aws

Guida per l'utente

# AWS Ground Station

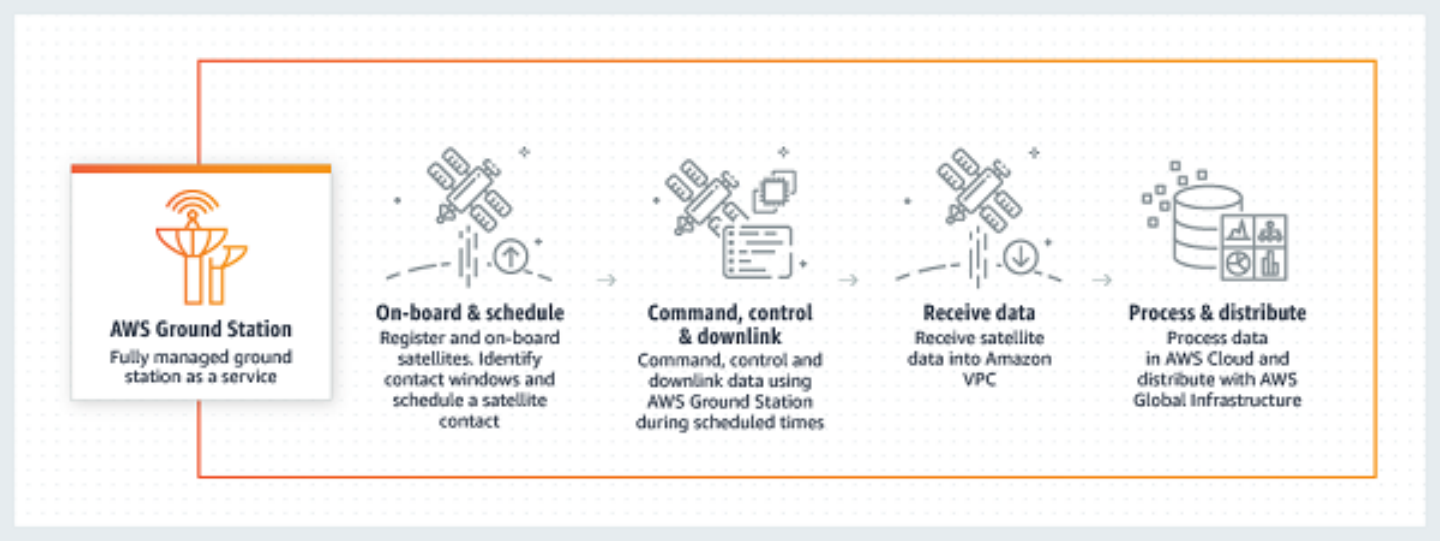
# AWS Ground Station: Guida per l'utente

# Table of Contents

# Cosa è AWS Ground Station?

AWS Ground Station è un servizio completamente gestito che consente di controllare la comunicazione satellitare, l'elaborazione dei dati satellitari e di scalare le operazioni satellitari. Questo significa che non è più necessario creare o gestire la propria infrastruttura di stazione terrestre.

AWS Ground Station ti permette di concentrarti sull'innovazione e sulla sperimentazione rapida di nuove applicazioni che caricano i dati satellitari e scalano dinamicamente l'utilizzo dei server e dello storage, invece che spendere risorse per l'utilizzo e la manutenzione delle stazioni terrestri personali.



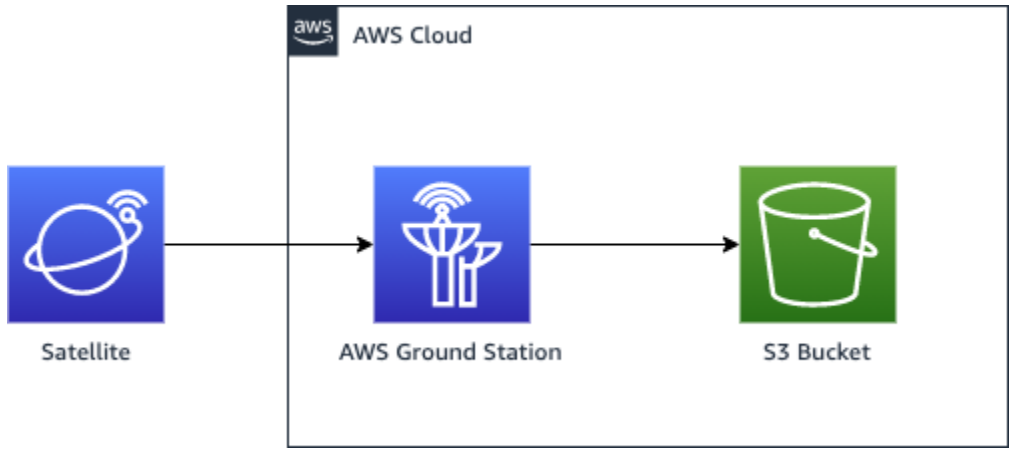
# Funzionamento di AWS Ground Station

Una prenotazione del satellite è anche nota come un contatto. Il satellite comunica con un' AWS Ground Station antenna durante i contatti. Puoi prenotare i contatti tramite un'API o tramite la AWS console specificando posizione, ora e informazioni sulla missione. I tuoi dati di contatto possono essere trasmessi in streaming da e verso un'istanza Amazon Elastic Compute Cloud (Amazon EC2) o distribuiti in modo asincrono a un bucket Amazon Simple Storage Service (Amazon S3) nel tuo account.

Puoi creare risorse di configurazione estensibili e riutilizzabili in modo da avere il controllo sulla configurazione delle antenne durante i contatti. AWS Ground Station Utilizzando profili di missione, puoi specificare la provenienza dei dati, il formato previsto e la destinazione di invio.

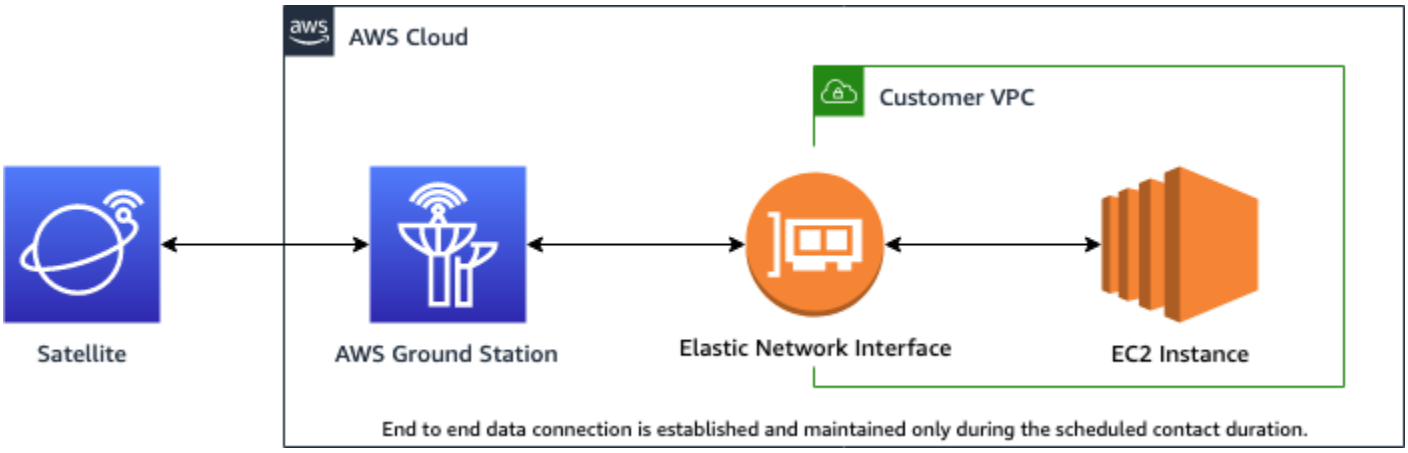
## Distribuzione dei dati ad Amazon S3

Con la consegna dei dati ad Amazon S3, i dati di contatto vengono inviati in modo asincrono a un bucket Amazon S3 del tuo account. I dati di contatto vengono forniti come file di acquisizione dei pacchetti (pcap) per consentire la riproduzione dei dati di contatto in una Software Defined Radio (SDR) o per estrarre i dati del payload dai file pcap per l'elaborazione. I file pcap vengono consegnati al tuo bucket Amazon S3 ogni 30 secondi quando i dati di contatto vengono ricevuti dall'hardware dell'antenna per consentire l'elaborazione dei dati di contatto durante il contatto, se lo desideri. Una volta ricevuti, puoi elaborare i dati utilizzando il tuo software di post-elaborazione o utilizzare altri servizi AWS come Amazon SageMaker 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.



# Distribuzione dei dati ad Amazon EC2

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




# Ulteriori informazioni

Con AWS Ground Station puoi accedere a più di 125 servizi tramite comunicazioni satellitari. Tieni presente quanto segue:

- Puoi possibile ricevere dati RF a banda stretta in banda S (da 2200 a 2300 MHz) o in banda X (da 7750 a 8400 MHz) a larghezze di banda fino a 54 MHz.
  - I dati RF S-Band vengono digitalizzati e forniti come flusso digitale in formato VITA-49 Signal Data/IP.
  - I dati della frequenza intermedia (IF) X-Band vengono digitalizzati e forniti come flusso digitale in formato VITA-49 Signal Data/IP.
- Puoi ricevere dati demodulati/decodificati a banda larga in banda X (da 7750 a 8400 MHz) a larghezze di banda fino a 500 MHz
  - I dati della frequenza intermedia (IF) X-Band sono demodulati, decodificati e forniti come flusso digitale in formato VITA-49 Extension Data/IP.
- È possibile ricevere dati DigiF (Digital Intermediate Frequency) a banda larga da 40 MHz a 400 MHz di larghezza di banda tramite l'agente. AWS Ground Station
  - AWS Ground Station Guida per l'utente dell'agentePer ulteriori informazioni su AWS Ground Station Agent e Wideband DigiF Data Delivery, vedere.
- Puoi trasmettere dati RF in S-Band (da 2025 a 2120 MHz) ad ampiezze di banda fino a 54 MHz.

- I dati RF vengono forniti AWS Ground Station come flusso digitale in formato VITA-49 Signal Data/IP.

- È necessario eseguire l'esecuzione AWS Ground Station da una regione che supporti. AWS AWS Ground Station Per visualizzare un elenco delle regioni supportate, consulta la tabella delle regioni dell'infrastruttura globale.
- Puoi fornire dati a un'istanza Amazon EC2 in esecuzione nella stessa regione dell'antenna oppure puoi utilizzare la distribuzione di dati tra regioni per inviare i dati da un'antenna a un'istanza Amazon EC2 nella tua regione AWS preferita. Le seguenti antenna-to-destination regioni sono attualmente disponibili:
  - 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)

## Termini del servizio

Puoi utilizzare i Servizi solo per archiviare, recuperare, servire, eseguire ed eseguire query su I tuoi contenuti di proprietà, concessi in licenza o lecitamente ottenuti da te. In questi termini di servizio, (a) "I tuoi contenuti" include qualsiasi "Contenuto aziendale" e "Contenuto del cliente" e (b) "Contenuti AWS" include le "Proprietà Amazon". Nell'ambito dei Servizi, puoi essere autorizzato a utilizzare un determinato software (inclusa la relativa documentazione) fornito da noi o da licenziatari di terze parti.

> **Important**
>
> Questo software non ti viene venduto né distribuito e puoi utilizzarlo esclusivamente nell'ambito dei Servizi. Non puoi trasferirlo al di fuori dei Servizi senza una specifica autorizzazione in tal senso.

## Componenti principali

I gruppi di endpoint, le configurazioni e i profili di missione Dataflow sono componenti fondamentali di. AWS Ground Station Questi componenti determinano come pianifichi i contatti, come le antenne comunicano con i satelliti e dove vengono consegnati i dati. Prima di iniziare AWS Ground Station, ti consigliamo di informarti su questi componenti. Esempi sono forniti nelle rispettive sezioni.

Argomenti



## Gruppi di endpoint del flusso di dati

Gli endpoint del flusso di dati definiscono il percorso in cui o da cui eseguire lo streaming dei dati durante i contatti. Gli endpoint vengono identificati da un nome a scelta durante l'esecuzione dei contatti. Questi nomi non devono essere univoci. Ciò consente di eseguire più contatti contemporaneamente utilizzando lo stesso profilo di missione.

L'indirizzo dell'elenco di endpoint è costituito da:

- `name` - Indirizzo IP dell'endpoint del flusso di dati.
- `port` - La porta a cui connettersi.

I dettagli di sicurezza di un endpoint sono costituiti da:

- `roleArn`- L'Amazon Resource Name (ARN) di un ruolo che AWS Ground Station assumerà la responsabilità di creare interfacce di rete elastiche (ENI) nel tuo VPC. Queste ENI fungono da punti di ingresso e di 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 posiziona interfacce di rete elastiche per inviare flussi alle tue istanze.

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

Esempio di politica di fiducia

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

```
{
  "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 policy sui ruoli

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

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

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

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.

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. Puoi eseguire più contatti contemporaneamente, ma tali contatti devono essere eseguiti su diversi gruppi di endpoint di dataflow.

I gruppi di endpoint Dataflow devono essere in grado di pianificare i contatti che li utilizzano. `HEALTHY` Di seguito sono elencati i motivi per cui i gruppi di endpoint Dataflow potrebbero non trovarsi in uno `HEALTHY` stato e le azioni correttive appropriate da intraprendere.

- `NO_REGISTERED_AGENT`- Avvia l'istanza EC2, che registrerà l'agente. Nota che è necessario disporre di un file di configurazione del controller valido affinché questa chiamata abbia successo. Per informazioni dettagliate sulla configurazione di tale file, consulta la AWS Ground Station Guida per l'utente dell'agente
- `INVALID_IP_OWNERSHIP`- Utilizza l' DeleteDataflowEndpointGroup API per eliminare il Dataflow Endpoint Group, quindi utilizza l' CreateDataflowEndpointGroup API per ricreare il Dataflow Endpoint Group utilizzando gli indirizzi IP e le porte associati all'istanza EC2.
- `UNVERIFIED_IP_OWNERSHIP`- L'indirizzo IP non è stato ancora convalidato. La convalida avviene periodicamente, quindi dovrebbe risolversi da sola.
- `NOT_AUTHORIZED_TO_CREATE_SLR`- L'account non è autorizzato a creare il ruolo collegato ai servizi necessario. Controlla la procedura di risoluzione dei problemi in Utilizzo di ruoli collegati ai servizi per Ground Station

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

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

## 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.

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

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

### Config di endpoint del flusso di dati

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

Puoi utilizzare le configurazioni degli endpoint dataflow per specificare quale endpoint di flusso di dati in un gruppo di endpoint dataflow da cui o verso il quale desideri che i dati fluiscano durante un contatto. I due parametri di una configurazione endpoint del flusso di dati specificano il nome e la regione dell'endpoint del flusso di dati. Quando prenoti un contatto, AWS Ground Station analizza il profilo di missione specificato e tenta di trovare un gruppo di endpoint dataflow che contenga tutti gli

endpoint del flusso di dati specificati dalle configurazioni degli endpoint dataflow contenute nel tuo profilo di missione.

La `dataflowEndpointName` proprietà di una configurazione di endpoint dataflow specifica quale endpoint di dataflow in un gruppo di endpoint dataflow verso quale 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.

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

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

## Config di registrazione S3

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

Puoi utilizzare le configurazioni di registrazione S3 per specificare un bucket Amazon S3 a cui desideri che vengano consegnati i dati in downlink. I due parametri di una configurazione di registrazione S3 specificano il bucket Amazon S3 e il ruolo IAM da assumere durante AWS Ground Station la consegna dei dati al bucket Amazon S3. Il ruolo IAM e il bucket Amazon S3 specificati devono soddisfare i seguenti criteri:

- Il nome del bucket Amazon S3 deve iniziare con. `aws-groundstation`
- Il ruolo IAM deve avere una politica di fiducia che consenta al responsabile del `groundstation.amazonaws.com` servizio di assumere il ruolo. Per un esempio, consulta la sezione Example Trust Policy di seguito. Durante la creazione della configurazione l'id della risorsa di configurazione non esiste, la policy di fiducia deve utilizzare un asterisco (*) al posto di *your-config-id*e può essere aggiornata dopo la creazione con l'id della risorsa di configurazione.
- Il ruolo IAM deve avere una policy IAM che consenta al ruolo di eseguire l'`s3:GetBucketLocation`azione sul bucket e l'`s3:PutObject`azione sugli oggetti del bucket. Se il bucket Amazon S3 dispone di una bucket policy, la bucket policy deve consentire anche al ruolo IAM di eseguire queste azioni. Per un esempio, consulta la sezione Example Role Policy di seguito.

Esempio di politica di fiducia

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

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

Esempio di policy sui ruoli

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

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation"
      ],
      "Resource": [
        "arn:aws:s3:::your-bucket-name"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3:::your-bucket-name/*"
      ]
    }
  ]
}
```

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

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

## 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.

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

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

## Config di downlink antenna

È possibile utilizzare le configurazioni di downlink dell'antenna per configurare l'antenna per il downlink durante il contatto. Sono costituite da una configurazione dello spettro che specifica la frequenza, la larghezza di banda e la polarizzazione da utilizzare durante il contatto in downlink. Se il tuo caso d'uso del downlink richiede la demodulazione o la decodifica, consulta il. Config di decodifica demodulazione downlink antenna

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

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

## Config di decodifica demodulazione downlink antenna

I config di decodifica demodulazione downlink antenna sono un tipo di config più complesso e personalizzabile che puoi utilizzare per eseguire il downlink dei contatti con demodulazione o decodifica. Se sei interessato a eseguire questi tipi di contatti, contatta il AWS Ground Station team. Ti aiuteranno a definire il config e il profilo di missione corretti per il tuo caso d'uso.

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

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

## Config di uplink antenna

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

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

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

## Config Uplink Echo

I config di uplink echo indicano all'antenna come eseguire un uplink echo. Questo effettua l'echo dei segnali inviati dall'antenna all'endpoint del flusso di dati. Un config di uplink echo contiene l'ARN di

un config uplink. L'antenna utilizza i parametri del config di uplink a cui fa riferimento l'ARN durante l'esecuzione di un uplink echo.

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

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

## Profili di 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 sarà configurata l'antenna e dove andranno i dati durante il contatto.

Oltre al monitoraggio, tutti i config, sono contenuti nel campo `dataflowEdges` del profilo di missione. Un singolo edge del flusso di dati è un elenco di due ARN: il primo è il config da e il secondo è il config a . Specificando un margine del flusso di dati tra due configurazioni, si indica AWS Ground Station da dove e verso dove devono fluire i dati durante un contatto. I config di monitoraggio non vengono utilizzati come parte di un edge del flusso di dati, ma vengono specificati come un campo separato.

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

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

- AWS::GroundStation::MissionProfile CloudFormation tipo di risorsa
- AWS CLI Riferimento al profilo di missione
- Riferimento all'API Mission Profile

# AWS Ground StationSedi

I clienti possono trasmettere e ricevere dati utilizzando le antenne AWS Ground Station nelle seguenti località: Stati Uniti (Oregon), Stati Uniti (Ohio), Stati Uniti (Alaska), Medio Oriente (Bahrain), Europa (Stoccolma), Asia Pacifico (Dubbo), Europa (Irlanda), Africa (Città del Capo), Stati Uniti (Hawaii), Asia Pacifico (Seoul), Asia Pacifico (Singapore) e Sud America (Punta Arené) gas).

I clienti possono fornire dati e configurare i propri contatti con la console AWS Ground Station nelle seguenti regioni: Stati Uniti occidentali (Oregon), Stati Uniti orientali (Ohio), Medio Oriente (Bahrein), Europa (Stoccolma), Asia Pacifico (Dubbo), Europa (Irlanda), Africa (Città del Capo), Stati Uniti orientali (Virginia settentrionale), Europa (Francoforte), Asia Pacifico (Seoul), Asia Pacifico (Singapore) e Sud America (San Paolo).

Nota: puoi creare risorse AWS Ground Station solo nelle regioni che ospitano la console AWS Ground Station menzionata nel paragrafo precedente.

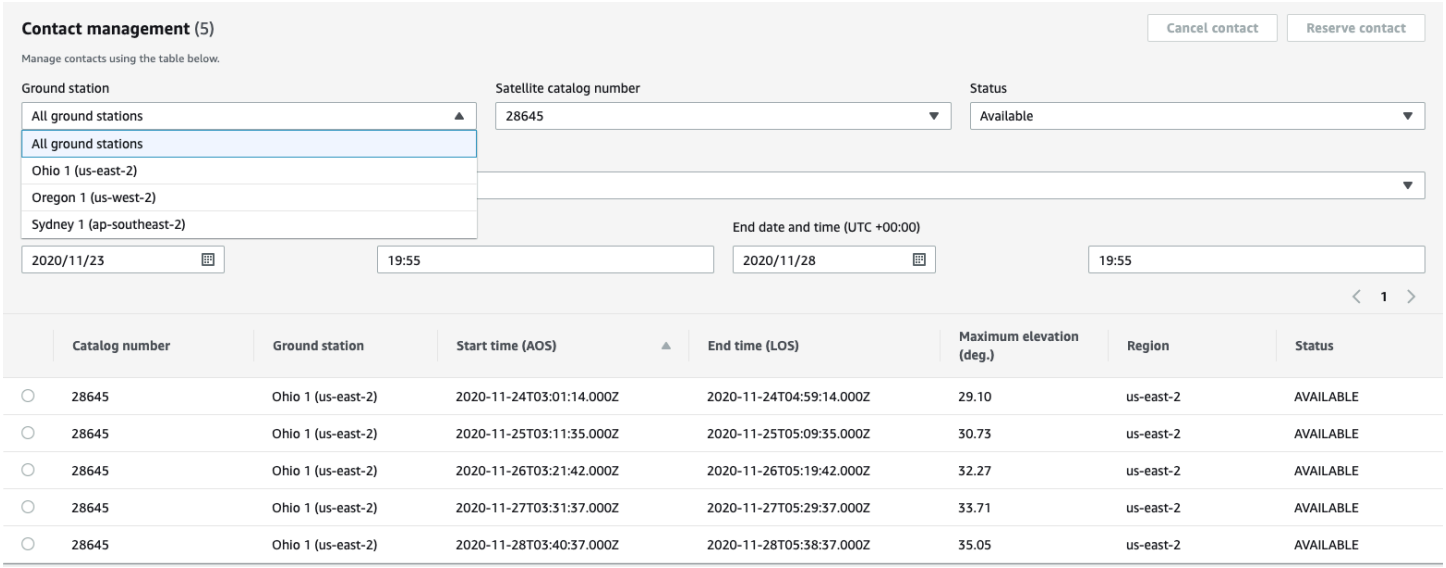

Argomenti

- Individuazione della regione AWS per una Ground Station

# Individuazione della regione AWS per una Ground Station

La rete globale AWS include sedi Ground Station che non si trovano fisicamente nella regione AWS a cui sono collegate. L'inserimento e la prenotazione dei contatti in una di queste sedi Ground Station devono essere eseguiti utilizzando la regione AWS a cui è collegata la Ground Station.

Esistono diversi metodi per determinare la regione AWS di una Ground Station. La pagina della AWS Ground Station console mostra la regione AWS di Ground Station sia nella tabella dei filtri che dei contatti, come mostrato nell'immagine seguente. L'SDK AWS contiene la regione AWS di Ground Station nella ListGroundStationrisposta. Infine, l'AWS CLI contiene la regione AWS di Ground Station nella list-ground-stationsrisposta.




Argomenti

- Esempio di Ground Station situata al di fuori di una regione AWS

## Esempio di Ground Station situata al di fuori di una regione AWS

Hawaii 1 è un esempio di sede Ground Station che non si trova fisicamente nella regione AWS a cui è connessa. La Hawaii 1 Ground Station si trova alle Hawaii, negli Stati Uniti, ma è collegata alla regione AWS us-west-2 (Oregon). Per elencare e prenotare contatti utilizzando Hawaii 1, devi avere un profilo di missione configurato nella regione AWS us-west-2 (Oregon) e utilizzare la regione AWS us-west-2 (Oregon) nella AWS Ground Station console, AWS CLI o AWS SDK.

- Per elencare e prenotare i contatti di Hawaii 1 nella console, devi utilizzare la AWS Ground Station console nella regione us-west-2 (Oregon). AWS Ground Station
- Per elencare e prenotare i contatti per Hawaii 1 utilizzando l'interfaccia a riga di comando di AWS, devi specificare la regione come us-west-2 utilizzando `--region` l'argomento CLI.
- Per elencare e prenotare i contatti per Hawaii 1 utilizzando l'SDK AWS, devi impostare la regione del tuo client su us-west-2. Il modo in cui lo imposti dipende dal linguaggio di programmazione che stai utilizzando. Un esempio di come impostarlo JavaScript è descritto nell'SDK AWS per la JavaScript documentazione. Per ulteriori informazioni, consulta la documentazione SDK specifica per la lingua.

# Configurazione AWS Ground Station

Prima di iniziare a utilizzare AWS Ground Station, è necessario sapere quali autorizzazioni AWS Identity and Access Management (IAM) sono necessarie e quali credenziali del veicolo spaziale fornire. Utilizzare la procedura seguente per impostare l'account.

Argomenti



## Iscriviti 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 pagina all'indirizzo https://portal.aws.amazon.com/billing/signup.
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 Servizi AWS nell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente amministrativo 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.

# Creazione di un utente amministratore

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. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

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

Creazione di un utente amministratore

1. Abilita Centro identità IAM.

   Per istruzioni, consulta Abilitazione di AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center .
2. In IAM Identity Center, assegna l'accesso amministrativo a un utente amministratore.

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

Accesso come utente amministratore

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

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

# Aggiungi le autorizzazioni Ground Station 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 AWS Management Console e apri la console IAM.
2. Creare una nuova policy. Utilizza le fasi seguenti:

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

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

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

```
{
  "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 console IAM, collega la policy che hai creato all'utente desiderato.

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

# Onboarding dei clienti

Per completare la registrazione del tuo AWS Ground Station account, consulta la sezione Satelliti e risorse nella pagina della AWS Ground Station console per i dettagli sull'onboarding. Il AWS Ground Station team collaborerà con te per aggiungere i satelliti al servizio. Una volta a bordo del satellite, il satellite sarà disponibile per la gestione di un contatto. Le istruzioni per la gestione di un contatto sono fornite nella sezione Inserimento e prenotazione dei contatti.

L'onboarding dei satelliti ti consentirà di inviare e ricevere dati da e verso il satellite. Oltre all'onboarding dei propri satelliti, i clienti possono anche eseguire l'onboarding dei seguenti satelliti per effettuare il downlink dei dati di trasmissione diretta utilizzando AWS Ground Station:

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

Una volta a bordo, è possibile accedere a questi satelliti per un uso immediato. AWS Ground Station mantiene una serie di AWS CloudFormation modelli preconfigurati per facilitare l'avvio del servizio. Le istruzioni e i dettagli per accedere e utilizzare questo modello sono disponibili nella sezione Crea le tue risorse utilizzando un AWS CloudFormation modello della guida per l'utente.

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

## Fasi successive

Il tuo AWS Ground Station account è ora configurato e pronto per la configurazione. Continuare su Nozioni di base per configurare le risorse per utilizzare AWS Ground Station.

# Guida introduttiva con AWS Ground Station

AWS Ground Station consente di comandare, controllare e effettuare il downlink dei dati dai satelliti.

Con AWS Ground Station, puoi programmare l'accesso alle antenne delle stazioni terrestri su base al minuto e pagare solo per il tempo di utilizzo dell'antenna. AWS Ground Station invia i tuoi dati di contatto in modo asincrono a un bucket Amazon Simple Storage Service (Amazon S3) nel tuo account o in modo sincrono trasmettendoli in streaming da e verso un'istanza Amazon Elastic Compute Cloud (Amazon EC2) nel tuo account. I passaggi seguenti descrivono come configurare le risorse necessarie per ricevere i dati di contatto in modo asincrono in un bucket Amazon S3. Consulta la Distribuzione dei dati ad Amazon EC2 guida per informazioni su come utilizzare la consegna dei dati ad Amazon EC2.

Argomenti



## Concetti di base

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

Quindi, continua Prerequisiti a scoprire i prerequisiti per iniziare. AWS Ground Station

## Prerequisiti

Prima di iniziare AWS Ground Station, assicurati di disporre di un AWS account con le credenziali corrette. Seguire la procedura riportata in Configurazione AWS Ground Station.

> **Note**
>
> Se utilizzerai DigiF Data Delivery a banda larga, consulta le istruzioni. AWS Ground Station Guida per l'utente dell'agente

Altrimenti, continua con. Passaggio 1: scegli un AWS CloudFormation modello

# Passaggio 1: scegli un AWS CloudFormation modello

Dopo essere saliti a bordo del satellite, è necessario definire i profili di missione per definire la configurazione dell' AWS Ground Station antenna per il downlink dei dati dal satellite. Per assisterti in questo processo, forniamo AWS CloudFormation modelli preconfigurati per DigiF Data Delivery a banda stretta e a banda larga che utilizzano satelliti di trasmissione pubblici. Questi modelli ti semplificano l'avvio dell'utilizzo. AWS Ground Station Per ulteriori informazioni su AWS CloudFormation, consulta What is AWS CloudFormation?

A seconda del tipo di contatto che desideri contattare, scegli il tipo di modello CFN appropriato dall'elenco seguente:

- Modelli di distribuzione dati S3 a banda stretta AWS CloudFormation.
- Modelli di distribuzione dati S3 a banda larga DigIf AWS CloudFormation.

Se non desideri utilizzare uno dei AWS CloudFormation modelli predefiniti, puoi visualizzare le istruzioni su. Creazione del proprio modello

## Modelli di distribuzione dati S3 a banda stretta AWS CloudFormation

### Modelli preconfigurati

Oggi puoi configurare più flussi di dati per contatto in modo che confluiscano in un bucket S3. Questi flussi di dati sono disponibili in due formati diversi. I flussi di dati contenenti dati VITA-49 Signal/IP possono essere configurati per segnali S-Band e X-Band fino a 54 MHz di larghezza di banda. I dati di estensione VITA-49 possono essere configurati per segnali X-Band demodulati e/o decodificati fino a 500 MHz di larghezza di banda.

AWS Ground Station fornisce modelli per entrambi i formati di flussi di dati che dimostrano come utilizzare il servizio. Utilizza questa guida per trovare il modello giusto per te.

Modelli disponibili

Puoi utilizzare un modello preconfigurato per ricevere dati di trasmissione diretta dai satelliti Aqua, SNPP, JPSS-1/NOAA-20 e Terra. Questi AWS CloudFormationmodelli contengono le risorse necessarie AWS Ground Station e Amazon S3 per pianificare ed eseguire contatti e ricevere i dati in

un bucket Amazon S3 del tuo account. Se Aqua, SNPP, JPSS-1/NOAA-20 e Terra non sono integrati nel tuo account, consulta Onboarding del cliente.

Modelli di distribuzione dei dati a banda stretta

Se utilizzi la distribuzione di dati a banda stretta per il tuo contatto, utilizza i modelli seguenti. AWS CloudFormation

- Il AWS CloudFormation modello denominato `AquaSnppJpss-1DemodDecodeS3DataDelivery.yml` contiene un bucket Amazon S3 e AWS Ground Station le risorse necessarie per pianificare i contatti e ricevere dati di trasmissione diretta demodulati e decodificati. Questo modello è un buon punto di partenza se si prevede di elaborare i dati utilizzando il software NASA Direct Readout Labs (RT-STPS e IPOPP).

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

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

  È possibile scaricare e visualizzare il modello nella console spostandosi all'URL seguente nel browser:

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

  È possibile specificare il modello direttamente AWS CloudFormation utilizzando il seguente link:

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

- 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 di segnale/IP VITA-49. Questo modello è un buon punto di partenza se prevedi di elaborare i dati utilizzando una radio definita dal software (SDR) per demodulare e decodificare i dati prima della post-elaborazione.

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

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

È possibile scaricare e visualizzare il modello nella console spostandosi all'URL seguente nel browser:

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

È possibile specificare il modello direttamente AWS CloudFormation utilizzando il seguente link:

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

Quali risorse definiscono questi modelli?

Entrambi i modelli contengono le stesse risorse, con l'unica differenza che sono le configurazioni dell'antenna. Per ulteriori informazioni, vedere la descrizione di Antenna Config di seguito.

- Amazon S3 Bucket: il bucket a cui verranno distribuiti i dati scaricati. Il nome di questo bucket inizia con `aws-groundstation` per soddisfare i criteri descritti in S3 Recording Config.
- Ruolo IAM: ruolo che il responsabile del `groundstation.amazonaws.com` servizio AWS Ground Station assume quando scrive i dati scaricati nel bucket Amazon S3.
- Amazon S3 Bucket Policy: una policy che consente al ruolo IAM di eseguire le seguenti azioni sul bucket Amazon S3 e sui relativi oggetti:
  - `s3:GetBucketLocation`
  - `s3:PutObject`
- Config di tracciamento - Una configurazione di AWS Ground Station tracciamento che definisce il modo in cui il sistema di antenna segue il satellite mentre si muove nel cielo.
- S3 Recording Config: AWS Ground Station una configurazione di registrazione S3 che fa riferimento al bucket Amazon S3 e al ruolo AWS Ground Station IAM da utilizzare per la distribuzione dei dati.
- Config antenna - Una configurazione AWS Ground Station dell'antenna che specifica come configurare l' AWS Ground Station antenna durante un contatto. Il `AquaSnppJpss-1DemodDecodeS3DataDelivery.yml` modello contiene una configurazione

demod decode dell'antenna in downlink che configura l' AWS Ground Station antenna per demodulare e decodificare i dati scaricati prima di inviarli al bucket Amazon S3. Contiene `AquaSnppJpss-1TerraDigIfS3DataDelivery.yml` invece una configurazione di downlink dell'antenna che configura l' AWS Ground Station antenna per fornire i dati ad Amazon S3 come pacchetti di segnale/IP VITA-49.

- Profilo di missione: un profilo di AWS Ground Station missione che raggruppa tutte le configurazioni per consentirti di pianificare ed eseguire contatti AWS Ground Station utilizzando le configurazioni a cui si fa riferimento.

## Modelli di distribuzione dati S3 a banda larga DigIf AWS CloudFormation

### Modelli di distribuzione dati DigiF a banda larga

Se utilizzi la trasmissione di dati Wideband Digital Intermediate Frequency (DiGIF) per il tuo contatto, utilizza i modelli seguenti. AWS CloudFormation

- Il AWS CloudFormation modello denominato `DirectBroadcastSatelliteWbDigIfS3DataDelivery.yml` contiene un bucket Amazon S3 e AWS Ground Station le risorse necessarie per pianificare i contatti e ricevere dati di trasmissione diretta di segnale/IP VITA-49 tramite l'agente. AWS Ground Station Questo modello è un buon punto di partenza se prevedi di elaborare i dati utilizzando una radio definita dal software (SDR) per demodulare e decodificare i dati prima della post-elaborazione. Per ulteriori informazioni sull'agente, vedere. AWS Ground Station AWS Ground Station Guida per l'utente dell'agente

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

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

  È possibile scaricare e visualizzare il modello nella console spostandosi all'URL seguente nel browser:

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

  È possibile specificare il modello direttamente AWS CloudFormation utilizzando il seguente link:

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

Quali risorse definisce questo modello?

- Amazon S3 Bucket: il bucket a cui verranno distribuiti i dati scaricati. Il nome di questo bucket inizia con `aws-groundstation` per soddisfare i criteri descritti in S3 Recording Config.
- Ruolo IAM: ruolo che il responsabile del `groundstation.amazonaws.com` servizio AWS Ground Station assume quando scrive i dati scaricati nel bucket Amazon S3.
- Amazon S3 Bucket Policy: una policy che consente al ruolo IAM di eseguire le seguenti azioni sul bucket Amazon S3 e sui relativi oggetti:
  - `s3:GetBucketLocation`
  - `s3:PutObject`
- AWS KMS Chiave: una AWS KMS chiave utilizzata per crittografare i flussi di dati.
- Ruolo chiave di Ground Station: il ruolo IAM che AWS Ground Station assumerà per accedere e utilizzare la AWS KMS chiave per decrittografare i flussi di dati
- Ground Station Key Access Policy - La policy IAM che definisce AWS Ground Station le azioni da intraprendere sulla Data Delivery Key
- Config di tracciamento - Una configurazione di AWS Ground Station tracciamento che definisce il modo in cui il sistema di antenna segue il satellite mentre si muove nel cielo.
- S3 Recording Config: AWS Ground Station una configurazione di registrazione S3 che fa riferimento al bucket Amazon S3 e al ruolo AWS Ground Station IAM da utilizzare per la distribuzione dei dati.
- Configurazioni antenna per Aqua, SNPP, JPSS-1/NOAA-20 e Terra: tre configurazioni di AWS Ground Station antenna separate che specificano come configurare l'antenna durante un contatto con Aqua, SNPP, JPSS-1/NOAA-20 e Terra. AWS Ground Station Il modello contiene una configurazione di downlink dell'antenna che configura l' AWS Ground Station antenna per fornire i dati ad Amazon S3 come pacchetti di segnale/IP VITA-49.
- Profili di missione per Aqua, SNPP, JPSS-1/NOAA-20 e Terra: tre profili di AWS Ground Station missione separati che AWS Ground Station raggruppano tutte le configurazioni per consentire di pianificare ed eseguire i contatti utilizzando le configurazioni a cui si fa riferimento con Aqua, SNPP, JPSS-1/NOAA-20 e Terra.

## Creazione del proprio modello

La configurazione delle risorse per pianificare ed eseguire i contatti per i propri satelliti richiede la configurazione AWS Ground Station delle risorse del proprio account in modo che corrispondano alle impostazioni del satellite. Questo è difficile da fare da soli. Il AWS Ground Station team è disponibile ad aiutarti a configurare AWS Ground Station le risorse del tuo account per il downlink e l'uplink verso il tuo satellite. Per configurare il tuo satellite con cui utilizzarlo AWS Ground Station, contatta AWS Support.

# Fase 2: Configurare uno AWS CloudFormation stack

Dopo aver scelto il modello più adatto al tuo caso d'uso, configura uno AWS CloudFormation stack. Le risorse create in questa procedura vengono configurate per la regione in cui ti trovi quando vengono create.

1. In AWS Management Console, scegli Servizi > CloudFormation.
2. Nel riquadro di navigazione selezionare Stacks (Stack). Quindi scegliere Crea stack > Con nuove risorse (standard).
3. Nella pagina Create stack (Crea stack), specificare il modello selezionato in the section called “Passaggio 1: scegli un AWS CloudFormation modello” eseguendo una delle seguenti operazioni.

    a. Selezionare l'URL Amazon S3 come origine del modello e copiare e incollare l'URL del modello che si desidera utilizzare nell'URL Amazon S3. Quindi, seleziona Next (Successivo).

    b. Selezionare Upload a template file (Carica un file modello) come origine modello e scegliere Choose File (Scegli file). Caricare il modello scaricato in the section called “Passaggio 1: scegli un AWS CloudFormation modello”. Quindi, seleziona Next (Successivo).
4. Esegui i passaggi seguenti nella pagina Specificare i dettagli dello stack:

    a. Immettere un nome nella casella Stack Name (Nome stack). Si consiglia di utilizzare un nome semplice per ridurre la possibilità di errori in futuro.

    b. Seleziona Avanti.
5. Configura le opzioni di stack e le opzioni avanzate per la tua istanza Amazon EC2.

    a. Aggiungere tutti i tag e le autorizzazioni nelle sezioni Tag e Permissions (Autorizzazioni).

b. Apportare le modifiche a Stack policy (Policy stack), Rollback configuration (Configurazione rollback), Notification options (Opzioni di notifica) e alle Stack creation options (Opzioni di creazione dello stack).

c. Seleziona Avanti.

6. Dopo aver esaminato i dettagli dello stack, selezionare il riconoscimento delle capacità e scegliere Create stack (Crea stack).

# AWS Ground Station Guida per l'utente dell'agente

Argomenti



# Panoramica

## Cos'è l' AWS Ground Station agente?

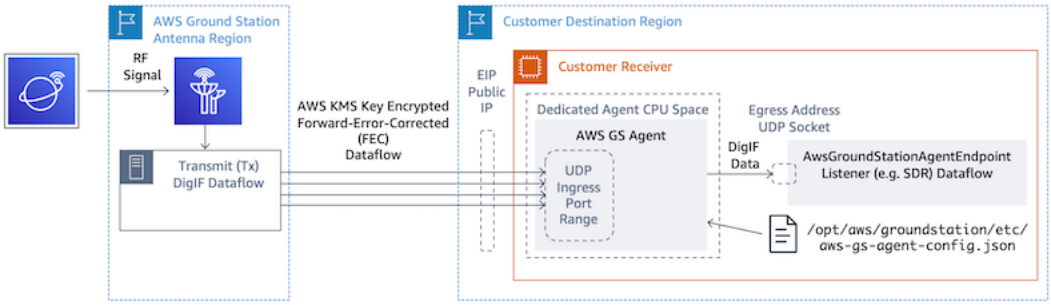
AWS Ground Station Agent, disponibile come RPM, consente AWS Ground Station ai clienti di ricevere (downlink) flussi di dati sincroni Wideband Digital Intermediate Frequency (DigiF) durante i contatti con AWS Ground Station. I clienti possono selezionare due opzioni per la consegna dei dati:

1. Distribuzione dei dati a un'istanza EC2: consegna dei dati a un'istanza EC2 di proprietà del cliente. AWS Ground Station i clienti gestiscono l'agente. AWS Ground Station Questa opzione può essere la soluzione migliore se è necessaria un'elaborazione dei dati quasi in tempo reale. Consulta la Distribuzione dei dati ad Amazon EC2 guida per informazioni sulla distribuzione dei dati EC2.

2. Distribuzione dei dati a un bucket S3 - Distribuzione dei dati a un bucket AWS S3 di proprietà del cliente tramite un servizio gestito Ground Station. Consulta la Guida introduttiva con AWS Ground Station guida per informazioni sulla distribuzione dei dati S3.

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

> **Note**
>
> Poiché la distribuzione dei dati S3 è un servizio gestito da Ground Station, questa guida si concentra sulla distribuzione dei dati alle istanze EC2.




Flusso di dati DigiF da una regione di AWS Ground Station antenna alla tua istanza EC2 con il tuo Software-Defined Radio (SDR) o un ascoltatore simile.

## Caratteristiche dell'agente AWS Ground Station

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 rete AWS.
- Distribuzione affidabile dei dati tramite Forward Error Correction (FEC).
- Distribuzione sicura dei dati utilizzando una AWS KMS chiave di crittografia gestita dal cliente.

# Requisiti dell'agente

> **Note**
>
> Questa guida per AWS Ground Station agenti presuppone che l'utente sia salito a bordo di Ground Station utilizzando la guida. Configurazione AWS Ground Station

L'istanza EC2 di AWS Ground Station Agent Receiver richiede un set di risorse AWS dipendenti per fornire in modo affidabile e sicuro i dati DigiF ai tuoi endpoint.

1. Un VPC in cui avviare il ricevitore EC2.
2. Una chiave AWS KMS per la crittografia/decrittografia dei dati.
3. Una chiave SSH o un profilo di istanza EC2 configurato per SSM Session Manager.
4. Regole del gruppo di rete/sicurezza per consentire quanto segue:
    1. Traffico UDP proveniente dalle AWS Ground Station porte specificate nel gruppo di endpoint dataflow. L'agente riserva una serie di porte contigue utilizzate per fornire dati agli endpoint del flusso di dati in ingresso.
    2. Accesso SSH alla tua istanza (Nota: in alternativa puoi utilizzare AWS Session Manager per accedere alla tua istanza EC2).
    3. Accesso in lettura a un bucket S3 accessibile pubblicamente per la gestione degli agenti.
    4. Traffico SSL sulla porta 443 che consente all'agente di comunicare con il servizio. AWS Ground Station
    5. Traffico proveniente dall'elenco dei AWS Ground Station prefissi gestiti. `com.amazonaws.global.groundstation`

Inoltre, è richiesta una configurazione VPC che includa una sottorete pubblica. Consulta la Guida per l'utente VPC per informazioni di base sulla configurazione della sottorete.

Configurazioni compatibili:

1. Un IP elastico associato all'istanza EC2 in una sottorete pubblica.
2. Un IP elastico associato a un ENI in una sottorete pubblica, collegato all'istanza EC2 (in qualsiasi sottorete).

Puoi utilizzare lo stesso gruppo di sicurezza dell'istanza EC2 o specificarne uno con almeno il set minimo di regole composto da:

- Traffico UDP proveniente dalle AWS Ground Station porte specificate nel gruppo di endpoint dataflow.

Consulta la sezione «Modelli DigiF Data Delivery a banda larga», ad Seleziona un modello esempio, modelli di data Delivery di AWS CloudFormation EC2 con queste risorse preconfigurate.

## Diagrammi VPC

Diagramma: un IP elastico associato all'istanza EC2 in una sottorete pubblica

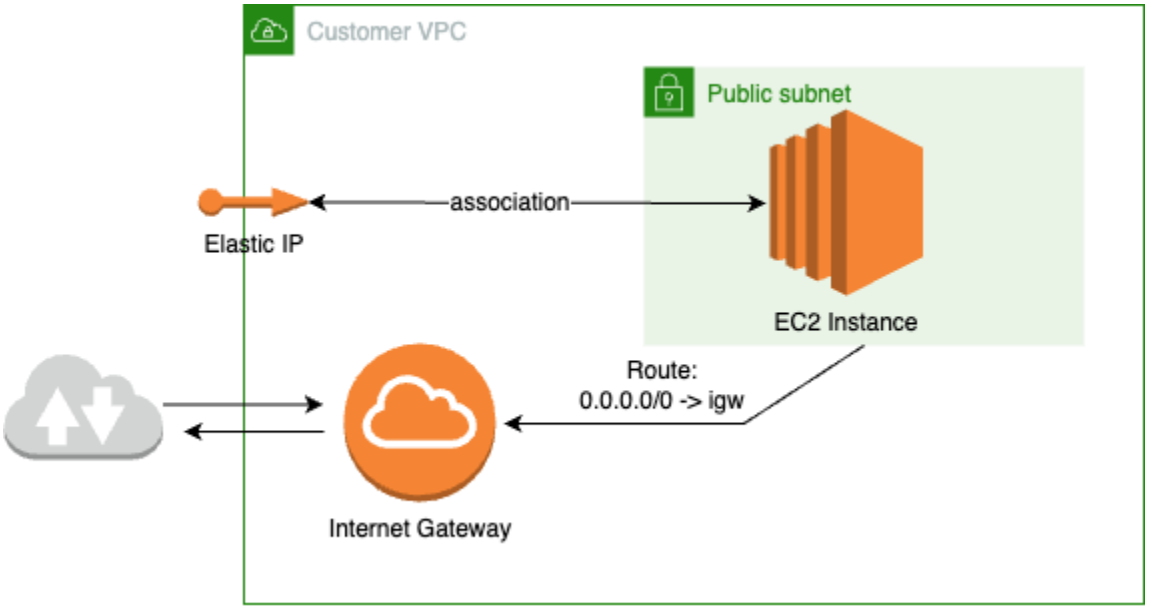
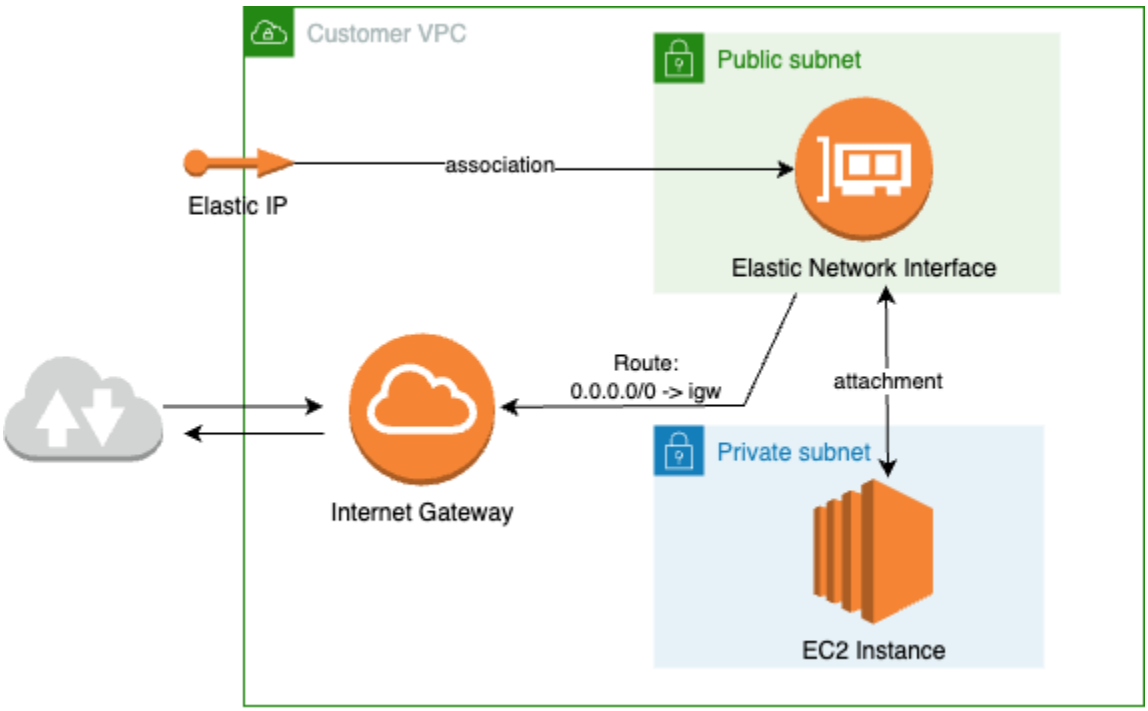



Diagramma: un IP elastico associato a un ENI in una sottorete pubblica, collegato all'istanza EC2 in una sottorete privata




## Sistema operativo supportato

Amazon Linux 2 con kernel 5.10+.

I tipi di istanze supportati sono elencati in Selezione delle istanze EC2 e pianificazione della CPU

# Distribuzione dei dati tramite agente AWS Ground Station

I diagrammi seguenti forniscono una panoramica del flusso di dati AWS Ground Station durante i contatti DiGIF (Wideband Digital Intermediate Frequency).

L' AWS Ground Station agente gestirà l'orchestrazione dei componenti del dataplane per un contatto. Prima di pianificare un contatto, l'agente deve essere configurato e avviato correttamente e deve essere registrato (la registrazione è automatica all'avvio dell'agente) con. AWS Ground Station Inoltre, il software di ricezione dei dati (ad esempio una radio definita dal software) deve essere in esecuzione e configurato per ricevere dati all'indirizzo AwsGroundStationAgentEndpointEgressAddress.

Dietro le quinte, l' AWS Ground Station agente riceverà le operazioni AWS Ground Station e annullerà la AWS KMS crittografia applicata in transito, prima di inoltrarle all'endpoint EgressAddress di destinazione dove è in ascolto la Software Defined Radio (SDR). L' AWS Ground Station agente

e i suoi componenti sottostanti rispetteranno i limiti della CPU impostati nel file di configurazione per garantire che non influiscano sulle prestazioni di altre applicazioni in esecuzione sull'istanza.

I clienti devono avere l' AWS Ground Station agente in esecuzione sull'istanza ricevente coinvolta nel contatto. Un singolo AWS Ground Station agente è in grado di orchestrare più flussi di dati, come illustrato di seguito, se il cliente preferisce ricevere tutti i flussi di dati su un'unica istanza del ricevitore.

## Flussi di dati multipli, ricevitore singolo

Scenario di esempio:

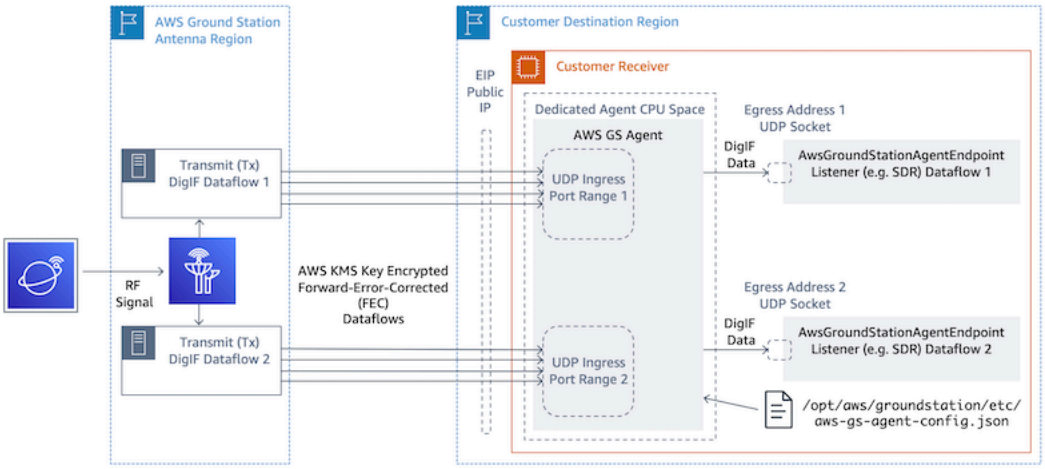
Il cliente desidera ricevere due downlink di antenne come flussi di dati DigiF sulla stessa istanza del ricevitore EC2. I due downlink saranno a 200 MHz e 100 MHz.

AwsGroundStationAgentEndpoints:

Saranno disponibili due `AwsGroundStationAgentEndpoint` risorse, una per ogni flusso di dati. Entrambi gli endpoint avranno lo stesso indirizzo IP pubblico (). `ingressAddress.socketAddress.name` Gli ingressi `portRange` non devono sovrapporsi, poiché i flussi di dati vengono ricevuti nella stessa istanza EC2. Entrambi devono `egressAddress.socketAddress.port` essere unici.

Pianificazione della CPU:

- 1 core (2 vCPU) per l'esecuzione del singolo AWS Ground Station agente sull'istanza.
- 6 core (12 vCPU) per ricevere DigiF Dataflow 1 (ricerca a 200 MHz nella tabella). Pianificazione principale della CPU
- 4 core (8 vCPU) per ricevere DigiF Dataflow 2 (ricerca a 100 MHz nella tabella). Pianificazione principale della CPU
- Spazio totale dedicato sulla CPU dell'agente = 11 core (22 vCPU) sullo stesso socket.




## Flussi di dati multipli, ricevitori multipli

Scenario di esempio:

Il cliente desidera ricevere due downlink di antenne come flussi di dati DigiF su diverse istanze di ricevitori EC2. Entrambi i downlink saranno a 400 MHz.

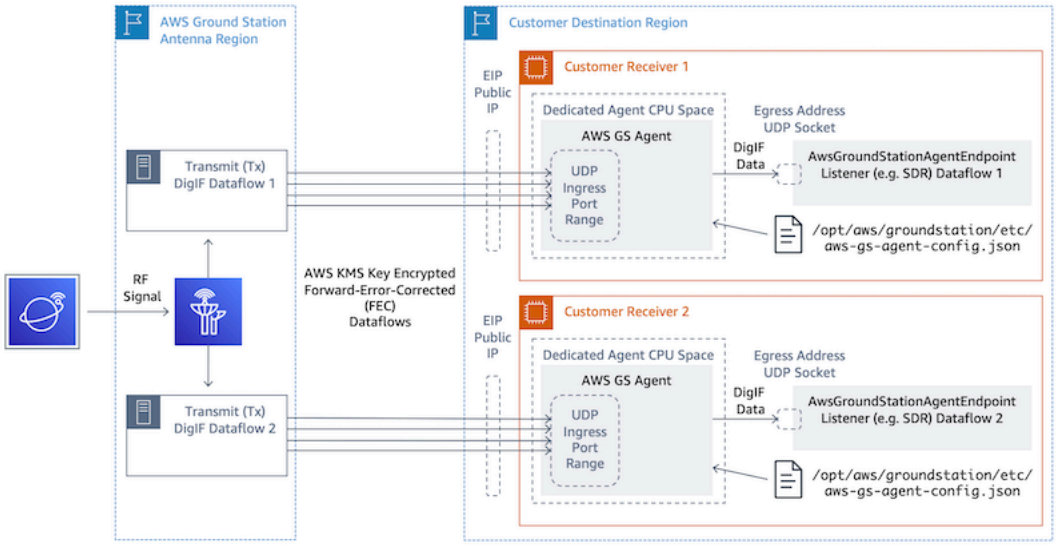
AwsGroundStationAgentEndpoints:

Saranno disponibili due `AwsGroundStationAgentEndpoint` risorse, una per ogni flusso di dati. Gli endpoint avranno un indirizzo IP pubblico diverso (). `ingressAddress.socketAddress.name` Non vi sono restrizioni sui valori delle porte per nessuna delle due `ingressAddress` o `egressAddress` poiché i flussi di dati vengono ricevuti su un'infrastruttura separata e non sono in conflitto tra loro.

Pianificazione della CPU:

- Istanza del ricevitore 1
  - 1 core (2 vCPU) per l'esecuzione del singolo AWS Ground Station agente sull'istanza.
  - 9 core (18 vCPU) per ricevere DigiF Dataflow 1 (ricerca a 400 MHz nella tabella). Pianificazione principale della CPU
  - Spazio totale dedicato sulla CPU dell'agente = 10 core (20 vCPU) sullo stesso socket.
- Istanza del ricevitore 2
  - 1 core (2 vCPU) per l'esecuzione del singolo AWS Ground Station agente sull'istanza.
  - 9 core (18 vCPU) per ricevere DigiF Dataflow 2 (ricerca a 400 MHz nella tabella). Pianificazione principale della CPU

- Spazio totale dedicato sulla CPU dell'agente = 10 core (20 vCPU) sullo stesso socket.




# Selezione delle istanze EC2 e pianificazione della CPU

## Tipi di istanze EC2 supportati

L' AWS Ground Station agente richiede core CPU dedicati per funzionare a causa dei flussi di lavoro di distribuzione dei dati ad alta intensità di calcolo. Supportiamo i seguenti tipi di istanze. Vedi Pianificazione principale della CPU per decidere quale tipo di istanza si adatta meglio al tuo caso d'uso.

| Tipo di istanza | vCPU predefinite | Core CPU predefiniti |
|---|---|---|
| c5.12xlarge | 48 | 24 |
| c5.18xlarge | 72 | 36 |
| c5.24xlarge | 96 | 48 |
| c5n.18xlarge | 72 | 36 |
| c5n.metal | 72 | 36 |
| c6i.32xlarge | 128 | 64 |

| Tipo di istanza | vCPU predefinite | Core CPU predefiniti |
|---|---|---|
| g4dn.12xlarge | 48 | 24 |
| g4dn.16xlarge | 64 | 32 |
| g4dn.metal | 96 | 48 |
| m4.16xlarge | 64 | 32 |
| m5.12xlarge | 48 | 24 |
| m5.24xlarge | 96 | 48 |
| m6i.32xlarge | 128 | 64 |
| p3dn.24xlarge | 96 | 48 |
| p4d.24xlarge | 96 | 48 |
| r5.24xlarge | 96 | 48 |
| r5.metal | 96 | 48 |
| r5n.24xlarge | 96 | 48 |
| r5n.metal | 96 | 48 |
| r6i.32xlarge | 128 | 64 |

## Pianificazione principale della CPU

L' AWS Ground Station agente richiede core di processore dedicati che condividano la cache L3 per ogni flusso di dati. L'agente è progettato per sfruttare le coppie di CPU Hyper-Threaded (HT) e richiede che le coppie HT siano riservate per il suo utilizzo. Una coppia hyper-threaded è una coppia di CPU virtuali (vCPU) contenute in un singolo core. La tabella seguente fornisce una mappatura della velocità dei dati del flusso di dati al numero richiesto di core riservati all'agente per un singolo flusso di dati. Questa tabella presuppone Cascade Lake o CPU più recenti ed è valida per qualsiasi tipo di istanza supportato. Se la larghezza di banda è compresa tra le voci della tabella, seleziona la successiva più alta.

L'agente necessita di un core riservato aggiuntivo per la gestione e il coordinamento, quindi il totale dei core richiesti sarà la somma dei core necessari (dal grafico seguente) per ogni flusso di dati più un singolo core aggiuntivo (2 vCPU).

| AntennaDownlink Larghezza di banda (MHz) | Velocità dati VITA-49.2 DigiF prevista (MB/s) | Numero di core (coppie di CPU HT) | vCPU totale |
|---|---|---|---|
| 50 | 1000 | 3 | 6 |
| 100 | 2000 | 4 | 8 |
| 150 | 3000 | 5 | 10 |
| 200 | 4000 | 6 | 12 |
| 250 | 5000 | 6 | 12 |
| 300 | 6000 | 7 | 14 |
| 350 | 7000 | 8 | 16 |
| 400 | 8000 | 9 | 18 |

## Raccolta di informazioni sull'architettura

`lscpu`fornisce informazioni sull'architettura del sistema. L'output di base mostra quali vCPU (etichettate come «CPU») appartengono a quali nodi NUMA (e ogni nodo NUMA condivide una cache L3). Di seguito esaminiamo un'`c5.24xlarge`istanza per raccogliere le informazioni necessarie per configurare l'agente. AWS Ground Station Ciò include informazioni utili come il numero di vCPU, core e l'associazione vCPU-nodo.

```
> lscpu
Architecture: x86_64
CPU op-mode(s): 32-bit, 64-bit
Byte Order: Little Endian
CPU(s): 96
```

```
On-line CPU(s) list: 0-95
Thread(s) per core: 2             <------
Core(s) per socket: 24
Socket(s): 2
NUMA node(s): 2
Vendor ID: GenuineIntel
CPU family: 6
Model: 85
Model name: Intel(R) Xeon(R) Platinum 8275CL CPU @ 3.00GHz
Stepping: 7
CPU MHz: 3601.704
BogoMIPS: 6000.01
Hypervisor vendor: KVM
Virtualization type: full
L1d cache: 32K
L1i cache: 32K
L2 cache: 1024K
L3 cache: 36608K
NUMA node0 CPU(s): 0-23,48-71     <------
NUMA node1 CPU(s): 24-47,72-95    <------
```

I core dedicati all' AWS Ground Station agente devono includere entrambe le VCPU per ogni core assegnato. Tutti i core di un flusso di dati devono esistere sullo stesso nodo NUMA. L'`-p`opzione per il `lscpu` comando ci fornisce le associazioni tra core e CPU necessarie per configurare l'agente. I campi pertinenti sono CPU (che è ciò che chiamiamo vCPU), Core e L3 (che indica quale cache L3 è condivisa da quel core). Si noti che sulla maggior parte dei processori Intel il nodo NUMA è uguale alla cache L3.

Considerate il seguente sottoinsieme dell'`lscpu -p` output per a `c5.24xlarge` (abbreviato e formattato per maggiore chiarezza).

```
CPU,Core,Socket,Node,,L1d,L1i,L2,L3
0   0    0      0     0   0   0  0
1   1    0      0     1   1   1  0
2   2    0      0     2   2   2  0
3   3    0      0     3   3   3  0
...
16  0    0      0     0   0   0  0
17  1    0      0     1   1   1  0
18  2    0      0     2   2   2  0
```

```
19  3    0      0     3   3   3  0
```

Dall'output possiamo vedere che Core 0 include vCPU 0 e 16, Core 1 include vCPU 1 e 17, Core 2 include vCPU 2 e 18. In altre parole, le coppie hyper-threaded sono: 0 e 16, 1 e 17, 2 e 18.

## Esempio di assegnazione della CPU

Ad esempio, utilizzeremo un'`c5.24xlarge`istanza per un downlink a banda larga a doppia polarità a 350 MHz. Dalla tabella in basso Pianificazione principale della CPU sappiamo che un downlink a 350 MHz richiede 8 core (16 vCPU) per il singolo flusso di dati. Ciò significa che questa configurazione a doppia polarità che utilizza due flussi di dati richiede un totale di 16 core (32 vCPU) più un core (2 vCPU) per l'agente.

Conosciamo l'output per include e. `lscpu` `c5.24xlarge` `NUMA node0 CPU(s): 0-23,48-71` `NUMA node1 CPU(s): 24-47,72-95` Poiché NUMA node0 ha più del necessario, assegneremo solo due core: 0-23 e 48-71.

Innanzitutto, selezioneremo 8 core per ogni flusso di dati che condividono una cache L3 o un nodo NUMA. Quindi cercheremo le vCPU corrispondenti (etichettate «CPU») nell'output in. `lscpu -p` Appendice: `lscpu -p` output (completo) per c5.24xlarge Un esempio di processo di selezione principale potrebbe essere simile al seguente:

- Riserva i core 0-1 per il sistema operativo.
- Flusso 1: seleziona i core 2-9 che vengono mappati alle vCPU 2-9 e 50-57.
- Flusso 2: seleziona i core 10-17 che vengono mappati alle vCPU 10-17 e 58-65.
- Agent core: seleziona il core 18 che viene mappato alle VCPUs 18 e 66.

Ciò si traduce in vCPU 2-18 e 51-66, quindi l'elenco da fornire all'agente è. `[2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66]` È necessario assicurarsi che i propri processi non siano in esecuzione su queste CPU come descritto in. Esecuzione di servizi e processi insieme all'agente AWS Ground Station

Notate che i core specifici selezionati in questo esempio sono alquanto arbitrari. Altri set di core funzionerebbero purché soddisfino il requisito di condividere tutti una cache L3 per ogni flusso di dati.

## Appendice: **`lscpu -p`** output (completo) per c5.24xlarge

```
> lscpu -p
# The following is the parsable format, which can be fed to other
# programs. Each different item in every column has an unique ID
# starting from zero.
# CPU,Core,Socket,Node,,L1d,L1i,L2,L3
0,0,0,0,,0,0,0,0
1,1,0,0,,1,1,1,0
2,2,0,0,,2,2,2,0
3,3,0,0,,3,3,3,0
4,4,0,0,,4,4,4,0
5,5,0,0,,5,5,5,0
6,6,0,0,,6,6,6,0
7,7,0,0,,7,7,7,0
8,8,0,0,,8,8,8,0
9,9,0,0,,9,9,9,0
10,10,0,0,,10,10,10,0
11,11,0,0,,11,11,11,0
12,12,0,0,,12,12,12,0
13,13,0,0,,13,13,13,0
14,14,0,0,,14,14,14,0
15,15,0,0,,15,15,15,0
16,16,0,0,,16,16,16,0
17,17,0,0,,17,17,17,0
18,18,0,0,,18,18,18,0
19,19,0,0,,19,19,19,0
20,20,0,0,,20,20,20,0
21,21,0,0,,21,21,21,0
22,22,0,0,,22,22,22,0
23,23,0,0,,23,23,23,0
24,24,1,1,,24,24,24,1
25,25,1,1,,25,25,25,1
26,26,1,1,,26,26,26,1
27,27,1,1,,27,27,27,1
28,28,1,1,,28,28,28,1
29,29,1,1,,29,29,29,1
30,30,1,1,,30,30,30,1
31,31,1,1,,31,31,31,1
32,32,1,1,,32,32,32,1
33,33,1,1,,33,33,33,1
34,34,1,1,,34,34,34,1
```

```
35,35,1,1,,35,35,35,1
36,36,1,1,,36,36,36,1
37,37,1,1,,37,37,37,1
38,38,1,1,,38,38,38,1
39,39,1,1,,39,39,39,1
40,40,1,1,,40,40,40,1
41,41,1,1,,41,41,41,1
42,42,1,1,,42,42,42,1
43,43,1,1,,43,43,43,1
44,44,1,1,,44,44,44,1
45,45,1,1,,45,45,45,1
46,46,1,1,,46,46,46,1
47,47,1,1,,47,47,47,1
48,0,0,0,,0,0,0,0
49,1,0,0,,1,1,1,0
50,2,0,0,,2,2,2,0
51,3,0,0,,3,3,3,0
52,4,0,0,,4,4,4,0
53,5,0,0,,5,5,5,0
54,6,0,0,,6,6,6,0
55,7,0,0,,7,7,7,0
56,8,0,0,,8,8,8,0
57,9,0,0,,9,9,9,0
58,10,0,0,,10,10,10,0
59,11,0,0,,11,11,11,0
60,12,0,0,,12,12,12,0
61,13,0,0,,13,13,13,0
62,14,0,0,,14,14,14,0
63,15,0,0,,15,15,15,0
64,16,0,0,,16,16,16,0
65,17,0,0,,17,17,17,0
66,18,0,0,,18,18,18,0
67,19,0,0,,19,19,19,0
68,20,0,0,,20,20,20,0
69,21,0,0,,21,21,21,0
70,22,0,0,,22,22,22,0
71,23,0,0,,23,23,23,0
72,24,1,1,,24,24,24,1
73,25,1,1,,25,25,25,1
74,26,1,1,,26,26,26,1
75,27,1,1,,27,27,27,1
76,28,1,1,,28,28,28,1
77,29,1,1,,29,29,29,1
78,30,1,1,,30,30,30,1
```

```
79,31,1,1,,31,31,31,1
80,32,1,1,,32,32,32,1
81,33,1,1,,33,33,33,1
82,34,1,1,,34,34,34,1
83,35,1,1,,35,35,35,1
84,36,1,1,,36,36,36,1
85,37,1,1,,37,37,37,1
86,38,1,1,,38,38,38,1
87,39,1,1,,39,39,39,1
88,40,1,1,,40,40,40,1
89,41,1,1,,41,41,41,1
90,42,1,1,,42,42,42,1
91,43,1,1,,43,43,43,1
92,44,1,1,,44,44,44,1
93,45,1,1,,45,45,45,1
94,46,1,1,,46,46,46,1
95,47,1,1,,47,47,47,1
```

# Installazione dell'agente

L' AWS Ground Station agente può essere installato nei seguenti modi:

1. AWS CloudFormation modello (consigliato).
2. Installazione manuale su Amazon EC2.

## Utilizzo del modello CloudFormation

Il CloudFormation modello di distribuzione dei dati EC2 crea le risorse AWS necessarie per fornire dati alla tua istanza EC2. Questo AWS CloudFormation modello utilizza l'AMI AWS Ground Station gestita su cui è preinstallato l' AWS Ground Station agente. Lo script di avvio dell'istanza EC2 creata popola quindi il file di configurazione dell'agente e applica il necessario tuning delle prestazioni (). Ottimizzazione delle prestazioni delle istanze EC2

### Fase 1: Creare risorse AWS

Crea il tuo stack di risorse AWS utilizzando un modelloModello DigiF a banda larga satellitare per trasmissione diretta (banda larga).

### Fase 2: Verifica lo stato dell'agente

Per impostazione predefinita, l'agente è configurato e attivo (avviato). Per verificare lo stato dell'agente puoi connetterti all'istanza EC2 (SSH o SSM Session Manager) e vedere. AWS Ground Station Stato dell'agente

## Installazione manuale su EC2

Sebbene Ground Station consigli l'uso CloudFormation di modelli per il provisioning delle risorse AWS, potrebbero esserci casi d'uso in cui il modello standard potrebbe non essere sufficiente. In questi casi, ti consigliamo di personalizzare il modello in base alle tue esigenze. Se ciò non soddisfa ancora i tuoi requisiti, puoi creare manualmente le tue risorse AWS e installare l'agente.

### Fase 1: Creare risorse AWS

Consulta le istruzioni Creazione e configurazione manuale delle risorse per configurare manualmente le risorse AWS necessarie per un contatto.

La AwsGroundStationAgentEndpointrisorsa definisce un endpoint per la ricezione di un flusso di dati DigiF AWS Ground Station tramite Agent ed è fondamentale per stabilire un contatto di successo. Sebbene la documentazione dell'API sia disponibile nell'API Reference, questa sezione discuterà brevemente i concetti relativi all'agente. AWS Ground Station

L'endpoint `ingressAddress` è il luogo in cui l' AWS Ground Station agente riceverà il traffico UDP AWS KMS crittografato dall'antenna. `socketAddressname`È l'IP pubblico dell'istanza EC2 (dall'EIP allegato). `portRange`Dovrebbero esserci almeno 300 porte contigue in un intervallo riservato a qualsiasi altro utilizzo. Per istruzioni, consulta Reserve Ingress Ports - Impacts Network. Queste porte devono essere configurate per consentire il traffico di ingresso UDP sul gruppo di sicurezza per il VPC in cui è in esecuzione l'istanza del ricevitore.

L'endpoint `egressAddress` è il luogo in cui l'agente consegnerà il flusso di dati DigiF al cliente. Il cliente deve disporre di un'applicazione (ad esempio SDR) che riceve i dati tramite un socket UDP in questa posizione.

### Fase 2: Creare un'istanza EC2

Sono supportate le seguenti AMI:

1. AWS Ground Station L'AMI, `groundstation-al2-gs-agent-ami-*` dove* è la data di creazione dell'AMI, viene fornita con l'agente installato (consigliato).

2. `amzn2-ami-kernel-5.10-hvm-x86_64-gp2`.

## Passaggio 3: scarica e installa l'agente

> **Note**
>
> I passaggi di questa sezione devono essere completati se non hai scelto l' AWS Ground Station Agent AMI nel passaggio precedente.

Scarica l'agente

L' AWS Ground Station agente è disponibile da bucket S3 specifici della regione e può essere scaricato su istanze EC2 supportate utilizzando la riga di comando AWS (CLI) da `s3://groundstation-wb-digif-software-${AWS::Region}/aws-groundstation-agent/latest/amazon_linux_2_x86_64/aws-groundstation-agent.rpm` cui $ {AWS::Region} si riferisce a una delle regioni di distribuzione dati e console AWS Ground Station supportate.

Esempio: scarica l'ultima versione rpm dalla regione AWS us-east-2 localmente nella cartella /tmp.

```
aws s3 --region us-east-2 cp s3://groundstation-wb-digif-software-us-east-2/aws-groundstation-agent/latest/amazon_linux_2_x86_64/aws-groundstation-agent.rpm /tmp
```

Se devi scaricare una versione specifica dell' AWS Ground Station agente, puoi scaricarla dalla cartella specifica della versione nel bucket S3.

Esempio: scarica la versione 1.0.2716.0 del file rpm dalla regione AWS us-east-2 localmente nella cartella /tmp.

```
aws s3 --region us-east-2 cp s3://groundstation-wb-digif-software-us-east-2/aws-groundstation-agent/1.0.2716.0/amazon_linux_2_x86_64/aws-groundstation-agent.rpm /tmp
```

> **Note**
>
> Se vuoi confermare che l'RPM che hai scaricato è stato fornito da, segui le istruzioni per. AWS Ground StationConvalida dell'installazione RPM

Installa l'agente

```
sudo yum install ${MY_RPM_FILE_PATH}

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

### Fase 4: Configurare l'agente

Dopo aver installato l'agente, è necessario aggiornare il file di configurazione dell'agente. Per informazioni, consulta Configurazione dell'agente.

### Fase 5: Applicare l'ottimizzazione delle prestazioni

AWS Ground Station Agent AMI: se hai scelto l' AWS Ground Station Agent AMI nel passaggio precedente, applica le seguenti ottimizzazioni delle prestazioni.

- Ottimizza le interruzioni hardware e le code di ricezione: influisce sulla CPU e sulla rete
- Reserve Ingress Ports - Impacts Network
- Riavvio

Altre AMI: se hai scelto un'altra AMI nel passaggio precedente, applica tutte le ottimizzazioni elencate sotto Ottimizzazione delle prestazioni delle istanze EC2 e riavvia l'istanza.

### Fase 6: Gestire l'agente

Per avviare, arrestare e controllare lo stato dell'agente, consultaGestire l'agente.

# Gestire l'agente

AWS Ground Station L'agente offre le seguenti funzionalità per la configurazione, l'avvio, l'arresto, l'aggiornamento, il downgrade e la disinstallazione dell'agente utilizzando gli strumenti di comando Linux integrati.

Argomenti



## AWS Ground Station Configurazione dell'agente

Vai a`/opt/aws/groundstation/etc`, che dovrebbe contenere un singolo file denominato aws-gs-agent-config .json. Per informazioni, consultare File di configurazione dell'agente.

## AWS Ground Station Agent Start

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

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

Dovrebbe produrre un output che mostri che l'agente è attivo.

```
aws-groundstation-agent.service - aws-groundstation-agent
```

```
Loaded: loaded (/usr/lib/systemd/system/aws-groundstation-agent.service; enabled;
 vendor preset: disabled)
Active: active (running) since Tue 2023-03-14 00:39:08 UTC; 1 day 13h ago
Docs: https://aws.amazon.com/ground-station/
Main PID: 8811 (aws-gs-agent)
CGroup: /system.slice/aws-groundstation-agent.service
##8811 /opt/aws/groundstation/bin/aws-gs-agent production
```

## AWS Ground Station Agente Stop

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

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

Dovrebbe produrre un output che mostri che l'agente è inattivo (fermato).

```
aws-groundstation-agent.service - aws-groundstation-agent
Loaded: loaded (/usr/lib/systemd/system/aws-groundstation-agent.service; enabled;
 vendor preset: disabled)
Active: inactive (dead) since Thu 2023-03-09 15:35:08 UTC; 6min ago
Docs: https://aws.amazon.com/ground-station/
Process: 84182 ExecStart=/opt/aws/groundstation/bin/launch-aws-gs-agent (code=exited,
 status=0/SUCCESS)
Main PID: 84182 (code=exited, status=0/SUCCESS)
```

## AWS Ground Station Aggiornamento dell'agente

1. Scarica la versione più recente dell'agente. Per informazioni, consulta Scarica l'agente.
2. Arresta l'agente di .

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

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

3. Aggiorna l'agente.

```
sudo yum update ${MY_RPM_FILE_PATH}

# check the new version has been installed correctly by comparing the agent version
 with the starting agent version
yum info aws-groundstation-agent

# reload the systemd configuration
sudo systemctl daemon-reload

# restart the agent
sudo systemctl restart aws-groundstation-agent

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

## AWS Ground Station Agent Downgrade

1. Scarica la versione per agenti di cui hai bisogno. Per informazioni, consulta Scarica l'agente.
2. Effettua il downgrade dell'agente.

```
# get the starting agent version
yum info aws-groundstation-agent

# stop the agent service
sudo systemctl stop aws-groundstation-agent

# downgrade the rpm
sudo yum downgrade ${MY_RPM_FILE_PATH}

# check the new version has been installed correctly by comparing the agent version
 with the starting agent version
yum info aws-groundstation-agent
```

```
# reload the systemd configuration
sudo systemctl daemon-reload

# restart the agent
sudo systemctl restart aws-groundstation-agent

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

## AWS Ground Station Disinstallazione dell'agente

La disinstallazione dell'agente rinominerà /opt/aws/groundstation/etc/ .json in aws-gs-agent-config / opt/aws/groundstation/etc/ .json.rpmsave. aws-gs-agent-config La reinstallazione dell'agente sulla stessa istanza scriverà i valori predefiniti per aws-gs-agent-config .json e dovrà essere aggiornato con i valori corretti corrispondenti alle risorse AWS. Per informazioni, consulta File di configurazione dell'agente.

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

## AWS Ground Station Stato dell'agente

Lo stato dell'agente è attivo (l'agente è in esecuzione) o inattivo (l'agente è fermo).

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

Un esempio di output mostra che l'agente è installato, inattivo (interrotto) e abilitato (avvia il servizio all'avvio).

```
aws-groundstation-agent.service - aws-groundstation-agent
Loaded: loaded (/usr/lib/systemd/system/aws-groundstation-agent.service; enabled;
 vendor preset: disabled)
Active: inactive (dead) since Thu 2023-03-09 15:35:08 UTC; 6min ago
```

```
Docs: https://aws.amazon.com/ground-station/
Process: 84182 ExecStart=/opt/aws/groundstation/bin/launch-aws-gs-agent (code=exited,
 status=0/SUCCESS)
Main PID: 84182 (code=exited, status=0/SUCCESS)
```

## AWS Ground Station Informazioni sull'RPM dell'agente

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

L'output è il seguente:

> **Note**
>
> La «versione» potrebbe essere diversa in base all'ultima versione pubblicata dall'agente.

```
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
Installed Packages
Name        : aws-groundstation-agent
Arch        : x86_64
Version     : 1.0.2677.0
Release     : 1
Size        : 51 M
Repo        : installed
Summary     : Client software for AWS Ground Station
URL         : https://aws.amazon.com/ground-station/
License     : Proprietary
Description : This package provides client applications for use with AWS Ground Station
```

# Configurazione dell'agente

Dopo aver installato l'agente, è necessario aggiornare il file di configurazione dell'agente all'indirizzo/opt/aws/groundstation/etc/aws-gs-agent-config.json.

# File di configurazione dell'agente

## Esempio

```
{
  "capabilities": [
    "arn:aws:groundstation:eu-central-1:123456789012:dataflow-endpoint-group/
bb6c19ea-1517-47d3-99fa-3760f078f100"
  ],
  "device": {
  "privateIps": [
    "127.0.0.1"
  ],
  "publicIps": [
    "1.2.3.4"
  ],
  "agentCpuCores":
 [ 24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,72,73,74,75,76,77,78,79,80,81
}
```

## Suddivisione del campo

capacità

Le funzionalità sono specificate come Dataflow Endpoint Group Amazon Resource Names.

Obbligatorio: True

Formato: String Array

- Valori: ability ARNs → String

Esempi:

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

dispositivo

Questo campo contiene campi aggiuntivi necessari per enumerare il «dispositivo» EC2 corrente.

Obbligatorio: True

Formato: oggetto

Membri:

- IP privati
- IP pubblici
- agentCpuCores
- Adattatori di rete

IP privati

Questo campo non è attualmente utilizzato, ma è incluso per casi d'uso futuri. Se non è incluso alcun valore, il valore predefinito è [«127.0.0.1»]

Obbligatorio: falso

Formato: String Array

- Valori: Indirizzi IP → Stringa

Esempio:

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

IP pubblici

IP elastico (EIP) per gruppo di endpoint di flussi di dati.

Obbligatorio: True

Formato: String Array

- Valori: Indirizzi IP → Stringa

Esempio:

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

AgentCPU Cores

Questo specifica quali core virtuali sono riservati al processo. aws-gs-agent Vedi i requisiti Pianificazione principale della CPU per impostare questo valore in modo appropriato.

Obbligatorio: True

Formato: Int Array

- Valori: Core Numbers → int

Esempio:

```
"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
]
```

Adattatori di rete

Corrisponde agli adattatori Ethernet, o alle interfacce collegate agli ENI, che riceveranno i dati.

Obbligatorio: falso

Formato: String Array

- Valori: nomi degli adattatori Ethernet (è possibile trovarli eseguendo`ifconfig`)

Esempio:

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

# Ottimizzazione delle prestazioni delle istanze EC2

> **Note**
>
> Se hai effettuato il provisioning delle risorse AWS utilizzando CloudFormation modelli, queste ottimizzazioni vengono applicate automaticamente. Se hai utilizzato un'AMI o hai creato manualmente l'istanza EC2, questi aggiustamenti delle prestazioni devono essere applicati per ottenere le prestazioni più affidabili.

Ricordati di riavviare l'istanza dopo aver applicato qualsiasi ottimizzazione.

Argomenti



## Ottimizza le interruzioni hardware e le code di ricezione: influisce sulla CPU e sulla rete

Questa sezione configura l'utilizzo dei core della CPU di systemd, SMP IRQ, Receive Packet Steering (RPS) e Receive Flow Steering (RFS). Vedi una serie Appendice: Parametri consigliati per Interrupt/RPS Tune di impostazioni consigliate in base al tipo di istanza che stai utilizzando.

1. Allontana i processi systemd dai core della CPU dell'agente.
2. Indirizza le richieste di interruzione hardware lontano dai core della CPU dell'agente.
3. Configura RPS per evitare che la coda hardware di una singola scheda di interfaccia di rete diventi un collo di bottiglia nel traffico di rete.
4. Configura RFS per aumentare la frequenza di accesso alla cache della CPU e quindi ridurre la latenza di rete.

Lo `set_irq_affinity.sh` script fornito dall'RPM configura tutto quanto sopra per te. Aggiungilo a crontab in modo che venga applicato ad ogni avvio:

```
echo "@reboot sudo /opt/aws/groundstation/bin/set_irq_affinity.sh
 '${interrupt_core_list}' '${rps_core_mask}' >> /var/log/user-data.log 2>&1" >>/var/
spool/cron/root
```

- Sostituiscilo `interrupt_core_list` con core riservati al kernel e al sistema operativo, in genere il primo e il secondo insieme a coppie di core hyperthreaded. Questo non dovrebbe sovrapporsi ai core selezionati sopra. (Es: '0,1,48,49' per un'istanza Hyper-Thread da 96 CPU).
- `rps_core_mask`è una maschera di bit esadecimale che specifica quali CPU devono elaborare i pacchetti in entrata, con ogni cifra che rappresenta 4 CPU. Deve inoltre essere separato da virgole ogni 8 caratteri a partire da destra. Si consiglia di abilitare tutte le CPU e lasciare che la cache gestisca il bilanciamento.
  - Per visualizzare l'elenco dei parametri consigliati per ogni tipo di istanza, fare riferimento a. Appendice: Parametri consigliati per Interrupt/RPS Tune
- Esempio di istanza da 96 CPU:

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

## Tune Rx Interrupt Coalescing - Impacts Network

La coalescenza delle interruzioni aiuta a prevenire l'inondazione del sistema host con troppe interruzioni e aiuta ad aumentare la velocità di trasmissione della rete. Con questa configurazione, i

pacchetti vengono raccolti e viene generata una singola interruzione ogni 128 microsecondi. Aggiungi a crontab in modo che venga applicato ad ogni avvio:

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

- Sostituisci `interface` con l'interfaccia di rete (adattatore ethernet) configurata per ricevere dati. In genere si `eth0` tratta dell'interfaccia di rete predefinita assegnata a un'istanza EC2.

## Tune Rx Ring Buffer - Impacts Network

Aumenta il numero di ingressi ad anello per il ring buffer Rx per evitare cadute o sovraccarichi di pacchetti durante le connessioni interrotte. Aggiungi al crontab in modo che sia impostato correttamente su ogni avvio:

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

- Sostituisci `interface` con l'interfaccia di rete (adattatore ethernet) configurata per ricevere dati. In genere si `eth0` tratta dell'interfaccia di rete predefinita assegnata a un'istanza EC2.
- Se si configura un'istanza c6i.32xlarge, il comando deve essere modificato per impostare il ring buffer su, anziché. `8192` `16384`

## Tune CPU C-State - Impatta la CPU

Imposta lo stato C della CPU per evitare l'inattività, che può causare la perdita di pacchetti durante l'avvio di un contatto. Richiede il riavvio dell'istanza.

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

## Reserve Ingress Ports - Impacts Network

Riservate tutte le porte nell'intervallo `AwsGroundStationAgentEndpoint` di porte degli indirizzi di ingresso per evitare conflitti con l'utilizzo del kernel. Il conflitto di utilizzo delle porte porterà a problemi di contatto e di consegna dei dati.

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

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

## Riavvio

Dopo che tutte le regolazioni sono state applicate correttamente, riavvia l'istanza per rendere effettive le ottimizzazioni.

```
sudo reboot
```

## Appendice: Parametri consigliati per Interrupt/RPS Tune

Questa sezione determina i valori dei parametri consigliati da utilizzare nella sezione di ottimizzazione Tune Hardware Interrupts and Receive Queues - Impacts CPU and Network.

| Family | Tipo di istanza | $ {interrupt_core_list} | $ {rps_core_mask} |
|---|---|---|---|
| c6i | • c6i.32xlarge | • 0,1,64,65 | • ffffffff, ffffffff, ffffffff, ffffffff |

| Family | Tipo di istanza | $ {interrupt_core_list} | $ {rps_core_mask} |
|---|---|---|---|
| c5 | • c5.24xlarge<br>• c5.18xlarge<br>• c5.12xlarge | • 0,1,48,49<br>• 0,1,36,37<br>• 0,1,24,25 | • ffffffff, ffffffff, ffffffff<br>• ff, ffffffff, ffffffff<br>• ffff, ffffffff |
| c5n | • c5n.metal<br>• c5n.18xlarge | • 0,1,36,37<br>• 0,1,36,37 | • ff, ffffffff, ffffffff<br>• ff, ffffffff, ffffffff |
| m5 | • m5.24xlarge<br>• m5.12xlarge | • 0,1,48,49<br>• 0,1,24,25 | • ffffffff, ffffffff, ffffffff<br>• ffff, ffffffff |
| r5 | • r5.metal<br>• r5.24xlarge | • 0,1,48,49<br>• 0,1,48,49 | • ffffffff, ffffffff, ffffffff<br>• ffffffff, ffffffff, ffffffff |
| r5n | • r5n.metal<br>• r5n.24xlarge | • 0,1,48,49<br>• 0,1,48,49 | • ffffffff, ffffffff, ffffffff<br>• ffffffff, ffffffff, ffffffff |

| Family | Tipo di istanza | ${interrupt_core_list} | ${rps_core_mask} |
|---|---|---|---|
| g4dn | • g4dn.metal<br>• g4dn.16xlarge<br>• g4dn.12xlarge | • 0,1,48,49<br>• 0,1,32,33<br>• 0,1,24,25 | • ffffffff, ffffffff, ffffffff<br>• ffffffff, ffffffff<br>• ffff, ffffffff |
| p4d | • p4d.24xlarge | • 0,1,48,49 | • ffffffff, ffffffff, ffffffff |
| p3dn | • p3dn.24xlarge | • 0,1,48,49 | • ffffffff, ffffffff, ffffffff |

# Preparati a prendere un contatto DigiF

1. Esamina CPU Core Planning per i flussi di dati desiderati e fornisci un elenco di core che l'agente può utilizzare. Per informazioni, consulta Pianificazione principale della CPU.
2. Esamina il file di configurazione dell' AWS Ground Station agente. Per informazioni, consulta AWS Ground Station Configurazione dell'agente.
3. Verificare che sia stata applicata la necessaria ottimizzazione delle prestazioni. Per informazioni, consulta Ottimizzazione delle prestazioni delle istanze EC2.
4. Conferma di seguire tutte le best practice indicate. Per informazioni, consulta Best practice.
5. Conferma che l' AWS Ground Station agente sia stato avviato prima dell'orario di inizio del contatto pianificato tramite:

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

6. Verifica che l' AWS Ground Station agente sia in buone condizioni prima dell'orario di inizio del contatto pianificato tramite:

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

Verifica che il `agentStatus` tuo `awsGroundStationAgentEndpoint` sia ATTIVO e che `auditResults` sia SANO.

# Best practice

## Le migliori pratiche EC2

Segui le attuali best practice di EC2 e assicurati una sufficiente disponibilità di archiviazione dei dati.

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

## Pianificatore Linux

Lo scheduler Linux può riordinare i pacchetti su socket UDP se i processi corrispondenti non sono collegati a un core specifico. Qualsiasi thread che invia o riceve dati UDP deve collegarsi a un core specifico per tutta la durata della trasmissione dei dati.

## AWS Ground Station Elenco di prefissi gestiti

Si consiglia di utilizzare l'elenco di prefissi `com.amazonaws.global.groundstation` gestito da AWS quando si specificano le regole di rete per consentire la comunicazione dall'antenna. Consulta Working with AWS Managed Prefix Lists per ulteriori informazioni su AWS Managed Prefix Lists.

## Limitazione del contatto singolo

AWS Ground Station Agent supporta più flussi per contatto, ma supporta solo un contatto alla volta. Per evitare problemi di pianificazione, non condividere un'istanza tra più gruppi di endpoint di flussi di dati. Se una configurazione a singolo agente è associata a più ARN DFEG diversi, non riuscirà a registrarsi.

## Esecuzione di servizi e processi insieme all'agente AWS Ground Station

Quando si avviano servizi e processi sulla stessa istanza EC2 dell' AWS Ground Station agente, è importante collegarli a vCPU non utilizzate dall' AWS Ground Station agente e dal kernel Linux,

poiché ciò può causare colli di bottiglia e persino la perdita di dati durante i contatti. Questo concetto di associazione a vCPU specifiche è noto come affinità.

Core da evitare:

- `agentCpuCores`da File di configurazione dell'agente
- `interrupt_core_list` da Ottimizza le interruzioni hardware e le code di ricezione: influisce sulla CPU e sulla rete.
  - I valori predefiniti possono essere trovati da Appendice: Parametri consigliati per Interrupt/RPS Tune

### Ad esempio, utilizzando un'**`c5.24xlarge`**istanza

Se hai specificato

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

e sono scappato

```
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
```

quindi evita i seguenti core:

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

### Servizi di affinitizzazione (systemd)

I servizi appena lanciati verranno automaticamente affinitizzati a quelli menzionati in precedenza. `interrupt_core_list` Se il caso d'uso dei servizi lanciati richiede core aggiuntivi o richiede core meno congestionati, segui questa sezione.

Controlla a quale affinità è attualmente configurato il tuo servizio con il comando:

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

Se vedi un valore vuoto come`CPUAffinity=`, significa che probabilmente utilizzerà i core predefiniti del comando precedente `...bin/set_irq_affinity.sh <using the cores here> ...`

Per sovrascrivere e impostare un'affinità specifica, trova la posizione del file di servizio eseguendo:

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

Apri e modifica il file (usando `vinano`, ecc.) e inseriscilo `CPUAffinity=<core list>` nella `[Service]` sezione come segue:

```
[Unit]
...

[Service]
...
CPUAffinity=2,3

[Install]
...
```

Salva il file e riavvia il servizio per applicare l'affinità con:

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

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

Per maggiori informazioni visita: Red Hat Enterprise Linux 8 - Gestione, monitoraggio e aggiornamento del kernel - Capitolo 27. Configurazione delle politiche CPU Affinity e NUMA utilizzando systemd.

## Affinitizzazione dei processi (script)

Si consiglia vivamente di affinitizzare manualmente gli script e i processi appena lanciati, poiché il comportamento predefinito di Linux consentirà loro di utilizzare qualsiasi core sulla macchina.

Per evitare conflitti di base per qualsiasi processo in esecuzione (come python, script bash, ecc.), avvia il processo con:

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

Se il processo è già in esecuzione, usa comandi come `pidoftop`, o `ps` per trovare l'ID di processo (PID) del processo specifico. Con il PID puoi vedere l'attuale affinità con:

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

e puoi modificarlo con:

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

Per ulteriori informazioni su taskset, vedere taskset - Linux man page

# Risoluzione dei problemi

## L'agente non riesce ad avviarsi

L' AWS Ground Station agente potrebbe non avviarsi per diversi motivi, ma lo scenario più comune potrebbe essere un file di configurazione dell'agente configurato in modo errato. Dopo aver avviato l'agente (vediAWS Ground Station Agent Start) potresti ottenere uno stato come:

```
#agent is automatically retrying a restart
aws-groundstation-agent.service - aws-groundstation-agent
Loaded: loaded (/usr/lib/systemd/system/aws-groundstation-agent.service; enabled;
 vendor preset: disabled)
Active: activating (auto-restart) (Result: exit-code) since Fri 2023-03-10 01:48:14
 UTC; 23s ago
Docs: https://aws.amazon.com/ground-station/
Process: 43038 ExecStart=/opt/aws/groundstation/bin/launch-aws-gs-agent (code=exited,
 status=101)
Main PID: 43038 (code=exited, status=101)
```

```
#agent has failed to start
aws-groundstation-agent.service - aws-groundstation-agent
Loaded: loaded (/usr/lib/systemd/system/aws-groundstation-agent.service; enabled;
 vendor preset: disabled)
Active: failed (Result: start-limit) since Fri 2023-03-10 01:50:15 UTC; 13s ago
Docs: https://aws.amazon.com/ground-station/
Process: 43095 ExecStart=/opt/aws/groundstation/bin/launch-aws-gs-agent (code=exited,
 status=101)
Main PID: 43095 (code=exited, status=101)
```

### Risoluzione dei problemi

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

potrebbe risultare in un output di:

```
launch-aws-gs-agent[43095]: Running with options Production(ProductionOptions
 { endpoint: None, region: None })
launch-aws-gs-agent[43095]: Loading Config
launch-aws-gs-agent[43095]: System has 96 logical cores
systemd[1]: aws-groundstation-agent.service: main process exited, code=exited,
 status=101/n/a
systemd[1]: Unit aws-groundstation-agent.service entered failed state.
```

Il mancato avvio dell'agente dopo «Loading Config» indica un problema con la configurazione dell'agente. Vedi File di configurazione dell'agente per verificare la configurazione dell'agente.

## AWS Ground Station Registri degli agenti

AWS Ground Station L'agente scrive informazioni sull'esecuzione dei contatti, sugli errori e sullo stato di integrità nei file di registro sull'istanza su cui è in esecuzione l'agente. È possibile visualizzare i file di registro connettendosi manualmente a un'istanza.

È possibile visualizzare i log degli agenti nella seguente posizione.

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

## Nessun contatto disponibile

La pianificazione dei contatti richiede un AWS Ground Station agente in buona salute. Conferma che il tuo AWS Ground Station agente sia stato avviato e che sia integro interrogando l' AWS Ground Station API tramite: get-dataflow-endpoint-group

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

Verifica che il `agentStatus` tuo `awsGroundStationAgentEndpoint` sia ATTIVO e che `auditResults` sia SANO.

# Ottenere supporto

Contatta il team di Ground Station tramite AWS Support.

1. Fornisci tutti `contact_id` i contatti interessati. Il AWS Ground Station team non può indagare su un contatto specifico senza queste informazioni.
2. Fornisci dettagli su tutte le procedure di risoluzione dei problemi già intraprese.
3. Fornisci eventuali messaggi di errore rilevati durante l'esecuzione dei comandi nella nostra guida alla risoluzione dei problemi.

# Note di rilascio dell'agente

## Versione più recente dell'agente

### Versione 1.0.3555.0

Data di rilascio: 27/03/2024

Data di fine del supporto: 31/08/2024

Checksum RPM:

- SHA 256: `108f3aceb00e5af549839cd766c56149397e448a6e1e1429c89a9eebb6bc0fc1`
- MD5: `65b72fa507fb0af32651adbb18d2e30f`

Modifiche:

- Aggiungi la metrica dell'agente per la versione eseguibile selezionata durante l'avvio del task.
- Aggiungi il supporto per i file di configurazione per evitare versioni eseguibili specifiche quando sono disponibili altre versioni.
- Aggiungi la diagnostica di rete e di routing.
- Funzionalità di sicurezza aggiuntive.
- Risolto il problema per cui alcuni errori di segnalazione delle metriche venivano scritti su stdout/journal anziché sul file di registro.
- Gestisci con garbo gli errori di socket irraggiungibili dalla rete.
- Misura la perdita di pacchetti e la latenza tra gli agenti di origine e di destinazione.
- Rilascia la aws-gs-datapipe versione 2.0 per supportare nuove funzionalità del protocollo e la possibilità di aggiornare in modo trasparente i contatti al nuovo protocollo.

## Versioni obsolete degli agenti

### Versione 1.0.2942.0

Data di rilascio: 26/06/2023

Data di fine del supporto: 31/05/2024

Checksum RPM:

- SHA 256: `7d94b642577504308a58bab28f938507f2591d4e1b2c7ea170b77bea97b5a9b6`
- MD5: `661ff2b8f11aba5d657a6586b56e0d8f`

Modifiche:

- Sono stati aggiunti i log degli errori relativi all'aggiornamento di Agent RPM su disco e per rendere effettive le modifiche è necessario il riavvio dell'agente.

- È stata aggiunta la convalida dell'ottimizzazione della rete per garantire che le fasi di ottimizzazione della guida per l'utente di Agent siano seguite e applicate correttamente.
- Risolto il bug che causava avvisi errati nei log di Agent sull'archiviazione dei log.
- Rilevamento migliorato della perdita di pacchetti.
- Installazione aggiornata dell'agente per impedire l'installazione o l'aggiornamento dell'RPM se l'agente è già in esecuzione.

## Versione 1.0.2716.0

Data di rilascio: 15/03/2023

Data di fine del supporto: 31/05/2024

Checksum RPM:

- SHA 256: `cb05b6a77dfcd5c66d81c0072ac550affbcefefc372cc5562ee52fb220844929`
- MD5: `65266490c4013b433ec39ee50008116c`

Modifiche:

- Abilita il caricamento dei log quando l'agente riscontra errori durante l'esecuzione delle attività.
- Risolve il bug di compatibilità con Linux negli script di ottimizzazione della rete forniti.

## Versione 1.0.2677.0

Data di rilascio: 15/02/2023

Data di fine del supporto: 31/05/2024

Checksum RPM:

- SHA 256: `77cfe94acb00af7ca637264b17c9b21bd7afdc85b99dffdd627aec9e99397489`
- MD5: `b8533be7644bb4d12ab84de21341adac`

Modifiche:

- Prima versione di Agent disponibile a livello generale.

# Convalida dell'installazione RPM

Di seguito sono riportati l'ultima versione RPM, l'hash MD5 convalidato da RPM e l'hash SHA256 utilizzando sha256sum. Questi valori, combinati, possono essere utilizzati per convalidare la versione RPM utilizzata per l'agente della stazione di terra.

## Versione più recente dell'agente

### Versione 1.0.3555.0

Data di rilascio: 27/03/2024

Data di fine del supporto: 31/08/2024

Checksum RPM:

- SHA 256: `108f3aceb00e5af549839cd766c56149397e448a6e1e1429c89a9eebb6bc0fc1`
- MD5: `65b72fa507fb0af32651adbb18d2e30f`

Modifiche:

- Aggiungi la metrica dell'agente per la versione eseguibile selezionata durante l'avvio del task.
- Aggiungi il supporto per i file di configurazione per evitare versioni eseguibili specifiche quando sono disponibili altre versioni.
- Aggiungi la diagnostica di rete e di routing.
- Funzionalità di sicurezza aggiuntive.
- Risolto il problema per cui alcuni errori di segnalazione delle metriche venivano scritti su stdout/journal anziché sul file di registro.
- Gestisci con garbo gli errori di socket irraggiungibili dalla rete.
- Misura la perdita di pacchetti e la latenza tra gli agenti di origine e di destinazione.
- Rilascia la aws-gs-datapipe versione 2.0 per supportare nuove funzionalità del protocollo e la possibilità di aggiornare in modo trasparente i contatti al nuovo protocollo.

## Verifica l'RPM

Gli strumenti necessari per verificare questa installazione RPM sono:

- sha256 sum
- giri/min

Entrambi gli strumenti sono disponibili di default su Amazon Linux 2. Questi strumenti ti aiuteranno a verificare che l'RPM che stai utilizzando sia la versione corretta. Per prima cosa scaricate l'RPM più recente dal bucket S3 (Scarica l'agenteper istruzioni su come scaricare l'RPM, consultate la sezione RPM). Una volta scaricato questo file, ci saranno alcune cose da controllare:

- Calcola la somma sha256sum del file RPM. Esegui la seguente azione dalla riga di comando dell'istanza di calcolo che stai utilizzando:

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

  Prendi questo valore e confrontalo con la tabella precedente. Ciò dimostra che il file RPM scaricato è un file valido da utilizzare che AWS Ground Station ha distribuito ai clienti. Se gli hash non corrispondono, non installare l'RPM ed eliminalo dall'istanza di calcolo.
- Controllate anche l'hash MD5 del file, per assicurarvi che l'RPM non sia stato compromesso. A tale scopo, utilizzate lo strumento da riga di comando RPM eseguendo il seguente comando:

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

  Verificate che l'hash MD5 elencato qui sia lo stesso dell'hash MD5 della versione riportata nella tabella precedente. Una volta che entrambi questi hash sono stati convalidati rispetto a questa tabella elencata in AWS Docs, il cliente può essere certo che l'RPM scaricato e installato sia la versione sicura e senza compromessi dell'RPM.

# Creazione di un elenco di contatti e prenotazione

Puoi inserire i dati satellitari, identificare le posizioni delle antenne, comunicare e pianificare il tempo di utilizzo delle antenne per i satelliti selezionati. utilizzando la console AWS Ground Station o l' AWS CLI. Puoi rivedere, annullare e pianificare nuovamente le prenotazioni di contatto fino a 8 giorni prima della scadenza pianificata. 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 del recapito dei dati tra regioni, vedere Utilizzo del servizio di recapito dei dati tra regioni.

Per pianificare i contatti, è necessario configurare le risorse. Se non sono state configurate le risorse, consulta Guida introduttiva.

Argomenti

- Utilizzo della console Ground Station
- Prenotazione e gestione dei contatti con AWS CLI

## Utilizzo della console Ground Station

Puoi utilizzare la AWS Ground Station console per prenotare, visualizzare e annullare le prenotazioni di contatto. Per utilizzare la AWS Ground Station console, apri la AWS Ground Station console e scegli Prenota subito i contatti.


Utilizza i seguenti argomenti per utilizzare la AWS Ground Station console per prenotare, visualizzare e annullare i contatti.

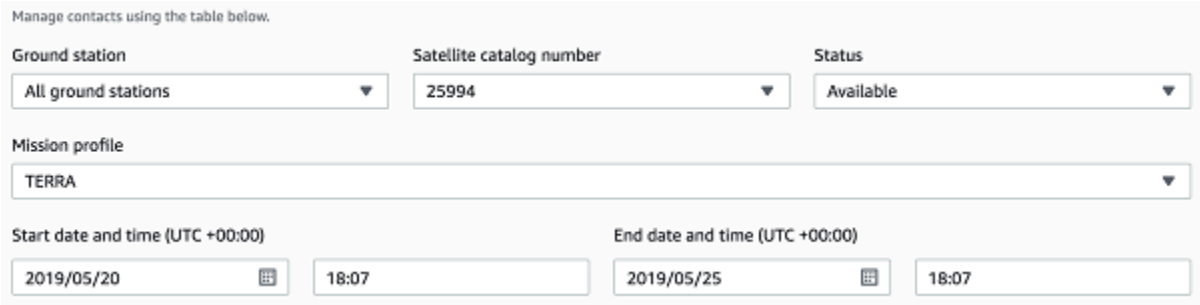
Argomenti



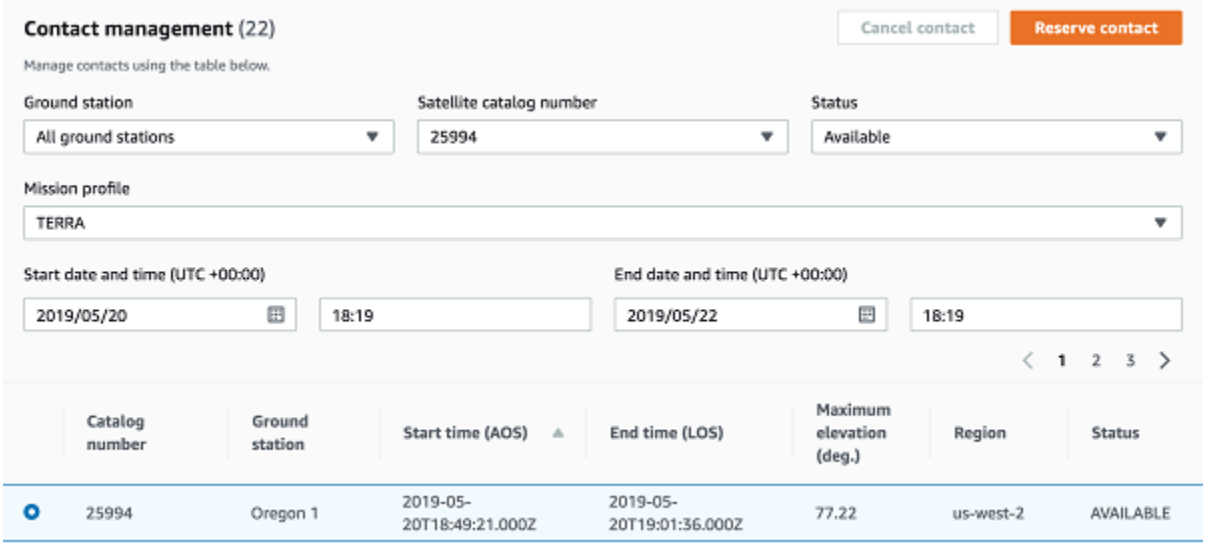
## Prenotare un contatto

Dopo aver effettuato l'accesso alla AWS Ground Station console, utilizza le risorse configurate per prenotare i contatti nella tabella di gestione dei contatti.

1. Nella tabella Contact management (Gestione contatti) scegliere i parametri che si desidera utilizzare per cercare i contatti disponibili. Verificare di visualizzare i contatti disponibili utilizzando il filtro Stato.



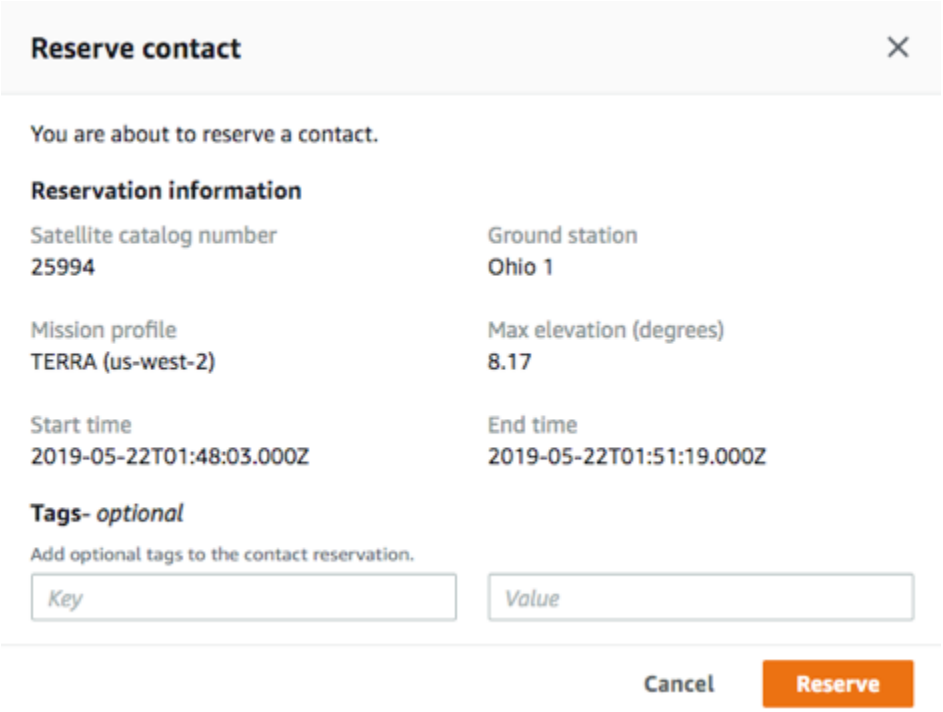

2. Selezionare un contatto che soddisfi i requisiti, quindi scegliere Reserve Contact (Prenota contatto).




3. Nella finestra di dialogo Riserva contatto esaminare le informazioni di prenotazione dei contatti.

   a. (facoltativo) In Tag, immettere una chiave e un valore per ogni tag che si desidera aggiungere.

   b. Scegliere Riserva.

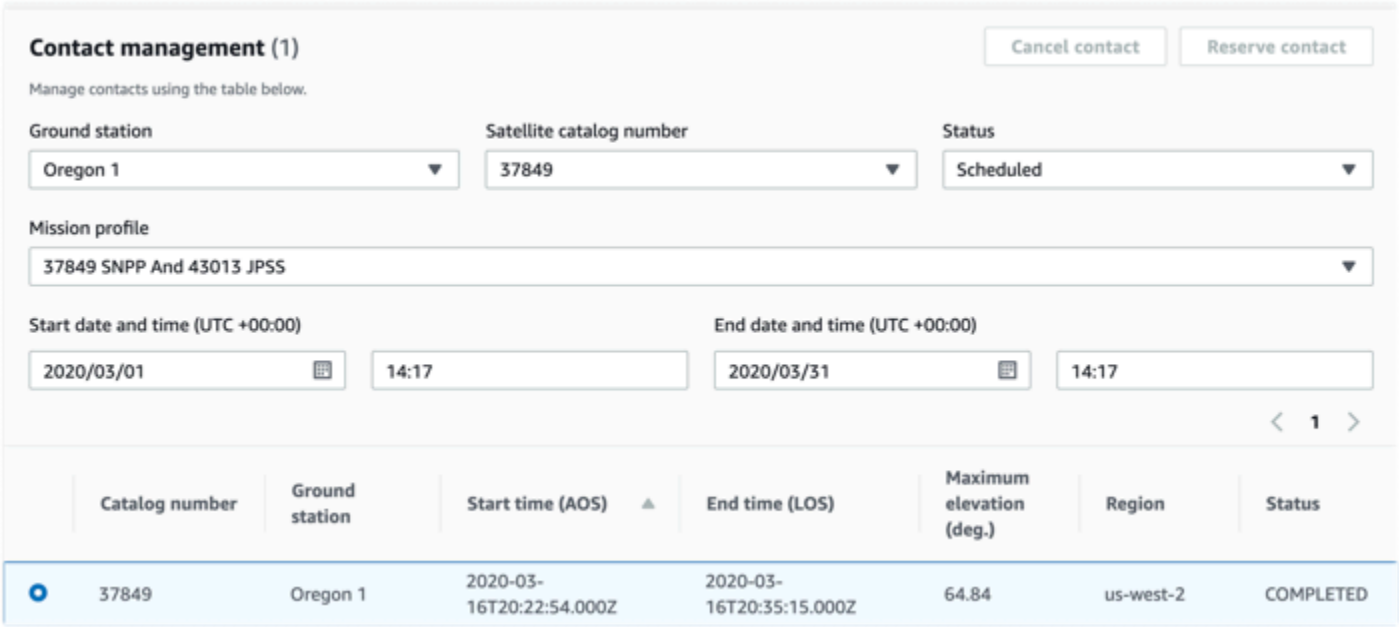


AWS Ground Station utilizzerà i dati di configurazione del tuo profilo di missione per eseguire un contatto presso la stazione di terra specificata.

## Visualizzare i contatti pianificati e completati

Una volta pianificati i contatti, è possibile utilizzare la AWS Ground Station console per visualizzare i dettagli dei contatti pianificati e completati.

Nella tabella Gestione contatti scegliere i parametri che si desidera utilizzare per cercare i contatti pianificati e completati. Assicurarsi di visualizzare i contatti pianificati o completati utilizzando il filtro Stato.

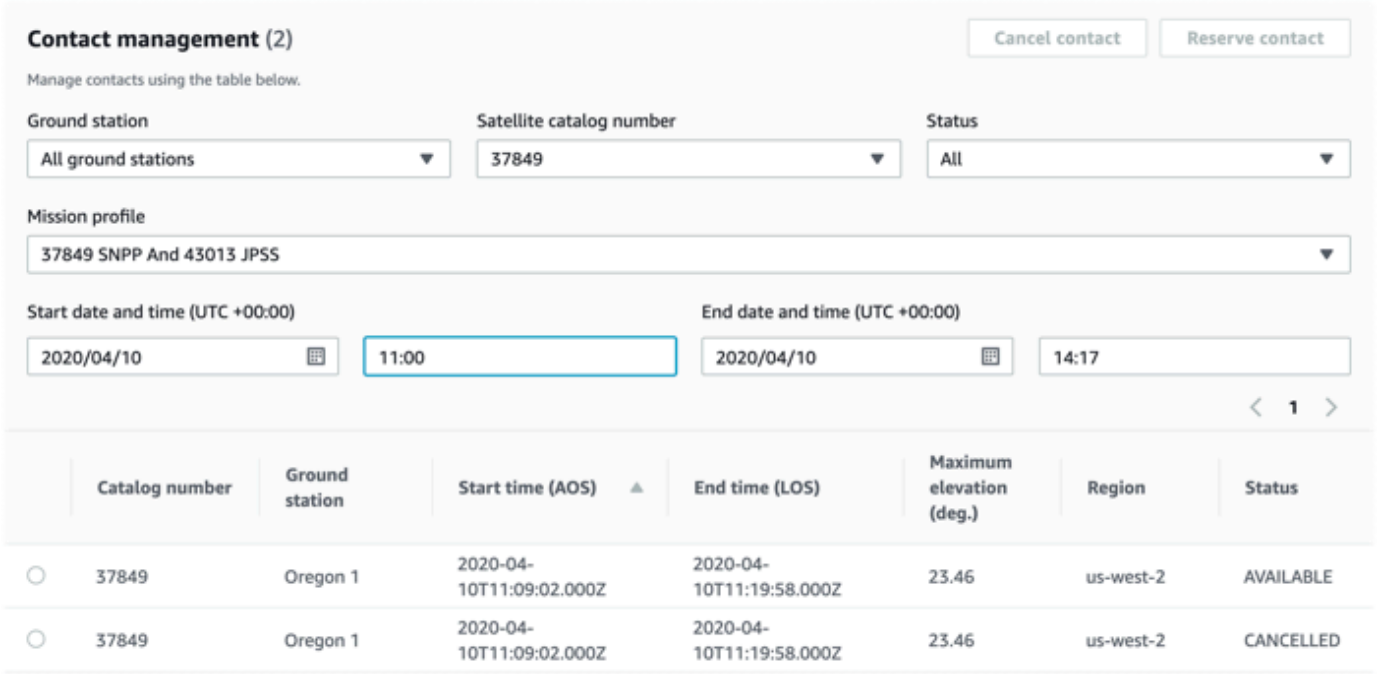



I contatti programmati o completati saranno elencati se corrispondono ai parametri.

## Annullamento dei contatti

È possibile utilizzare la AWS Ground Station console per annullare i contatti pianificati

1. Nella tabella Gestione contatti scegliere i parametri che si desidera utilizzare per cercare i contatti pianificati e completati. Verificare di visualizzare i contatti pianificati utilizzando il filtro Stato.
2. Scegliere il contatto che si desidera annullare nell'elenco dei contatti pianificati. Quindi, scegliere Cancel Contact (Annulla contatto).
3. Nella finestra di dialogo Cancel contact (Annulla contatto) scegliere Ok.




Lo stato del contatto sarà ANNULLATO.

## Denominazione dei satelliti

La AWS Ground Station console ha la capacità di visualizzare un nome definito dall'utente per un satellite insieme al Norad ID quando si utilizza la pagina Contatti. La visualizzazione del nome del satellite semplifica notevolmente la selezione del satellite corretto durante la programmazione. Per fare ciò, è possibile utilizzare i tag.

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

AWS Ground Station CLI

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

- Assicuratevi che sia installato AWS CLI . Per informazioni sull'installazione AWS CLI, consulta Installazione della versione 2 dell'interfaccia a riga di comando di AWS.
- Assicurati che AWS CLI sia configurato. Per informazioni sulla configurazione AWS CLI, consulta Configurazione della versione 2 dell'interfaccia a riga di comando di AWS.

- Puoi salvare le impostazioni di configurazione e le credenziali utilizzate più di frequente nei file gestiti dall' AWS CLI. Hai bisogno di queste impostazioni e credenziali per prenotare e gestire i tuoi contatti. AWS Ground Station AWS CLI Per ulteriori informazioni sul salvataggio delle impostazioni di configurazione e credenziali, consulta Impostazioni file di configurazione e credenziali.

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

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

Assegna un nome a un satellite

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

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

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

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

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

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

to:

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

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

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

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

```
aws groundstation tag-resource --region us-west-2 --resource-arn
 arn:aws:groundstation:us-
west-2:111111111111:satellite/11111111-2222-3333-4444-555555555555 --tags {\"Name\":
\"AQUA\"}
```

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

Cambia il nome di un satellite

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

```
aws groundstation tag-resource --region us-west-2 --resource-arn
 arn:aws:groundstation:us-
```

```
west-2:111111111111:satellite/11111111-2222-3333-4444-555555555555 --tags {\"Name\":
\"NewName\"}
```

Rimuovi il nome di un satellite

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

```
aws groundstation untag-resource --region us-west-2 --resource-arn
 arn:aws:groundstation:us-
west-2:111111111111:satellite/11111111-2222-3333-4444-555555555555 --tag-keys Name
```

# Prenotazione e gestione dei contatti con AWS CLI

Puoi utilizzarlo AWS CLI per prenotare e gestire i tuoi contatti in AWS Ground Station. Prima di utilizzare AWS CLI per prenotare e gestire i contatti, devono essere soddisfatti i seguenti AWS CLI prerequisiti:

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

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

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

Utilizza i seguenti argomenti per prenotare, visualizzare e annullare i contatti con AWS CLI.

Argomenti



## Visualizza ed elenca i contatti con AWS CLI

Per elencare e visualizzare `CANCELLED` o utilizzare `SCHEDULED` i contatti AWS CLI, esegui `aws groundstation list-contacts` con i seguenti parametri. `COMPLETED`

- Ora di inizio – Specificare l'ora di inizio del contatto con `--start-time <value>`. Di seguito è riportato un formato di valore temporale accettabile: `YYYY-MM-DDTHH:MM:SSZ`
- Ora di fine – Specificare l'ora di fine del contatto con `--end-time <value>`. Di seguito è riportato un formato di valore temporale accettabile: `YYYY-MM-DDTHH:MM:SSZ`
- Elenco di stato – Specificare lo stato del contatto con `--status-list <value>`. I valori accettabili includono `AVAILABLE`, `CANCELLED`, `COMPLETED` o `SCHEDULED`. Per visualizzare un elenco completo di valori validi, vedere list-contacts.

Per elencare e visualizzare `AVAILABLE` AWS CLI i contatti sono necessari i seguenti parametri oltre a quelli sopra elencati.

- ID stazione di terra – Specificare l'ID della stazione di terra con `--ground-station <value>`.
- Profilo missione ARN - Specificare l'ARN del profilo della missione con `--mission-profile-arn <value>`.
- Satellite ARN – Specificare il satellite ARN con `--satellite-arn <value>`.

È possibile utilizzare i comandi `list` per cercare le risorse. Per ulteriori informazioni sulla specificazione dei parametri, consulta list-contacts

Di seguito viene fornito un comando di esempio per elencare i contatti disponibili.

```
aws groundstation --region us-east-2 list-contacts --ground-station 'Ohio 1'
 --mission-profile-arn 'arn:aws:groundstation:us-east-2:123456789012:mission-
```

```
profile/11111111-2222-3333-4444-555555555555' --satellite-arn
 'arn:aws:groundstation::123456789012:satellite/11111111-2222-3333-4444-555555555555'
 --start-time '2020-04-10T00:09:22Z' --end-time '2020-04-10T00:11:22' --status-list
 'AVAILABLE'
```

Di seguito viene fornito un esempio di un elenco di contatti disponibili.

```
{
  "contactList": [
    {
      "contactStatus": "AVAILABLE",
      "endTime": "2020-04-15T03:16:35-06:00",
      "groundStation": "Oregon 1",
      "maximumElevation": {
        "unit": "DEGREE_ANGLE",
        "value": 11.22
      },
      "missionProfileArn": "arn:aws:groundstation:us-west-2:111111111111:mission-
profile/11111111-2222-3333-4444-555555555555",
      "region": "us-west-2",
      "satelliteArn":
 "arn:aws:groundstation::111111111111:satellite/11111111-2222-3333-4444-555555555555",
      "startTime": "2020-04-15T03:06:08-06:00"
    }
  ]
}
```

## Prenota un contatto con AWS CLI

AWS CLI ti dà la possibilità di prenotare i contatti di minuto in minuto. Questa funzionalità è esclusiva di AWS CLI e non può essere eseguita nella AWS Ground Station console.

Per prenotare i contatti con AWS CLI, esegui `aws groundstation reserve-contact` con i seguenti parametri.

- ID stazione di terra – Specificare l'ID della stazione di terra con `--ground-station <value>`.
- Profilo missione ARN - Specificare l'ARN del profilo della missione con `--mission-profile-arn <value>`.
- Satellite ARN – Specificare il satellite ARN con `--satellite-arn <value>`.
- Ora di inizio – Specificare l'ora di inizio del contatto con `--start-time <value>`. Di seguito è riportato un formato di valore temporale accettabile: `YYYY-MM-DDTHH:MM:SSZ`

- Ora di fine – Specificare l'ora di fine del contatto con `--end-time <value>`. Di seguito è riportato un formato di valore temporale accettabile: `YYYY-MM-DDTHH:MM:SSZ`

La prenotazione dei contatti è un processo asincrono. La risposta al `reserve-contact` comando fornisce l'identificatore del contatto. Per determinare l'esito del processo di prenotazione asincrono, utilizzare. `describe-contact` Per ulteriori informazioni su questo argomento, vedere la sezione seguente intitolata. Descrivi un contatto con AWS CLI

È possibile utilizzare i comandi `list` per cercare le risorse. Per ulteriori informazioni sulla specificazione dei parametri, vedere reserve-contact.

Di seguito viene fornito un esempio di comando di prenotazione di un contatto.

```
aws groundstation reserve-contact --ground-station 'Ohio 1' --mission-
profile-arn 'arn:aws:groundstation:us-east-2:123456789012:mission-
profile/11111111-2222-3333-4444-555555555555' --satellite-arn
 'arn:aws:groundstation::123456789012:satellite/11111111-2222-3333-4444-555555555555'
 --start-time '2020-04-10T00:09:22Z' --end-time '2020-04-10T00:11:22'
```

Di seguito viene fornito un esempio di contatto riservato con successo.

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

## Descrivi un contatto con AWS CLI

Per visualizzare lo stato di un contatto/prenotazione con AWS CLI, usa il comando `describe-contact` CLI. Ciò è utile per verificare l'esito del processo asincrono di prenotazione dei contatti, monitorare lo stato di un contatto in corso e determinare lo stato di un contatto finito.

Per descrivere i contatti con AWS CLI, `aws groundstation describe-contact` esegui con i seguenti parametri.

- ID contatto: specifica il tuo ID di contatto con`--contact-id <value>`.

È possibile utilizzare i comandi `list` per cercare le risorse. Per ulteriori informazioni sulla specificazione dei parametri, consulta describe-contact.

Di seguito viene fornito un esempio di comando per descrivere un contatto.

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

Di seguito viene fornito un esempio di contatto pianificato con successo.

```
{
  "groundStation": "Ireland 1",
  "tags": {},
  "missionProfileArn": "arn:aws:groundstation:us-west-2:111111111111:mission-
profile/11111111-2222-3333-4444-555555555555",
  "region": "us-west-2",
  "contactId": "11111111-2222-3333-4444-555555555555",
  "prePassStartTime": 1645850471.0,
  "postPassEndTime": 1645851172.0,
  "startTime": 1645850591.0,
  "maximumElevation": {
      "value": 12.66,
      "unit": "DEGREE_ANGLE"
  },
  "satelliteArn":
 "arn:aws:groundstation::111111111111:satellite/11111111-2222-3333-4444-555555555555",
  "endTime": 1645851052.0,
  "contactStatus": "SCHEDULED"
}
```

## Annulla un contatto con AWS CLI

Per annullare un contatto con AWS CLI, esegui `aws groundstation cancel-contact` con i seguenti parametri.

- Regione – Specificare la regione della Ground station con `--region <value>`.
- ID contatto – Specificare l'ID contatto con `--contact-id <value>`.

È possibile utilizzare i comandi `list` per cercare le risorse. Per ulteriori informazioni sulla specificazione dei parametri, consulta cancel-contacts

Di seguito viene fornito un esempio di comando di prenotazione di un contatto.

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

Di seguito viene fornito un esempio di contatto annullato con successo.

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

# Distribuzione dei dati ad Amazon EC2

AWS Ground Station invia i tuoi dati di contatto in modo asincrono a un bucket Amazon Simple Storage Service (Amazon S3) nel tuo account o in modo sincrono trasmettendoli in streaming da e verso un'istanza Amazon Elastic Compute Cloud (Amazon EC2) nel tuo account. I passaggi seguenti descrivono come configurare le risorse necessarie per lo streaming dei dati di contatto da e verso un'istanza Amazon EC2. Consulta la Guida introduttiva con AWS Ground Station guida per informazioni sulla distribuzione dei dati ad Amazon S3.

Argomenti



## Fase 1: creazione di una coppia di chiavi SSH EC2

Se non ne hai già una, crea una nuova coppia di key pair nella console Amazon EC2 per ogni AWS regione in cui intendi ricevere dati. Seguire i passaggi riportati di seguito.

1. Nella tua AWS Management Console, scegli una AWS regione in cui intendi prenotare i contatti. Devi creare una key pair per ogni AWS regione che scegli.

   > **Note**
   >
   > AWS Ground Station non è ancora disponibile per tutte le regioni. Assicurati che AWS Ground Station sia supportato dalla AWS regione desiderata. Per ulteriori informazioni sulla posizione delle AWS Ground Station antenne, consulta le domande frequenti su AWS Ground Station.

2. Segui la guida Create Key Pairs nella Amazon EC2 User Guide per creare le coppie di chiavi.
3. Ripetere l'operazione per altre AWS regioni, se necessario.

# Fase 2: configurazione del VPC

La configurazione completa di un VPC non viene descritta in questa guida. Se non si dispone di un VPC esistente già personalizzato, è possibile utilizzare il VPC predefinito creato nel proprio account AWS . Ti consigliamo di aggiungere un bastione Linux al tuo VPC in modo da poter accedere tramite SSH alle tue istanze Amazon EC2 senza collegare un indirizzo IP pubblico. Per ulteriori informazioni sulla configurazione di un bastion Linux nel VPC,consulta Linux Bastion Hosts on AWS.

Per comodità, di seguito sono riportate le istruzioni per aggiungere rapidamente un bastion host al tuo ambiente Linux. AWS Sebbene non sia richiesta, è considerata la best practice.

1. Accedi al tuo AWS account.
2. Nella pagina Linux Bastion Host on the AWS Cloud: Quick Start Reference Deployment scegliere Launch Quick Start (per il nuovo VPC).
3. Nella pagina Create Stack (Crea stack) scegliere Next (Successivo). Il modello è precompilato.
4. Nella pagina dei dettagli Specify stack (Specifica dettagli) apportare modifiche nelle caselle seguenti:

   a. Immettere un nome di stack per l'host nella casella Stack name (Nome stack).

   b. In Availability Zones (Zone disponibilità), selezionare le zone di disponibilità che si desidera utilizzare per le sottoreti nel VPC. È necessario selezionare almeno due zone di disponibilità.

   c. In Allowed bastion external access CIDR (CIDR accesso esterno bastion consentito), immettere il blocco CIDR da cui si desidera abilitare l'accesso SSH. In caso di dubbi, è possibile utilizzare il valore 0.0.0.0/0 per abilitare l'accesso SSH da qualsiasi host con la chiave SSH.

   d. Per Key pair name (Nome coppia chiavi), scegliere il nome della coppia di chiavi creata in the section called “Fase 1: creazione di una coppia di chiavi SSH EC2”.

   e. Per il tipo di istanza Bastion, scegliere t2.micro.

   > **Important**
   >
   > Il tipo di istanza t2.micro non è disponibile per la regione Europa (Stoccolma) (eu-north-1). Se utilizzi AWS Ground Station nella regione Europa (Stoccolma) (eu-north-1), scegli t3.micro.

   f. Per l' inoltro TCP, scegliere true.

g. (Facoltativo) Apportare altre modifiche secondo necessità. Per personalizzare la distribuzione, è possibile modificare la configurazione VPC, selezionare il numero e il tipo di istanze di bastion host, consentire inoltro TCP o X11 e abilitare un banner predefinito o personalizzato per i bastion host.

h. Seleziona Successivo.

5. Nella pagina Configure stack options (Configura opzioni stack) apportare modifiche in base alle proprie necessità.
6. Seleziona Successivo.
7. Esaminare i dettagli del bastion host e selezionare i due riconoscimenti di funzionalità. Scegliere Create stack (Crea stack).

# Passaggio 3: scegli e personalizza un modello AWS CloudFormation

Oggi, è possibile configurare più flussi di dati per contatto nel VPC. Questi flussi di dati sono disponibili in due formati diversi. I flussi di dati contenenti dati VITA-49 Signal/IP possono essere configurati per segnali S-Band e X-Band fino a 54 MHz di larghezza di banda. I dati di estensione VITA-49 possono essere configurati per segnali X-Band demodulati e/o decodificati fino a 500 MHz di larghezza di banda.

Dopo aver eseguito l'onboarding del satellite, devi definire i profili di missione e creare istanze per elaborare o eseguire il push dei flussi di dati da o verso il satellite. Per assisterti in questo processo, forniamo AWS CloudFormation modelli preconfigurati che utilizzano satelliti di trasmissione pubblici. Questi modelli ti semplificano l'avvio dell'utilizzo. AWS Ground Station Per ulteriori informazioni su AWS CloudFormation, consulta What is AWS CloudFormation?

È importante notare che è necessario disporre di un software di elaborazione dati o di archiviazione dati che ascolti il lato localhost di Data Defender dell'istanza Amazon EC2. Questo software è ciò che utilizzerai per archiviare e/o elaborare i dati forniti all'istanza Amazon EC2 durante un contatto.

## Configurazione delle impostazioni delle istanze Amazon EC2

I AWS CloudFormation modelli forniti in questa sezione sono configurati per utilizzare i tipi di istanze Amazon EC2 m5.4xlarge per impostazione predefinita. Tuttavia, ti invitiamo a personalizzare e scegliere le impostazioni dell'istanza Amazon EC2 corrette per il tuo caso d'uso. Quando si scelgono

le impostazioni dell'istanza, è necessario considerare requisiti quali I/O di storage e prestazioni della CPU. Ad esempio, l'esecuzione di un modem del software su un'istanza del ricevitore può richiedere istanze ottimizzate per il calcolo con più core e una velocità clock superiore. Il modo migliore per determinare le impostazioni dell'istanza corrette per il tuo caso d'uso è testare le impostazioni dell'istanza con il tuo carico di lavoro e Amazon EC2 semplifica il passaggio da una configurazione all'altra. Utilizzo dei modelli e personalizzazione delle impostazioni dell'istanza in base alle proprie esigenze.

Come raccomandazione generale, AWS Ground Station incoraggia l'uso di istanze che supportano reti avanzate per uplink e downlink, come AWS Nitro System. Per ulteriori informazioni sulle reti avanzate, consulta Abilitazione delle reti avanzate con Elastic Network Adapter (ENA) sulle istanze Linux.

Oltre a configurare i tipi di istanze Amazon EC2, i modelli configurano AWS CloudFormation le Amazon Machine Images (AMI) di base da utilizzare per l'istanza. La AWS Ground Station base contiene il software necessario per ricevere i dati dal servizio preinstallato sull'istanza EC2. Per ulteriori informazioni sulle AMI, consulta Amazon Machine Images (AMI).

## Creazione e configurazione manuale delle risorse

I AWS CloudFormation modelli di esempio in questa sezione configurano tutte le risorse necessarie per iniziare a eseguire i contatti satellitari. Se preferisci creare e configurare manualmente le risorse necessarie per iniziare a eseguire i contatti satellitari, dovrai fare quanto segue:

- Crea AWS Ground Station configurazioni. Per ulteriori informazioni sulla creazione manuale di AWS Ground Station configurazioni, consulta Create Config AWS CLI Command Reference o Create Config API Reference.
- Crea un profilo di missione. AWS Ground Station Per ulteriori informazioni sulla creazione manuale di un profilo di AWS Ground Station missione, consulta Create Mission Profile AWS CLI Command Reference o Create Mission Profile API Reference.
- Crea un gruppo di AWS Ground Station endpoint dataflow. Per ulteriori informazioni sulla creazione manuale di un gruppo di endpoint AWS Ground Station dataflow, consulta Create Dataflow Endpoint Group AWS CLI Command Reference o Create Dataflow Endpoint Group API Reference.
- Crea un'istanza EC2. Per ulteriori informazioni sulla creazione manuale di un'istanza EC2 da utilizzare con AWS Ground Station, consulta. Crea un'istanza Amazon EC2
- Configura le impostazioni del gruppo di sicurezza dell'istanza EC2 per consentire l'invio di dati AWS Ground Station da/verso l'istanza EC2. Per ulteriori informazioni sulla configurazione

manuale delle impostazioni del gruppo di sicurezza dell'istanza EC2, consulta Create Security Group AWS CLI Command Reference o Create Security Group API Reference.

## Seleziona un modello

AWS Ground Station fornisce modelli che dimostrano come utilizzare il servizio e sono accessibili in diversi modi. Utilizza questa guida per trovare il modello giusto per te.

Utilizzo di un modello preconfigurato

Puoi utilizzare un modello preconfigurato per ricevere dati di trasmissione diretta dai satelliti Aqua, SNPP, JPSS-1/NOAA-20 e Terra. Questi modelli contengono le risorse AWS CloudFormation necessarie per pianificare ed eseguire i contatti. Il `AquaSnppJpss` modello comprende le AWS CloudFormation risorse necessarie per ricevere dati di trasmissione diretta demodulati e decodificati. Utilizza questo modello come punto di partenza se prevedi di elaborare i dati utilizzando il software NASA Direct Readout Labs (RT-STPS e IPOPP). Il modello `AquaSnppJpssTerraDigIF` comprende le risorse AWS CloudFormation necessarie per ricevere dati di trasmissione diretta digitalizzata a frequenza intermedia (DigiF). Utilizza questo modello come punto di partenza per l'elaborazione dei dati utilizzando una radio definita dal software (SDR). Il `DirectBroadcastSatelliteWbDigIfEc2DataDelivery` modello comprende le AWS CloudFormation risorse necessarie per ricevere dati di trasmissione diretta a frequenza intermedia digitalizzata a banda larga (DigiF) tramite l'agente. AWS Ground Station

Modelli di distribuzione dati a banda stretta:

- the section called “AquaSnppJpss Modello (banda stretta)”
- the section called “AquaSnppJpssTerraDigModello IF (banda stretta)”

Modelli di distribuzione dati DigiF a banda larga:

- the section called “Modello DigiF a banda larga satellitare per trasmissione diretta (banda larga)”

> **Important**
>
> I satelliti devono essere integrati nel servizio per poter accedere alle AMI con i modelli. AWS CloudFormation

Utilizzo dei propri satelliti

La configurazione dei tuoi satelliti richiede un diverso insieme di parametri e risorse. Questo è difficile da fare da soli. Il AWS Ground Station team è disponibile per aiutarvi a configurare i vostri satelliti per l'uso e può aiutarvi a configurare le risorse per i flussi di eco in downlink, uplink e uplink. Per configurare il tuo satellite con cui utilizzarlo AWS Ground Station, contatta AWS Support.

## Accesso ai modelli

Puoi accedere ai modelli nel bucket regionale Amazon S3 riportato di seguito. Nota: il collegamento seguente utilizza un endpoint S3 regionale. Passa `<us-west-2>` alla regione in cui stai creando lo stack. AWS CloudFormation

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

È inoltre possibile scaricare i modelli utilizzando l' AWS CLI. Per informazioni sulla configurazione di AWS CLI, vedere Configurazione di. AWS CLI

## AquaSnppJpss Modello (banda stretta)

Il AWS CloudFormation modello denominato `AquaSnppJpss.yml` è progettato per darti un accesso rapido per iniziare a ricevere dati per i satelliti Aqua, SNPP e JPSS-1/NOAA-20. Contiene un'istanza Amazon EC2 e AWS Ground Station le risorse necessarie per pianificare i contatti e ricevere dati di trasmissione diretta demodulati e decodificati. Questo modello è un buon punto di partenza se si prevede di elaborare i dati utilizzando il software NASA Direct Readout Labs (RT-STPS e IPOPP).

Se Aqua, SNPP e JPSS-1/NOAA-20 non sono integrati nel tuo account, consulta Onboarding del cliente.

> **Important**
>
> L'istanza Amazon EC2 deve essere interrotta prima di applicare il modello. Verifica che l'istanza venga interrotta finché non sei pronto per utilizzarla.

È possibile accedere al modello accedendo al bucket S3 di onboarding del cliente. Si noti che i collegamenti sottostanti utilizzano un bucket S3 regionale. Passa `<us-west-2>` alla regione in cui stai creando lo AWS CloudFormation stack.

> **Note**
>
> Le seguenti istruzioni utilizzano YAML. Tuttavia, i modelli sono disponibili sia in formato YAML che JSON. Per utilizzare JSON, sostituire `<.yml>` con `<.json>`.

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

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

È possibile scaricare e visualizzare il modello nella console spostandosi all'URL seguente nel browser:

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

È possibile specificare il modello direttamente AWS CloudFormation utilizzando il seguente link:

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

Quali risorse definisce il modello?

Il modello `AquaSnppJpss` include le seguenti risorse:

- Ruolo del servizio di consegna dati: AWS Ground Station assume questo ruolo per creare/eliminare ENI nell'account per lo streaming dei dati.
- (Facoltativo) Istanza ricevente: l'istanza Amazon EC2 che invierà/riceverà dati da/verso il tuo satellite utilizzando. AWS Ground Station
  - Instance Security Group: il gruppo di sicurezza per la tua istanza Amazon EC2.
  - Ruolo dell'istanza: il ruolo della tua istanza Amazon EC2.
  - Profilo dell'istanza: il profilo dell'istanza per la tua istanza Amazon EC2.
  - Cluster Placement Group: il gruppo di collocamento in cui viene lanciata l'istanza Amazon EC2.
- Dataflow Endpoint Security Group: il gruppo di sicurezza a cui appartiene l'elastic network interface creata AWS Ground Station . Per impostazione predefinita, questo gruppo di sicurezza AWS Ground Station consente lo streaming del traffico verso qualsiasi indirizzo IP nel tuo VPC. È possibile modificarlo in modo da limitare il traffico a un insieme specifico di indirizzi IP.

- Receiver Instance Network Interface: un'interfaccia di rete elastica che fornisce un indirizzo IP fisso AWS Ground Station a cui connettersi. Questa interfaccia si collega all'istanza del ricevitore su `eth1`.
- Receiver Instance Interface Attachment: un'interfaccia di rete elastica che si collega all'istanza Amazon EC2.
- (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) Verifica EC2 per i contatti: l'opzione di utilizzare Lambda per configurare un sistema di verifica delle istanze Amazon EC2 per i contatti con notifica SNS. È importante notare che ciò potrebbe comportare costi a seconda dell'utilizzo corrente.
- Dataflow Endpoint Group: il gruppo di endpoint AWS Ground Station dataflow che definisce gli endpoint utilizzati per inviare/ricevere dati da/verso il satellite. Come parte della creazione del gruppo di endpoint dataflow, AWS Ground Station crea un'interfaccia di rete elastica nell'account per lo streaming dei dati.
- Configurazione di tracciamento - La configurazione di AWS Ground Station tracciamento definisce il modo in cui il sistema di antenna segue il satellite mentre si muove nel cielo.
- Ground Station Amazon Machine Image Retrieval Lambda: l'opzione per selezionare il software installato nell'istanza e l'AMI preferita. Le opzioni software includono e. `DDX 2.6.2 Only` `DDX 2.6.2 with qRadio 3.6.0` Se desideri utilizzare DigiF Data Delivery a banda larga e l' AWS Ground Station agente, utilizza il. AquaSnppJpssTerraDigModello IF (banda stretta) Queste opzioni continueranno ad espandersi man mano che verranno rilasciati aggiornamenti e funzionalità software aggiuntivi.

Inoltre, il modello fornisce le seguenti risorse per i satelliti Aqua, SNPP, JPSS-1/NOAA-20:

- Una configurazione downlink demod/decode per JPSS-1/NOAA-20 e SNPP e una configurazione downlink demod/decode per Aqua
- Un profilo di missione per JPSS-1/NOAA-20 e SNPP e un profilo di missione per Aqua

I valori e i parametri per i satelliti in questo modello sono già popolati. Questi parametri ne facilitano l'uso AWS Ground Station immediato con questi satelliti. 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 Data Defender per ricevere il flusso di dati dalla AWS Ground Station porta definita dall'endpoint dataflow. Una volta ricevuti, i dati sono disponibili per il consumo tramite la porta UDP 50000 sull'adattatore di loopback dell'istanza del ricevitore. Per ulteriori informazioni sulla configurazione di un gruppo di endpoint dataflow, consulta Gruppo. AWS::GroundStation::DataflowEndpoint

## AquaSnppJpssTerraDigModello IF (banda stretta)

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 Aqua, SNPP, JPSS-1/NOAA-20 e Terra. Contiene un'istanza Amazon EC2 e le AWS CloudFormation risorse necessarie per ricevere dati di trasmissione diretta DigiF non elaborati. Questo modello è un buon punto di partenza per l'elaborazione dei dati utilizzando una radio definita dal software (SDR).

Se Aqua, SNPP, JPSS-1/NOAA-20 e Terra non sono integrati nel tuo account, consulta Onboarding del cliente.

> **Important**
>
> L'istanza Amazon EC2 deve essere interrotta prima di applicare il modello. Verifica che l'istanza venga interrotta finché non sei pronto per utilizzarla.

È possibile accedere al modello accedendo al bucket S3 di onboarding del cliente. Si noti che i collegamenti sottostanti utilizzano un bucket S3 regionale. Passa `<us-west-2>` alla regione in cui stai creando lo AWS CloudFormation stack.

> **Note**
>
> Le seguenti istruzioni utilizzano YAML. Tuttavia, i modelli sono disponibili sia in formato YAML che JSON. Per utilizzare JSON, sostituire `<.yml>` con `<.json>`.

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

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

È possibile scaricare e visualizzare il modello nella console spostandosi all'URL seguente nel browser:

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

È possibile specificare il modello direttamente AWS CloudFormation utilizzando il seguente link:

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

Quali risorse definisce il modello?

Il modello `AquaSnppJpssTerraDigIF` include le seguenti risorse:

- Ruolo del servizio di consegna dati: AWS Ground Station assume questo ruolo per creare/eliminare ENI nell'account per lo streaming dei dati.
- (Facoltativo) Istanza ricevente: l'istanza Amazon EC2 che invierà/riceverà dati da/verso il tuo satellite utilizzando. AWS Ground Station
  - Instance Security Group: il gruppo di sicurezza per la tua istanza Amazon EC2.
  - Ruolo dell'istanza: il ruolo della tua istanza Amazon EC2.
  - Profilo dell'istanza: il profilo dell'istanza per la tua istanza Amazon EC2.
  - Cluster Placement Group: il gruppo di collocamento in cui viene lanciata l'istanza Amazon EC2.
- Dataflow Endpoint Security Group: il gruppo di sicurezza a cui appartiene l'elastic network interface creata AWS Ground Station . Per impostazione predefinita, questo gruppo di sicurezza AWS Ground Station consente lo streaming del traffico verso qualsiasi indirizzo IP nel tuo VPC. È possibile modificarlo in modo da limitare il traffico a un insieme specifico di indirizzi IP.
- Receiver Instance Network Interface: un'interfaccia di rete elastica che fornisce un indirizzo IP fisso AWS Ground Station a cui connettersi. Questa interfaccia si collega all'istanza del ricevitore su `eth1`.
- Receiver Instance Interface Attachment: un'interfaccia di rete elastica che si collega all'istanza Amazon EC2.

- (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) Verifica EC2 per i contatti: l'opzione di utilizzare Lambda per configurare un sistema di verifica delle istanze Amazon EC2 per i contatti con notifica SNS. È importante notare che ciò potrebbe comportare costi a seconda dell'utilizzo corrente.
- Dataflow Endpoint Group: il gruppo di endpoint AWS Ground Station dataflow che definisce gli endpoint utilizzati per inviare/ricevere dati da/verso il satellite. Come parte della creazione del gruppo di endpoint dataflow, AWS Ground Station crea un'interfaccia di rete elastica nell'account per lo streaming dei dati.
- Configurazione di tracciamento - La configurazione di AWS Ground Station tracciamento definisce il modo in cui il sistema di antenna segue il satellite mentre si muove nel cielo.
- Config endpoint Downlink Dig IF - Un endpoint definito utilizzato per eseguire il downlink dei dati dal satellite.
- Ground Station Amazon Machine Image Retrieval Lambda: l'opzione per selezionare il software installato nell'istanza e l'AMI preferita. Le opzioni software includono e. `DDX 2.6.2 Only` `DDX 2.6.2 with qRadio 3.6.0` Queste opzioni continueranno ad espandersi man mano che verranno rilasciati aggiornamenti e funzionalità software aggiuntivi.

Inoltre, il modello fornisce le seguenti risorse per i satelliti Aqua, SNPP, JPSS-1/NOAA-20 e Terra:

- Una configurazione dell'antenna Downlink DigiF per Aqua, SNPP, JPSS-1/NOAA-20 e Terra.
- Un profilo di missione per JPSS-1/NOAA-20 e SNPP, un profilo di missione per Aqua e un profilo di missione per Terra.

I valori e i parametri per i satelliti in questo modello sono già popolati. Questi parametri ne facilitano l'uso AWS Ground Station immediato con questi satelliti. 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 Data Defender per ricevere il flusso di dati dalla AWS Ground Station porta definita dall'endpoint dataflow. Una volta ricevuti, i dati sono disponibili per il consumo tramite la porta UDP 50000 sull'adattatore di loopback dell'istanza del

ricevitore. Per ulteriori informazioni sulla configurazione di un gruppo di endpoint dataflow, consulta Gruppo. AWS::GroundStation::DataflowEndpoint

## Modello DigiF a banda larga satellitare per trasmissione diretta (banda larga)

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 Aqua, SNPP, JPSS-1/NOAA-20 e Terra. Contiene un'istanza Amazon EC2 e le AWS CloudFormation risorse necessarie per ricevere dati di trasmissione diretta DigiF non elaborati. Questo modello è un buon punto di partenza per l'elaborazione dei dati utilizzando una radio definita dal software (SDR).

Se Aqua, SNPP, JPSS-1/NOAA-20 e Terra non sono integrati nel tuo account, consulta Onboarding del cliente.

> **Important**
>
> L'istanza Amazon EC2 deve essere interrotta prima di applicare il modello. Verifica che l'istanza venga interrotta finché non sei pronto per utilizzarla.

È possibile accedere al modello accedendo al bucket S3 di onboarding del cliente. Si noti che i collegamenti sottostanti utilizzano un bucket S3 regionale. Passa `<us-west-2>` alla regione in cui stai creando lo AWS CloudFormation stack.

> **Note**
>
> Le seguenti istruzioni utilizzano YAML. Tuttavia, i modelli sono disponibili sia in formato YAML che JSON. Per utilizzare JSON, sostituire `<.yml>` con `<.json>`.

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 .
```

È possibile scaricare e visualizzare il modello nella console spostandosi all'URL seguente nel browser:

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

È possibile specificare il modello direttamente 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 definisce il modello?

Il modello `DirectBroadcastSatelliteWbDigIfEc2DataDelivery` include le seguenti risorse:

- (Facoltativo) Istanza ricevente: l'istanza Amazon EC2 che invierà/riceverà dati da/verso il tuo satellite utilizzando. AWS Ground Station
  - Instance Security Group: il gruppo di sicurezza per la tua istanza Amazon EC2.
  - Ruolo dell'istanza: il ruolo della tua istanza Amazon EC2.
  - Profilo dell'istanza: il profilo dell'istanza per la tua istanza Amazon EC2.
  - Cluster Placement Group: il gruppo di collocamento in cui viene lanciata l'istanza Amazon EC2.
- Chiave di consegna dei dati: AWS KMS chiave utilizzata per crittografare i flussi di dati.
- Ruolo chiave di Ground Station: il ruolo IAM che AWS Ground Station assumerà per accedere e utilizzare la AWS KMS chiave per decrittografare i flussi di dati
- Ground Station Key Access Policy - La policy IAM che definisce AWS Ground Station le azioni da intraprendere sulla Data Delivery Key
- Interfaccia di rete elastica dell'istanza del ricevitore - (Condizionale) Un'interfaccia di rete elastica viene creata nella sottorete specificata da, PublicSubnetIdse fornita. Questa operazione è necessaria se l'istanza del ricevitore si trova in una sottorete privata. L'elastic network interface verrà associata all'EIP e collegata all'istanza del ricevitore.
- IP elastico dell'istanza del ricevitore: un IP elastico AWS Ground Station a cui connettersi. Si collega all'istanza del ricevitore o all'interfaccia elastic network.
- Una delle seguenti associazioni IP elastiche:
  - Associazione da istanza del ricevitore a Elastic IP: l'associazione dell'IP elastico all'istanza del ricevitore, se non PublicSubnetIdè specificata. Ciò richiede che tale SubnetIdriferimento sia una sottorete pubblica.

  - Associazione Elastic Network Interface to Elastic IP Association dell'istanza del ricevitore: l'associazione dell'IP elastico all'interfaccia di rete elastica dell'istanza del ricevitore, se PublicSubnetIdspecificata.
- (Facoltativo) CloudWatch Event Triggers - AWS Lambda Funzione che viene attivata utilizzando CloudWatch gli eventi inviati AWS Ground Station prima e dopo un contatto. La AWS Lambda funzione avvierà e, facoltativamente, interromperà l'istanza del ricevitore.
- (Facoltativo) Verifica EC2 per i contatti: l'opzione di utilizzare Lambda per configurare un sistema di verifica delle istanze Amazon EC2 per i contatti con notifica SNS. È importante notare che ciò potrebbe comportare costi a seconda dell'utilizzo corrente.
- Dataflow Endpoint Group: il gruppo di endpoint AWS Ground Station dataflow che definisce gli endpoint utilizzati per inviare/ricevere dati da/verso il satellite.
- Configurazione di tracciamento - La configurazione di AWS Ground Station tracciamento definisce il modo in cui il sistema di antenna segue il satellite mentre si muove nel cielo.

Inoltre, il modello fornisce le seguenti risorse per i satelliti Aqua, SNPP, JPSS-1/NOAA-20 e Terra:

- Una configurazione di downlink per JPSS-1/NOAA-20 e SNPP, una configurazione di downlink per Aqua e una configurazione di downlink per Terra.
- Un profilo di missione per JPSS-1/NOAA-20 e SNPP, un profilo di missione per Aqua e un profilo di missione per Terra.

I valori e i parametri per i satelliti in questo modello sono già popolati. Questi parametri ne facilitano l'uso AWS Ground Station immediato con questi satelliti. 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, vedere. AWS Ground Station Guida per l'utente dell'agente

# Crea un'istanza Amazon EC2

> **Note**
>
> Non è necessario né consigliato creare le risorse per AWS Ground Station (incluse le istanze Amazon EC2) manualmente, poiché AWS Ground Station fornisce AWS CloudFormation modelli predefiniti a tale scopo (per ulteriori informazioni, consulta Passaggio 3: scegli e personalizza un modello AWS CloudFormation la pagina). Se l'utilizzo AWS CloudFormation dei modelli non è adatto al tuo caso d'uso, continua a leggere.

AWS Ground Station fornisce AMI Amazon EC2 precaricate con il software necessario per la distribuzione dei dati su un'istanza Amazon EC2 per la distribuzione di dati a banda stretta o a banda larga. DigIf

> **Important**
>
> I satelliti devono essere integrati nel servizio per poter accedere alle AMI. AWS Ground Station

## AMI Amazon EC2 con DataDefender

Questa AMI è preinstallata con il DataDefender software e viene utilizzata per i contatti in downlink per la consegna di dati a banda stretta.

Lo schema di denominazione per questo AMI è`groundstation-al2-ddx$DDX_VERSION-ami-$DATE_PUBLISHED`. Una nuova AMI DDX viene pubblicata poco dopo la pubblicazione di una nuova AMI Amazon EC2 AL2. Se si AWS Ground Station decide di supportare una nuova versione del DataDefender software, verrà pubblicata una nuova AMI utilizzando la versione aggiornata.

Selezione di un AWS Ground Station AMI con DataDefender

Puoi accedere all' AWS Ground Station AMI tramite la scheda AMI nella console Amazon EC2. Una volta in quella pagina, le AMI sono accessibili tramite il filtro Immagini private.

Ti consigliamo di ordinare le AMI in base alla data di pubblicazione e di utilizzare l'AMI pubblicata più di recente denominata. `groundstation-al2-ddx$DDX_VERSION-ami-$DATE_PUBLISHED`

### AMI Amazon EC2 con agente AWS Ground Station

Questa AMI è preinstallata con l' AWS Ground Station agente e viene utilizzata per i contatti in downlink DigiF a banda larga.

Lo schema di denominazione per questo AMI è `groundstation-al2-gs-agent-ami-*` dove * è la data di creazione dell'AMI. Una nuova AMI AWS Ground Station Agent viene pubblicata poco dopo la pubblicazione di una nuova AMI Amazon EC2 AL2 o quando viene rilasciata una nuova versione AWS Ground Station dell'Agent RPM.

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

Selezione di un AWS Ground Station AGENT AMI

Puoi accedere all'AMI dell' AWS Ground Station agente tramite la scheda AMI nella console Amazon EC2. Una volta in quella pagina, le AMI sono accessibili tramite il filtro Immagini pubbliche.

Ti consigliamo di ordinare le AMI in base alla data di pubblicazione e di utilizzare l'AMI pubblicata più di recente denominata. `groundstation-al2-gs-agent-ami-$DATE_PUBLISHED`

## Fase 4: Configurare uno stack AWS CloudFormation

Dopo aver scelto il modello più adatto al tuo caso d'uso, configura uno AWS CloudFormation stack. Le risorse create in questa procedura vengono configurate per la regione in cui ti trovi quando vengono create. Ciò include il profilo della missione e le relative proprietà che determinano in quale regione vengono consegnati i dati.

1. In AWS Management Console, scegli Servizi > CloudFormation.
2. Nel riquadro di navigazione selezionare Stacks (Stack). Quindi scegliere Crea stack > Con nuove risorse (standard).
3. Nella pagina Create stack (Crea stack), specificare il modello selezionato in the section called “Seleziona un modello” eseguendo una delle seguenti operazioni.

    a. Selezionare l'URL Amazon S3 come origine del modello e copiare e incollare l'URL del modello che si desidera utilizzare nell'URL Amazon S3. Quindi, seleziona Next (Successivo).

b. Selezionare Upload a template file (Carica un file modello) come origine modello e scegliere Choose File (Scegli file). Caricare il modello scaricato in the section called “Seleziona un modello”. Quindi, seleziona Next (Successivo).

4. Nella pagina dei dettagli Specify stack (Specifica stack), apportare le seguenti modifiche:

   a. Immettere un nome nella casella Stack Name (Nome stack). Si consiglia di utilizzare un nome semplice per ridurre la possibilità di errori in futuro.

   b. Per CloudWatchEventActions, scegli quali azioni eseguire per l' CloudWatch evento che si attiva prima e dopo un contatto.

   c. Per CreateEC2 VerificationForContacts, scegli se configurare o meno un sistema di verifica (utilizzando Lambda) delle tue istanze EC2 per i contatti con notifica SNS. È importante notare che ciò potrebbe comportare costi a seconda dell'utilizzo corrente.

   d. Per CreateReceiverInstance, scegli se vuoi creare o meno un'istanza di ricevitore Amazon EC2.

   e. Scegliere la chiave SSH creata in the section called “Fase 1: creazione di una coppia di chiavi SSH EC2”.

   f. Scegli l'SubnetIdistanza in cui desideri creare la tua istanza Amazon EC2.

      Se si utilizza l' AWS Ground Station agente, è necessaria una sottorete pubblica, per il posizionamento dell'istanza o un'interfaccia di rete elastica; se si specifica una sottorete privata SubnetIdin cui collocare l'istanza, è necessario specificare anche una sottorete pubblica PublicSubnetId(vedi sotto) da utilizzare con l'agente. AWS Ground Station

      Per i casi d'uso diversi da agenti, consigliamo di collocare l'istanza Amazon EC2 in una sottorete privata come best practice, sebbene non sia obbligatoria. È possibile usare Linux Bastion Hosts su AWS Cloud: Quick Start Reference Deployment per creare automaticamente una sottorete privata se non è già stato configurato l’account con tale sottorete in the section called “Fase 2: configurazione del VPC”.

      > **Note**
      >
      > La tua organizzazione potrebbe avere un'altra sottorete dedicata per la tua istanza Amazon EC2.

   g. (Facoltativo) Scegli l'opzione PublicSubnetIdda utilizzare solo se utilizzi l' AWS Ground Station agente con un'istanza in una sottorete privata. Questo è necessario se è stata specificata una sottorete privata in. SubnetId

Questa sottorete deve trovarsi nel tuo account nella stessa zona di disponibilità specificata da. SubnetId L'immissione di a PublicSubnetIdcomporterà la creazione di un'interfaccia di rete elastica nella sottorete pubblica fornita, collegata all'istanza. Questa interfaccia viene utilizzata per l'accesso alla rete AWS Ground Station dell'agente dall'istanza dell'utente, che si trova nella sottorete privata specificata in. SubnetId

h. Scegliere lo stack VPC creato in the section called “Fase 2: configurazione del VPC”.

i. Seleziona Successivo.

5. Configura le opzioni di stack e le opzioni avanzate per la tua istanza Amazon EC2.

   a. Aggiungere tutti i tag e le autorizzazioni nelle sezioni Tag e Permissions (Autorizzazioni).

   b. Apportare le modifiche a Stack policy (Policy stack), Rollback configuration (Configurazione rollback), Notification options (Opzioni di notifica) e alle Stack creation options (Opzioni di creazione dello stack).

   c. Seleziona Successivo.

6. Dopo aver esaminato i dettagli dello stack, selezionare il riconoscimento delle capacità e scegliere Create stack (Crea stack).

## Fase 5: installazione e configurazione del processore/radio FE

L'istanza Amazon EC2 definita nel AWS CloudFormation modello non dispone di un processore Front End (FE) o di una radio definita dal software (SDR) installati per impostazione predefinita. È necessario installare un processore FE o SDR per elaborare i pacchetti VITA-49 in streaming da/verso il sistema di antenne AWS Ground Station .

Il modo di installare e configurare il processore FE o SDR varia in base a quale processore FE o SDR si sta utilizzando. L’installazione di un processore FE o SDR non rientra nell'ambito di questa guida utente.

Per installare e configurare il processore/radio FE, contattare AWS Support.

> **Important**
>
> È consigliabile eseguire il processore FE o SDR sulle istanze create dal AWS CloudFormation modello per garantire i vantaggi dei flussi di dati DTLS da/verso Data Defender.

# Fasi successive

Il tuo AWS Ground Station account e le tue risorse sono ora configurati e pronti per l'uso. Queste risorse possono essere utilizzate nella AWS Ground Station console, dove è possibile inserire dati satellitari, identificare le posizioni delle antenne, comunicare e programmare l'ora dell'antenna per i satelliti selezionati. È inoltre possibile iniziare a utilizzare diversi strumenti per monitorare l'attività e configurare gli allarmi.

Per ulteriori informazioni, consultare i seguenti argomenti:

- Creazione di un elenco di contatti e prenotazione
- Monitoraggio AWS Ground Station

# Utilizzo del servizio di recapito dei dati tra regioni

La AWS Ground Station funzionalità di distribuzione dei dati tra regioni offre la flessibilità necessaria per inviare i dati da un'antenna a un'istanza Amazon EC2 nella tua regione AWS. 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. È disponibile solo nelle seguenti antenna-to-destination regioni quando si utilizza la consegna dei dati ad Amazon EC2:

- 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 distribuzione di dati tra regioni, è necessario che sia configurato un AWS CloudFormation modello. Per ulteriori informazioni sulla scelta e la personalizzazione dei AWS CloudFormation modelli, consulta. Passaggio 3: scegli e personalizza un modello AWS CloudFormation

Utilizzare i seguenti argomenti per utilizzare il recapito dei dati tra regioni in AWS Ground Station.

Argomenti

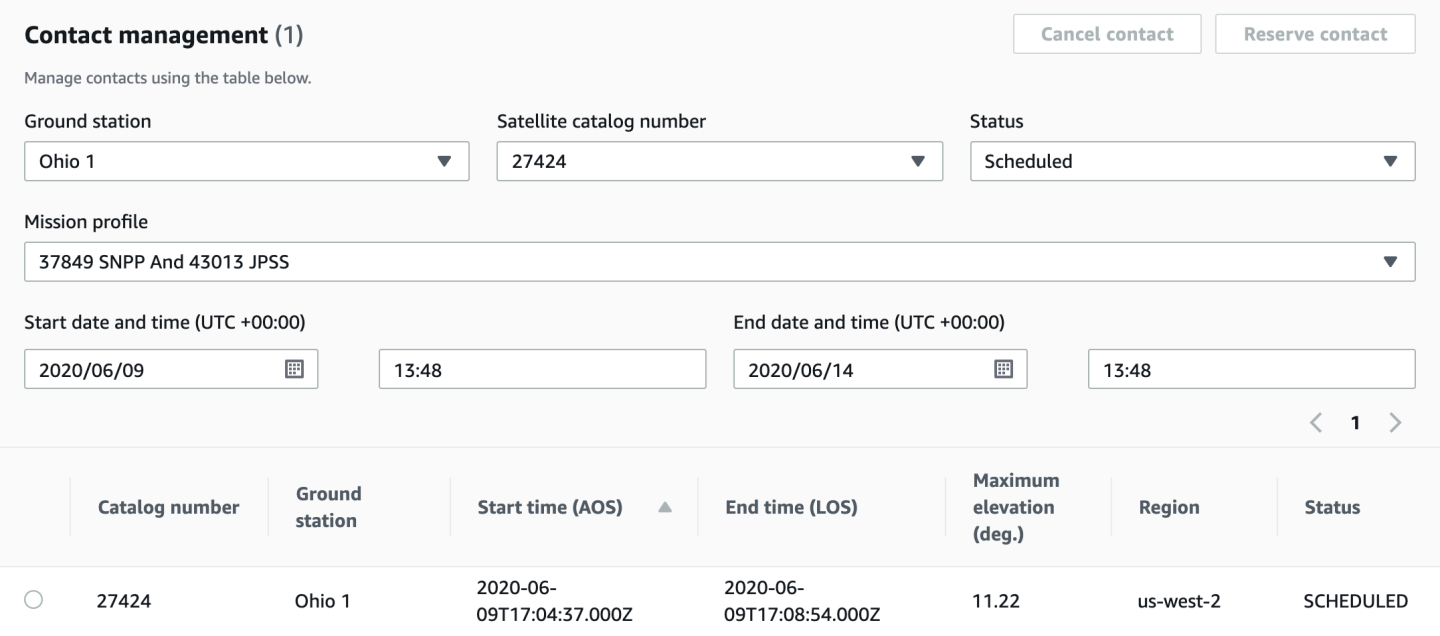


## Per utilizzare il recapito dei dati tra regioni nella console

Quando prenoti un contatto nella AWS Ground Station console, scegli il profilo di missione configurato per fornire i dati di contatto nella regione desiderata. Assicurarsi che tutti i parametri siano corretti e scegliere Prenota contatto. Se nella console non viene visualizzato il profilo missione desiderato, verificare di aver creato il profilo missione nella regione in cui si sta visualizzando la console.

Dopo aver prenotato il contatto, è possibile visualizzare i contatti programmati per verificare di avere programmato il recapito dei dati tra regioni visualizzando la posizione dell'antenna della stazione di terra e la regione di destinazione. L'immagine seguente mostra un contatto pianificato per il recapito

dei dati tra regioni. Il contatto è configurato per utilizzare le antenne della stazione di terra dell'Ohio e fornire dati all'Oregon.




# Per utilizzare il recapito dei dati tra regioni con l'interfaccia CLI di AWS

Quando prenoti un contatto AWS CLI, scegli il profilo di missione configurato per fornire i dati di contatto nella regione desiderata. Specificare l'ARN del profilo missione desiderato con `--mission-profile-arn <value>`. Assicurarsi che tutti i parametri siano corretti ed eseguire il comando. Se non viene visualizzato l'ARN del profilo missione desiderato durante la visualizzazione e l'elenco dei contatti, verificare di aver creato il profilo missione nella regione in cui stai eseguendo AWS CLI.

Dopo aver prenotato il contatto, è possibile visualizzare i contatti programmati per verificare di avere programmato il recapito dei dati tra regioni visualizzando la posizione dell'antenna della stazione di terra e la regione di destinazione. L'output seguente mostra un contatto pianificato per il recapito dei dati tra regioni. Il contatto è configurato per utilizzare le antenne della stazione di terra dell'Ohio e recapitare i dati all'Oregon.

```
{
  "contactList": [
    {
      "contactId": "11111111-2222-3333-4444-555555555555",
      "contactStatus": "SCHEDULED",
```

```
      "endTime": "2020-05-05T03:16:35-06:00",
      "groundStation": "Ohio 1",
      "maximumElevation": {
        "unit": "DEGREE_ANGLE",
        "value": 26.74
      },
      "missionProfileArn": "arn:aws:groundstation:us-west-2:123456789012:mission-
profile/11111111-2222-3333-4444-555555555555",
      "postPassEndTime": "2020-05-05T03:17:35-06:00",
      "prePassStartTime": "2020-05-05T03:04:08-06:00",
      "region": "us-west-2",
      "satelliteArn":
 "arn:aws:groundstation::123456789012:satellite/11111111-2222-3333-4444-555555555555",
      "startTime": "2020-05-05T03:06:08-06:00"
    }
  ]
}
```

# Monitoraggio AWS Ground Station

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

- Amazon CloudWatch Events offre un flusso quasi in tempo reale di eventi di sistema che descrivono i cambiamenti nelle AWS risorse. CloudWatch Events consente l'elaborazione automatizzata basata sugli eventi, poiché puoi scrivere regole che controllano determinati eventi e attivano azioni automatizzate in altri AWS servizi quando si verificano tali eventi. Per ulteriori informazioni su Amazon CloudWatch Events, consulta la Amazon CloudWatch Events User Guide.
- AWS EventBridge Events offre un flusso quasi in tempo reale di eventi di sistema che descrivono i cambiamenti nelle AWS risorse. EventBridge Events consente l'elaborazione automatizzata basata sugli eventi, poiché puoi scrivere regole che controllano determinati eventi e attivano azioni automatizzate in altri AWS servizi quando si verificano tali eventi. Per ulteriori informazioni sugli EventBridge eventi, consulta la Amazon EventBridge Events User Guide.
- AWS CloudTrailacquisisce le chiamate API e gli eventi correlati effettuati da o per conto del tuo AWS account e invia i file di log a un bucket Amazon S3 da te specificato. Puoi identificare quali utenti e account hanno richiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute. Per ulteriori informazioni in merito AWS CloudTrail, consulta la Guida per l'AWS CloudTrail 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 Amazon CloudWatch Metrics.
- AWS Notifiche all'utente può essere utilizzato per configurare canali di distribuzione per ricevere notifiche sugli AWS Ground Station eventi. L'utente riceverà una notifica quando un evento corrisponde a una regola specificata. 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 console. Notifiche all'utente supporta l'aggregazione, che può ridurre il numero di notifiche ricevute durante eventi specifici.

Utilizza gli argomenti seguenti per monitorare AWS Ground Station.

Argomenti

# Automazione AWS Ground Station con gli eventi

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

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

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

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

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

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

## Eventi di esempio

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

Modifica dello stato di contatto della Ground Station

Se si desidera eseguire un'operazione specifica quando un contatto imminente cambia stato, è possibile impostare una regola per automatizzare questa operazione. Questo è utile per quando si desidera ricevere notifiche sulle modifiche di stato del contatto. Se desideri cambiare quando ricevi questi eventi, puoi modificare il tuo profilo di missione e. contactPrePassDurationSecondscontactPostPassDurationSeconds Gli eventi vengono inviati alla regione da cui è stato pianificato il contatto.

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: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 “Stati dei contatti di Ground Station”.

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`.

Cambio di stato delle effemeridi di Ground Station

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

Un esempio è fornito di seguito.

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

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

# Registrazione delle chiamate AWS Ground Station API con AWS CloudTrail

AWS Ground Station è integrato con AWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, un ruolo o un AWS servizio in AWS Ground Station. CloudTrail acquisisce tutte le chiamate API AWS Ground Station come eventi. Le chiamate acquisite includono chiamate dalla AWS Ground Station console e chiamate di codice alle operazioni AWS Ground Station API. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per. AWS Ground Station Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare a quale richiesta è stata inviata AWS Ground Station, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

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

## AWS Ground Station Informazioni in CloudTrail

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

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

- Panoramica della creazione di un trail
- CloudTrail Servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail

- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

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

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

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.

Per ulteriori informazioni, vedete l'elemento CloudTrail userIdentity.

## Comprensione delle AWS Ground Station voci dei file di registro

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

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

Esempio: ReserveContact

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINICIPLE_ID",
        "arn": "arn:aws:sts::123456789012:user/Alice",
        "accountId": "123456789012",
```

```
        "accessKeyId": "EXAMPLE_KEY_ID",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2019-05-15T21:11:59Z"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EX_PRINICIPLE_ID",
                "arn": "arn:aws:iam::123456789012:role/Alice",
                "accountId": "123456789012",
                "userName": "Alice"
            }
        }
    },
    "eventTime": "2019-05-15T21:14:37Z",
    "eventSource": "groundstation.amazonaws.com",
    "eventName": "ReserveContact",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "127.0.0.1",
    "userAgent": "Coral/Jakarta",
    "requestParameters": {
        "satelliteArn":
 "arn:aws:groundstation::123456789012:satellite/11111111-2222-3333-4444-555555555555",
        "groundStation": "Ohio 1",
        "startTime": 1558356107,
        "missionProfileArn": "arn:aws:groundstation:us-east-2:123456789012:mission-
profile/11111111-2222-3333-4444-555555555555",
        "endTime": 1558356886
    },
    "responseElements": {
        "contactId": "11111111-2222-3333-4444-555555555555"
    },
    "requestID": "11111111-2222-3333-4444-555555555555",
    "eventID": "11111111-2222-3333-4444-555555555555",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "11111111-2222-3333-4444-555555555555"
}
```

# 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 su un grafico o come codice sorgente 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

| Parametro | Descrizione |
| --- | --- |
| `AzimuthAngle` | L'angolo di azimut dell'antenna. Il vero nord è 0 gradi e l'est è 90 gradi.<br><br>Unità: gradi |
| `BitErrorRate` | Il tasso di errore sui bit in un determinato numero di trasmissioni di bit. Gli errori di bit sono causati da rumore, distorsione o interferenza<br><br>Unità: errori di bit per unità di tempo |
| `BlockErrorRate` | Il tasso di errore dei blocchi in un determinato numero di blocchi ricevuti. Gli errori dei blocchi sono causati da interferenze.<br><br>Unità: Blocchi errati/Numero totale di blocchi |
| `CarrierFrequencyRecovery_Cn0` | Rapporto tra densità portante e rumore per unità di larghezza di banda.<br><br>Unità: Decibel-Hertz (dB-Hz) |
| `CarrierFrequencyRecovery_Locked` | Impostato su 1 quando il circuito di recupero della frequenza portante del demodulatore è bloccato e 0 quando è sbloccato. |

| Parametro | Descrizione |
| --- | --- |
| | Unità: senza unità |
| `CarrierFrequencyRecovery_OffsetFrequency_Hz` | 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.<br><br>Unità: hertz (Hz) |
| `ElevationAngle` | L'angolo di elevazione dell'antenna. L'orizzonte è di 0 gradi e lo zenit è di 90 gradi.<br><br>Unità: gradi |
| `Es/N0` | Il rapporto tra l'energia per simbolo e la densità spettrale della potenza del rumore.<br><br>Unità: decibel (dB) |
| `ReceivedPower` | La potenza del segnale misurata nel demodulatore/decodificatore.<br><br>Unità: decibel rispetto ai milliwatt (dBm) |
| `SymbolTimingRecovery_ErrorVectorMagnitude` | La grandezza del vettore di errore tra i simboli ricevuti e i punti ideali della costellazione.<br><br>Unità: percentuale |
| `SymbolTimingRecovery_Locked` | Impostato su 1 quando il ciclo di ripristino del simbolo del demodulatore è bloccato e 0 quando è sbloccato<br><br>Unità: senza unità |

| Parametro | Descrizione |
| --- | --- |
| `SymbolTimingRecovery_Offset SymbolRate` | L'offset tra la frequenza simbolica stimata e la frequenza simbolica del segnale ideale. Ciò è causato dallo spostamento Doppler e dall'offs et dell'oscillatore locale tra il veicolo spaziale e il sistema di antenna.<br><br>Unità: simboli/secondo |

### Per quali dimensioni vengono utilizzate? AWS Ground Station

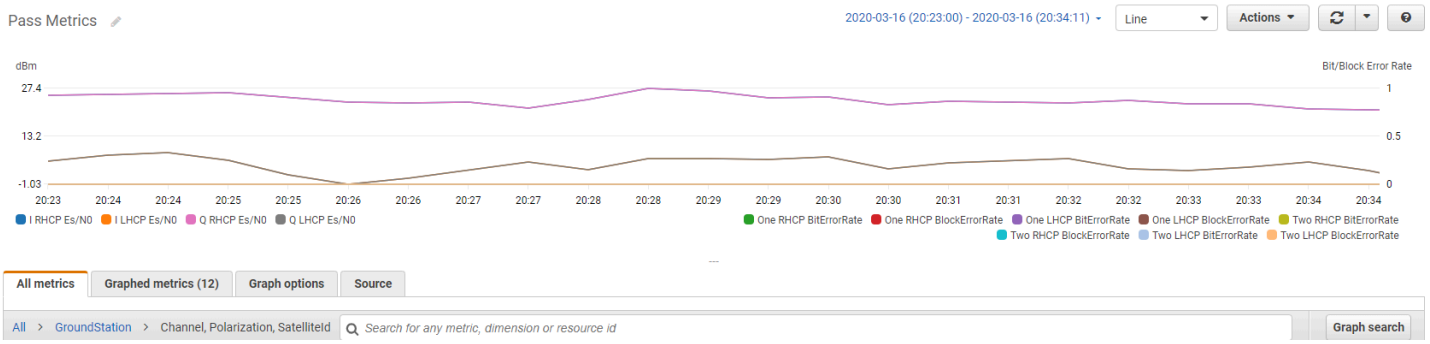
È possibile filtrare AWS Ground Station i dati utilizzando le seguenti dimensioni.

| Dimensione | Descrizione |
| --- | --- |
| `Channel` | I canali per ogni contatto includono Uno, Due, I (in fase) e Q (quadratura). |
| `Polarization` | La polarizzazione per ogni contatto include LHCP (Left Hand Circular Polarized) o RHCP (Right Hand Circular Polarized). |
| `SatelliteId` | L'ID satellitare contiene l'ARN del satellite per i tuoi contatti. |

## Visualizzazione dei parametri

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

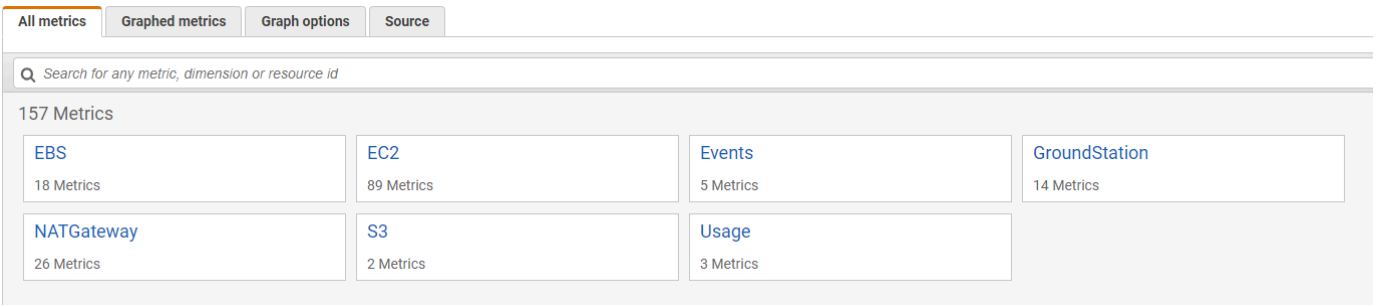
Inoltre, i dati acquisiti entro i primi 60 secondi non conterranno informazioni sufficienti per produrre parametri significativi e probabilmente non verranno visualizzati. Per visualizzare metriche significative, si consiglia di visualizzare i dati dopo 60 secondi.



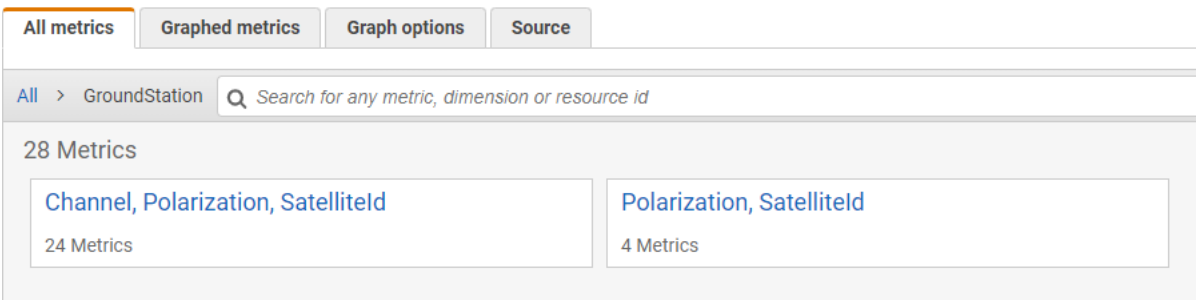

Per ulteriori informazioni sulla rappresentazione grafica delle metriche in CloudWatch, consulta Graphing AWS Ground Station Metrics.

## 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 creare un grafico di un parametro, seleziona la casella di controllo associata al parametro. Per selezionare tutte i parametri, seleziona la casella di controllo nella riga dell'intestazione 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 dell'AWS CLI.
2. Crea un file JSON di configurazione CloudWatch dell'agente. Per istruzioni sulla creazione di un file di configurazione CloudWatch dell'agente, consulta Creare il file di configurazione CloudWatch dell'agente.
3. Elenca le CloudWatch metriche disponibili `aws cloudwatch list-metrics` eseguendo.
4. Modifica il file JSON creato nel passaggio 2 in modo che corrisponda ai parametri `SatellitID`.

> **Note**
>
> Non ridurre il `Period` campo a un valore inferiore a 60. AWS Ground Station pubblica le metriche ogni 60 secondi e non verrà restituita alcuna metrica se il valore viene ridotto.

5. Esegui `aws cloudwatch get-metric-data` indicando i periodi di tempo dei pass e il file JSON di configurazione CloudWatch dell'agente. Un esempio è fornito di seguito.

```
aws cloudwatch get-metrics-data –start-time 2020-02-26T19:12:00Z –end-time
 2020-02-26T19:24:00Z –metric-data-queries file://metricdata.json
```

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”: “myQuery”,
              “Label”: “Es/N0”,
              “Timestamps”: [
                  “2020-02-18T19:44:00Z”,
                  “2020-02-18T19:43:00Z”,
                  “2020-02-18T19:42:00Z”,
                  “2020-02-18T19:41:00Z”,
                  “2020-02-18T19:40:00Z”,
                  “2020-02-18T19:39:00Z”,
                  “2020-02-18T19:38:00Z”,
                  “2020-02-18T19:37:00Z”,
              ],
              “Values”: [
                  24.58344556958329,
                  24.251638725562216,
                  22.919391450230158,
                  22.83838908204037,
                  23.303086848486842,
                  22.845261784583364,
                  21.34531397048953,
                  19.171561698261222
              ],
              “StatusCode”: “Complete”
          }
      ]
      “Messages”: []
}
```

# Risoluzione dei problemi

La seguente documentazione può aiutarti a risolvere i problemi che potrebbero impedire il corretto completamento di un AWS Ground Station contatto.

Argomenti



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

Se non riesci a completare con successo un AWS Ground Station contatto, dovrai verificare che l'istanza Amazon EC2 sia in esecuzione, verificare che Data Defender sia in esecuzione e verificare che lo stream Data Defender sia configurato correttamente.

Prerequisito

Le seguenti procedure presuppongono che un'istanza Amazon EC2 sia già configurata. Per configurare un'istanza Amazon EC2 in AWS Ground Station, consulta Getting Started.

## Passaggio 1: verificare che l'istanza EC2 sia in esecuzione

1. Individua l'istanza Amazon EC2 utilizzata per il contatto per il quale stai risolvendo i problemi. Utilizza le fasi seguenti:
    a. Nella CloudFormationdashboard, seleziona lo stack che contiene l'istanza Amazon EC2.
    b. Scegli la scheda Risorse e individua la tua istanza Amazon EC2 nella colonna Logical ID. Verificare che l'istanza venga creata nella colonna Stato.
    c. Nella colonna ID fisico, scegli il link per la tua istanza Amazon EC2. Verrai reindirizzato alla console di gestione di Amazon EC2.
2. Nella console di gestione di Amazon EC2, assicurati che lo stato dell'istanza Amazon EC2 sia in esecuzione.

3. Se l'istanza è in esecuzione, procedere al passaggio successivo. Se l'istanza non è in esecuzione, avviare l'istanza utilizzando il seguente passaggio.

    - Con l'istanza Amazon EC2 selezionata, scegli Azioni > Stato dell'istanza > Avvia.

## Fase 2: Determinare il tipo di applicazione Dataflow utilizzata

Se utilizzi l'AWS Ground Station agente per la consegna dei dati, reindirizza alla sezione Troubleshooting Agent. AWS Ground Station

Altrimenti, se utilizzi l'applicazione Data Defender (DDX), continua a farlo. the section called "Passaggio 3: Verificare che Data Defender sia in esecuzione"

## Passaggio 3: Verificare che Data Defender sia in esecuzione

La verifica dello stato di Data Defender richiede la connessione alla tua istanza in Amazon EC2. Per ulteriori dettagli sulla connessione all'istanza, vedere Connettiti all'istanza Linux.

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

1. Apri un terminale o un prompt dei comandi e connettiti alla tua istanza Amazon EC2 utilizzando SSH. Porta di inoltro 80 dell'host remoto per visualizzare l'interfaccia utente web di Data Defender. I comandi seguenti mostrano come utilizzare SSH per connettersi a un'istanza Amazon EC2 tramite un bastione con il port forwarding abilitato.

    > **Note**
    >
    > È necessario sostituire <SSH KEY><BASTION HOST>e <HOST>con la chiave ssh specifica, il nome host bastion e il nome host dell'istanza Amazon EC2.

    Per Windows

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

    Per Mac

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

2. Verificare che Data Defender (chiamato anche DDX) sia in esecuzione grepping (controllo) per 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 Data Defender è in esecuzione, passa a the section called "Passaggio 4: verifica che Data Defender Stream sia configurato". In alternativa, passa alla fase successiva.

3. Avvia Data Defender utilizzando il comando show di seguito.

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

   Se Data Defender è in esecuzione dopo aver utilizzato il comando, passa a the section called "Passaggio 4: verifica che Data Defender Stream sia configurato". In alternativa, passa alla fase successiva.

4. Controlla i seguenti file utilizzando i comandi riportati di seguito per verificare se si sono verificati errori durante l'installazione e la configurazione di Data Defender.

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

   > **Note**
   >
   > Un problema comune rilevato durante l'ispezione di questi file è che l'Amazon VPC su cui è in esecuzione l'istanza Amazon EC2 non ha accesso ad Amazon S3 per scaricare i file di installazione. Se scopri nei tuoi log che questo è il problema, controlla le impostazioni Amazon VPC e del gruppo di sicurezza dell'istanza EC2 per assicurarti che non blocchino l'accesso ad Amazon S3.

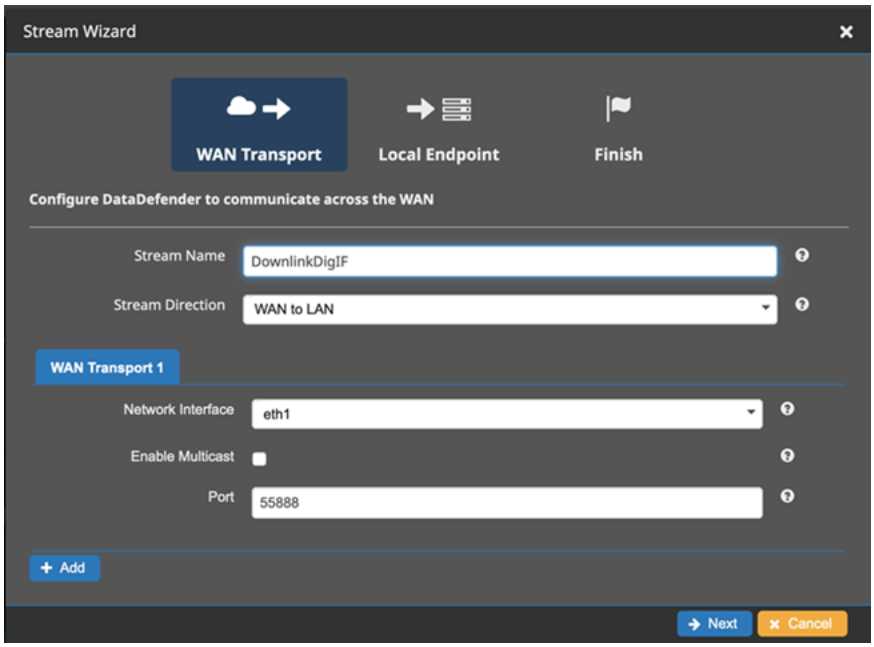
Se Data Defender è in esecuzione dopo aver verificato le impostazioni di Amazon VPC, continua a farlo. the section called “Passaggio 4: verifica che Data Defender Stream sia configurato”
Se il problema persiste, contatta AWS Support e invia i file di registro con una descrizione del problema.

## Passaggio 4: verifica che Data Defender Stream sia configurato

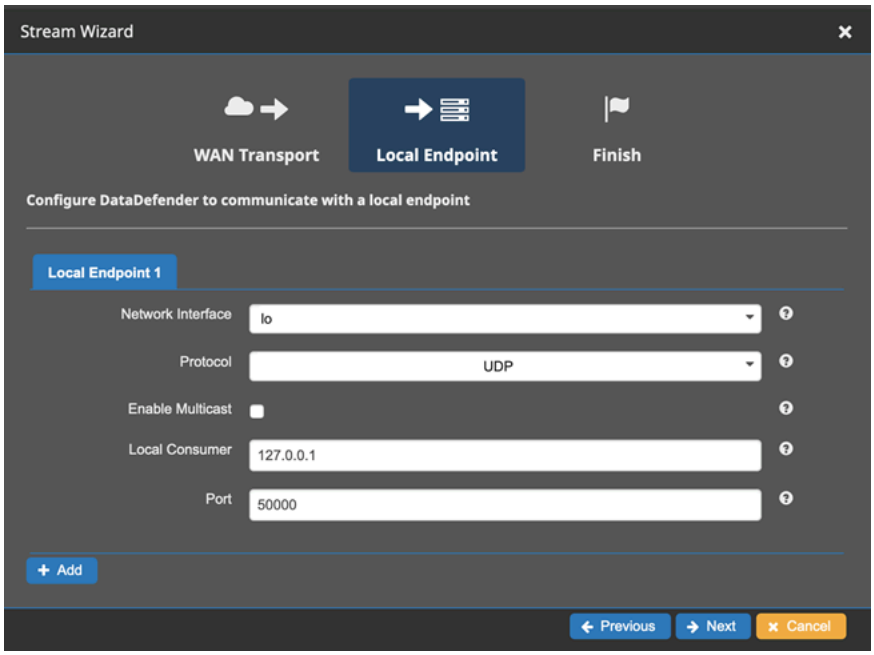
1. In un browser Web, accedere all'interfaccia utente Web DDX immettendo il seguente indirizzo nella barra degli indirizzi: localhost:8080 Quindi, premere Invio.
2. Nella DataDefenderdashboard, scegli Vai ai dettagli.
3. Seleziona il tuo flusso dall'elenco dei flussi e scegli Modifica flusso.
4. Nella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

   a. Nel riquadro WAN Transport (Trasporto WAN) verificare che WAN to LAN (Da WAN a LAN) sia selezionata per Stream Direction (Direzione flusso).

   b. Nella casella Port (Porta) verificare che la porta WAN scelta per il gruppo endpoint del flusso dati sia presente. Per impostazione predefinita, questa porta è 55888. Quindi, seleziona 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 sulla quale riceverai i dati dopo che Data Defender li avrà ricevuti dal AWS Ground Station servizio. 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 l'istanza Amazon EC2 e Data Defender siano entrambi in esecuzione e configurati correttamente per ricevere dati da. AWS Ground Station Se si continuano a riscontrare problemi, contattare il supporto AWS.

# Stati dei contatti di Ground Station

Lo stato di un AWS Ground Station contatto fornisce informazioni su cosa sta succedendo a quel contatto in un determinato momento.

## Stati dei contatti

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

- DISPONIBILE - Il contatto è disponibile per essere prenotato.
- PIANIFICAZIONE - Il contatto è in fase di pianificazione.

- PIANIFICATO: il contatto è stato pianificato con successo.
- FAILED_TO_SCHEDULE - Il contatto non è riuscito a pianificare.
- PREPASS - Il contatto inizierà presto 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.
- COMPLETATO - Il contatto è stato completato con successo.
- NON RIUSCITO: il contatto non è riuscito a causa di un problema con la configurazione delle risorse del cliente.
- AWS_FAILED - Il contatto non è riuscito a causa di un problema nel servizio. AWS Ground Station
- ANNULLAMENTO - Il contatto è in fase di cancellazione.
- AWS_CANCELLED - Il contatto è stato annullato dal servizio. AWS Ground Station La manutenzione dell'antenna o del sito è un esempio di quando ciò potrebbe accadere.
- ANNULLATO: il contatto è stato annullato dal cliente.

Guide per la risoluzione

- the section called “Risoluzione dei problemi relativi ai contatti con”
- the section called “Risoluzione dei problemi relativi ai contatti FAILED_TO_SCHEDULE”

## Risoluzione dei problemi relativi ai contatti con

Un contatto avrà lo stato di contatto terminale non riuscito quando AWS Ground Station viene rilevato un problema con la configurazione delle risorse del cliente. Di seguito sono riportati i casi d'uso più comuni che possono causare contatti non riusciti, insieme ai passaggi per la risoluzione dei problemi.

> **Note**
>
> Questa guida è specifica per lo stato del contatto FAILED e non è destinata ad altri stati di errore, come AWS_FAILED, AWS_CANCELLED o FAILED_TO_SCHEDULE. Per ulteriori informazioni sullo stato dei contatti, vedere the section called “Stati dei contatti di Ground Station”

## Casi d'uso non riusciti di Data Defender (DDX)

Di seguito è riportato l'elenco dei casi d'uso comuni che possono comportare lo stato di contatto NON RIUSCITO per i flussi di dati basati su DDX:

- Customer DDX non si connette mai - La connessione DDX tra AWS Ground Station Antenna e Customer Dataflow Endpoint Group per uno o più flussi di dati non è mai stata stabilita.
- Customer DDX Connects Late - La connessione DDX tra AWS Ground Station Antenna e Customer Dataflow Endpoint Group per uno o più flussi di dati è stata stabilita dopo l'orario di inizio del contatto.

Per qualsiasi caso di errore del flusso di dati DDX, si consiglia di esaminare quanto segue:

- Verifica che l'istanza Amazon EC2 del destinatario sia stata avviata correttamente, prima dell'orario di inizio del contatto.
- Verifica che il DDX fosse attivo e funzionante durante il contatto.

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

## AWS Ground Station Casi d'uso non riusciti dell'agente

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

- Customer Agent Never Reporting Status - L'agente responsabile dell'orchestrazione della consegna dei dati sul Customer 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.
- Customer Agent ha iniziato in ritardo - L'agente responsabile dell'orchestrazione della consegna dei dati sul Customer Dataflow Endpoint Group per uno o più flussi di dati è stato avviato in ritardo, dopo l'orario di inizio del contatto.

Per qualsiasi caso di errore del flusso di dati di AWS Ground Station Agent, si consiglia di esaminare quanto segue:

- Verifica che l'istanza Amazon EC2 del destinatario sia stata avviata correttamente, prima dell'orario di inizio del contatto.
- Verifica che l'applicazione Agent fosse attiva e funzionante all'inizio e durante il contatto.
- Verifica che l'applicazione Agent e l'istanza Amazon EC2 non siano state chiuse entro 15 secondi dalla fine del contatto. Ciò fornisce all'agente il tempo sufficiente per segnalare AWS Ground Station lo stato.

Consulta la sezione relativa the section called “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 contatti FAILED_TO_SCHEDULE

Un contatto sarà FAILED_TO_SCHEDULE quando AWS Ground Station rileva un problema con la configurazione delle risorse del cliente o all'interno del sistema interno. Un contatto che termina con uno stato FAILED_TO_SCHEDULE fornirà facoltativamente un contesto aggiuntivo. `errorMessage` Per informazioni sulla descrizione dei contatti, vedere. the section called “Descrivi un contatto con AWS CLI”

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

> **Note**
>
> Questa guida è specifica per lo stato dei contatti FAILED_TO_SCHEDULE e non è destinata ad altri stati di errore, come AWS_FAILED, AWS_CANCELLED o FAILED. Per ulteriori informazioni sugli stati dei contatti, consulta the section called “Stati dei contatti di Ground Station”

## Le impostazioni specificate in Antenna Downlink Demod Decode Config non sono supportate

Il profilo di missione utilizzato per pianificare questo contatto aveva una antenna-downlink-demod-decode configurazione non valida.

Configurazione esistente AntennaDownlinkDemodDecode in precedenza

- Se le tue antenna-downlink-demod-decode configurazioni sono state modificate di recente, torna a una versione funzionante in precedenza prima di provare a programmare.
- Se si tratta di una modifica intenzionale a una configurazione esistente o a una configurazione esistente in precedenza che non viene più pianificata correttamente, segui il passaggio successivo su come inserire una nuova configurazione. AntennaDownlinkDemodDecode

Configurazione appena creata AntennaDownlinkDemodDecode

Contattaci AWS Ground Station direttamente per aggiungere la tua nuova configurazione. Crea un caso con AWS Support, incluso `contactId` quello terminato nello stato FAILED_TO_SCHEDULE

## Risoluzione dei problemi generali

Se i passaggi precedenti per la risoluzione dei problemi non hanno risolto il problema:

- Riprova a pianificare il contatto o pianifica un altro contatto utilizzando lo stesso profilo di missione. Per informazioni, consulta the section called “Prenota un contatto con AWS CLI”.
- Se continui a ricevere lo stato FAILED_TO_SCHEDULE per questo profilo di missione, contatta AWS Support

# Sicurezza in AWS Ground Station

LaPer AWS, la sicurezza del cloud inhalaèmassimaprioritaria.priorità. In quanto cliente AWS, potrai trarre vantaggio da un'architettura di data center e di rete progettata per soddisfare i requisiti delle aziende più esigenti a livello di sicurezza. AWS fornisce strumenti e caratteristiche specifici per la sicurezza per aiutare a raggiungere gli obiettivi di sicurezza. Questi strumenti e caratteristiche includono sicurezza di rete, gestione della configurazione, controllo degli accessi e protezione dei dati.

Durante l'utilizzoAWS Ground Station, ti consigliamo di seguire le migliori pratiche del settore e implementare la end-to-end crittografia. AWS fornisce API per integrare la crittografia e la protezione dei dati. Per ulteriori informazioni sulla sicurezza AWS, consulta il whitepaper Introduzione alla sicurezza AWS .

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

Argomenti

- Identity and Access Management per AWS Ground Station
- Utilizzo di ruoli collegati ai servizi per Ground Station
- AWS Policy gestite da per AWS Ground Station

# Identity and Access Management per AWS Ground Station

AWS Identity and Access Management (IAM) è un Servizio AWS che consente agli amministratori di controllare in modo sicuro l'accesso alle risorse AWS. Gli amministratori IAM controllano chi è autenticato (accesso effettuato) e autorizzato (dispone di autorizzazioni) a utilizzare risorse AWS Ground Station. IAM è un Servizio AWS che è possibile utilizzare senza alcun costo aggiuntivo.

Argomenti

- Destinatari
- Autenticazione con identità
- Gestione dell'accesso con policy
- Funzionamento di AWS Ground Stationcon IAM
- Esempi di policy basate su identità per AWS Ground Station

- Risoluzione dei problemi di identità e accesso in AWS Ground Station

## Destinatari

Le modalità di utilizzo di AWS Identity and Access Management (IAM) cambiano in base alle operazioni eseguite in AWS Ground Station.

Utente del servizio: se utilizzi il servizio AWS Ground Station per eseguire il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. All'aumentare del numero di funzionalità AWS Ground Station utilizzate per il lavoro, potrebbero essere necessarie ulteriori autorizzazioni. 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 di identità e accesso in AWS Ground Station.

Amministratore del servizio: se sei il responsabile delle risorse AWS Ground Station presso la tua azienda, probabilmente disponi dell'accesso completo a AWS Ground Station. Il tuo compito è determinare le caratteristiche e le risorse AWS Ground Station a cui gli utenti del servizio devono accedere. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per ulteriori informazioni su come la tua azienda può utilizzare IAM con AWS Ground Station, consulta Funzionamento di AWS Ground Stationcon IAM.

Amministratore IAM: un amministratore IAM potrebbe essere interessato a ottenere dei dettagli su come scrivere policy per gestire l'accesso a AWS Ground Station. Per visualizzare policy basate su identità di AWS Ground Station di esempio che puoi utilizzare in IAM, consulta Esempi di policy basate su identità per AWS Ground Station.

## Autenticazione con identità

L'autenticazione è la procedura di accesso ad AWS con le credenziali di identità. Devi essere autenticato (connesso a AWS) come utente root Utente root dell'account AWS, come utente IAM o assumere un ruolo IAM.

Puoi accedere ad AWS come identità federata utilizzando le credenziali fornite attraverso un'origine di identità. Gli utenti AWS IAM Identity Center (Centro identità IAM), l'autenticazione Single Sign-On (SSO) dell'azienda e le credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Se accedi ad AWS tramite la federazione, assumi indirettamente un ruolo.

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

Se accedi ad AWS in modo programmatico, AWS fornisce un Software Development Kit (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le richieste utilizzando le tue credenziali. Se non utilizzi gli strumenti AWS, devi firmare le richieste personalmente. Per ulteriori informazioni sulla firma delle richieste, consulta Firma delle richieste AWS nella Guida per l'utente IAM.

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

### Utente root di un Account AWS

Quando crei un Account AWS, inizi con una singola identità di accesso che ha accesso completo a tutti i Servizi AWS e le risorse nell'account. Tale identità è detta utente root Account AWS ed è possibile accedervi 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 utilizzarle per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente di IAM.

### Identità federata

Come best practice, richiedi agli utenti umani, compresi quelli che richiedono l'accesso di amministratore, di utilizzare la federazione con un provider di identità per accedere a Servizi AWSutilizzando credenziali temporanee.

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

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. È possibile creare utenti e gruppi in IAM Identity Center oppure connettersi e sincronizzarsi con un

gruppo di utenti e gruppi nell'origine di identità per utilizzarli in tutte le applicazioni e gli Account AWS. Per ulteriori informazioni sul Centro identità IAM, consulta Cos'è Centro identità IAM? nella Guida per l'utente di AWS IAM Identity Center.

## Utenti e gruppi IAM

Un utente IAM è una identità all'interno del tuo Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, per casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente di IAM.

Un gruppo IAM 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 avere un gruppo denominato Amministratori IAM e concedere a tale gruppo le autorizzazioni per amministrare le risorse IAM.

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 utente IAM (invece di un ruolo) nella Guida per l'utente di IAM.

## Ruoli IAM

Un ruolo IAM è un'identità all'interno di un Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. È possibile assumere temporaneamente un ruolo IAM nella AWS Management Console mediante lo scambio di ruoli. È possibile assumere un ruolo chiamando un'azione AWS CLI o API AWS oppure utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente di IAM.

I ruoli IAM 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 ulteriori informazioni sulla federazione dei ruoli, consulta Creazione di un ruolo per un provider di identità di terza parte nella Guida per l'utente di IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per ulteriori informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center.

- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, per alcuni dei Servizi AWS, è possibile collegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.
- Accesso multi-servizio: alcuni Servizi AWS utilizzano funzionalità in altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è comune che tale 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.
  - Inoltro delle sessioni di accesso (FAS): quando si utilizza un utente o un ruolo IAM per eseguire operazioni in AWS, tale utente o ruolo viene considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra azione in un servizio diverso. FAS utilizza le autorizzazioni del principale che effettua la chiamata a un Servizio AWS, combinate con il Servizio AWS richiedente, per effettuare richieste a servizi a valle. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che necessita di interazioni con altri Servizi AWS o risorse per essere portata a termine. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è un ruolo IAM assunto da un servizio per eseguire operazioni per conto dell'utente. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.
  - Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un Servizio AWS. Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli

collegati ai servizi sono visualizzati nell'account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

- Applicazioni in esecuzione su Amazon EC2: è possibile utilizzare un ruolo IAM per gestire credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 che eseguono richieste di AWS CLIo dell'API AWS. Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un ruolo AWS a un'istanza EC2, affinché sia disponibile per tutte le relative applicazioni, puoi creare un profilo dell'istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente di IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta Quando creare un ruolo IAM (invece di un utente) nella Guida per l'utente di IAM.

## Gestione dell'accesso con policy

Per controllare l'accesso a AWS è possibile creare policy e collegarle a identità o risorse AWS. Una policy è un oggetto in AWS che, quando associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste policy quando un principale IAM (utente, utente root o sessione ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle policy viene archiviata in AWSsotto forma di documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente di IAM.

Gli amministratori possono utilizzare le policy AWSJSON per specificare l'accesso ai diversi elementi. 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 amministratore IAM può creare policy IAM. Successivamente l'amministratore può aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'azione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dalla AWS Management Console, la AWS CLI o l'API AWS.

## Policy basate su identità

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

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono incorporate direttamente in un singolo utente, gruppo o ruolo. Le policy gestite sono policy autonome che possono essere collegate a più utenti, gruppi e ruoli in Account AWS. Le policy gestite includono le policy gestite da AWS e le policy gestite dal cliente. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente di IAM.

## Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile allegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è allegata 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 Servizi AWS.

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

## Liste di controllo degli accessi (ACL)

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

Amazon S3, AWS WAF e Amazon VPC sono esempi di servizi che supportano le ACL. Per maggiori informazioni sulle ACL, consulta Panoramica delle liste di controllo degli accessi (ACL) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

## Altri tipi di policy

AWS supporta altri tipi di policy 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 delle autorizzazioni è una funzione avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo 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 IAM nella Guida per l'utente di IAM.
- Policy di controllo dei servizi (SCP): le SCP sono policy JSON che specificano il numero massimo di autorizzazioni per un'organizzazione o unità organizzativa (OU) in AWS Organizations. AWS Organizationsè un servizio per il raggruppamento e la gestione centralizzata degli Account AWSmultipli di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. La SCP limita le autorizzazioni per le entità negli account membri, compreso ogni Utente root dell'account AWS. Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations.
- 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 Policy di sessione nella Guida per l'utente di IAM.

## 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 AWSdetermina se consentire una richiesta quando sono coinvolti più tipi di policy, consultare Logica di valutazione delle policy nella Guida per l'utente di IAM.

# Funzionamento di AWS Ground Stationcon IAM

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

Funzionalità IAM che è possibile utilizzare con AWS Ground Station

| Funzionalità IAM | Supporto di AWS Ground Station |
|---|---|
| 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 |
| Liste di controllo degli accessi (ACL) | No |
| ABAC (tag nelle policy) | Sì |
| Credenziali temporanee | Sì |
| Autorizzazioni del principale | Sì |
| ☻Ruoli di servizio | No |
| Ruoli collegati al servizio | Sì |

Per ottenere un quadro generale del funzionamento di AWS Ground Stationde altri servizi AWScon la maggior parte delle caratteristiche di IAM, consulta Servizi AWSsupportati da IAM nella Guida per l'utente IAM.

## Policy basate su identità per AWS Ground Station

| | |
|---|---|
| Supporta le policy basate su identità | Sì |

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

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

Esempi di policy basate su identità per AWS Ground Station

Per visualizzare esempi di policy basate su identità AWS Ground Station, consulta Esempi di policy basate su identità per AWS Ground Station.

## Policy basate su risorse all'interno di AWS Ground Station

| | |
|---|---|
| Supporta le policy basate su risorse | No |

Le policy basate su risorse sono documenti di policy JSON che è possibile allegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è allegata 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 Servizi AWS.

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy 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 l'entità principale e la risorsa si trovano in diversi Account AWS, un amministratore IAM nell'account attendibile deve concedere all'entità principale (utente o ruolo) anche l'autorizzazione per 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 Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente IAM.

## Operazioni di policy per AWS Ground Station

| | |
|---|---|
| Supporta le azioni di policy | Sì |

Gli amministratori possono utilizzare le policy JSON AWS per specificare gli accessi ai diversi elementi. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le azioni di policy hanno spesso lo stesso nome dell'operazione API AWS. Ci sono alcune eccezioni, ad esempio le azioni di sola autorizzazione che non hanno un'operazione API corrispondente. 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 delle azioni di AWS Ground Station, consulta Operazioni definite da AWS Ground Station nella Guida di riferimento per l'autorizzazione del servizio.

Le operazioni delle policy in AWS Ground Station utilizzano il seguente prefisso prima dell'operazione:

```
groundstation
```

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

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

Per visualizzare esempi di policy basate su identità AWS Ground Station, consulta Esempi di policy basate su identità per AWS Ground Station.

## Risorse relative alle policy per AWS Ground Station

| | |
|---|---|
| Supporta le risorse di policy | Sì |

Gli amministratori possono utilizzare le policy JSON AWS per specificare gli accessi ai diversi elementi. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'azione. Le istruzioni devono includere un elemento `Resource` o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (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 di tipi di risorse AWS Ground Station e dei relativi ARN, consulta Risorse definite da AWS Ground Station nella Guida di riferimento sull'autorizzazione del servizio. Per informazioni sulle operazioni con cui è possibile specificare l'ARN di ogni risorsa, consulta la sezione Operazioni definite da AWS Ground Station.

Per visualizzare esempi di policy basate su identità AWS Ground Station, consulta Esempi di policy basate su identità per AWS Ground Station.

## Chiavi di condizione delle policy per AWS Ground Station

| | |
|---|---|
| Supporta le chiavi di condizione delle policy specifiche del servizio | Sì |

Gli amministratori possono utilizzare le policy JSON AWS per specificare gli accessi ai diversi elementi. 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 specifichi più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione `OR` logica. 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, puoi autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

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

Per visualizzare un elenco di chiavi di condizione AWS Ground Station, consulta Chiavi di condizione per AWS Ground Station nella Guida di riferimento sull'autorizzazione del servizio. Per informazioni su operazioni e risorse con cui è possibile utilizzare una chiave di condizione, consulta la sezione Operazioni definite da AWS Ground Station.

Per visualizzare esempi di policy basate su identità AWS Ground Station, consulta Esempi di policy basate su identità per AWS Ground Station.

## Liste di controllo degli accessi in AWS Ground Station

| | |
|---|---|
| Supporta le ACL | No |

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni ad accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

## ABAC con AWS Ground Station

| | |
|---|---|
| Supporta ABAC (tag nelle policy) | Sì |

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, tali attributi sono denominati tag. È possibile collegare dei tag alle entità IAM (utenti o ruoli) e a numerose risorse AWS. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

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 su ABAC, consulta Che cos'è ABAC? nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

## Utilizzo di credenziali temporanee con AWS Ground Station

| | |
|---|---|
| Supporta le credenziali temporanee | Sì |

Alcuni Servizi AWS non funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, inclusi i Servizi AWS che funzionano con le credenziali temporanee, consulta Servizi AWS supportati da IAM nella Guida per l'utente IAM.

Le credenziali temporanee sono utilizzate se si accede alla AWS Management Console utilizzando qualsiasi metodo che non sia la combinazione di nome utente e password. Ad esempio, quando accedi ad AWS utilizzando il collegamento Single Sign-On (SSO) della tua azienda, tale processo crea in automatico credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta Cambio di un ruolo (console) nella Guida per l'utente di IAM.

È possibile creare manualmente credenziali temporanee utilizzando la AWS CLIo l'API AWS. È quindi possibile utilizzare tali credenziali temporanee per accedere ad AWS. AWSconsiglia di generare le

credenziali temporanee dinamicamente anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza provvisorie in IAM.

## Autorizzazioni del principale tra servizi per AWS Ground Station

| | |
|---|---|
| Supporta sessioni di accesso diretto (FAS) | Sì |

Quando si utilizza un utente o un ruolo IAM per eseguire operazioni in AWS, si viene considerati un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'azione che attiva un'altra azione in un servizio diverso. FAS utilizza le autorizzazioni del principale che effettua la chiamata a un Servizio AWS, combinate con il Servizio AWS richiedente, per effettuare richieste a servizi a valle. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che necessita di interazioni con altri Servizi AWS o risorse per essere portata a termine. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Inoltro sessioni di accesso.

## Ruoli di servizio per AWS Ground Station

| | |
|---|---|
| Supporta i ruoli di servizio | No |

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWSnella Guida per l'utente IAM.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe compromettere la funzionalità di AWS Ground Station. Modifica i ruoli di servizio solo quando AWS Ground Station fornisce le indicazioni per farlo.

## Ruoli collegati ai servizi per l'AWS Ground Station

| | |
|---|---|
| Supporta i ruoli collegati ai servizi | Sì |

Un ruolo collegato ai servizi è un tipo di ruolo di servizio che è collegato a un Servizio AWS. Il servizio può assumere il ruolo per eseguire un'operazione per tuo conto. I ruoli collegati ai servizi sono visualizzati nell'account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

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

## Esempi di policy basate su 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 sono in grado di eseguire attività utilizzando la AWS Management Console, l'AWS Command Line Interface (AWS CLI) o l'API AWS. Per concedere agli utenti l'autorizzazione per eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

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

Per informazioni dettagliate sulle azioni e sui tipi di risorse definiti da AWS Ground Station, incluso il formato degli ARN per ogni tipo di risorsa, consulta Operazioni, risorse e chiavi di condizione per AWS Ground Station nella Guida di riferimento per l'autorizzazione del servizio.

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 policy basate su identità determinano se qualcuno può creare, accedere o eliminare risorse AWS Ground Station nel tuo account. Queste operazioni possono comportare costi aggiuntivi per l'Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Nozioni di base sulle policy gestite da AWSe passaggio alle autorizzazioni con privilegio minimo: per le informazioni di base su come concedere autorizzazioni a utenti e carichi di lavoro, utilizza le policy gestite da AWSche concedono le autorizzazioni per molti casi d'uso comuni. Sono disponibili nel tuo Account AWS. Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente di AWSspecifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste 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 di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi inoltre utilizzare le condizioni per concedere l'accesso alle operazioni di servizio, ma solo se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per IAM Access Analyzer nella Guida per l'utente di IAM.
- Richiesta dell'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o utenti root nel tuo Account AWS, attiva MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Configurazione dell'accesso alle API protetto con MFA nella Guida per l'utente di IAM.

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

## Utilizzo della console di AWS Ground Station

Per accedere alla console AWS Ground Station è necessario disporre di un insieme di autorizzazioni minimo. Queste autorizzazioni devono consentire di elencare e visualizzare i dettagli relativi alle risorse AWS Ground Station nel 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 le autorizzazioni minime della console agli utenti che effettuano chiamate solo alla AWS CLI o all'API AWS. Al contrario, concedi l'accesso solo alle operazioni che corrispondono all'operazione API che stanno cercando di eseguire.

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

## Consentire agli utenti di visualizzare le loro autorizzazioni

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

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

```
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

## Risoluzione dei problemi di identità e accesso in AWS Ground Station

Utilizza le informazioni seguenti per diagnosticare e risolvere i problemi comuni che possono verificarsi durante l'utilizzo di AWS Ground Station e di IAM.

Argomenti

- Non sono autorizzato a eseguire un'operazione in AWS Ground Station
- Non sono autorizzato a eseguire iam: PassRole
- Voglio consentire alle persone esterne al mio account Account AWSdi accedere alle mie risorse AWS Ground Station

### Non sono autorizzato a eseguire un'operazione in AWS Ground Station

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

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

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

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

Per ulteriore assistenza con l'accesso, 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 Servizi AWS consentono di passare un ruolo esistente a tale servizio, invece di creare un nuovo ruolo di servizio o un ruolo collegato ai servizi. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

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

Per ulteriore assistenza con l'accesso, contatta l'amministratore AWS. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

## Voglio consentire alle persone esterne al mio account Account AWSdi accedere alle mie risorse AWS Ground Station

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 servizi che supportano policy basate su risorse o liste di controllo accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per capire se AWS Ground Station supporta queste funzionalità, consulta Funzionamento di AWS Ground Stationcon IAM.

- Per informazioni su come garantire l'accesso alle risorse negli Account AWSche possiedi, consulta Fornire l'accesso a un utente IAM in un altro Account AWS in tuo possesso nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso alle risorse ad Account AWS di terze parti, consulta Fornire l'accesso agli Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente di IAM.
- Per informazioni sulle differenze tra l'utilizzo di ruoli e policy basate su risorse per l'accesso multi-account, consultare Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

# Utilizzo di ruoli collegati ai servizi per Ground Station

AWS Ground Station utilizza ruoli collegati al servizio AWS Identity and Access Management (IAM). Un ruolo collegato ai servizi è un tipo di ruolo IAM univoco collegato direttamente a Ground Station. I ruoli collegati ai servizi sono definiti automaticamente da Ground Station e includono tutte le autorizzazioni richieste dal servizio per eseguire chiamate agli altriAWS servizi per tuo conto.

Un ruolo collegato ai servizi semplifica la configurazione di Ground Station perché ti permette di evitare l'aggiunta manuale delle autorizzazioni necessarie. Ground Station definisce le autorizzazioni dei relativi ruoli collegati ai servizi e, salvo diversamente definito, solo Ground Station potrà assumere i propri ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consulta Servizi AWS che funzionano con IAM e cerca i servizi che riportano Yes (Sì) nella colonna Service-linked roles (Ruoli collegati ai servizi). Scegli Yes (Sì) in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

## Autorizzazioni del ruolo collegato ai servizi per Ground Station

Ground Station usa il ruolo collegato ai servizi denominato AWSServiceRoleForGroundStationDataflowEndpointGroup: Aws GroundStation usa questo ruolo collegato ai servizi per richiamare EC2 per trovare gli indirizzi IPv4 pubblici.

Ai fini dell' AWSServiceRoleForGroundStationDataflowEndpointGroup assunzione del ruolo, il ruolo collegato ai servizi considera attendibili i seguenti servizi:

- `groundstation.amazonaws.com`

La policy delle autorizzazioni del ruolo denominata AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy consente a Ground Station di eseguire le seguenti operazioni sulle risorse specificate:

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

  L'azione consente a Ground Station di elencare tutti gli IP associati agli EIP.

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

  L'azione consente a Ground Station di ottenere informazioni sulle interfacce di rete associate alle istanze EC2

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

## Creazione di un ruolo collegato ai servizi per Ground Station

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando creiAWS CLI un DataflowEndpointGroup ruolo collegato ai serviziAWS, Ground Station crea automaticamente il ruolo collegato ai servizi.

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 di nuovo il ruolo collegato ai servizi automaticamente.

È possibile utilizzare la console IAM anche per creare un ruolo collegato ai servizi con il caso d'uso Data Delivery to Amazon EC2. In AWS CLI o in AWS API, crea un ruolo collegato ai servizi con il nome di servizio `groundstation.amazonaws.com`. Per ulteriori informazioni, consulta Creazione di un ruolo collegato ai servizi nella Guida per l'utente IAM. Se elimini il ruolo collegato ai servizi, puoi utilizzare lo stesso processo per crearlo nuovamente.

## Modifica di un ruolo collegato ai servizi per Ground Station

Ground Station non consente di modificare il ruolo AWSServiceRoleForGroundStationDataflowEndpointGroup collegato ai servizi. Dopo aver creato

un ruolo collegato ai servizi, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

## Eliminazione di un ruolo collegato ai servizi per Ground Station

Se non è più necessario utilizzare una caratteristica o un servizio che richiede un ruolo collegato ai servizi, 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 ai servizi solo dopo aver eliminato il DataflowEndpointGroups ruolo collegato ai servizi. Questo ti protegge dalla possibilità di revocare inavvertitamente le autorizzazioni del tuo DataflowEndpointGroups. Se un ruolo collegato ai servizi viene utilizzato con più ruoli DataflowEndpointGroups, è necessario eliminare tutti quelli DataflowEndpointGroups che utilizzano tale ruolo collegato ai servizi, prima di poterlo eliminare.

> **Note**
>
> Se il servizio Ground Station utilizza tale ruolo quando provi a eliminare le risorse, è possibile che l'eliminazione abbia esito negativo. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare le risorse della Ground Station utilizzate dal AWSServiceRoleForGroundStationDataflowEndpointGroup

- Elimina DataflowEndpointGroups tramite l'interfaccia a riga di comando di AWS o l'API AWS.

Per eliminare manualmente il ruolo collegato ai servizi utilizzando IAM

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

## Regioni supportate per i ruoli collegati ai servizi Ground Station

Ground Station supporta l'utilizzo di ruoli collegati ai servizi in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, consultate ate ate la tabella delle regioni.

## Risoluzione dei problemi

`NOT_AUTHORIZED_TO_CREATE_SLR`- Ciò indica che il ruolo nel tuo account utilizzato per chiamare l' CreateDataflowEndpointGroup API non dispone dell'`iam:CreateServiceLinkedRole`autorizzazione. Un amministratore con l'`iam:CreateServiceLinkedRole`autorizzazione deve creare manualmente il ruolo collegato al servizio per il tuo account.

# AWS Policy gestite da per AWS Ground Station

UnAWSla policy gestita è una politica autonoma creata e amministrata daAWS.AWSle policy 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 cheAWSle policy gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i casi d'uso specifici perché sono disponibili per tuttiAWSclienti da utilizzare. Ti consigliamo di ridurre ulteriormente le autorizzazioni definendopolitiche gestite dai clientiche sono specifici per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle policy gestite da AWS. SeAWSaggiorna le autorizzazioni definite in unAWSpolicy gestita, l'aggiornamento riguarda tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la policy.AWSè molto probabile che aggiorni unAWSpolitica gestita quando è nuovaServizio AWSviene avviato o nuove operazioni API diventano disponibili per i servizi esistenti.

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

## AWSPolicy gestita: AWSGroundStationAgentInstancePolicy

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

Questa policy concede le autorizzazioni di AWS Ground Station Agent a un'istanza cliente che consentono all'istanza di inviare e ricevere dati durante i contatti con la Ground Station. Tutte le autorizzazioni contenute in questa politica provengono dal servizio Ground Station.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `groundstation`— Consente alle istanze degli endpoint di dataflow di chiamare le API di Ground Station Agent.

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

## AWSPolicy gestita: AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy

Non è possibile collegare AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy alle entità IAM. Questa policy è associata a un ruolo collegato ai servizi che consente a AWS Ground Station di eseguire operazioni per tuo conto. Per ulteriori informazioni, vedereUtilizzo di ruoli collegati al servizio.

Questa politica concede le autorizzazioni EC2 che consentonoAWS Ground Stationper trovare indirizzi IPv4 pubblici.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `ec2:DescribeAddresses`— PermetteAWS Ground Stationper elencare tutti gli IP associati agli EIP per tuo conto.
- `ec2:DescribeNetworkInterfaces`— PermetteAWS Ground Stationper ottenere informazioni sulle interfacce di rete associate alle istanze EC2 per tuo conto.

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

## Aggiornamenti di AWS Ground Station alle policy gestite da AWS

Visualizza i dettagli sugli aggiornamenti alle policy gestite da AWS per AWS Ground Station da quando questo servizio ha iniziato a tenere traccia delle modifiche. Per gli avvisi automatici sulle modifiche apportate a questa pagina, sottoscrivi il feed RSS nella pagina della cronologia dei documenti di AWS Ground Station.

| Modifica | Descrizione | Data |
| --- | --- | --- |
| AWSGroundStationAgentInstancePolicy: nuova policy | AWS Ground Stationha aggiunto una nuova policy per fornire le autorizzazioni all'istanza dell'endpoint Dataflow per utilizzare AWS Ground Station Agent. | 12 aprile 2023 |
| AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy: nuova policy | AWS Ground Stationè stata aggiunta una nuova politica che concede a EC2 le autorizzazioni necessarieAWS Ground Stationper trovare gli indirizzi IPv4 pubblici associati agli EIP e le interfacce di rete associate alle istanze EC2. | 02 novembre 2022 |
| AWS Ground Station ha iniziato il rilevamento delle modifiche | AWS Ground Station ha iniziato a monitorare le modifiche per le policy gestite da AWS. | 1 marzo 2021 |

# Crittografia dei dati a riposo per AWS Ground Station

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

- Chiavi di proprietà di AWS: 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 proprietà di AWS 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 le chiavi di proprietà di AWS 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 le policy e le sovvenzioni IAM
  - Abilitare e disabilitare le policy delle chiavi
  - Ruotare i materiali crittografici delle chiavi
  - Aggiungere tag
  - Creare alias delle chiavi
  - Pianificare l'eliminazione delle chiavi

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

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

| Tipo di dati | Crittografia con chiavi di proprietà di AWS | 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, si applicano le tariffe AWS KMS per l'utilizzo di una chiave gestita dal cliente. Per informazioni sui prezzi, consulta Prezzi di AWS Key Management Service.
> Per ulteriori informazioni su AWS KMS, consulta la AWS KMS Developer Guide.

## Come AWS Ground Station utilizza le sovvenzioni in KMS AWS

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 KMS. CreateGrant AWS Le sovvenzioni in AWS KMS vengono utilizzate per AWS Ground Station consentire l'accesso a una chiave KMS in un account cliente.

AWS Ground Station richiede la concessione per utilizzare la chiave gestita dal cliente per le seguenti operazioni interne:

- Invia `GenerateDataKey` richieste a AWS KMS per generare chiavi dati crittografate dalla chiave gestita dal cliente.
- Invia `Decrypt` richieste a AWS KMS per decrittografare le chiavi dati crittografate in modo che possano essere utilizzate per crittografare i tuoi dati.
- Invia `Encrypt` richieste a AWS KMS per 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 farà sì che il contatto finisca in uno stato NON RIUSCITO.

# Creazione di una chiave gestita dal cliente

È possibile creare una chiave simmetrica gestita dal cliente utilizzando la console di AWS gestione o le API AWS KMS.

## Per creare una chiave simmetrica gestita dal cliente

Segui i passaggi per la creazione di una chiave simmetrica gestita dal cliente nella Key Management Service Developer Guide AWS .

## 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 operazioni API:

`kms:CreateGrant`- Aggiunge una concessione a una chiave gestita dal cliente. Concede il controllo dell'accesso a una chiave KMS specificata, che consente l'accesso alle operazioni AWS Ground Station di concessione 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 `GenerateDataKey` per generare una chiave dati crittografata e archiviarla, poiché la chiave dati non viene utilizzata immediatamente per crittografare.
- Chiama `Decrypt` per utilizzare la chiave dati crittografata memorizzata per accedere ai dati crittografati.

- Chiama `Encrypt` per utilizzare la chiave dati per crittografare i dati.
- 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 di dichiarazioni di policy IAM 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 policy, 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 dal cliente AWS KMS

# 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 KMS utilizza il contesto di crittografia come dati autenticati aggiuntivi per supportare la crittografia autenticata. Quando includi un contesto di crittografia in una richiesta di crittografia dei dati, AWS KMS associa il contesto di crittografia ai dati crittografati. Per decrittografare i dati, nella richiesta deve essere incluso lo stesso contesto di crittografia.

## AWS Ground Station 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 Ephemeris:

Le chiavi concesse per la crittografia delle risorse effemeridi sono legate a uno specifico ARN satellitare

```
"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

È possibile utilizzare il contesto di crittografia nelle policy delle chiavi e nelle policy IAM come `conditions` per controllare l'accesso alla chiave simmetrica gestita dal cliente. È possibile utilizzare i vincoli del contesto di crittografia in una concessione.

AWS Ground Station utilizza un vincolo di contesto di crittografia nelle concessioni per controllare l'accesso alla chiave gestita dal cliente nel tuo account o nella tua regione. Il vincolo della concessione richiede che le operazioni consentite dalla concessione utilizzino il contesto di crittografia specificato.

Di seguito sono riportati alcuni esempi di istruzioni delle policy 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 dal cliente AWS KMS 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 le operazioni KMS chiamate da AWS Ground Station per accedere ai dati crittografati dalla chiave gestita dal cliente.

## **`CreateGrant`**(Cloudtrail)

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

# 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 effemeridi. AWS Ground Station

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 linee associati all'ID NORAD del satellite. Tutte le effemeridi predefinite hanno una priorità pari a 0. Di conseguenza, verranno sostituite, sempre, da tutte le effemeridi personalizzate non scadute caricate tramite l'API ephemeris, che deve sempre avere una priorità pari o superiore a 1.

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

# Quali effemeridi vengono utilizzate

Le effemeridi hanno una priorità, una data di scadenza e una bandiera abilitata. 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. Gli orari di contatto disponibili restituiti da si basano su queste effemeridi. ListContacts 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

Utilizza l'DescribeContact API per 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 l'DescribeContact API, puoi determinare la parte dei tuoi contatti futuri che è inutilizzabile a causa del veicolo spaziale che opera al di fuori della maschera del sito di trasmissione/ricezione confrontando il contatto programmato `endTime` con quello restituito `startTime` e. `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, consulta: Domande frequenti su Ground Station.

## 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. `GetSatellite` `ListSatellites` 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 AWS Ground Station calcolare la traiettoria del satellite.

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

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

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

```
{
    "satelliteId": "e1cfe0c7-67f9-4d98-bad2-06dbfc2d14a2",
    "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"
      }
  }
```

# Fornitura di dati sulle effemeridi personalizzati

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

L'accesso all'API Ephemeris viene fornito solo in base alle necessità. I clienti che richiedono la possibilità di caricare dati personalizzati sulle effemeridi devono contattare aws-groundstation@amazon.com.

## Panoramica

L'API Ephemeris consente di caricare effemeridi personalizzate da utilizzare con un satellite. AWS Ground Station [Queste effemeridi sostituiscono le effemeridi predefinite di Space Track (vedi: Default Ephemeris Data).]

Il caricamento delle effemeridi destinate ai clienti 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

## Creazione di effemeridi personalizzate

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

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

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

## Crea un set di effemeridi TLE tramite API

Il client AWS Ground Station boto3 può essere utilizzato per caricare un set di effemeridi a due elementi di linea (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).

Un set TLE è un oggetto in formato JSON che unisce uno o più TLE per costruire una traiettoria continua. I TLE nel set TLE devono formare un insieme continuo che possiamo usare per costruire una traiettoria (cioè nessun intervallo di tempo tra i TLE in un set TLE). Di seguito è riportato un set TLE di esempio:

```
# 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 dei TLE in un set TLE devono corrispondere esattamente per essere una traiettoria valida e continua.

Un set TLE 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 ID delle effemeridi che può essere utilizzato per fare riferimento alle effemeridi in futuro. Ad esempio, possiamo utilizzare l'ID delle effemeridi fornito nella chiamata precedente per verificare lo stato delle effemeridi:

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

Di seguito viene fornito un esempio di risposta derivante dall'azione `DescribeEphemeris`

```
{
  "creationTime": 1620254718.765,
  "enabled": true,
  "name": "Example Ephemeris",
  "ephemerisId": "fde41049-14f7-413e-bd7b-EXAMPLE01",
  "priority": 2,
  "status": "VALIDATING",
  "suppliedData": {
    "tle": {
      "ephemerisData": "[{\"tleLine1\": \"1 25994U 99068A   20318.54719794  .00000075
 00000-0  26688-4 0  9997\",\"tleLine2\": \"2 25994  98.2007  30.6589 0001234  89.2782
  18.9934 14.57114995111906\",\"validTimeRange\": {\"startTime\": 1620254712000,
\"endTime\": 1620859512000}}]"
    }
  }
}
```

Si consiglia di eseguire il polling del `DescribeEphemeris` percorso o utilizzare gli eventi di Cloudwatch per tenere traccia dello stato delle effemeridi caricate, poiché deve passare attraverso un flusso di lavoro di convalida asincrono prima di essere impostato e diventare utilizzabile per la pianificazione e l'esecuzione dei contatti. `ENABLED`

Nota che l'ID NORAD presente in tutti i TLE del set TLE, negli esempi precedenti, deve corrispondere all'ID NORAD assegnato al satellite `25994` nel database Space Track.

## Caricamento dei dati Ephemeris da un bucket S3

È anche possibile caricare un file ephemeris 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 inattivi 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 effemeridi OEM da un bucket S3

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

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

```
{
    "creationTime": 1620254718.765,
    "enabled": true,
    "name": "Example Ephemeris",
    "ephemerisId": "fde41049-14f7-413e-bd7b-EXAMPLE02",
    "priority": 2,
    "status": "VALIDATING",
    "suppliedData": {
    "oem": {
        "sourceS3Object": {
            "bucket": "ephemeris-bucket-for-testing",
            "key": "test_data.oem"
        }
    }
}
```

# Risoluzione dei problemi di effemeridi non validi

Quando viene caricata un'effemeride personalizzata,AWS Ground Station viene sottoposta a un flusso di lavoro di convalida asincrono prima di diventare`ENABLED`. Questo flusso di lavoro garantisce che gli identificatori satellitari, i metadati e la traiettoria siano validi.

Quando un'effemeride fallisce la convalida,`DescribeEphemeris` restituirà un EphemerisInvalidReason, che fornisce informazioni sul motivo per cui le effemeridi hanno fallito la convalida. I valori potenziali di EphemerisInvalidReasonsono i seguenti:

| Value (Valore) | Descrizione | Risoluzione dei problemi di |
|---|---|---|
| METADATA_INVALID | Gli identificatori del veicolo spaziale forniti, come l'ID del satellite, non sono validi | Controlla l'ID NORAD o altri identificatori forniti nei dati delle effemeridi |
| INTERVALLO TEMPORALE _INVALID | Gli orari di inizio, fine o scadenza non sono validi per le effemeridi fornite | Assicurati che l'ora di inizio sia precedente a `ora` (si consiglia di impostare l'ora di inizio qualche minuto in 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 di un veicolo spaziale non valida | Verificare che la traiettoria fornita sia continua e sia per il satellite corretto. |
| ERRORE DI CONVALIDA | Si è verificato un errore interno del servizio durante l'elabora zione delle effemeridi per la convalida | nuovo caricamento |

Di seguito viene fornito un esempio di`DescribeEphemeris` risposta per`INVALID` un'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"
      }
    }
  },
}
```

## Ripristino dei dati predefiniti sulle effemeridi

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

Per ripristinare le effemeridi Space Track predefinite, è necessario eseguire una delle seguenti operazioni:

- Eliminare (utilizzare`DeleteEphemeris`) o disabilitare (utilizzare`UpdateEphemeris`) tutte le effemeridi abilitate fornite dal cliente. 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 `GetSatellite` e verificando che quella delle effemeridi correnti per il satellite sia. `source` `SPACE_TRACK` Vedi Default Ephemeris Data per ulteriori informazioni sulle effemeridi predefinite.

# AWS Ground Station Maschere del sito

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

- Caratteristiche del terreno geografico che circonda l'antenna. Ad esempio, ciò include elementi come montagne o edifici che bloccherebbero un segnale a radiofrequenza (RF) o impedirebbero la trasmissione.
- Interferenza a radiofrequenza (RFI) Ciò influisce sia sulla capacità di ricezione (sorgenti RFI esterne che influiscono su un segnale di downlink nelle antenne AWS Ground Station) sia sulla capacità di trasmissione (il segnale RF trasmesso dalle antenne di AWS Ground Station con un impatto negativo sui ricevitori esterni).
- Autorizzazioni legali. Le autorizzazioni dei siti locali per utilizzare AWS Ground Station in ciascuna regione possono includere restrizioni specifiche, come un angolo di elevazione minimo per la trasmissione.

Queste maschere del sito possono cambiare nel tempo. Ad esempio, è possibile costruire nuovi edifici vicino a un'antenna, le sorgenti RFI potrebbero cambiare o l'autorizzazione legale potrebbe essere rinnovata con diverse restrizioni. Le maschere del sito AWS Ground Station sono disponibili per i clienti 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, ogni cliente può disporre di maschere aggiuntive a causa delle restrizioni sulla propria autorizzazione legale a comunicare con i propri satelliti in una determinata regione. Tali maschere possono essere configurate in AWS Ground Station per case-by-case garantire la conformità quando si utilizza AWS Ground Station per comunicare con questi satelliti. Contatta il team di AWS Ground Station per ulteriori dettagli.

## Impatto delle maschere del sito sugli orari di contatto disponibili

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

Quando elenca gli orari di contatto disponibili utilizzando l' ListContacts operazione, AWS Ground Station restituirà gli orari di visibilità in base a quando il satellite salirà al di sopra e si posizionerà al di sotto della maschera di downlink. Gli orari di contatto disponibili si basano su questa finestra di visibilità della maschera di downlink. Ciò garantisce che i clienti non prenotino o paghino un orario quando il loro 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 ai clienti 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. I clienti sono responsabili 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 al cliente, anche se parti del tempo riservato non sono disponibili per l'uplink.

# Cronologia dei documenti per la guida AWS Ground Station dell'utente

La tabella seguente descrive le modifiche importanti alla documentazione dall'ultima versione di AWS Ground Station.

| Modifica | Descrizione | Data di rilascio |
| --- | --- | --- |
| Nuova caratteristica | I contatti possono ora essere programmati fino a 30 secondi al di fuori degli intervalli di visibilità. I tempi di visibilità sono inclusi nelle DescribeContact risposte. | 26 marzo 2024 |
| Aggiornamento della documentazione | Organizzazione migliorata e aggiunta la sezione «Selezione delle istanze EC2 e pianificazione della CPU». | 6 marzo 2024 |
| Aggiornamento della documentazione | Sono state aggiunte nuove best practice alla Guida per l'utente dell' AWS Ground Station agente per l'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 il riferimento ad AWS Notifiche all'utente nella documentazione di monitorag gio. | 6 agosto 2023 |
| Aggiornamento della documentazione | Sono state aggiunte istruzioni per etichettare i satelliti con un nome da mostrare nella console. AWS Ground Station | 26 luglio 2023 |

| Modifica | Descrizione | Data di rilascio |
| --- | --- | --- |
| Nuova caratteristica | Aggiunta la Guida per l'utente dell' AWS Ground Station agente per il rilascio di DigiF Data Delivery a banda larga | 12 aprile 2023 |
| Aggiornamenti delle policy gestite da AWS: nuova policy AWS gestita | AWS Ground Station ha aggiunto una nuova politica denominata AWSGroundStationAgentInstancePolicy. | 12 aprile 2023 |
| Nuova caratteristica | È stata aggiornata la guida per l'utente per il rilascio di CPE Preview. | 9 novembre 2022 |
| Aggiornamenti delle policy gestite da AWS: nuova policy AWS gestita | AWS Ground Station ha aggiunto la AWSServiceRoleForGroundStationDataflowEndpointGroup service-linked-role (SLR) che include una nuova politica denominata AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy. | 02 novembre 2022 |
| Nuova caratteristica | È stata aggiornata la guida per l'utente per includere l'integrazione con AWS CLI. | 17 aprile 2020 |
| Nuova caratteristica | 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 caratteristica | 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 |

| Modifica | Descrizione | Data di rilascio |
| --- | --- | --- |
| 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 di 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 introdutt iva, 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.