aws

Guida per l'utente

AWS Ground Station

AWS Ground Station: Guida per l'utente

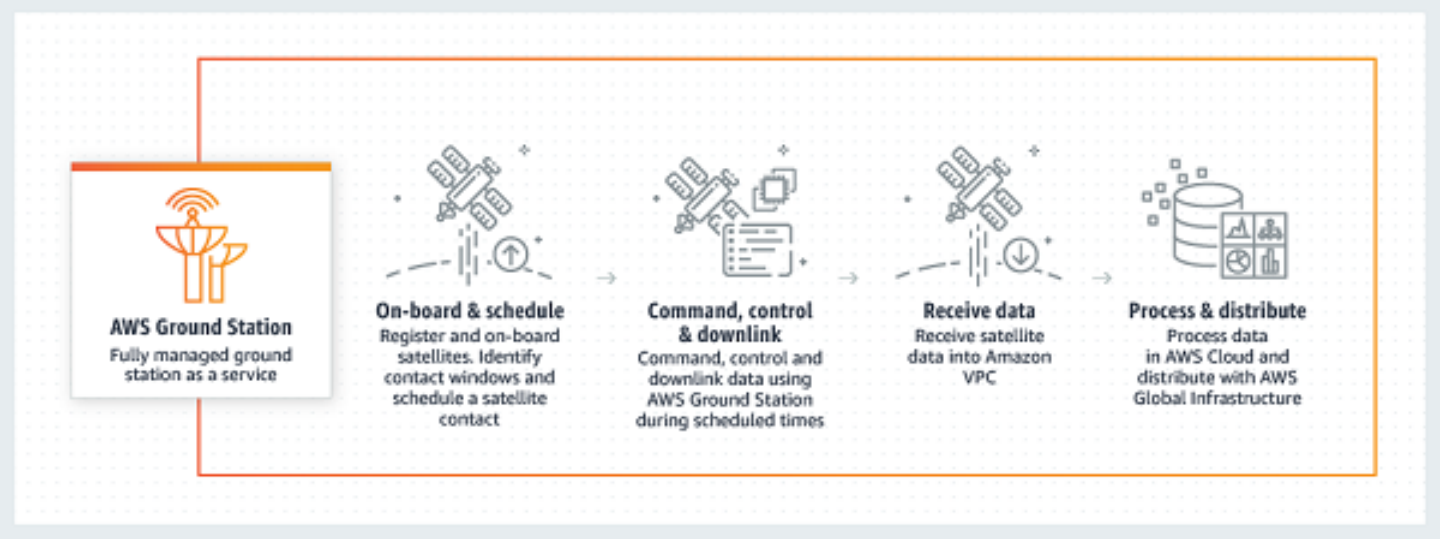
Table of Contents

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 AWS la rete globale in fibra a bassa latenza e ad alta larghezza di banda, potete 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'EC2istanza 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 -49). VITA

- 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 alla navicella spaziale ed esegui altre attività avanzate ricevendo il segnale trasmesso su un'antenna fisicamente collocata.
- Software Defined Radio (SDR)/Front End Processor (FEP): utilizza il tuo processore esistente SDR e/oFEP, che è in grado di funzionare su un'EC2istanza Amazon, per elaborare i tuoi dati in tempo reale, inviare/ricevere le forme d'onda esistenti e generare 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 dati interregionale: 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 la AWS Ground Station API Guida di riferimento. Il API riferimento descrive in dettaglio tutte le API AWS Ground Station operazioni. Fornisce inoltre esempi di richieste, risposte ed errori per i protocolli di servizi Web supportati. Puoi usare il AWS CLI, o an 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. Posizioni Contattaci all'<indirizzo aws-groundstation@amazon.com> se il tuo caso d'uso richiede funzionalità aggiuntive, offerte di localizzazione aggiuntive o posizioni delle antenne più precise.

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

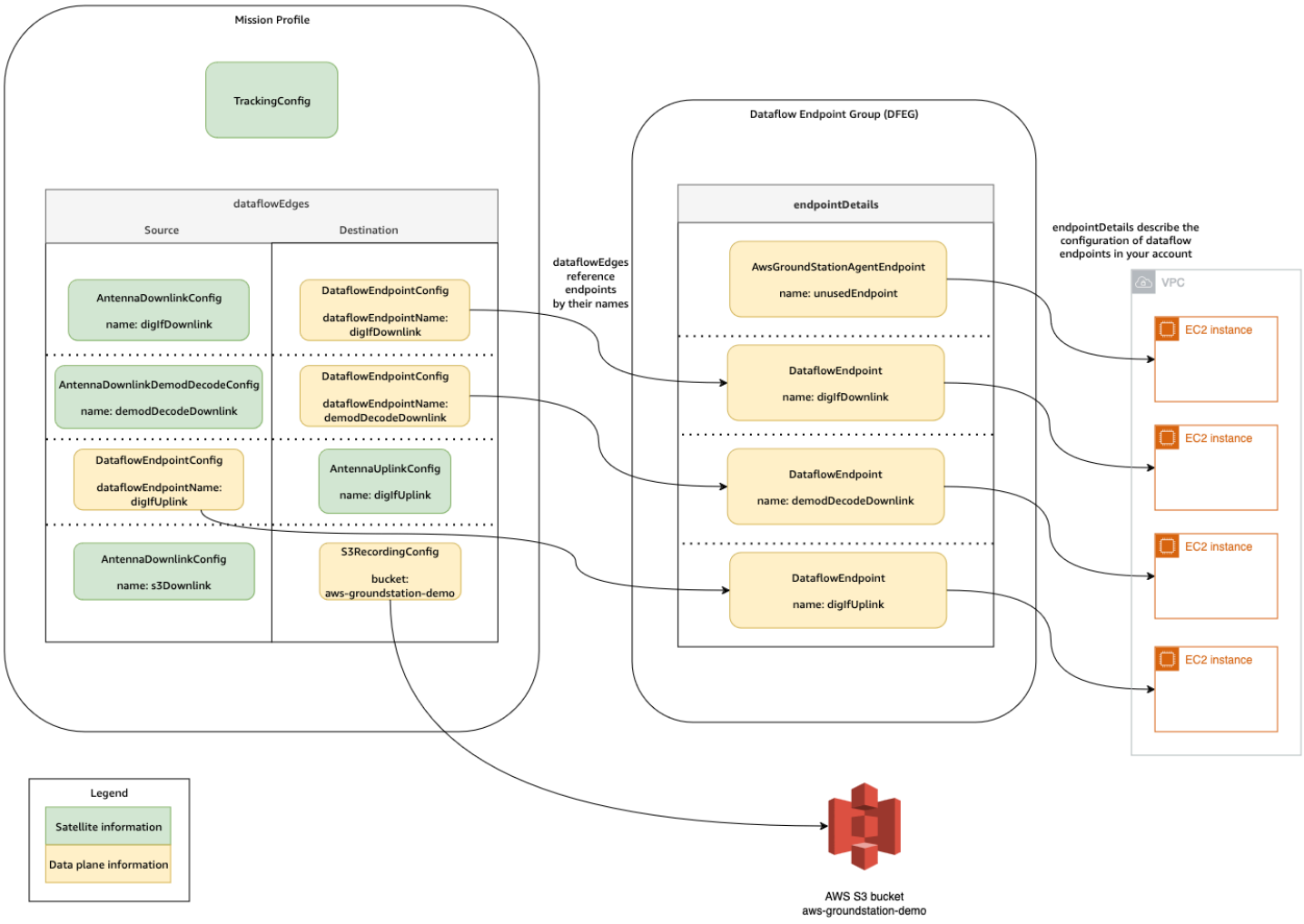
Le informazioni sulla frequenza satellitare, le informazioni sul piano dati e altri dettagli sono incapsulati in un profilo di missione. Il profilo di missione è una raccolta di componenti di configurazione. Ciò consente di riutilizzare i componenti di configurazione in diversi profili di missione in 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 AmazonVPC, Amazon S3 e EC2 Amazon che verranno utilizzate durante un contatto, consulta. Flussi di dati
- Per i dettagli sul comportamento di ciascuna configurazione, consulta. Config
- Per dettagli specifici su tutti i parametri previsti, vedere. Profilo della 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 viene utilizzato per mostrare 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:

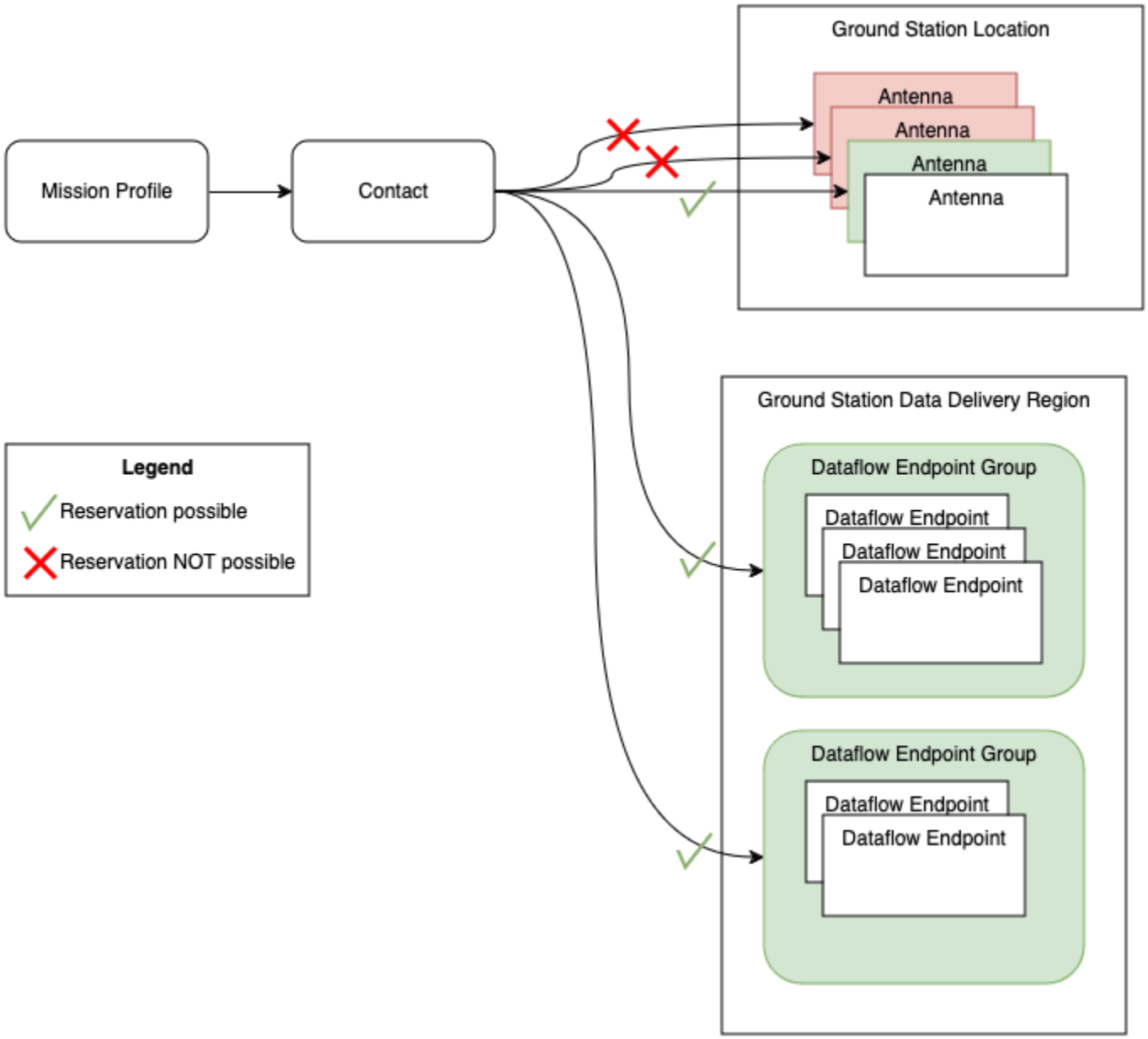
- Downlink sincrono di dati digitali a frequenza intermedia verso un'EC2istanza Amazon gestita da te. Denotato dal nome. digIfDownlink
- Downlink asincrono di dati digitali a frequenza intermedia verso un bucket Amazon S3. Denotato dal aws-groundstation-demonome del bucket.
- Downlink sincrono di dati demodulati e decodificati verso un'istanza Amazon EC2 gestita da te. Denotato dal nome. demodDecodeDownlink
- Uplink sincrono di dati da un'EC2istanza 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 la valutazione, verrà visualizzato lo stato del contatto. SCHEDULING

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



I contatti che possono essere eseguiti e che hanno disponibilità si traducono in SCHEDULEDcontatti. Con un contatto programmato, le risorse necessarie per effettuare il contatto sono state riservate AWS nelle regioni necessarie, come definito dal profilo della missione. I contatti che non possono essere eseguiti o che hanno parti non disponibili daranno luogo a contatti FAILED_TO_ SCHEDULE. Vedi Risoluzione dei problemi relativi ai FAILED contatti _TO_ SCHEDULE per i dettagli sul debug.

Esecuzione dei contatti

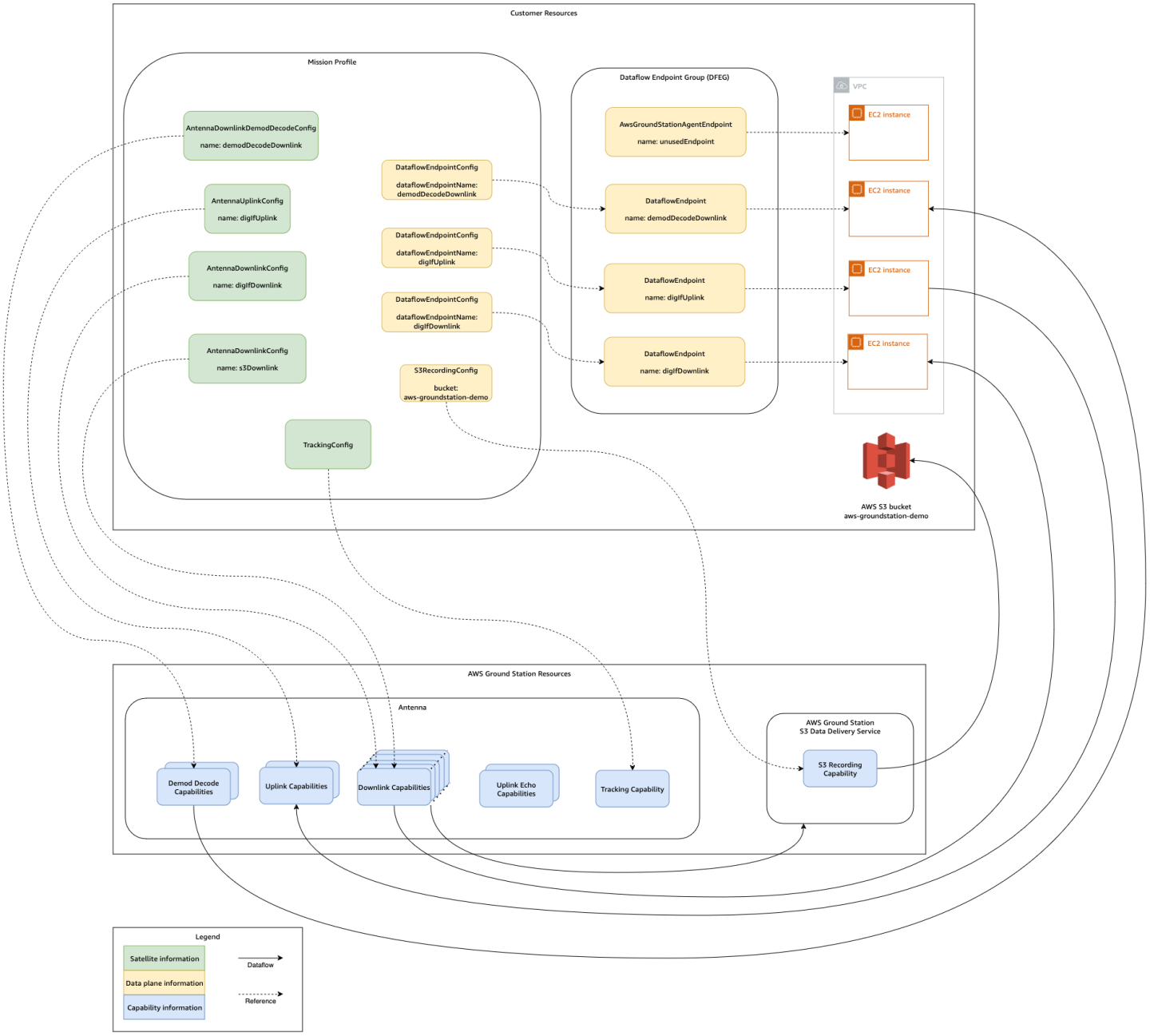
AWS Ground Station orchestrerà automaticamente le risorse AWS gestite durante la prenotazione dei contatti. Se applicabile, sei responsabile dell'orchestrazione delle EC2 risorse definite dal tuo

profilo di missione come endpoint del flusso di dati. AWS Ground Station fornisce AWS EventBridge eventi per automatizzare l'orchestrazione delle risorse per ridurre i costi. Per ulteriori dettagli, consulta Automazione AWS Ground Station con eventi.

Durante il contatto, viene fornita la telemetria sulle prestazioni del contatto a. AWS CloudWatch Per informazioni su come monitorare i contatti durante l'esecuzione, consulta. Monitoraggio

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 determineranno lo stato del COMPLETEDcontatto. Nei contatti per i quali errori di servizio hanno causato problemi di consegna dei dati durante il contatto verrà visualizzato FAILED lo stato AWS_. I contatti in cui gli errori del cliente o dell'utente hanno causato problemi di consegna dei dati durante il contatto restituiranno uno FAILEDstato. 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 Ciclo di vita dei contatti.

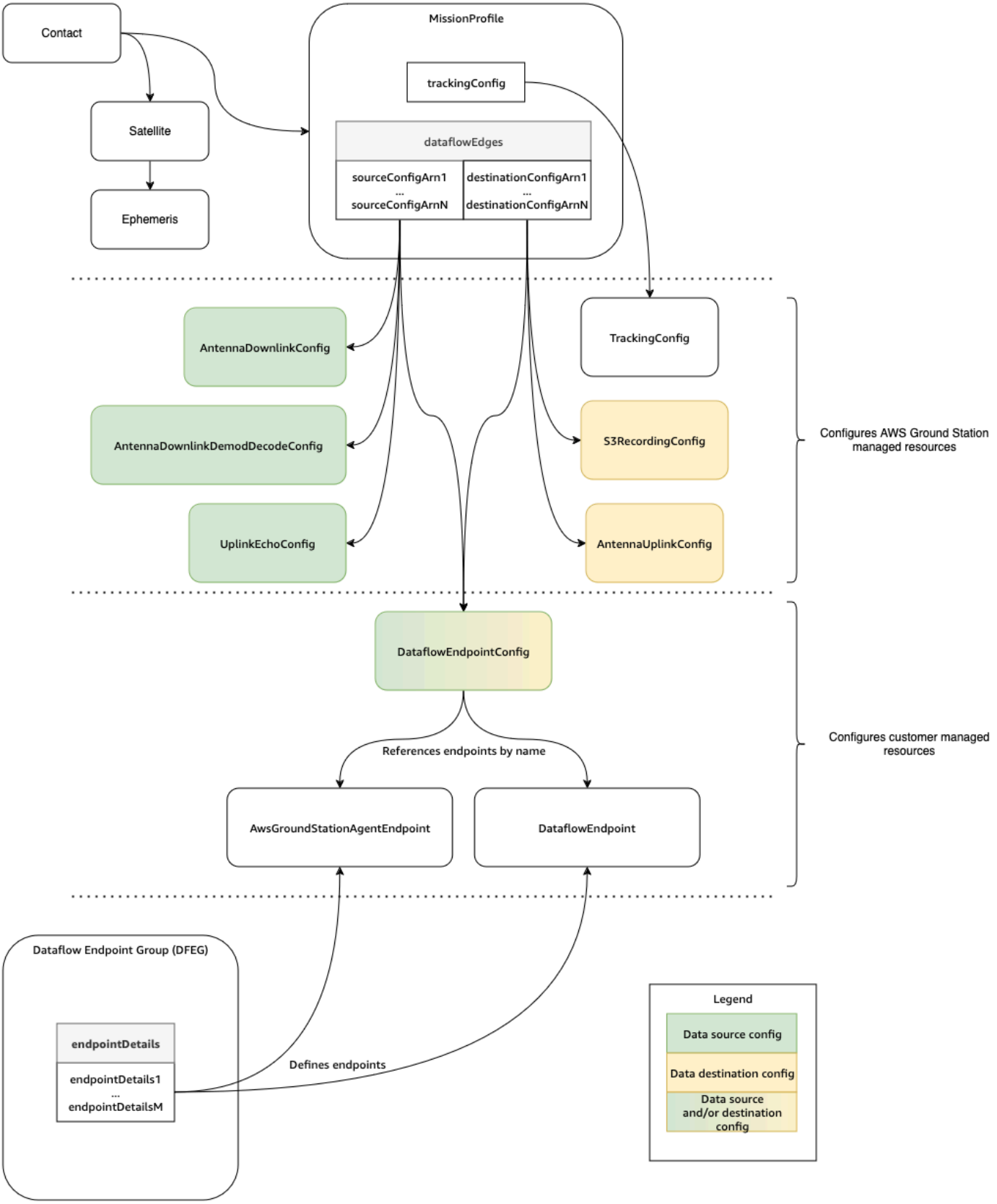
Gemello digitale

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 sito e GPS coordinate 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 AWS Ground Station gemello digitale.

Componenti 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

Profilo della 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.

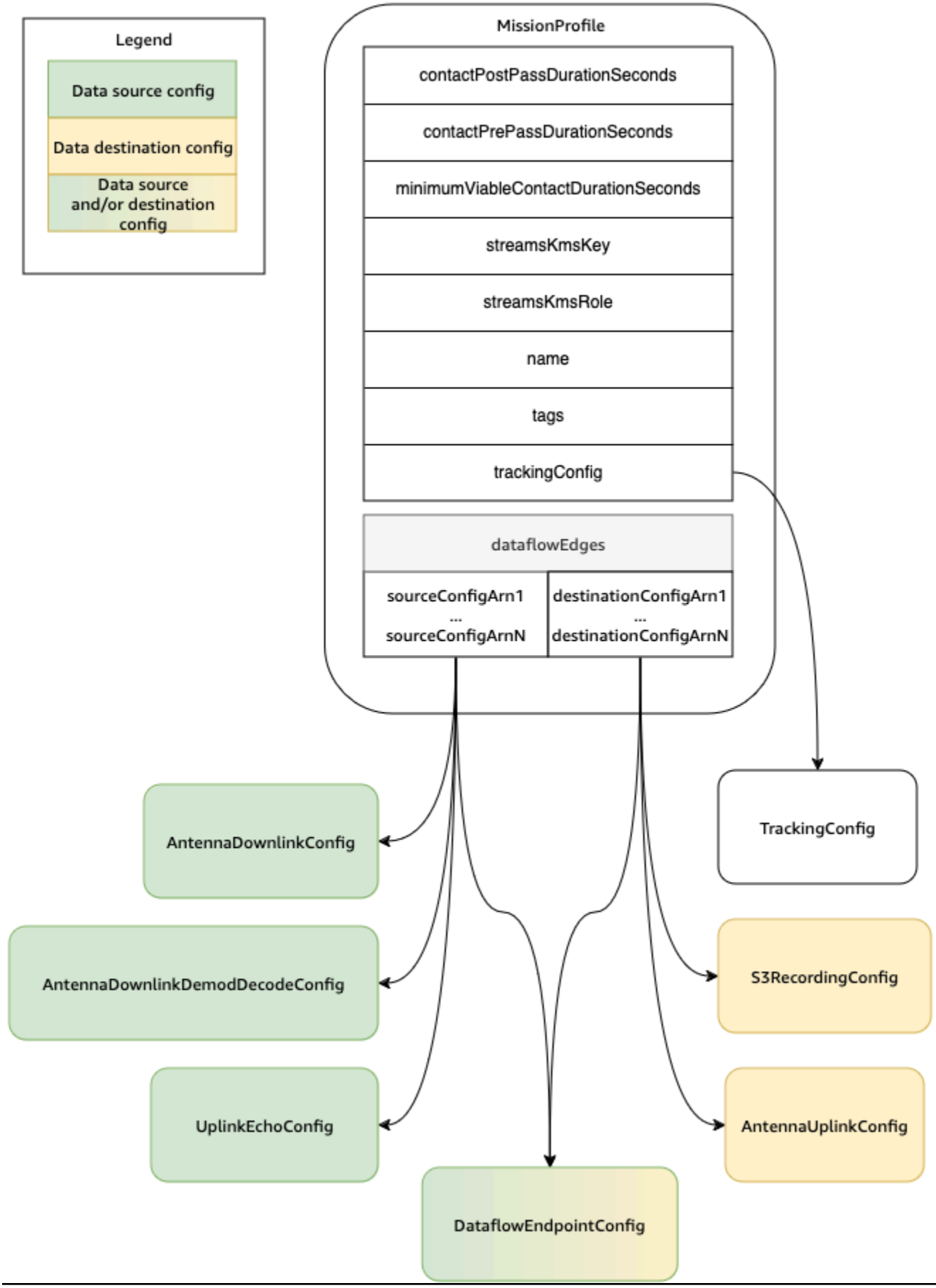
Le configurazioni di tracciamento sono specificate come campo unico all'interno del profilo di missione. Le configurazioni di tracciamento vengono utilizzate per specificare la preferenza per l'utilizzo del tracciamento del programma e del tracciamento automatico durante il contatto. Per ulteriori informazioni,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

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, leggiCiclo 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. Si prega di fare riferimentoCrittografia dei dati durante il transito per AWS Ground Station.


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

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

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

Config

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 due categorie:

- Configurazioni di tracciamento
- Configurazioni Dataflow

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	Origine/destinazione del flusso di dati
AntennaDownlinkConfig	Origine
AntennaDownlinkDemodDecodeConfig	Origine
UplinkEchoConfig	Origine
S3 RecordingConfig	Destinazione
AntennaUplinkConfig	Destinazione
DataflowEndpointConfig	Origine e/o destinazione

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

- AWS::GroundStation: :Tipo di risorsa Config CloudFormation
- Riferimento alla configurazione AWS CLI
- Riferimento alla configurazione API

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 utilizzata la traccia automatica. Si prega di fare riferimento Dati sulle effemeridi satellitari 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 AWS CloudFormation, il AWS Command Line Interface, o il AWS Ground Station API.

- AWSProprietà::GroundStation: :Config TrackingConfig CloudFormation
- AWS CLI Riferimento alla configurazione (vedi la `trackingConfig -> (structure)` sezione)
- TrackingConfig APIriferimento

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 Signal Data/IP. Per informazioni più dettagliate su come costruire flussi di dati con questa configurazione, vedi 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 downlink dell'antenna utilizzando AWS CloudFormation, il, o il. AWS Command Line Interface AWS Ground Station API

- AWSProprietà::GroundStation: :Config AntennaDownlinkConfig CloudFormation
- AWS CLI Riferimento alla configurazione (vedi la `antennaDownlinkConfig -> (structure)` sezione)
- AntennaDownlinkConfig APIriferimento

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 demodulazione e/o decodifica.
`<Se sei interessato a eseguire questi tipi di contatti, contatta il team inviand`
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 demodulato/decodificato. Per informazioni più dettagliate su come costruire flussi di dati con questa configurazione, vedi Flussi di dati

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

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

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 spettrale con frequenza, polarizzazione e potenza isotropa irradiata effettiva bersaglio (). 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 formato Signal Data/IP. Per informazioni più dettagliate su come costruire flussi di dati con questa configurazione, vedi Flussi di dati

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

- AWSProprietà::GroundStation: :Config AntennaUplinkConfig CloudFormation
- AWS CLI Riferimento alla configurazione (vedi la `antennaUplinkConfig -> (structure)` sezione)
- AntennaUplinkConfig APIriferimento

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. Una configurazione uplink echo contiene una configurazione uplink. ARN L'antenna utilizza i parametri della configurazione uplink a cui fa riferimento quando esegue un uplink echo. ARN

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

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

- AWSProprietà::GroundStation: :Config UplinkEchoConfig CloudFormation
- AWS CLI Riferimento alla configurazione (vedi la `uplinkEchoConfig -> (structure)` sezione)
- UplinkEchoConfig APIriferimento

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 dataflow 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, altrimenti diventerà _TO_. SCHEDULED FAILED 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. Flussi di datiPer ulteriori informazioni sui flussi di dati interregionali, consulta.

Consulta Gruppi 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 Flussi di dati

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

- AWSProprietà::GroundStation: :Config DataflowEndpointConfig CloudFormation
- AWS CLI Riferimento alla configurazione (vedi la `dataflowEndpointConfig -> (structure)` sezione)
- DataflowEndpointConfig APIriferimento

Config di registrazione Amazon S3

> **Note**
>
> Le configurazioni di registrazione di Amazon S3 vengono utilizzate solo per la consegna di dati ad Amazon S3 e non vengono utilizzate per la consegna di 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 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 IAM ruolo 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 della configurazione, l'id della risorsa di configurazione non esiste, la politica di fiducia deve utilizzare un asterisco (*) al posto di *your-config-id* e può essere aggiornato dopo la creazione con l'id della risorsa di configurazione.

Esempio di politica di fiducia

Per ulteriori informazioni su come aggiornare la politica di fiducia di un ruolo, consulta la sezione Gestione dei IAM ruoli nella Guida per l'IAMutente.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "groundstation.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "your-account-id"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:groundstation:config-region:your-account-id:config/
s3-recording/your-config-id"
        }
      }
    }
  ]
}
```

- Il IAM ruolo deve avere una IAM politica 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 ha una policy bucket, la policy bucket deve consentire anche al IAM ruolo 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 politica relativa ai ruoli, consulta Managing IAM policy nella Guida per l'IAMutente.

```
{
  "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 S3 utilizzando AWS CloudFormation, il, o il AWS Command Line Interface. AWS Ground Station API

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

Gruppi di endpoint Dataflow

Gli endpoint Dataflow definiscono la posizione in cui desiderate che i dati vengano trasmessi in modo sincrono da o verso 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.

> **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` Risoluzione dei problemi DataflowEndpointGroups in uno HEALTHY stato diverso

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

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

Endpoint del flusso di dati

I membri di un gruppo di endpoint dataflow sono endpoint dataflow. Gli endpoint Dataflow possono essere definiti per utilizzare l'agente o funzionare con un'applicazione endpoint dataflow. AWS Ground Station Per entrambi i tipi di istanze, creerai i costrutti di supporto (ad esempio gli indirizzi IP) prima di creare il gruppo di endpoint dataflow. Consulta 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.

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. Utilizza un AWS Ground Station Agent Dataflow Endpoint quando desideri eseguire il downlink di più del 50% di Digital Signal Data. MHz
Per creare 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 del segnale digitale, il downlink di meno del 50% dei dati del segnale digitale o il downlink dei dati dei segnali demodulati/decodificati. MHz 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 di creare Elastic Network Interfaces (ENIs) nel tuoVPC. 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 AWS Ground Station inserisce interfacce di rete elastiche per inviare flussi alle istanze.

Il IAM ruolo assegnato `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 IAM ruolo deve avere una IAM politica 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 politica 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",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "your-account-id"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:groundstation:dataflow-endpoint-region:your-
account-id:dataflow-endpoint-group/your-endpoint-id"
        }
      }
    }
  ]
}
```

Esempio di politica sui ruoli

Per ulteriori informazioni su come aggiornare o allegare una politica relativa ai ruoli, consulta Managing IAM policy nella Guida per l'IAMutente.

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

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups"
      ]
    }
  ]
}
```

AWS Ground Station Agente

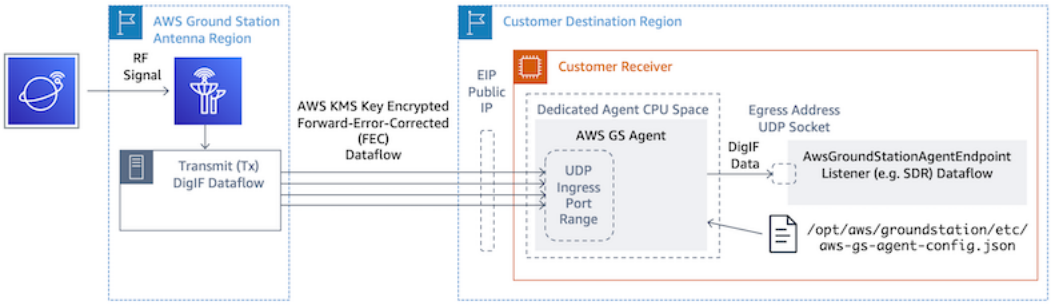
Che cos'è l' AWS Ground Station agente?

AWSGround Station Agent AWS Ground Station consente di ricevere (downlink) flussi di dati sincroni a banda larga digitale a frequenza intermedia (DigiF) durante i contatti con Ground Station. AWS È possibile selezionare due opzioni per la consegna dei dati:

1. Consegna dei dati a un'EC2istanza: consegna dei dati a un'EC2istanza 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 Flussi di dati sezione per informazioni sulla consegna EC2 dei dati.
2. Consegna dei dati a 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 consegna dei dati S3.

Entrambe le modalità di distribuzione dei dati richiedono la creazione di un set di AWS risorse. Si consiglia vivamente di CloudFormation utilizzarlo per creare AWS le proprie risorse per garantire affidabilità, precisione e supportabilità. Ogni contatto può fornire dati solo a EC2 o 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 () o un listener simile. SDR



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, durante la quale sarà necessario 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 AWS servizi 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. È possibile visualizzare l'attività corrente dell'account e gestire l'account in qualsiasi momento accedendo all'indirizzo https://aws.amazon.com/ e selezionando Il mio account.

Crea un utente con accesso amministrativo

Dopo la registrazione 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 AWS Management Consolecome 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 Signing in as the root user della Guida per l'utente di Accedi ad AWS .
2. Attiva l'autenticazione a più fattori (MFA) per il tuo utente root.

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

Crea un utente con accesso amministrativo

1. Abilita IAM Identity Center.

   Per istruzioni, consulta Abilitazione di AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center .
2. In IAM Identity Center, concedi 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 i valori predefiniti IAM Identity Center directory nella Guida per l'AWS IAM Identity Center utente.

Accesso come utente amministratore

- Per accedere con l'utente dell'IAMIdentity Center, utilizza l'accesso URL che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

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

Assegna l'accesso a ulteriori utenti

1. In IAM Identity Center, crea un set di autorizzazioni che segua la migliore pratica di applicazione delle autorizzazioni con privilegi minimi.

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 le AWS Ground Station 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 a AWS Management Console e apri la IAMconsole.
2. Creare una nuova policy. Utilizza le fasi seguenti:

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

   b. Nella JSONscheda, modificalo JSON con uno dei seguenti valori. Usa quello JSON che funziona meglio per la tua applicazione.

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

```
{
  "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:

```
{
  "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

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

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

Per ulteriori informazioni sugli IAM utenti e sulle relative politiche, consulta la Guida per l'IAMutente.

Fase 1: 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. 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 Posizioni sezione per determinare se il vostro satellite soddisfa le caratteristiche geografiche e di radiofrequenza.
2. Per iniziare l'onboarding del tuo satellite verso AWS Ground Station, invia un'e-mail a `<aws-groundstation@amazon.com>` con 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. AWS Ground Station gemello digitale
3. Una volta esaminata e approvata la richiesta, AWS Ground Station richiederemo 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 dei satelliti AWS Ground Station può essere effettuata tramite la risorsa tag API con AWS CLI o uno dei. AWS SDKs Questa guida tratterà l'uso del tag AWS Ground Station CLI per etichettare il satellite di trasmissione pubblica Aqua (Norad ID 27424) in. `us-west-2`

AWS Ground Station CLI

AWS CLI Possono essere usati per 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 AWS CLI versione 2.
- Assicurati che AWS CLI sia configurato. Per informazioni sulla configurazione AWS CLI, vedere Configurazione della AWS CLI versione 2.
- 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 AWS Ground Station contatti. 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 CLI comandi di AWS Ground Station per familiarizzare con i comandi disponibili. Segui la struttura dei AWS CLI comandi quando usi questo servizio e dai un prefisso `groundstation` ai comandi per specificarli AWS Ground Station come servizio che desideri utilizzare. Per ulteriori informazioni sulla struttura dei AWS CLI comandi, consulta Command Structure nella AWS CLI pagina. 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 il ARN satellite o i satelliti che desideri etichettare. Questo può essere fatto tramite l'elenco dei satelliti API in: AWS CLI

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

L'esecuzione del CLI comando 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 l'etichettatura è che la risorsa tag API richiede un valore regionale e quello ARN restituito da ARN list-satellites è globale. Per il passaggio successivo, dovresti aggiungere la ARN regione in cui vorresti vedere il tag (probabilmente la regione in cui effettui la programmazione). Per questo esempio, stiamo usando`us-west-2`. Con questa modifica, 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 la risorsa tag API 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 ARN nuovamente tag-resource with the 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 la risorsa untagAPI. Ciò API richiede il satellite ARN con la regione in cui si trova il tag e un elenco di chiavi dei tag. Per il nome, la chiave del tag è"Name". Un esempio di chiamata a questo API comando usando il AWS CLI seguente aspetto:

```
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 propri satelliti, è possibile 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/ -20 NOAA
- Terra

Una volta a bordo, è possibile accedere a questi satelliti per un uso immediato. AWS Ground Station mantiene una serie di AWS 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.

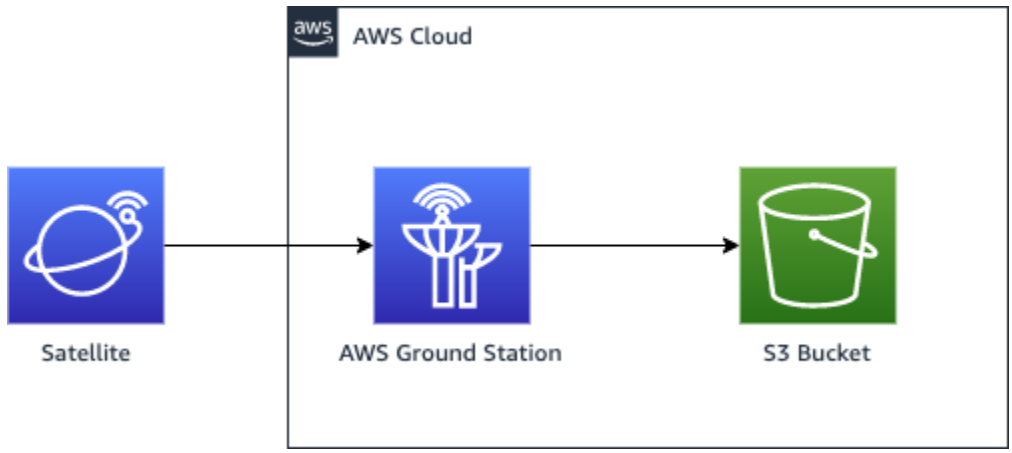
Per ulteriori informazioni su questi satelliti e sul tipo di dati che trasmettono, vedi Aqua, JPSS-1/ NOAA -20 and e Terra SNPP.

Fase 2: 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 AWS servizi come Amazon SageMaker 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.



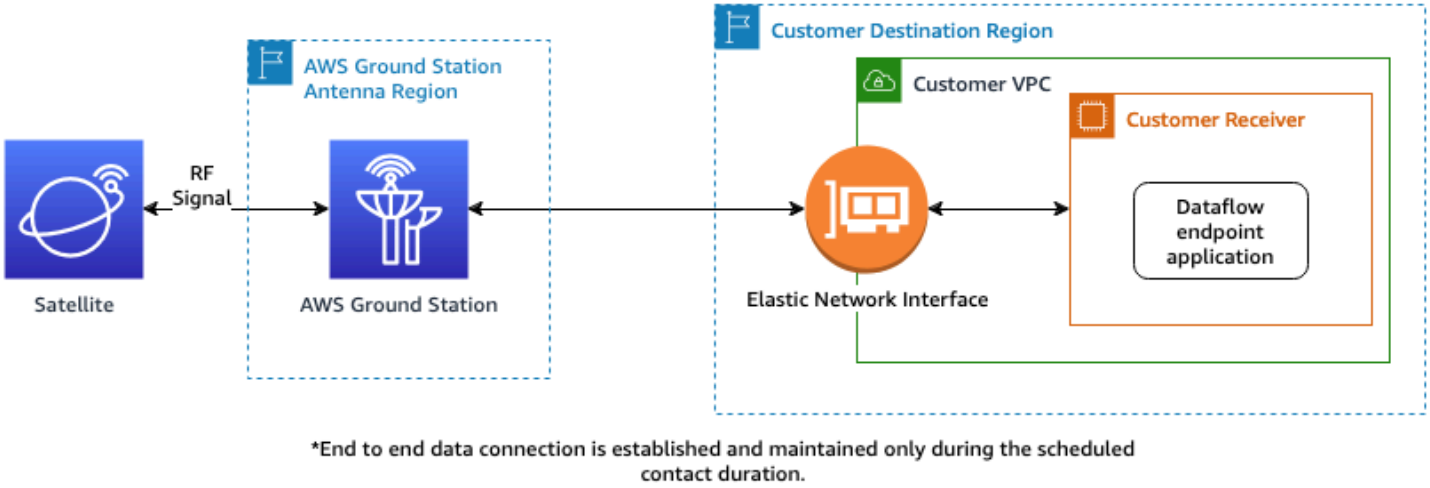
Per utilizzare questo percorso, dovrai creare un bucket Amazon S3 in cui distribuire AWS Ground Station i dati. Nel passaggio successivo, dovrai anche creare un Config di registrazione S3 nel passaggio successivo. Fai riferimento alle restrizioni sulla denominazione dei Config di registrazione Amazon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

Distribuzione sincrona dei dati

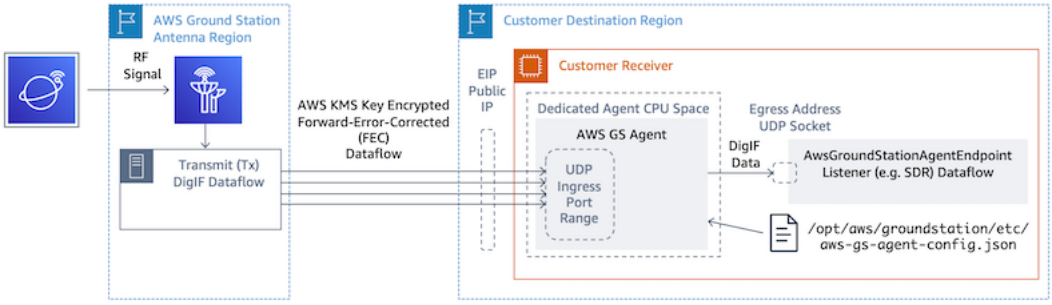
Con la consegna dei dati ad AmazonEC2, i dati di contatto vengono trasmessi in streaming da e verso l'EC2istanza Amazon. Puoi elaborare i dati in tempo reale sulla tua EC2 istanza Amazon o inoltrarli per la post-elaborazione.

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 aEC2- Installazione e configurazione. Per creare il tuo Dataflow Endpoint Group, fai riferimento a. Gruppi 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.



Fase 3: Creare configurazioni

A questo punto hai identificato il satellite, i percorsi di comunicazione e le IAM risorse 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 EC2 istanza Amazon.

Configurazioni satellitari

Le configurazioni satellitari riguardano il modo in cui AWS Ground Station è possibile comunicare con il satellite. Farai riferimento alle informazioni raccolte inFase 1: onboarding via satellite.

- 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.

Fase 4: Creare il profilo della missione

Con le configurazioni create nel passaggio precedente, hai identificato come tracciare il tuo satellite e i possibili modi per comunicare con il tuo satellite. In questa fase costruirai 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 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 Automazione AWS Ground Station con eventi.
7. [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.

Passaggi successivi

Ora che hai un satellite a bordo e un profilo di missione valido, sei pronto per pianificare 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.
- Il. AWS SDK ReserveContactAPI.

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

AWS Ground Station mantiene una serie di AWS 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 SDR Blink (e il repository associato aws-samples/) GitHub aws-groundstation-wbdigif-snpp

Posizioni

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

Individuazione della AWS regione per l'ubicazione di una stazione di terra

La rete AWS Ground Station globale include stazioni di terra che non si trovano fisicamente nella AWSregione a cui sono collegate. L'elenco delle stazioni terrestri a cui hai accesso può essere recuperato tramite la AWS SDK ListGroundStationrisposta. Di seguito è riportato l'elenco completo delle ubicazioni delle stazioni terrestri, con altre in arrivo a breve. Consultate la guida all'onboarding per aggiungere o modificare le approvazioni dei siti per i vostri satelliti.

Nome Ground Station	Ubicazione della Ground Station	AWSNome della regione	AWSCodice regionale	Note
Alaska 1	Alaska, USA	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, USA	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, USA	Stati Uniti orientali (Ohio)	us-east-2	
Oregon 1	Oregon, USA	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	AWSNome della regione	AWSCodice regionale	Note
Singapore 1	Singapore	Asia Pacific (Singapore)	ap-southeast-1	
Stoccolma 1	Stoccolma, Svezia	Europa (Stoccolma)	eu-north-1	

AWS Ground Station regioni supportate AWS

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

Disponibilità dei gemelli digitali

AWS Ground Station gemello digitaleè disponibile in tutte le AWSregioni 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 (RFIsorgenti esterne che influiscono su un segnale di downlink verso le antenne AWS Ground Station) sia sulla capacità di trasmissione (il segnale RF trasmesso dalle antenne 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 all'ubicazione di un'antenna, cambiare RFI le sorgenti o rinnovare l'autorizzazione legale con diverse restrizioni. Le maschere del sito AWS Ground Station sono disponibili in base a un accordo di non divulgazione ()NDA.

Maschere specifiche per il cliente

Oltre alle maschere del sito AWS Ground Station presenti 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 in modo case-by-case da garantire la conformità quando si utilizza AWS Ground Station per comunicare con questi satelliti. Contatta il team di AWS Ground Station per maggiori 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 al momento in cui 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 posizione di 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 - 8400 MHz	50 - 400 MHz	RHCP	Downlink a banda larga in banda X	La larghezza di banda aggregata deve essere inferiore a 400 MHz e gli intervalli di frequenza utilizzati
antenna - downlink	7750 - 8400 MHz	50 - 400 MHz	RHCP		
antenna - downlink	7750 - 8400 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 - 8400 MHz	50 - 400 MHz	RHCP		non devono sovrapporsi. Punta Arenas 1 max è 167. MHz Richiede GS Agent.
antenna - downlink	7750 - 8400 MHz	50 - 400 MHz	RHCP		
antenna - downlink	7750 - 8400 MHz	50 - 400 MHz	LHCP		
antenna - downlink	7750 - 8400 MHz	50 - 400 MHz	LHCP		
antenna - downlink	7750 - 8400 MHz	50 - 400 MHz	LHCP		
antenna - downlink	7750 - 8400 MHz	50 - 400 MHz	LHCP		
antenna - downlink	7750 - 8400 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		
antenna - downlink	7750 - 8400 MHz	Fino a 40 MHz	RHCP	Downlink a banda stretta in banda X	È possibile utilizzare una sola polarizzazione alla volta
antenna - downlink	7750 - 8400 MHz	Fino a 40 MHz	LHCP		

Tipo di capacità	Intervallo di frequenza	Intervallo di larghezza di banda	Polarization	Common Name (Nome comune)	Note
antenna-uplink	2025 - 2110 MHz	Fino a 40 MHz	RHCP	Uplink in banda S	È possibile utilizzare una sola polarizzazione alla volta EIRP20-53 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 - 8400 MHz	Fino a 500 MHz	RHCP	Downlink demodulato e decodificato a banda larga in banda X	
antenna-downlink-demod-decode	7750 - 8400 MHz	Fino a 500 MHz	LHCP		
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.

Dati sulle effemeridi satellitari

Un'effemeride, effemeridi plurale, 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.

AWS Ground Station utilizza i dati delle effemeridi per determinare quando i contatti diventano disponibili per il satellite e comandare correttamente le antenne della rete in modo che puntino verso il satellite. AWS Ground Station Per impostazione predefinita, non è richiesta alcuna azione per fornire AWS Ground Station effemeridi se al satellite è assegnato un ID. NORAD

Argomenti

Dati sulle effemeridi predefiniti

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 del satellite. TLEs NORAD Tutte le effemeridi predefinite hanno una priorità pari a 0. Di conseguenza, verranno sostituite, sempre, da tutte le effemeridi personalizzate non scadute caricate tramite le effemeridi, che devono sempre avere una priorità pari o superiore a 1API.

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

Fornitura di dati sulle effemeridi personalizzati

> **Important**
>
> Le effemeridi si trovano attualmente in uno API stato di anteprima

L'accesso alle effemeridi API viene fornito solo in base alle necessità.
<Se hai bisogno della possibilità di caricare dati personalizzati sulle effemeri

Panoramica

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

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

> **Note**
>
> Quando si forniscono effemeridi personalizzate prima che venga assegnato un numero di catalogo satellitare al satellite, è possibile utilizzare 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 TLE o dei OEM metadati (ad esempio 24000A per un veicolo lanciato nel 2024).
> Per ulteriori informazioni sul formato di, vedete Set di elementi a due righe. TLEs Per ulteriori informazioni sul formato diOEMs, vedereOEMformato effemeridi.

OEMformato effemeridi

AWS Ground Station elabora le effemeridi fornite dal OEM cliente secondo lo standard con alcune restrizioni aggiuntive. CCSDS OEMi file devono essere in formato. KVN La tabella seguente illustra i diversi campi di un file OEM e come si AWS Ground Station differenzia dallo CCSDS standard.

Sezione	Campo	CCSDSobbligatorio	AWS Ground Station richiesto	Note
Header	CCSDS_OEM_VERS	Sì	Sì	Valore richiesto: 2.0
	COMMENT	No	No	
	CLASSIFICATION	No	No	
	CREATION_DATE	Sì	Sì	
	ORIGINATOR	Sì	Sì	
	MESSAGE_ID	No	No	
Metadati	META_START	Sì	Sì	
	COMMENT	No	No	
	OBJECT_NAME	Sì	Sì	
	OBJECT_ID	Sì	Sì	
	CENTER_NAME	Sì	Sì	Valore richiesto: Terra
	REF_FRAME	Sì	Sì	Valori accettati: EME2 ITRF2000.000
	REF_FRAME_EPOCH	No	Non supportato*	Non necessario perché i REF_ accettati FRAMEs hanno un'epoca implicita

Sezione	Campo	CCSDSobbligatorio	AWS Ground Station richiesto	Note
	TIME_SYSTEM	Sì	Sì	Valore richiesto: UTC
	START_TIME	Sì	Sì	
	USEABLE_START_TIME	No	No	
	USEABLE_STOP_TIME	No	No	
	STOP_TIME	Sì	Sì	
	INTERPOLATION	No	Sì	Necessario in modo da AWS Ground Station poter generare angoli di puntamento accurati per i contatti.
	INTERPOLATION_DEGREES	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`

Sezione	Campo	CCSDSobbligatorio	AWS Ground Station richiesto	Note
	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`
	Z_ DDOT	No	No	Rappresentato in `km/s^2`
Matrice di covarianza	COVARIANCE_START	No	No	
	EPOCH	No	No	
	COV_REF_FRAME	No	No	
	COVARIANCE_STOP	No	No	

* Se nel file fornito AWS Ground Station sono incluse righe non supportate daOEM, la OEM convalida avrà esito negativo.

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

- CCSDS_ OEM _ VERS deve essere`2.0`.
- REF_ FRAME deve essere uno `EME2000` o l'altro`ITRF2000`.
- REF_ FRAME _ non EPOCH è supportato da AWS Ground Station.
- CENTER_ NAME deve essere`Earth`.
- TIME_ SYSTEM deve essere`UTC`.
- INTERPOLATIONe INTERPOLATION _ DEGREES sono entrambi obbligatori per AWS Ground Station CPE.

Esempio di OEM effemeridi in formato KVN

Di seguito è riportato un esempio troncato di OEM effemeride in formato per l'emittente satellitare pubblica -1. KVN JPSS

```
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 personalizzata

È possibile creare un'effemeride personalizzata utilizzando l'azione in. CreateEphemeris AWS Ground Station API 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 elemento a due righe () set ephemeris tramite TLE API

Il AWS SDKs, e CLI può essere usato per caricare un set di effemeridi a due righe (TLE) tramite la chiamata. AWS Ground Station CreateEphemeris Queste effemeridi verranno utilizzate al posto dei dati sulle effemeridi predefiniti per un satellite (vedi Default Ephemeris Data). Questo esempio mostra come eseguire questa operazione utilizzando AWS SDKfor Python (Boto3).

Un TLE set è un oggetto JSON formattato che unisce uno o più oggetti TLEs insieme per costruire una traiettoria continua. Ciò che TLEs fa parte del TLE set deve formare un insieme continuo che possiamo usare per costruire una traiettoria (cioè nessun intervallo di tempo tra un set e l'altro). TLEs TLE Di seguito è riportato un set di esempioTLE:

```
# example_tle_set.json
[
    {
        "tleLine1": "1 25994U 99068A   20318.54719794  .00000075  00000-0  26688-4 0
 9997",
        "tleLine2": "2 25994  98.2007  30.6589 0001234  89.2782  18.9934
 14.57114995111906",
        "validTimeRange": {
            "startTime": 12345,
            "endTime": 12346
        }
    },
    {
        "tleLine1": "1 25994U 99068A   20318.54719794  .00000075  00000-0  26688-4 0
 9997",
        "tleLine2": "2 25994  98.2007  30.6589 0001234  89.2782  18.9934
 14.57114995111906",
        "validTimeRange": {
            "startTime": 12346,
            "endTime": 12347
        }
    }
]
```

> **Note**
>
> Gli intervalli di tempo di TLEs in un TLE set devono corrispondere esattamente per essere una traiettoria valida e continua.

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

```
tle_ephemeris_id = ground_station_boto3_client.create_ephemeris( name="Example
 Ephemeris", satelliteId="2e925701-9485-4644-b031-EXAMPLE01", enabled=True,
 expirationTime=datetime.now(timezone.utc) + timedelta(days=3), priority=2,
    ephemeris = {
      "tle": {
        "tleData": [
            {
                "tleLine1": "1 25994U 99068A   20318.54719794  .00000075  00000-0
 26688-4 0  9997",
                "tleLine2": "2 25994  98.2007  30.6589 0001234  89.2782  18.9934
 14.57114995111906",
                "validTimeRange": {
                    "startTime": datetime.now(timezone.utc),
                    "endTime": datetime.now(timezone.utc) + timedelta(days=7)
                }
            }
        ]
      }
    })
```

Questa chiamata restituirà un elemento ephemerisId che può essere utilizzato per fare riferimento alle effemeridi in futuro. Ad esempio, possiamo usare quanto fornito ephemerisId dalla chiamata precedente per verificare lo stato delle effemeridi:

```
client.describe_ephemeris(ephemerisId=tle_ephemeris_id['ephemerisId'])
```

Di seguito viene fornito un esempio di risposta all'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.

Nota che l'NORADID totale del TLE set, TLEs negli esempi precedenti, deve corrispondere all'NORADID assegnato al satellite 25994 nel database Space-Track.

Esempio: caricamento di dati Ephemeris da un bucket S3

È anche possibile caricare un file di effemeridi 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 a riposo sono dettagliate in AWS Ground Station : Data Encryption At Rest For AWS Ground Station

Di seguito è riportato un esempio di caricamento di un file di OEM effemeridi da un bucket S3

```
s3_oem_ephemeris_id = ground_station_client.create_ephemeris( name="2022-10-26
 S3 OEM Upload", satelliteId="fde41049-14f7-413e-bd7b-EXAMPLE01", enabled=True,
 expirationTime=datetime.now(timezone.utc) + timedelta(days=5), priority=2,
    ephemeris = {
        "oem": {
            "s3Object": {
                "bucket": "ephemeris-bucket-for-testing",
                "key": "test_data.oem",
            }
        }
    })
```

Di seguito è riportato un esempio di dati restituiti dall'DescribeEphemerisazione richiesta per le OEM effemeridi 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"
      }
    }
  }
}
```

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 (ed è il repository associato AWS Ground Station aws-samples/) AWS Ground Station GitHub aws-groundstation-cpe

Quali effemeridi vengono utilizzate

Le effemeridi hanno una priorità, una data di scadenza e un flag abilitato. Insieme, determinano quali effemeridi vengono utilizzate per un satellite. Può essere attiva una sola effemeride 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 più alto 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. `ENABLED`AWS Ground Station Questa effemeride predefinita ha priorità 0.

Effetto delle nuove effemeridi sui contatti pianificati in precedenza

Utilizzate il DescribeContact APIper visualizzare gli effetti delle nuove effemeridi sui contatti pianificati in precedenza restituendo i tempi di visibilità attivi.

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 di trasmissione/ricezione. Pertanto, ti consigliamo di annullare e riprogrammare i tuoi contatti futuri dopo aver caricato una nuova effemeride che differisce notevolmente dalle precedenti. Con DescribeContact API, potete determinare la parte dei vostri contatti futuri che è inutilizzabile a causa del veicolo spaziale che opera al di fuori della maschera del sito di trasmissione/ricezione 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.

Ottenere 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

Le effemeridi predefinite includeranno solo i campi e. `source` `epoch` `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 a. API

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

```
{
    "satelliteId": "e1cfe0c7-67f9-4d98-bad2-06dbfc2d14a2",
    "satelliteArn": "arn:aws:groundstation::111122223333:satellite/e1cfe0c7-67f9-4d98-
bad2-06dbfc2d14a2",
    "noradSatelliteID": 12345,
    "groundStations": [
        "Example Ground Station 1",
        "Example Ground Station 2"
    ],
    "currentEphemeris": {
        "source": "SPACE_TRACK",
        "epoch": 8888888888
    }
}
```

Esempio **`GetSatellite`** di un satellite che utilizza un'effemeride personalizzata

```
{
      "satelliteId": "e1cfe0c7-67f9-4d98-bad2-06dbfc2d14a2",
      "satelliteArn": "arn:aws:groundstation::111122223333:satellite/
e1cfe0c7-67f9-4d98-bad2-06dbfc2d14a2",
      "noradSatelliteID": 12345,
      "groundStations": [
          "Example Ground Station 1",
          "Example Ground Station 2"
      ],
      "currentEphemeris": {
          "source": "CUSTOMER_PROVIDED",
          "ephemerisId": "e1cfe0c7-67f9-4d98-bad2-06dbfc2d14a2",
          "name": "My Ephemeris"
      }
  }
```

Ripristino dei dati di effemeridi predefiniti

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.

Per ripristinare le effemeridi Space-Track predefinite, è necessario eseguire 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 sulle effemeridi predefiniti.

Flussi di dati

AWS Ground Station utilizza una relazione tra nodo e perimetro per creare 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 sezioni seguenti descrivono come configurare le altre AWS risorse 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. Config

Argomenti

- AWS Ground Station interfacce del piano dati
- Utilizzo della distribuzione di dati tra regioni
- S3 - Installazione e configurazione
- VPC- Installazione e configurazione
- EC2- Installazione e configurazione

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 inferiore a 54MHz) i dati vengono forniti come -49 pacchetti Signal Data/IP Format. VITA
  - (Larghezza di banda da greater-than-or-equal -a 54) i dati vengono forniti come pacchetti di classe 2MHz. AWS Ground Station

- antenna-downlink-demod-decode
  - I dati vengono forniti come pacchetti di dati/IP demodulati/decodificati.
- antenna-uplink
  - I dati devono essere consegnati come pacchetti in formato VITA-49 Signal Data/IP.
- antenna-uplink-echo
  - I dati vengono consegnati come pacchetti in formato VITA-49 Signal Data/IP.

Utilizzo della 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 regione AWS Ground Station supportataAWS. Ciò significa che puoi mantenere la tua infrastruttura in un'unica AWS regione e pianificare i contatti in qualsiasi regione in AWS Ground Station Posizioni cui sei registrato.

La consegna dei dati tra regioni è attualmente disponibile in tutte le regioni AWS Ground Station supportate quando si ricevono i dati di contatto in un bucket Amazon S3. AWS Ground Station gestirà tutti gli aspetti della consegna per te.

La consegna di dati tra regioni ad Amazon EC2 con l' AWS Ground Station agente è disponibile in tutte le antenna-to-destination regioni. Non è richiesta alcuna configurazione o approvazione univoche per questa configurazione.

La consegna di dati tra regioni ad Amazon EC2 utilizzando un endpoint di flusso di dati è disponibile per impostazione predefinita* nelle regioni descritte di seguito. antenna-to-destination

- Regione degli Stati Uniti orientali (Ohio) (us-east-2) a Regione degli Stati Uniti occidentali (Oregon) (us-west-2)
- Regione degli Stati Uniti occidentali (Oregon) (us-west-2) a Regione degli Stati Uniti orientali (Ohio) (us-east-2)

Per utilizzare la consegna di dati tra regioni a un'EC2istanza Amazon, l'endpoint dataflow-endpoint deve essere creato nella tua AWS regione corrente e devi specificare la stessa regione. dataflow-endpoint-config

Le informazioni precedenti che descrivono in dettaglio le regioni supportate e i metodi di consegna per la consegna dei dati tra regioni sono riepilogate nella tabella seguente.

Metodo di ricezione	Regione dell'antenna	Regione di ricezione
Distribuzione dati Amazon S3	Tutti a bordo AWS Ground Station Posizioni	Tutte le regioni AWS Ground Station
AWS Ground Station Agente su Amazon EC2	Tutti a bordo AWS Ground Station Posizioni	Tutte le regioni AWS Ground Station
Endpoint Dataflow su Amazon* EC2	Regione Stati Uniti orientali (Ohio) (us-east-2)	Regione Stati Uniti occidentali (Oregon) (us-west-2)
	Regione Stati Uniti occidentali (Oregon) (us-west-2)	Regione Stati Uniti orientali (Ohio) (us-east-2)

*Le antenna-to-destination regioni aggiuntive non elencate richiedono una configurazione speciale di Amazon EC2 e del software. Contattaci all'<indirizzo aws-groundstation@amazon.com> per le istruzioni di onboarding.

S3 - Installazione e configurazione

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 IAM ruolo che autorizzi a scrivere file nel bucket. AWS Ground Station

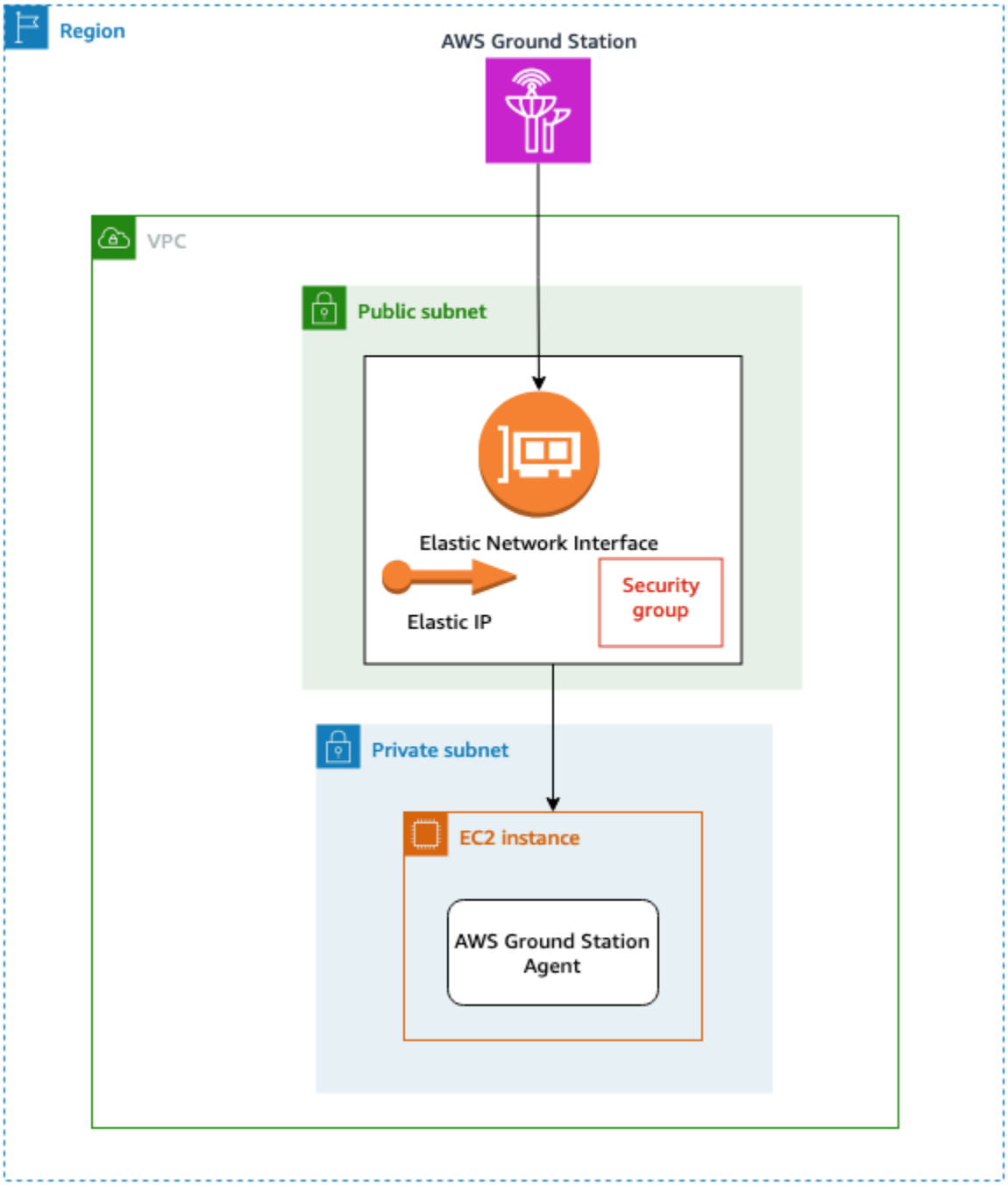
Consulta Config di registrazione Amazon S3 le restrizioni sulla creazione di bucket, IAM ruoli o AWS Ground Station configurazioni Amazon S3.

VPC- Installazione e configurazione

Una guida completa per configurare un VPC non rientra nell'ambito di questa guida. Per una comprensione approfondita, consulta la Guida per l'AWSVPCutente.

In questa sezione, viene descritto come il tuo endpoint Amazon EC2 e 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 su cui verranno utilizzati i vostriVPC, consultate. Esempi di configurazioni del profilo di missione

VPCConfigurazione con AWS Ground Station Agent



I dati satellitari vengono forniti a un'istanza di AWS Ground Station Agent 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 AWS di rete. 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 di For Agent VPC Delivery. AWS Ground Station

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

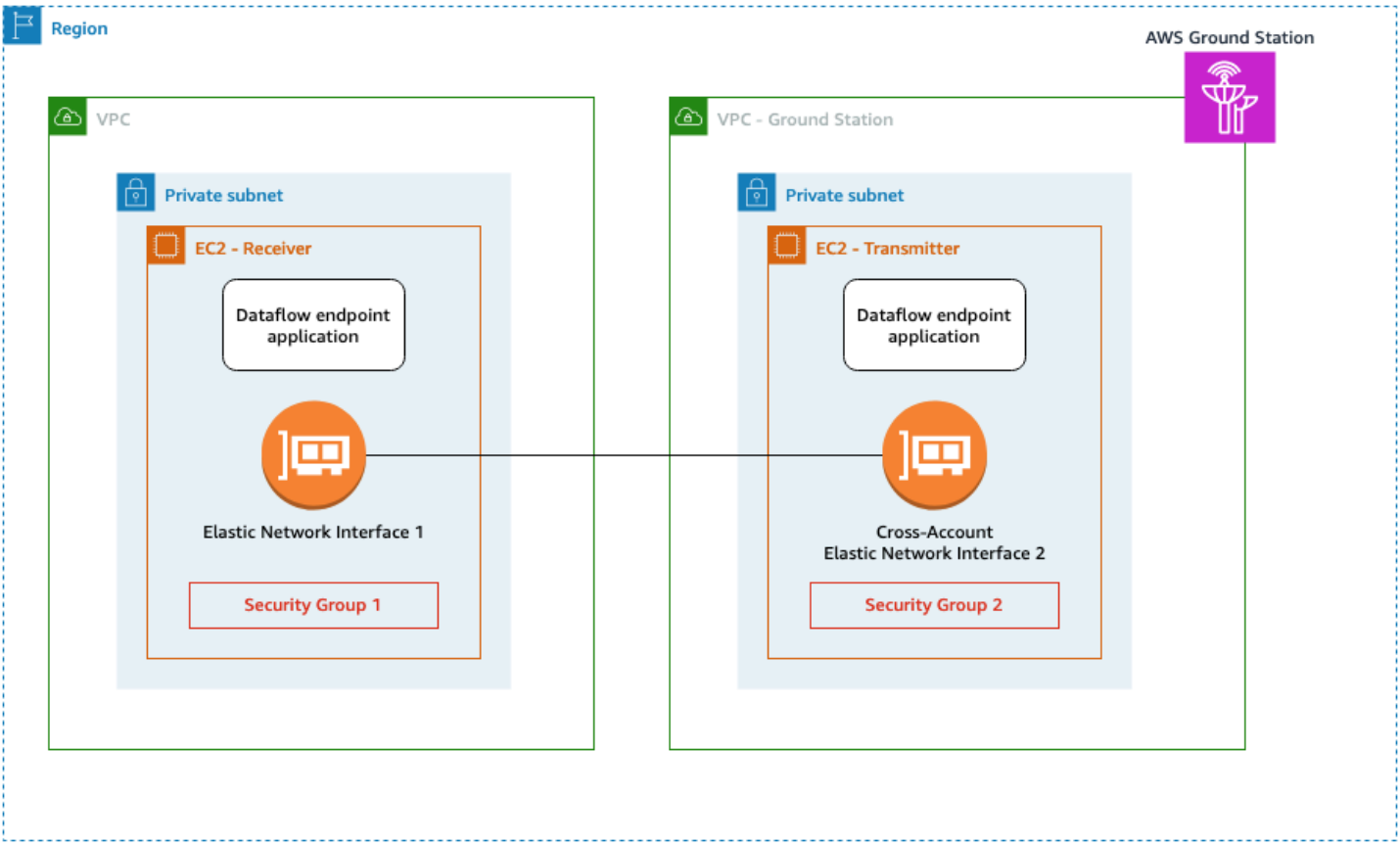
Elastic Network Interface (ENI): dovrai associare il gruppo di sicurezza di cui sopra a questo ENI e inserirlo nella tua sottorete pubblica.

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
```

VPCconfigurazione 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 account VPC di proprietà di. AWS Ground Station I dati arrivano quindi alla tua EC2 istanza tramite l'ENIallegato 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 la consegna degli endpoint VPC for dataflow.

IAMRuolo: il IAM ruolo fa parte dell'endpoint Dataflow e non è mostrato nel diagramma. Il IAM ruolo utilizzato per creare e collegare l'account incrociato ENI all'EC2istanza AWS Ground Station Amazon.

Gruppo di sicurezza 1: questo gruppo di sicurezza è collegato a quello ENI che verrà associato all'EC2istanza Amazon nel tuo account. Deve consentire il UDP traffico 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 posizionarlo in una sottorete.

Security Group 2: questo gruppo di sicurezza è referenziato nel Dataflow Endpoint. Questo gruppo di sicurezza verrà allegato a ENI quello che AWS Ground Station verrà utilizzato per inserire i dati nel tuo account.

Regione: per ulteriori informazioni sulle regioni supportate per le connessioni interregionali, consultaUtilizzo della 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"
```

EC2- Installazione e configurazione

La configurazione corretta dell'EC2istanza è necessaria per la consegna sincrona di -49 dati di segnale/IP o VITA -49 di estensione data/IP da fornire tramite l'VITAagente o un endpoint di flusso di dati. AWS Ground Station 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 sistema 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 software comuni per facilitare la configurazione dell'EC2istanza.

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.

Radio definita dal software () 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 all'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).

Contatti

È possibile inserire dati satellitari, identificare le posizioni delle antenne, comunicare e programmare l'orario dell'antenna per satelliti selezionati utilizzando la AWS Ground Station console o AWS SDK nella lingua desiderata. 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. Utilizzo della distribuzione di dati tra regioni

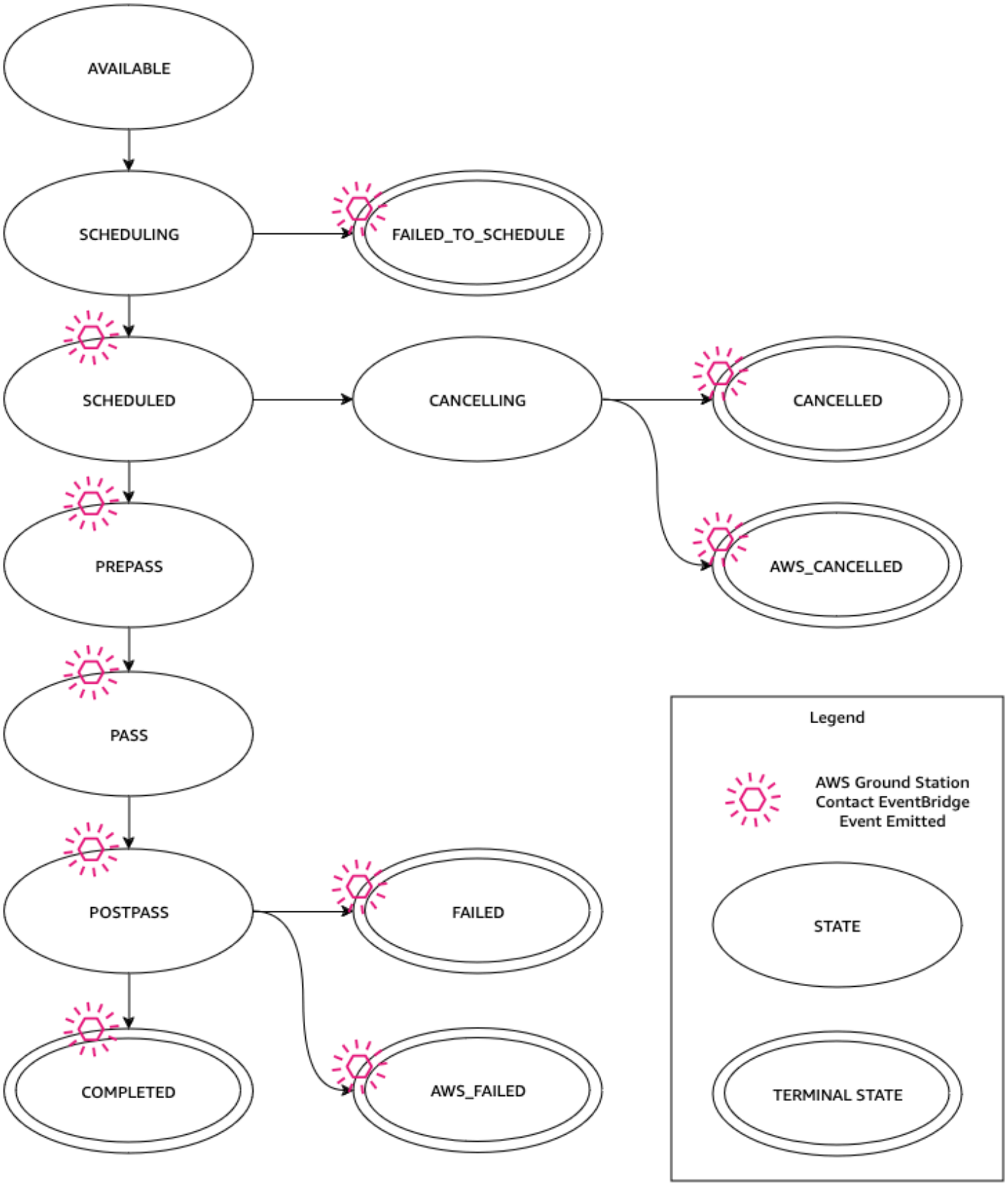
Per pianificare i contatti, è necessario configurare le risorse. Se non hai configurato le tue risorse, consultaNozioni di base.

* 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

Ciclo di vita dei contatti

La comprensione del ciclo di vita dei contatti può aiutare a determinare come configurare l'automazione e durante le attività di risoluzione dei problemi. 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,, FAILED _TO_COMPLETED,FAILED, _ e _ sono stati SCHEDULE CANCELLED terminaliAWS. CANCELLED AWS FAILED I contatti non passeranno da uno stato terminale. AWS Ground Station stati dei contattiPer ulteriori informazioni su ciò che indica ogni stato, consulta la sezione.


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

Di seguito è riportato l'elenco degli stati che un contatto può avere:

- AVAILABLE- Il contatto è disponibile per essere prenotato.
- SCHEDULING- Il contatto è in fase di pianificazione.
- SCHEDULED- Il contatto è stato pianificato con successo.
- FAILED_TO_ SCHEDULE - Il contatto non è riuscito a programmare.
- PREPASS- Il contatto inizierà a breve e le risorse sono in fase di preparazione.
- PASS- Il contatto è attualmente in esecuzione e con il satellite è in corso la comunicazione.
- POSTPASS- La comunicazione è stata completata e le risorse utilizzate vengono ripulite.
- COMPLETED- Il contatto è stato completato senza errori.
- FAILED- Il contatto non è riuscito a causa di un problema con la configurazione delle risorse.
- AWS_ FAILED - Il contatto non è riuscito a causa di un problema nel AWS Ground Station servizio.
- CANCELLING- Il contatto è in fase di annullamento.
- 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.
- CANCELLED- Il contatto è stato annullato da te.

AWS Ground Station gemello digitale

La funzionalità digital twin per ti AWS Ground Station offre un ambiente in cui puoi 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 iniziareFase 1: onboarding via satellite, 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. AWS SDK ListGroundStations Le stazioni di terra gemelle digitali sono copie esatte delle stazioni di terra elencate Posizioni con un prefisso modificabile in Ground Station Nome di «Digital Twin». Ciò include le loro funzionalità di metadati e antenna, incluse, a titolo esemplificativo, la maschera del sito e le coordinate effettive. GPS Al momento, la funzionalità digital twin non supporta la consegna dei dati come descritto inFlussi di dati.

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

Monitoraggio

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

- AWS EventBridge Events fornisce 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, in quanto è possibile 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 API chiamate e gli eventi correlati effettuati da o per conto del tuo AWS account e invia i file di registro 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'utentepuò 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. È possibile ricevere notifiche per gli eventi tramite più canali, tra cui e-mail, notifiche chat AWS Chatbot o notifiche push AWS Console Mobile Application. Puoi anche visualizzare le notifiche nel Centro notifiche della AWS console. Notifiche all'utente aggregazione dei supporti, che può ridurre il numero di notifiche ricevute durante eventi specifici.

Usa i seguenti argomenti per monitorare AWS Ground Station.

Argomenti

- Automazione AWS Ground Station con eventi
- Registrazione delle AWS Ground Station API chiamate con AWS CloudTrail
- Metriche con Amazon CloudWatch

Automazione AWS Ground Station con eventi

> **Note**
>
> In questo documento viene utilizzato ovunque il termine «evento». CloudWatch Events e EventBridge sono lo stesso servizio sottostante eAPI. È possibile creare regole per abbinare gli eventi in arrivo e indirizzarli verso le destinazioni per l'elaborazione 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 includono:

- Invocare una funzione AWS Lambda
- Richiamo del comando Amazon EC2 Run
- Inoltro dell'evento a Amazon Kinesis Data Streams
- Attivazione di una macchina a stati AWS Step Functions
- Notifica di un SNS argomento 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 EC2 Amazon in base allo stato dell'evento.
- Pubblicazione su un SNS argomento Amazon 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

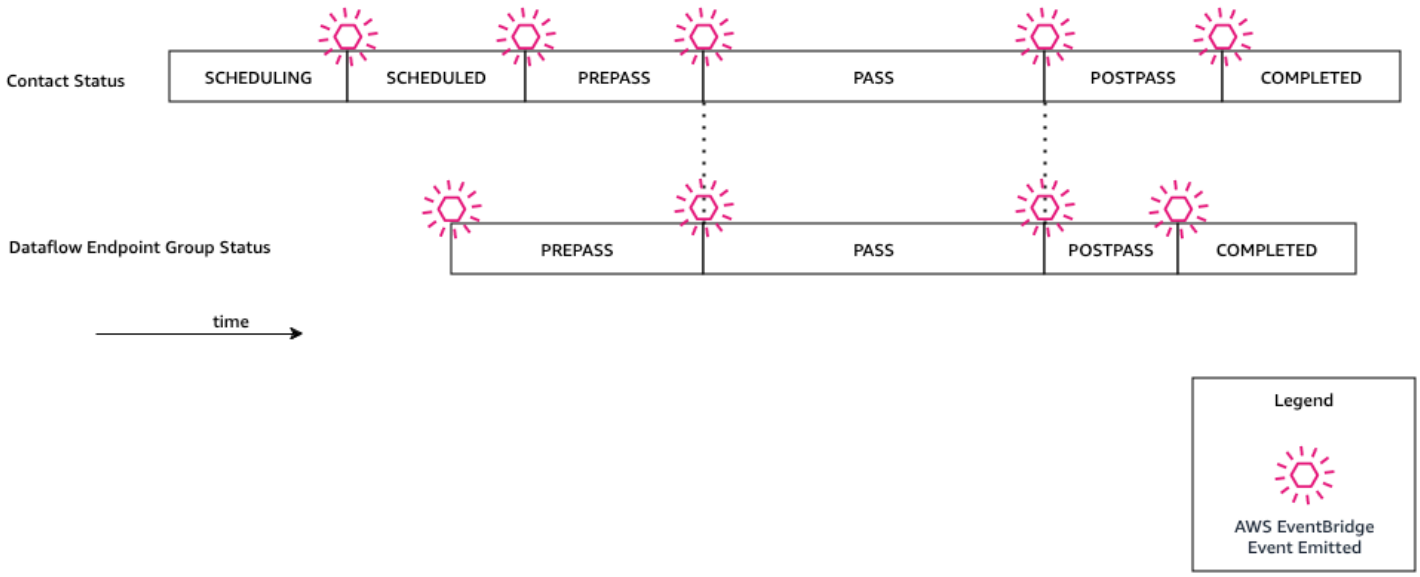
> **Note**
>
> Tutti gli eventi generati da AWS Ground Station hanno «aws.groundstation» come valore per «source».

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

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

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` includonoENABLED,,,VALIDATING, INVALID ERROR DISABLED EXPIRED

Registrazione delle AWS Ground Station API chiamate 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 API chiamate AWS Ground Station come eventi. Le chiamate acquisite includono chiamate dalla AWS Ground Station console e chiamate in codice alle AWS Ground Station API operazioni. 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, 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 crei un percorso nella console, il percorso si applica a tutte le AWS regioni. 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 di Amazon SNS Notifications 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 nel Reference.AWS Ground Station API 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 l'CloudTrail userIdentityelemento.

Comprendere AWS Ground Station le 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 stack ordinata delle API chiamate 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"
}
```


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.

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.

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

Parametro	Dimensioni parametro	Descrizione
		Gli errori dei blocchi sono causati da interferenze. Unità: Blocchi errati/Numero totale di blocchi
`CarrierFrequencyRecovery_Cn0`	Categoria, Config, SatelliteId	Rapporto tra portante e densità di rumore per unità di larghezza di banda. Unità: Decibel-Hertz (dB-Hz)
`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

Parametro	Dimensioni parametro	Descrizione
`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)
`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)

Parametro	Dimensioni parametro	Descrizione
`ReceivedPower`	Polarizzazione, SatelliteId	La potenza del segnale misurata nel demodulatore/decodificatore. Unità: decibel rispetto ai milliwatt () dBm
`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

Parametro	Dimensioni parametro	Descrizione
`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.

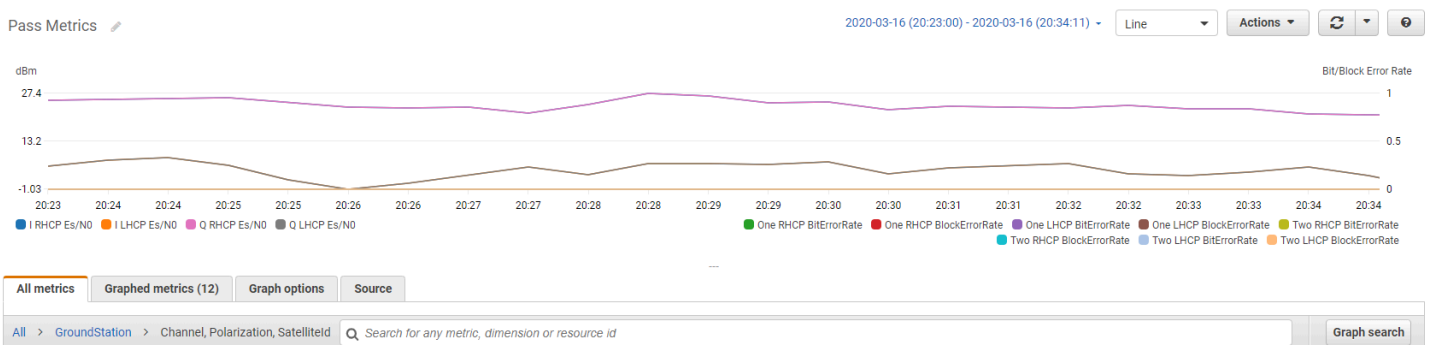
Dimensione	Descrizione
`Category`	Demodulazione o decodifica.
`Channel`	I canali per ogni contatto includono Uno, Due, I (in fase) e Q (quadratura).
`Config`	Un'antenna downlink demod decode config arn.
`Polarization`	La polarizzazione per ogni contatto include LHCP (Polarizzata circolare sinistra) o RHCP (Polarizzata circolare destra).

Dimensione	Descrizione
`SatelliteId`	L'ID satellitare contiene il satellite per ARN 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 la scadenza di quel periodo di 3 ore. Se devi visualizzare le metriche in base a 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.

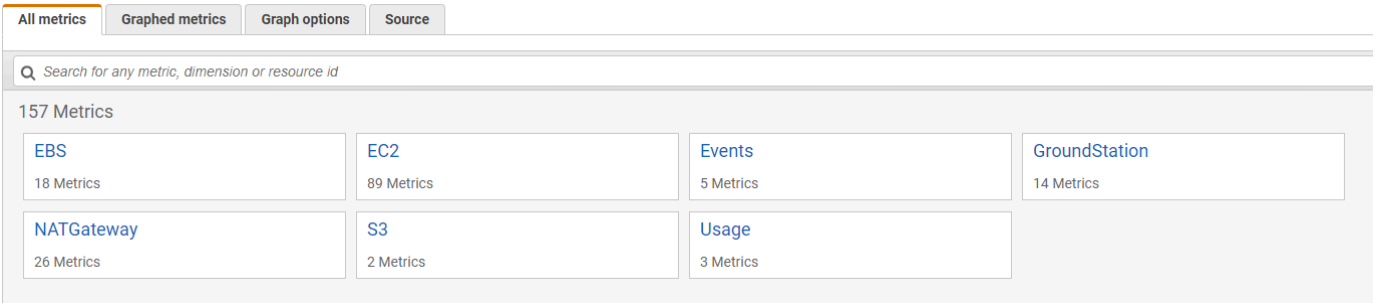
Inoltre, i dati acquisiti entro i primi 60 secondi non conterranno informazioni sufficienti per produrre parametri significativi e probabilmente non verranno visualizzati. Per visualizzare metriche significative, si consiglia di visualizzare i dati dopo 60 secondi.



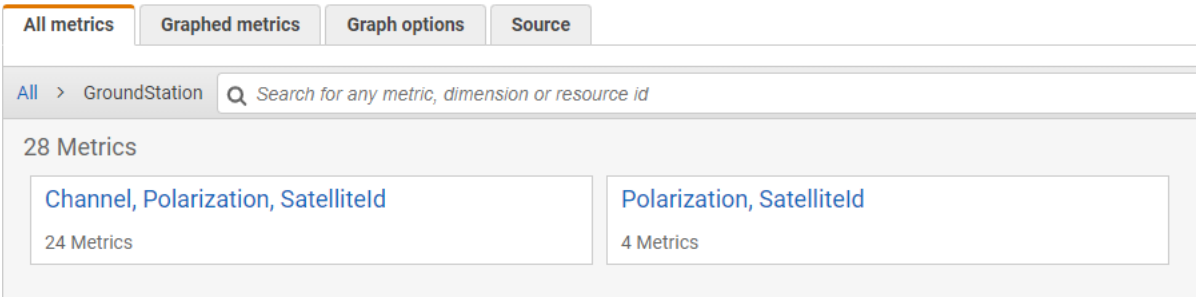
Per ulteriori informazioni sulla rappresentazione grafica delle AWS Ground Station metriche in CloudWatch, consulta Graphing Metrics.

Per visualizzare i parametri tramite la console

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



4. Seleziona le dimensioni metriche desiderate (ad esempio, Canale, Polarizzazione,). SatelliteId



5. La scheda All metrics (Tutti i parametri) visualizza tutti i parametri per tale dimensione nello spazio dei nomi. Puoi eseguire le operazioni indicate di seguito:

   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

1. Assicurati che AWS CLI sia installato. Per informazioni sull'installazione AWS CLI, consulta Installazione della AWS CLI versione 2.
2. Utilizza il get-metric-datametodo di 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 --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": ""
   }
}
```

3. Elenca le CloudWatch metriche disponibili `aws cloudwatch list-metrics` 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**
>
> A causa di una limitazione di CloudWatch, 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 sulla limitazione, consulta: Visualizza le metriche CloudWatch disponibili

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

5. 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 --cli-input-json file://
<nameOfConfigurationFileCreatedInStep2>.json
```

I parametri verranno fornite con i timestamp del tuo contatto. Di seguito viene fornito un esempio di output AWS Ground Station delle metriche.


```
{
   "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. AWSfornisce strumenti e funzionalità specifici per la sicurezza per aiutarti a raggiungere i tuoi 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, si consiglia di seguire le migliori pratiche del settore e di implementare la crittografia. end-to-end AWSconsente APIs di integrare la crittografia e la protezione dei dati. Per ulteriori informazioni sulla AWS sicurezza, consulta il white paper Introduzione alla AWS sicurezza.

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 dispositivo AWS servizio che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. IAMgli amministratori controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse. AWS Ground Station IAMè un dispositivo AWS servizio che puoi utilizzare senza costi aggiuntivi.

Argomenti

- 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 usi AWS Identity and Access Management (IAM) varia a seconda del lavoro che svolgi. AWS Ground Station

Utente del servizio: se utilizzi il AWS Ground Station servizio per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più AWS Ground Station funzionalità per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di AWS Ground Station, consulta Risoluzione dei problemi AWS Ground Station di identità e accesso.

Amministratore del servizio: se sei responsabile delle AWS Ground Station risorse della tua azienda, probabilmente hai pieno accesso a AWS Ground Station. È tuo compito determinare a quali AWS Ground Station funzionalità e risorse devono accedere gli utenti del servizio. È quindi necessario inviare richieste all'IAMamministratore per modificare le autorizzazioni degli utenti del servizio. Consulta le informazioni contenute in questa pagina per comprendere i concetti di base diIAM. Per ulteriori informazioni su come la tua azienda può utilizzare IAM con AWS Ground Station, consultaCome AWS Ground Station funziona con IAM.

IAMamministratore: se sei un IAM amministratore, potresti voler conoscere i dettagli su come scrivere politiche a cui gestire l'accesso AWS Ground Station. Per visualizzare esempi di policy AWS Ground Station basate sull'identità che puoi utilizzare inIAM, 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. È necessario autenticarsi (accedere a AWS) come Utente root dell'account AWS, come IAM utente o assumendo un ruolo. IAM

È possibile accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAMIdentity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Quando

accedi come identità federata, l'amministratore aveva precedentemente configurato la federazione delle identità utilizzando i ruoli. IAM Quando si accede AWS utilizzando la federazione, si assume indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando () per firmare crittograficamente le tue richieste utilizzando le tue credenziali. CLI Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta Firmare AWS API le richieste nella Guida per l'IAMutente.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'AWS IAM Identity Center utente e Utilizzo dell'autenticazione a più fattori (MFA) AWS nella Guida per l'IAMutente.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte AWS servizi le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per l'elenco completo delle attività che richiedono l'accesso come utente root, consulta Attività che richiedono le credenziali dell'utente root nella Guida per l'IAMutente.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere AWS servizi utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, un provider di identità Web AWS Directory Service, la directory Identity Center o qualsiasi utente che accede AWS servizi utilizzando credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per informazioni su IAM Identity Center, vedi Cos'è IAM Identity Center? nella Guida AWS IAM Identity Center per l'utente.

IAM users and groups

Un IAMutente è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Laddove possibile, consigliamo di fare affidamento su credenziali temporanee anziché creare IAM utenti con credenziali a lungo termine come password e chiavi di accesso. Tuttavia, se hai casi d'uso specifici che richiedono credenziali a lungo termine con IAM gli utenti, ti consigliamo di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta Ruotare regolarmente le chiavi di accesso per i casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente. IAM

Un IAMgruppo è un'identità che specifica un insieme di utenti. IAM Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, è possibile assegnare un nome a un gruppo IAMAdminse concedere a tale gruppo le autorizzazioni per IAM amministrare le risorse.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Quando creare un IAM utente (anziché un ruolo) nella Guida per l'IAMutente.

IAMruoli

Un IAMruolo è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un IAM utente, ma non è associato a una persona specifica. È possibile assumere temporaneamente un IAM ruolo in AWS Management Console cambiando ruolo. È possibile assumere un ruolo chiamando un' AWS APIoperazione AWS CLI or o utilizzando un'operazione personalizzataURL. Per ulteriori informazioni sui metodi di utilizzo dei ruoli, vedere Utilizzo IAM dei ruoli nella Guida per l'IAMutente.

IAMi ruoli con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per informazioni sui ruoli per la federazione, vedere Creazione di un ruolo per un provider di identità di terze parti nella Guida per l'IAMutente. Se utilizzi IAM Identity Center, configuri un set di autorizzazioni. Per controllare a cosa possono accedere le identità dopo l'autenticazione, IAM Identity Center correla il set di autorizzazioni a un ruolo in. IAM Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .
- Autorizzazioni IAM utente temporanee: un IAM utente o un ruolo può assumere il IAM ruolo di assumere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso su più account: puoi utilizzare un IAM ruolo per consentire a qualcuno (un responsabile fidato) di un altro account di accedere alle risorse del tuo account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni AWS servizi, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per conoscere la differenza tra ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta la sezione Accesso alle risorse su più account IAM nella Guida per l'utente. IAM
- Accesso tra servizi: alcuni AWS servizi utilizzano funzionalità in altri. AWS servizi Ad esempio, quando effettui una chiamata in un servizio, è normale che quel servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Sessioni di accesso diretto (FAS): quando utilizzi un IAM utente o un ruolo per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FASutilizza le autorizzazioni del principale che chiama an AWS servizio, in combinazione con la richiesta di effettuare richieste AWS servizio ai servizi downstream. FASle richieste vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri AWS servizi o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli FAS delle politiche relative alle richieste, consulta Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è un IAMruolo che un servizio assume per eseguire azioni per conto dell'utente. Un IAM amministratore può creare, modificare ed eliminare un ruolo di servizio dall'internoIAM. Per ulteriori informazioni, vedere Creazione di un ruolo per delegare le autorizzazioni a un utente AWS servizio nella Guida per l'IAMutente.
  - Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. AWS servizio Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli

collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un IAM amministratore può visualizzare, ma non modificare le autorizzazioni per i ruoli collegati al servizio.

- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un IAM ruolo per gestire le credenziali temporanee per le applicazioni in esecuzione su un'EC2istanza e che effettuano AWS CLI o richiedono AWS API. È preferibile archiviare le chiavi di accesso all'interno dell'EC2istanza. Per assegnare un AWS ruolo a un'EC2istanza e renderlo disponibile per tutte le sue applicazioni, create un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull'EC2istanza di ottenere credenziali temporanee. Per ulteriori informazioni, consulta Usare un IAM ruolo per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella Guida per l'IAMutente.

Per sapere se utilizzare IAM ruoli o IAM utenti, consulta Quando creare un IAM ruolo (anziché un utente) nella Guida per l'IAMutente.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e associandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come JSON documenti. Per ulteriori informazioni sulla struttura e il contenuto dei documenti relativi alle JSON politiche, vedere Panoramica delle JSON politiche nella Guida per l'IAMutente.

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

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un IAM amministratore può creare IAM politiche. L'amministratore può quindi aggiungere le IAM politiche ai ruoli e gli utenti possono assumerli.

IAMle politiche definiscono le autorizzazioni per un'azione indipendentemente dal metodo utilizzato per eseguire l'operazione. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale criterio può ottenere informazioni sul ruolo da AWS Management Console, da o da. AWS CLI AWS API

Policy basate su identità

I criteri basati sull'identità sono documenti relativi alle politiche di JSON autorizzazione che è possibile allegare a un'identità, ad esempio un IAM utente, un gruppo di utenti o un ruolo. Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una politica basata sull'identità, consulta Creazione di politiche nella Guida per l'utente. IAM IAM

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli all'interno del tuo. Account AWS Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una politica gestita o una politica in linea, consulta Scelta tra politiche gestite e politiche in linea nella Guida per l'IAMutente.

Policy basate su risorse

Le politiche basate sulle risorse sono documenti di JSON policy allegati a una risorsa. Esempi di politiche basate sulle risorse sono le policy di trust dei IAM ruoli 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. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. AWS servizi

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

Elenchi di controllo degli accessi () 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. ACLssono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy. JSON

Amazon S3 e Amazon VPC sono esempi di servizi che supportano. AWS WAF ACLs Per ulteriori informazioniACLs, consulta la panoramica di Access control list (ACL) nella Amazon Simple Storage Service Developer Guide.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite di autorizzazioni è una funzionalità avanzata in cui si impostano le autorizzazioni massime che una politica basata sull'identità può concedere a un'entità (utente o ruolo). IAM IAM È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal`sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità nella Guida per l'utente. IAM IAM
- Politiche di controllo del servizio (SCPs): SCPs sono JSON politiche che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità di un'organizzazione, puoi applicare le politiche di controllo del servizio (SCPs) a uno o tutti i tuoi account. SCPLimita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna Utente root dell'account AWS. Per ulteriori informazioni su Organizations andSCPs, consulta le politiche di controllo dei servizi nella Guida AWS Organizations per l'utente.
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta le politiche di sessione nella Guida IAM per l'utente.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per informazioni su come AWS determinare se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle politiche nella Guida per l'IAMutente.

Come AWS Ground Station funziona con IAM

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

IAMfunzionalità che puoi usare con AWS Ground Station

IAMcaratteristica	AWS Ground Station supporto
Policy basate su identità	Sì
Policy basate su risorse	No
Azioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione della policy (specifica del servizio)	Sì
ACLs	No
ABAC(tag nelle politiche)	Sì
Credenziali temporanee	Sì
Autorizzazioni del principale	Sì
☻Ruoli di servizio	No
Ruoli collegati al servizio	Sì

Per avere una panoramica generale del funzionamento AWS Ground Station e degli altri AWS servizi con la maggior parte delle IAM funzionalità, consulta AWS i servizi che funzionano con la maggior parte delle funzionalità IAM nella Guida per l'IAMutente.

Politiche basate sull'identità per AWS Ground Station

Supporta le policy basate su identità: sì

Le politiche basate sull'identità sono documenti relativi alle politiche di JSON autorizzazione che è possibile allegare a un'identità, ad esempio un IAM utente, un gruppo di utenti o un ruolo. Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una politica basata sull'identità, consulta Creazione di politiche nella Guida per l'utente. IAM IAM

Con le politiche IAM basate sull'identità, puoi specificare azioni e risorse consentite o negate, nonché le condizioni in base alle quali le azioni sono consentite o negate. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per ulteriori informazioni su tutti gli elementi che è possibile utilizzare in una JSON politica, vedere il riferimento agli elementi IAM JSON della politica nella Guida per l'IAMutente.

Esempi di policy 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 politiche basate sulle risorse sono documenti di JSON policy allegati a una risorsa. Esempi di politiche basate sulle risorse sono le policy di trust dei IAM ruoli 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. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. AWS servizi

Per abilitare l'accesso tra più account, puoi specificare un intero account o IAM entità in un altro account come principale in una politica basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa sono diversi Account AWS, un IAM amministratore dell'account fidato deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta Cross Account Resource Access IAM nella Guida IAM per l'utente.

Azioni politiche per AWS Ground Station

Supporta le operazioni di policy: si

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

L'`Action`elemento di una JSON policy descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a una policy. Le azioni politiche in genere hanno lo stesso nome dell' AWS APIoperazione associata. Esistono alcune eccezioni, come le azioni basate solo sulle autorizzazioni che non hanno un'operazione corrispondente. API Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi 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 di policy: sì

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

L'elemento `Resource` JSON policy specifica l'oggetto o gli oggetti a cui si applica l'azione. Le istruzioni devono includere un elemento `Resource`o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il relativo Amazon Resource Name (ARN). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, 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 relativiARNs, consulta Resources defined by AWS Ground Station nel Service Authorization Reference. Per sapere con quali azioni è possibile specificare le caratteristiche ARN di ciascuna risorsa, vedere 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

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 AWS JSON le politiche per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition`(o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition`è facoltativo. Puoi 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.

Se specifichi più elementi `Condition`in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND`logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica`OR`. Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, è possibile concedere a un IAM utente l'autorizzazione ad accedere a una risorsa solo se è contrassegnata con il

suo nome IAM utente. Per ulteriori informazioni, consulta gli elementi IAM della politica: variabili e tag nella Guida IAM per l'utente.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'IAMutente.

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

ACLsin AWS Ground Station

SupportiACLs: no

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

ABACcon AWS Ground Station

Supporti ABAC (tag nelle politiche): Sì

Il controllo degli accessi basato sugli attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. È possibile allegare tag a IAM entità (utenti o ruoli) e a molte AWS risorse. L'etichettatura di entità e risorse è il primo passo diABAC. Quindi si progettano ABAC politiche per consentire le operazioni quando il tag del principale corrisponde al tag sulla risorsa a cui sta tentando di accedere.

ABACè utile in ambienti in rapida crescita e aiuta in situazioni in cui la gestione delle politiche diventa complicata.

Per controllare l'accesso basato su tag, fornisci 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 Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni suABAC, vedere Cos'è? ABAC nella Guida IAM per l'utente. Per visualizzare un tutorial con i passaggi per la configurazioneABAC, consulta Utilizzare il controllo di accesso basato sugli attributi (ABAC) nella Guida per l'IAMutente.

Utilizzo di credenziali temporanee con AWS Ground Station

Supporta le credenziali temporanee: sì

Alcuni AWS servizi non funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che AWS servizi funzionano con credenziali temporanee, consulta la sezione AWS servizi relativa alla funzionalità IAM nella Guida per l'IAMutente.

Si utilizzano credenziali temporanee se si accede AWS Management Console utilizzando qualsiasi metodo tranne il nome utente e la password. Ad esempio, quando accedete AWS utilizzando il link Single Sign-on (SSO) della vostra azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sul cambio di ruolo, consulta Passare a un ruolo (console) nella Guida per l'IAMutente.

È possibile creare manualmente credenziali temporanee utilizzando AWS CLI o AWS API. È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, vedere Credenziali di sicurezza temporanee in. IAM

Autorizzazioni principali per più servizi per AWS Ground Station

Supporta sessioni di accesso diretto (FAS): Sì

Quando utilizzi un IAM utente o un ruolo per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FASutilizza le autorizzazioni del principale che chiama an AWS servizio, in combinazione con la richiesta AWS servizio per effettuare richieste ai servizi downstream. FASle richieste vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri AWS servizi o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli FAS delle politiche relative alle richieste, consulta Forward access sessions.

Ruoli di servizio per AWS Ground Station

Supporta i ruoli di servizio: No

Un ruolo di servizio è un IAMruolo che un servizio assume per eseguire azioni per conto dell'utente. Un IAM amministratore può creare, modificare ed eliminare un ruolo di servizio dall'internoIAM. Per ulteriori informazioni, vedere Creazione di un ruolo per delegare le autorizzazioni a un utente AWS servizio nella Guida per l'IAMutente.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe compromettere la funzionalità. AWS Ground Station 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 ruoli collegati ai servizi: Sì

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. AWS servizio Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un IAM amministratore può visualizzare, ma non modificare le autorizzazioni per i ruoli collegati al servizio.

Per informazioni dettagliate sulla creazione o la gestione di ruoli collegati ai servizi, consulta AWS Servizi compatibili con. 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 . Inoltre, non possono eseguire attività utilizzando AWS Management Console, AWS Command Line Interface (AWS CLI) o. AWS API Per concedere agli utenti il permesso di eseguire azioni sulle risorse di cui hanno bisogno, un IAM amministratore può creare IAM policy. L'amministratore può quindi aggiungere le IAM politiche ai ruoli e gli utenti possono assumerli.

Per informazioni su come creare una politica IAM basata sull'identità utilizzando questi documenti di esempioJSON, consulta Creazione di IAM politiche nella Guida per l'IAMutente.

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 di 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 crei o modifichi policy basate su identità, segui 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 ulteriori informazioni, consulta le politiche AWS gestite o le politiche AWS gestite per le funzioni lavorative nella Guida per l'IAMutente.
- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le IAM politiche, concedi solo le autorizzazioni necessarie per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo per applicare le autorizzazioni, consulta Politiche e autorizzazioni nella Guida IAM per l'utente. IAM IAM
- Utilizza le condizioni nelle IAM politiche per limitare ulteriormente l'accesso: puoi aggiungere una condizione alle tue politiche per limitare l'accesso ad azioni e risorse. Ad esempio, puoi scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzandoSSL. È inoltre possibile utilizzare condizioni per concedere l'accesso alle azioni di servizio se vengono utilizzate tramite uno specifico AWS servizio, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta Elementi IAM JSON della politica: Condizione nella Guida IAM per l'utente.
- Usa IAM Access Analyzer per convalidare IAM le tue policy e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio delle IAM policy () e alle best practice. JSON IAM IAMAccess Analyzer fornisce

più di 100 controlli delle politiche e consigli pratici per aiutarti a creare policy sicure e funzionali. Per ulteriori informazioni, vedere Convalida delle policy di IAM Access Analyzer nella Guida per l'utente. IAM

- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede l'utilizzo di IAM utenti o di un utente root Account AWS, attiva questa opzione MFA per una maggiore sicurezza. Per richiedere MFA quando vengono richiamate API le operazioni, aggiungi MFA delle condizioni alle tue politiche. Per ulteriori informazioni, consulta Configurazione dell'APIaccesso MFA protetto nella Guida per l'IAMutente.

Per ulteriori informazioni sulle procedure consigliate inIAM, consulta la sezione Procedure consigliate in materia di sicurezza IAM nella Guida per l'IAMutente.

Utilizzo della console di 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 concedere autorizzazioni minime per la console agli utenti che effettuano chiamate solo verso il AWS CLI o il. AWS API Consenti invece l'accesso solo alle azioni che corrispondono all'APIoperazione che stanno cercando di eseguire.

Per garantire che utenti e ruoli possano continuare a utilizzare la AWS Ground Station console, allega anche la policy AWS Ground Station *`ConsoleAccess`* o la policy *`ReadOnly`* AWS gestita alle entità. Per ulteriori informazioni, consulta Aggiungere autorizzazioni a un utente nella Guida per l'IAMutente.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra come è possibile creare una politica che consenta IAM agli utenti di visualizzare le politiche in linea e gestite allegate alla loro identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando o a livello di codice. AWS CLI AWS API

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

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

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 AWS Ground Station eIAM.

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 disponi dell'autorizzazione per eseguire un'operazione, le tue policy devono essere aggiornate in modo che ti sei consentito eseguire tale operazione.

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

```
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 assistenza, contatta l'amministratore. AWS 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 AWS servizi 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 IAM utente denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in. AWS Ground Station Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare 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 assistenza, contatta AWS l'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 ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se AWS Ground Station supporta queste funzionalità, consulta. Come AWS Ground Station funziona con IAM
- Per informazioni su Account AWS come fornire l'accesso alle risorse di tua proprietà, consulta Fornire l'accesso a un IAM utente di un altro Account AWS utente di tua proprietà nella Guida per l'IAMutente.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a persone Account AWS di proprietà di terzi nella Guida per l'IAMutente.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso agli utenti autenticati esternamente (federazione delle identità) nella Guida per l'IAMutente.
- Per conoscere la differenza tra l'utilizzo di ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta la sezione Accesso alle risorse tra account nella Guida per l'utente. IAM 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 Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i tuoi 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 AWS servizio viene lanciata una nuova o quando diventano disponibili nuove API operazioni per i servizi esistenti.

Per ulteriori informazioni, consulta le politiche AWS gestite nella Guida IAM per l'utente.

AWS politica gestita: AWSGroundStationAgentInstancePolicy

Puoi allegare la `AWSGroundStationAgentInstancePolicy` politica alle tue IAM identità.

Questa politica concede le autorizzazioni di AWS Ground Station agente alla tua EC2 istanza Amazon 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 dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

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

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

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

AWS politica gestita: AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy

Non puoi collegarti AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy alle tue IAM entità. 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 EC2 autorizzazioni che consentono di AWS Ground Station trovare indirizzi pubbliciIPv4.

Dettagli dell'autorizzazione

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 EC2 istanze per conto dell'utente.

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

```
                "ec2:DescribeNetworkInterfaces"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS Ground Station aggiornamenti alle politiche gestite AWS

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 RSS feed nella pagina della cronologia dei AWS Ground Station documenti.

Modifica	Descrizione	Data
AWSGroundStationAgentInstancePolicy: nuova policy	AWS Ground Station ha aggiunto una nuova politica per fornire all'istanza dell'endpoint dataflow le autorizzazioni per utilizzare Ground Station AWS Agent.	12 aprile 2023
AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy: nuova policy	AWS Ground Station ha aggiunto una nuova politica che concede EC2 le autorizzazioni per consentire AWS Ground Station di trovare IPv4 indirizzi pubblici associati EIPs e 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.	

Utilizzo di ruoli collegati ai servizi per Ground Station

AWS Ground Station utilizza AWS Identity and Access Management (IAM) ruoli collegati al servizio. Un ruolo collegato al servizio è un tipo unico di IAM ruolo 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 politica di fiducia e la politica delle autorizzazioni e tale politica di autorizzazione non può essere associata a nessun'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 ai servizi per tale servizio.

Autorizzazioni di ruolo collegate al servizio per Ground Station

Ground Station utilizza il ruolo collegato al servizio denominato AWSServiceRoleForGroundStationDataflowEndpointGroup: AWS GroundStation utilizza questo ruolo collegato al servizio per richiamare per trovare indirizzi pubbliciEC2. IPv4

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

- `groundstation.amazonaws.com`

La politica di autorizzazione dei ruoli denominata AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy 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 aEIPs.

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

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

È necessario configurare le autorizzazioni per consentire a un'IAMentità (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato al servizio. Per ulteriori informazioni, consulta Autorizzazioni dei ruoli collegati 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 ruolo DataflowEndpointGroup in AWS CLI o il AWS API, Ground Station crea automaticamente il ruolo collegato al servizio.

Se elimini questo ruolo collegato ai servizi, puoi 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 IAM console per creare un ruolo collegato al servizio con lo EC2 use case Data Delivery to Amazon. In AWS CLI o il 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 al servizio nella Guida per l'utente. IAM Se elimini il ruolo collegato ai servizi, puoi 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 AWSServiceRoleForGroundStationDataflowEndpointGroup collegato al servizio. Dopo aver creato un ruolo collegato al servizio, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. Tuttavia, è possibile modificare la descrizione del ruolo utilizzando. IAM Per ulteriori informazioni, consulta Modifica di un ruolo collegato al servizio nella Guida per l'IAMutente.

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 AWSServiceRoleForGroundStationDataflowEndpointGroup

- Eliminare DataflowEndpointGroups tramite AWS CLI o il AWSAPI.

Per eliminare manualmente il ruolo collegato al servizio utilizzando IAM

Usa la IAM console AWS CLI, o il AWS API per eliminare il ruolo collegato al AWSServiceRoleForGroundStationDataflowEndpointGroup servizio. Per ulteriori informazioni, vedere Eliminazione di un ruolo collegato al servizio 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 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.

- AWSchiavi 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 AWS Key Management Service Developer Guide.

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 per aggiungere un secondo livello di crittografia rispetto alla 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 IAM politiche e sovvenzioni
  - 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 AWS Key Management Service Developer Guide.

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

Tipo di dati	AWScrittografia a chiave proprietaria	Crittografia con chiavi gestite dal cliente (opzionale)
Dati sulle effemeridi utilizzati per calcolare la traiettoria di un satellite	Abilitato	Abilitato

> **Note**
>
> AWS Ground Station abilita automaticamente la crittografia dei dati inattivi utilizzando chiavi AWS proprietarie 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 prezzi del servizio di gestione delle AWS chiavi.
> Per ulteriori informazioni AWS KMS, consulta la Guida per AWS KMS gli sviluppatori.

Come AWS Ground Station utilizza le sovvenzioni in 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 KMS chiave nel tuo account.

AWS Ground Station richiede la concessione dell'utilizzo della chiave gestita dal cliente per le seguenti operazioni interne:

- Invia GenerateDataKeyrichieste per AWS KMS generare chiavi dati crittografate dalla tua chiave gestita dal cliente.

- Invia le richieste Decrypt a per AWS KMS decrittografare le chiavi di dati crittografate in modo che possano essere utilizzate per crittografare i dati.
- Invia le richieste Encrypt a per AWS KMS crittografare i dati forniti.

Puoi revocare l'accesso alla concessione o rimuovere l'accesso del servizio alla chiave gestita dal cliente 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 quei 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 causerà la fine del contatto in uno stato. FAILED

Creazione di una chiave gestita dal cliente

È possibile creare una chiave simmetrica gestita dal cliente utilizzando la console di AWS gestione 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 AWS Key Management Service Developer Guide.

Policy della 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, puoi specificare una policy della chiave. Per ulteriori informazioni, consulta Gestire l'accesso alle chiavi gestite dal cliente nella AWS Key Management Service Developer Guide.

Per utilizzare la chiave gestita dal cliente con AWS Ground Station le tue risorse, nella policy chiave devono essere consentite le seguenti API operazioni:

`kms:CreateGrant`- Aggiunge una concessione a una chiave gestita dal cliente. Concede il controllo dell'accesso a una KMS chiave specificata, che consente l'accesso alle operazioni di concessione AWS Ground Station richieste. Per ulteriori informazioni sull'utilizzo di Grants, consulta la AWS Key Management Service Developer Guide.

Ciò consente AWS ad Amazon di effettuare le seguenti operazioni:

- Chiama GenerateDataKeyper generare una chiave dati crittografata e archiviarla, poiché la chiave dati non viene utilizzata immediatamente per la crittografia.
- 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.
- Configura un preside in pensione per consentire al servizio di farlo. `RetireGrant`

`kms:DescribeKey`- Fornisce i dettagli chiave gestiti dal cliente AWS Ground Station per consentire la convalida della chiave prima di tentare di creare una concessione sulla chiave fornita.

Di seguito sono riportati alcuni esempi IAM di dichiarazioni politiche che è possibile aggiungere AWS Ground Station

```
"Statement" : [
  {"Sid" : "Allow access to principals authorized to use AWS Ground Station",
    "Effect" : "Allow",
    "Principal" : {
      "AWS" : "*"
    },
    "Action" : [
      "kms:DescribeKey",
      "kms:CreateGrant"
    ],
    "Resource" : "*",
    "Condition" : {
    "StringEquals" : {
        "kms:ViaService" : "groundstation.amazonaws.com",
        "kms:CallerAccount" : "111122223333"
    }
  },
  {"Sid": "Allow access for key administrators",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:root"
    },
    "Action" : [
      "kms:*"
      ],
    "Resource": "arn:aws:kms:region:111122223333:key/key_ID"
  },
  {"Sid" : "Allow read-only access to key metadata to the account",
```

```
    "Effect" : "Allow",
    "Principal" : {
      "AWS" : "arn:aws:iam::111122223333:root"
    },
    "Action" : [
      "kms:Describe*",
      "kms:Get*",
      "kms:List*",
      "kms:RevokeGrant"
    ],
    "Resource" : "*"
  }
]
```

Per ulteriori informazioni sulla specificazione delle autorizzazioni in una politica, consulta la AWS Key Management Service Developer Guide.

Per ulteriori informazioni sulla risoluzione dei problemi di accesso tramite chiave, consulta la AWS Key Management Service Developer Guide.

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

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 set facoltativo di coppie chiave-valore che contengono ulteriori informazioni contestuali sui dati. AWS KMSutilizza 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 contesto di crittografia

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

Contesto di crittografia delle effemeridi:

Le chiavi concesse per la crittografia delle risorse sulle effemeridi sono legate a un satellite specifico ARN

```
"encryptionContext": {
    "aws:groundstation:arn":
 "arn:aws:groundstation::111122223333:satellite/00a770b0-082d-45a4-80ed-SAMPLE"
}
```

> **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

Puoi utilizzare il contesto di crittografia nelle politiche e IAM nelle politiche chiave `conditions` per controllare l'accesso alla tua 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 nell'account o nella regione dell'utente. 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 delle chiavi 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.

```
{"Sid": "Enable DescribeKey",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/ExampleReadOnlyRole"
     },
     "Action": "kms:DescribeKey",
     "Resource": "*"
},{"Sid": "Enable CreateGrant",
     "Effect": "Allow",
     "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/ExampleReadOnlyRole"
     },
     "Action": "kms:CreateGrant",
     "Resource": "*",
     "Condition": {
        "StringEquals": {
            "kms:EncryptionContext:aws:groundstation:arn":
 "arn:aws:groundstation::111122223333:satellite/00a770b0-082d-45a4-80ed-SAMPLE"
        }
     }
}
```

Monitoraggio delle chiavi di crittografia per AWS Ground Station

Quando utilizzi una chiave gestita AWS KMS dal cliente con AWS Ground Station le tue risorse, puoi utilizzare AWS CloudTrail CloudWatch i log di Amazon per tenere traccia delle richieste AWS Ground Station inviate a AWS KMS. Gli esempi seguenti sono AWS CloudTrail eventi per `CreateGrant` `GenerateDataKeyDecrypt`, `Encrypt` e per `DescribeKey` monitorare KMS le operazioni chiamate da AWS Ground Station per accedere ai dati crittografati dalla chiave gestita dal cliente.

`CreateGrant`(Cloudtrail)

Quando utilizzi una chiave gestita AWS KMS dal cliente per crittografare le tue risorse effemeridi, AWS Ground Station invia una `CreateGrant` richiesta per tuo conto per accedere alla chiave del tuo account. KMS AWS La concessione AWS Ground Station creata è specifica per la

risorsa associata alla chiave gestita dal AWS KMS cliente. Inoltre, AWS Ground Station utilizza l'`RetireGrant`operazione per rimuovere una concessione quando si elimina una risorsa.

L'evento di esempio seguente registra l'operazione `CreateGrant`:


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AAAAAAAAAAAAAAAAAAAAA:SampleUser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/SampleUser01",
        "accountId": "111122223333",
        "accessKeyId": "ASIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AAAAAAAAAAAAAAAAAAAAA",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-02-22T22:22:22Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2022-02-22T22:22:22Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "111.11.11.11",
    "userAgent": "ExampleDesktop/1.0 (V1; OS)",
    "requestParameters": {
        "operations": [
            "GenerateDataKeyWithoutPlaintext",
            "Decrypt",
            "Encrypt"
        ],
        "constraints": {
            "encryptionContextSubset": {
```

```
                "aws:groundstation:arn":
 "arn:aws:groundstation::111122223333:satellite/00a770b0-082d-45a4-80ed-SAMPLE"
            }
        },
        "granteePrincipal": "groundstation.us-west-2.amazonaws.com",
        "retiringPrincipal": "groundstation.us-west-2.amazonaws.com",
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "responseElements": {
        "grantId":
 "0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE"
    },
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

`DescribeKey`(Cloudtrail)

Quando utilizzi una chiave gestita AWS KMS dal cliente per crittografare le tue risorse effemeridi, AWS Ground Station invia una `DescribeKey` richiesta 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": "AAAAAAAAAAAAAAAAAAAAA:SampleUser01",
```

```
        "arn": "arn:aws:sts::111122223333:assumed-role/User/Role",
        "accountId": "111122223333",
        "accessKeyId": "ASIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AAAAAAAAAAAAAAAAAAAAA",
                "arn": "arn:aws:iam::111122223333:role/Role",
                "accountId": "111122223333",
                "userName": "User"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-02-22T22:22:22Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2022-02-22T22:22:22Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DescribeKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
```

```
    "eventCategory": "Management"
}
```

GenerateDataKey(Cloudtrail)

Quando utilizzi una chiave gestita AWS KMS dal cliente per crittografare le tue risorse effemeridi, AWS Ground Station invia una `GenerateDataKey` richiesta KMS a per generare una chiave dati con cui crittografare i tuoi dati.

L'evento di esempio seguente registra l'operazione `GenerateDataKey`:

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2022-02-22T22:22:22Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keySpec": "AES_256",
        "encryptionContext": {
            "aws:groundstation:arn":
 "arn:aws:groundstation::111122223333:satellite/00a770b0-082d-45a4-80ed-SAMPLE",
            "aws:s3:arn":
 "arn:aws:s3:::customerephemerisbucket/0034abcd-12ab-34cd-56ef-123456SAMPLE"
        },
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
```

```
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "sharedEventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventCategory": "Management"
}
```

`Decrypt`(Cloudtrail)

Quando si utilizza una chiave gestita AWS KMS dal cliente per crittografare le risorse effemeridi, AWS Ground Station utilizza l'`Decrypt`operazione di decrittografia delle effemeridi fornita se è già crittografata 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`:

```
{
    "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 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 EC2 istanze Amazon 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 ogni metodo.

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 EC2 istanza Amazon decrittograferà automaticamente lo stream 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 configurazioni aggiuntive.

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 aPanoramica 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 il Joint Polar Satellite System 1 (JPSS-1) Spacecraft High Rate Data (HRD) 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 all'ID 43013. NORAD

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 del. ICD Di questi quattro percorsi di comunicazione, solo il singolo 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.
- SMDpercorso (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 HRD percorso (downlink) alla frequenza MHz centrale 7812 con una velocità dati di 15 Mbps. Ha una larghezza di MHz banda di 30, ed è. right-hand-circular-polarized Quando sei a bordo di JPSS -1 con AWS Ground Station, questo è il percorso di comunicazione a cui hai accesso. Questo percorso di comunicazione contiene dati scientifici sugli strumenti, dati di ingegneria degli strumenti, dati di telemetria degli strumenti e dati sulla manutenzione dei veicoli spaziali in tempo reale.

Confrontando i potenziali percorsi di dati, vediamo che i percorsi di comando (uplink), telemetria (downlink) e (downlink) soddisfano le capacità di frequenza, larghezza di HRD banda e utilizzo simultaneo multicanale di. AWS Ground Station Il SMD percorso non è compatibile in quanto la frequenza centrale non è compresa nell'intervallo dei ricevitori esistenti. Per ulteriori informazioni sulle funzionalità supportate, vedereAWS Ground Station Funzionalità del sito.

> **Note**
>
> Poiché il SMD percorso 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 inICD, 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 HRD comunicazione 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 demodulare e decodificare i dati 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 Fase 2: Pianifica i percorsi di comunicazione del flusso di dati guida introduttiva.

Tutti i seguenti frammenti di modello appartengono alla sezione Risorse del AWS 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 AWS 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 Fase 3: Creare configurazioni come iniziare.

Avrai bisogno di un tracking-config per impostare le tue preferenze sull'uso dell'autotrack. La selezione PREFERREDcome autotrack può migliorare la qualità del segnale, ma non è necessario soddisfare la qualità del segnale perché la qualità delle effemeridi -1 è sufficiente. JPSS

```
 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 Fase 4: Creare il profilo della 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 hai la possibilità di pianificare JPSS -1 contatti per la consegna asincrona dei dati da qualsiasi dispositivo integrato. AWS Ground Station Posizioni

Di seguito è riportato un AWS CloudFormation modello completo che include tutte le risorse descritte in questa sezione combinate in un unico modello che può essere utilizzato direttamente. AWS CloudFormation

Il AWS 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 VITA Signal/IP -49.

Se AquaSNPP, JPSS -1/ NOAA -20 e Terra non sono presenti nel tuo account, vedi. Fase 1: onboarding via satellite

> **Note**
>
> Puoi accedere al modello accedendo al bucket Amazon S3 per l'onboarding dei clienti. 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 AWS CloudFormation stack.
> Inoltre, le seguenti istruzioni utilizzanoYAML. Tuttavia, i modelli sono disponibili in entrambi YAML i JSON formati. Per utilizzarloJSON, sostituisci l'estensione del `.yml` file con `.json` quando scarichi il modello.

Per scaricare il modello utilizzando AWS CLI, utilizzate il seguente comando:

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

Puoi visualizzare e scaricare il modello nella console accedendo a quanto segue URL nel tuo browser:

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

Puoi specificare il modello direttamente AWS 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 HRD comunicazione come frequenza intermedia digitale (DigiF) ed elaborarlo così come viene ricevuto da un'applicazione endpoint dataflow su un'EC2istanza Amazon utilizzando un. SDR

Percorsi di comunicazione

Questa sezione rappresenta una Fase 2: Pianifica i percorsi di comunicazione del flusso di dati guida introduttiva. Per questo esempio, creerai due sezioni nel tuo AWS CloudFormation modello: le sezioni Parametri e Risorse.

> **Note**
>
> Per ulteriori informazioni sul contenuto di un AWS 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 AWS 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, al momento della creazione dello AWS CloudFormation stack, dovrai fornire l'AMIID specifico della regione corretto. Per informazioni, consulta AWS Ground Station Immagini di macchine Amazon (AMIs).

I frammenti di modello rimanenti appartengono alla sezione Risorse del modello. AWS 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'EC2istanza, disporrete di un unico percorso di consegna sincrono. Distribuzione sincrona dei datiIn base alla sezione, devi configurare un'EC2istanza 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:
      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 Fase 3: Creare configurazioni come iniziare.

Avrai bisogno di un tracking-config per impostare le tue preferenze sull'uso dell'autotrack. La selezione PREFERREDcome autotrack può migliorare la qualità del segnale, ma non è necessario soddisfare la qualità del segnale perché la qualità delle effemeridi -1 è sufficiente. JPSS

```
 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 Fase 4: Creare il profilo della 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 hai la possibilità di programmare JPSS -1 contatti per la trasmissione sincrona dei dati da qualsiasi dispositivo di bordo AWS Ground Station Posizioni.

Di seguito è riportato un AWS CloudFormation modello completo che include tutte le risorse descritte in questa sezione combinate in un unico modello che può essere utilizzato direttamente. AWS CloudFormation

Il AWS 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 AquaSNPP, JPSS -1/ NOAA -20 e Terra. Contiene un'EC2istanza Amazon e le AWS CloudFormation risorse necessarie per ricevere dati di trasmissione diretta DigiF non elaborati.

Se AquaSNPP, JPSS -1/ NOAA -20 e Terra non sono presenti nel tuo account, consulta. Fase 1: onboarding via satellite

> **Note**
>
> Puoi accedere al modello accedendo al bucket Amazon S3 per l'onboarding dei clienti. 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 AWS CloudFormation stack.
> Inoltre, le seguenti istruzioni utilizzanoYAML. Tuttavia, i modelli sono disponibili in entrambi YAML i JSON formati. Per utilizzarloJSON, sostituisci l'estensione del `.yml` file con `.json` quando scarichi il modello.

Per scaricare il modello utilizzando AWS CLI, utilizzate il seguente comando:

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

Puoi visualizzare e scaricare il modello nella console accedendo a quanto segue URL nel tuo browser:

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

Puoi specificare il modello direttamente AWS 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) EC2Verifica per i contatti: l'opzione di utilizzare Lambda per configurare un sistema di verifica delle EC2 istanze Amazon per i contatti con SNS notifica. 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 quello che preferisci. AMI 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 e Terra). SNPP
- Configurazioni aggiuntive di antenna e downlink - Configurazioni di downlink dell'antenna per altri satelliti di trasmissione pubblica (Aqua e Terra). SNPP

I valori e i parametri per i satelliti in questo modello sono già popolati. Questi parametri ne facilitano l'utilizzo 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 UDP porta 50000 sull'adattatore di loopback dell'istanza del ricevitore. Per ulteriori informazioni sulla configurazione di un gruppo di endpoint dataflow, consulta Gruppo. AWS::GroundStation::DataflowEndpoint

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 HRD comunicazione come dati di trasmissione diretta demodulati e decodificati utilizzando un endpoint di flusso di dati. Questo esempio è un buon punto di partenza se intendete elaborare i dati utilizzando il software NASA Direct Readout Labs (RT- and). STPS IPOPP

Percorsi di comunicazione

Questa sezione rappresenta una Fase 2: Pianifica i percorsi di comunicazione del flusso di dati guida introduttiva. Per questo esempio, creerai due sezioni nel tuo AWS CloudFormation modello: le sezioni Parametri e Risorse.

> **Note**
>
> Per ulteriori informazioni sul contenuto di un AWS 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 AWS 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, al momento della creazione dello AWS CloudFormation stack, dovrai fornire l'AMIID specifico della regione corretto. Per informazioni, consulta AWS Ground Station Immagini di macchine Amazon (AMIs).

I frammenti di modello rimanenti appartengono alla sezione Risorse del modello. AWS 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'EC2istanza, disporrete di un unico percorso di consegna sincrono. Distribuzione sincrona dei datiIn base alla sezione, devi impostare e configurare un'EC2istanza 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 Fase 3: Creare configurazioni guida per l'utente.

Avrai bisogno di un tracking-config per impostare le tue preferenze sull'uso dell'autotrack. La selezione PREFERREDcome autotrack può migliorare la qualità del segnale, ma non è necessario soddisfare la qualità del segnale perché la qualità delle effemeridi -1 è sufficiente. JPSS

```
  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 Fase 4: Creare il profilo della 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 hai la possibilità di programmare JPSS -1 contatti per la trasmissione sincrona dei dati da qualsiasi dispositivo di bordo AWS Ground Station Posizioni.

Di seguito è riportato un AWS CloudFormation modello completo che include tutte le risorse descritte in questa sezione combinate in un unico modello che può essere utilizzato direttamente. AWS CloudFormation

Il AWS CloudFormation modello denominato `AquaSnppJpss.yml` è progettato per darti un accesso rapido per iniziare a ricevere dati per i satelliti Aqua e JPSS -1/ NOAA -20. SNPP Contiene un'EC2istanza Amazon e le AWS Ground Station risorse necessarie per pianificare i contatti e ricevere dati di trasmissione diretta demodulati e decodificati.

Se AquaSNPP, JPSS -1/ NOAA -20 e Terra non sono presenti nel tuo account, consulta. Fase 1: onboarding via satellite

> **Note**
>
> Puoi accedere al modello accedendo al bucket Amazon S3 per l'onboarding dei clienti. 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 AWS CloudFormation stack.
> Inoltre, le seguenti istruzioni utilizzanoYAML. Tuttavia, i modelli sono disponibili in entrambi YAML i JSON formati. Per utilizzarloJSON, sostituisci l'estensione del `.yml` file con `.json` quando scarichi il modello.

Per scaricare il modello utilizzando AWS CLI, utilizzate il seguente comando:

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

Puoi visualizzare e scaricare il modello nella console accedendo a quanto segue URL nel tuo browser:

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

Puoi specificare il modello direttamente AWS 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) EC2Verifica per i contatti: l'opzione di utilizzare Lambda per configurare un sistema di verifica delle EC2 istanze Amazon per i contatti con SNS notifica. 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 da installare nell'istanza e quello che preferisci. AMI 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 e Terra). SNPP
- Configurazioni aggiuntive di antenna e downlink - Configurazioni di downlink dell'antenna per altri satelliti di trasmissione pubblica (Aqua e Terra). SNPP

I valori e i parametri per i satelliti in questo modello sono già popolati. Questi parametri ne facilitano l'utilizzo 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 l'utilizzo tramite la UDP porta 50000 sull'adattatore di loopback dell'istanza del ricevitore. Per ulteriori informazioni sulla configurazione di un gruppo di endpoint dataflow, consulta Gruppo. AWS::GroundStation::DataflowEndpoint

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 HRD comunicazione 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. EC2 SDR

> **Note**
>
> Il segnale del percorso di JPSS HRD comunicazione effettivo ha una larghezza di banda di 30MHz, ma configurerai 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 per essere ricevuto dall' AWS Ground Station agente per questo esempio.

Percorsi di comunicazione

Questa sezione rappresenta una Fase 2: Pianifica i percorsi di comunicazione del flusso di dati guida introduttiva. Per questo esempio, avrai bisogno di una sezione aggiuntiva nel tuo AWS CloudFormation modello che non è stata utilizzata negli altri esempi, la sezione Mappature.

> **Note**
>
> Per ulteriori informazioni sul contenuto di un AWS CloudFormation modello, consulta Sezioni relative ai modelli.

Inizierai configurando una sezione Mappature nel tuo AWS 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. VPCConfigurazione con AWS Ground Station Agent

```
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 AWS 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, al momento della creazione dello AWS CloudFormation stack, dovrai fornire l'AMIID specifico della regione corretto. Per informazioni, consulta AWS Ground Station Immagini di macchine Amazon (AMIs).

I frammenti di modello rimanenti appartengono alla sezione Risorse del modello. AWS 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'EC2istanza Amazon, sai che avrai un unico percorso di distribuzione sincrono. Secondo la Distribuzione sincrona dei dati sezione, devi configurare un'EC2istanza Amazon con AWS Ground Station Agent e creare uno o più gruppi di endpoint di dataflow. Inizierai configurando prima Amazon VPC for the AWS Ground Station Agent.

```
  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 VPC configurazioni supportate dall' AWS Ground Station agente, consulta Requisiti AWS Ground Station dell'agente - VPC diagrammi.

Successivamente, configurerai l'EC2istanza 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 Fase 3: Creare configurazioni come iniziare.

Avrai bisogno di un tracking-config per impostare le tue preferenze sull'uso dell'autotrack. La selezione PREFERREDcome autotrack può migliorare la qualità del segnale, ma non è necessario soddisfare la qualità del segnale perché la qualità delle effemeridi -1 è sufficiente. JPSS

```
 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 Fase 4: Creare il profilo della 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 hai la possibilità di programmare JPSS -1 contatti per la trasmissione sincrona dei dati da qualsiasi dispositivo di bordo AWS Ground Station Posizioni.

Di seguito è riportato un AWS CloudFormation modello completo che include tutte le risorse descritte in questa sezione combinate in un unico modello che può essere utilizzato direttamente. AWS CloudFormation

Il AWS 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 AquaSNPP, JPSS -1/ NOAA -20 e Terra. Contiene un'EC2istanza Amazon e le AWS CloudFormation risorse necessarie per ricevere dati di trasmissione diretta DigiF non elaborati tramite AWS Ground Station Agent.

Se AquaSNPP, JPSS -1/ NOAA -20 e Terra non sono presenti nel tuo account, consulta. Fase 1: onboarding via satellite

> **Note**
>
> Puoi accedere al modello accedendo al bucket Amazon S3 per l'onboarding dei clienti. 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 AWS CloudFormation stack.
> Inoltre, le seguenti istruzioni utilizzanoYAML. Tuttavia, i modelli sono disponibili in entrambi YAML i JSON formati. Per utilizzarloJSON, sostituisci l'estensione del `.yml` file con `.json` quando scarichi il modello.

Per scaricare il modello utilizzando AWS CLI, utilizzate il seguente comando:

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

Puoi visualizzare e scaricare il modello nella console accedendo a quanto segue URL nel tuo browser:

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

Puoi specificare il modello direttamente AWS 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 EIP e collegata all'istanza del ricevitore.
- IP elastico dell'istanza del ricevitore: un IP elastico a cui connettersi. AWS Ground Station Si collega all'istanza del ricevitore o all'interfaccia di rete elastica.
- 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 SNS notifica. 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 e TerraSNPP).
- Configurazioni aggiuntive di antenna e downlink - Configurazioni di downlink dell'antenna per altri satelliti di trasmissione pubblica (Aqua e Terra). SNPP

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 Gruppo. AWS::GroundStation::DataflowEndpoint 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

Risoluzione dei problemi relativi ai contatti che forniscono dati ad Amazon EC2

Se non riesci a completare correttamente un AWS Ground Station contatto, dovrai verificare che l'EC2istanza Amazon 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'EC2istanza Amazon sia già configurata. Per configurare un'EC2istanza Amazon in AWS Ground Station, consulta Getting Started.

Passaggio 1: verifica che l'EC2istanza sia in esecuzione

1. Individua l'EC2istanza Amazon utilizzata per il contatto che stai risolvendo. Utilizza le fasi seguenti:

a. Nella AWS CloudFormationdashboard, seleziona lo stack che contiene la tua EC2 istanza Amazon.

b. Scegli la scheda Risorse e individua la tua EC2 istanza Amazon nella colonna Logical ID. Verificare che l'istanza venga creata nella colonna Stato.

c. Nella colonna ID fisico, scegli il link per la tua EC2 istanza Amazon. Verrai reindirizzato alla console di EC2 gestione di Amazon.

2. Nella console di EC2 gestione Amazon, assicurati che Amazon EC2 Instance State 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'EC2istanza Amazon selezionata, scegli Azioni > Stato dell'istanza > Avvia.

Fase 2: Determinare il tipo di applicazione dataflow utilizzata

Se utilizzi l'AWS Ground Station agente per la consegna dei dati, reindirizza alla sezione Troubleshooting Agent. AWS Ground Station Altrimenti, se stai utilizzando l'applicazione DataDefender (DDX), continua a the section called “Passaggio 3: Verificate che l'applicazione Dataflow sia in esecuzione” farlo.

Passaggio 3: Verificate che l'applicazione Dataflow sia in esecuzione

La verifica dello stato di DataDefender richiede la connessione alla tua istanza in AmazonEC2. Per maggiori dettagli sulla connessione alla tua istanza, vedi Connect to your Linux istance.

La procedura seguente fornisce i passaggi per la risoluzione dei problemi utilizzando i comandi in un SSH client.

1. Apri un terminale o un prompt dei comandi e connettiti alla tua EC2 istanza Amazon utilizzandoSSH. Inoltra la porta 80 dell'host remoto per visualizzare l'interfaccia utente DataDefender web. I comandi seguenti mostrano come connettersi SSH a un'EC2istanza Amazon tramite un bastione con il port forwarding abilitato.

> **Note**
>
> Devi sostituire < SSH KEY >, < > e < BASTION HOST HOST > con la tua chiave ssh specifica, il nome host bastion e il nome host dell'EC2istanza Amazon.

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 ancheDDX) 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, continua con il 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 su VPC cui è in esecuzione l'EC2istanza Amazon 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 di Amazon VPC e del gruppo di sicurezza dell'EC2istanza per assicurarti che non blocchino l'accesso ad Amazon S3.

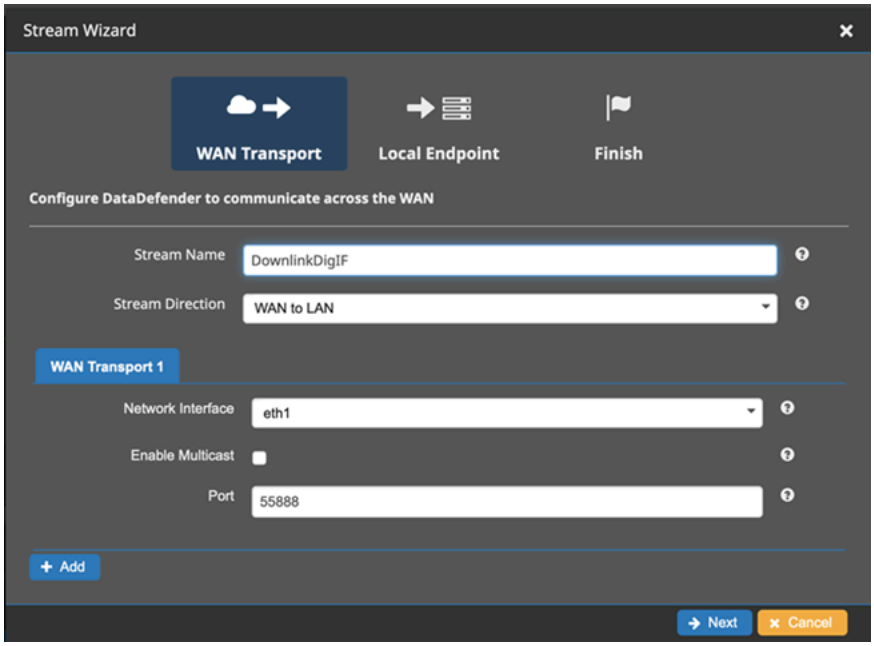
Se DataDefender è in esecuzione dopo aver verificato VPC le impostazioni di Amazon, continua a farlothe section called “Passaggio 4: Verifica che il flusso dell'applicazione Dataflow sia configurato”. Se il problema persiste, contatta l'AWSassistenza e invia i file di registro con una descrizione del problema.

Passaggio 4: Verifica che il flusso dell'applicazione Dataflow sia configurato

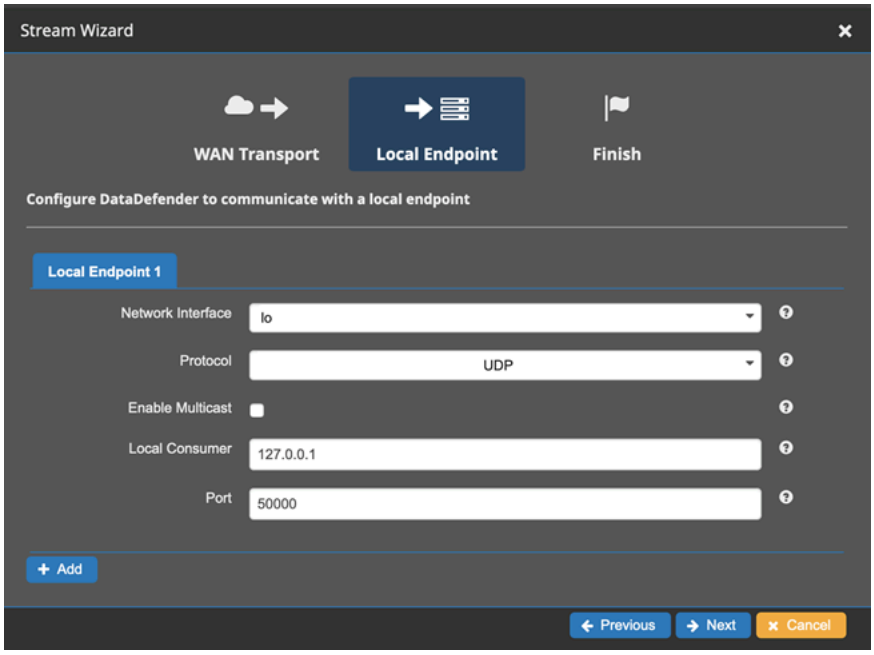
1. In un browser Web, accedete alla vostra interfaccia utente DataDefender web inserendo il seguente indirizzo nella barra degli indirizzi: localhost:8080. Quindi, premere Invio.
2. Nella DataDefenderdashboard, scegli Vai ai dettagli.
3. Seleziona il tuo flusso dall'elenco dei flussi e scegli Modifica flusso.
4. Nella finestra di dialogo Stream Wizard (Creazione guidata flusso), eseguire le operazioni seguenti:

   a. Nel riquadro WANTrasporto, assicurati che WAN LAN sia selezionato per Stream Direction.

   b. Nella casella Porta, assicurati che sia presente la WAN porta che hai scelto per il tuo gruppo di endpoint dataflow. Per impostazione predefinita, questa porta è 55888. Quindi, seleziona Next (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 su cui riceverai i dati dopo averli DataDefender ricevuti dal servizio. AWS Ground Station Quindi, seleziona Next (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 EC2 istanza Amazon e io DataDefender siamo entrambi in esecuzione e configurati correttamente per ricevere dati da AWS Ground Station. Se continui a riscontrare problemi, contatta l'AWSassistenza.

Risoluzione dei problemi dei FAILED contatti

Un contatto avrà lo stato di contatto del terminale pari a FAILEDquando AWS Ground Station rileva un problema con la configurazione delle risorse. Di seguito sono riportati i casi d'uso più comuni che possono causare FAILEDcontatti, insieme ai passaggi per la risoluzione dei problemi.

> **Note**
>
> Questa guida è specifica per lo stato dei FAILEDcontatti e non è destinata ad altri stati di errore, come AWS_FAILED, _ o AWS_TO_ CANCELLED. FAILED SCHEDULE Per ulteriori informazioni sullo stato dei contatti, vedere the section called “AWS Ground Station stati dei contatti”

Casi d'uso degli endpoint Dataflow FAILED

Di seguito è riportato l'elenco dei casi d'uso comuni che possono determinare lo stato dei FAILEDcontatti per i flussi di dati basati sugli 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.

Per qualsiasi caso di errore degli endpoint Dataflow, si consiglia di esaminare quanto segue:

- Verifica che l'EC2istanza Amazon 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.

Consulta la sezione relativa Risoluzione dei problemi relativi ai contatti che forniscono dati ad Amazon EC2 per procedure di risoluzione dei problemi più specifiche.

AWS Ground Station Casi FAILED d'uso degli agenti

Di seguito è riportato l'elenco dei casi d'uso comuni che possono determinare lo stato dei FAILEDcontatti per i flussi di dati basati su agenti:

- 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'EC2istanza Amazon 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'EC2istanza Amazon non siano state chiuse entro 15 secondi dalla fine del contatto. Ciò fornisce all'agente il tempo sufficiente per segnalare lo stato a AWS Ground Station.

Consulta la sezione relativa Risoluzione dei problemi relativi ai contatti che forniscono dati ad Amazon EC2 per procedure di risoluzione dei problemi più specifiche.

Risoluzione dei problemi relativi ai FAILED contatti _TO_ SCHEDULE

Un contatto termina in uno SCHEDULE stato FAILED_TO_ quando AWS Ground Station rileva un problema relativo alla configurazione delle risorse o all'interno del sistema interno. Un contatto che termina in uno SCHEDULE stato FAILED_TO_ fornirà facoltativamente un contesto aggiuntivo. `errorMessage` Per informazioni sulla descrizione dei contatti, vedere. DescribeContactAPI

Di seguito sono riportati i casi d'uso comuni che possono causare SCHEDULE contatti FAILED_TO_, insieme ai passaggi per la risoluzione dei problemi.

> **Note**
>
> Questa guida è specifica per lo stato dei SCHEDULE contatti FAILED_TO_ e non è destinata ad altri stati di errore, come _, _ o. AWS FAILED AWS CANCELLED FAILED Per ulteriori informazioni sullo stato 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 AWSSupport che includa `contactId` quello terminato nello FAILEDstato _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 SCHEDULE lo stato FAILED_TO_ per questo profilo di missione, contatta il servizio clienti AWS

Risoluzione dei problemi DataflowEndpointGroups in uno HEALTHY stato diverso

Di seguito sono elencati i motivi per cui i gruppi di endpoint del flusso di dati potrebbero non trovarsi in uno `HEALTHY` stato e le azioni correttive appropriate da intraprendere.

- `NO_REGISTERED_AGENT`- Avvia l'EC2istanza, che registrerà l'agente. Nota che è necessario disporre di un file di configurazione del controller valido affinché questa chiamata abbia successo. Per i dettagli sulla configurazione di quel file, consulta la AWS Ground Station Agente
- `INVALID_IP_OWNERSHIP`- Utilizzate il DeleteDataflowEndpointGroup API Dataflow Endpoint Group, quindi utilizzate il Dataflow Endpoint Group, quindi utilizzate il CreateDataflowEndpointGroup API 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 Utilizzo di ruoli collegati ai servizi per Ground Station

Risoluzione dei problemi relativi alle effemeridi non valide

Quando viene caricata un'effemeride personalizzata, viene sottoposta a un flusso di lavoro di convalida asincrono AWS Ground Station prima di diventare. `ENABLED` Questo flusso di lavoro garantisce la validità degli identificatori satellitari, dei metadati e della traiettoria.

Quando un'effemeride fallisce la convalida, restituisce un, `DescribeEphemeris` che fornisce informazioni sul motivo per cui le effemeridi non sono EphemerisInvalidReasonriuscite a convalidare. I valori potenziali di sono i seguenti: EphemerisInvalidReason

Valore	Descrizione	azione di risoluzione dei problemi
METADATA_INVALID	Gli identificatori dei veicoli spaziali forniti, come l'ID satellitare, non sono validi	Controlla l'NORADID o gli altri identificatori forniti nei dati sulle effemeridi

Valore	Descrizione	azione di risoluzione dei problemi
TIME_RANGE_INVALID	Le ore di inizio, fine o scadenza non sono valide per le effemeridi fornite	Assicurati che l'ora di inizio sia precedente a «adesso» (si consiglia di impostare l'ora di inizio qualche minuto rispetto al passato), che l'ora di fine sia successiva all'ora di inizio e che l'ora di fine sia successiva all'ora di scadenza
TRAJECTORY_INVALID	Le effemeridi fornite definisco no una traiettoria del veicolo spaziale non valida	Verificate che la traiettoria fornita sia continua e corrispon da al satellite corretto.
VALIDATION_ERROR	Si è verificato un errore interno del servizio durante l'elabora zione delle effemeridi per la convalida	Riprova a caricare

Di `DescribeEphemeris` seguito viene fornito un esempio di risposta per un'`INVALID`effemeride:

```
{
  "creationTime": 1000000000.00,
  "enabled": false,
  "ephemerisId": "d5a8a6ac-8a3a-444e-927e-EXAMPLE1",
  "name": "Example",
  "priority": 2,
  "status": "INVALID",
  "invalidReason": "METADATA_INVALID",
  "suppliedData": {
    "tle": {
      "sourceS3Object": {
        "bucket": "my-s3-bucket",
        "key": "myEphemerisKey",
        "version": "ephemerisVersion"
      }
    }
```

```
  },
}
```

> **Note**
>
> Se lo stato di un'effemeride è`ERROR`, l'effemeride non è dovuta a un problema con il servizio. `ENABLED` AWS Ground Station Dovresti provare a fornire nuovamente le effemeridi tramite. `CreateEphemeris` Le nuove effemeridi potrebbero insorgere se il problema fosse transitorio`ENABLED`.

Risoluzione dei 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 PCAP file vuoti o nessun PCAP file se utilizzi S3 Data Delivery. 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 una trasmissione satellitare pubblica gestita daNOAA, potresti trovare un messaggio che descrive un'interruzione o una manovra nella pagina Satellite Alert Messages. NOAA 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. Fornitura di dati sulle effemeridi personalizzati

AWS Ground Station interruzione

Se AWS Ground Station causa un errore o lo annulla, AWS Ground Station imposterà lo stato del contatto su _ o AWSAWS_ FAILED. CANCELLED Per ulteriori informazioni sul ciclo di vita dei contatti, consulta. Ciclo di vita dei contatti In alcuni casi, AWS Ground Station può verificarsi un errore che impedisce l'invio dei dati al tuo account, ma non fa sì che il contatto assuma lo stato AWS_ FAILED o 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.

Quote e limiti

È possibile visualizzare le regioni supportate, gli endpoint associati e le quote negli endpoint e nelle quote.AWS Ground Station

È possibile utilizzare la console Service Quotas AWS APIe la AWS CLIper richiedere aumenti delle quote, quando necessario.

Termini del servizio

Per i termini del AWS Ground Station servizio, consulta i Termini AWS di servizio.

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
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	RSSFeed aggiunto 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 migliorat a e aggiunta della sezione «Selezione e CPU pianifica zione delle EC2 istanze».	6 marzo 2024

Aggiornamento della documentazione	Sono state aggiunte nuove best practice alla Guida per l'utente dell' AWS Ground Station agente per l'esecuzione 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 DirectBroadcastSatelliteWbDigIfEc 2.	14 febbraio 2024
Aggiornamento della documentazione	È stato aggiunto un riferimento AWS Notifiche all'utente 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	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 AWSGroundStationAgentInstancePolicy.	12 aprile 2023

Nuova funzionalità	Aggiornata la guida per l'utente per il rilascio di CPE Preview.	9 novembre 2022
Nuova politica AWS gestita	AWS Ground Station ha aggiunto il AWSServiceRoleForGroundStationDataflowEndpointGroup 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.	5 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 AWS 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

Glossario per AWS

Per la terminologia AWS più recente, consultare il glossario AWS nella documentazione di riferimento per 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.