblica che utilizza un endpoint di flusso di dati (banda stretta)

Questo esempio si basa sull'analisi effettuata nella sezione della guida per l'utente. JPSS-1 - Trasmissione pubblica via satellite (PBS) - Valutazione

Per completare questo esempio, devi ipotizzare uno scenario: desideri acquisire il percorso di comunicazione HRD come frequenza intermedia digitale (DigiF) ed elaborarlo così come viene ricevuto da un'applicazione endpoint dataflow su un'istanza Amazon utilizzando un SDR. EC2

Percorsi di comunicazione

Questa sezione rappresenta una Pianifica i percorsi di comunicazione del flusso di dati guida introduttiva. Per questo esempio, creerai due sezioni nel tuo CloudFormation modello: le sezioni Parametri e Risorse.

> **Note**
>
> Per ulteriori informazioni sul contenuto di un CloudFormation modello, consulta Sezioni relative ai modelli.

Nella sezione Parametri, aggiungerai i seguenti parametri. Specificherai i valori per questi quando creerai lo stack tramite la CloudFormation console.

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

  ReceiverAMI:
```

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

> **Note**
>
> Devi creare una key pair e fornire il nome per il EC2 `EC2Key` parametro Amazon. Vedi Creare una coppia di key pair per la tua EC2 istanza Amazon.
> Inoltre, dovrai fornire l'ID AMI specifico della regione corretto al momento della creazione dello CloudFormation stack. Per informazioni, consulta AWS Ground Station Immagini di macchine Amazon (AMIs).

I frammenti di modello rimanenti appartengono alla sezione Risorse del modello. CloudFormation

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

Considerando lo scenario in cui prevediamo di fornire un unico percorso di comunicazione a un' EC2 istanza, disporrete di un unico percorso di consegna sincrono. Distribuzione sincrona dei datiIn base alla sezione, devi configurare un' EC2 istanza Amazon con un'applicazione endpoint dataflow e creare uno o più gruppi di endpoint dataflow.

```
  # 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
```

Inoltre, dovrai anche creare le politiche e i ruoli appropriati AWS Ground Station per consentire la creazione di un'elastic network interface (ENI) nel tuo account.

```
  # 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 configurazioni

Questa sezione rappresenta Crea configurazioni come iniziare.

Avrai bisogno di un tracking-config per impostare le tue preferenze sull'uso dell'autotrack. La selezione di PREFERRED come autotrack può migliorare la qualità del segnale, ma non è necessario soddisfare la qualità del segnale perché la qualità delle effemeridi JPSS-1 è sufficiente.

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

In base al percorso di comunicazione, è necessario definire una configurazione antenna-downlink per rappresentare la parte satellitare, nonché una configurazione dataflow-endpoint per fare riferimento al gruppo di endpoint dataflow che definisce i dettagli dell'endpoint.

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

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

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

AWS Ground Station profilo della missione

Questa sezione rappresenta una Crea un profilo di missione guida introduttiva.

Ora che hai le configurazioni associate, puoi usarle per costruire il flusso di dati. Utilizzerai le impostazioni predefinite per i parametri rimanenti.

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

Mettendolo insieme

Con le risorse di cui sopra, ora avete la possibilità di pianificare i contatti JPSS-1 per la consegna sincrona dei dati da qualsiasi dispositivo integrato. AWS Ground Station AWS Ground Station Sedi

Di seguito è riportato un CloudFormation modello completo che include tutte le risorse descritte in questa sezione combinate in un unico modello che può essere utilizzato direttamente. CloudFormation

Il CloudFormation modello denominato `AquaSnppJpssTerraDigIF.yml` è progettato per darti un accesso rapido per iniziare a ricevere dati digitalizzati a frequenza intermedia (DigiF) per i satelliti Aqua, SNPP, JPSS-1/NOAA-20 e Terra. Contiene un' EC2 istanza Amazon e le CloudFormation risorse necessarie per ricevere dati di trasmissione diretta DigiF non elaborati.

Se Aqua, SNPP, JPSS-1/NOAA-20 e Terra non sono presenti nel tuo account, consulta. Satellite a bordo

> **Note**
>
> Puoi accedere al modello accedendo al bucket Amazon S3 per l'onboarding del cliente utilizzando credenziali valide. AWS I collegamenti seguenti utilizzano un bucket Amazon S3 regionale. Modifica il codice `us-west-2` regionale per rappresentare la regione corrispondente in cui desideri creare lo CloudFormation stack.
> Inoltre, le seguenti istruzioni utilizzano YAML. Tuttavia, i modelli sono disponibili sia in formato YAML che JSON. Per usare JSON, sostituisci l'estensione del `.yml` file con `.json` quando scarichi il modello.

Per scaricare il modello utilizzando AWS CLI, usa il seguente comando:

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

È possibile scaricare e visualizzare il modello nella console spostandosi all'URL seguente nel browser:

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

È possibile specificare il modello direttamente CloudFormation utilizzando il seguente link:

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

Quali risorse aggiuntive definisce il modello?

Il `AquaSnppJpssTerraDigIF` modello include le seguenti risorse aggiuntive:

- (Facoltativo) CloudWatch Event Triggers: AWS Lambda funzione che viene attivata utilizzando CloudWatch gli eventi inviati AWS Ground Station prima e dopo un contatto. La AWS Lambda funzione avvierà e, facoltativamente, interromperà l'istanza del ricevitore.
- (Facoltativo) EC2 Verifica per i contatti: l'opzione di utilizzare Lambda per configurare un sistema di verifica delle EC2 istanze Amazon per i contatti con notifica SNS. È importante notare che ciò potrebbe comportare costi a seconda dell'utilizzo corrente.
- Ground Station Amazon Machine Image Retrieval Lambda: l'opzione per selezionare il software installato nell'istanza e l'AMI preferita. Le opzioni software includono e. `DDX 2.6.2 Only` `DDX 2.6.2 with qRadio 3.6.0` Queste opzioni continueranno ad espandersi man mano che verranno rilasciati aggiornamenti e funzionalità software aggiuntivi.
- Profili di missione aggiuntivi: profili di missione per altri satelliti di trasmissione pubblica (Aqua, SNPP e Terra).
- Configurazioni antenna-downlink aggiuntive - Configurazioni downlink dell'antenna per altri satelliti di trasmissione pubblica (Aqua, SNPP e Terra).

I valori e i parametri per i satelliti in questo modello sono già popolati. Questi parametri ne facilitano l'uso immediato con questi satelliti. AWS Ground Station Non è necessario configurare i propri valori per utilizzarli AWS Ground Station quando si utilizza questo modello. Tuttavia, è possibile personalizzare i valori in modo che il modello funzioni per il caso d'uso.

Dove ricevo i miei dati?

Il gruppo endpoint del flusso di dati è configurato per utilizzare l'interfaccia di rete dell'istanza del ricevitore creata come parte del modello. L'istanza del ricevitore utilizza un'applicazione dataflow endpoint per ricevere il flusso di dati dalla AWS Ground Station porta definita dall'endpoint dataflow. Una volta ricevuti, i dati sono disponibili per il consumo tramite la porta UDP 50000 sull'adattatore di loopback dell'istanza del ricevitore. Per ulteriori informazioni sulla configurazione di un gruppo di endpoint dataflow, consulta. AWS::GroundStation::DataflowEndpointGroup

Trasmissione satellitare pubblica che utilizza un endpoint di flusso di dati (demodulato e decodificato)

Questo esempio si basa sull'analisi effettuata nella sezione della guida per l'utente. JPSS-1 - Trasmissione pubblica via satellite (PBS) - Valutazione

Per completare questo esempio, è necessario ipotizzare uno scenario: si desidera acquisire il percorso di comunicazione HRD come dati di trasmissione diretta demodulati e decodificati utilizzando un endpoint di flusso di dati. Questo esempio è un buon punto di partenza se prevedi di elaborare i dati utilizzando il software NASA Direct Readout Labs (RT-STPS e IPOPP).

Percorsi di comunicazione

Questa sezione rappresenta una Pianifica i percorsi di comunicazione del flusso di dati guida introduttiva. Per questo esempio, creerai due sezioni nel tuo CloudFormation modello: le sezioni Parametri e Risorse.

> **Note**
>
> Per ulteriori informazioni sul contenuto di un CloudFormation modello, consulta Sezioni relative ai modelli.

Nella sezione Parametri, aggiungerai i seguenti parametri. Specificherai i valori per questi quando creerai lo stack tramite la CloudFormation console.

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

  ReceiverAMI:
    Description: The Ground Station DDX AMI ID you want to use. Please note
 that AMIs are region specific. For instructions on how to retrieve an AMI
```

```
 see https://docs.aws.amazon.com/ground-station/latest/ug/dataflows.ec2-
configuration.html#dataflows.ec2-configuration.amis
    Type: AWS::EC2::Image::Id
```

> **Note**
>
> Devi creare una key pair e fornire il nome per il EC2 `EC2Key` parametro Amazon. Vedi Creare una coppia di key pair per la tua EC2 istanza Amazon.
> Inoltre, dovrai fornire l'ID AMI specifico della regione corretto al momento della creazione dello CloudFormation stack. Per informazioni, consulta AWS Ground Station Immagini di macchine Amazon (AMIs).

I frammenti di modello rimanenti appartengono alla sezione Risorse del modello. CloudFormation

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

Considerando lo scenario in cui prevediamo di fornire un unico percorso di comunicazione a un' EC2 istanza, disporrete di un unico percorso di consegna sincrono. Distribuzione sincrona dei datiIn base alla sezione, devi configurare un' EC2 istanza Amazon con un'applicazione endpoint dataflow e creare uno o più gruppi di endpoint dataflow.

```
  # 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
```

Avrai anche bisogno delle politiche, dei ruoli e dei profili appropriati AWS Ground Station per consentire la creazione di un'elastic network interface (ENI) nel tuo account.

```
  # 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 configurazioni

Questa sezione rappresenta la Crea configurazioni guida per l'utente.

Avrai bisogno di un tracking-config per impostare le tue preferenze sull'uso dell'autotrack. La selezione di PREFERRED come autotrack può migliorare la qualità del segnale, ma non è necessario soddisfare la qualità del segnale perché la qualità delle effemeridi JPSS-1 è sufficiente.

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

In base al percorso di comunicazione, è necessario definire una configurazione per rappresentare la parte satellitare, nonché una antenna-downlink-demod-decodeconfigurazione dataflow-endpoint per fare riferimento al gruppo di endpoint del flusso di dati che definisce i dettagli dell'endpoint.

> **Note**
>
> Per i dettagli su come impostare i valori per e, consulta. `DemodulationConfig` `DecodeConfig` Config di decodifica demodulazione downlink antenna

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

```
        AntennaDownlinkDemodDecodeConfig:
          SpectrumConfig:
            CenterFrequency:
              Value: 7812
              Units: "MHz"
            Polarization: "RIGHT_HAND"
            Bandwidth:
              Value: 30
              Units: "MHz"
          DemodulationConfig:
            UnvalidatedJSON: '{
              "type":"QPSK",
              "qpsk":{
                "carrierFrequencyRecovery":{
                  "centerFrequency":{
                    "value":7812,
                    "units":"MHz"
                  },
                  "range":{
                    "value":250,
                    "units":"kHz"
                  }
                },
                "symbolTimingRecovery":{
                  "symbolRate":{
                    "value":15,
                    "units":"Msps"
                  },
                  "range":{
                    "value":0.75,
                    "units":"ksps"
                  },
                  "matchedFilter":{
                    "type":"ROOT_RAISED_COSINE",
                    "rolloffFactor":0.5
                  }
                }
              }
            }'
          DecodeConfig:
            UnvalidatedJSON: '{
              "edges":[
                {
                  "from":"I-Ingress",
```

```
      "to":"IQ-Recombiner"
    },
    {
      "from":"Q-Ingress",
      "to":"IQ-Recombiner"
    },
    {
      "from":"IQ-Recombiner",
      "to":"CcsdsViterbiDecoder"
    },
    {
      "from":"CcsdsViterbiDecoder",
      "to":"NrzmDecoder"
    },
    {
      "from":"NrzmDecoder",
      "to":"UncodedFramesEgress"
    }
  ],
  "nodeConfigs":{
    "I-Ingress":{
      "type":"CODED_SYMBOLS_INGRESS",
      "codedSymbolsIngress":{
        "source":"I"
      }
    },
    "Q-Ingress":{
      "type":"CODED_SYMBOLS_INGRESS",
      "codedSymbolsIngress":{
        "source":"Q"
      }
    },
    "IQ-Recombiner":{
      "type":"IQ_RECOMBINER"
    },
    "CcsdsViterbiDecoder":{
      "type":"CCSDS_171_133_VITERBI_DECODER",
      "ccsds171133ViterbiDecoder":{
        "codeRate":"ONE_HALF"
      }
    },
    "NrzmDecoder":{
      "type":"NRZ_M_DECODER"
    },
```

```
              "UncodedFramesEgress":{
                "type":"UNCODED_FRAMES_EGRESS"
              }
            }
          }'
```

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

AWS Ground Station profilo della missione

Questa sezione rappresenta Crea un profilo di missione la guida per l'utente.

Ora che hai le configurazioni associate, puoi usarle per costruire il flusso di dati. Utilizzerai le impostazioni predefinite per i parametri rimanenti.

```
 # 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
```

Mettendolo insieme

Con le risorse di cui sopra, ora avete la possibilità di pianificare i contatti JPSS-1 per la consegna sincrona dei dati da qualsiasi dispositivo integrato. AWS Ground Station AWS Ground Station Sedi

Di seguito è riportato un CloudFormation modello completo che include tutte le risorse descritte in questa sezione combinate in un unico modello che può essere utilizzato direttamente. CloudFormation

Il CloudFormation modello denominato `AquaSnppJpss.yml` è progettato per darti un accesso rapido per iniziare a ricevere dati per i satelliti Aqua, SNPP e JPSS-1/NOAA-20. Contiene un' EC2 istanza Amazon e le AWS Ground Station risorse necessarie per pianificare i contatti e ricevere dati di trasmissione diretta demodulati e decodificati.

Se Aqua, SNPP, JPSS-1/NOAA-20 e Terra non sono presenti nel tuo account, consulta. Satellite a bordo

> **Note**
>
> Puoi accedere al modello accedendo al bucket Amazon S3 per l'onboarding del cliente utilizzando credenziali valide. AWS I collegamenti seguenti utilizzano un bucket Amazon S3 regionale. Modifica il codice `us-west-2` regionale per rappresentare la regione corrispondente in cui desideri creare lo CloudFormation stack.
> Inoltre, le seguenti istruzioni utilizzano YAML. Tuttavia, i modelli sono disponibili sia in formato YAML che JSON. Per usare JSON, sostituisci l'estensione del `.yml` file con `.json` quando scarichi il modello.

Per scaricare il modello utilizzando AWS CLI, usa il seguente comando:

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

È possibile scaricare e visualizzare il modello nella console spostandosi all'URL seguente nel browser:

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

È possibile specificare il modello direttamente CloudFormation utilizzando il seguente link:

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

Quali risorse aggiuntive definisce il modello?

Il `AquaSnppJpss` modello include le seguenti risorse aggiuntive:

- (Facoltativo) CloudWatch Event Triggers: AWS Lambda funzione che viene attivata utilizzando CloudWatch gli eventi inviati AWS Ground Station prima e dopo un contatto. La AWS Lambda funzione avvierà e, facoltativamente, interromperà l'istanza del ricevitore.
- (Facoltativo) EC2 Verifica per i contatti: l'opzione di utilizzare Lambda per configurare un sistema di verifica delle EC2 istanze Amazon per i contatti con notifica SNS. È importante notare che ciò potrebbe comportare costi a seconda dell'utilizzo corrente.
- Ground Station Amazon Machine Image Retrieval Lambda: l'opzione per selezionare il software installato nell'istanza e l'AMI preferita. Le opzioni software includono e. `DDX 2.6.2 Only` `DDX 2.6.2 with qRadio 3.6.0` Se desideri utilizzare DigiF Data Delivery a banda larga e l' AWS Ground Station agente, consulta. Trasmissione pubblica via satellite che utilizza AWS Ground Station Agent (banda larga) Queste opzioni continueranno ad espandersi man mano che verranno rilasciati aggiornamenti e funzionalità software aggiuntivi.
- Profili di missione aggiuntivi: profili di missione per altri satelliti di trasmissione pubblica (Aqua, SNPP e Terra).
- Configurazioni antenna-downlink aggiuntive - Configurazioni downlink dell'antenna per altri satelliti di trasmissione pubblica (Aqua, SNPP e Terra).

I valori e i parametri per i satelliti in questo modello sono già popolati. Questi parametri ne facilitano l'uso immediato con questi satelliti. AWS Ground Station Non è necessario configurare i propri valori per utilizzarli AWS Ground Station quando si utilizza questo modello. Tuttavia, è possibile personalizzare i valori in modo che il modello funzioni per il caso d'uso.

Dove ricevo i miei dati?

Il gruppo endpoint del flusso di dati è configurato per utilizzare l'interfaccia di rete dell'istanza del ricevitore creata come parte del modello. L'istanza del ricevitore utilizza un'applicazione dataflow endpoint per ricevere il flusso di dati dalla AWS Ground Station porta definita dall'endpoint dataflow. Una volta ricevuti, i dati sono disponibili per il consumo tramite la porta UDP 50000 sull'adattatore di loopback dell'istanza del ricevitore. Per ulteriori informazioni sulla configurazione di un gruppo di endpoint dataflow, consulta. AWS::GroundStation::DataflowEndpointGroup

Trasmissione pubblica via satellite che utilizza AWS Ground Station Agent (banda larga)

Questo esempio si basa sull'analisi effettuata nella JPSS-1 - Trasmissione pubblica via satellite (PBS) - Valutazione sezione della guida per l'utente.

Per completare questo esempio, è necessario ipotizzare uno scenario: si desidera acquisire il percorso di comunicazione HRD come frequenza intermedia digitale a banda larga (DigiF) ed elaborarlo così come viene ricevuto dall'agente AWS Ground Station su un'istanza Amazon utilizzando un SDR. EC2

> **Note**
>
> L'effettivo segnale del percorso di comunicazione JPSS HRD ha una larghezza di banda di 30 MHz, ma sarà necessario configurare la configurazione antenna-downlink per trattarlo come un segnale con una MHz larghezza di banda di 100 in modo che possa fluire attraverso il percorso corretto che deve essere ricevuto dall' AWS Ground Station agente per questo esempio.

Percorsi di comunicazione

Questa sezione rappresenta una Pianifica i percorsi di comunicazione del flusso di dati guida introduttiva. Per questo esempio, avrai bisogno di una sezione aggiuntiva nel tuo CloudFormation modello che non è stata utilizzata negli altri esempi, la sezione Mappature.

> **Note**
>
> Per ulteriori informazioni sul contenuto di un CloudFormation modello, consulta Sezioni relative ai modelli.

Inizierai configurando una sezione Mappature nel tuo CloudFormation modello per gli elenchi di AWS Ground Station prefissi per regione. Ciò consente di fare facilmente riferimento agli elenchi di prefissi da parte del gruppo di sicurezza delle EC2 istanze Amazon. Per ulteriori informazioni sull'utilizzo di un elenco di prefissi, consulta. Configurazione 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
```

Nella sezione Parametri, aggiungerai i seguenti parametri. Specificherai i valori per questi quando creerai lo stack tramite la CloudFormation console.

```
Parameters:
  EC2Key:
    Description: The SSH key used to access the EC2 receiver instance. Choose any
 SSH key if you are not creating an EC2 receiver instance. For instructions on how to
```

```
 create an SSH key see https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/create-
key-pairs.html
    Type: AWS::EC2::KeyPair::KeyName
    ConstraintDescription: must be the name of an existing EC2 KeyPair.

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

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

> **Note**
>
> Devi creare una key pair e fornire il nome per il EC2 `EC2Key` parametro Amazon. Vedi Creare una coppia di key pair per la tua EC2 istanza Amazon.
> Inoltre, dovrai fornire l'ID AMI specifico della regione corretto al momento della creazione dello CloudFormation stack. Per informazioni, consulta AWS Ground Station Immagini di macchine Amazon (AMIs).

I frammenti di modello rimanenti appartengono alla sezione Risorse del modello. CloudFormation

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

Considerando il nostro scenario di fornitura di un unico percorso di comunicazione a un' EC2 istanza Amazon, sai che avrai un unico percorso di distribuzione sincrono. Secondo la Distribuzione sincrona dei dati sezione, devi configurare un' EC2 istanza Amazon con AWS Ground Station Agent e creare uno o più gruppi di endpoint di dataflow. Inizierai configurando innanzitutto Amazon VPC per l' AWS Ground Station agente.

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

  PublicSubnet:
    Type: AWS::EC2::Subnet
    Properties:
      VpcId: !Ref ReceiverVPC
      MapPublicIpOnLaunch: 'true'
      AvailabilityZone: !Ref AZ
      CidrBlock: 10.0.0.0/20
      Tags:
      - Key: "Name"
        Value: "AWS Ground Station Example - PBS to AWS Ground Station Agent Public
Subnet"
      - Key: "Description"
        Value: "Subnet for EC2 instance receiving AWS Ground Station data"

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

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

  Route:
    Type: AWS::EC2::Route
    DependsOn: InternetGateway
    Properties:
```

```
      RouteTableId: !Ref RouteTable
      DestinationCidrBlock: '0.0.0.0/0'
      GatewayId: !Ref InternetGateway

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

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

> **Note**
>
> Per ulteriori informazioni sulle configurazioni VPC supportate dall' AWS Ground Station agente, vedere Requisiti dell'AWS Ground Station agente - Diagrammi VPC.

Successivamente, configurerai l' EC2 istanza Amazon 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
```

Avrai anche bisogno delle politiche, dei ruoli e dei profili appropriati AWS Ground Station per consentire la creazione dell'elastic network interface (ENI) nel tuo account.

```
 # 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 configurazioni

Questa sezione rappresenta Crea configurazioni come iniziare.

Avrai bisogno di un tracking-config per impostare le tue preferenze sull'uso dell'autotrack. La selezione di PREFERRED come autotrack può migliorare la qualità del segnale, ma non è necessario soddisfare la qualità del segnale perché la qualità delle effemeridi JPSS-1 è sufficiente.

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

In base al percorso di comunicazione, è necessario definire una configurazione antenna-downlink per rappresentare la parte satellitare, nonché una configurazione dataflow-endpoint per fare riferimento al gruppo di endpoint dataflow che definisce i dettagli dell'endpoint.

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

 # The AWS Ground Station Dataflow Endpoint Config that defines the endpoint used to
downlink data
 # from your satellite.
 DownlinkDigIfEndpointConfig:
   Type: AWS::GroundStation::Config
   Properties:
     Name: "Aqua SNPP JPSS Terra Downlink DigIF Endpoint Config"
     ConfigData:
       DataflowEndpointConfig:
```

```
          DataflowEndpointName: !Join [ "-" , [ !Ref "AWS::StackName" , "Downlink" ] ]
          DataflowEndpointRegion: !Ref AWS::Region
```

AWS Ground Station profilo della missione

Questa sezione rappresenta una Crea un profilo di missione guida introduttiva.

Ora che hai le configurazioni associate, puoi usarle per costruire il flusso di dati. Utilizzerai le impostazioni predefinite per i parametri rimanenti.

```
 # 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
```

Mettendolo insieme

Con le risorse di cui sopra, ora avete la possibilità di pianificare i contatti JPSS-1 per la consegna sincrona dei dati da qualsiasi dispositivo integrato. AWS Ground Station AWS Ground Station Sedi

Di seguito è riportato un CloudFormation modello completo che include tutte le risorse descritte in questa sezione combinate in un unico modello che può essere utilizzato direttamente. CloudFormation

Il CloudFormation modello denominato `DirectBroadcastSatelliteWbDigIfEc2DataDelivery.yml` è progettato per darti un accesso

rapido per iniziare a ricevere dati digitalizzati a frequenza intermedia (DigiF) per i satelliti Aqua, SNPP, JPSS-1/NOAA-20 e Terra. Contiene un' EC2 istanza Amazon e le CloudFormation risorse necessarie per ricevere dati di trasmissione diretta DigiF non elaborati tramite AWS Ground Station Agent.

Se Aqua, SNPP, JPSS-1/NOAA-20 e Terra non sono presenti nel tuo account, consulta. Satellite a bordo

> **Note**
>
> Puoi accedere al modello accedendo al bucket Amazon S3 per l'onboarding del cliente utilizzando credenziali valide. AWS I collegamenti seguenti utilizzano un bucket Amazon S3 regionale. Modifica il codice `us-west-2` regionale per rappresentare la regione corrispondente in cui desideri creare lo CloudFormation stack.
> Inoltre, le seguenti istruzioni utilizzano YAML. Tuttavia, i modelli sono disponibili sia in formato YAML che JSON. Per usare JSON, sostituisci l'estensione del `.yml` file con `.json` quando scarichi il modello.

Per scaricare il modello utilizzando AWS CLI, usa il seguente comando:

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

È possibile scaricare e visualizzare il modello nella console spostandosi all'URL seguente nel browser:

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

È possibile specificare il modello direttamente CloudFormation utilizzando il seguente link:

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

Quali risorse aggiuntive definisce il modello?

Il `DirectBroadcastSatelliteWbDigIfEc2DataDelivery` modello include le seguenti risorse aggiuntive:

- Interfaccia di rete elastica dell'istanza del ricevitore - (Condizionale) Un'interfaccia di rete elastica viene creata nella sottorete specificata da, PublicSubnetIdse fornita. Questa operazione è necessaria se l'istanza del ricevitore si trova in una sottorete privata. L'elastic network interface verrà associata all'EIP e collegata all'istanza del ricevitore.
- IP elastico dell'istanza del ricevitore: un IP elastico AWS Ground Station a cui connettersi. Si collega all'istanza del ricevitore o all'interfaccia elastic network.
- Una delle seguenti associazioni IP elastiche:
  - Associazione da istanza del ricevitore a Elastic IP: l'associazione dell'IP elastico all'istanza del ricevitore, se non PublicSubnetIdè specificata. Ciò richiede che tale SubnetIdriferimento sia una sottorete pubblica.
  - Associazione Elastic Network Interface to Elastic IP Association dell'istanza del ricevitore: l'associazione dell'IP elastico all'interfaccia di rete elastica dell'istanza del ricevitore, se PublicSubnetIdspecificata.
- (Facoltativo) CloudWatch Event Triggers - AWS Lambda Funzione che viene attivata utilizzando CloudWatch gli eventi inviati AWS Ground Station prima e dopo un contatto. La AWS Lambda funzione avvierà e, facoltativamente, interromperà l'istanza del ricevitore.
- (Facoltativo) Amazon EC2 Verification for Contacts: l'opzione di utilizzare Lambda per configurare un sistema di verifica delle EC2 istanze Amazon per i contatti con notifica SNS. È importante notare che ciò potrebbe comportare costi a seconda dell'utilizzo corrente.
- Profili di missione aggiuntivi: profili di missione per altri satelliti di trasmissione pubblica (Aqua, SNPP e Terra).
- Configurazioni antenna-downlink aggiuntive - Configurazioni downlink dell'antenna per altri satelliti di trasmissione pubblica (Aqua, SNPP e Terra).

I valori e i parametri per i satelliti in questo modello sono già popolati. Questi parametri ne facilitano l'uso immediato con questi satelliti. AWS Ground Station Non è necessario configurare i propri valori per utilizzarli AWS Ground Station quando si utilizza questo modello. Tuttavia, è possibile personalizzare i valori in modo che il modello funzioni per il caso d'uso.

Dove ricevo i miei dati?

Il gruppo endpoint del flusso di dati è configurato per utilizzare l'interfaccia di rete dell'istanza del ricevitore creata come parte del modello. L'istanza del ricevitore utilizza l' AWS Ground Station agente per ricevere il flusso di dati dalla AWS Ground Station porta definita dall'endpoint dataflow. Per ulteriori informazioni sulla configurazione di un gruppo di endpoint dataflow, consulta.

AWS::GroundStation::DataflowEndpointGroup Per ulteriori informazioni sull' AWS Ground Station agente, consulta Cos'è l'agente? AWS Ground Station

Risoluzione dei problemi

La seguente documentazione può aiutarti a risolvere i problemi che possono verificarsi durante l'utilizzo. AWS Ground Station

Argomenti

Risolvi i problemi relativi ai contatti che forniscono dati ad Amazon EC2

Se non riesci a completare con successo un AWS Ground Station contatto, dovrai verificare che l'istanza Amazon EC2 sia in esecuzione, verificare che l'applicazione endpoint dataflow sia in esecuzione e verificare che lo stream dell'applicazione endpoint dataflow sia configurato correttamente.

> **Note**
>
> DataDefender (DDX) è un esempio di applicazione endpoint dataflow attualmente supportata da AWS Ground Station

Prerequisito

Le seguenti procedure presuppongono che un'istanza Amazon EC2 sia già configurata. Per configurare un'istanza Amazon EC2 in AWS Ground Station, consulta Getting Started.

Passaggio 1: verifica che l'istanza EC2 sia in esecuzione

La procedura seguente mostra come trovare l'istanza Amazon EC2 nella console e avviarla se non è in esecuzione.

1. Individua l'istanza Amazon EC2 utilizzata per il contatto per il quale stai risolvendo i problemi. Utilizza le fasi seguenti:

   a. Nella CloudFormationdashboard, seleziona lo stack che contiene l'istanza Amazon EC2.

   b. Scegli la scheda Risorse e individua la tua istanza Amazon EC2 nella colonna Logical ID. Verificare che l'istanza venga creata nella colonna Stato.

   c. Nella colonna ID fisico, scegli il link per la tua istanza Amazon EC2. Verrai reindirizzato alla console di gestione di Amazon EC2.

2. Nella console di gestione Amazon EC2, assicurati che lo stato dell'istanza Amazon EC2 sia in esecuzione.

3. Se l'istanza è in esecuzione, procedere al passaggio successivo. Se l'istanza non è in esecuzione, avviare l'istanza utilizzando il seguente passaggio.

   - Con l'istanza Amazon EC2 selezionata, scegli Azioni > Stato dell'istanza > Avvia.

Fase 2: Determinare il tipo di applicazione di flusso di dati utilizzata

Se utilizzi l'AWS Ground Station agente per la consegna dei dati, reindirizza alla sezione Troubleshooting Agent. AWS Ground Station Altrimenti, se utilizzi l'applicazione DataDefender (DDX), continua a farlo. the section called "Passaggio 3: Verificare che l'applicazione Dataflow sia in esecuzione"

Passaggio 3: Verificare che l'applicazione Dataflow sia in esecuzione

La verifica dello stato di DataDefender richiede la connessione alla tua istanza in Amazon EC2. Per maggiori dettagli sulla connessione alla tua istanza, vedi Connect to your Linux istance.

La procedura seguente fornisce la procedura di risoluzione dei problemi utilizzando i comandi in un client SSH.

1. Apri un terminale o un prompt dei comandi e connettiti alla tua istanza Amazon EC2 utilizzando SSH. Inoltra la porta 80 dell'host remoto per visualizzare l' DataDefender interfaccia utente Web.

I comandi seguenti mostrano come utilizzare SSH per connettersi a un'istanza Amazon EC2 tramite un bastione con il port forwarding abilitato.

> **Note**
>
> È necessario sostituire <SSH KEY><BASTION HOST>e <HOST>con la chiave ssh specifica, il nome host bastion e il nome host dell'istanza Amazon EC2.

Per 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>
```

Per Mac

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

2. Verifica che DataDefender (chiamato anche DDX) sia in esecuzione eseguendo grepping (controllando) la presenza di un processo in esecuzione denominato ddx nell'output. Il comando per grepping (controllo) per un processo in esecuzione e un output di esempio di successo è fornito di seguito.

```
[ec2-user@Receiver-Instance ~]$ ps -ef | grep ddx
          Rtlogic   4977      1 10 Oct16 ?        2-00:22:14 /opt/rtlogic/ddx/
bin/ddx -m/opt/rtlogic/ddx/modules -p/opt/rtlogic/ddx/plugins -c/opt/rtlogic/
ddx/bin/ddx.xml -umask=077 -daemon -f installed=true -f security=true -f enable
 HttpsForwarding=true
          Ec2-user 18787 18657  0 16:51 pts/0      00:00:00 grep -color=auto ddx
```

Se DataDefender è in esecuzione, vai a the section called "Passaggio 4: verifica che il flusso dell'applicazione Dataflow sia configurato" Altrimenti, vai al passaggio successivo.

3. Inizia a DataDefender usare il comando show qui sotto.

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

Se DataDefender è in esecuzione dopo aver usato il comando, passa a the section called "Passaggio 4: verifica che il flusso dell'applicazione Dataflow sia configurato" Altrimenti, continua con il passaggio successivo.

4. Controlla i seguenti file usando i comandi seguenti per vedere se ci sono stati errori durante l'installazione e la configurazione. DataDefender

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

> **Note**
>
> Un problema comune rilevato durante l'ispezione di questi file è che l'Amazon VPC su cui è in esecuzione l'istanza Amazon EC2 non ha accesso ad Amazon S3 per scaricare i file di installazione. Se scopri nei tuoi log che questo è il problema, controlla le impostazioni Amazon VPC e del gruppo di sicurezza dell'istanza EC2 per assicurarti che non blocchino l'accesso ad Amazon S3.

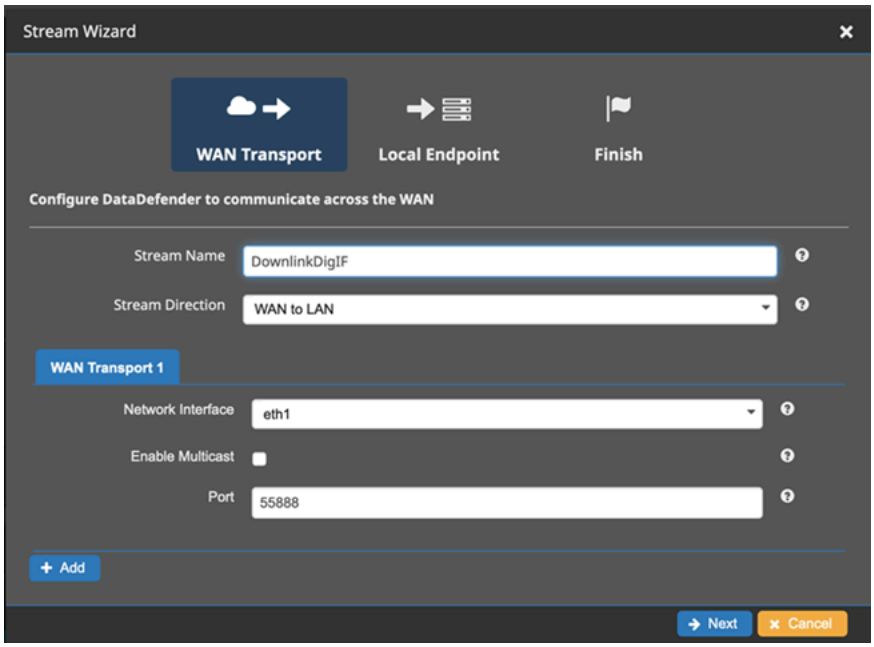
Se DataDefender è in esecuzione dopo aver verificato le impostazioni di Amazon VPC, continua a farlo. the section called "Passaggio 4: verifica che il flusso dell'applicazione Dataflow sia configurato" Se il problema persiste, contatta AWS Support e invia i file di registro con una descrizione del problema.

Passaggio 4: verifica che il flusso dell'applicazione Dataflow sia configurato

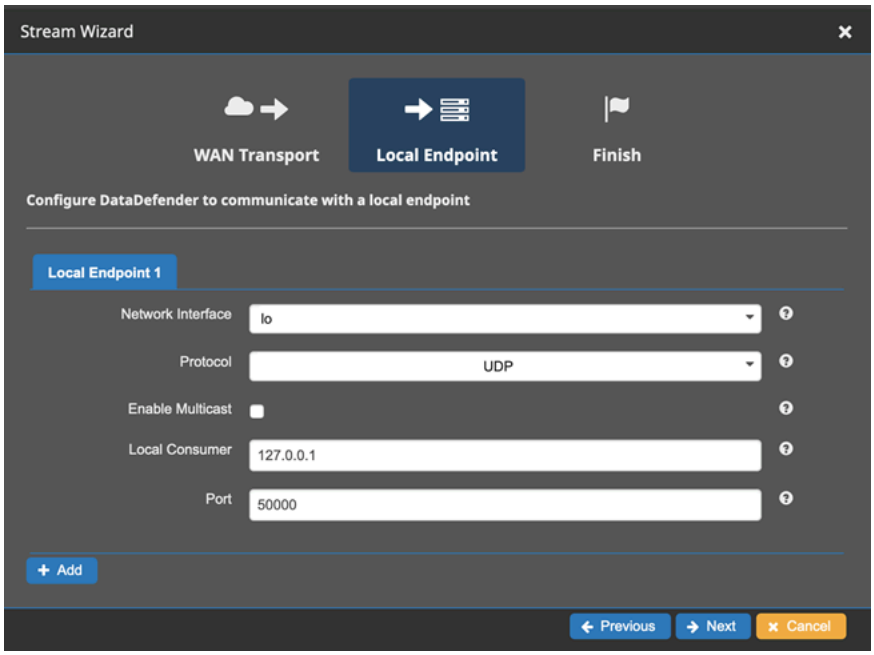
1. In un browser Web, accedete alla vostra interfaccia utente DataDefender web inserendo il seguente indirizzo nella barra degli indirizzi: localhost:8080. Quindi, premere Invio.
2. Nella DataDefenderdashboard, scegli Vai ai dettagli.
3. Seleziona il tuo flusso dall'elenco dei flussi e scegli Modifica flusso.
4. Nella finestra di dialogo Stream Wizard (Creazione guidata flusso), eseguire le operazioni seguenti:

   a. Nel riquadro WAN Transport (Trasporto WAN) verificare che WAN to LAN (Da WAN a LAN) sia selezionata per Stream Direction (Direzione flusso).

b. Nella casella Port (Porta) verificare che la porta WAN scelta per il gruppo endpoint del flusso dati sia presente. Per impostazione predefinita, questa porta è 55888. Quindi, seleziona Successivo.



c. Nel riquadro Local Endpoint (Endpoint locale) verificare che nella casella Porta sia presente una porta valida. Per impostazione predefinita, questa porta è 50000. Questa è la porta sulla quale riceverai i tuoi dati dopo DataDefender averli ricevuti dal AWS Ground Station servizio. Quindi, seleziona Successivo.



d. Scegliere Fine nel menu rimanente se sono stati modificati i valori. In caso contrario, è possibile annullare il menu Stream Wizard (Procedura guidata flussi).

Ora ti sei assicurato che la tua istanza Amazon EC2 sia in esecuzione DataDefender e configurata correttamente per ricevere dati da. AWS Ground Station Continua su the section called "Passaggio 5: assicurati di avere un numero sufficiente di indirizzi IP disponibili nella sottorete delle istanze del ricevitore".

Passaggio 5: assicurati di avere un numero sufficiente di indirizzi IP disponibili nella sottorete delle istanze del ricevitore

La procedura seguente mostra come trovare il numero di indirizzi IP disponibili in un'istanza di ricevitore Amazon EC2 nella console.

1. Per ogni istanza del ricevitore Amazon EC2 utilizzata per il contatto stai risolvendo i problemi. Utilizza le fasi seguenti:

   a. Nella CloudFormationdashboard, seleziona lo stack che contiene l'istanza Amazon EC2.

   b. Scegli la scheda Risorse e individua la tua istanza Amazon EC2 nella colonna Logical ID. Verificare che l'istanza venga creata nella colonna Stato.

   c. Nella colonna ID fisico, scegli il link per la tua istanza Amazon EC2. Verrai reindirizzato alla console di gestione di Amazon EC2.

2. Nella console di gestione Amazon EC2, trova e fai clic sul link Subnet ID nel riepilogo dell'istanza del ricevitore Amazon EC2. Verrai reindirizzato alla console di gestione Amazon VPC corrispondente.

3. Seleziona la sottorete corrispondente nella console di gestione Amazon VPC e controlla i dettagli della sottorete per gli indirizzi disponibili. IPv4 Se questo numero non è almeno pari agli endpoint di flusso di dati che utilizzano questa istanza di ricevitore Amazon EC2, procedi come segue:

   a. Aggiorna la sottorete CidrBlockcorrispondente del CloudFormation modello per ridimensionarla correttamente. Per maggiori dettagli sul dimensionamento delle sottoreti, consulta Subnet CIDR blocks.

   b. Ridistribuisci lo stack con il modello aggiornato. CloudFormation

Se continui a riscontrare problemi, contatta AWS Support.

Risolvi i problemi relativi ai contatti NON RIUSCITI

Un contatto avrà lo stato di contatto del terminale non riuscito quando AWS Ground Station rileva un problema con la configurazione delle risorse. Di seguito sono riportati i casi d'uso più comuni che possono causare contatti non riusciti, insieme ai passaggi per la risoluzione dei problemi.

> **Note**
>
> Questa guida riguarda specificamente lo stato dei contatti FAILED e non è destinata ad altri stati di errore, come AWS_FAILEDAWS_CANCELLED, o FAILED_TO_SCHEDULE. Per ulteriori informazioni sugli stati dei contatti, vedere the section called "AWS Ground Station stati dei contatti"

Casi d'uso di Dataflow Endpoint FAILED

Di seguito è riportato l'elenco dei casi d'uso comuni che possono comportare lo stato di contatto NON RIUSCITO per i flussi di dati basati su endpoint Dataflow:

- L'endpoint Dataflow non si connette mai: la connessione tra AWS Ground Station Antenna e il Dataflow Endpoint Group per uno o più flussi di dati non è mai stata stabilita.
- L'endpoint Dataflow si connette in ritardo: la connessione tra AWS Ground Station Antenna e il Dataflow Endpoint Group per uno o più flussi di dati è stata stabilita dopo l'ora di inizio del contatto.
- La sottorete dell'endpoint Dataflow non dispone di indirizzi IP disponibili: la soluzione di data delivery di Dataflow non è in grado AWS Ground Station di creare un ENI nella rete privata perché non dispone di alcun indirizzo IP disponibile nella sottorete dell'istanza ricevente.
- La sottorete dell'endpoint Dataflow non è valida: la soluzione di distribuzione dei dati AWS Ground Station dell'utente non è in grado di creare un ENI nella rete privata a causa dell'impossibilità di accedere alla sottorete fornita specificata nel Dataflow Endpoint Group.

Per qualsiasi caso di errore degli endpoint dataflow, si consiglia di esaminare quanto segue:

- Verifica che l'istanza Amazon EC2 del destinatario sia stata avviata correttamente, prima dell'orario di inizio del contatto.
- Verifica che il software dataflow endpoint fosse attivo e funzionante durante il contatto.
- Assicurati di avere almeno un indirizzo IP disponibile per endpoint di flusso di dati per sottorete di istanza del ricevitore.

- Assicurati che le sottoreti associate al tuo Dataflow Endpoint Group, tramite i flussi di dati configurati in, rimangano attive e disponibili per. Configurare e configurare Amazon VPC AWS Ground Station

Consulta la sezione successiva per procedure di risoluzione dei problemi più specifiche. Risolvi i problemi relativi ai contatti che forniscono dati ad Amazon EC2

AWS Ground Station Casi d'uso dell'agente FAILED

Di seguito è riportato l'elenco dei casi d'uso comuni che possono comportare lo stato di contatto NON RIUSCITO per i flussi di dati basati su Agent:

- AWS Ground Station Stato dell'agente non segnalato: l'agente responsabile dell'orchestrazione della consegna dei dati sul Dataflow Endpoint Group per uno o più flussi di dati non ha mai segnalato correttamente lo stato a. AWS Ground Station Questo aggiornamento dello stato dovrebbe avvenire entro pochi secondi dall'ora di fine del contatto.
- AWS Ground Station Agente avviato in ritardo: l'agente responsabile dell'orchestrazione della consegna dei dati sul Dataflow Endpoint Group per uno o più flussi di dati è stato avviato in ritardo, dopo l'orario di inizio del contatto.

Per qualsiasi caso di errore del flusso di dati di AWS Ground Station Agent, si consiglia di esaminare quanto segue:

- Verifica che l'istanza Amazon EC2 del destinatario sia stata avviata correttamente, prima dell'orario di inizio del contatto.
- Verifica che l'applicazione Agent fosse attiva e funzionante all'inizio e durante il contatto.
- Verifica che l'applicazione Agent e l'istanza Amazon EC2 non siano state chiuse entro 15 secondi dalla fine del contatto. Ciò fornisce all'agente il tempo sufficiente per segnalare AWS Ground Station lo stato.

Consulta la sezione relativa Risolvi i problemi relativi ai contatti che forniscono dati ad Amazon EC2 per procedure di risoluzione dei problemi più specifiche.

Risoluzione dei problemi relativi ai contatti FAILED_TO_SCHEDULE

Un contatto terminerà in uno stato FAILED_TO_SCHEDULE quando AWS Ground Station rileva un problema con la configurazione delle risorse o all'interno del sistema interno. Un contatto che termina con uno stato FAILED_TO_SCHEDULE fornirà facoltativamente un contesto aggiuntivo. `errorMessage` Per informazioni sulla descrizione dei contatti, consulta l'API. DescribeContact

Di seguito sono riportati i casi d'uso comuni che possono causare contatti FAILED_TO_SCHEDULE, insieme ai passaggi per la risoluzione dei problemi.

> **Note**
>
> Questa guida riguarda specificamente lo stato dei contatti FAILED_TO_SCHEDULE e non è destinata ad altri stati di errore, come, o FAILED. AWS_FAILEDAWS_CANCELLED Per ulteriori informazioni sugli stati dei contatti, vedere the section called "AWS Ground Station stati dei contatti"

Le impostazioni specificate in Antenna Downlink Demod Decode Config non sono supportate.

Il profilo di missione utilizzato per pianificare questo contatto aveva una antenna-downlink-demod-decode configurazione non valida.

Configurazione esistente AntennaDownlinkDemodDecode in precedenza

- Se le tue antenna-downlink-demod-decode configurazioni sono state modificate di recente, torna a una versione funzionante in precedenza prima di provare a programmare.
- Se si tratta di una modifica intenzionale a una configurazione esistente o a una configurazione esistente in precedenza che non viene più pianificata correttamente, segui il passaggio successivo su come inserire una nuova configurazione. AntennaDownlinkDemodDecode

Configurazione appena creata AntennaDownlinkDemodDecode

Contattaci AWS Ground Station direttamente per aggiungere la tua nuova configurazione. Crea un caso con AWS Support, incluso `contactId` quello terminato nello stato FAILED_TO_SCHEDULE

Risoluzione dei problemi generali

Se i passaggi precedenti per la risoluzione dei problemi non hanno risolto il problema:

- Riprova a pianificare il contatto o pianifica un altro contatto utilizzando lo stesso profilo di missione. Per informazioni su come prenotare un contatto, consulta. ReserveContact
- Se continui a ricevere lo stato FAILED_TO_SCHEDULE per questo profilo di missione, contatta AWS Support

Risolvi i problemi DataflowEndpointGroups non in uno stato SANO

Di seguito sono elencati i motivi per cui i gruppi di endpoint del flusso di dati potrebbero non essere in uno `HEALTHY` stato e le azioni correttive appropriate da intraprendere.

- `NO_REGISTERED_AGENT`- Avvia l'istanza EC2, che registrerà l'agente. Nota che è necessario disporre di un file di configurazione del controller valido affinché questa chiamata abbia successo. Per ulteriori informazioni sulla configurazione di tale file, consulta la Usa AWS Ground Station agente
- `INVALID_IP_OWNERSHIP`- Utilizza l' DeleteDataflowEndpointGroup API per eliminare il Dataflow Endpoint Group, quindi utilizza l' CreateDataflowEndpointGroup API per ricreare il Dataflow Endpoint Group utilizzando gli indirizzi IP e le porte associati all'istanza EC2.
- `UNVERIFIED_IP_OWNERSHIP`- L'indirizzo IP non è stato ancora convalidato. La convalida avviene periodicamente, quindi dovrebbe risolversi da sola.
- `NOT_AUTHORIZED_TO_CREATE_SLR`- L'account non è autorizzato a creare il ruolo collegato ai servizi necessario. Consulta la procedura di risoluzione dei problemi in Usa ruoli collegati ai servizi per Ground Station

Risoluzione dei problemi relativi alle effemeridi non valide

Quando carichi i dati sulle effemeridi su, questi vengono sottoposti a un flusso di lavoro di convalida asincrono. AWS Ground Station Se la convalida fallisce, lo stato delle effemeridi cambierà in. `INVALID` Il messaggio di errore contenuto nella DescribeEphemerisrisposta fornisce informazioni dettagliate per aiutarti a identificare e risolvere il problema.

Comprensione degli errori di convalida delle effemeridi

Quando la convalida di un'effemeride fallisce, la risposta dell'DescribeEphemerisAPI include due campi per facilitare la diagnosi del problema:

errorCode

Un codice leggibile da una macchina che identifica l'errore di convalida specifico. Può essere usato per la gestione degli errori programmatici.

errorMessage

Una descrizione leggibile dall'uomo dell'errore di convalida con dettagli specifici su cosa è andato storto e indicazioni su come correggerlo.

Esempio di DescribeEphemerisrisposta per un'effemeride non valida:

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

Errori di convalida comuni per le effemeridi TLE

Di seguito sono riportati gli errori di convalida più comuni riscontrati durante il caricamento delle effemeridi TLE:

Numero di catalogo satellitare non corrispondente

Errore: «Il numero di catalogo satellitare presente nelle effemeridi non corrisponde al numero di catalogo satellitare del satellite associato»

Soluzione: verificate che il numero di ID/satellite catalogo NORAD nelle vostre linee TLE corrisponda al numero di catalogo satellitare del vostro satellite. `00000`Utilizzatelo per i satelliti senza un numero di catalogo assegnato.

Movimento medio non valido

Errore: «Il movimento medio delle effemeridi fornite differisce troppo dalle effemeridi di riferimento più recenti»

Soluzione: verificate che i dati TLE siano corretti e rappresentino un'orbita valida. Ground Station utilizza le effemeridi Space-Track come riferimento durante la convalida.

Errori di convalida comuni per le effemeridi OEM

Di seguito sono riportati gli errori di convalida più comuni riscontrati durante il caricamento di effemeridi OEM:

Quadro di riferimento non valido

Errore: «REF_FRAME non è supportato»

Soluzione: aggiorna il file OEM per utilizzare uno dei quadri di riferimento supportati: o. EME2000 ITRF2000

Campi obbligatori mancanti

Errore: «Campo di metadati mancante: INTERPOLAZIONE»

Soluzione: aggiungi i campi INTERPOLATION e INTERPOLATION_DEGREE alla sezione dei metadati OEM. Questi sono necessari per generare angoli di puntamento accurati dell'antenna. AWS Ground Station

Sistema orario non supportato

Errore: «Il TIME_SYSTEM non è supportato»

Soluzione: assicurati che il file OEM utilizzi l'UTC come sistema orario.

Versione OEM non supportata

Errore: «Il CCSDS_OEM_VERS non è supportato»

Soluzione: assicurati che il tuo file OEM utilizzi CCSDS OEM versione 2.0.

Errori di convalida comuni per le effemeridi di elevazione dell'azimut

Di seguito sono riportati gli errori di convalida più comuni riscontrati durante il caricamento di effemeridi di elevazione dell'azimut:

Dati mancanti azimuth/elevation

Errore: «Nessun TimeAzEl campo era presente in almeno uno AzElSegment»

Soluzione: assicurati che ogni segmento nei dati di elevazione azimutale contenga almeno una coppia con tag temporali azimuth/elevation .

Intervallo di angoli azimutali non valido (gradi)

Errore: "AzEl az deve essere maggiore o uguale a -180 e minore o uguale a 360 gradi»

Soluzione: verificate che gli angoli di azimut siano compresi tra [-180, 360] gradi.

Intervallo di angoli di elevazione non valido (gradi)

Errore: "AzEl el deve essere maggiore o uguale a -90 e minore o uguale a 90 gradi»

Soluzione: verificate che gli angoli di elevazione siano compresi tra [-90, 90] gradi.

Intervallo di angoli azimutali non valido (radianti)

Errore: "AzEl az deve essere maggiore o uguale a -pi e minore o uguale a 2pi radianti»

Soluzione: verificate che gli angoli di azimut siano compresi tra [-π, 2π] radianti.

Intervallo di angoli di elevazione non valido (radianti)

Errore: "AzEl el deve essere maggiore o uguale a -pi/2 e minore o uguale a pi/2 radianti»

Soluzione: verificate che gli angoli di elevazione siano compresi tra [-π, 2] radianti.

Valori temporali non monotonici

Errore: « TimeAzEl Gli elementi all'interno di un AzElSegment devono essere in ordine temporale»

Soluzione: assicurati che i valori temporali in ogni segmento aumentino rigorosamente.

Segmenti fuori ordine

Errore: "AzElSegments deve essere temporalmente in ordine»

Soluzione: assicuratevi che i segmenti siano disposti in ordine cronologico.

Segmenti sovrapposti

Errore: «L'intervallo di tempo di almeno un segmento si sovrappone a quello di altri segmenti»

Soluzione: assicurati che ogni segmento abbia un intervallo di tempo unico e non sovrapposto. Il valore `endTime` di un segmento non deve superare quello `startTime` del segmento successivo.

Fasi per la risoluzione dei problemi

Se le tue effemeridi non vengono convalidate, segui questi passaggi per risolvere il problema:

1. Chiama DescribeEphemeriscon il tuo Ephemeris ID per recuperare l'and. `errorCode` `errorMessage`
2. Controlla il messaggio di errore per dettagli specifici su quale controllo di convalida non è riuscito.
3. Correggi i problemi identificati nei dati sulle effemeridi.
4. Carica una nuova effemeride con i dati corretti utilizzando. CreateEphemeris
5. Monitora il nuovo stato delle effemeridi finché non raggiunge lo stato. `ENABLED`
6. Elimina le effemeridi non valide usando DeleteEphemerisse non sono più necessarie.

Riferimento completo al codice di errore

Le sezioni seguenti forniscono una mappatura completa di tutti i `errorCode` valori che possono essere restituiti quando la convalida delle effemeridi fallisce, organizzata per categoria di alto livello. `invalidReason`

Motivo non valido: **`METADATA_INVALID`**

Questi errori si verificano quando i campi di metadati obbligatori sono mancanti, sono formattati in modo errato o contengono valori non supportati nei dati delle effemeridi.

Codice di errore	Messaggio di errore
MISMATCHED_SATCAT_ID	Il numero di catalogo satellitare presente nelle effemeridi TLE non corrisponde al numero di catalogo satellitare del satellite associato

Codice di errore	Messaggio di errore
OEM_VERSION_UNSUPPORTED	Le effemeridi in OEM non sono `CCSDS_OEM_VERS` supportate. Valori supportati: [] `2.0`
ORIGINATOR_MISSING	Il campo di `ORIGINATOR` intestazione non è presente nelle effemeridi OEM
DATA_CREAZIONE_MANCANTE	Il campo di `CREATION_DATE` intestazione non è presente nelle effemeridi OEM
NOME_OGGETTO MANCANTE	Il campo dei `OBJECT_NAME` metadati non è presente nelle effemeridi OEM
OBJECT_ID_MISSING	Il campo dei `OBJECT_ID` metadati non è presente nelle effemeridi OEM
REF_FRAME_UNSUPPORTED	Le effemeridi `REF_FRAME` in OEM non sono supportate. Valori supportati: [,] `EME2000` `ITRF2000`
REF_FRAME_EPOCH_UN SUPPORTED	Il campo dei `REF_FRAME_EPOCH` metadati nelle effemeridi OEM non è supportato. Rimuovi questo campo dalle effemeridi
TIME_SYSTEM_UNSUPPORTED	Le effemeridi `TIME_SYSTEM` in OEM non sono supportat e. Valori supportati: [] `UTC`
CENTER_BODY_UNSUPPORTED	Le effemeridi `CENTER_BODY` in OEM non sono supportat e. Valori supportati: [] `Earth`
INTERPOLAZIONE_MANCANTE	Il campo dei `INTERPOLATION` metadati non è presente nelle effemeridi OEM
INTERPOLATION_DEGREE_INVALI D	Il grado di interpolazione nelle effemeridi OEM deve essere maggiore di 0 per il metodo di interpolazione
AZ_EL_SEGMENT_LIST_MISSING	Il campo è mancante `azElSegmentList`
INSUFFICIENT_TIME_AZ_EL	Nessun campo `TimeAzEl`era presente in almeno uno `azElSegmentList`

Motivo non valido: **`TIME_RANGE_INVALID`**

Questi errori si verificano quando le effemeridi contengono intervalli di tempo non validi, inclusi problemi relativi agli start/end orari, all'ordinamento dei segmenti, ai segmenti sovrapposti o alle incongruenze temporali.

Codice di errore	Messaggio di errore
TEMPO_DI_INIZIO IN_FUTURO	L'ora di inizio delle effemeridi è nel futuro, ma deve essere nel passato
TEMPO_FINE_IN_PASSATO	Effemeridi: la fine dei tempi è nel passato, ma deve essere nel futuro
TIME_EXPIRATION_TOO_EARLY	L'ora di scadenza fornita è precedente all'ora di fine delle effemeridi
TIME_START_METADAT A_TOO_EARLY	Il valore dei `START_TIME` metadati è precedente alla prima data presente nei dati sulle effemeridi OEM
STOP_TIME_METADATA _TOO_LATE	Il valore dei `STOP_TIME` metadati è successivo all'ultima ora presente nei dati sulle effemeridi OEM
AZ_EL_SEGMENT_END_ TIME_BEFORE_START_TIME	Il valore di almeno un segmento di dati è precedente a quello del segmento `endTimestartTime`
AZ_EL_SEGMENT_TIME S_OVERLAP	L'intervallo di tempo di almeno un segmento si sovrappon e a quello di altri intervalli di tempo del segmento
AZ_EL_SEGMENTS_OUT _OF_ORDER	I segmenti non sono ordinati temporalmente
TIME_AZ_EL_ITEMS_OUT_OF_ORD ER	Gli articoli all'interno di a devono essere temporane amente in `TimeAzEl`ordine `AzElSegment`
AZ_EL_SEGMENT_REFE RENCE_EPOCH_INVALID	L'epoca di riferimento per un segmento non è valida o è formattata in modo errato
AZ_EL_SEGMENT_START_TIME_IN VALID	L'ora di inizio nell'intervallo di tempo valido di un segmento non inizia dopo il primo segmento

Codice di errore	Messaggio di errore
AZ_EL_SEGMENT_END_TIME_INVALID	L'ora di fine nell'intervallo di tempo valido di un segmento non termina dopo l'ultimo segmento
AZ_EL_SEGMENT_VALID_TIME_RANGE_INVALID	L'intervallo di tempo valido per un segmento non è valido
AZ_EL_SEGMENT_END_TIME_TOO_LATE	L'ora di fine di un segmento supera la durata massima consentita dall'epoca di riferimento
AZ_EL_TOTAL_DURATION_EXCEEDED	La durata totale su tutti i segmenti supera la durata massima consentita dell'angolo di puntamento

Motivo non valido: **`TRAJECTORY_INVALID`**

Questi errori si verificano quando le effemeridi contengono dati di traiettoria non validi, inclusi problemi con parametri orbitali, intervalli angolari o unità.

Codice di errore	Messaggio di errore
MEAN_MOTION_INVALID	Il movimento medio delle effemeridi TLE fornite differisce troppo dalle effemeridi di riferimento più recenti. Nota: Ground Station utilizza le effemeridi Space-Track come riferimento durante la convalida
TIME_AZ_EL_AZ_RADIAN_RANGE_INVALID	AzEl `az`deve essere maggiore o uguale a -π e minore o uguale a 2π radianti
TIME_AZ_EL_EL_RADIAN_RANGE_INVALID	AzEl `el`deve essere maggiore o uguale a -π /2 e minore o uguale a π /2 radianti
TIME_AZ_EL_AZ_DEGREE_RANGE_INVALID	AzEl `az`deve essere maggiore o uguale a -180 e minore o uguale a 360 gradi
TIME_AZ_EL_EL_DEGREE_RANGE_INVALID	AzEl `el`deve essere maggiore o uguale a -90 gradi e minore o uguale a 90 gradi

Codice di errore	Messaggio di errore
TIME_AZ_EL_ANGLE_UNITS_INVALID	Unità angolari non valide AzEl

Motivo non valido: **KMS_KEY_INVALID**

Questi errori si verificano quando si verificano problemi con la chiave AWS Key Management Service (KMS) utilizzata per crittografare i dati delle effemeridi.

Codice di errore	Messaggio di errore
INSUFFICIENT_KMS_PERMISSIONS	Ground Station non dispone di autorizzazioni sufficienti per accedere alla chiave KMS di questa effemeride

Motivo non valido: **VALIDATION_ERROR**

Questi errori si verificano quando ci sono problemi generali di convalida con i dati sulle effemeridi che non rientrano nelle altre categorie specifiche.

Codice di errore	Messaggio di errore
INTERNAL_ERROR	Si è verificato un errore interno durante la convalida delle effemeridi
FILE_FORMAT_INVALID	Il formato del file delle effemeridi non è valido o è danneggiato. Verifica che il file sia conforme al formato previsto per il tipo di effemeridi

Risolvi i problemi relativi ai contatti che non hanno ricevuto dati

È possibile che un contatto appaia con successo, ma non abbia comunque ricevuto alcun dato. Ciò può significare che ricevi file PCAP vuoti o nessun file PCAP se utilizzi la consegna dei dati S3. Ciò può accadere per diversi motivi. Di seguito vengono illustrate alcune delle cause e come affrontarle.

Configurazione errata del downlink

A ogni contatto che riceve dati da un satellite verrà associato Config di downlink antenna un o. Config di decodifica demodulazione downlink antenna Se la configurazione specificata non è conforme al segnale trasmesso da un satellite, non AWS Ground Station sarà in grado di ricevere il segnale trasmesso. Ciò comporterà l'impossibilità di ricevere dati da AWS Ground Station.

Per risolvere questo problema, verifica che le configurazioni che stai utilizzando corrispondano al segnale trasmesso dal tuo satellite. Ad esempio, verifica di aver impostato la frequenza centrale, la larghezza di banda, la polarizzazione e, se necessario, i parametri di demodulazione e decodifica corretti.

Manovra satellitare

A volte un satellite può eseguire una manovra che disabilita temporaneamente alcuni dei suoi sistemi di comunicazione. La manovra può anche modificare in modo significativo la posizione del satellite nel cielo. AWS Ground Station non sarà in grado di ricevere un segnale da un satellite che non trasmette un segnale o se le effemeridi utilizzate fanno sì che l' AWS Ground Station antenna punti in un punto del cielo in cui il satellite non è presente.

Se stai cercando di comunicare con un satellite di trasmissione pubblica gestito dal NOAA, potresti trovare un messaggio che descrive un'interruzione o una manovra nella pagina NOAA Satellite Alert Messages. Il messaggio può includere una cronologia di quando è prevista la ripresa della trasmissione dei dati, oppure può essere pubblicata in un messaggio successivo.

Se state comunicando con i vostri satelliti, è vostra responsabilità comprendere le vostre operazioni satellitari e in che modo ciò potrebbe influire sulla comunicazione. AWS Ground Station Se state eseguendo una manovra che influirà sulla traiettoria del satellite, ciò può includere la fornitura di dati aggiornati sulle effemeridi personalizzati. Per ulteriori informazioni sulla fornitura di dati sulle effemeridi personalizzati, vedere. Comprendi come AWS Ground Station utilizza le effemeridi

AWS Ground Station interruzione

Se AWS Ground Station causa un errore o lo annulla, AWS Ground Station imposterà lo stato del contatto su AWS_FAILED, o. AWS_CANCELLED Per ulteriori informazioni sul ciclo di vita dei contatti, consulta. Comprendi il ciclo di vita dei contatti In alcuni casi, AWS Ground Station può verificarsi un errore che impedisce la trasmissione dei dati al tuo account, ma non fa sì che il contatto assuma lo stato AWS_FAILEDo AWS_CANCELLED. Quando ciò accade, AWS Ground Station

dovresti pubblicare un evento specifico dell'account nella dashboard AWS Health. Per ulteriori informazioni sulla dashboard AWS Health, consulta AWS Health User Guide.

Risolvere i problemi di telemetria

Utilizza le seguenti informazioni per risolvere i problemi più comuni relativi alla telemetria.

Problemi di configurazione comuni

Errori di autorizzazione IAM

Sintomi

Quando si chiama `CreateConfig` per creare un TelemetrySinkConfig, viene visualizzato un errore:

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

Cause

- Il ruolo IAM specificato in TelemetrySinkConfig non dispone delle autorizzazioni necessarie per scrivere nel flusso Kinesis Data Streams.
- La policy di fiducia sul ruolo IAM non consente di AWS Ground Station assumere il ruolo.
- L' TelemetrySinkConfig ARN del flusso Kinesis Data Streams non è corretto o lo stream non esiste.

Soluzioni

1. Verifica che il ruolo IAM esista e disponga delle autorizzazioni corrette. Rivedi Fase 2: Creare un TelemetrySinkConfig e assicurati che tutti i passaggi siano stati seguiti.
2. Verifica che AWS Ground Station possa assumere il tuo ruolo di IAM:

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

   Verifica che la politica di fiducia `groundstation.amazonaws.com` sia inclusa come responsabile del servizio affidabile.
3. Verifica che il ruolo IAM disponga delle autorizzazioni Kinesis richieste:

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

Assicurati che la policy `kinesis:DescribeStream` includa e `kinesis:PutRecords` autorizzazioni per il tuo stream. `kinesis:PutRecord`

4. Verifica che il flusso Kinesis Data Streams esista e che l'ARN sia corretto:

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

5. Se utilizzi la crittografia gestita dal cliente, verifica che il ruolo IAM `kms:GenerateDataKey` disponga dell'autorizzazione per la tua chiave. AWS KMS

PassRole errori di autorizzazione

Sintomi

Quando si chiama`CreateConfig`, viene visualizzato un errore che indica che non si dispone dell'autorizzazione per passare il ruolo IAM.

Soluzione

Assicurati che il tuo utente o ruolo IAM disponga dell'`iam:PassRole`autorizzazione per il ruolo IAM di telemetria. Aggiungi la seguente policy al tuo utente o ruolo:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetRole",
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::99999999999:role/your-stream-name"
    }
  ]
}
```

Problemi di configurazione del flusso Kinesis Data Streams

Sintomi

La consegna della telemetria non riesce o è intermittente.

Cause

- Lo stream Kinesis Data Streams ha una capacità insufficiente per il throughput di telemetria.
- Lo stream viene utilizzato da altre applicazioni, con conseguente limitazione della scrittura.

Soluzioni

1. Controlla lo stato dello stream:

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

2. Monitora la limitazione della scrittura utilizzando CloudWatch le metriche:

```
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. Se viene rilevata una limitazione, considera:

    - Passaggio alla modalità di capacità su richiesta per la scalabilità automatica.
    - Utilizzo di uno stream dedicato per AWS Ground Station la telemetria.
    - Se si utilizza la modalità provisioned, aumentare il numero di shard.

Problemi di consegna della telemetria

Nessun dato di telemetria visualizzato

Sintomi

Dopo aver pianificato un contatto con un profilo di missione abilitato alla telemetria, nel flusso Kinesis Data Streams non viene visualizzato alcun dato di telemetria.

Possibili cause e soluzioni

Il profilo di missione non ha la telemetria abilitata

Verifica che il profilo di missione utilizzato per il contatto includa: `telemetrySinkConfigArn`

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

Controlla l'output del `telemetrySinkConfigArn` campo. Se non è presente, il profilo di missione non ha la telemetria abilitata.

Problema con le autorizzazioni dei ruoli IAM

Consulta la procedura per la risoluzione dei problemi di autorizzazione IAM riportata in Errori di autorizzazione IAM.

Lo stream Kinesis Data Streams non esiste o si trova nella regione sbagliata

Verifica che lo stream esista nella regione corretta:

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

Il contatto non è ancora iniziato

La consegna della telemetria inizia all'ora di inizio del contatto. Verifica che il contatto sia iniziato controllando lo stato del contatto:

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

Dati di telemetria intermittenti

Sintomi

I dati di telemetria vengono forniti in modo incoerente rispetto alle lacune o ai record mancanti.

Possibili cause

- Problemi o limitazione della capacità dello streaming di Kinesis Data Streams. Per informazioni, consulta Problemi di configurazione del flusso Kinesis Data Streams.
- Problemi di connettività di rete tra AWS Ground Station e lo stream Kinesis Data Streams.

Soluzioni

- Monitora le CloudWatch metriche del flusso di Kinesis Data Streams per verificare la presenza di limitazioni o errori.
- Assicurati che lo stream utilizzi la modalità di capacità su richiesta o disponga di una capacità fornita sufficiente.
- Utilizza uno stream dedicato per la AWS Ground Station telemetria per evitare conflitti con altre applicazioni.

Problemi relativi al formato dei dati

Errori di analisi JSON

Sintomi

L'applicazione riscontra errori durante l'analisi dei record di telemetria come JSON.

Soluzioni

- Verifica della decodifica Base64: i dati nello stream Kinesis Data Streams sono codificati in Base64. Assicurati di decodificare i dati prima di analizzarli come JSON. Per ulteriori informazioni, consulta Lettura dei dati dal flusso Kinesis Data Streams.
- Verifica la presenza di record vuoti: AWS Ground Station può inviare record di convalida vuoti durante la creazione di un. TelemetrySinkConfig La tua applicazione dovrebbe gestire con garbo i record vuoti o non corretti.
- Implementa l'analisi sensibile alla versione: analizza prima i `telemetryVersion` campi `telemetryTypeAndVersiontelemetryType`, e per determinare lo schema appropriato per ogni record.

Tipi o versioni di telemetria sconosciuti

Sintomi

L'applicazione presenta tipi o versioni di telemetria che non riconosce.

Soluzione

Questo è un comportamento previsto in quanto nel tempo potrebbero essere introdotti nuovi tipi di telemetria e nuove versioni dello schema. L'applicazione deve:

- Registra tipi e versioni sconosciuti per il monitoraggio.
- Continua a elaborare i tipi e le versioni noti.
- Implementa una gestione corretta per schemi sconosciuti.

Per ulteriori informazioni sul controllo delle versioni dello schema, vedere. Versionamento ed evoluzione dello schema

Utilizzo della guida

Se continui a riscontrare problemi dopo aver seguito la procedura di risoluzione dei problemi, contatta l' AWS assistenza.

Informazioni da fornire

Quando contatti l'assistenza, fornisci le seguenti informazioni:

- Contatta con IDs problemi
- ID del profilo di missione utilizzato
- TelemetrySinkConfig ARN
- ARN per lo streaming di Kinesis Data Streams
- Ruolo IAM, ARN e policy allegate
- Messaggi di errore provenienti da CloudWatch Logs o dall'applicazione
- Indicazioni temporali in cui si sono verificati i problemi
- Procedure di risoluzione dei problemi già eseguite

Per AWS Ground Station assistenza generale, consulta la Guida AWS Ground Station per l'utente.

Quote e limiti

È possibile visualizzare le regioni supportate, gli endpoint associati e le quote negli endpoint e nelle quote.AWS Ground Station

Puoi utilizzare la console Service Quotas, l'API AWS e la CLI AWSper richiedere un aumento delle quote, se necessario.

Termini del servizio

Per i termini del AWS Ground Station servizio, consulta i Termini di servizio AWS.

Cronologia dei documenti per la guida AWS Ground Station dell'utente

La tabella seguente descrive le modifiche importanti in ogni versione della Guida per l' AWS Ground Station utente.

Modifica	Descrizione	Data
Aggiornamento della documentazione	Ha aggiunto funzionalità aggiuntive all' CancelContact API e include informazioni su tali funzionalità e implicazioni di misurazione. Per ulteriori informazioni, consulta Understand contact metering.	10 dicembre 2025
Aggiornamento della documentazione	Ha chiarito che le CloudWatch metriche vengono emesse nella regione associata alla stazione terrestre del contatto. Collegamenti interrotti fissi.	2 dicembre 2025
Politica AWS gestita aggiornata	AWS Ground Station ha aggiornato la politica gestita `AWSGroundStationAgentInstancePolicy` per includere autorizzazioni aggiuntive per il recupero della risposta alle attività. URLs Per informazioni, consulta AWS Ground Station gli aggiornamenti delle politiche gestite. AWS	13 novembre 2025

Nuova funzionalità	È stata aggiornata la guida per l'utente per includere le effemeridi di innalzamento dell'azimut. Per ulteriori informazioni, vedere Fornire dati sulle effemeridi di elevazione dell'azimut	22 ottobre 2025
Aggiornamento della documentazione	La distribuzione dei dati in più regioni non richiede più configurazioni o approvazioni speciali. Per ulteriori informazioni, consulta Utilizzare la distribuzione di dati tra regioni.	11 settembre 2025
Aggiornamento della documentazione	Sono stati aggiunti chiarimenti sull'utilizzo da parte dei contatti delle risorse configurate.	4 aprile 2025
Nuova funzionalità	È stata aggiornata la guida per l'utente per includere il gemello AWS Ground Station digitale.	6 agosto 2024
Aggiornamento della documentazione	Sono state aggiornate molte sezioni della guida per l'utente, inclusi nuovi diagrammi, esempi e altro.	18 luglio 2024
Aggiornamento della documentazione	Aggiunto il feed RSS alla Guida per l'utente.	18 luglio 2024
Aggiornamento della documentazione	Dividi la guida per l'utente dell' AWS Ground Station agente in una guida utente separata.	18 luglio 2024

Nuova funzionalità	I contatti possono ora essere programmati fino a 30 secondi al di fuori degli intervalli di visibilità. I tempi di visibilità sono inclusi nelle DescribeC ontact risposte.	26 marzo 2024
Aggiornamento della documentazione	Organizzazione migliorata e aggiunta la sezione «Selezion e delle EC2 istanze e pianifica zione della CPU».	6 marzo 2024
Aggiornamento della documentazione	Sono state aggiunte nuove best practice alla Guida per l'utente dell' AWS Ground Station agente per l'esecuzi one di servizi e processi insieme all' AWS Ground Station agente.	23 febbraio 2024
Aggiornamento della documentazione	Aggiunta la pagina Agent Release Notes.	21 febbraio 2024
Aggiornamento del modello	È stato aggiunto il supporto per una sottorete pubblica separata nel DataDelivery modello DirectBroadcastSat elliteWbDigIfEc 2.	14 febbraio 2024
Aggiornamento della documentazione	È stato aggiunto il riferimen to ad AWS Notifiche all'utent e nella documentazione di monitoraggio.	6 agosto 2023
Aggiornamento della documentazione	Sono state aggiunte istruzioni per etichettare i satelliti con un nome da mostrare nella AWS Ground Station console.	26 luglio 2023

Nuova funzionalità	È stata aggiunta la Guida per l'utente dell' AWS Ground Station agente per il rilascio di DigiF Data Delivery a banda larga.	12 aprile 2023
Nuova politica gestita AWS	AWS Ground Station ha aggiunto una nuova politica denominata AWSGround StationAgentInstancePolicy.	12 aprile 2023
Nuova funzionalità	Aggiornata la guida per l'utente per il rilascio di CPE Preview.	09 novembre 2022
Nuova politica AWS gestita	AWS Ground Station ha aggiunto la AWSService RoleForGroundStationDataflowEndpointGroup service-linked-role (SLR) che include una nuova politica denominata AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy.	2 novembre 2022
Nuova funzionalità	È stata aggiornata la guida per l'utente per includere l'integrazione con AWS CLI.	17 aprile 2020
Nuova funzionalità	È stata aggiornata la guida per l'utente per includere l'integrazione con CloudWatch Metrics.	24 febbraio 2020
Nuovo modello	Public Broadcast Satellites (AquaSnppJpss modello) aggiunti alla Guida per l' AWS Ground Station utente.	19 febbraio 2020

Nuova funzionalità	Aggiornata la guida per l'utente per includere il recapito dei dati tra regioni geografiche.	05 febbraio 2020
Aggiornamento della documentazione	Esempi e descrizioni aggiornati per il monitoraggio AWS Ground Station con CloudWatch Events.	4 febbraio 2020
Aggiornamento della documentazione	Le posizioni dei modelli sono state aggiornate e le sezioni Guida introduttiva e Risoluzione dei problemi sono state riviste.	19 dicembre 2019
Nuova sezione per la risoluzione dei problemi	Sezione di risoluzione dei problemi aggiunta alla Guida per AWS Ground Station l'utente.	7 novembre 2019
Nuovo argomento introduttivo	È stato aggiornato l'argomento Guida introduttiva, che include i CloudFormation modelli più recenti.	1° luglio 2019
Versione Kindle	Versione Kindle pubblicata della Guida per l'AWS Ground Station utente.	20 giugno 2019
Nuovo servizio e guida	Questa è la versione iniziale AWS Ground Station e la Guida per l'AWS Ground Station utente.	23 maggio 2019

AWS Glossario

Per la AWS terminologia più recente, consultate il AWS glossario nella sezione Reference.Glossario AWS

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.