Benutzerhandbuch

AWS Ground Station

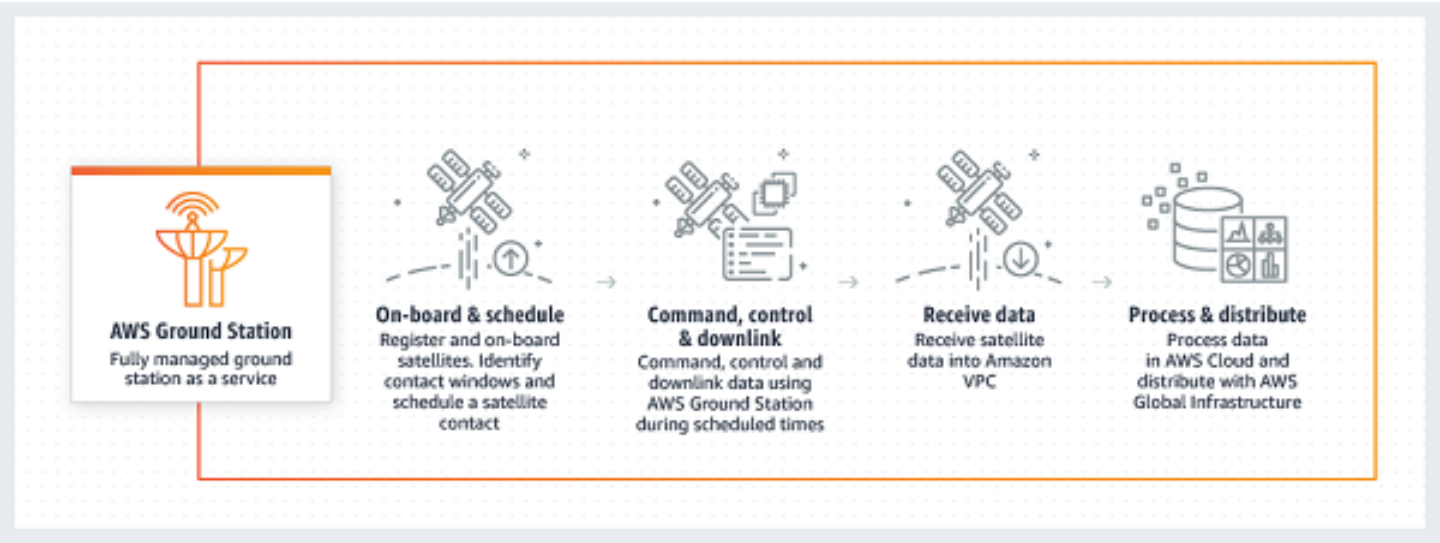
AWS Ground Station: Benutzerhandbuch

Table of Contents

Was ist AWS Ground Station?

AWS Ground Station ist ein vollständig verwalteter Service, mit dem Sie die Satellitenkommunikation steuern, Satellitendaten verarbeiten und Ihre Satellitenoperationen skalieren können. Das bedeutet, dass Sie keine eigene Bodenstation-Infrastruktur mehr aufzubauen oder zu verwalten brauchen.

AWS Ground Station ermöglicht es Ihnen, sich auf die Entwicklung und das schnelle Experimentieren mit neuen Anwendungen zu konzentrieren, mit denen Sie Satellitendaten aufnehmen und Ihre Server- und Satellitennutzung dynamisch skalieren können, anstatt Ressourcen für den Betrieb und die Verwaltung Ihrer eigenen Bodenstationen aufzuwenden.



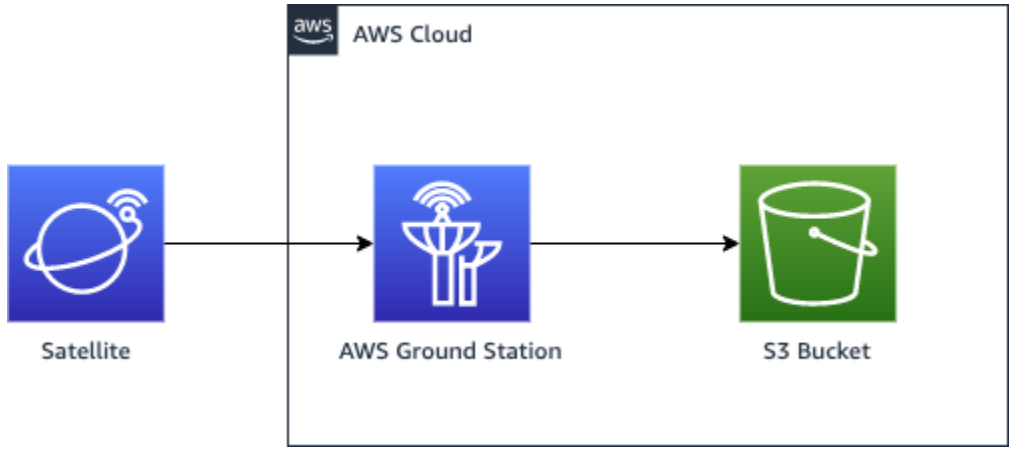
Funktionsweise von AWS Ground Station

Eine Satellitenreservierung wird auch als Kontakt bezeichnet. Ihr Satelliten kommuniziert bei Kontakten mit einer AWS Ground Station Antenne. Sie können Kontakte über eine API oder über die AWS Konsole reservieren, indem Sie Standort, Zeit und Missionsinformationen angeben. Ihre Kontaktdaten können zu und von einer Amazon Elastic Compute Cloud (Amazon EC2)-Instance gestreamt oder asynchron an einen Amazon Simple Storage Service (Amazon S3)-Bucket in Ihrem Konto übermittelt werden.

Sie können erweiterbare und wiederverwendbare Konfigurationsressourcen erstellen, damit Sie die Kontrolle darüber haben, wie AWS Ground Station die Antennen während Ihrer Kontakte konfiguriert werden. Mit Missionsprofilen können Sie angeben, woher die Daten stammen, welches Format sie haben sollen und wohin sie gesendet werden sollen.

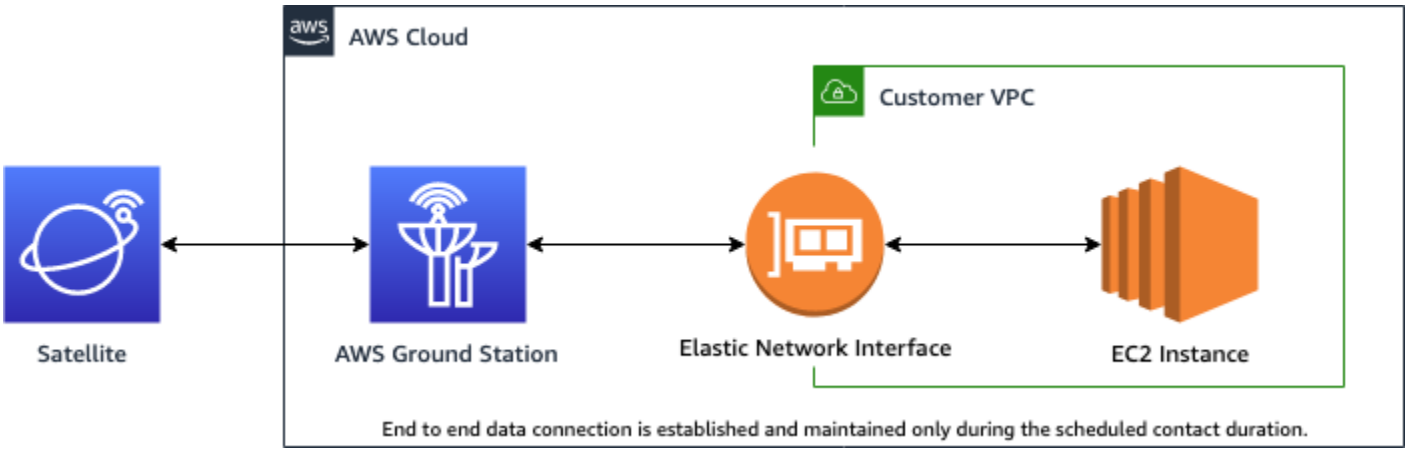
Datenbereitstellung an Amazon S3

Mit der Datenbereitstellung an Amazon S3 werden Ihre Kontaktdaten asynchron an einen Amazon S3-Bucket in Ihrem Konto übermittelt. Ihre Kontaktdaten werden als Paketerfassungsdateien (Pcap) bereitgestellt, um die Kontaktdaten in einem Software Defined (SDR) wiederzugeben oder die Nutzlastdaten aus den Pcap-Dateien zur Verarbeitung zu extrahieren. Die Pcap-Dateien werden alle 30 Sekunden an Ihren Amazon S3-Bucket übermittelt, wenn die Kontaktdaten von der Antennenhardware empfangen werden, damit die Kontaktdaten bei Bedarf während des Kontakts verarbeitet werden können. Nach dem Empfang können Sie die Daten mit Ihrer eigenen Nachbearbeitungssoftware verarbeiten oder andere AWS-Services wie Amazon SageMaker oder Amazon Rekognition nutzen. Die Datenbereitstellung an Amazon S3 ist nur für die Downlinking von Daten von Ihrem Satelliten verfügbar. Es ist nicht möglich, Daten von Amazon S3 aus mit Ihrem Satelliten zu verknüpfen.



Datenbereitstellung an Amazon EC2

Mit der Datenbereitstellung an Amazon EC2 werden Ihre Kontaktdaten zu und von Ihrer Amazon EC2 gestreamt. Sie können Ihre Daten in Echtzeit auf Ihrer Amazon EC2 verarbeiten oder die Daten zur Nachbearbeitung weiterleiten.



Weitere Informationen

Mit können AWS Ground Station Sie über Satellitenkommunikation auf mehr als 125 Services zugreifen. Beachten Sie Folgendes:

- Sie können Schmalband-HF-Daten im S-Band (2200 bis 2300 MHz) oder X-Band (7750 bis 8400 MHz) bei Bandbreiten bis zu 54 MHz empfangen.
  - Die S-Band-HF-Daten werden digitalisiert und als digitaler Stream im VITA-49-Signaldaten-/IP-Format bereitgestellt.
  - X-Band Intermediate Frequency (IF)-Daten werden digitalisiert und als digitaler Stream im VITA-49-Signaldaten-/IP-Format bereitgestellt.
- Sie können Breitband-demodulierte/dekodierte Daten im X-Band (7750 bis 8400 MHz) bei Bandbreiten bis zu 500 MHz empfangen
  - X-Band Intermediate Frequency (IF)-Daten werden demoduliert, dekodiert und als digitaler Stream im VITA-49 Erweiterungsdaten-/IP-Format bereitgestellt.
- Sie können Broadband Digital Intermediate Frequency (DigIF)-Daten von 40 MHz bis 400 MHz Bandbreite über den - AWS Ground Station Agenten empfangen.
  - AWS Ground Station Benutzerhandbuch für Agenten Weitere Informationen zum AWS Ground Station Agent und zur Wideband-DigIF-Datenbereitstellung finden Sie unter .
- Sie können HF-Daten im S-Band (2025 bis 2120 MHz) mit Bandbreiten bis zu 54 MHz übertragen.

  - Die RF-Daten werden AWS Ground Station als digitaler Stream im VITA-49-Signaldaten/IP-Format bereitgestellt.
- Sie müssen AWS Ground Station von einer - AWS Region aus ausführen, die unterstützt AWS Ground Station. Eine Liste der unterstützten Regionen finden Sie in der Regionstabelle der globalen Infrastruktur.
- Sie können Daten an eine Amazon EC2-Instance übermitteln, die in derselben Region wie die Antenne ausgeführt wird, oder Sie können die regionsübergreifende Datenübermittlung verwenden, um Ihre Daten von einer Antenne an eine Amazon EC2-Instance in Ihrer bevorzugten AWS-Region zu senden. Die folgenden antenna-to-destination Regionen sind derzeit verfügbar:
  - Region USA Ost (Ohio) (us-ost-2) bis Region USA West (Oregon) (us-west-2)
  - Region USA West (Oregon) (us-west-2) bis Region USA Ost (Ohio) (us-ost-2)

Servicebedingungen

Sie dürfen die Services ausschließlich zum Speichern, Abrufen, Abfragen und Ausführen von Inhalten verwenden, die Ihnen gehören, für Sie lizenziert sind oder rechtmäßig von erworben wurden. Gemäß der Verwendung in diesen Nutzungsbedingungen bezieht sich (a) „Ihre Inhalte“ auf beliebige „Inhalte des Unternehmens“ und auf beliebige „Kundeninhalte“ und (b) „AWS-Inhalte“ auf "Eigentum von Amazon". Sie sind möglicherweise berechtigt, als Teil der Services bestimmte Software (einschließlich der zugehörigen Dokumentation) zu nutzen, die von uns oder Drittanbieter-Lizenzgebern bereitgestellt wird.

> **Important**
>
> Diese Software wird weder an Sie verkauft noch an Sie verteilt und Sie dürfen Sie ausschließlich als Teil der Services verwenden. Ohne entsprechende ausdrückliche Genehmigung dürfen Sie sie nicht außerhalb der Services übertragen.

Kernkomponenten

Datenfluss-Endpunktgruppen, Konfigurationen und Missionsprofile sind Kernkomponenten von AWS Ground Station. Diese Komponenten bestimmen, wie Sie Ihre Kontakte planen, wie die Antennen mit Ihren Satelliten kommunizieren und wo Ihre Daten bereitgestellt werden. Bevor Sie mit beginnen AWS Ground Station, empfehlen wir Ihnen, sich mit diesen Komponenten vertraut zu machen. Beispiele finden Sie in den jeweiligen Abschnitten.

Themen

Datenflussendpunktgruppen

Datenflussendpunkte definieren den Ort, zu oder aus dem die Daten während des Kontakts gestreamt werden sollen. Die Endpunkte werden durch einen Namen Ihrer Wahl identifiziert, wenn Sie Kontakte ausführen. Diese Namen müssen nicht eindeutig sein. Dadurch können mehrere Kontakte gleichzeitig mit demselben Missionsprofil ausgeführt werden.

Die Endpunktlistenadresse besteht aus den folgenden Elementen:

- `name` – IP-Adresse dieses Datenflussesendpunkts.
- `port` – Der Port an, mit dem eine Verbindung hergestellt werden soll.

Die Sicherheitsdetails eines Endpunkts bestehen aus den folgenden Elementen:

- `roleArn` – Der Amazon-Ressourcenname (ARN) einer Rolle, die AWS Ground Station übernimmt, um Elastic Network Interfaces (ENIs) in Ihrer VPC zu erstellen. Diese ENIs dienen als Ein- und Ausreißpunkte von Daten, die während eines Kontakts gestreamt werden.
- `securityGroupIds` – Die Sicherheitsgruppen, die den der Elastic Network-Schnittstellen angefügt werden sollen.
- `subnetIds` – Eine Liste von Subnetzen, in denen Elastic Network-Schnittstellen AWS Ground Station platziert, um Streams an Ihre Instances zu senden.

Die an übergebene IAM-Rolle `roleArn` muss über eine Vertrauensrichtlinie verfügen, die es dem `groundstation.amazonaws.com` Service-Prinzipal ermöglicht, die Rolle zu übernehmen. Ein Beispiel finden Sie im Abschnitt Beispiel-Vertrauensrichtlinie unten. Während der Endpunkterstellung ist die Endpunktressourcen-ID nicht vorhanden, daher muss die Vertrauensrichtlinie ein Sternchen (`*`) anstelle von verwenden*`your-endpoint-id`*. Dies kann nach der Erstellung aktualisiert werden, um die Endpunktressourcen-ID zu verwenden, um die Vertrauensrichtlinie auf diese spezifische Datenfluss-Endpunktgruppe zu beschränken.

Die IAM-Rolle muss über eine IAM-Richtlinie verfügen, die AWS Ground Station das Einrichten der ENIs erlaubt. Ein Beispiel finden Sie im Abschnitt Beispiel für eine Rollenrichtlinie unten.

Beispiel für eine Vertrauensrichtlinie

Weitere Informationen zum Aktualisieren der Vertrauensrichtlinie einer Rolle finden Sie unter Verwalten von IAM-Rollen im IAM-Benutzerhandbuch.

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

Beispiel für eine Rollenrichtlinie

Weitere Informationen zum Aktualisieren oder Anfügen einer Rollenrichtlinie finden Sie unter Verwalten von IAM-Richtlinien im IAM-Benutzerhandbuch.

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

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

Datenflussendpunkte werden stets als Teil einer Datenflussendpunktgruppe erstellt. Durch das Einfügen mehrerer Datenflussendpunkte in eine Gruppe bestätigen Sie, dass die angegebenen Endpunkte während eines einzelnen Kontakts gemeinsam verwendet werden können. Wenn ein Kontakt beispielsweise Daten an drei getrennte Datenflussendpunkte senden muss, muss es drei Endpunkte in einer einzelnen Datenflussendpunktgruppe geben, die mit den Datenflussendpunkt-Configs in Ihrem Missionsprofil übereinstimmen.

Wenn eine oder mehrere Ressourcen in einer Datenflussendpunktgruppe für einen Kontakt verwendet wird oder werden, wird die gesamte Gruppe für die Dauer des Kontakts reserviert. Sie können mehrere Kontakte gleichzeitig ausführen, aber diese Kontakte müssen auf verschiedenen Datenfluss-Endpunktgruppen ausgeführt werden.

Datenfluss-Endpunktgruppen müssen sich im `HEALTHY` Status befinden, um Kontakte mit ihnen zu planen. Im Folgenden sind die Gründe aufgeführt, warum sich Ihre Datenfluss-Endpunktgruppen möglicherweise nicht in einem -`HEALTHY`Zustand befinden, sowie die entsprechenden Korrekturmaßnahmen, die ergriffen werden sollen.

- `NO_REGISTERED_AGENT` – Starten Sie Ihre EC2-Instance, die den Agenten registriert. Beachten Sie, dass Sie über eine gültige Controller-Konfigurationsdatei verfügen müssen, damit dieser Aufruf erfolgreich ist. Einzelheiten zur Konfiguration AWS Ground Station Benutzerhandbuch für Agenten dieser Datei finden Sie unter .
- `INVALID_IP_OWNERSHIP` – Verwenden Sie die DeleteDataflowEndpointGroup API, um die Datenfluss-Endpunktgruppe zu löschen, und verwenden Sie dann die CreateDataflowEndpointGroup API, um die Datenfluss-Endpunktgruppe mithilfe von IP-Adressen und Ports neu zu erstellen, die der EC2-Instance zugeordnet sind.

- `UNVERIFIED_IP_OWNERSHIP` – Die IP-Adresse wurde noch nicht validiert. Die Validierung erfolgt regelmäßig, sodass sie sich selbst auflösen sollte.
- `NOT_AUTHORIZED_TO_CREATE_SLR` – Das Konto ist nicht autorisiert, die erforderliche serviceverknüpfte Rolle zu erstellen. Überprüfen Sie die Schritte zur Fehlerbehebung in Verwenden von serviceverknüpften Ground Station

Weitere Informationen zum Ausführen von Operationen an Datenfluss-Endpunktgruppen mithilfe von AWS CloudFormation, der AWS Command Line Interface oder der AWS Ground Station -API finden Sie in der folgenden Dokumentation.

- AWS::GroundStation::DataflowEndpoint CloudFormation Gruppenressourcentyp
- AWS CLI Referenz zur Datenfluss-Endpunktgruppe
- API-Referenz für Datenfluss-Endpunktgruppen

Configs

Configs sind Ressourcen, die AWS Ground Station verwendet, um die Parameter für jeden Aspekt Ihres Kontakts zu definieren. Fügen Sie die gewünschten Configs einem Missionsprofil hinzu. Dieses Missionsprofil wird anschließend während der Ausführung des Kontakts verwendet. Sie können verschiedene Arten von Configs definieren.

In der folgenden Dokumentation finden Sie weitere Informationen zum Ausführen von Operationen an Konfigurationen mithilfe von AWS Command Line Interface, AWS CloudFormation der oder der AWS Ground Station -API. Links zur Dokumentation für bestimmte Konfigurationstypen finden Sie im Folgenden.

- AWS::GroundStation::Config CloudFormation Ressourcentyp
- AWS CLI Konfigurationsreferenz
- Config-API-Referenz

Datenflussendpunkt-Config

> **Note**
>
> Datenflussendpunktkonfigurationen werden nur für die Datenbereitstellung an Amazon EC2 und nicht für die Datenbereitstellung an Amazon S3 verwendet.

Sie können Datenfluss-Endpunktkonfigurationen verwenden, um anzugeben, von welchem Datenfluss-Endpunkt in einer Datenfluss-Endpunktgruppe Daten während eines Kontakts fließen sollen oder zu welchem Datenfluss sollen. Die beiden Parameter einer Datenflussendpunktkonfiguration geben den Namen und die Region des Datenflussendpunkts an. Bei der Reservierung eines Kontakts AWS Ground Station analysiert das von Ihnen angegebene Missionsprofil und versucht, eine Datenflussendpunktgruppe zu finden, die alle Datenflussendpunkte enthält, die in den Datenflussendpunktkonfigurationen in Ihrem Missionsprofil angegeben sind.

Die -`dataflowEndpointName`Eigenschaft einer Datenfluss-Endpunktkonfiguration gibt an, zu welchem Datenfluss-Endpunkt in einer Datenfluss-Endpunktgruppe welche oder von welchen Daten während eines Kontakts fließen.

Die -`dataflowEndpointRegion`Eigenschaft gibt an, in welcher Region sich der Datenfluss-Endpunkt befindet. Wenn in Ihrer Datenfluss-Endpunktkonfiguration eine Region angegeben ist, AWS Ground Station sucht nach einem Datenfluss-Endpunkt in der angegebenen Region. Wenn keine Region angegeben ist, AWS Ground Station wird standardmäßig die Ground Station-Region des Kontakts verwendet. Ein Kontakt gilt als regionsübergreifender Datenzustellungskontakt, wenn die Region Ihres Datenflussendpunkts nicht mit der Ground Station-Region des Kontakts übereinstimmt.

Weitere Informationen zum Ausführen von Operationen an Datenflussendpunktkonfigurationen mithilfe von AWS CloudFormation, der AWS Command Line Interface oder der AWS Ground Station -API finden Sie in der folgenden Dokumentation.

- AWS::GroundStation::Config DataflowEndpointConfig CloudFormation Eigenschaft
- AWS CLI Konfigurationsreferenz (siehe `dataflowEndpointConfig -> (structure)` Abschnitt)
- DataflowEndpointConfig API-Referenz

S3-Aufzeichnungskonfiguration

> **Note**
>
> S3-Aufzeichnungskonfigurationen werden nur für die Datenbereitstellung an Amazon S3 und nicht für die Datenbereitstellung an Amazon EC2 verwendet.

Sie können S3-Aufzeichnungskonfigurationen verwenden, um einen Amazon S3-Bucket anzugeben, an den Sie Downlink-Daten liefern möchten. Die beiden Parameter einer S3-Aufzeichnungskonfiguration geben den Amazon S3-Bucket und die IAM-Rolle AWS Ground Station an, die annehmen soll, wenn die Daten an Ihren Amazon S3-Bucket übermittelt werden. Die angegebene IAM-Rolle und der angegebene Amazon S3-Bucket müssen die folgenden Kriterien erfüllen:

- Der Name des Amazon S3-Buckets muss mit beginnen`aws-groundstation`.
- Die IAM-Rolle muss über eine Vertrauensrichtlinie verfügen, die es dem `groundstation.amazonaws.com` Service-Prinzipal ermöglicht, die Rolle zu übernehmen. Ein Beispiel finden Sie im Abschnitt Beispiel-Vertrauensrichtlinie unten. Während der Konfigurationserstellung ist die ID der Konfigurationsressource nicht vorhanden, muss die Vertrauensrichtlinie ein Sternchen (`*`) anstelle von verwenden *`your-config-id`* und kann nach der Erstellung mit der ID der Konfigurationsressource aktualisiert werden.
- Die IAM-Rolle muss über eine IAM-Richtlinie verfügen, die es der Rolle ermöglicht, die `s3:GetBucketLocation` Aktion für den Bucket und die `s3:PutObject` Aktion für die Objekte des Buckets auszuführen. Wenn der Amazon S3-Bucket über eine Bucket-Richtlinie verfügt, muss die Bucket-Richtlinie der IAM-Rolle auch erlauben, diese Aktionen auszuführen. Ein Beispiel finden Sie im Abschnitt Beispiel für eine Rollenrichtlinie unten.

Beispiel für eine Vertrauensrichtlinie

Weitere Informationen zum Aktualisieren der Vertrauensrichtlinie einer Rolle finden Sie unter Verwalten von IAM-Rollen im IAM-Benutzerhandbuch.

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

Beispiel für eine Rollenrichtlinie

Weitere Informationen zum Aktualisieren oder Anfügen einer Rollenrichtlinie finden Sie unter Verwalten von IAM-Richtlinien im IAM-Benutzerhandbuch.

```
{
  "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/*"
      ]
    }
  ]
}
```

Weitere Informationen zum Ausführen von Operationen an S3-Aufzeichnungskonfigurationen mithilfe von AWS CloudFormation, der AWS Command Line Interface oder der AWS Ground Station -API finden Sie in der folgenden Dokumentation.

- AWS::GroundStation::Config S3RecordingConfig CloudFormation -Eigenschaft
- AWS CLI Konfigurationsreferenz (siehe `s3RecordingConfig -> (structure)` Abschnitt)
- S3RecordingConfig API-Referenz

Nachverfolgungs-Config

Sie können im Missionsprofil Nachverfolgungs-Configs verwenden, um festzulegen, ob während Ihrer Kontakte die automatische Nachverfolgung (Autotrack) aktiviert sein soll. Diese Config besitzt einen einzigen Parameter: `autotrack`. Der Parameter `autotrack` kann die folgenden Werte haben:

- `REQUIRED` – Die automatische Nachverfolgung (Autotrack) ist für Ihre Kontakte erforderlich.
- `PREFERRED` – Die automatische Nachverfolgung (Autotrack) wird für Kontakte zwar bevorzugt, Kontakte können jedoch auch ohne automatische Nachverfolgung ausgeführt werden.
- `REMOVED` – Für Ihre Kontakte soll keine automatische Nachverfolgung (Autotrack) verwendet werden.

In der folgenden Dokumentation finden Sie weitere Informationen zum Ausführen von Operationen zur Nachverfolgung von Konfigurationen mithilfe von AWS Command Line Interface, AWS CloudFormation der oder der AWS Ground Station -API.

- AWS::GroundStation::Config TrackingConfig CloudFormation Eigenschaft
- AWS CLI Konfigurationsreferenz (siehe `trackingConfig -> (structure)` Abschnitt)
- TrackingConfig API-Referenz

Antennen-Downlink-Config

Sie können die Antenne Downlink-Konfigurationen verwenden, um die Antenne für Downlink während Ihres Kontakts zu konfigurieren. Sie bestehen aus einer Spectrum-Konfiguration, die die Häufigkeit, Bandbreite und Telefonie angibt, die während Ihres Downlink-Kontakts verwendet werden sollen. Wenn Ihr Downlink-Anwendungsfall eine Demodulierung oder Dekodierung erfordert, finden Sie weitere Informationen unter Antennen-Downlink-Demod-Decode-Config.

In der folgenden Dokumentation finden Sie weitere Informationen zum Ausführen von Operationen an Antennen-Downlink-Konfigurationen mithilfe von AWS Command Line Interface, AWS CloudFormation der oder der AWS Ground Station -API.

- AWS::GroundStation::Config AntennaDownlinkConfig CloudFormation Eigenschaft
- AWS CLI Konfigurationsreferenz (siehe `antennaDownlinkConfig -> (structure)` Abschnitt)
- AntennaDownlinkConfig API-Referenz

Antennen-Downlink-Demod-Decode-Config

Antennen-Downlink-Demod-Decode-Configs stellen einen komplexeren und anpassbaren Config-Typ dar, den Sie zum Ausführen von Downlink-Kontakten mit Demod oder Decode verwenden können. Wenn Sie an der Ausführung dieser Arten von Kontakten interessiert sind, wenden Sie sich an das -AWS Ground Station Team. Wir helfen Ihnen, die richtige Config und das richtige Missionsprofil für Ihren Anwendungsfall zu definieren.

In der folgenden Dokumentation finden Sie weitere Informationen dazu, wie Sie Operationen an den Dekodierungskonfigurationen für Antennen-Downlinks mithilfe von AWS Command Line Interface, AWS CloudFormation der oder der AWS Ground Station -API ausführen.

- AWS::GroundStation::Config AntennaDownlinkDemodDecodeConfig CloudFormation Eigenschaft
- AWS CLI Konfigurationsreferenz (siehe `antennaDownlinkDemodDecodeConfig -> (structure)` Abschnitt)
- AntennaDownlinkDemodDecodeConfig API-Referenz

Antennen-Uplink-Config

Sie können Antennen-Uplink-Konfigurationen verwenden, um die Antenne für Uplink während Ihres Kontakts zu konfigurieren. Sie bestehen aus einer Spektrumkonfiguration mit Frequenz, Telefonie und zieleffektiver isfrequenter Radiationsleistung (EIRP). Informationen zum Konfigurieren eines Kontakts für Uplink-Loopback finden Sie unter Uplink-Echokonfiguration.

In der folgenden Dokumentation finden Sie weitere Informationen dazu, wie Sie Operationen an Antennen-Uplink-Konfigurationen mithilfe von AWS Command Line Interface, AWS CloudFormation der oder der AWS Ground Station -API ausführen.

- AWS::GroundStation::Config AntennaUplinkConfig CloudFormation Eigenschaft
- AWS CLI Konfigurationsreferenz (siehe `antennaUplinkConfig -> (structure)` Abschnitt)
- AntennaUplinkConfig API-Referenz

Uplink-Echokonfiguration

Uplink-Echo-Configs teilen der Antenne mit, wie ein Uplink-Echo ausgeführt werden soll. Dadurch wird das von der Antenne gesendeten Signal an Ihren Datenflussendpunkt als Echo zurückgeben. Eine Uplink-Echo-Config enthält den ARN einer Uplink-Config. Der Antenne verwendet während der Ausführung eines Uplink-Echos die Parameter aus der Uplink-Config, auf die durch den ARN verwiesen wird.

Weitere Informationen zum Ausführen von Operationen an Uplink-Echokonfigurationen mithilfe von AWS CloudFormation, der AWS Command Line Interface oder der AWS Ground Station -API finden Sie in der folgenden Dokumentation.

- AWS::GroundStation::Config UplinkEchoConfig CloudFormation Eigenschaft
- AWS CLI Konfigurationsreferenz (siehe `uplinkEchoConfig -> (structure)` Abschnitt)
- UplinkEchoConfig API-Referenz

Missionsprofil

Missionsprofile enthalten Configs und Parameter, mit denen festgelegt wird, wie Kontakte ausgeführt werden. Wenn Sie einen Kontakt reservieren oder nach verfügbaren Kontakten suchen, stellen Sie das Missionsprofil bereit, das Sie verwenden möchten. Missionsprofile bringen alle Ihre

Konfigurationen zusammen und definieren, wie die Antenne konfiguriert wird und wohin die Daten während Ihres Kontakts übertragen werden.

Abgesehen von den Nachverfolgungs-Configs sind alle Configs im `dataflowEdges`-Feld des Missionsprofils enthalten. Eine einzelne Datenflussgrenze stellt eine Liste von zwei ARNs dar. Der erste ARN ist die from-Config und der zweite ist die to-Config. Durch die Angabe einer Datenfluss-Edge zwischen zwei Konfigurationen teilen Sie mit, AWS Ground Station wohin und wohin Daten während eines Kontakts fließen sollen. Nachverfolgungs-Configs werden nicht als Teil einer Datenflussgrenze verwendet, sondern als eigenes Feld angegeben.

Das Feld `name` im Missionsprofil hilft Ihnen, die von Ihnen erstellten Missionsprofilen zu unterscheiden.

In der folgenden Dokumentation finden Sie weitere Informationen zum Ausführen von Operationen an Missionsprofilen mithilfe von AWS Command Line Interface, AWS CloudFormation der oder der AWS Ground Station -API.

- AWS::GroundStation::MissionProfile CloudFormation Ressourcentyp
- AWS CLI Referenz zum Missionsprofil
- API-Referenz für Mission Profile

AWS Ground StationStandorte

Kunden können Daten mit den Antennen der AWS Ground Station an den folgenden Standorten übertragen und empfangen: USA (Oregon), USA (Ohio), USA (Alaska), Naher Osten (Bahrain), Europa (Stockholm), Asien-Pazifik (Dubbo), Europa (Irland), Afrika (Kapstadt), USA (Hawaii), Asien-Pazifik (Seoul), Asien-Pazifik (Singapur) und Südamerika (Punta Arenas).

Kunden können Daten bereitstellen und ihre Kontakte mit der AWS Ground Station Station-Konsole in den folgenden Regionen konfigurieren: USA West (Oregon), USA Ost (Ohio), Naher Osten (Bahrain), Europa (Stockholm), Asien-Pazifik (Dubbo), Europa (Irland), Afrika (Kapstadt), USA Ost (Nord-Virginia), Europa (Frankfurt), Asien-Pazifik (Seoul), Asien-Pazifik (Singapur) und Südamerika (São Paulo).

Hinweis: Sie können AWS-Bodenstationsressourcen nur in den Regionen erstellen, in denen die im vorherigen Absatz erwähnte AWS Ground Station Station-Konsole gehostet wird.

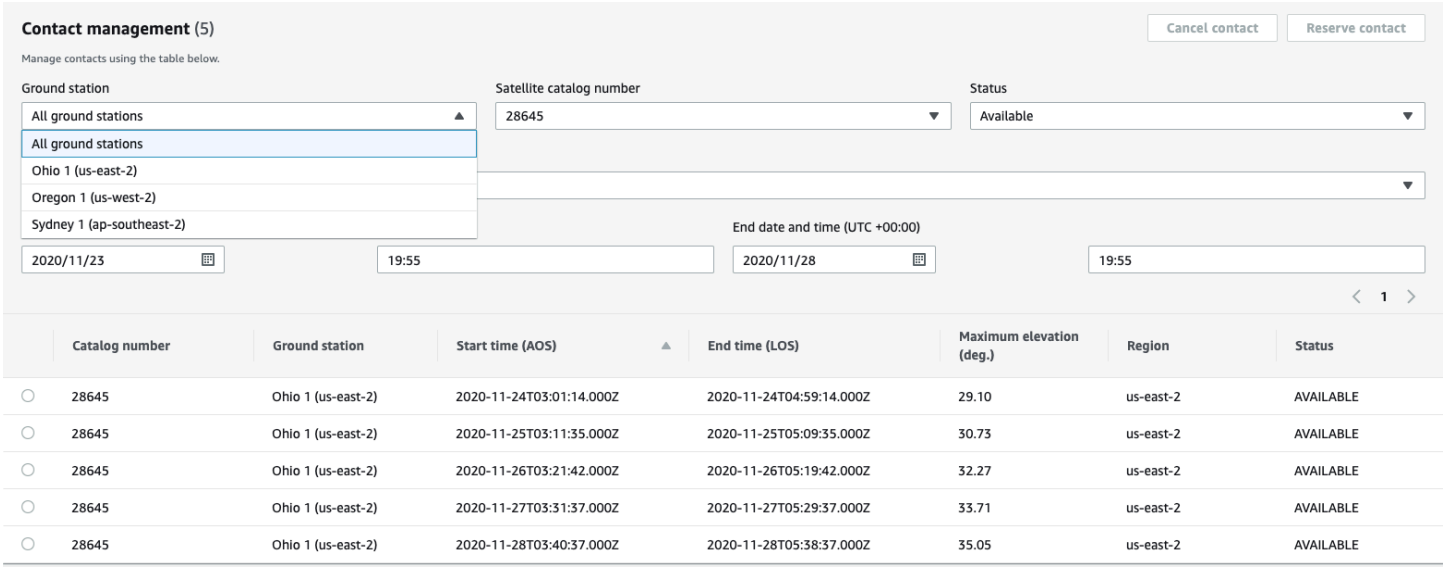
Themen

- Die AWS-Region für eine Ground Station finden

Die AWS-Region für eine Ground Station finden

Das globale AWS-Netzwerk umfasst Ground Station, die sich nicht physisch in der AWS-Region befinden, mit der sie verbunden sind. Das Auflisten und Reservieren von Kontakten an einem dieser Bodenstation-Standorte muss in der AWS-Region erfolgen, mit der die Ground Station verbunden ist.

Es gibt mehrere Methoden, um die AWS-Region einer Bodenstation zu bestimmen. Auf der AWS Ground Station Konsolenseite wird die AWS-Region der Bodenstation angezeigt, wenn sie sowohl in der Filter- als auch in der Kontakttabelle angezeigt wird, wie in der Abbildung unten gezeigt. Das AWS-SDK enthält die AWS-Region der Bodenstation in der ListGroundStationAntwort. Schließlich enthält die AWS-CLI die AWS-Region der Bodenstation in der list-ground-stationsAntwort.



Themen

- Beispiel für eine Ground Station außerhalb einer AWS-Region

Beispiel für eine Ground Station außerhalb einer AWS-Region

Hawaii 1 ist ein Beispiel für einen Standort einer Ground Station, der sich nicht physisch in der AWS-Region befindet, mit der er verbunden ist. Die Ground Station Hawaii 1 befindet sich in Hawaii, USA, ist aber mit der AWS-Region US-West-2 (Oregon) verbunden. Um Kontakte mit Hawaii 1 aufzulisten und zu reservieren, müssen Sie ein Missionsprofil in der AWS-Region US-West-2 (Oregon) konfiguriert haben und die AWS-Region US-West-2 (Oregon) in der AWS Ground Station Konsole, der AWS-CLI oder dem AWS-SDK verwenden.

- Um Kontakte für Hawaii 1 in der AWS Ground Station Konsole aufzulisten und zu reservieren, müssen Sie die AWS Ground Station Konsole in der Region US-West-2 (Oregon) verwenden.
- Um Kontakte für Hawaii 1 mithilfe der AWS-CLI aufzulisten und zu reservieren, müssen Sie die Region mithilfe des `--region` CLI-Arguments als us-west-2 angeben.
- Um Kontakte für Hawaii 1 mithilfe des AWS-SDK aufzulisten und zu reservieren, müssen Sie die Region Ihres Kunden auf us-west-2 festlegen. Wie Sie dies einstellen, hängt von der Programmiersprache ab, die Sie verwenden. Ein Beispiel dafür, wie Sie dies einrichten können, JavaScript ist im AWS-SDK zur JavaScript Dokumentation beschrieben. Weitere Informationen finden Sie in der sprachspezifischen SDK-Dokumentation.

Einrichten AWS Ground Station

Bevor Sie mit der Nutzung beginnen AWS Ground Station, müssen Sie wissen, welche AWS Identity and Access Management (IAM-) Berechtigungen Sie benötigen und welche Zugangsdaten für Raumfahrzeuge Sie angeben müssen. Führen Sie die folgenden Schritte aus, um Ihr Konto zu erstellen.

Themen

Melden Sie sich an für ein AWS-Konto

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/signup.
2. Folgen Sie den Online-Anweisungen.

   Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Administratorbenutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu https://aws.amazon.com/ auf und klicken Sie auf Mein Konto.

Erstellen eines Administratorbenutzers

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich AWS Management Consoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Anmelden als Root-Benutzer im AWS-Anmeldung Benutzerhandbuch zu.
2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

   Anweisungen finden Sie unter Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer (Konsole) im IAM-Benutzerhandbuch.

Erstellen eines Administratorbenutzers

1. Aktivieren Sie das IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.
2. Gewähren Sie einem Administratorbenutzer im IAM Identity Center Administratorzugriff.

   Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie IAM-Identity-Center-Verzeichnis im Benutzerhandbuch unter Benutzerzugriff mit der Standardeinstellung konfigurieren.AWS IAM Identity Center

Anmelden als Administratorbenutzer

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Access-Portal.

Fügen Sie Ihrem AWS Konto Bodenstationsberechtigungen hinzu

Für die Nutzung AWS Ground Station ohne Administratorrechte müssen Sie eine neue Richtlinie erstellen und sie Ihrem AWS Konto zuordnen.

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die IAM-Konsole.
2. Eine neue Richtlinie erstellen. Gehen Sie dazu wie folgt vor:

   a. Wählen Sie im Navigationsbereich Policies (Richtlinien) und dann Create Policy (Richtlinie erstellen) aus.

   b. Bearbeiten Sie das JSON auf der Registerkarte JSON mit einem der folgenden Werte. Verwenden Sie das JSON, das für Ihre Anwendung am besten geeignet ist.

   - Stellen Sie für Administratorrechte der Ground Station Aktion wie folgt auf Groundstation: * ein:

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

   - Für Nur-Lese-Berechtigungen legen SieAction (Aktion) auf groundstation:Get*, groundstation:List* und groundstation:Describe* wie folgt fest:

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

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "groundstation:Get*",
        "groundstation:List*",
        "groundstation:Describe*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

- Für zusätzliche Sicherheit durch Multifaktor-Authentifizierung setzen Sie Action auf groundstation: * und Condition/Bool auf aws ::true wie folgt: MultiFactorAuthPresent

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

3. Fügen Sie in der IAM-Konsole die von Ihnen erstellte Richtlinie dem gewünschten Benutzer hinzu.

Weitere Informationen über IAM-Benutzer und das Anfügen von Richtlinien finden Sie im IAM-Benutzerhandbuch.

Onboarding für Kunden

Einzelheiten zum Onboarding finden Sie auf der AWS Ground Station Konsolenseite im Bereich Satelliten und Ressourcen, um die Registrierung für Ihr AWS Ground Station Konto abzuschließen. Das AWS Ground Station Team arbeitet mit Ihnen zusammen, um Ihre Satelliten in den Dienst einzubinden. Sobald das Onboarding Ihres Satelliten durchgeführt haben, steht er für die Verwaltung eines Kontakts zur Verfügung. Anweisungen zur Verwaltung eines Kontakts finden Sie unter Kontakte auflisten und reservieren.

Bei Onboarding Ihrer Satelliten erhalten Sie Zugang zum Senden und Empfangen von Daten an und vom Satelliten. Neben dem Onboarding Ihrer eigenen Satelliten können Kunden auch das Onboarding folgender Satelliten durchführen, um ein direktes Downlinking von Broadcast-Daten mit AWS Ground Station zu ermöglichen:

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

Sobald sie an Bord sind, können diese Satelliten für den sofortigen Einsatz abgerufen werden. AWS Ground Station verwaltet eine Reihe vorkonfigurierter AWS CloudFormation Vorlagen, um den Einstieg in den Service zu erleichtern. Anweisungen und Details für den Zugriff auf und die Verwendung dieser Vorlage finden Sie im Abschnitt „Ressourcen mithilfe einer AWS CloudFormation Vorlage erstellen“ des Benutzerhandbuchs.

Weitere Informationen über diese Satelliten und die Art der von ihnen übertragenen Daten finden Sie unter Aqua, JPSS-1/NOAA-20 und SNPP sowie Terra.

Nächste Schritte

Ihr AWS Ground Station Konto ist jetzt eingerichtet und bereit für die Konfiguration. Fahren Sie mit Erste Schritte fort, um Ihre Ressourcen zur Verwendung von AWS Ground Station zu konfigurieren.

Erste Schritte mit AWS Ground Station

AWS Ground Station Mit können Sie Daten von Ihren Satelliten aus befehlen, steuern und herunterverknüpfen.

Mit können AWS Ground Station Sie den Zugriff auf Ground Station-Antennen pro Minute planen und nur für die verwendete Antennenzeit bezahlen. AWS Ground Station liefert Ihre Kontaktdaten asynchron an einen Amazon Simple Storage Service (Amazon S3)-Bucket in Ihrem Konto oder synchron, indem es sie an und von einer Amazon Elastic Compute Cloud (Amazon EC2)-Instance in Ihrem Konto streamt. In den folgenden Schritten wird beschrieben, wie Sie die Ressourcen konfigurieren, die für den asynchronen Empfang von Kontaktdaten in einem Amazon S3-Bucket erforderlich sind. Weitere Informationen zur Verwendung der Datenbereitstellung für Amazon EC2 finden Sie im -Datenlieferung an Amazon EC2Leitfaden.

Themen

Basic-Konzepte

Bevor Sie beginnen, sollten Sie sich mit den grundlegenden Konzepten in vertraut machen AWS Ground Station. Weitere Informationen finden Sie unter Kernkomponenten.

Fahren Sie dann mit fort, Voraussetzungen um mehr über die Voraussetzungen für die ersten Schritte mit zu erfahren AWS Ground Station.

Voraussetzungen

Bevor Sie mit beginnen AWS Ground Station, stellen Sie sicher, dass Sie über ein AWS Konto mit den richtigen Anmeldeinformationen verfügen. Führen Sie die Schritte unter Einrichten AWS Ground Station aus.

> **Note**
>
> Wenn Sie die Wideband-DigIF-Datenbereitstellung verwenden, finden Sie Anweisungen unter AWS Ground Station Benutzerhandbuch für Agenten .

Andernfalls fahren Sie mit fortSchritt 1: Auswählen einer - AWS CloudFormation Vorlage.

Schritt 1: Auswählen einer - AWS CloudFormation Vorlage

Nachdem Sie Ihren Satelliten integriert haben, müssen Sie Missionsprofile definieren, um die AWS Ground Station Antennenkonfiguration für Downlink-Daten von Ihrem Satelliten zu definieren. Um Sie bei diesem Prozess zu unterstützen, stellen wir vorkonfigurierte AWS CloudFormation Vorlagen sowohl für die Bereitstellung von Redunband- als auch für die Wideband-DigIF-Daten bereit, die öffentliche Broadcast-Satelliten verwenden. Diese Vorlagen erleichtern Ihnen die Verwendung von AWS Ground Station. Weitere Informationen zu AWS CloudFormation finden Sie unter Was ist AWS CloudFormation?

Wählen Sie je nach Art des Kontakts, den Sie nehmen möchten, den entsprechenden CFN-Vorlagentyp aus der folgenden Liste aus:

- AWS CloudFormation Vorlagen für die Bereitstellung von Daten in S3 .
- Breitebandvorlagen AWS CloudFormation für die DigIf S3-Datenbereitstellung.

Wenn Sie keine der vorgefertigten AWS CloudFormation Vorlagen verwenden möchten, finden Sie Anweisungen unter Erstellen einer eigenen Vorlage.

AWS CloudFormation Vorlagen für die Bereitstellung von Daten in S3

Vorkonfigurierte Vorlagen

Heute können Sie mehrere Datenströme pro Kontakt so konfigurieren, dass sie in einen S3-Bucket fließen. Diese Datenströme sind in zwei verschiedenen Formaten verfügbar. Datenströme mit VITA-49-Signal-/IP-Daten können für S-Band- und X-Band-Signale bis zu 54 MHz in Bandbreite konfiguriert werden. VITA-49 Erweiterungsdaten/IPs können für demodulierte und/oder dekodierte X-Band-Signale bis 500 MHz Bandbreite konfiguriert werden.

AWS Ground Station stellt Vorlagen für beide Datenstromformate bereit, die zeigen, wie der Service verwendet wird. Verwenden Sie diese Anleitung, um die richtige Vorlage für Sie zu finden.

Verfügbare Vorlagen

Sie können eine vorkonfigurierte Vorlage verwenden, um direkte Broadcast-Daten von den Satelliten Aqua, SNPP, JPSS-1/NOAA-20 und Terra zu empfangen. Diese AWS CloudFormation Vorlagen enthalten die erforderlichen AWS Ground Station und Amazon S3-Ressourcen, um Kontakte zu planen und auszuführen und die Daten in einem Amazon S3-Bucket in Ihrem Konto zu empfangen. Wenn Aqua, SNPP und JPSS-1/NOAA-20 und Terra nicht in Ihr Konto integriert sind, finden Sie weitere Informationen unter Kunden-Onboarding.

Vorlagen für die Datenbereitstellung im Bundband

Wenn Sie die Datenzustellung für Ihren Kontakt verwenden, verwenden Sie die folgenden AWS CloudFormation Vorlagen.

- Die AWS CloudFormation Vorlage mit dem Namen `AquaSnppJpss-1DemodDecodeS3DataDelivery.yml` enthält einen Amazon S3-Bucket und die erforderlichen AWS Ground Station Ressourcen, um Kontakte zu planen und demodulierte und dekodierte Direktübertragungsdaten zu erhalten. Diese Vorlage ist ein guter Ausgangspunkt, wenn Sie planen, die Daten mit der NASA Direct Readout Labs Software (RT-STPS und IPOPP) zu verarbeiten.

  Verwenden Sie den folgenden Befehl AWS CLI, um die Vorlage mit herunterzuladen:

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

  Die Vorlage kann in der Konsole angezeigt und heruntergeladen werden, indem Sie in Ihrem Browser zur folgenden URL navigieren:

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

  Sie können die Vorlage AWS CloudFormation über den folgenden Link direkt in angeben:

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

- Die AWS CloudFormation Vorlage mit dem Namen `AquaSnppJpss-1TerraDigIfS3DataDelivery.yml` enthält einen Amazon S3-Bucket und die erforderlichen AWS Ground Station Ressourcen, um Kontakte zu planen und VITA-49-Signal/IP-Direct-Broadcast-Daten zu erhalten. Diese Vorlage ist ein guter Ausgangspunkt, wenn Sie planen, die Daten mit einem softwaredefinierten Optionsfeld (SDR) zu verarbeiten, um die Daten vor der Nachbearbeitung zu demodulieren und zu dekodieren.

  Verwenden Sie den folgenden Befehl AWS CLI, um die Vorlage mit herunterzuladen:

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

  Die Vorlage kann in der Konsole angezeigt und heruntergeladen werden, indem Sie in Ihrem Browser zur folgenden URL navigieren:

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

  Sie können die Vorlage AWS CloudFormation über den folgenden Link direkt in angeben:

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

Welche Ressourcen definieren diese Vorlage?

Beide Vorlagen enthalten dieselben Ressourcen, wobei der einzige Unterschied die Antennenkonfigurationen ist. Weitere Informationen finden Sie in der Beschreibung der Antenna-Konfiguration unten.

- Amazon S3-Bucket – Der Bucket, an den die Downlink-Daten übermittelt werden. Der Name dieses Buckets beginnt mit `aws-groundstation`, um die in S3 Recording Config beschriebenen Kriterien zu erfüllen.
- IAM-Rolle – Eine Rolle, die vom `groundstation.amazonaws.com` Service-Prinzipal übernommen werden kann, der beim Schreiben der verlinkten Daten in Ihren Amazon S3-Bucket AWS Ground Station übernimmt.
- Amazon S3-Bucket-Richtlinie – Eine Richtlinie, die es der IAM-Rolle ermöglicht, die folgenden Aktionen für Ihren Amazon S3-Bucket und seine Objekte auszuführen:

  - `s3:GetBucketLocation`
  - `s3:PutObject`
- Tracking Config – Eine AWS Ground Station Tracking-Konfiguration, die definiert, wie das Antennensystem Ihren Satelliten verfolgt, während er durch den Sternchen läuft.
- S3-Aufzeichnungskonfiguration – Eine AWS Ground Station S3-Aufzeichnungskonfiguration, die auf den Amazon S3-Bucket und die IAM-Rolle verweist, die bei der Bereitstellung Ihrer Daten verwendet AWS Ground Station werden soll.
- Antenna Config – Eine AWS Ground Station Antennenkonfiguration, die angibt, wie die AWS Ground Station Antenne während eines Kontakts konfiguriert wird. Die `AquaSnppJpss-1DemodDecodeS3DataDelivery.yml` Vorlage enthält eine Konfiguration für die Demod-Dekodierung der Antenne, die die AWS Ground Station Antenne so konfiguriert, dass die Downlink-Daten vor der Bereitstellung an Ihren Amazon S3-Bucket demoduliert und dekodiert werden. enthält `AquaSnppJpss-1TerraDigIfS3DataDelivery.yml` stattdessen eine Antennen-Downlink-Konfiguration, die die AWS Ground Station Antenne so konfiguriert, dass die Daten als VITA-49-Signal/IP-Pakete an Amazon S3 übermittelt werden.
- Missionsprofil – Ein AWS Ground Station Missionsprofil, das alle AWS Ground Station Konfigurationen gruppiert, damit Sie Kontakte mithilfe der referenzierten Konfigurationen planen und ausführen können.

Breitebandvorlagen AWS CloudFormation für die DigIf S3-Datenbereitstellung

Breitenband-DigIF-Datenbereitstellungsvorlagen

Wenn Sie die DigIF-Datenzustellung (Breitband Digital Intermediate Frequency) für Ihren Kontakt verwenden, verwenden Sie die folgenden AWS CloudFormation Vorlagen.

- Die AWS CloudFormation Vorlage mit dem Namen `DirectBroadcastSatelliteWbDigIfS3DataDelivery.yml` enthält einen Amazon S3-Bucket und die erforderlichen AWS Ground Station Ressourcen, um Kontakte zu planen und VITA-49-Signal/IP-Direct-Broadcast-Daten über den - AWS Ground Station Agenten zu empfangen. Diese Vorlage ist ein guter Ausgangspunkt, wenn Sie planen, die Daten mit einem softwaredefinierten Optionsfeld (SDR) zu verarbeiten, um die Daten vor der Nachbearbeitung zu demodulieren und zu dekodieren. Weitere Informationen zum - AWS Ground Station Agent finden Sie unter AWS Ground Station Benutzerhandbuch für Agenten.

Verwenden Sie den folgenden Befehl AWS CLI, um die Vorlage mit herunterzuladen:

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

Die Vorlage kann in der Konsole angezeigt und heruntergeladen werden, indem Sie in Ihrem Browser zur folgenden URL navigieren:

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

Sie können die Vorlage AWS CloudFormation über den folgenden Link direkt in angeben:

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

Welche Ressourcen definiert diese Vorlage?

- Amazon S3-Bucket – Der Bucket, an den die Downlink-Daten übermittelt werden. Der Name dieses Buckets beginnt mit `aws-groundstation`, um die in S3 Recording Config beschriebenen Kriterien zu erfüllen.
- IAM-Rolle – Eine Rolle, die vom -`groundstation.amazonaws.com`Service-Prinzipal übernommen werden kann, der beim Schreiben der verlinkten Daten in Ihren Amazon S3-Bucket AWS Ground Station übernimmt.
- Amazon S3-Bucket-Richtlinie – Eine Richtlinie, die es der IAM-Rolle ermöglicht, die folgenden Aktionen für Ihren Amazon S3-Bucket und seine Objekte auszuführen:
  - `s3:GetBucketLocation`
  - `s3:PutObject`
- AWS KMS Schlüssel – Ein AWS KMS Schlüssel, der zum Verschlüsseln von Datenflüssen verwendet wird.
- Ground Station-Schlüsselrolle – Die IAM- AWS Ground Station Rolle, die übernimmt, um auf zuzugreifen und den AWS KMS Schlüssel zum Entschlüsseln von Datenströmen zu verwenden
- Ground Station-Schlüsselzugriffsrichtlinie – Die IAM-Richtlinie, die die Aktionen definiert, die auf dem Datenbereitstellungsschlüssel ausgeführt werden AWS Ground Station können

- Tracking Config – Eine AWS Ground Station Tracking-Konfiguration, die definiert, wie das Antennensystem Ihren Satelliten verfolgt, während er durch den Sternchen läuft.
- S3-Aufzeichnungskonfiguration – Eine AWS Ground Station S3-Aufzeichnungskonfiguration, die auf den Amazon S3-Bucket und die IAM-Rolle verweist AWS Ground Station , die bei der Bereitstellung Ihrer Daten verwenden soll.
- Antenna-Konfigurationen für Bol, SNPP, JPSS-1/NOAA-20 und Terra – Drei separate AWS Ground Station Antennenkonfigurationen, die angeben, wie die AWS Ground Station Antenne während eines Kontakts mit Bol, SNPP, JPSS-1/NOAA-20 und Terra konfiguriert werden soll. Die Vorlage enthält eine Antennen-Downlink-Konfiguration, die die AWS Ground Station Antenne so konfiguriert, dass die Daten als VITA-49-Signal/IP-Pakete an Ihre Amazon S3 übermittelt werden.
- Missionsprofile für, SNPP, JPSS-1/NOAA-20 und Terra – Drei separate AWS Ground Station Missionsprofile, die alle AWS Ground Station Konfigurationen gruppieren, damit Sie Kontakte mithilfe der Konfigurationen planen und ausführen können, auf die mit Bol, SNPP, JPSS-1/NOAA-20 und Terra verwiesen wird.

Erstellen einer eigenen Vorlage

Um die Ressourcen für die Planung und Ausführung von Kontakten für Ihre eigenen Satelliten zu konfigurieren, müssen Sie die AWS Ground Station Ressourcen in Ihrem Konto so konfigurieren, dass sie den Einstellungen Ihres Satelliten entsprechen. Es ist nicht einfach, dies allein zu tun. Das AWS Ground Station Team steht Ihnen bei der Konfiguration der AWS Ground Station Ressourcen in Ihrem Konto zur Verfügung, um Downlinks von und Uplinks zu Ihrem Satelliten herzustellen. Um Ihren eigenen Satelliten für die Verwendung mit zu konfigurieren AWS Ground Station, wenden Sie sich an den AWS Support .

Schritt 2: Konfigurieren eines - AWS CloudFormation Stacks

Nachdem Sie die Vorlage ausgewählt haben, die für Ihren Anwendungsfall am besten geeignet ist, konfigurieren Sie einen - AWS CloudFormation Stack. Die in diesem Verfahren erstellten Ressourcen werden für die Region konfiguriert, in der Sie sich bei der Erstellung befinden.

1. Wählen Sie in der die AWS Management Console Option Services > CloudFormation aus.
2. Klicken Sie im Navigationsbereich auf Stacks. Klicken Sie dann auf Create stack (Stack erstellen) > With new resources (standard) (Mit neuen Ressourcen (Standard)).

3. Geben Sie auf der Seite Create Stack (Stack erstellen) die Vorlage an, die Sie in the section called “Schritt 1: Auswählen einer - AWS CloudFormation Vorlage” ausgewählt haben, indem Sie wie folgt vorgehen:

   a. Wählen Sie Amazon S3 URL als Vorlagenquelle und kopieren Sie die URL der Vorlage, die Sie in Amazon S3 URL verwenden möchten. Wählen Sie anschließend Weiter.

   b. Wählen Sie Upload a template file (Eine Vorlagendatei hochladen) als Ihre Vorlagenquelle aus und klicken Sie anschließend auf Choose File (Datei auswählen). Laden Sie die in the section called “Schritt 1: Auswählen einer - AWS CloudFormation Vorlage” heruntergeladene Vorlage hoch. Wählen Sie anschließend Weiter.

4. Führen Sie die folgenden Schritte auf der Seite Stack-Details angeben aus:

   a. Geben Sie in das Feld Stack Name (Stack-Name) einen Namen ein. Wir empfehlen, einen einfachen Namen zu verwenden, um die Gefahr von Fehlern in der Zukunft zu verringern.

   b. Wählen Sie Weiter aus.

5. Konfigurieren Sie Stack-Optionen und erweiterte Optionen für Ihre Amazon EC2-Instance.

   a. Fügen Sie in den Abschnitten Tagsund Permissions (Berechtigungen) alle Tags und Berechtigungen hinzu.

   b. Nehmen Sie alle Änderungen für Ihre Stack-Richtlinie, Rollback-Konfiguration, Benachrichtigungsoptionen, und Stack-Erstellungsoptionenvor.

   c. Wählen Sie Weiter aus.

6. Nachdem Sie die Details zum Stack überprüft haben, wählen Sie die Bestätigung der Capabilities (Funktionen) und klicken auf Create stack (Stapel erstellen).

AWS Ground Station Benutzerhandbuch für Agenten

Themen

Übersicht

Was ist der AWS Ground Station Agent?

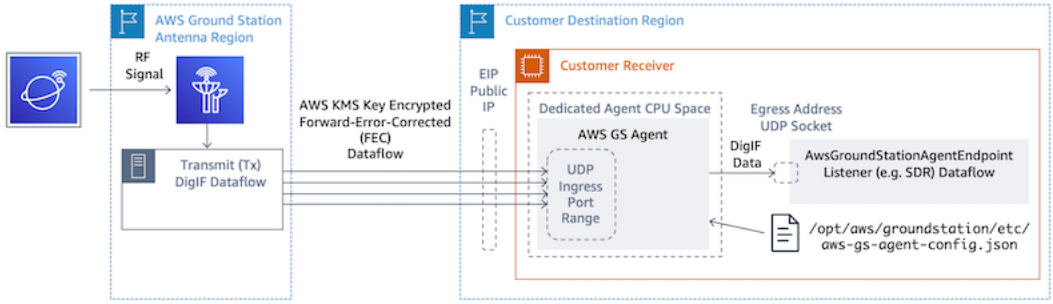
Der AWS Ground Station Agent, der als RPM erhältlich ist, ermöglicht es AWS Ground Station Kunden, bei Kontakten mit der AWS Ground Station synchrone Wideband Digital Intermediate Frequency (DigIF) -Datenflüsse zu empfangen (Downlink). Kunden können zwei Optionen für die Datenbereitstellung wählen:

1. Datenlieferung an eine EC2-Instance — Datenlieferung an eine kundeneigene EC2-Instance. AWS Ground Station Kunden verwalten den AWS Ground Station Agenten. Diese Option eignet sich möglicherweise am besten für Sie, wenn Sie eine Datenverarbeitung nahezu in Echtzeit benötigen. Informationen zur EC2-Datenbereitstellung finden Sie im Datenlieferung an Amazon EC2 Leitfaden.

2. Datenlieferung an einen S3-Bucket — Datenlieferung an einen kundeneigenen AWS S3-Bucket über einen von Ground Station verwalteten Service. Informationen zur S3-Datenlieferung finden Sie im Erste Schritte mit AWS Ground Station Leitfaden.

Bei beiden Arten der Datenbereitstellung müssen Kunden eine Reihe von AWS-Ressourcen erstellen. Die Verwendung von CloudFormation Vorlagen zur Erstellung Ihrer AWS-Ressourcen wird dringend empfohlen, um Zuverlässigkeit, Genauigkeit und Unterstützbarkeit zu gewährleisten. Jeder Kontakt kann nur Daten an EC2 oder S3 liefern, aber nicht an beide gleichzeitig.

> **Note**
>
> Da es sich bei S3 Data Delivery um einen von der Ground Station verwalteten Service handelt, konzentriert sich dieser Leitfaden auf die Datenbereitstellung an Ihre EC2-Instance (s).



DigiF-Datenfluss von einer AWS Ground Station Antennenregion zu Ihrer EC2-Instance mit Ihrem Software-Defined Radio (SDR) oder einem ähnlichen Listener.

Funktionen des Agenten AWS Ground Station

Der AWS Ground Station Agent empfängt Downlink-Daten (Digital Intermediate Frequency, DigIF) und sendet entschlüsselte Daten aus, die Folgendes ermöglichen:

- DigiF-Downlink-Fähigkeit von 40 MHz bis 400 MHz Bandbreite.
- DigiF-Datenübermittlung mit hoher Rate und geringem Jitter an jede öffentliche IP (AWS Elastic IP) im AWS-Netzwerk.
- Zuverlässige Datenlieferung mit Forward Error Correction (FEC).

- Sichere Datenübermittlung mit einem vom Kunden verwalteten AWS KMS Schlüssel zur Verschlüsselung.

Agentenanforderungen

> **Note**
>
> In diesem Leitfaden für AWS Ground Station Agenten wird davon ausgegangen, dass Sie mithilfe des Leitfadens an die Ground Station eingestiegen sind. Einrichten AWS Ground Station

Die EC2-Instance des AWS Ground Station Agent-Empfängers benötigt eine Reihe von abhängigen AWS-Ressourcen, um DigiF-Daten zuverlässig und sicher an Ihre Endgeräte zu liefern.

1. Eine VPC, in der der EC2-Empfänger gestartet werden soll.
2. Ein AWS-KMS-Schlüssel für die Datenverschlüsselung/-entschlüsselung.
3. Ein SSH-Schlüssel oder ein EC2-Instanzprofil, das für SSM Session Manager konfiguriert ist.
4. Netzwerk-/Sicherheitsgruppenregeln, die Folgendes ermöglichen:
    1. UDP-Verkehr von AWS Ground Station den Ports, die in Ihrer Datenfluss-Endpunktgruppe angegeben sind. Der Agent reserviert eine Reihe von zusammenhängenden Ports, die zur Übertragung von Daten an die Endpunkte des eingehenden Datenflusses verwendet werden.
    2. SSH-Zugriff auf Ihre Instance (Hinweis: Sie können alternativ AWS Session Manager verwenden, um auf Ihre EC2-Instance zuzugreifen).
    3. Lesezugriff auf einen öffentlich zugänglichen S3-Bucket für die Agentenverwaltung.
    4. SSL-Verkehr auf Port 443 ermöglicht es dem Agenten, mit dem AWS Ground Station Dienst zu kommunizieren.
    5. Verkehr aus der Liste der AWS Ground Station verwalteten Präfixe`com.amazonaws.global.groundstation`.

Darüber hinaus ist eine VPC-Konfiguration mit einem öffentlichen Subnetz erforderlich. Hintergrundinformationen zur Subnetzkonfiguration finden Sie im VPC-Benutzerhandbuch.

Kompatible Konfigurationen:

1. Eine Elastic IP, die Ihrer EC2-Instance in einem öffentlichen Subnetz zugeordnet ist.
2. Eine Elastic IP, die einer ENI in einem öffentlichen Subnetz zugeordnet ist und mit Ihrer EC2-Instance verbunden ist (in einem beliebigen Subnetz).

Sie können dieselbe Sicherheitsgruppe wie Ihre EC2-Instance verwenden oder eine mit mindestens den folgenden Mindestregeln angeben:

- UDP-Verkehr von AWS Ground Station den Ports, die in Ihrer Datenfluss-Endpunktgruppe angegeben sind.

Weitere Informationen finden Sie im Abschnitt „Vorlagen für die Bereitstellung von Breitband-DigIF-Daten“, in denen Auswahl einer Vorlage beispielsweise AWS CloudFormation EC2-Datenliefervorlagen mit diesen Ressourcen vorkonfiguriert sind.

VPC-Diagramme

Diagramm: Eine Elastic IP, die Ihrer EC2-Instance in einem öffentlichen Subnetz zugeordnet ist

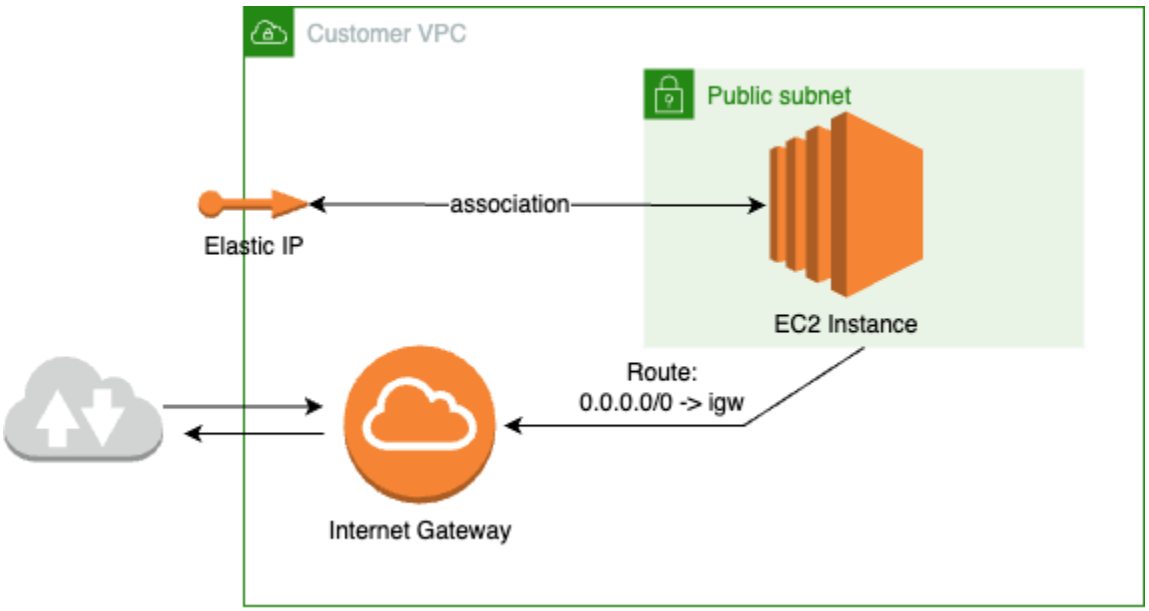
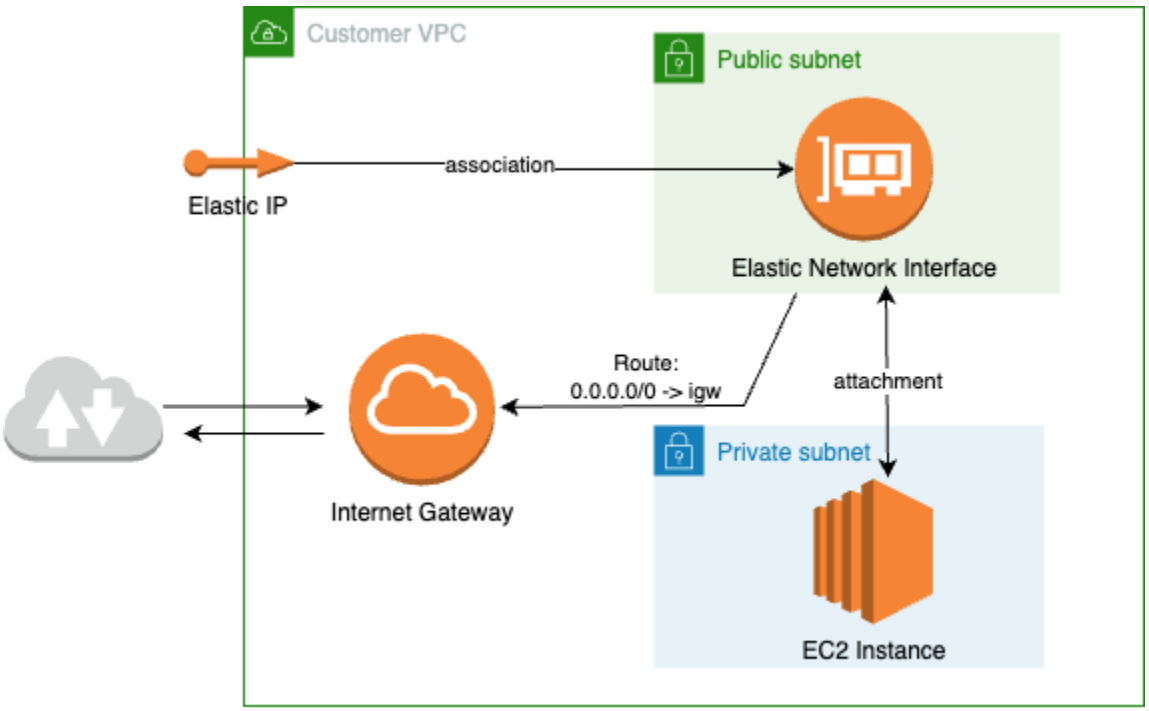


Diagramm: Eine Elastic IP, die einer ENI in einem öffentlichen Subnetz zugeordnet ist und mit Ihrer EC2-Instance in einem privaten Subnetz verbunden ist



Unterstütztes Betriebssystem

Amazon Linux 2 mit Kernel 5.10+.

Die unterstützten Instance-Typen sind unter aufgeführt Auswahl der EC2-Instance und CPU-Planung

Datenzustellung über einen AWS Ground Station Agenten

Die folgenden Diagramme geben einen Überblick darüber, wie Daten AWS Ground Station bei Kontakten mit Breitband-Digitalinterfrequenz (DigIF) durchfließen.

Der AWS Ground Station Agent kümmert sich um die Orchestrierung der Datenebenenkomponenten für einen Kontakt. Vor der Planung eines Kontakts muss der Agent korrekt konfiguriert, gestartet und registriert sein (die Registrierung erfolgt automatisch beim Start des Agenten). AWS Ground Station Darüber hinaus muss die Datenempfangssoftware (z. B. ein softwaredefiniertes Radio) ausgeführt und so konfiguriert sein, dass sie Daten an der Ausgangsadresse AwsGroundStationAgentEndpointempfängt.

Im Hintergrund empfängt der AWS Ground Station Agent Aufgaben von der AWS KMS Verschlüsselung, die während der Übertragung angewendet wurde, AWS Ground Station und macht sie rückgängig, bevor er sie an den Zielendpunkt EgressAddress weiterleitet, an dem Ihr

Software Defined Radio (SDR) zuhört. Der AWS Ground Station Agent und die zugrundeliegenden Komponenten respektieren die in der Konfigurationsdatei festgelegten CPU-Grenzen, um sicherzustellen, dass die Leistung anderer Anwendungen, die auf der Instanz ausgeführt werden, nicht beeinträchtigt wird.

Kunden müssen den AWS Ground Station Agenten auf der Empfängerinstanz ausführen lassen, die am Kontakt beteiligt war. Ein einzelner AWS Ground Station Agent kann mehrere Datenflüsse orchestrieren, wie unten dargestellt, wenn der Kunde es vorzieht, alle Datenflüsse auf einer einzigen Empfängerinstanz zu empfangen.

Mehrere Datenflüsse, ein einziger Empfänger

Beispielszenario:

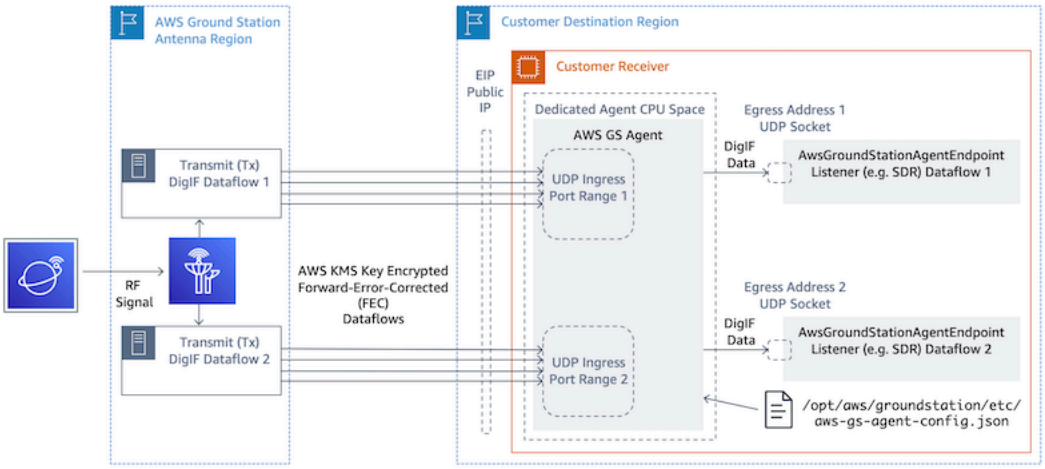
Der Kunde möchte zwei Antennen-Downlinks als DigiF-Datenflüsse auf derselben EC2-Empfängerinstanz empfangen. Die beiden Downlinks werden 200 MHz und 100 MHz haben.

AwsGroundStationAgentEndpoints:

Es wird zwei `AwsGroundStationAgentEndpoint` Ressourcen geben, eine für jeden Datenfluss. Beide Endpunkte werden dieselbe öffentliche IP-Adresse () haben. `ingressAddress.socketAddress.name` Die Eingänge sollten `portRange` sich nicht überschneiden, da die Datenflüsse auf derselben EC2-Instance empfangen werden. Beide müssen einzigartig sein`egressAddress.socketAddress.port`.

CPU-Planung:

- 1 Kern (2 vCPU) zum Ausführen des Single AWS Ground Station Agents auf der Instance.
- 6 Kerne (12 vCPU) für den Empfang von DigIF Dataflow 1 (200-MHz-Suche in der Tabelle). Planung von CPU-Kernen
- 4 Kerne (8 vCPU) für den Empfang von DigIF Dataflow 2 (100-MHz-Suche in der Tabelle). Planung von CPU-Kernen
- Gesamter dedizierter Agenten-CPU-Speicherplatz = 11 Kerne (22 vCPU) auf demselben Socket.



Mehrere Datenflüsse, mehrere Empfänger

Beispielszenario:

Der Kunde möchte zwei Antennen-Downlinks als DigiF-Datenflüsse auf verschiedenen EC2-Empfängerinstanzen erhalten. Beide Downlinks werden 400 MHz haben.

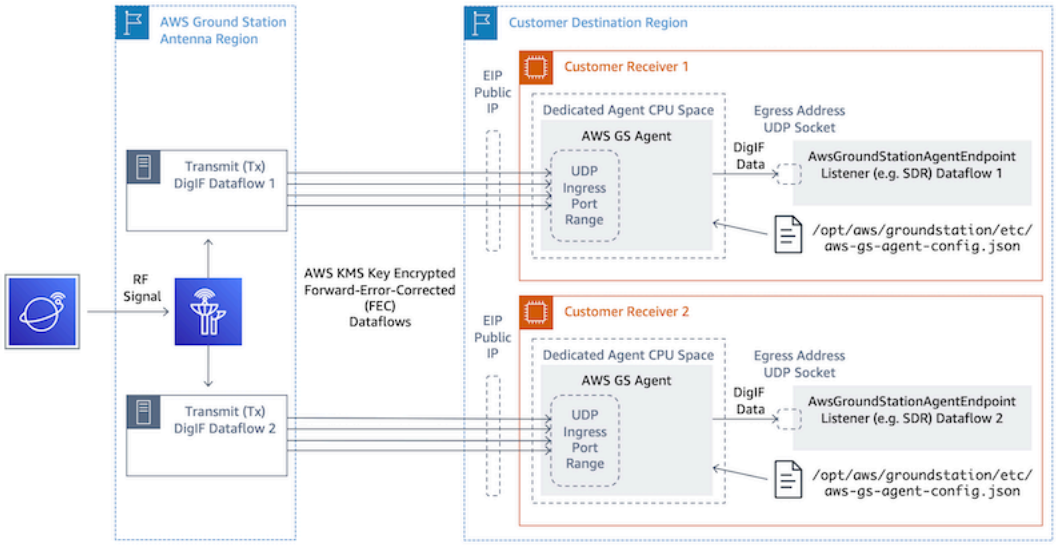
AwsGroundStationAgentEndpoints:

Es wird zwei `AwsGroundStationAgentEndpoint` Ressourcen geben, eine für jeden Datenfluss. Die Endpunkte werden eine andere öffentliche IP-Adresse () haben. `ingressAddress.socketAddress.name` Es gibt keine Beschränkung der Portwerte für beide`ingressAddress`, `egressAddress` da die Datenflüsse auf einer separaten Infrastruktur empfangen werden und nicht miteinander in Konflikt geraten.

CPU-Planung:

- Empfänger-Instanz 1
  - 1 Kern (2 vCPU) zum Ausführen des Single AWS Ground Station Agents auf der Instance.
  - 9 Kerne (18 vCPU) für den Empfang von DigIF Dataflow 1 (400-MHz-Suche in der Tabelle). Planung von CPU-Kernen
  - Gesamter dedizierter Agenten-CPU-Speicherplatz = 10 Kerne (20 vCPU) auf demselben Socket.
- Empfänger-Instanz 2
  - 1 Kern (2 vCPU) zum Ausführen des Single AWS Ground Station Agents auf der Instance.
  - 9 Kerne (18 vCPU) für den Empfang von DigIF Dataflow 2 (400-MHz-Suche in der Tabelle). Planung von CPU-Kernen

- Gesamter dedizierter Agenten-CPU-Speicherplatz = 10 Kerne (20 vCPU) auf demselben Socket.



Auswahl der EC2-Instance und CPU-Planung

Unterstützte EC2-Instance-Typen

Aufgrund der rechenintensiven Datenbereitstellungsworkflows benötigt der AWS Ground Station Agent für den Betrieb dedizierte CPU-Kerne. Wir unterstützen die folgenden Instance-Typen. Planung von CPU-KernenEntscheiden Sie selbst, welcher Instance-Typ am besten zu Ihrem Anwendungsfall passt.

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne
c5.12xlarge	48	24
c5.18xlarge	72	36
c5.24xlarge	96	48
c5n.18xlarge	72	36
c5n.metal	72	36
c6i.32xlarge	128	64

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne
g4dn.12xgroß	48	24
g4dn.16xgroß	64	32
g4dn.metal	96	48
m4.16xlarge	64	32
m5.12xlarge	48	24
m5.24xlarge	96	48
m6i.32xlarge	128	64
p3dn.24xgroß	96	48
p4d.24xgroß	96	48
r5.24xlarge	96	48
r5.metal	96	48
r5n.24xlarge	96	48
r5n.metal	96	48
r6i.32xlarge	128	64

Planung von CPU-Kernen

Der AWS Ground Station Agent benötigt dedizierte Prozessorkerne, die sich den L3-Cache für jeden Datenfluss teilen. Der Agent ist für die Nutzung von CPU-Paaren mit Hyper-Threading (HT) konzipiert und erfordert, dass HT-Paare für seine Verwendung reserviert werden. Ein Hyper-Thread-Paar ist ein Paar virtueller CPUs (vCPU), die in einem einzelnen Kern enthalten sind. Die folgende Tabelle bietet eine Zuordnung der Datenfluss-Datenrate zur erforderlichen Anzahl von Kernen, die für den Agenten für einen einzelnen Datenfluss reserviert sind. In dieser Tabelle wird von Cascade Lake- oder neueren CPUs ausgegangen und sie gilt für alle unterstützten Instance-Typen. Wenn Ihre Bandbreite zwischen den Einträgen in der Tabelle liegt, wählen Sie die nächsthöhere aus.

Der Agent benötigt einen zusätzlichen reservierten Kern für Verwaltung und Koordination. Die Gesamtzahl der benötigten Kerne entspricht also der Summe der benötigten Kerne (aus der folgenden Tabelle) für jeden Datenfluss plus einem einzelnen zusätzlichen Kern (2 vCPUs).

AntennaDownlink Bandbreite (MHz)	Erwartete VITA-49.2 DigiF-Datenrate (MB/s)	Anzahl der Kerne (HT-CPU-Paare)	vCPU insgesamt
50	1000	3	6
100	2000	4	8
150	3000	5	10
200	4000	6	12
250	5000	6	12
300	6 000	7	14
350	7000	8	16
400	8000	9	18

Sammeln von Architekturinformationen

`lscpu`bietet Informationen über die Architektur Ihres Systems. Die Basisausgabe zeigt, welche vCPUs (als „CPU“ bezeichnet) zu welchen NUMA-Knoten gehören (und jeder NUMA-Knoten teilt sich einen L3-Cache). Im Folgenden untersuchen wir eine `c5.24xlarge` Instanz, um die für die Konfiguration des Agenten erforderlichen Informationen zu sammeln. AWS Ground Station Dazu gehören nützliche Informationen wie die Anzahl der vCPUs, Kerne und die Zuordnung von vCPU zu Knoten.

```
> 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    <------
```

Dem AWS Ground Station Agenten zugewiesene Kerne sollten beide vCPUs für jeden zugewiesenen Kern enthalten. Alle Kerne für einen Datenfluss müssen auf demselben NUMA-Knoten vorhanden sein. Die `-p` Option für den `lscpu` Befehl liefert uns die Core-zu-CPU-Zuordnungen, die für die Konfiguration des Agenten erforderlich sind. Die relevanten Felder sind CPU (was wir als vCPU bezeichnen), Core und L3 (was angibt, welcher L3-Cache von diesem Kern gemeinsam genutzt wird). Beachten Sie, dass bei den meisten Intel-Prozessoren der NUMA-Knoten dem L3-Cache entspricht.

Betrachten Sie die folgende Teilmenge der `lscpu -p` Ausgabe als Beispiel `c5.24xlarge` (aus Gründen der Übersichtlichkeit abgekürzt und formatiert).

```
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
```

Aus der Ausgabe können wir ersehen, dass Core 0 die vCPUs 0 und 16, Core 1 die vCPUs 1 und 17 und Core 2 die vCPUs 2 und 18 umfasst. Mit anderen Worten, die Hyper-Thread-Paare sind: 0 und 16, 1 und 17, 2 und 18.

Beispiel für eine CPU-Zuweisung

Als Beispiel verwenden wir eine `c5.24xlarge` Instanz für einen Breitband-Downlink mit doppelter Polarität bei 350 MHz. Aus der Tabelle in wissen Planung von CPU-Kernen wir, dass ein 350-MHz-Downlink 8 Kerne (16 vCPUs) für den einzelnen Datenfluss benötigt. Das bedeutet, dass dieses Setup mit dualer Polarität, das zwei Datenflüsse verwendet, insgesamt 16 Kerne (32 vCPUs) plus einen Kern (2 vCPUs) für den Agenten benötigt.

Wir wissen, dass die Ausgabe für und beinhaltet. `lscpu` `c5.24xlarge` `NUMA node0 CPU(s): 0-23,48-71` `NUMA node1 CPU(s): 24-47,72-95` Da NUMA-Node0 mehr hat, als wir benötigen, werden wir nur die Kerne 0-23 und 48-71 zuweisen.

Zunächst wählen wir 8 Kerne für jeden Datenfluss aus, die sich einen L3-Cache oder einen NUMA-Knoten teilen. Dann suchen wir in der `lscpu -p` Ausgabe nach den entsprechenden vCPUs (mit „CPU“ bezeichnet). Anhang: `lscpu -p` Ausgabe (vollständig) für c5.24xlarge Ein Beispiel für einen Kernauswahlprozess könnte wie folgt aussehen:

- Reservieren Sie die Kerne 0-1 für das Betriebssystem.
- Flow 1: Wählen Sie die Kerne 2-9 aus, die den vCPUs 2-9 und 50-57 zugeordnet sind.
- Flow 2: Wählen Sie die Kerne 10-17 aus, die den vCPUs 10-17 und 58-65 zugeordnet sind.
- Agentenkern: Wählen Sie Core 18 aus, der den vCPUs 18 und 66 zugeordnet ist.

Dies führt zu den vCPUs 2-18 und 51-66, sodass die Liste, die dem Agenten zur Verfügung gestellt werden muss, lautet. `[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]` Sie sollten sicherstellen, dass Ihre eigenen Prozesse nicht auf diesen CPUs ausgeführt werden, wie unter beschrieben. Dienste und Prozesse werden zusammen mit dem Agenten ausgeführt AWS Ground Station

Beachten Sie, dass die in diesem Beispiel ausgewählten spezifischen Kerne etwas willkürlich sind. Andere Gruppen von Kernen würden funktionieren, solange sie die Anforderung erfüllen, dass sich alle für jeden Datenfluss einen L3-Cache teilen.

Anhang: **`lscpu -p`** Ausgabe (vollständig) für 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
```

Den Agenten installieren

Der AWS Ground Station Agent kann auf folgende Weise installiert werden:

1. AWS CloudFormation Vorlage (empfohlen).
2. Manuelle Installation auf Amazon EC2.

Vorlage verwenden CloudFormation

Die CloudFormation EC2-Datenliefervorlage erstellt die erforderlichen AWS-Ressourcen, um Daten an Ihre EC2-Instance zu liefern. Diese AWS CloudFormation Vorlage verwendet das AWS Ground Station verwaltete AMI, auf dem der AWS Ground Station Agent vorinstalliert ist. Das Boot-Skript der erstellten EC2-Instance füllt dann die Agenten-Konfigurationsdatei auf und wendet die erforderliche Leistungsoptimierung an (). Leistungsoptimierung der EC2-Instance

Schritt 1: AWS-Ressourcen erstellen

Erstellen Sie Ihren AWS-Ressourcen-Stack mithilfe einer VorlageBreitband-DigIF-Vorlage für Satelliten-Breitbandübertragung (Breitband).

Schritt 2: Überprüfen Sie den Agentenstatus

Standardmäßig ist der Agent konfiguriert und aktiv (gestartet). Um den Agentenstatus zu überprüfen, können Sie eine Verbindung zur EC2-Instance (SSH oder SSM Session Manager) herstellen und nachschauen. AWS Ground Station Status des Agenten

Manuelle Installation auf EC2

Ground Station empfiehlt zwar die Verwendung von CloudFormation Vorlagen für die Bereitstellung Ihrer AWS-Ressourcen, es kann jedoch Anwendungsfälle geben, in denen die Standardvorlage möglicherweise nicht ausreicht. In solchen Fällen empfehlen wir Ihnen, die Vorlage an Ihre Bedürfnisse anzupassen. Wenn das immer noch nicht Ihren Anforderungen entspricht, können Sie Ihre AWS-Ressourcen manuell erstellen und den Agenten installieren.

Schritt 1: AWS-Ressourcen erstellen

Anweisungen Manuelles Erstellen und Konfigurieren von Ressourcen zur manuellen Einrichtung der AWS-Ressourcen, die für einen Kontakt erforderlich sind, finden Sie unter.

Die AwsGroundStationAgentEndpointRessource definiert einen Endpunkt für den Empfang eines DigiF-Datenflusses über den AWS Ground Station Agenten und ist entscheidend für die erfolgreiche Kontaktaufnahme. Die API-Dokumentation befindet sich zwar in der API-Referenz, in diesem Abschnitt werden jedoch kurz Konzepte behandelt, die für den Agenten relevant sind. AWS Ground Station

Auf dem Endpunkt empfängt der AWS Ground Station Agent AWS KMS verschlüsselten UDP-Verkehr von der Antenne. `ingressAddress` Das `socketAddress` `name` ist die öffentliche IP der EC2-Instance (von der angehängten EIP). Es `portRange` sollten mindestens 300 zusammenhängende Ports in einem Bereich sein, der für jegliche andere Nutzung reserviert wurde. Detaillierte Anweisungen finden Sie unter Eingangsports reservieren — wirkt sich auf das Netzwerk aus. Diese Ports müssen so konfiguriert werden, dass sie eingehenden UDP-Verkehr in der Sicherheitsgruppe für die VPC zulassen, auf der die Empfängerinstanz ausgeführt wird.

Der Endpunkt `egressAddress` ist der Ort, an dem der Agent den DigiF-Datenfluss an den Kunden weitergibt. Der Kunde sollte über eine Anwendung (z. B. SDR) verfügen, die die Daten über einen UDP-Socket an diesem Standort empfängt.

Schritt 2: EC2-Instanz erstellen

Die folgenden AMIs werden unterstützt:

1. AWS Ground Station AMI — `groundstation-al2-gs-agent-ami-*` wobei * das Datum ist, an dem das AMI erstellt wurde — wird mit installiertem Agenten geliefert (empfohlen).
2. `amzn2-ami-kernel-5.10-hvm-x86_64-gp2`.

Schritt 3: Laden Sie den Agenten herunter und installieren Sie ihn

> **Note**
>
> Die Schritte in diesem Abschnitt müssen abgeschlossen werden, wenn Sie im vorherigen Schritt nicht das AWS Ground Station Agent-AMI ausgewählt haben.

Laden Sie den Agenten herunter

Der AWS Ground Station Agent ist in regionsspezifischen S3-Buckets verfügbar und kann über die AWS-Befehlszeile (CLI) auf Support-EC2-Instances heruntergeladen werden, `s3://groundstation-wb-digif-software-${AWS::Region}/aws-groundstation-agent/latest/amazon_linux_2_x86_64/aws-groundstation-agent.rpm` wobei $ {AWS::Region} auf eine der unterstützten AWS-Bodenstationskonsole und Datenlieferregionen verweist.

Beispiel: Laden Sie die neueste RPM-Version aus der AWS-Region us-east-2 lokal in den Ordner / tmp herunter.

```
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
```

Wenn Sie eine bestimmte Version des AWS Ground Station Agenten herunterladen müssen, können Sie sie aus dem versionsspezifischen Ordner im S3-Bucket herunterladen.

Beispiel: Laden Sie Version 1.0.2716.0 von rpm aus der AWS-Region us-east-2 lokal in den Ordner /tmp herunter.

```
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**
>
> Wenn Sie überprüfen möchten, ob das RPM, das Sie heruntergeladen haben, verkauft wurde, folgen Sie den Anweisungen für. AWS Ground StationÜberprüfung der RPM-Installation

Installieren Sie den Agenten

```
sudo yum install ${MY_RPM_FILE_PATH}

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

Schritt 4: Konfigurieren Sie den Agenten

Nach der Installation des Agenten müssen Sie die Agenten-Konfigurationsdatei aktualisieren. Siehe Den Agenten konfigurieren.

Schritt 5: Wenden Sie die Leistungsoptimierung an

AWS Ground Station Agent-AMI: Wenn Sie im vorherigen Schritt das AWS Ground Station Agent-AMI ausgewählt haben, wenden Sie die folgenden Leistungsoptimierungen an.

- Hardware-Interrupts und Empfangswarteschlangen optimieren — wirkt sich auf CPU und Netzwerk aus
- Eingangsports reservieren — wirkt sich auf das Netzwerk aus
- Neustart

Andere AMIs: Wenn Sie im vorherigen Schritt ein anderes AMI ausgewählt haben, wenden Sie alle unter aufgeführten Optimierungen an Leistungsoptimierung der EC2-Instance und starten Sie die Instance neu.

Schritt 6: Den Agenten verwalten

Informationen zum Starten, Beenden und Überprüfen des Agentenstatus finden Sie unterDen Agenten verwalten.

Den Agenten verwalten

AWS Ground Station Der Agent bietet die folgenden Funktionen zum Konfigurieren, Starten, Stoppen, Aktualisieren, Herabstufen und Deinstallieren des Agenten mithilfe der integrierten Linux-Befehlstools.

Topics

- AWS Ground Station Konfiguration des Agenten
- AWS Ground Station Start des Agenten
- AWS Ground Station Agent beendet
- AWS Ground Station Agenten-Upgrade
- AWS Ground Station Downgrade des Agenten
- AWS Ground Station Deinstallation des Agenten
- AWS Ground Station Status des Agenten
- AWS Ground Station RPM-Informationen für den Agenten

AWS Ground Station Konfiguration des Agenten

Navigieren Sie zu`/opt/aws/groundstation/etc`, das eine einzelne Datei namens aws-gs-agent-config .json enthalten sollte. Siehe Agent-Konfigurationsdatei

AWS Ground Station Start des Agenten

```
#start
```

```
sudo systemctl start aws-groundstation-agent

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

Sollte eine Ausgabe erzeugen, die zeigt, dass der Agent aktiv ist.

```
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 Agent beendet

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

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

Sollte eine Ausgabe erzeugen, die zeigt, dass der Agent inaktiv (gestoppt) ist.

```
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 Agenten-Upgrade

1. Laden Sie die neueste Version des Agenten herunter. Siehe Laden Sie den Agenten herunter.
2. Beenden des -Agenten.

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

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

3. Aktualisieren Sie den Agenten.

```
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 Downgrade des Agenten

1. Laden Sie die benötigte Agentenversion herunter. Siehe Laden Sie den Agenten herunter.
2. Führen Sie ein Downgrade des Agenten durch.

```
# 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 Deinstallation des Agenten

Bei der Deinstallation des Agenten wird /opt/aws/groundstation/etc/ .json in /opt/aws/groundstation/etc/ .json.rpmsave aws-gs-agent-config umbenannt. aws-gs-agent-config Wenn Sie den Agenten erneut auf derselben Instance installieren, werden Standardwerte für aws-gs-agent-config .json geschrieben und müssen mit den richtigen Werten aktualisiert werden, die Ihren AWS-Ressourcen entsprechen. Siehe Agent-Konfigurationsdatei.

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

AWS Ground Station Status des Agenten

Der Agentenstatus ist entweder aktiv (Agent läuft) oder inaktiv (Agent ist gestoppt).

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

Eine Beispielausgabe zeigt, dass der Agent installiert, inaktiv (gestoppt) und aktiviert (Dienst beim Booten starten) ist.

```
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 RPM-Informationen für den Agenten

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

Die Ausgabe sieht wie folgt aus:

> **Note**
>
> Die „Version“ kann je nach der zuletzt vom Agenten veröffentlichten Version unterschiedlich sein.

```
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
```

Den Agenten konfigurieren

Nach der Installation des Agenten müssen Sie die Agenten-Konfigurationsdatei unter aktualisieren/opt/aws/groundstation/etc/aws-gs-agent-config.json.

Agent-Konfigurationsdatei

Beispiel

```
{
  "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
}
```

Aufschlüsselung der Felder

Funktionen

Funktionen werden als Amazon-Ressourcennamen für Dataflow-Endpunktgruppen angegeben.

Erforderlich: True

Format: Zeichenketten-Array

- Werte: Fähigkeit ARNs → Zeichenfolge

Beispiele:

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

Gerät

Dieses Feld enthält zusätzliche Felder, die zur Aufzählung des aktuellen EC2- „Geräts“ erforderlich sind.

Erforderlich: True

Format: Objekt

Mitglieder:

- Private IPs
- Öffentliche IPs
- agentCpuCores
- Netzwerkadapter

Private IPs

Dieses Feld wird derzeit nicht verwendet, ist aber für future Anwendungsfälle enthalten. Wenn kein Wert enthalten ist, wird standardmäßig [„127.0.0.1“] verwendet

Erforderlich: Falsch

Format: Zeichenketten-Array

- Werte: IP-Adressen → Zeichenfolge

Beispiel:

```
"privateIps": [
```

```
    "127.0.0.1"
],
```

Öffentliche IP-Adressen

Elastic IP (EIP) pro Datenfluss-Endpunktgruppe.

Erforderlich: True

Format: Zeichenketten-Array

- Werte: IP-Adressen → Zeichenfolge

Beispiel:

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

AgentCPU-Cores

Dies gibt an, welche virtuellen Kerne für den Prozess reserviert sind. aws-gs-agent Informationen zu Planung von CPU-Kernen den Anforderungen für die angemessene Einstellung dieses Werts finden Sie unter.

Erforderlich: True

Format: Int-Array

- Werte: Kernzahlen → int

Beispiel:

```
"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
]
```

Netzwerkadapter

Dies entspricht den Ethernet-Adaptern oder Schnittstellen, die an ENIs angeschlossen sind und Daten empfangen.

Erforderlich: Falsch

Format: Zeichenketten-Array

- Werte: Namen von Ethernet-Adaptern (kann durch Ausführen gefunden werden`ifconfig`)

Beispiel:

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

Leistungsoptimierung der EC2-Instance

> **Note**
>
> Wenn Sie Ihre AWS-Ressourcen mithilfe von CloudFormation Vorlagen bereitgestellt haben, werden diese Optimierungen automatisch angewendet. Wenn Sie ein AMI verwendet oder Ihre EC2-Instance manuell erstellt haben, müssen diese Leistungsoptimierungen angewendet werden, um die zuverlässigste Leistung zu erzielen.

Denken Sie daran, Ihre Instance neu zu starten, nachdem Sie alle Optimierungen vorgenommen haben.

Topics

- Hardware-Interrupts und Empfangswarteschlangen optimieren — wirkt sich auf CPU und Netzwerk aus
- Tune Rx Interrupt Coalescing — Auswirkungen auf das Netzwerk

- Tune Rx Ring Buffer — Wirkt sich auf das Netzwerk aus
- CPU C-State abstimmen — Wirkt sich auf die CPU aus
- Eingangsports reservieren — wirkt sich auf das Netzwerk aus
- Neustart

Hardware-Interrupts und Empfangswarteschlangen optimieren — wirkt sich auf CPU und Netzwerk aus

In diesem Abschnitt wird die CPU-Core-Nutzung von Systemd, SMP IRQs, Receive Packet Steering (RPS) und Receive Flow Steering (RFS) konfiguriert. Eine Reihe von empfohlenen Einstellungen, Anhang: Empfohlene Parameter für Interrupt/RPS Tune die auf dem von Ihnen verwendeten Instanztyp basieren, finden Sie unter.

1. Platzieren Sie systemd-Prozesse von den CPU-Kernen der Agenten fern.
2. Leitet Hardware-Interrupt-Anfragen von den CPU-Kernen der Agenten weg.
3. Konfigurieren Sie RPS so, dass die Hardware-Warteschlange einer einzelnen Netzwerkschnittstellenkarte nicht zu einem Engpass im Netzwerkverkehr wird.
4. Konfigurieren Sie RFS, um die CPU-Cache-Trefferquote zu erhöhen und dadurch die Netzwerklatenz zu reduzieren.

Das vom RPM bereitgestellte `set_irq_affinity.sh` Skript konfiguriert alle oben genannten Funktionen für Sie. Fügen Sie es zu Crontab hinzu, damit es bei jedem Start angewendet wird:

```
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
```

- Ersetzt `interrupt_core_list` durch Kerne, die für den Kernel und das Betriebssystem reserviert sind — typischerweise den ersten und zweiten, zusammen mit Hyperthread-Kernpaaren. Dies sollte sich nicht mit den oben ausgewählten Kernen überschneiden. (Beispiel: '0,1,48,49' für eine Hyperthread-Instanz mit 96 CPUs).
- `rps_core_mask`ist eine hexadezimale Bitmaske, die angibt, welche CPUs eingehende Pakete verarbeiten sollen, wobei jede Ziffer für 4 CPUs steht. Sie muss außerdem alle 8 Zeichen,

beginnend von rechts, durch Kommas getrennt werden. Es wird empfohlen, alle CPUs zuzulassen und das Balancing vom Caching übernehmen zu lassen.

  - Eine Liste der empfohlenen Parameter für jeden Instance-Typ finden Sie unter. Anhang: Empfohlene Parameter für Interrupt/RPS Tune

- Beispiel für eine 96-CPU-Instanz:

```
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 — Auswirkungen auf das Netzwerk

Interrupt Coalescing verhindert, dass das Hostsystem mit zu vielen Interrupts überflutet wird, und erhöht den Netzwerkdurchsatz. Bei dieser Konfiguration werden Pakete gesammelt und alle 128 Mikrosekunden ein einziger Interrupt generiert. Zu crontab hinzufügen, damit es bei jedem Start angewendet wird:

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

- `interface`Ersetzen Sie es durch die Netzwerkschnittstelle (Ethernet-Adapter), die für den Empfang von Daten konfiguriert ist. In der Regel ist dies der Fall, `eth0` da dies die Standard-Netzwerkschnittstelle ist, die einer EC2-Instance zugewiesen ist.

Tune Rx Ring Buffer — Wirkt sich auf das Netzwerk aus

Erhöhen Sie die Anzahl der Ringeinträge für den Rx-Ringpuffer, um Paketverluste oder -überläufe bei Burst-Verbindungen zu verhindern. Fügen Sie dem Crontab Folgendes hinzu, damit es bei jedem Start richtig eingestellt ist:

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

- `interface`Ersetzen Sie es durch die Netzwerkschnittstelle (Ethernet-Adapter), die für den Empfang von Daten konfiguriert ist. In der Regel ist dies der Fall, `eth0` da dies die Standard-Netzwerkschnittstelle ist, die einer EC2-Instance zugewiesen ist.
- Wenn Sie eine c6i.32xlarge-Instance einrichten, muss der Befehl so geändert werden, dass der Ringpuffer auf statt auf gesetzt wird. `8192` `16384`

CPU C-State abstimmen — Wirkt sich auf die CPU aus

Stellen Sie den CPU-C-Status ein, um einen Leerlauf zu verhindern, der zu Paketverlusten beim Start eines Kontakts führen kann. Erfordert einen Neustart der Instanz.

```
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
```

Eingangsports reservieren — wirkt sich auf das Netzwerk aus

Reservieren Sie alle Ports in Ihrem `AwsGroundStationAgentEndpoint` Eingangsadress-Portbereich, um Konflikte bei der Kernel-Nutzung zu vermeiden. Ein Konflikt bei der Portnutzung führt dazu, dass der Kontakt und die Datenübermittlung fehlschlagen.

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

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

Neustart

Nachdem alle Optimierungen erfolgreich angewendet wurden, starten Sie die Instanz neu, damit die Optimierungen wirksam werden.

```
sudo reboot
```

Anhang: Empfohlene Parameter für Interrupt/RPS Tune

In diesem Abschnitt werden die empfohlenen Parameterwerte für die Verwendung im Abschnitt Feinabstimmung von Hardware-Interrupts und Empfangswarteschlangen — Auswirkungen auf CPU und Netzwerk festgelegt.

Familie	Instance-Typ	${interrupt_core_list}	${rps_core_mask}
c6i	• c6i.32xlarge	• 0,1,64,65	• ffffffff, ffffffff, ffffffff, ffffffff
c5	• c5.24xlarge • c5.18xlarge • c5.12xlarge	• 0,1,48,49 • 0,1,36,37 • 0,1,24,25	• ffffffff, ffffffff, ffffffff • ff, ffffffff, ffffffff • ffff, ffffffff
c5n	• c5n.metal • c5n.18xlarge	• 0,1,36,37 • 0,1,36,37	• ff, ffffffff, ffffffff • ff, ffffffff, ffffffff
m5	• m5.24xlarge • m5.12xlarge	• 0,1,48,49 • 0,1,24,25	• ffffffff, ffffffff, ffffffff • ffff, ffffffff

Familie	Instance-Typ	$ {interrupt_core_list}	$ {rps_core_mask}
r5	• r5.metal • r5.24xlarge	• 0,1,48,49 • 0,1,48,49	• ffffffff, ffffffff, ffffffff • ffffffff, ffffffff, ffffffff
r5n	• r5n.metal • r5n.24xlarge	• 0,1,48,49 • 0,1,48,49	• ffffffff, ffffffff, ffffffff • ffffffff, ffffffff, ffffffff
g4dn	• g4dn.metal • g4dn.16xgroß • g4dn.12xgroß	• 0,1,48,49 • 0,1,32,33 • 0,1,24,25	• ffffffff, ffffffff, ffffffff • ffffffff, ffffffff • ffff, ffffffff
p4d	• p4d.24xgroß	• 0,1,48,49	• ffffffff, ffffffff, ffffffff
p3dn	• p3dn.24xgroß	• 0,1,48,49	• ffffffff, ffffffff, ffffffff

Bereiten Sie sich darauf vor, einen DigiF-Kontakt aufzunehmen

1. Suchen Sie in CPU Core Planning nach den gewünschten Datenflüssen und stellen Sie eine Liste der Kerne bereit, die der Agent verwenden kann. Siehe Planung von CPU-Kernen.

2. Überprüfen Sie die AWS Ground Station Agent-Konfigurationsdatei. Siehe AWS Ground Station Konfiguration des Agenten.
3. Vergewissern Sie sich, dass die erforderliche Leistungsoptimierung vorgenommen wurde. Siehe Leistungsoptimierung der EC2-Instance.
4. Vergewissern Sie sich, dass Sie alle genannten bewährten Methoden befolgen. Siehe Bewährte Methoden.
5. Vergewissern Sie sich, dass der AWS Ground Station Agent vor der geplanten Startzeit des Kontakts gestartet wurde, indem Sie:

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

6. Stellen Sie sicher, dass der AWS Ground Station Agent vor der geplanten Startzeit des Kontakts fehlerfrei ist, indem Sie:

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

   Vergewissern Sie sich`agentStatus`, dass Ihr `awsGroundStationAgentEndpoint` Computer AKTIV und der GESUND `auditResults` ist.

Bewährte Methoden

Bewährte EC2-Praktiken

Befolgen Sie die aktuellen Best Practices für EC2 und stellen Sie eine ausreichende Verfügbarkeit von Datenspeichern sicher.

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

Linux-Scheduler

Der Linux-Scheduler kann Pakete auf UDP-Sockets neu anordnen, wenn die entsprechenden Prozesse nicht an einen bestimmten Kern gebunden sind. Jeder Thread, der UDP-Daten sendet oder empfängt, sollte sich für die Dauer der Datenübertragung an einen bestimmten Kern anheften.

AWS Ground Station Liste der verwalteten Präfixe

Es wird empfohlen, die von `com.amazonaws.global.groundstation` AWS verwaltete Präfixliste zu verwenden, wenn Sie die Netzwerkregeln angeben, um die Kommunikation von der Antenne aus zu ermöglichen. Weitere Informationen zu AWS Managed Prefix Lists finden Sie unter Arbeiten mit AWS-verwalteten Präfixlisten.

Beschränkung auf einen einzigen Kontakt

Der AWS Ground Station Agent unterstützt mehrere Streams pro Kontakt, unterstützt jedoch jeweils nur einen Kontakt. Um Planungsprobleme zu vermeiden, sollten Sie eine Instance nicht für mehrere Datenfluss-Endpunktgruppen gemeinsam nutzen. Wenn eine einzelne Agentenkonfiguration mehreren verschiedenen DFEG-ARNs zugeordnet ist, kann sie nicht registriert werden.

Dienste und Prozesse werden zusammen mit dem Agenten ausgeführt AWS Ground Station

Wenn Dienste und Prozesse auf derselben EC2-Instance wie der AWS Ground Station Agent gestartet werden, ist es wichtig, sie an vCPUs zu binden, die nicht vom AWS Ground Station Agenten und dem Linux-Kernel verwendet werden, da dies zu Engpässen und sogar Datenverlust bei Kontakten führen kann. Dieses Konzept der Bindung an spezifische vCPUs wird Affinität genannt.

Zu vermeidende Kerne:

- `agentCpuCores`von Agent-Konfigurationsdatei
- `interrupt_core_list` von Hardware-Interrupts und Empfangswarteschlangen optimieren — wirkt sich auf CPU und Netzwerk aus.
  - Standardwerte finden Sie unter Anhang: Empfohlene Parameter für Interrupt/RPS Tune

Als Beispiel mit einer **`c5.24xlarge`** Instanz

Wenn du angegeben hast

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

und rannte

```
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
```

vermeide dann die folgenden Kerne:

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

Affinitialisieren von Diensten (systemd)

Neu eingeführte Dienste werden automatisch mit den zuvor genannten Diensten affinitiiert. `interrupt_core_list` Wenn der Anwendungsfall Ihrer gestarteten Dienste zusätzliche Kerne erfordert oder weniger ausgelastete Kerne benötigt, gehen Sie wie in diesem Abschnitt beschrieben vor.

Prüfen Sie mit dem folgenden Befehl, für welche Affinität Ihr Service derzeit konfiguriert ist:

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

Wenn Sie einen leeren Wert wie sehen`CPUAffinity=`, bedeutet das, dass wahrscheinlich die Standardkerne aus dem obigen Befehl verwendet werden `...bin/set_irq_affinity.sh <using the cores here> ...`

Um eine bestimmte Affinität zu überschreiben und festzulegen, suchen Sie den Speicherort der Servicedatei, indem Sie Folgendes ausführen:

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

Öffnen und ändern Sie die Datei (mit `vinano`, usw.) und fügen Sie sie `CPUAffinity=<core list>` in den `[Service]` Abschnitt ein wie:

```
[Unit]
...

[Service]
```

```
...
CPUAffinity=2,3

[Install]
...
```

Speichern Sie die Datei und starten Sie den Dienst neu, um die Affinität anzuwenden mit:

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

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

Weitere Informationen finden Sie unter: Red Hat Enterprise Linux 8 — Verwaltung, Überwachung und Aktualisierung des Kernels — Kapitel 27. Konfiguration von CPU-Affinity- und NUMA-Richtlinien mithilfe von systemd.

Affinitialisierung von Prozessen (Skripten)

Es wird dringend empfohlen, neu gestartete Skripte und Prozesse manuell zu affinitialisieren, da das Standardverhalten von Linux es ihnen ermöglicht, jeden Kern auf dem Computer zu verwenden.

Um Kernkonflikte bei laufenden Prozessen (wie Python, Bash-Skripten usw.) zu vermeiden, starten Sie den Prozess mit:

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

Wenn der Prozess bereits läuft, verwenden Sie Befehle wie`pidof`, oder`top`, `ps` um die Prozess-ID (PID) des spezifischen Prozesses zu ermitteln. Mit der PID können Sie die aktuelle Affinität sehen zu:

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

und kann es modifizieren mit:

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

Weitere Informationen zu Taskset finden Sie auf der Manpage taskset — Linux

Fehlerbehebung

Der Agent kann nicht gestartet werden

Der AWS Ground Station Agent kann aus verschiedenen Gründen nicht gestartet werden, aber das häufigste Szenario ist möglicherweise eine falsch konfigurierte Agenten-Konfigurationsdatei. Nach dem Start des Agenten (sieheAWS Ground Station Start des Agenten) erhalten Sie möglicherweise einen Status wie:

```
#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)
```

Fehlerbehebung

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

könnte zu einer Ausgabe führen von:

```
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.
```

Wenn der Agent nicht gestartet werden kann, nachdem „Config geladen“ wurde, liegt ein Problem mit der Agentenkonfiguration vor. Informationen Agent-Konfigurationsdatei zur Überprüfung Ihrer Agentenkonfiguration finden Sie unter.

AWS Ground Station Agent-Protokolle

AWS Ground Station Der Agent schreibt Informationen über Kontaktausführungen, Fehler und den Integritätsstatus in die Protokolldateien der Instanz, auf der der Agent ausgeführt wird. Sie können die Protokolldateien anzeigen, indem Sie manuell eine Verbindung zu einer Instanz herstellen.

Sie können Agentenprotokolle an der folgenden Stelle einsehen.

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

Keine Kontakte verfügbar

Für die Planung von Kontakten ist ein funktionstüchtiger AWS Ground Station Agent erforderlich. Bitte vergewissern Sie sich, dass Ihr AWS Ground Station Agent gestartet wurde und fehlerfrei ist, indem Sie die AWS Ground Station API get-dataflow-endpoint-group wie folgt abfragen:

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

Vergewissern Sie sich`agentStatus`, dass Ihr `awsGroundStationAgentEndpoint` Computer AKTIV und der GESUND `auditResults` ist.

Supportanfragen

Kontaktieren Sie das Ground Station Station-Team über den AWS-Support.

1. Geben `contact_id` Sie alle betroffenen Kontakte an. Ohne diese Informationen kann das AWS Ground Station Team einen bestimmten Kontakt nicht untersuchen.
2. Geben Sie Einzelheiten zu allen bereits unternommenen Schritten zur Fehlerbehebung an.
3. Geben Sie in unserer Anleitung zur Fehlerbehebung alle Fehlermeldungen an, die bei der Ausführung der Befehle gefunden wurden.

Agent-Versionshinweise

Aktuelle Agent-Version

Version 1.0.3555.0

Datum der Veröffentlichung: 27.03.2024

Datum des Endes des Support: 31.08.2024

RPM-Prüfsummen:

- SHA256: `108f3aceb00e5af549839cd766c56149397e448a6e1e1429c89a9eebb6bc0fc1`
- MD 5: `65b72fa507fb0af32651adbb18d2e30f`

Änderungen:

- Fügen Sie beim Start der Aufgabe eine Agent-Metrik für die ausgewählte Version der ausführbaren Datei hinzu.

- Fügen Sie Unterstützung für Konfigurationsdateien hinzu, um bestimmte ausführbare Versionen zu vermeiden, wenn andere Versionen verfügbar sind.
- Fügen Sie Netzwerk- und Routing-Diagnosen hinzu.
- Zusätzliche Sicherheitsfunktionen.
- Behebung eines Problems, bei dem einige Fehler bei der Metrikberichterstattung in die Standardausgabe oder das Journal statt in die Protokolldatei geschrieben wurden.
- Gehen Sie ordnungsgemäß mit Socket-Fehlern um, die über das Netzwerk nicht erreichbar sind.
- Messen Sie den Paketverlust und die Latenz zwischen Quell- und Zielagenten.
- Veröffentlichen Sie aws-gs-datapipe Version 2.0, um neue Protokollfunktionen zu unterstützen und Kontakte transparent auf das neue Protokoll umzustellen.

Veraltete Agent-Versionen

Version 1.0.2942.0

Datum der Veröffentlichung: 26.06.2023

Datum des Endes des Support: 31.05.2024

RPM-Prüfsummen:

- SHA256: `7d94b642577504308a58bab28f938507f2591d4e1b2c7ea170b77bea97b5a9b6`
- MD 5: `661ff2b8f11aba5d657a6586b56e0d8f`

Änderungen:

- Es wurden Fehlerprotokolle für den Fall hinzugefügt, dass das Agent-RPM auf der Festplatte aktualisiert wird und der Agent neu gestartet werden muss, damit die Änderungen wirksam werden.
- Es wurde eine Überprüfung der Netzwerkoptimierung hinzugefügt, um sicherzustellen, dass die Optimierungsschritte im Benutzerhandbuch für den Agenten befolgt und korrekt angewendet werden.
- Behebung eines Fehlers, der zu falschen Warnungen in den Agent-Protokollen über die Archivierung von Protokollen führte.
- Die Erkennung von Paketverlusten wurde verbessert.
- Die Agenteninstallation wurde aktualisiert, um die Installation oder das Upgrade des RPM zu verhindern, wenn der Agent bereits läuft.

Version 1.0.2716.0

Veröffentlichungsdatum: 15.03.2023

Datum des Endes des Support: 31.05.2024

RPM-Prüfsummen:

- SHA256: `cb05b6a77dfcd5c66d81c0072ac550affbcefefc372cc5562ee52fb220844929`
- MD 5: `65266490c4013b433ec39ee50008116c`

Änderungen:

- Aktiviert das Hochladen von Protokollen, wenn der Agent beim Ausführen von Aufgaben ausfällt.
- Behebt einen Linux-Kompatibilitätsfehler in den bereitgestellten Netzwerk-Tuning-Skripten.

Version 1.0.2677.0

Veröffentlichungsdatum: 15.02.2023

Datum des Endes des Support: 31.05.2024

RPM-Prüfsummen:

- SHA256: `77cfe94acb00af7ca637264b17c9b21bd7afdc85b99dffdd627aec9e99397489`
- MD 5: `b8533be7644bb4d12ab84de21341adac`

Änderungen:

- Erste allgemein verfügbare Agent-Version.

Überprüfung der RPM-Installation

Die neueste RPM-Version, der anhand von RPM validierte MD5-Hash und der SHA256-Hash mit sha256sum sind unten aufgeführt. Diese Werte können zusammen verwendet werden, um zu überprüfen, welche RPM-Version für den Bodenstationsagenten verwendet wird.

Aktuelle Agent-Version

Version 1.0.3555.0

Datum der Veröffentlichung: 27.03.2024

Datum des Endes des Support: 31.08.2024

RPM-Prüfsummen:

- SHA256: `108f3aceb00e5af549839cd766c56149397e448a6e1e1429c89a9eebb6bc0fc1`
- MD 5: `65b72fa507fb0af32651adbb18d2e30f`

Änderungen:

- Fügen Sie beim Start der Aufgabe eine Agent-Metrik für die ausgewählte Version der ausführbaren Datei hinzu.
- Fügen Sie Unterstützung für Konfigurationsdateien hinzu, um bestimmte ausführbare Versionen zu vermeiden, wenn andere Versionen verfügbar sind.
- Fügen Sie Netzwerk- und Routing-Diagnosen hinzu.
- Zusätzliche Sicherheitsfunktionen.
- Behebung eines Problems, bei dem einige Fehler bei der Metrikberichterstattung in die Standardausgabe oder das Journal statt in die Protokolldatei geschrieben wurden.
- Gehen Sie ordnungsgemäß mit Socket-Fehlern um, die über das Netzwerk nicht erreichbar sind.
- Messen Sie den Paketverlust und die Latenz zwischen Quell- und Zielagenten.
- Veröffentlichen Sie aws-gs-datapipe Version 2.0, um neue Protokollfunktionen zu unterstützen und Kontakte transparent auf das neue Protokoll umzustellen.

Überprüfen Sie das RPM

Folgende Tools benötigen Sie, um diese RPM-Installation überprüfen zu können:

- sha256sum
- U/min

Beide Tools sind standardmäßig auf Amazon Linux 2 verfügbar. Mithilfe dieser Tools können Sie überprüfen, ob es sich bei dem von Ihnen verwendeten RPM um die richtige Version handelt. Laden Sie zunächst das neueste RPM aus dem S3-Bucket herunter (Anweisungen Laden Sie den Agenten herunter zum Herunterladen des RPM finden Sie unter). Sobald diese Datei heruntergeladen ist, müssen Sie einige Dinge überprüfen:

- Berechne die SHA256-Summe der RPM-Datei. Führen Sie die folgende Aktion von der Befehlszeile der Recheninstanz aus, die Sie verwenden:

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

  Nehmen Sie diesen Wert und vergleichen Sie ihn mit der obigen Tabelle. Dies zeigt, dass es sich bei der heruntergeladenen RPM-Datei um eine gültige, nutzbare Datei handelt, die AWS Ground Station an Kunden verkauft hat. Wenn die Hashes nicht übereinstimmen, installieren Sie das RPM nicht und löschen Sie es aus der Recheninstanz.
- Überprüfen Sie auch den MD5-Hash der Datei, um sicherzustellen, dass das RPM nicht kompromittiert wurde. Verwenden Sie dazu das RPM-Befehlszeilentool, indem Sie den folgenden Befehl ausführen:

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

  Stellen Sie sicher, dass der hier aufgeführte MD5-Hash mit dem MD5-Hash der Version übereinstimmt, die in der obigen Tabelle aufgeführt ist. Sobald diese beiden Hashes anhand dieser Tabelle validiert wurden, die in den AWS-Dokumenten aufgeführt ist, kann der Kunde sicher sein, dass es sich bei dem heruntergeladenen und installierten RPM um die sichere und ungefährdete Version des RPM handelt.

Auflisten und Reservieren von Kontakten

Sie können mithilfe der AWS Ground Station -Konsole oder AWS CLI Satellitendaten eingeben, den Standort von Antennen identifizieren und Antennenzeit für ausgewählte Satelliten angeben und planen. Sie können Kontaktreservierungen bis zu acht Tage vor dem geplanten Zeitpunkt überprüfen, stornieren und neu planen. Darüber hinaus können Sie die Details Ihres Preisplans für reservierte Minuten einsehen, wenn Sie das Preismodell für AWS Ground Station reservierte Minuten verwenden.

AWS Ground Station unterstützt die regionsübergreifende Datenbereitstellung. Die Konfigurationen des Datenflussendpunkts, die Teil des ausgewählten Missionsprofils sind, bestimmen, in welche(n) Region(en) die Daten übermittelt werden. Weitere Informationen zur Verwendung der regionsübergreifenden Datenübermittlung finden Sie unter Verwenden eines regionsübergreifenden Datenübermittlungsdiensts.

Um Kontakte zu planen, müssen Ihre Ressourcen konfiguriert sein. Wenn Sie Ihre Ressourcen noch nicht konfiguriert haben, finden Sie Anweisungen unter Erste Schritte.

Themen

Verwenden der Ground Station-Konsole

Sie können die AWS Ground Station Konsole verwenden, um Kontaktreservierungen zu reservieren, anzusehen und zu stornieren. Um die AWS Ground Station Konsole zu verwenden, öffnen Sie die AWS Ground Station Konsole und wählen Sie Kontakte jetzt reservieren.

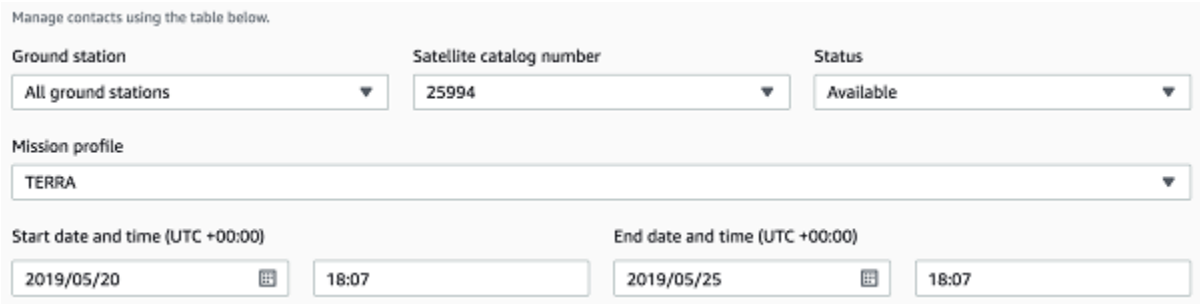
Verwenden Sie die folgenden Themen, um die AWS Ground Station Konsole zum Reservieren, Anzeigen und Stornieren von Kontakten zu verwenden.

Themen

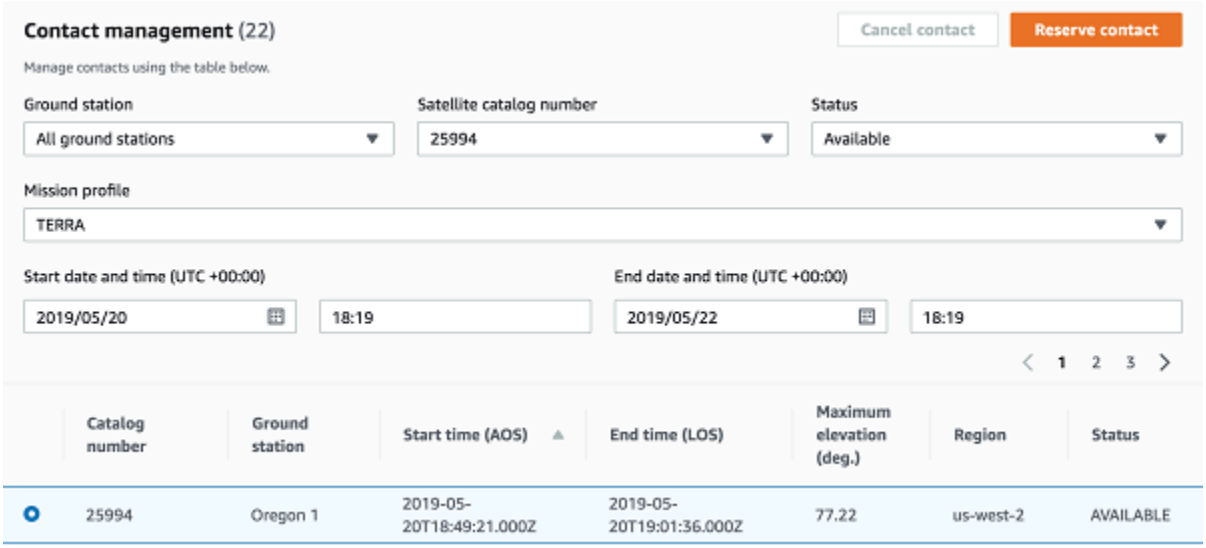
Reservieren eines Kontakts

Verwenden Sie nach dem Zugriff auf die AWS Ground Station Konsole Ihre konfigurierten Ressourcen, um Kontakte in der Kontaktverwaltungstabelle zu reservieren.

1. Wählen Sie in der Tabelle Contact management (Kontaktverwaltung) die Parameter aus, mit denen Sie nach verfügbaren Kontakten suchen möchten. Stellen Sie sicher, dass Sie Kontakte mit dem Status Available (Verfügbar) anzeigen, indem Sie den Filter Status verwenden.



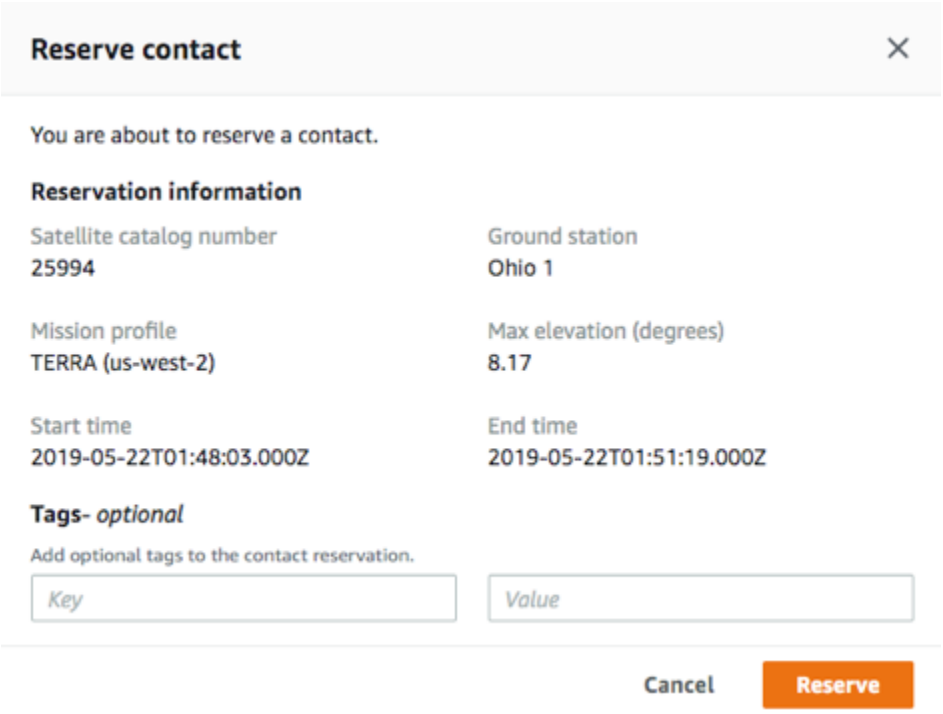
2. Wählen Sie einen Kontakt, der Ihre Anforderungen erfüllt, und anschließend Reserve contact (Kontakt reservieren) aus.



3. Überprüfen Sie im Dialogfeld Reserve Contact (Kontakt reservieren) Ihre Kontaktreservierungsinformationen.

   a. (Optional) Geben Sie unter Tags einen Schlüssel und einen Wert für jedes Tag ein, das Sie hinzufügen möchten.

   b. Wählen Sie Reserve (Reservieren).

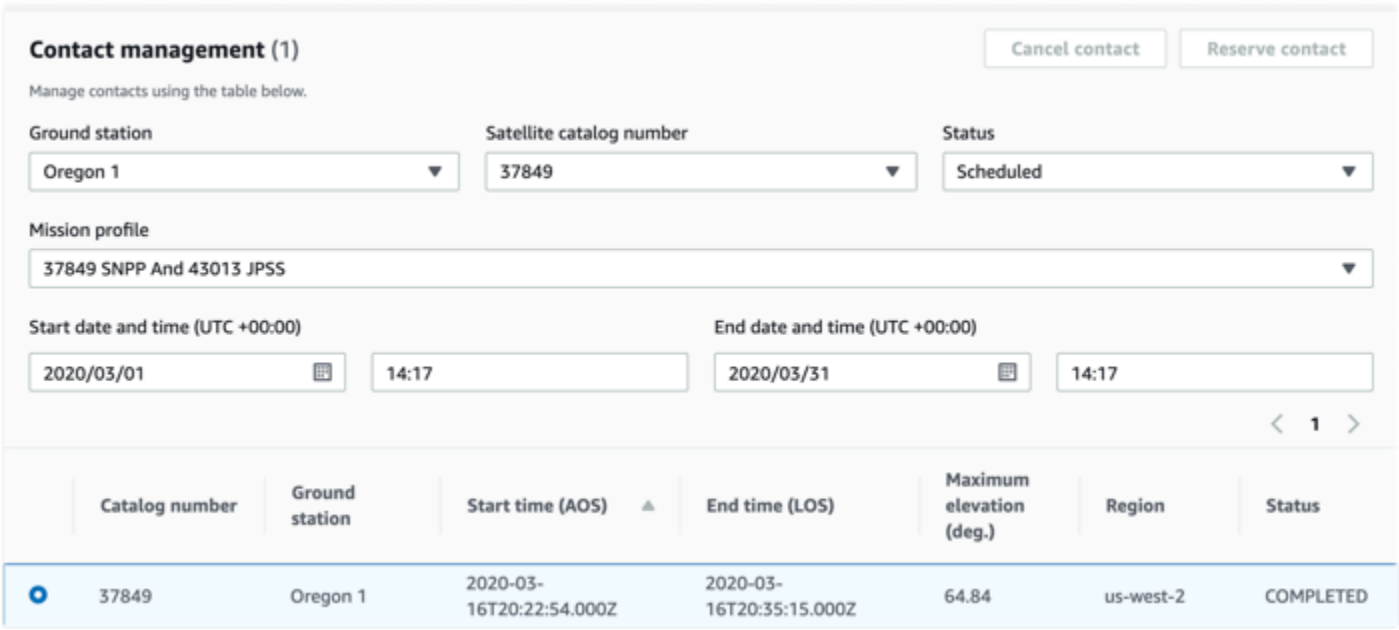


AWS Ground Station verwendet die Konfigurationsdaten aus Ihrem Missionsprofil, um einen Kontakt an der angegebenen Bodenstation auszuführen.

Anzeigen geplanter und abgeschlossener Kontakte

Sobald Sie Kontakte geplant haben, können Sie die AWS Ground Station Konsole verwenden, um die Details der geplanten und abgeschlossenen Kontakte einzusehen.

Wählen Sie in der Tabelle Contact management (Kontaktverwaltung) die Parameter aus, mit denen Sie nach geplanten und abgeschlossenen Kontakten suchen möchten. Stellen Sie mithilfe des Statusfilters sicher, dass Sie Geplante oder Abgeschlossene Kontakte anzeigen.



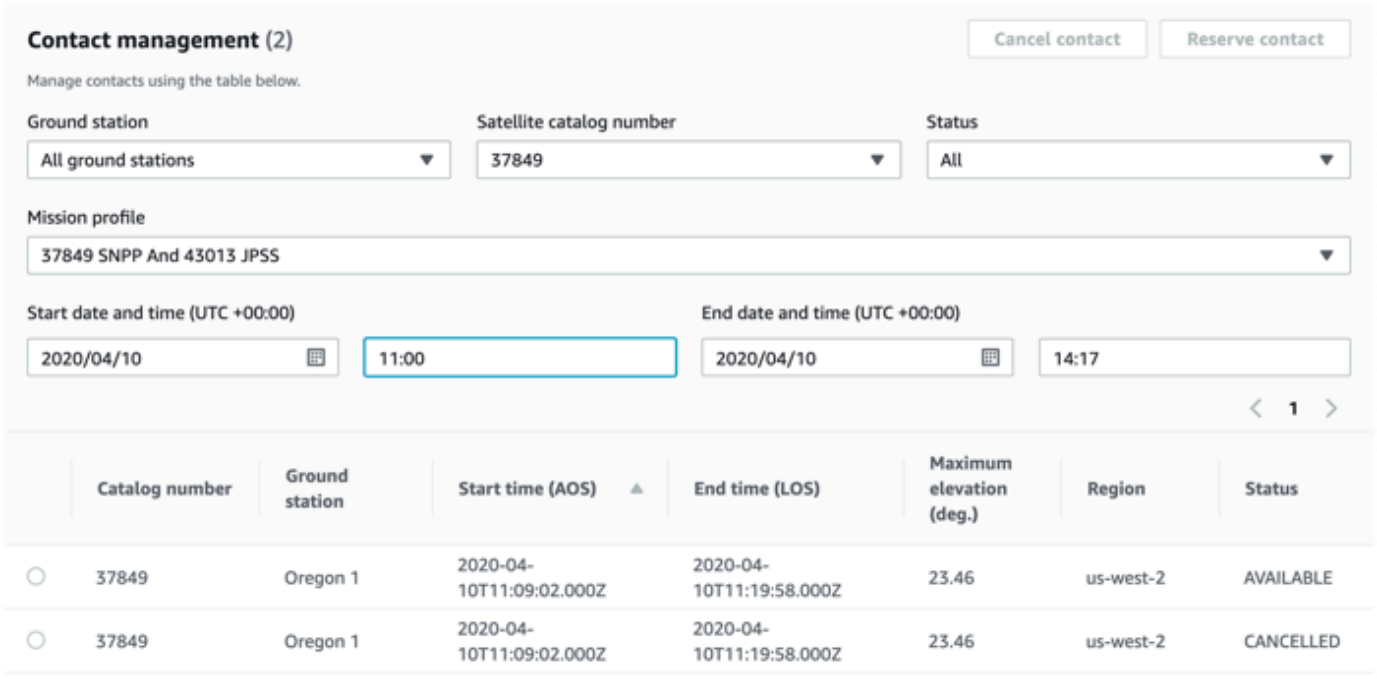
Ihre geplanten oder abgeschlossenen Kontakte werden aufgelistet, sofern die Kontakte mit den Parametern übereinstimmen.

Abbrechen von Kontakten

Sie können die AWS Ground Station Konsole verwenden, um geplante Kontakte zu stornieren

1. Wählen Sie in der Tabelle Contact management (Kontaktverwaltung) die Parameter aus, mit denen Sie nach geplanten und abgeschlossenen Kontakten suchen möchten. Stellen Sie sicher, dass Sie Kontakte mit dem Status Scheduled (Geplant) anzeigen, indem Sie den Filter Status verwenden.
2. Wählen Sie in der Liste der geplanten Kontakte den Kontakt aus, den Sie stornieren möchten. Wählen Sie dann Cancel Contact (Kontakt abbrechen) aus.

3. Wählen Sie im Dialogfeld Cancel contact (Kontakt abbrechen) die Option OK aus.



Der Status des Kontakts lautet CANCELLED.

Benennen von Satelliten

Die AWS Ground Station Konsole kann bei Verwendung der Kontaktseite einen benutzerdefinierten Namen für einen Satelliten zusammen mit der Norad-ID anzeigen. Die Anzeige des Satellitennamens erleichtert die Auswahl des richtigen Satelliten bei der Planung erheblich. Dazu können Tags verwendet werden.

Das Taggen von AWS-Bodenstation-Satelliten kann über die Tag-Resource-API mit der AWS-CLI oder einem der AWS-SDKs erfolgen. In diesem Handbuch wird die Verwendung der AWS Ground Station CLI zur Kennzeichnung des öffentlich-rechtlichen Rundfunksatelliten Aqua (Norad ID 27424) beschrieben. `us-west-2`

AWS Ground Station CLI

Das AWS CLI kann zur Interaktion mit verwendet werden. AWS Ground Station Bevor Sie Ihre Satelliten AWS CLI zur Kennzeichnung verwenden können, müssen die folgenden AWS CLI Voraussetzungen erfüllt sein:

- Stellen Sie sicher, dass AWS CLI das installiert ist. Informationen zur Installation AWS CLI finden Sie unter Installation der AWS-CLI Version 2.
- Stellen Sie sicher, dass dies konfiguriert AWS CLI ist. Informationen zur Konfiguration finden AWS CLI Sie unter Konfiguration der AWS-CLI Version 2.
- Speichern Sie Ihre häufig verwendeten Konfigurationseinstellungen und Anmeldeinformationen in Dateien, die mit der AWS CLI verwaltet werden. Sie benötigen diese Einstellungen und Anmeldeinformationen, um Ihre AWS Ground Station Kontakte zu reservieren und zu verwalten AWS CLI. Weitere Informationen zum Speichern der Konfigurations- und Anmeldeinformationseinstellungen finden Sie unter Konfigurations- und Anmeldeinformationsdatei-Einstellungen.

Sobald AWS CLI es konfiguriert und einsatzbereit ist, sehen Sie sich die Befehlsreferenzseite der AWS Ground Station CLI an, um sich mit den verfügbaren Befehlen vertraut zu machen. Folgen Sie der AWS CLI Befehlsstruktur, wenn Sie diesen Service verwenden, und stellen Sie Ihren Befehlen ein Präfix voran`groundstation`, um den Service anzugeben AWS Ground Station , den Sie verwenden möchten. Weitere Informationen zur AWS CLI Befehlsstruktur finden Sie unter Befehlsstruktur auf der AWS-CLI-Seite. Eine beispielhafte Befehlsstruktur ist unten angegeben.

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

Benennen Sie einen Satelliten

Zuerst benötigen Sie den ARN für die Satelliten, die Sie taggen möchten. Dies kann über die List-Satellites-API in der AWS-CLI erfolgen:

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

Wenn Sie den obigen CLI-Befehl ausführen, wird eine Ausgabe zurückgegeben, die der folgenden ähnelt:

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

Suchen Sie den Satelliten, den Sie markieren möchten, und notieren Sie sich den`satelliteArn`. Ein wichtiger Vorbehalt beim Tagging besteht darin, dass die Tag-Resource-API einen regionalen ARN benötigt und der von List-Satellites zurückgegebene ARN global ist. Im nächsten Schritt sollten Sie den ARN um die Region erweitern, in der Sie das Tag sehen möchten (wahrscheinlich die Region, in der Sie planen). Für dieses Beispiel verwenden `us-west-2` wir. Mit dieser Änderung wird der ARN von:

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

auf:

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

Um den Satellitennamen in der Konsole anzuzeigen, muss der Satellit über ein Tag mit `“Name"` dem Schlüssel verfügen. Da wir die verwenden, müssen die AWS CLI Anführungszeichen außerdem mit einem umgekehrten Schrägstrich maskiert werden. Das Tag wird ungefähr so aussehen:

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

Als Nächstes rufen Sie die Tag-Resource-API auf, um den Satelliten zu taggen. Dies kann auf folgende Weise geschehen AWS CLI :

```
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\"}
```

Danach können Sie den Namen, den Sie für den Satelliten festgelegt haben, in der AWS Ground Station Konsole sehen.

Ändern Sie den Namen für einen Satelliten

Wenn Sie den Namen für einen Satelliten ändern möchten, können Sie Tag-Resource mit dem Satelliten-ARN einfach erneut mit demselben "Name" Schlüssel aufrufen, jedoch mit einem anderen Wert im Tag. Dadurch wird das bestehende Tag aktualisiert und der neue Name wird in der Konsole angezeigt. Ein Beispielaufruf dafür sieht wie folgt aus:

```
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\"}
```

Entferne den Namen für einen Satelliten

Der für einen Satelliten festgelegte Name kann mit der Untag-Resource-API entfernt werden. Diese API benötigt den Satelliten-ARN mit der Region, in der sich das Tag befindet, und eine Liste von Tag-Schlüsseln. Für den Namen lautet der Tag-Schlüssel"Name". Ein Beispielaufruf dieser API über die AWS-CLI sieht wie folgt aus:

```
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
```

Kontakte reservieren und verwalten mit AWS CLI

Sie können es verwenden AWS CLI , um Ihre Kontakte in AWS Ground Station zu reservieren und zu verwalten. Vor der Nutzung AWS CLI zur Reservierung und Verwaltung von Kontakten müssen die folgenden AWS CLI Voraussetzungen erfüllt sein:

- Stellen Sie sicher, dass AWS CLI das installiert ist. Informationen zur Installation AWS CLI finden Sie unter Installation der AWS-CLI Version 2.
- Stellen Sie sicher, dass dies konfiguriert AWS CLI ist. Informationen zur Konfiguration finden AWS CLI Sie unter Konfiguration der AWS-CLI Version 2.
- Speichern Sie Ihre häufig verwendeten Konfigurationseinstellungen und Anmeldeinformationen in Dateien, die mit der AWS CLI verwaltet werden. Sie benötigen diese Einstellungen und Anmeldeinformationen, um Ihre AWS Ground Station Kontakte zu reservieren und zu verwalten AWS CLI. Weitere Informationen zum Speichern der Konfigurations- und

Anmeldeinformationseinstellungen finden Sie unter Konfigurations- und Anmeldeinformationsdatei-Einstellungen.

Sobald AWS CLI es konfiguriert und einsatzbereit ist, sehen Sie sich die Befehlsreferenzseite der AWS Ground Station CLI an, um sich mit den verfügbaren Befehlen vertraut zu machen. Folgen Sie der AWS CLI Befehlsstruktur, wenn Sie diesen Service verwenden, und stellen Sie Ihren Befehlen ein Präfix voran`groundstation`, um den Service anzugeben AWS Ground Station , den Sie verwenden möchten. Weitere Informationen zur AWS CLI Befehlsstruktur finden Sie unter Befehlsstruktur auf der AWS-CLI-Seite. Eine beispielhafte Befehlsstruktur ist unten angegeben.

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

Verwenden Sie die folgenden Themen, um Kontakte zu reservieren, einzusehen und zu stornieren AWS CLI.

Themen

- Kontakte anzeigen und auflisten mit AWS CLI
- Reservieren Sie einen Kontakt mit AWS CLI
- Beschreiben Sie einen Kontakt mit AWS CLI
- Stornieren Sie einen Kontakt mit AWS CLI

Kontakte anzeigen und auflisten mit AWS CLI

Führen Sie die folgenden Parameter aus `CANCELLEDCOMPLETED`, um `SCHEDULED` Kontakte aufzulisten und anzuzeigen oder Kontakte `aws groundstation list-contacts` mit AWS CLI anzuzeigen.

- Start Time (Startzeit) – Geben Sie mit `--start-time <value>` die Startzeit Ihres Kontakts an. Folgendes ist ein akzeptables Zeitwertformat: `YYYY-MM-DDTHH:MM:SSZ`
- End Time (Endzeit) – Geben Sie mit `--end-time <value>` die Endzeit Ihres Kontakts an. Folgendes ist ein akzeptables Zeitwertformat: `YYYY-MM-DDTHH:MM:SSZ`
- Status List (Statusliste) – Geben Sie mit `--status-list <value>` den Status Ihres Kontakts an. Zu den zulässigen Werten gehören `AVAILABLE`, `CANCELLED`, `COMPLETED` oder `SCHEDULED`. Eine vollständige Liste der gültigen Werte finden Sie unter list-contacts.

Zum Auflisten und Anzeigen von `AVAILABLE` Kontakten mit AWS CLI den folgenden Parametern sind zusätzlich zu den oben aufgeführten Parametern erforderlich.

- Ground Station ID (Ground Station-ID) – Geben Sie mit `--ground-station <value>` die ID Ihrer Ground Station an.
- Mission Profile ARN (Mission-Profil-ARN) – Geben Sie mit `--mission-profile-arn <value>` Ihre Mission-Profil-ARN an.
- Satellite ARN (Satelliten-ARN) - Geben Sie mit `--satellite-arn <value>` Ihren Satelliten-ARN an.

Sie können `list`-Befehle verwenden, um Ihre Ressourcen zu suchen. Weitere Informationen zur Angabe Ihrer Parameter finden Sie unter list-contacts

Ein Beispielbefehl zum Auflisten verfügbarer Kontakte finden Sie unten.

```
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'
```

Ein Beispiel für eine Liste der verfügbaren Kontakte finden Sie unten.

```
{
  "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"
```

```
    }
  ]
}
```

Reservieren Sie einen Kontakt mit AWS CLI

AWS CLI bietet Ihnen die Möglichkeit, Kontakte minutenweise zu reservieren. Diese Funktion gibt es nur bei AWS CLI und kann nicht in der AWS Ground Station Konsole ausgeführt werden.

Um Kontakte mit zu reservieren AWS CLI, führen Sie die Ausführung `aws groundstation reserve-contact` mit den folgenden Parametern aus.

- Ground Station ID (Ground Station-ID) – Geben Sie mit `--ground-station <value>` die ID Ihrer Ground Station an.
- Mission Profile ARN (Mission-Profil-ARN) – Geben Sie mit `--mission-profile-arn <value>` Ihre Mission-Profil-ARN an.
- Satellite ARN (Satelliten-ARN) - Geben Sie mit `--satellite-arn <value>` Ihren Satelliten-ARN an.
- Start Time (Startzeit) – Geben Sie mit `--start-time <value>` die Startzeit Ihres Kontakts an. Folgendes ist ein akzeptables Zeitwertformat: `YYYY-MM-DDTHH:MM:SSZ`
- End Time (Endzeit) – Geben Sie mit `--end-time <value>` die Endzeit Ihres Kontakts an. Folgendes ist ein akzeptables Zeitwertformat: `YYYY-MM-DDTHH:MM:SSZ`

Die Kontaktreservierung ist ein asynchroner Vorgang. Die Antwort auf den `reserve-contact` Befehl enthält die Kontakt-ID. Um das Ergebnis des asynchronen Reservierungsvorgangs zu ermitteln, verwenden Sie`describe-contact`. Weitere Informationen dazu finden Sie im Abschnitt unten mit dem TitelBeschreiben Sie einen Kontakt mit AWS CLI.

Sie können `list`-Befehle verwenden, um Ihre Ressourcen zu suchen. Weitere Informationen zur Angabe Ihrer Parameter finden Sie unter reserve-contact.

Ein Beispielbefehl zum Reservieren eines Kontakts finden Sie unten.

```
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'
```

Ein Beispiel für einen erfolgreich reservierten Kontakt finden Sie unten.

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

Beschreiben Sie einen Kontakt mit AWS CLI

Verwenden Sie den `describe-contact` CLI-Befehl AWS CLI, um den Status eines Kontakts/einer Reservierung mit anzuzeigen. Dies ist hilfreich, um das Ergebnis des asynchronen Kontaktreservierungsprozesses zu überprüfen, den Status eines in Bearbeitung befindlichen Kontakts zu überwachen und den Status eines abgeschlossenen Kontakts zu ermitteln.

Um Kontakte mit zu beschreiben AWS CLI, verwenden Sie die `aws groundstation describe-contact` folgenden Parameter.

- Kontakt-ID — Geben Sie Ihre Kontakt-ID mit ein`--contact-id <value>`.

Sie können `list`-Befehle verwenden, um Ihre Ressourcen zu suchen. Weitere Informationen zur Angabe Ihrer Parameter finden Sie unter describe-contact.

Im Folgenden finden Sie einen Beispielbefehl zur Beschreibung eines Kontakts.

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

Im Folgenden finden Sie ein Beispiel für einen erfolgreich geplanten Kontakt.

```
{
  "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"
}
```

Stornieren Sie einen Kontakt mit AWS CLI

Um einen Kontakt mit abzubrechen AWS CLI, führen Sie den Vorgang `aws groundstation cancel-contact` mit den folgenden Parametern aus.

- Region – Geben Sie mit `--region <value>` die Region Ihrer Ground Station an.
- Contact ID (Kontakt-ID) – Geben Sie mit `--contact-id <value>` die Kontakt-ID an.

Sie können `list`-Befehle verwenden, um Ihre Ressourcen zu suchen. Weitere Informationen zur Angabe Ihrer Parameter finden Sie unter cancel-contacts

Ein Beispielbefehl zum Reservieren eines Kontakts finden Sie unten.

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

Ein Beispiel für einen erfolgreich abgebrochenen Kontakt finden Sie unten.

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

Datenlieferung an Amazon EC2

AWS Ground Station übermittelt Ihre Kontaktdaten asynchron an einen Amazon Simple Storage Service (Amazon S3) -Bucket in Ihrem Konto oder synchron, indem sie zu und von einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance in Ihrem Konto gestreamt werden. In den folgenden Schritten wird beschrieben, wie Sie die Ressourcen konfigurieren, die für das Streamen von Kontaktdaten zu und von einer Amazon EC2 EC2-Instance erforderlich sind. Informationen zur Datenlieferung an Amazon S3 finden Sie im Erste Schritte mit AWS Ground Station Leitfaden.

Themen

Schritt 1: Erstellen eines EC2-SSH-Schlüsselpaars

Falls Sie noch keines haben, erstellen Sie in der Amazon EC2 EC2-Konsole für jede AWS Region, in der Sie Daten empfangen möchten, ein neues key pair. Führen Sie die folgenden Schritte aus:

1. Wählen Sie in Ihrer AWS Management Console AWS Region eine Region aus, in der Sie Kontakte reservieren möchten. Sie müssen für jede AWS Region, die Sie auswählen, ein key pair erstellen.

   > **Note**
   >
   > AWS Ground Station ist noch nicht für alle Regionen verfügbar. Stellen Sie sicher, AWS Ground Station dass dies von Ihrer gewünschten AWS Region unterstützt wird. Weitere Informationen zu AWS Ground Station Antennenstandorten finden Sie unter Häufig gestellte Fragen zu AWS Ground Station.

2. Folgen Sie der Anleitung Create Key Pairs im Amazon EC2 EC2-Benutzerhandbuch, um die Schlüsselpaare zu erstellen.

3. Wiederholen Sie den Vorgang bei Bedarf für andere AWS Regionen.

Schritt 2: Einrichten Ihrer VPC

Die vollständige Einrichtung einer VPC geht über den Rahmen dieses Handbuchs hinaus. Wenn Sie nicht bereits eine VPC haben, die angepasst ist, können Sie die in Ihrem AWS -Konto erstellte Standard-VPC verwenden. Wir empfehlen, Ihrer VPC eine Linux-Bastion hinzuzufügen, damit Sie per SSH auf Ihre Amazon EC2 EC2-Instances zugreifen können, ohne eine öffentliche IP-Adresse anzuhängen. Weitere Informationen zum Konfigurieren einer Linux-Bastion in Ihrer VPC finden Sie unter Linux Bastion Hosts on AWS (Linux-Bastion-Hosts auf AWS).

Der Einfachheit halber finden Sie im Folgenden Anweisungen zum schnellen Hinzufügen eines Bastion-Hosts zu Ihrer Linux-Umgebung. AWS Dies ist zwar nicht erforderlich, wird aber als bewährte Vorgehensweise empfohlen.

1. Loggen Sie sich in Ihr AWS Konto ein.
2. Wählen Sie auf der Seite Linux Bastion Hosts on the AWS Cloud: Quick Start Reference Deployment (Linux-Bastion-Hosts in der AWS-Cloud: Schnellstart-Referenz-Bereitstellung) die Option Launch Quick Start (for new VPC) (Quick-Start (für neue VPC) starten) aus.
3. Klicken Sie auf der Seite Create Stack (Stack erstellen) auf Next (Weiter). Die Vorlage ist bereits vorausgefüllt.
4. Nehmen Sie auf der Detailseite Specify stack (Stack angeben) in den folgenden Feldern Bearbeitungen und Änderungen vor:

    a. Geben Sie im Feld Stack Name einen Stack-Namen für Ihren Host ein.

    b. Wählen Sie unter Availability Zones die Availability Zones aus, die Sie für die Subnetze in der VPC verwenden möchten. Es müssen mindestens zwei Availability Zones ausgewählt werden.

    c. Geben Sie unter Allowed bastion external access CIDR (CIDR mit zulässigem externen Zugriff auf Bastion), den CIDR-Block ein, von dem Sie den SSH-Zugriff aktivieren möchten. Wenn Sie sich nicht sicher sind, können Sie den Wert 0.0.0.0/0 verwenden, um den SSH-Zugriff von jedem Host zu aktivieren, der über den SSH-Schlüssel verfügt.

    d. Wählen Sie für Key pair name (Schlüsselpaarname) den Namen des Schlüsselpaares aus, den Sie in the section called “Schritt 1: Erstellen eines EC2-SSH-Schlüsselpaars” festgelegt haben.

    e. Wählen Sie für Bastion-Instance-Typ die Option t2.micro aus.

> **Important**
>
> Der Instance-Typ t2.micro ist für die Region Europa (Stockholm) (eu-north-1) nicht verfügbar. Wenn Sie AWS Ground Station in der Region Europa (Stockholm) (eu-north-1) verwenden, wählen Sie t3.micro.

f. Wählen Sie bei der TCP-Weiterleitung trueaus.

g. (Optional) Nehmen Sie bei Bedarf weitere Bearbeitungen und Änderungen vor. Um Ihre Bereitstellung anzupassen, können Sie Ihre VPC-Konfiguration ändern, die Anzahl und den Typ der Bastion-Host-Instances wählen, die Weiterleitung über TCP oder X11 aktivieren sowie ein standardmäßiges oder benutzerdefiniertes Banner für Ihre Bastion-Hosts aktivieren.

h. Wählen Sie Weiter aus.

5. Nehmen Sie auf der Seite Configure stack options (Stack-Optionen konfigurieren) bei Bedarf Bearbeitungen und Änderungen vor.
6. Wählen Sie Weiter aus.
7. Überprüfen Sie die Details zu Ihrem Bastion-Host und wählen Sie die beiden Bestätigungen für die Funktionen aus. Wählen Sie anschließend Create Stack (Stack erstellen) aus.

Schritt 3: Wählen Sie eine Vorlage aus und passen Sie sie an AWS CloudFormation

Heute können Sie mehrere Datenströme pro Kontakt in Ihren VPC fließen lassen. Diese Datenströme sind in zwei verschiedenen Formaten verfügbar. Datenströme mit VITA-49-Signal-/IP-Daten können für S-Band- und X-Band-Signale bis zu 54 MHz in Bandbreite konfiguriert werden. VITA-49 Erweiterungsdaten/IPs können für demodulierte und/oder dekodierte X-Band-Signale bis 500 MHz Bandbreite konfiguriert werden.

Nach der Hinzufügung Ihres Satelliten müssen Sie Missionsprofile definieren und Instances erstellen, um Daten-Streams von oder zu Ihrem Satelliten zu verarbeiten oder per Push zu senden. Um Sie bei diesem Prozess zu unterstützen, stellen wir vorkonfigurierte AWS CloudFormation Vorlagen zur Verfügung, die öffentliche Rundfunksatelliten verwenden. Diese Vorlagen erleichtern Ihnen den Einstieg in die Nutzung AWS Ground Station. Weitere Informationen zu AWS CloudFormation finden Sie unter Was ist AWS CloudFormation?

Es ist wichtig zu beachten, dass Sie über Datenverarbeitungssoftware oder Datenspeichersoftware verfügen müssen, die die Localhost-Seite von Data Defender der Amazon EC2 EC2-Instance überwacht. Diese Software verwenden Sie, um die Daten zu speichern und/oder zu verarbeiten, die während eines Kontakts an die Amazon EC2 EC2-Instance übermittelt wurden.

Konfiguration Ihrer Amazon EC2 EC2-Instance-Einstellungen

Die in diesem Abschnitt bereitgestellten AWS CloudFormation Vorlagen sind standardmäßig für die Verwendung von Amazon EC2 EC2-Instance-Typen vom Typ m5.4xlarge konfiguriert. Wir empfehlen Ihnen jedoch, die richtigen Amazon EC2 EC2-Instance-Einstellungen für Ihren Anwendungsfall anzupassen und auszuwählen. Anforderungen wie Speicher-E/A und CPU-Leistung sollten bei der Auswahl Ihrer Instance-Einstellungen berücksichtigt werden. Zum Beispiel erfordert das Ausführen eines Software-Modems auf einer Empfänger-Instance möglicherweise für die Datenverarbeitung optimierte Instances mit mehr Cores und einer höheren Taktfrequenz. Die beste Methode, um die richtigen Instance-Einstellungen für Ihren Anwendungsfall zu ermitteln, besteht darin, Ihre Instance-Einstellungen mit Ihrer Arbeitslast zu testen. Amazon EC2 macht es einfach, zwischen den Instance-Einstellungen zu wechseln. Verwenden Sie die Vorlagen und passen Sie die Instance-Einstellungen an Ihre Bedürfnisse an.

Als allgemeine Empfehlung AWS Ground Station empfiehlt es sich, Instances zu verwenden, die Enhanced Networking für Ihre Uplinks und Downlinks unterstützen, wie z. B. das AWS Nitro System. Weitere Informationen zum erweiterten Netzwerk finden Sie unter Aktivieren von Enhanced Networking-Funktionen mit dem Elastic Network Adapter (ENA) in Linux-Instances.

Zusätzlich zur Konfiguration von Amazon EC2 EC2-Instance-Typen konfigurieren die AWS CloudFormation Vorlagen die Amazon Machine Images (AMI) -Basisdaten, die für die Instance verwendet werden sollen. Die AWS Ground Station Basis enthält die Software, die für den Empfang von Daten aus dem auf Ihrer EC2-Instance vorinstallierten Service erforderlich ist. Weitere Informationen zu AMIs finden Sie unter Amazon Machine Images (AMI).

Manuelles Erstellen und Konfigurieren von Ressourcen

Mit den AWS CloudFormation Beispielvorlagen in diesem Abschnitt werden alle Ressourcen konfiguriert, die für den Beginn der Ausführung von Satellitenkontakten erforderlich sind. Wenn Sie es vorziehen, die Ressourcen, die für die Ausführung von Satellitenkontakten erforderlich sind, manuell zu erstellen und zu konfigurieren, müssen Sie wie folgt vorgehen:

- AWS Ground Station Konfigurationen erstellen. Weitere Informationen zum manuellen Erstellen von AWS Ground Station Konfigurationen finden Sie unter Create Config AWS CLI Command Reference oder Create Config API Reference.
- Erstellen Sie ein AWS Ground Station Missionsprofil. Weitere Informationen zur manuellen Erstellung eines AWS Ground Station Missionsprofils finden Sie unter Create Mission Profile (AWS CLI Command Reference) oder Create Mission Profile API-Referenz.
- Erstellen Sie eine AWS Ground Station Datenfluss-Endpunktgruppe. Weitere Informationen zum manuellen Erstellen einer AWS Ground Station Datenfluss-Endpunktgruppe finden Sie unter Create Dataflow Endpoint Group AWS CLI Command Reference oder Create Dataflow Endpoint Group API-Referenz.
- Erstellen Sie eine EC2-Instanz. Weitere Informationen zum manuellen Erstellen einer EC2-Instance zur Verwendung mit finden Sie AWS Ground Station unter. Erstellen Sie eine Amazon EC2 EC2-Instance
- Konfigurieren Sie die Sicherheitsgruppeneinstellungen Ihrer EC2-Instance so, dass Daten AWS Ground Station zu/von Ihrer EC2-Instance gesendet werden können. Weitere Informationen zur manuellen Konfiguration der Sicherheitsgruppeneinstellungen Ihrer EC2-Instance finden Sie unter Create Security Group AWS CLI Command Reference oder Create Security Group API Reference.

Auswahl einer Vorlage

AWS Ground Station bietet Vorlagen, die demonstrieren, wie der Service verwendet wird, und auf die auf unterschiedliche Weise zugegriffen werden kann. Verwenden Sie diese Anleitung, um die richtige Vorlage für Sie zu finden.

Verwenden einer vorkonfigurierten Vorlage

Sie können eine vorkonfigurierte Vorlage verwenden, um direkte Broadcast-Daten von den Satelliten Aqua, SNPP, JPSS-1/NOAA-20 und Terra zu empfangen. Diese Vorlagen enthalten die erforderlichen AWS CloudFormation -Ressourcen zum Planen und Ausführen von Kontakten. Die `AquaSnppJpss` Vorlage umfasst die erforderlichen AWS CloudFormation Ressourcen für den Empfang demodulierter und dekodierter Direktübertragungsdaten. Verwenden Sie diese Vorlage als Ausgangspunkt, wenn Sie die Daten mit der NASA Direct Readout Labs-Software (RT-STPS und IPOPP) verarbeiten möchten. Die `AquaSnppJpssTerraDigIF`-Vorlage enthält die notwendigen AWS CloudFormation -Ressourcen. um rohe digitalisierte Zwischenfrequenz-Direkt-Broadcast-Daten (DigiF) zu empfangen. Verwenden Sie diese Vorlage als Ausgangspunkt für die Verarbeitung der Daten mit einem Software Defined Radio

(SDR). Die `DirectBroadcastSatelliteWbDigIfEc2DataDelivery` Vorlage umfasst die erforderlichen AWS CloudFormation Ressourcen, um rohe digitale Breitband-Zwischenfrequenz-Direktübertragungsdaten (DigIF) über den Agenten zu empfangen. AWS Ground Station

Vorlagen für die Bereitstellung von Schmalband-Daten:

- the section called “AquaSnppJpss Vorlage (Schmalband)”
- the section called “AquaSnppJpssTerraDigIF-Vorlage (Schmalband)”

Vorlagen für die Bereitstellung von Breitband-DigIF-Daten:

- the section called “Breitband-DigIF-Vorlage für Satelliten-Breitbandübertragung (Breitband)”

> **Important**
>
> Satelliten müssen in den Dienst eingebunden sein, um mit den Vorlagen auf AMIs zugreifen zu können. AWS CloudFormation

Verwenden ihrer eigenen Satelliten

Für die Konfiguration Ihrer eigenen Satelliten sind unterschiedliche Parameter und Ressourcen erforderlich. Es ist nicht einfach, dies allein zu tun. Das AWS Ground Station Team hilft Ihnen gerne bei der Konfiguration Ihrer eigenen Satelliten für den Einsatz und kann Ihnen bei der Konfiguration von Ressourcen für Downlink-, Uplink- und Uplink-Echostreams helfen. Wenden Sie sich an den AWS-Support AWS Ground Station, um Ihren eigenen Satelliten für die Verwendung mit zu konfigurieren.

Zugriff auf Vorlagen

Sie können unten im regionalen Amazon S3 S3-Bucket auf die Vorlagen zugreifen. Hinweis: Im folgenden Link wird ein regionaler S3-Endpunkt verwendet. Wechseln Sie `<us-west-2>` zu der Region, in der Sie den AWS CloudFormation Stack erstellen.

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

Sie können die Vorlagen auch mit dem AWS CLI herunterladen. Informationen zur Konfiguration von finden Sie unter Konfiguration von AWS CLI. AWS CLI

AquaSnppJpss Vorlage (Schmalband)

Die angegebene AWS CloudFormation Vorlage `AquaSnppJpss.yml` soll Ihnen einen schnellen Zugriff ermöglichen, um mit dem Empfang von Daten für die Satelliten Aqua, SNPP und JPSS-1/NOAA-20 zu beginnen. Es enthält eine Amazon EC2 EC2-Instance und die erforderlichen AWS Ground Station Ressourcen, um Kontakte zu planen und demodulierte und dekodierte Direktübertragungsdaten zu empfangen. Diese Vorlage ist ein guter Ausgangspunkt, wenn Sie planen, die Daten mit der NASA Direct Readout Labs Software (RT-STPS und IPOPP) zu verarbeiten.

Wenn Aqua, SNPP und JPSS-1/NOAA-20 nicht in Ihr Konto integriert sind, finden Sie weitere Informationen unter Kunden-Onboarding.

> **Important**
>
> Die Amazon EC2 EC2-Instance muss gestoppt werden, bevor die Vorlage angewendet werden kann. Stellen Sie sicher, dass die Instance gestoppt ist, bis Sie sie verwenden können.

Sie können auf die Vorlage zugreifen, indem Sie auf den S3-Bucket für das Kunden-Onboarding zugreifen. Beachten Sie, dass die folgenden Links einen regionalen S3-Bucket verwenden. Wechseln Sie `<us-west-2>` zu der Region, in der Sie den AWS CloudFormation Stack erstellen.

> **Note**
>
> Die folgenden Anweisungen verwenden YAML. Die Vorlagen sind jedoch sowohl im YAML- als auch im JSON-Format verfügbar. Um JSON zu verwenden, ersetzen Sie `<.yml>` durch `<.json>`.

Verwenden Sie den folgenden Befehl AWS CLI, um die Vorlage herunterzuladen:

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

Die Vorlage kann in der Konsole angezeigt und heruntergeladen werden, indem Sie in Ihrem Browser zur folgenden URL navigieren:

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

Sie können die Vorlage direkt AWS CloudFormation über den folgenden Link angeben:

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

Welche Ressourcen definiert die Vorlage?

Die `AquaSnppJpss`-Vorlage beinhaltet die folgenden Ressourcen:

- Rolle „Datenlieferdienst“ — AWS Ground Station übernimmt diese Rolle, um ENIs in Ihrem Konto zu erstellen/zu löschen, um Daten zu streamen.
- (Optional) Receiver-Instance — Die Amazon EC2 EC2-Instance, die Daten zu/von Ihrem Satelliten sendet/empfängt mit. AWS Ground Station
  - Instance-Sicherheitsgruppe — Die Sicherheitsgruppe für Ihre Amazon EC2 EC2-Instance.
  - Instance-Rolle — Die Rolle für Ihre Amazon EC2 EC2-Instance.
  - Instance-Profil — Das Instance-Profil für Ihre Amazon EC2 EC2-Instance.
  - Cluster Placement Group — Die Placement-Gruppe, in der Ihre Amazon EC2 EC2-Instance gestartet wird.
- Dataflow Endpoint Security Group — Die Sicherheitsgruppe, zu der die von erstellte elastic network interface AWS Ground Station gehört. Standardmäßig ermöglicht AWS Ground Station diese Sicherheitsgruppe das Streamen von Datenverkehr an eine beliebige IP-Adresse in Ihrer VPC. Sie können dies so ändern, dass der Datenverkehr auf einen bestimmten Satz von IP-Adressen beschränkt wird.
- Receiver Instance Network Interface — Eine elastic network interface, die eine feste IP-Adresse für AWS Ground Station die Verbindung bereitstellt. Diese wird an die Receiver-Instance auf `eth1` angehängt.
- Receiver Instance Interface Attachment — Eine elastic network interface, die an Ihre Amazon EC2-Instance angeschlossen wird.
- (Optional) CloudWatch Ereignisauslöser — AWS Lambda Funktion, die mithilfe von CloudWatch Ereignissen ausgelöst wird, die AWS Ground Station vor und nach einem Kontakt gesendet wurden. Die AWS Lambda Funktion startet und stoppt optional Ihre Receiver-Instanz.
- (Optional) EC2-Verifizierung für Kontakte — Die Option, Lambda zu verwenden, um ein Überprüfungssystem für Ihre Amazon EC2 EC2-Instance (s) für Kontakte mit SNS-

Benachrichtigung einzurichten. Bitte beachten Sie, dass hierfür je nach Ihrer aktuellen Nutzung Gebühren anfallen können.

- Dataflow-Endpunktgruppe — Die AWS Ground Station Datenfluss-Endpunktgruppe, die die Endpunkte definiert, die zum Senden/Empfangen von Daten zu/von Ihrem Satelliten verwendet werden. AWS Ground Station Erstellt im Rahmen der Erstellung der Dataflow-Endpunktgruppe eine elastic network interface in Ihrem Konto, um Daten zu streamen.
- Tracking-Konfiguration — Die AWS Ground Station Tracking-Konfiguration definiert, wie das Antennensystem Ihren Satelliten verfolgt, wenn er sich durch den Himmel bewegt.
- Ground Station Amazon Machine Image Retrieval Lambda — Die Option, um auszuwählen, welche Software in Ihrer Instance installiert ist, und das AMI Ihrer Wahl. Die Softwareoptionen umfassen `DDX 2.6.2 Only` und. `DDX 2.6.2 with qRadio 3.6.0` Wenn Sie Wideband DigIF Data Delivery und den AWS Ground Station Agent verwenden möchten, verwenden Sie bitte den. AquaSnppJpssTerraDigIF-Vorlage (Schmalband) Diese Optionen werden mit der Veröffentlichung zusätzlicher Softwareupdates und Funktionen weiter ausgebaut.

Darüber hinaus bietet die Vorlage die folgenden Ressourcen für die Satelliten Aqua, SNPP, JPSS-1/NOAA-20:

- Eine Downlink-Demod/Dekodierungskonfiguration für JPSS-1/NOAA-20 und SNPP sowie eine Downlink-Demod/Dekodierungskonfiguration für Aqua
- Ein Missionsprofil für JPSS-1/NOAA-20 und SNPP und ein Missionsprofil für Aqua

Die Werte und Parameter für die Satelliten in dieser Vorlage sind bereits ausgefüllt. Diese Parameter erleichtern Ihnen die AWS Ground Station sofortige Verwendung mit diesen Satelliten. Sie müssen keine eigenen Werte konfigurieren, um diese Vorlage AWS Ground Station verwenden zu können. Sie können die Werte jedoch anpassen, damit die Vorlage für Ihren Anwendungsfall funktioniert.

Wo erhalte ich meine Daten?

Die Datenverkehr-Endpunktgruppe wird so eingerichtet, dass die als Teil der Vorlage erstellte Netzwerkschnittstelle der Receiver-Instance verwendet wird. Die Empfängerinstanz verwendet Data Defender, um den Datenstrom von AWS Ground Station dem durch den Datenflussendpunkt definierten Port zu empfangen. Nach Erhalt stehen die Daten über den UDP-Port 50000 auf dem Loopbackadapter der Receiver-Instance zur Verfügung. Weitere Informationen zum Einrichten einer Datenfluss-Endpunktgruppe finden Sie unter Gruppe. AWS::GroundStation::DataflowEndpoint

AquaSnppJpssTerraDigIF-Vorlage (Schmalband)

Die genannte AWS CloudFormation Vorlage `AquaSnppJpssTerraDigIF.yml` soll Ihnen einen schnellen Zugriff ermöglichen, um mit dem Empfang digitalisierter Zwischenfrequenzdaten (DigIF) für die Satelliten Aqua, SNPP, JPSS-1/NOAA-20 und Terra zu beginnen. Es enthält eine Amazon EC2 EC2-Instance und die erforderlichen AWS CloudFormation Ressourcen für den Empfang von DigiF-Direct-Broadcast-Rohdaten. Diese Vorlage ist ein guter Ausgangspunkt für die Verarbeitung der Daten mit einem Software Defined Radio (SDR).

Wenn Aqua, SNPP und JPSS-1/NOAA-20 und Terra nicht in Ihr Konto integriert sind, finden Sie weitere Informationen unter Kunden-Onboarding.

> **Important**
>
> Die Amazon EC2 EC2-Instance muss gestoppt werden, bevor die Vorlage angewendet werden kann. Stellen Sie sicher, dass die Instance gestoppt ist, bis Sie sie verwenden können.

Sie können auf die Vorlage zugreifen, indem Sie auf den S3-Bucket für das Kunden-Onboarding zugreifen. Beachten Sie, dass die folgenden Links einen regionalen S3-Bucket verwenden. Wechseln Sie `<us-west-2>` zu der Region, in der Sie den AWS CloudFormation Stack erstellen.

> **Note**
>
> Die folgenden Anweisungen verwenden YAML. Die Vorlagen sind jedoch sowohl im YAML- als auch im JSON-Format verfügbar. Um JSON zu verwenden, ersetzen Sie `<.yml>` durch `<.json>`.

Verwenden Sie den folgenden Befehl AWS CLI, um die Vorlage herunterzuladen:

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

Die Vorlage kann in der Konsole angezeigt und heruntergeladen werden, indem Sie in Ihrem Browser zur folgenden URL navigieren:

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

Sie können die Vorlage direkt AWS CloudFormation über den folgenden Link angeben:

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

Welche Ressourcen definiert die Vorlage?

Die `AquaSnppJpssTerraDigIF`-Vorlage beinhaltet die folgenden Ressourcen:

- Rolle „Datenlieferdienst“ — AWS Ground Station übernimmt diese Rolle, um ENIs in Ihrem Konto zu erstellen/zu löschen, um Daten zu streamen.
- (Optional) Receiver-Instance — Die Amazon EC2 EC2-Instance, die Daten zu/von Ihrem Satelliten sendet/empfängt mit. AWS Ground Station
  - Instance-Sicherheitsgruppe — Die Sicherheitsgruppe für Ihre Amazon EC2 EC2-Instance.
  - Instance-Rolle — Die Rolle für Ihre Amazon EC2 EC2-Instance.
  - Instance-Profil — Das Instance-Profil für Ihre Amazon EC2 EC2-Instance.
  - Cluster Placement Group — Die Placement-Gruppe, in der Ihre Amazon EC2 EC2-Instance gestartet wird.
- Dataflow Endpoint Security Group — Die Sicherheitsgruppe, zu der die von erstellte elastic network interface AWS Ground Station gehört. Standardmäßig ermöglicht AWS Ground Station diese Sicherheitsgruppe das Streamen von Datenverkehr an eine beliebige IP-Adresse in Ihrer VPC. Sie können dies so ändern, dass der Datenverkehr auf einen bestimmten Satz von IP-Adressen beschränkt wird.
- Receiver Instance Network Interface — Eine elastic network interface, die eine feste IP-Adresse für AWS Ground Station die Verbindung bereitstellt. Diese wird an die Receiver-Instance auf `eth1` angehängt.
- Receiver Instance Interface Attachment — Eine elastic network interface, die an Ihre Amazon EC2-Instance angeschlossen wird.
- (Optional) CloudWatch Ereignisauslöser — AWS Lambda Funktion, die mithilfe von CloudWatch Ereignissen ausgelöst wird, die AWS Ground Station vor und nach einem Kontakt gesendet wurden. Die AWS Lambda Funktion startet und stoppt optional Ihre Receiver-Instanz.
- (Optional) EC2-Verifizierung für Kontakte — Die Option, Lambda zu verwenden, um ein Überprüfungssystem für Ihre Amazon EC2 EC2-Instance (s) für Kontakte mit SNS-

Benachrichtigung einzurichten. Bitte beachten Sie, dass hierfür je nach Ihrer aktuellen Nutzung Gebühren anfallen können.

- Dataflow-Endpunktgruppe — Die AWS Ground Station Datenfluss-Endpunktgruppe, die die Endpunkte definiert, die zum Senden/Empfangen von Daten zu/von Ihrem Satelliten verwendet werden. AWS Ground Station Erstellt im Rahmen der Erstellung der Dataflow-Endpunktgruppe eine elastic network interface in Ihrem Konto, um Daten zu streamen.
- Tracking-Konfiguration — Die AWS Ground Station Tracking-Konfiguration definiert, wie das Antennensystem Ihren Satelliten verfolgt, wenn er sich durch den Himmel bewegt.
- Downlink Dig IF Endpoint Config - Ein definierter Endpunkt für das Downlinking von Daten von Ihrem Satelliten.
- Ground Station Amazon Machine Image Retrieval Lambda — Die Option, um auszuwählen, welche Software in Ihrer Instance installiert ist, und das AMI Ihrer Wahl. Die Softwareoptionen umfassen `DDX 2.6.2 Only` und. `DDX 2.6.2 with qRadio 3.6.0` Diese Optionen werden mit der Veröffentlichung zusätzlicher Softwareupdates und Funktionen weiter erweitert.

Darüber hinaus bietet die Vorlage die folgenden Ressourcen für die Satelliten Aqua, SNPP, JPSS-1/NOAA-20 und Terra:

- Eine Downlink DigiF Antennenkonfiguration für Aqua, SNPP, JPSS-1/NOAA-20 und Terra.
- Ein Missionsprofil für JPSS-1/NOAA-20 und SNPP, ein Missionsprofil für Aqua und ein Missionsprofil für Terra.

Die Werte und Parameter für die Satelliten in dieser Vorlage sind bereits ausgefüllt. Diese Parameter erleichtern Ihnen die AWS Ground Station sofortige Verwendung mit diesen Satelliten. Sie müssen keine eigenen Werte konfigurieren, um diese Vorlage AWS Ground Station verwenden zu können. Sie können die Werte jedoch anpassen, damit die Vorlage für Ihren Anwendungsfall funktioniert.

Wo erhalte ich meine Daten?

Die Datenverkehr-Endpunktgruppe wird so eingerichtet, dass die als Teil der Vorlage erstellte Netzwerkschnittstelle der Receiver-Instance verwendet wird. Die Empfängerinstanz verwendet Data Defender, um den Datenstrom von AWS Ground Station dem durch den Datenflussendpunkt definierten Port zu empfangen. Nach Erhalt stehen die Daten über den UDP-Port 50000 auf dem Loopbackadapter der Receiver-Instance zur Verfügung. Weitere Informationen zum Einrichten einer Datenfluss-Endpunktgruppe finden Sie unter Gruppe. AWS::GroundStation::DataflowEndpoint

Breitband-DigIF-Vorlage für Satelliten-Breitbandübertragung (Breitband)

Die genannte AWS CloudFormation Vorlage `DirectBroadcastSatelliteWbDigIfEc2DataDelivery.yml` soll Ihnen einen schnellen Zugriff ermöglichen, um mit dem Empfang digitalisierter Zwischenfrequenzdaten (DigIF) für die Satelliten Aqua, SNPP, JPSS-1/NOAA-20 und Terra zu beginnen. Es enthält eine Amazon EC2 EC2-Instance und die erforderlichen AWS CloudFormation Ressourcen für den Empfang von DigiF-Direct-Broadcast-Rohdaten. Diese Vorlage ist ein guter Ausgangspunkt für die Verarbeitung der Daten mit einem Software Defined Radio (SDR).

Wenn Aqua, SNPP und JPSS-1/NOAA-20 und Terra nicht in Ihr Konto integriert sind, finden Sie weitere Informationen unter Kunden-Onboarding.

> **Important**
>
> Die Amazon EC2 EC2-Instance muss gestoppt werden, bevor die Vorlage angewendet werden kann. Stellen Sie sicher, dass die Instance gestoppt ist, bis Sie sie verwenden können.

Sie können auf die Vorlage zugreifen, indem Sie auf den S3-Bucket für das Kunden-Onboarding zugreifen. Beachten Sie, dass die folgenden Links einen regionalen S3-Bucket verwenden. Wechseln Sie `<us-west-2>` zu der Region, in der Sie den AWS CloudFormation Stack erstellen.

> **Note**
>
> Die folgenden Anweisungen verwenden YAML. Die Vorlagen sind jedoch sowohl im YAML- als auch im JSON-Format verfügbar. Um JSON zu verwenden, ersetzen Sie `<.yml>` durch `<.json>`.

Verwenden Sie den folgenden Befehl AWS CLI, um die Vorlage herunterzuladen:

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

Die Vorlage kann in der Konsole angezeigt und heruntergeladen werden, indem Sie in Ihrem Browser zur folgenden URL navigieren:

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

Sie können die Vorlage direkt AWS CloudFormation über den folgenden Link angeben:

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

Welche Ressourcen definiert die Vorlage?

Die `DirectBroadcastSatelliteWbDigIfEc2DataDelivery`-Vorlage beinhaltet die folgenden Ressourcen:

- (Optional) Receiver-Instance — Die Amazon EC2 EC2-Instance, die Daten zu/von Ihrem Satelliten sendet/empfängt mit. AWS Ground Station
  - Instance-Sicherheitsgruppe — Die Sicherheitsgruppe für Ihre Amazon EC2 EC2-Instance.
  - Instance-Rolle — Die Rolle für Ihre Amazon EC2 EC2-Instance.
  - Instance-Profil — Das Instance-Profil für Ihre Amazon EC2 EC2-Instance.
  - Cluster Placement Group — Die Placement-Gruppe, in der Ihre Amazon EC2 EC2-Instance gestartet wird.
- Datenlieferschlüssel — AWS KMS Schlüssel, der zur Verschlüsselung von Datenflüssen verwendet wird.
- Schlüsselrolle der Ground Station — Die IAM-Rolle, die den Zugriff auf und AWS Ground Station die Verwendung des AWS KMS Schlüssels zur Entschlüsselung von Datenflüssen übernimmt
- Schlüsselzugriffsrichtlinie für Ground Station — Die IAM-Richtlinie, die festlegt, welche Aktionen mit dem Data Delivery Key ausgeführt werden AWS Ground Station können
- Receiver Instance Elastic Network Interface — (Bedingt) Eine elastic network interface wird in dem von angegebenen Subnetz erstellt, PublicSubnetIdfalls bereitgestellt. Dies ist erforderlich, wenn sich die Empfängerinstanz in einem privaten Subnetz befindet. Die elastic network interface wird mit der EIP verknüpft und an die Empfängerinstanz angehängt.
- Receiver Instance Elastic IP — Eine elastische IP, mit der eine Verbindung hergestellt AWS Ground Station wird. Dies wird an die Empfängerinstanz oder die elastic network interface angehängt.
- Eine der folgenden Elastic IP-Assoziationen:

  - Zuordnung zwischen Receiver Instance und Elastic IP — Die Zuordnung der Elastic IP zu Ihrer Receiver-Instance, falls PublicSubnetIdnicht angegeben. Dazu muss SubnetIdauf ein öffentliches Subnetz verwiesen werden.
  - elastic network interface der Receiver Instance to Elastic IP Association — Die Zuordnung der Elastic IP zur Elastic Network-Schnittstelle der Receiver-Instance, sofern PublicSubnetIdangegeben.
- (Optional) CloudWatch Event-Trigger — AWS Lambda Funktion, die mithilfe von CloudWatch Ereignissen ausgelöst wird, die AWS Ground Station vor und nach einem Kontakt gesendet wurden. Die AWS Lambda Funktion startet und stoppt optional Ihre Receiver-Instanz.
- (Optional) EC2-Verifizierung für Kontakte — Die Option, Lambda zu verwenden, um ein Überprüfungssystem für Ihre Amazon EC2 EC2-Instance (s) für Kontakte mit SNS-Benachrichtigung einzurichten. Bitte beachten Sie, dass hierfür je nach Ihrer aktuellen Nutzung Gebühren anfallen können.
- Dataflow-Endpunktgruppe — Die AWS Ground Station Datenfluss-Endpunktgruppe, die die Endpunkte definiert, die zum Senden/Empfangen von Daten zu/von Ihrem Satelliten verwendet werden.
- Tracking-Konfiguration — Die AWS Ground Station Tracking-Konfiguration definiert, wie das Antennensystem Ihren Satelliten verfolgt, wenn er sich durch den Himmel bewegt.

Darüber hinaus bietet die Vorlage die folgenden Ressourcen für die Satelliten Aqua, SNPP, JPSS-1/NOAA-20 und Terra:

- Eine Downlink-Konfiguration für JPSS-1/NOAA-20 und SNPP, eine Downlink-Konfiguration für Aqua und eine Downlink-Konfiguration für Terra.
- Ein Missionsprofil für JPSS-1/NOAA-20 und SNPP, ein Missionsprofil für Aqua und ein Missionsprofil für Terra.

Die Werte und Parameter für die Satelliten in dieser Vorlage sind bereits ausgefüllt. Diese Parameter erleichtern Ihnen die sofortige Verwendung mit diesen Satelliten. AWS Ground Station Sie müssen keine eigenen Werte konfigurieren, um diese Vorlage AWS Ground Station verwenden zu können. Sie können die Werte jedoch anpassen, damit die Vorlage für Ihren Anwendungsfall funktioniert.

Wo erhalte ich meine Daten?

Die Datenverkehr-Endpunktgruppe wird so eingerichtet, dass die als Teil der Vorlage erstellte Netzwerkschnittstelle der Receiver-Instance verwendet wird. Die Empfängerinstanz verwendet

den AWS Ground Station Agenten, um den Datenstrom von AWS Ground Station dem durch den Datenflussendpunkt definierten Port zu empfangen. Weitere Informationen zum Einrichten einer Datenfluss-Endpunktgruppe finden Sie unter Gruppe. AWS::GroundStation::DataflowEndpoint Weitere Informationen zum AWS Ground Station Agenten finden Sie unter. AWS Ground Station Benutzerhandbuch für Agenten

Erstellen Sie eine Amazon EC2 EC2-Instance

> **Note**
>
> Es ist weder notwendig noch empfehlenswert, Ihre Ressourcen AWS Ground Station (einschließlich Amazon EC2 EC2-Instances) manuell zu erstellen, da hierfür AWS Ground Station vorgefertigte AWS CloudFormation Vorlagen bereitgestellt werden (weitere Informationen finden Sie unterSchritt 3: Wählen Sie eine Vorlage aus und passen Sie sie an AWS CloudFormation). Wenn die Verwendung von AWS CloudFormation Vorlagen für Ihren Anwendungsfall nicht funktioniert, lesen Sie bitte weiter.

AWS Ground Station bietet Amazon EC2 EC2-AMIs, auf denen die Software vorinstalliert ist, die für die Datenlieferung auf einer Amazon EC2 EC2-Instance für Narrowband- oder Wideband-Datenlieferung erforderlich ist. DigIf

> **Important**
>
> Satelliten müssen in den Service eingebunden sein, um auf die AMIs zugreifen zu können. AWS Ground Station

Amazon EC2 AMI mit DataDefender

Dieses AMI ist in der DataDefender Software vorinstalliert und wird für Downlink-Kontakte zur Schmalband-Datenübermittlung verwendet.

Das Benennungsschema für dieses AMI lautet`groundstation-al2-ddx$DDX_VERSION-ami-$DATE_PUBLISHED`. Kurz nach der Veröffentlichung eines neuen AL2-Amazon EC2-AMI wird ein neues DDX-AMI veröffentlicht. Wenn Sie AWS Ground Station sich für die Unterstützung einer neuen Version der DataDefender Software entscheiden, wird ein neues AMI mit der aktualisierten Version veröffentlicht.

Auswahl eines AWS Ground Station AMI mit DataDefender

Sie können über die Registerkarte AMIs in der Amazon EC2 EC2-Konsole auf das AWS Ground Station AMI zugreifen. Sobald Sie sich auf dieser Seite befinden, können Sie über den Filter Private Images auf die AMIs zugreifen.

Wir empfehlen, die AMIs nach dem Veröffentlichungsdatum zu sortieren und das zuletzt veröffentlichte AMI mit dem Namen zu verwenden`groundstation-al2-ddx$DDX_VERSION-ami-$DATE_PUBLISHED`.

Amazon EC2 AMI mit dem Agenten AWS Ground Station

Dieses AMI ist mit dem AWS Ground Station Agenten vorinstalliert und wird für Breitband-DigiF-Downlink-Kontakte verwendet.

Das Benennungsschema für dieses AMI ist`groundstation-al2-gs-agent-ami-*`, wobei * das Datum ist, an dem das AMI erstellt wurde. Ein neues AWS Ground Station Agent-AMI wird kurz nach der Veröffentlichung eines neuen AL2-Amazon EC2-AMI oder wenn eine neue Version des AWS Ground Station Agent-RPM veröffentlicht wird, veröffentlicht.

Weitere Informationen über den AWS Ground Station Agenten finden Sie unter. AWS Ground Station Benutzerhandbuch für Agenten

Auswahl eines AWS Ground Station Agent-AMI

Sie können über die Registerkarte AMIs in der Amazon EC2 EC2-Konsole auf das AWS Ground Station Agent-AMI zugreifen. Sobald Sie sich auf dieser Seite befinden, können Sie über den Filter Öffentliche Bilder auf die AMIs zugreifen.

Wir empfehlen, die AMIs nach dem Veröffentlichungsdatum zu sortieren und das zuletzt veröffentlichte AMI mit dem Namen zu verwenden`groundstation-al2-gs-agent-ami-$DATE_PUBLISHED`.

Schritt 4: Einen AWS CloudFormation Stack konfigurieren

Nachdem Sie die Vorlage ausgewählt haben, die am besten zu Ihrem Anwendungsfall passt, konfigurieren Sie einen AWS CloudFormation Stack. Die in diesem Verfahren erstellten Ressourcen werden für die Region konfiguriert, in der Sie sich bei der Erstellung befinden. Dazu gehören das Missionsprofil und die jeweiligen Eigenschaften, die bestimmen, an welche Region Ihre Daten übermittelt werden.

1. Wählen Sie im AWS Management ConsoleDienste > CloudFormation.
2. Klicken Sie im Navigationsbereich auf Stacks. Klicken Sie dann auf Create stack (Stack erstellen) > With new resources (standard) (Mit neuen Ressourcen (Standard)).
3. Geben Sie auf der Seite Create Stack (Stack erstellen) die Vorlage an, die Sie in the section called “Auswahl einer Vorlage” ausgewählt haben, indem Sie wie folgt vorgehen:

   a. Wählen Sie Amazon S3 URL als Vorlagenquelle und kopieren Sie die URL der Vorlage, die Sie in Amazon S3 URL verwenden möchten. Wählen Sie anschließend Weiter.

   b. Wählen Sie Upload a template file (Eine Vorlagendatei hochladen) als Ihre Vorlagenquelle aus und klicken Sie anschließend auf Choose File (Datei auswählen). Laden Sie die in the section called “Auswahl einer Vorlage” heruntergeladene Vorlage hoch. Wählen Sie anschließend Weiter.
4. Nehmen Sie auf der Seite Specify stack details (Stack-Details angeben) die folgenden Änderungen vor:

   a. Geben Sie in das Feld Stack Name (Stack-Name) einen Namen ein. Wir empfehlen, einen einfachen Namen zu verwenden, um die Gefahr von Fehlern in der Zukunft zu verringern.

   b. Wählen Sie für aus CloudWatchEventActions, welche Aktionen für das CloudWatch Ereignis ausgeführt werden sollen, das vor und nach einem Kontakt ausgelöst wird.

   c. Wählen Sie für CreateEC2 ausVerificationForContacts, ob Sie ein Überprüfungssystem (mit Lambda) Ihrer EC2-Instance (en) für Kontakte mit SNS-Benachrichtigung einrichten möchten oder nicht. Es ist wichtig zu beachten, dass hierfür je nach Ihrer aktuellen Nutzung Gebühren anfallen können.

   d. Wählen Sie für CreateReceiverInstance, ob Sie eine Amazon EC2 EC2-Empfänger-Instance erstellen möchten oder nicht.

   e. Wählen Sie den SSH-Schlüssel aus, den Sie in the section called “Schritt 1: Erstellen eines EC2-SSH-Schlüsselpaars” erstellt haben.

   f. Wählen Sie die aus, SubnetIdin der Sie Ihre Amazon EC2 EC2-Instance erstellen möchten.

      Wenn Sie den AWS Ground Station Agenten verwenden, ist ein öffentliches Subnetz erforderlich, entweder für die Platzierung der Instance oder eine elastic network interface. Wenn Sie ein privates Subnetz angeben, SubnetIdin dem Ihre Instance platziert werden soll, müssen Sie auch ein öffentliches Subnetz angeben PublicSubnetId(siehe unten), das mit dem Agenten verwendet werden soll. AWS Ground Station

Für Anwendungsfälle ohne Agenten empfehlen wir als bewährte Methode, Ihre Amazon EC2 EC2-Instance in einem privaten Subnetz zu platzieren, obwohl dies nicht erforderlich ist. Sie können die Linux Bastion Hosts in der AWS Cloud: Quick Start Reference Deployment verwenden, um automatisch ein privates Subnetz zu erstellen, wenn Sie Ihr Konto noch nicht mit einem solchen in the section called “Schritt 2: Einrichten Ihrer VPC” konfiguriert haben.

> **Note**
>
> Ihre Organisation verfügt möglicherweise über ein anderes Subnetz, das für Ihre Amazon EC2 EC2-Instance reserviert ist.

g. (Optional) Wählen Sie die Option PublicSubnetId, die nur verwendet werden soll, wenn Sie den AWS Ground Station Agenten mit einer Instance in einem privaten Subnetz verwenden. Dies ist erforderlich, wenn Sie in ein privates Subnetz angegeben haben. SubnetId

   Dieses Subnetz muss sich in Ihrem Konto in derselben Verfügbarkeitszone befinden wie die von angegebene. SubnetId Die Bereitstellung von PublicSubnetIdführt zur Erstellung einer elastic network interface im bereitgestellten öffentlichen Subnetz, das mit Ihrer Instance verbunden ist. Diese Schnittstelle wird für den AWS Ground Station Agent-Netzwerkzugriff von Ihrer Instance aus verwendet, die sich in dem privaten Subnetz befindet, das in angegeben ist. SubnetId

h. Wählen Sie den VPC-Stack aus, den Sie in the section called “Schritt 2: Einrichten Ihrer VPC” erstellt haben.

i. Wählen Sie Weiter aus.

5. Konfigurieren Sie Stack-Optionen und erweiterte Optionen für Ihre Amazon EC2 EC2-Instance.

   a. Fügen Sie in den Abschnitten Tagsund Permissions (Berechtigungen) alle Tags und Berechtigungen hinzu.

   b. Nehmen Sie alle Änderungen für Ihre Stack-Richtlinie, Rollback-Konfiguration, Benachrichtigungsoptionen, und Stack-Erstellungsoptionenvor.

   c. Wählen Sie Weiter aus.

6. Nachdem Sie die Details zum Stack überprüft haben, wählen Sie die Bestätigung der Capabilities (Funktionen) und klicken auf Create stack (Stapel erstellen).

Schritt 5: Installieren und Konfigurieren von FE Prozessor/Funkgerät

Auf der in der AWS CloudFormation Vorlage definierten Amazon EC2 EC2-Instance ist standardmäßig kein Front-End-Prozessor (FE) oder Software Defined Radio (SDR) installiert. Sie müssen einen FE-Prozessor oder ein SDR installieren, um die zu/von dem AWS Ground Station - Antennensystem gestreamten VITA-49-Pakete verarbeiten zu können.

Wie Sie Ihren FE-Prozessor oder Ihr SDR installieren und konfigurieren, hängt davon ab, welchen FE-Prozessor oder welches SDR Sie verwenden. Die Installation eines FE-Prozessors oder SDR ist nicht Gegenstand dieses Benutzerhandbuchs.

Zum Installieren und Konfigurieren des FE-Prozessors/Funkgeräts wenden Sie sich bitte an den AWS-Support.

> **Important**
>
> Es hat sich bewährt, Ihren FE-Prozessor oder SDR auf den mit der AWS CloudFormation Vorlage erstellten Instances auszuführen, um sicherzustellen, dass die Vorteile der DTLS-Datenströme zum/von Data Defender genutzt werden.

Nächste Schritte

Ihr AWS Ground Station Konto und Ihre Ressourcen sind jetzt konfiguriert und einsatzbereit. Diese Ressourcen stehen in der AWS Ground Station Konsole zur Verfügung, in der Sie Satellitendaten eingeben, Antennenstandorte identifizieren, kommunizieren und die Antennenzeit für ausgewählte Satelliten planen können. Sie können auch verschiedene Tools verwenden, um Aktivitäten zu überwachen und Alarme zu konfigurieren.

Weitere Informationen finden Sie in den folgenden Themen:

- Auflisten und Reservieren von Kontakten
- Überwachung AWS Ground Station

Verwenden eines regionsübergreifenden Datenübermittlungsdiensts

Die AWS Ground Station regionsübergreifende Datenbereitstellungsfunktion bietet Ihnen die Flexibilität, Ihre Daten von einer Antenne an eine Amazon EC2-Instance in Ihrer AWS-Region zu senden. Die regionsübergreifende Datenbereitstellung ist derzeit in allen AWS Ground Station unterstützten Regionen verfügbar, wenn Sie Ihre Kontaktdaten in einem Amazon S3-Bucket empfangen. Sie ist nur in den folgenden antenna-to-destination Regionen verfügbar, wenn die Datenbereitstellung an Amazon EC2 verwendet wird:

- Region USA Ost (Ohio) (us-ost-2) bis Region USA West (Oregon) (us-west-2)
- Region USA West (Oregon) (us-west-2) bis Region USA Ost (Ohio) (us-ost-2)

Um die regionsübergreifende Datenbereitstellung zu verwenden, sollten Sie eine - AWS CloudFormation Vorlage konfiguriert haben. Weitere Informationen zur Auswahl und Anpassung von AWS CloudFormation Vorlagen finden Sie unter Schritt 3: Wählen Sie eine Vorlage aus und passen Sie sie an AWS CloudFormation.

Verwenden Sie die folgenden Themen, um die bereichsübergreifende Datenübermittlung in AWS Ground Station zu verwenden.

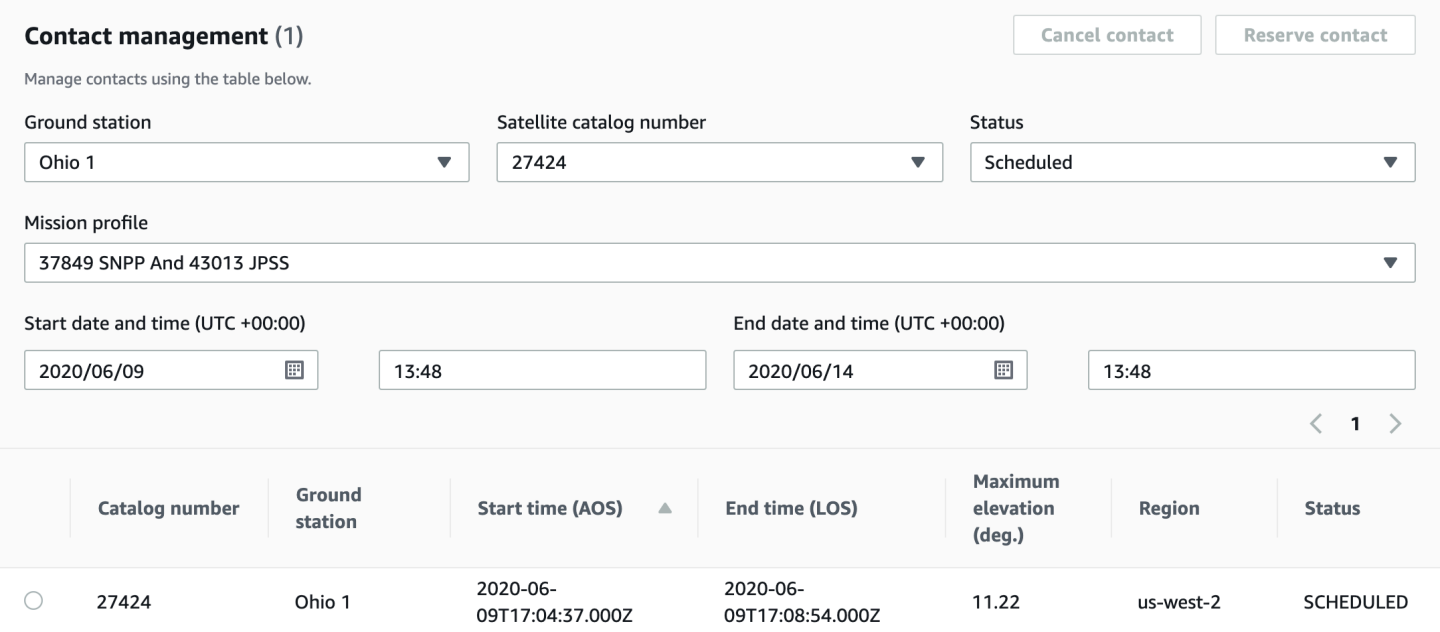
Themen

- So verwenden Sie die regionsübergreifende Datenübermittlung in der Konsole
- So verwenden Sie die regionsübergreifende Datenübermittlung mit der AWS-CLI

So verwenden Sie die regionsübergreifende Datenübermittlung in der Konsole

Wenn Sie einen Kontakt in der Konsole reservieren, wählen Sie das Missionsprofil aus, das für die Übermittlung der Kontaktdaten an die gewünschte Region konfiguriert ist. AWS Ground Station Stellen Sie sicher, dass alle Parameter korrekt sind und wählen Sie Kontakt reservieren. Wenn das gewünschte Missionsprofil in der Konsole nicht angezeigt wird, stellen Sie sicher, dass Sie das Missionsprofil in der Region erstellt haben, in der Sie die Konsole anzeigen.

Nachdem Sie Ihren Kontakt reserviert haben, können Sie geplante Kontakte anzeigen um zu überprüfen, ob Sie die regionsübergreifende Datenübermittlung geplant haben, indem Sie den Standort der Bodenstationsantenne und die Zielregion anzeigen. Die folgende Abbildung zeigt einen Kontakt, der für die regionsübergreifende Datenübermittlung geplant ist. Der Kontakt ist so konfiguriert, dass er die Antennen der Bodenstation in Ohio benutzt und Daten an Oregon übermittelt.



So verwenden Sie die regionsübergreifende Datenübermittlung mit der AWS-CLI

Wenn Sie einen Kontakt in reservieren AWS CLI, wählen Sie das Missionsprofil aus, das so konfiguriert ist, dass die Kontaktdaten an Ihre gewünschte Region übermittelt werden. Geben Sie den ARN des gewünschten Missionsprofils mit `--mission-profile-arn <value>` an. Stellen Sie sicher, dass alle Parameter korrekt sind, und führen Sie den Befehl aus. Wenn der gewünschte Missionsprofil-ARN beim Anzeigen und Auflisten von Kontakten nicht angezeigt wird, stellen Sie sicher, dass Sie das Missionsprofil in der Region erstellt haben, in der Sie die AWS CLI ausführen.

Nachdem Sie Ihren Kontakt reserviert haben, können Sie geplante Kontakte anzeigen um zu überprüfen, ob Sie die regionsübergreifende Datenübermittlung geplant haben, indem Sie den Standort der Bodenstationsantenne und die Zielregion anzeigen. Die folgende Ausgabe zeigt einen Kontakt, der für die regionsübergreifende Datenübermittlung geplant ist. Der Kontakt ist so konfiguriert, dass er die Bodenstationsantennen in Ohio verwendet und die Daten an Oregon bereitstellt.

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

Überwachung AWS Ground Station

Überwachung ist wichtig, um die Zuverlässigkeit, Verfügbarkeit und Performance von AWS Ground Station aufrechtzuerhalten. AWS bietet die folgenden Überwachungstools, um zu beobachten AWS Ground Station, zu melden, wenn etwas nicht stimmt, und gegebenenfalls automatische Maßnahmen zu ergreifen.

- Amazon CloudWatch Events bietet einen Stream von Systemereignissen, die Änderungen an AWS Ressourcen beschreiben, nahezu in Echtzeit. CloudWatch Events ermöglicht automatisiertes ereignisgesteuertes Rechnen, da Sie Regeln schreiben können, die auf bestimmte Ereignisse achten und automatisierte Aktionen in anderen AWS Diensten auslösen können, wenn diese Ereignisse eintreten. Weitere Informationen zu Amazon CloudWatch Events finden Sie im Amazon CloudWatch Events-Benutzerhandbuch.
- AWS EventBridge Events bietet einen Stream von Systemereignissen, die Änderungen an AWS Ressourcen beschreiben, nahezu in Echtzeit. EventBridge Events ermöglicht automatisiertes ereignisgesteuertes Computing, da Sie Regeln schreiben können, die auf bestimmte Ereignisse achten und automatisierte Aktionen in anderen AWS Services auslösen können, wenn diese Ereignisse eintreten. Weitere Informationen zu EventBridge Veranstaltungen finden Sie im Amazon EventBridge Events-Benutzerhandbuch.
- AWS CloudTrailerfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS Kontos getätigt wurden, und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket. Sie können die Benutzer und Konten, die AWS aufgerufen haben, identifizieren, sowie die Quell-IP-Adresse, von der diese Aufrufe stammen, und den Zeitpunkt der Aufrufe ermitteln. Weitere Informationen dazu AWS CloudTrail finden Sie im AWS CloudTrail Benutzerhandbuch.
- Amazon CloudWatch Metrics erfasst bei der Nutzung Kennzahlen für Ihre geplanten Kontakte AWS Ground Station. CloudWatch Mit Metrics können Sie Daten auf der Grundlage Ihres Kanals, Ihrer Polarisation und Ihrer Satelliten-ID analysieren, um die Signalstärke und Fehler bei Ihren Kontakten zu ermitteln. Weitere Informationen finden Sie unter Amazon CloudWatch Metrics verwenden.
- AWS Benutzerbenachrichtigungen kann verwendet werden, um Lieferkanäle einzurichten, um über AWS Ground Station Ereignisse informiert zu werden. Sie erhalten eine Benachrichtigung, wenn ein Ereignis einer von Ihnen angegebenen Regel entspricht. Sie können Benachrichtigungen für Ereignisse über mehrere Kanäle erhalten, einschließlich E-Mail-, AWS Chatbot-Chat- oder AWS Console Mobile Application-Push-Benachrichtigungen. Sie können Benachrichtigungen auch im Konsolen-Benachrichtigungscenter anzeigen. Benutzerbenachrichtigungen unterstützt

die Aggregation, wodurch die Anzahl der Benachrichtigungen, die Sie bei bestimmten Ereignissen erhalten, verringert werden kann.

Verwenden Sie die folgenden Themen zur Überwachung von AWS Ground Station.

Themen

Automatisieren AWS Ground Station mit Ereignissen

> **Note**
>
> In diesem Dokument wird durchgängig der Begriff „Ereignis“ verwendet. CloudWatch Bei Ereignissen und EventBridge handelt es sich um denselben zugrunde liegenden Dienst und dieselbe API. Regeln für den Abgleich eingehender Ereignisse und deren Weiterleitung an Ziele zur Verarbeitung können mit beiden Diensten erstellt werden.

Ereignisse ermöglichen es Ihnen, Ihre AWS Dienste zu automatisieren und automatisch auf Systemereignisse wie Probleme mit der Anwendungsverfügbarkeit oder Ressourcenänderungen zu reagieren. Ereignisse aus AWS Diensten werden nahezu in Echtzeit übermittelt. Sie können einfache Regeln schreiben, um anzugeben, welche Ereignisse für Sie interessant sind und welche automatisierten Aktionen durchgeführt werden sollen, wenn sich für ein Ereignis eine Übereinstimmung mit einer Regel ergibt. Die folgenden Aktionen können beispielsweise automatisch ausgelöst werden:

- Eine AWS Lambda Funktion aufrufen
- Aufrufen eines Amazon EC2 Run Command
- Weiterleiten des Ereignisses an Amazon Kinesis Data Streams
- Aktivierung einer AWS Step Functions Zustandsmaschine
- Ein Amazon SNS SNS-Thema oder eine Warteschlange benachrichtigen AWS SMS

Einige Beispiele für die Verwendung von Ereignissen mit AWS Ground Station sind:

- Aufrufen einer Lambda-Funktion, um das Starten und Stoppen von Amazon EC2 EC2-Instances basierend auf dem Ereignisstatus zu automatisieren.
- Veröffentlichung in einem Amazon SNS SNS-Thema, wenn sich der Status eines Kontakts ändert. Diese Themen können so eingerichtet werden, dass E-Mail-Benachrichtigungen am Anfang oder Ende von Kontakten gesendet werden.

Weitere Informationen finden Sie im Amazon CloudWatch Events-Benutzerhandbuch oder im Amazon EventBridge Events-Benutzerhandbuch.

Beispielereignisse

> **Note**
>
> Alle von AWS Ground Station generierten Ereignisse haben „aws.groundstation“ als Wert für „source“.

Änderung des Ground Station-Kontaktzustands

Wenn Sie eine bestimmte Aktion ausführen möchten, sobald ein bevorstehender Kontakt den Zustand ändert, können Sie eine -Regel einrichten, um diese Aktion zu automatisieren. Dies ist hilfreich, wenn Sie Benachrichtigungen über die Zustandsänderungen Ihres Kontakts erhalten möchten. Wenn Sie ändern möchten, wann Sie diese Ereignisse erhalten, können Sie die Einstellungen und in Ihrem Missionsprofil ändern. contactPrePassDurationSecondscontactPostPassDurationSeconds Die Ereignisse werden in die Region gesendet, in der der Kontakt geplant wurde.

Nachstehend finden Sie ein Beispiel.

```
{
    "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"
}
```

Die möglichen Werte für `contactStatus` sind in definiertthe section called “Kontaktstatus der Ground Station”.

Zustandsänderung der Ground Station-Datenfluss-Endpunktgruppen

Wenn Sie eine Aktion ausführen möchten, sobald Ihre Datenflussendpunktgruppe zum Empfang von Daten verwendet wird, können Sie eine -Regel einrichten, um diese Aktion zu automatisieren. Auf diese Weise können Sie verschiedene Aktionen als Reaktion auf die Zustandsänderungen des Datenflussendpunktgruppen-Status ausführen. Wenn Sie ändern möchten, wann Sie diese Ereignisse empfangen, verwenden Sie eine Datenfluss-Endpunktgruppe mit einem anderen contactPrePassDurationSecondsund. contactPostPassDurationSeconds Dieses Ereignis wird in die Region der Datenfluss-Endpunktgruppe gesendet.

Nachstehend finden Sie ein Beispiel.

```
{
    "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"
}
```

Mögliche Zustände für `dataflowEndpointGroupState` umfassen `PREPASS`, `PASS`, `POSTPASS` und `COMPLETED`.

Änderung des Zustands der Ground Station Ephemeris

Wenn Sie eine Aktion ausführen möchten, wenn sich der Status einer Ephemeride ändert, können Sie eine Regel einrichten, um diese Aktion zu automatisieren. Auf diese Weise können Sie verschiedene Aktionen ausführen, wenn sich der Status einer Ephemeride ändert. Sie können beispielsweise eine Aktion ausführen, wenn die Validierung einer Ephemeride abgeschlossen ist, und das ist jetzt der Fall. `ENABLED` Die Benachrichtigung über dieses Ereignis wird an die Region gesendet, in die die Ephemeride hochgeladen wurde.

Nachstehend finden Sie ein Beispiel.

```
    {
    "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"
    }
    }
```

Zu den möglichen Zuständen `ephemerisStatus` gehören`ENABLED`,,`VALIDATING`,`INVALID`, `ERROR` `DISABLED` `EXPIRED`

AWS Ground Station API-Aufrufe protokollieren mit AWS CloudTrail

AWS Ground Station ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Dienst in ausgeführt wurden AWS Ground Station. CloudTrail erfasst alle API-Aufrufe AWS Ground Station als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der AWS Ground Station Konsole und Codeaufrufen für die AWS Ground Station API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für AWS Ground Station. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen. Anhand der von gesammelten Informationen können Sie die Anfrage ermitteln CloudTrail, an die die Anfrage gestellt wurde AWS Ground Station, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details.

Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrail Benutzerhandbuch.

AWS Ground Station Informationen in CloudTrail

CloudTrail ist in Ihrem AWS Konto aktiviert, wenn Sie das Konto erstellen. Wenn eine Aktivität in stattfindet AWS Ground Station, wird diese Aktivität zusammen mit anderen CloudTrail AWS Serviceereignissen im Ereignisverlauf in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem AWS Konto ansehen, suchen und herunterladen. Weitere Informationen finden Sie unter Ereignisse mit CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS Konto, einschließlich der Ereignisse für AWS Ground Station, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung

von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Pfad in der Konsole anlegen, gilt dieser für alle AWS-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails
- CloudTrail Unterstützte Dienste und Integrationen
- Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

Alle AWS Ground Station Aktionen werden von der AWS Ground Station API-Referenz protokolliert CloudTrail und sind in dieser dokumentiert. Beispielsweise generieren Aufrufe von `CancelContact` und `ListConfigs` Aktionen Einträge in den CloudTrail Protokolldateien. `ReserveContact`

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management (IAM-) Benutzeranmeldedaten gestellt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.

Weitere Informationen finden Sie unter dem CloudTrail UserIdentity-Element.

Grundlegendes zu Einträgen AWS Ground Station in Protokolldateien

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `ReserveContact` Aktion demonstriert.

Beispiel: 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"
}
```

Metriken mit Amazon CloudWatch

Erfasst während eines Kontakts AWS Ground Station automatisch Daten und sendet sie CloudWatch zur Analyse an. Ihre Daten können in einer Grafik oder als Quellcode in der CloudWatch Amazon-Konsole angezeigt werden. Weitere Informationen zum Zugriff und zu CloudWatch Metriken finden Sie unter Amazon CloudWatch Metrics verwenden.

AWS Ground Station Metriken und Dimensionen

Welche Metriken sind verfügbar?

Die folgenden Metriken sind bei erhältlich AWS Ground Station.

Metrik	Beschreibung
`AzimuthAngle`	Der Azimutwinkel der Antenne. Der wahre Norden ist 0 Grad und der Osten ist 90 Grad. Einheiten: Grad
`BitErrorRate`	Die Fehlerrate bei Bits bei einer bestimmten Anzahl von Bitübertragungen. Bitfehler werden durch Rauschen, Verzerrungen oder Störungen verursacht Einheiten: Bitfehler pro Zeiteinheit
`BlockErrorRate`	Die Fehlerquote von Blöcken in einer bestimmten Anzahl empfangener Blöcke. Blockfehler werden durch Störungen verursacht. Einheiten: Fehlerhafte Blöcke/Gesamtzahl der Blöcke

Metrik	Beschreibung
`CarrierFrequencyRecovery_Cn0`	Verhältnis zwischen Träger und Rauschdichte pro Bandbreiteneinheit. Einheiten: Dezibel-Hertz (dB-Hz)
`CarrierFrequencyRecovery_Locked`	Wird auf 1 gesetzt, wenn die Trägerfrequenz-Wiederherstellungsschleife des Demodulators gesperrt ist, und auf 0, wenn sie entsperrt ist. Einheiten: ohne Einheit
`CarrierFrequencyRecovery_OffsetFrequency_Hz`	Der Offset zwischen der geschätzten Signalmitte und der idealen Mittenfrequenz. Dies wird durch die Dopplerverschiebung und den Offset des Lokaloszillators zwischen Raumfahrzeug und Antennensystem verursacht. Einheiten: Hertz (Hz)
`ElevationAngle`	Der Höhenwinkel der Antenne. Der Horizont ist 0 Grad und der Zenit ist 90 Grad. Einheiten: Grad
`Es/N0`	Das Verhältnis von Energie pro Symbol zur spektralen Leistungsdichte des Rauschens. Einheiten: Dezibel (dB)
`ReceivedPower`	Die gemessene Signalstärke im Demodulator/Decoder. Einheiten: Dezibel im Verhältnis zu Milliwatt (dBm)
`SymbolTimingRecovery_ErrorVectorMagnitude`	Die Größe des Fehlervektors zwischen empfangenen Symbolen und idealen Konstellationspunkten. Einheiten: Prozent

Metrik	Beschreibung
`SymbolTimingRecovery_Locked`	Wird auf 1 gesetzt, wenn die Zeitwiederherstell ungsschleife des Demodulatorsymbols gesperrt ist, und auf 0, wenn sie entsperrt ist Einheiten: ohne Einheit
`SymbolTimingRecovery_Offset SymbolRate`	Der Offset zwischen der geschätzten Symbolrate und der idealen Signalsymbolrate. Dies wird durch die Dopplerverschiebung und den Offset des Lokaloszi llators zwischen Raumfahrzeug und Antennensystem verursacht. Einheiten: Symbole/Sekunde

Wofür werden Dimensionen verwendet? AWS Ground Station

Sie können AWS Ground Station Daten anhand der folgenden Dimensionen filtern.

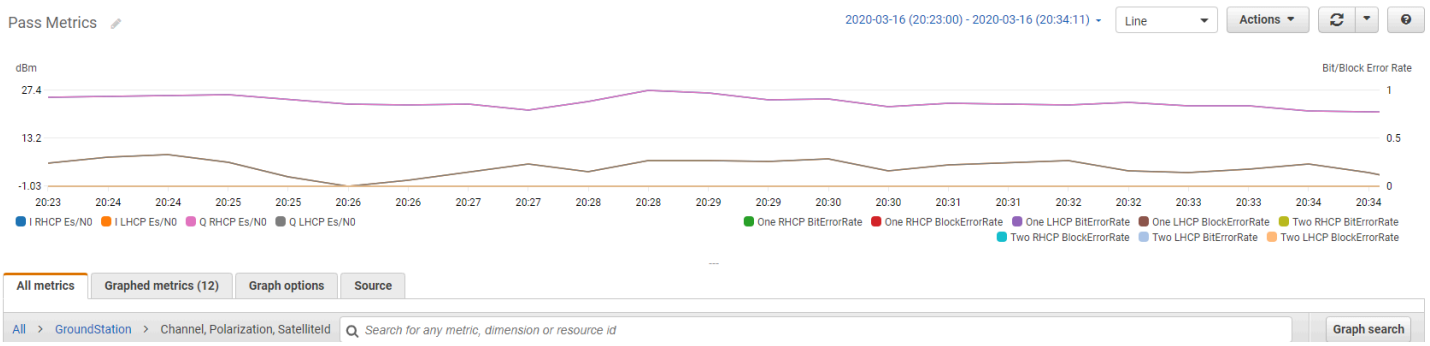
Dimension	Beschreibung
`Channel`	Die Kanäle für jeden Kontakt umfassen One, Two, I (In-Phase) und Q (Quadrature).
`Polarization`	Die Polarisierung für jeden Kontakt umfasst LHCP (Left Hand Circular Polarized) oder RHCP (Right Hand Circular Polarized).
`SatelliteId`	Die Satelliten-ID enthält den ARN des Satelliten für Ihre Kontakte.

Anzeigen von -Metriken

Wenn Sie grafische Metriken anzeigen, ist es wichtig zu beachten, dass das Aggregationsfenster bestimmt, wie Ihre Metriken angezeigt werden. Jede Metrik in einem Kontakt kann 3 Stunden lang als Daten pro Sekunde angezeigt werden, nachdem die Daten empfangen wurden. Nach Ablauf

dieses Zeitraums von 3 Stunden werden Ihre Daten von CloudWatch Metrics als Daten pro Minute aggregiert. Wenn Sie Ihre Messwerte anhand einer Messung von Daten pro Sekunde anzeigen möchten, wird empfohlen, Ihre Daten innerhalb von 3 Stunden nach dem Empfang der Daten anzuzeigen oder sie außerhalb von Metrics beizubehalten. CloudWatch

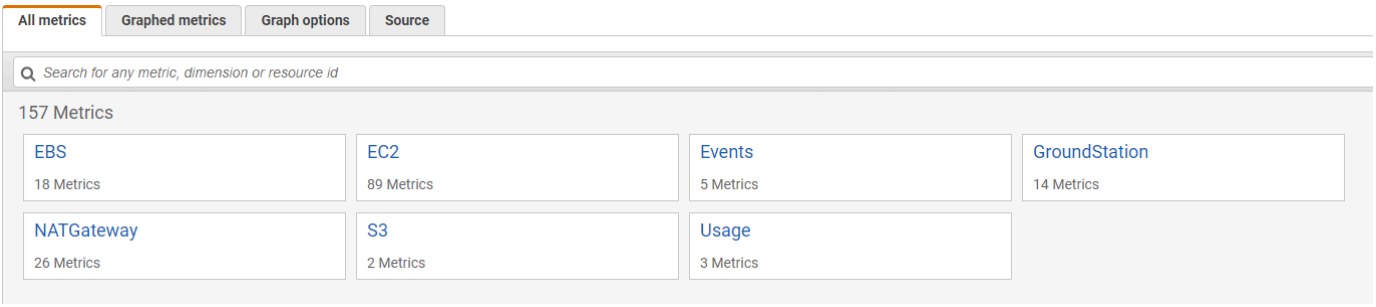
Darüber hinaus enthalten alle innerhalb der ersten 60 Sekunden erfassten Daten nicht genügend Informationen, um aussagekräftige Metriken zu erzeugen, und werden wahrscheinlich nicht angezeigt. Um aussagekräftige Metriken anzuzeigen, empfiehlt es sich, Ihre Daten nach 60 Sekunden anzuzeigen.



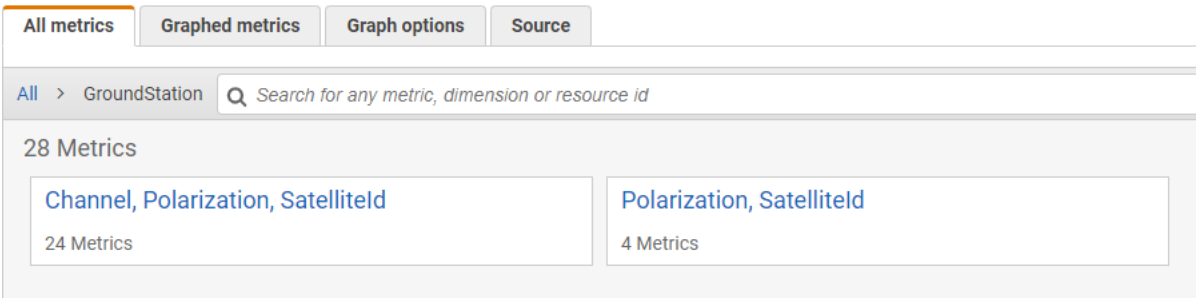
Weitere Informationen zur grafischen Darstellung von Metriken finden Sie unter AWS Ground Station Metriken grafisch darstellen. CloudWatch

So zeigen Sie Metriken mithilfe der -Konsole an

1. Öffnen Sie die CloudWatch -Konsole.
2. Wählen Sie im Navigationsbereich Metriken aus.
3. Wählen Sie den GroundStation-Namespace.



4. Wählen Sie die gewünschten metrischen Dimensionen aus (z. B. Kanal, Polarisation,. SatelliteId



5. Die Registerkarte All metrics zeigt alle Metriken für diese Dimension im Namespace an. Sie haben die folgenden Möglichkeiten:

   a. Um die Tabelle sortieren, verwenden Sie die Spaltenüberschrift.

   b. Um eine Metrik grafisch darzustellen, aktivieren Sie das der Metrik zugeordnete Kontrollkästchen. Um alle Metriken auszuwählen, aktivieren Sie das Kontrollkästchen in der Kopfzeile der Tabelle.

   c. Um nach Ressource zu filtern, müssen Sie zunächst die Ressourcen-ID und dann die Option Zu Suche hinzufügen auswählen.

   d. Um nach Metrik zu filtern, müssen Sie den Metriknamen und anschließend Add to search (Zur Suche hinzufügen) auswählen.

Um Metriken anzuzeigen, verwenden Sie AWS CLI

1. Stellen Sie sicher, dass AWS CLI das installiert ist. Informationen zur Installation finden Sie AWS CLI unter Installation der AWS-CLI.
2. Erstellen Sie eine JSON-Datei für die CloudWatch Agentenkonfiguration. Anweisungen zum Erstellen einer CloudWatch Agenten-Konfigurationsdatei finden Sie unter CloudWatch Agenten-Konfigurationsdatei erstellen.
3. Listet die verfügbaren CloudWatch Metriken auf, indem Sie den Befehl ausführen`aws cloudwatch list-metrics`.
4. Ändern Sie die JSON-Datei, die Sie in Schritt 2 erstellt haben, sodass sie mit der `SatellitID` aus Ihren Metriken übereinstimmt.

> **Note**
>
> Reduzieren Sie das `Period` Feld nicht auf einen Wert unter 60. AWS Ground Station veröffentlicht alle 60 Sekunden Metriken und es werden keine Metriken zurückgegeben, wenn der Wert reduziert wird.

5. Führen Sie die Ausführung `aws cloudwatch get-metric-data` mit den Zeiträumen Ihrer Pässe und Ihrer JSON-Datei für die CloudWatch Agentenkonfiguration aus. Nachstehend finden Sie ein Beispiel.

```
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
```

Metriken werden mit Zeitstempel von Ihrem Kontakt zur Verfügung gestellt. Im Folgenden finden Sie ein Beispiel für die Ausgabe von AWS Ground Station Metriken.

```
{
      “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”: []
}
```

Fehlerbehebung

Die folgende Dokumentation kann Ihnen bei der Behebung von Problemen helfen, die dazu führen können, dass ein AWS Ground Station Kontakt nicht erfolgreich abgeschlossen werden kann.

Themen

Problembehandlung bei Kontakten, die Daten an Amazon EC2 liefern

Wenn Sie einen AWS Ground Station Kontakt nicht erfolgreich abschließen können, müssen Sie überprüfen, ob Ihre Amazon EC2 EC2-Instance läuft, ob Data Defender läuft und ob Ihr Data Defender-Stream ordnungsgemäß konfiguriert ist.

Voraussetzung

Bei den folgenden Verfahren wird davon ausgegangen, dass eine Amazon EC2 EC2-Instance bereits eingerichtet ist. Informationen zum Einrichten einer Amazon EC2 EC2-Instance finden Sie unter Erste Schritte. AWS Ground Station

Schritt 1: Überprüfen, ob Ihre EC2-Instance ausgeführt wird

1. Suchen Sie die Amazon EC2 EC2-Instance, die für den Kontakt verwendet wurde, für den Sie eine Fehlerbehebung durchführen. Gehen Sie dazu wie folgt vor:

    a. Wählen Sie in Ihrem CloudFormationDashboard den Stack aus, der Ihre Amazon EC2 EC2-Instance enthält.

    b. Wählen Sie die Registerkarte Ressourcen und suchen Sie Ihre Amazon EC2 EC2-Instance in der Spalte Logische ID. Stellen Sie sicher, dass die Instance in der Spalte Status erstellt wurde.

    c. Wählen Sie in der Spalte Physikalische ID den Link für Ihre Amazon EC2 EC2-Instance aus. Dadurch gelangen Sie zur Amazon EC2-Managementkonsole.

2. Stellen Sie in der Amazon EC2-Managementkonsole sicher, dass Ihr Amazon EC2 EC2-Instance-Status läuft.
3. Wenn Ihre Instance ausgeführt wird, fahren Sie mit dem nächsten Schritt fort. Wenn Ihre Instance nicht ausgeführt wird, starten Sie die Instance mit dem folgenden Schritt.

    - Wenn Ihre Amazon EC2 EC2-Instance ausgewählt ist, wählen Sie Actions > Instance State > Start.

Schritt 2: Ermitteln Sie den Typ der verwendeten Dataflow-Anwendung

Wenn Sie den AWS Ground Station Agenten für die Datenübermittlung verwenden, leiten Sie bitte zum Abschnitt Troubleshooting AWS Ground Station Agent weiter.

Andernfalls fahren Sie fort, wenn Sie die Data Defender-Anwendung (DDX) verwenden. the section called “Schritt 3: Stellen Sie sicher, dass Data Defender läuft”

Schritt 3: Stellen Sie sicher, dass Data Defender läuft

Um den Status von Data Defender zu überprüfen, müssen Sie eine Verbindung zu Ihrer Instance in Amazon EC2 herstellen. Weitere Informationen zum Herstellen einer Verbindung mit Ihrer Instance finden Sie unter Verbinden mit Ihrer Linux-Instanz.

Das folgende Verfahren enthält Schritte zur Problembehandlung mit Befehlen in einem SSH-Client.

1. Öffnen Sie ein Terminal oder eine Befehlszeile und stellen Sie mithilfe von SSH eine Verbindung zu Ihrer Amazon EC2 EC2-Instance her. Leiten Sie Port 80 des Remote-Hosts weiter, um die Data Defender Web UI anzuzeigen. Die folgenden Befehle zeigen, wie SSH verwendet wird, um über eine Bastion mit aktivierter Portweiterleitung eine Verbindung zu einer Amazon EC2 EC2-Instance herzustellen.

    > **Note**
    >
    > Sie müssen <SSH KEY><BASTION HOST>, und durch <HOST>Ihren spezifischen SSH-Schlüssel, Ihren Bastion-Hostnamen und Ihren Amazon EC2 EC2-Instance-Hostnamen ersetzen.

    Für 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>
```

Für 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. Überprüfen Sie zudem, dass Data Defender (auch DDX genannt) ausgeführt wird, indem Sie überprüfen, ob ein Prozess namens „ddx“ in der Ausgabe ausgeführt wird (Grepping). Der Befehl zum Grepping (Prüfen) eines laufenden Prozesses und eine erfolgreiche Beispielausgabe finden Sie unten.

```
[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
```

Wenn Data Defender ausgeführt wird, fahren Sie mit the section called “Schritt 4: Stellen Sie sicher, dass Ihr Data Defender-Stream konfiguriert ist” fort. Fahren Sie andernfalls mit dem nächsten Schritt fort.

3. Starten Sie Data Defender mit dem unten gezeigten Befehl.

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

Wenn Data Defender nach der Verwendung des Befehls ausgeführt wird, fahren Sie mit the section called “Schritt 4: Stellen Sie sicher, dass Ihr Data Defender-Stream konfiguriert ist” fort. Fahren Sie andernfalls mit dem nächsten Schritt fort.

4. Überprüfen Sie die folgenden Dateien mit den folgenden Befehlen, um festzustellen, ob Fehler bei der Installation und Konfiguration von Data Defender aufgetreten sind.

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

> **Note**
>
> Ein häufiges Problem, das bei der Überprüfung dieser Dateien festgestellt wurde, ist, dass die Amazon VPC, in der Ihre Amazon EC2 EC2-Instance ausgeführt wird, keinen Zugriff auf Amazon S3 hat, um die Installationsdateien herunterzuladen. Wenn Sie in Ihren Protokollen feststellen, dass dies das Problem ist, überprüfen Sie die Amazon VPC- und Sicherheitsgruppeneinstellungen Ihrer EC2-Instance, um sicherzustellen, dass sie den Zugriff auf Amazon S3 nicht blockieren.

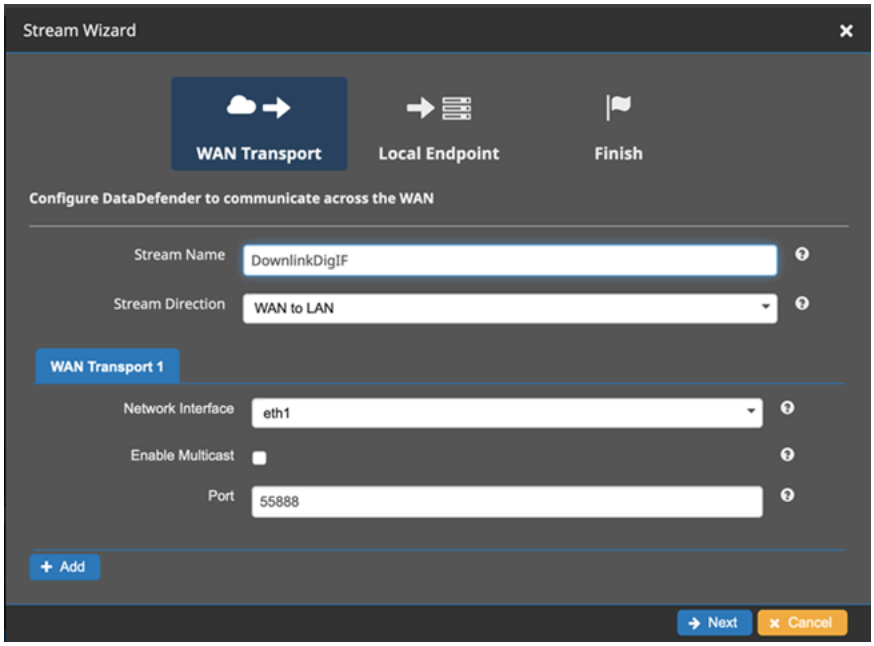
Wenn Data Defender läuft, nachdem Sie Ihre Amazon VPC-Einstellungen überprüft haben, fahren Sie fortthe section called “Schritt 4: Stellen Sie sicher, dass Ihr Data Defender-Stream konfiguriert ist”. Wenn das Problem weiterhin besteht, wenden Sie sich an den AWS Support und senden Sie Ihre Protokolldateien mit einer Beschreibung Ihres Problems.

Schritt 4: Stellen Sie sicher, dass Ihr Data Defender-Stream konfiguriert ist

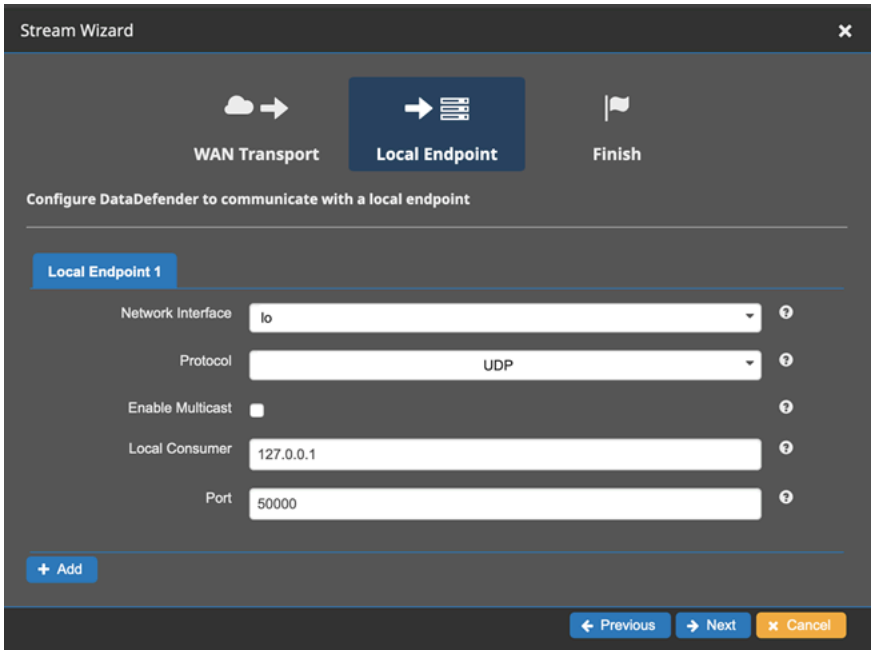
1. Greifen Sie in einem Webbrowser auf Ihre DDX-Web-Benutzeroberfläche zu, indem Sie die folgende Adresse in die Adressleiste eingeben: localhost:8080 Drücken Sie anschließend die Eingabetaste.
2. Wählen Sie im DataDefenderDashboard die Option Gehe zu Details aus.
3. Wählen Sie Ihren Stream aus der Liste der Streams aus und wählen Sie Edit Stream (Stream bearbeiten) aus.
4. Führen Sie im Dialogfeld Stream-Assistent die folgenden Schritte aus:

    a. Stellen Sie im Bereich WAN-Transport sicher, dass WAN zu LAN als Stream-Richtung ausgewählt ist.

    b. Stellen Sie im Feld Port sicher, dass der WAN-Port, den Sie für Ihre Datenfluss-Endpunktgruppe ausgewählt haben, vorhanden ist. Standardmäßig ist dies der Port 55888. Wählen Sie anschließend Weiter.



c. Stellen Sie im Bereich Lokaler Endpunkt sicher, dass im Feld Port ein gültiger Port vorhanden ist. Standardmäßig ist dies der Port 50000. Dies ist der Port, an dem Sie Ihre Daten erhalten, nachdem Data Defender sie vom AWS Ground Station Dienst erhalten hat. Wählen Sie anschließend Weiter.



d. Wählen Sie im verbleibenden Menü die Option Finish (Fertig) aus, wenn Sie Werte geändert haben. Andernfalls können Sie das Menü Stream Wizard (Stream-Assistent) durch Abbrechen verlassen.

Sie haben jetzt sichergestellt, dass Ihre Amazon EC2 EC2-Instance und Data Defender ordnungsgemäß ausgeführt und für den Empfang von AWS Ground Station Daten konfiguriert sind. Wenn weiterhin Probleme auftreten, wenden Sie sich an den AWS Support.

Kontaktstatus der Ground Station

Der Status eines AWS Ground Station Kontakts gibt Aufschluss darüber, was mit diesem Kontakt zu einem bestimmten Zeitpunkt passiert.

Kontaktstatus

Im Folgenden finden Sie eine Liste der Status, die ein Kontakt haben kann:

- VERFÜGBAR — Der Kontakt kann reserviert werden.
- TERMINPLANUNG — Der Kontakt ist gerade dabei, einen Termin zu vereinbaren.
- GEPLANT — Der Kontakt wurde erfolgreich geplant.
- FAILED_TO_SCHEDULE — Der Kontakt konnte nicht geplant werden.
- PREPASS — Der Kontakt beginnt bald und die Ressourcen werden vorbereitet.
- PASS — Der Kontakt wird gerade ausgeführt und es wird mit dem Satelliten kommuniziert.
- POSTPASS — Die Kommunikation ist abgeschlossen und die verwendeten Ressourcen werden bereinigt.
- ABGESCHLOSSEN — Der Kontakt wurde erfolgreich abgeschlossen.
- FEHLGESCHLAGEN — Der Kontakt ist aufgrund eines Problems mit der Konfiguration der Kundenressourcen fehlgeschlagen.
- AWS_FAILED — Der Kontakt ist aufgrund eines Dienstproblems fehlgeschlagen. AWS Ground Station
- STORNIERUNG — Der Kontakt wird gerade storniert.
- AWS_CANCELLED — Der Kontakt wurde vom Service storniert. AWS Ground Station Die Wartung von Antennen oder Standorten ist ein Beispiel dafür, wann dies passieren könnte.
- STORNIERT — Der Kontakt wurde vom Kunden storniert.

Anleitungen zur Fehlerbehebung

- the section called “Fehlerbehebung bei FEHLGESCHLAGENEN Kontakten”

- the section called “Fehlerbehebung bei FAILED_TO_SCHEDULE-Kontakten”

Fehlerbehebung bei FEHLGESCHLAGENEN Kontakten

Ein Kontakt hat den Terminal-Kontaktstatus FAILED, wenn ein Problem mit der Konfiguration der Kundenressourcen AWS Ground Station festgestellt wird. Nachfolgend finden Sie die häufigsten Anwendungsfälle, die zu FEHLGESCHLAGENEN Kontakten führen können, sowie Schritte zur Problembehebung.

> **Note**
>
> Dieses Handbuch bezieht sich speziell auf den Kontaktstatus FAILED und nicht auf andere Fehlerstatus wie AWS_FAILED, AWS_CANCELLED oder FAILED_TO_SCHEDULE. Weitere Informationen zum Kontaktstatus finden Sie unter the section called “Kontaktstatus der Ground Station”

Anwendungsfälle von Data Defender (DDX) FAILED

Im Folgenden finden Sie eine Liste der häufigsten Anwendungsfälle, die bei DDX-basierten Datenflüssen zu einem Kontaktstatus FAILED führen können:

- Kunden-DDX stellt keine Verbindung her — Die DDX-Verbindung zwischen AWS Ground Station Antenna und Customer Dataflow Endpoint Group für einen oder mehrere Datenflüsse wurde nie hergestellt.
- Kunden-DDX-Verbindungen zu spät — Die DDX-Verbindung zwischen AWS Ground Station Antenne und Customer Dataflow Endpoint Group für einen oder mehrere Datenflüsse wurde nach der Startzeit des Kontakts hergestellt.

Für alle Fälle, in denen DDX-Datenflüsse ausfallen, wird empfohlen, Folgendes zu prüfen:

- Vergewissern Sie sich, dass die Amazon EC2 EC2-Empfängerinstanz vor der Startzeit des Kontakts erfolgreich gestartet wurde.
- Vergewissern Sie sich, dass DDX während des Kontakts betriebsbereit war.

Spezifischere Schritte the section called “Problembehandlung bei Kontakten, die Daten an Amazon EC2 liefern” zur Fehlerbehebung finden Sie im Abschnitt über.

AWS Ground Station Anwendungsfälle von Agent FAILED

Im Folgenden finden Sie eine Liste der häufigsten Anwendungsfälle, die bei agentenbasierten Datenflüssen zu einem Kontaktstatus FEHLGESCHLAGEN führen können:

- Status des Kundenagenten nie gemeldet — Der Agent, der für die Orchestrierung der Datenübermittlung auf der Kundendataflow-Endpunktgruppe für einen oder mehrere Datenflüsse verantwortlich ist, hat dem Kunden den Status nie erfolgreich gemeldet. AWS Ground Station Diese Statusaktualisierung sollte innerhalb weniger Sekunden nach dem Ende des Kontakts erfolgen.
- Der Kundenagent hat zu spät gestartet — Der Agent, der für die Orchestrierung der Datenzustellung auf der Customer Dataflow-Endpunktgruppe für einen oder mehrere Datenflüsse verantwortlich ist, wurde zu spät gestartet, also nach der Startzeit des Kontakts.

Für alle Fälle, in denen der AWS Ground Station Agenten-Datenfluss ausfällt, wird empfohlen, Folgendes zu prüfen:

- Vergewissern Sie sich, dass die Amazon EC2 EC2-Empfängerinstanz vor der Startzeit des Kontakts erfolgreich gestartet wurde.
- Vergewissern Sie sich, dass die Agent-Anwendung beim Start und während des Kontakts aktiv war.
- Vergewissern Sie sich, dass die Agent-Anwendung und die Amazon EC2 EC2-Instance nicht innerhalb von 15 Sekunden nach Kontaktende heruntergefahren wurden. Dadurch hat der Agent ausreichend Zeit, um dem Agenten den Status zu AWS Ground Station melden.

Spezifischere Schritte zur Fehlerbehebung finden Sie im Abschnitt über. the section called “Problembehandlung bei Kontakten, die Daten an Amazon EC2 liefern”

Fehlerbehebung bei FAILED_TO_SCHEDULE-Kontakten

Ein Kontakt führt FAILED_TO_SCHEDULE durch, wenn ein Problem mit der Konfiguration der Kundenressourcen oder innerhalb des internen Systems AWS Ground Station festgestellt wird. Ein Kontakt, der im Status FAILED_TO_SCHEDULE endet, bietet optional einen zusätzlichen Kontext. `errorMessage` Hinweise zur Beschreibung von Kontakten finden Sie unter. the section called “Beschreiben Sie einen Kontakt mit AWS CLI”

Nachfolgend finden Sie die häufigsten Anwendungsfälle, die zu FAILED_TO_SCHEDULE-Kontakten führen können, sowie Schritte zur Problembehebung.

> **Note**
>
> Dieses Handbuch bezieht sich speziell auf den Kontaktstatus FAILED_TO_SCHEDULE und ist nicht für andere Fehlerstatus wie AWS_FAILED, AWS_CANCELLED oder FAILED vorgesehen. Weitere Informationen zum Kontaktstatus finden Sie unter the section called “Kontaktstatus der Ground Station”

Die in Ihrer Antenna Downlink Demod Decode Config angegebenen Einstellungen werden nicht unterstützt

Das Missionsprofil, das zur Planung dieses Kontakts verwendet wurde, hatte eine antenna-downlink-demod-decode ungültige Konfiguration.

Zuvor vorhandene AntennaDownlinkDemodDecode Konfiguration

- Wenn Ihre antenna-downlink-demod-decode Konfigurationen kürzlich geändert wurden, kehren Sie zu einer zuvor funktionierenden Version zurück, bevor Sie versuchen, einen Zeitplan zu erstellen.
- Falls es sich dabei um eine absichtliche Änderung an einer bestehenden Konfiguration handelte oder um eine bereits bestehende Konfiguration, die nicht mehr erfolgreich geplant wird, folgen Sie dem nächsten Schritt, um eine neue AntennaDownlinkDemodDecode Konfiguration zu integrieren.

Neu erstellte Konfiguration AntennaDownlinkDemodDecode

Wenden Sie sich AWS Ground Station direkt an, um Ihre neue Konfiguration zu integrieren. Erstellen Sie einen Fall mit dem AWS-Support, einschließlich des Falls`contactId`, der mit dem Status FAILED_TO_SCHEDULE endete

Allgemeine Fehlerbehebungsschritte

Wenn die vorherigen Schritte zur Fehlerbehebung Ihr Problem nicht gelöst haben:

- Versuchen Sie erneut, den Kontakt zu planen, oder vereinbaren Sie einen anderen Kontakt mit demselben Missionsprofil. Siehe the section called “Reservieren Sie einen Kontakt mit AWS CLI”.

- Wenn Sie weiterhin den Status FAILED_TO_SCHEDULE für dieses Missionsprofil erhalten, wenden Sie sich an den AWS-Support

Sicherheit in AWS Ground Station

Die Sicherheit in der Cloud hat bei AWS höchste Priorität. Als AWS-Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die eingerichtet wurde, um die Anforderungen der anspruchsvollsten Organisationen in puncto Sicherheit zu erfüllen. AWS bietet sicherheitsspezifische Tools und Funktionen, mit denen Sie Ihre Sicherheitsziele erreichen können. Zu diesen Tools und Funktionen gehören Netzwerksicherheit, Konfigurationsverwaltung, Zugriffskontrolle und Datensicherheit.

Bei der Verwendung empfehlen wir IhnenAWS Ground Station, die branchenweit bewährten Methoden zu befolgen und end-to-end Verschlüsselung zu implementieren. AWS stellt APIs zur Integration von Verschlüsselung und Datenschutz bereit. Weitere Informationen zur AWS-Sicherheit finden Sie im Whitepaper Introduction to AWS Security.

In den folgenden Themen wird beschrieben, wie Ihre -Ressourcen geschützt werden.

Themen

Identitäts- und Zugriffsverwaltung für AWS Ground Station

AWS Identity and Access Management (IAM) ist ein AWS-Service, mit dem Administratoren den Zugriff auf AWS-Ressourcen sicher steuern können. IAM-Administratoren steuern, wer authentifiziert (angemeldet) und autorisiert (Berechtigungen besitzt) ist, um AWS Ground Station Ressourcen zu nutzen. IAM ist ein AWS-Service, den Sie ohne zusätzliche Kosten verwenden können.

Themen

- Fehlerbehebung für AWS Ground Station-Identität und -Zugriff

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, unterscheidet sich je nach Ihrer Arbeit in AWS Ground Station.

Service user (Service-Benutzer) – Wenn Sie den AWS Ground Station-Service zur Ausführung von Aufgaben verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen bereit, die Sie benötigen. Wenn Sie für Ihre Arbeit weitere AWS Ground Station-Funktionen ausführen, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Funktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Unter Fehlerbehebung für AWS Ground Station-Identität und -Zugriff finden Sie nützliche Informationen für den Fall, dass Sie keinen Zugriff auf eine Funktion in AWS Ground Station haben.

Service administrator (Service-Administrator) – Wenn Sie in Ihrem Unternehmen für AWS Ground Station-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollständigen Zugriff auf AWS Ground Station. Es ist Ihre Aufgabe, zu bestimmen, auf welche AWS Ground Station-Funktionen und Ressourcen Ihre Service-Benutzer zugreifen sollen. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen dazu, wie Ihr Unternehmen IAM mit AWS Ground Station verwenden kann, finden Sie unter Featuresweise von AWS Ground Station mit IAM.

IAM-Administrator – Wenn Sie als IAM-Administrator fungieren, sollten Sie Einzelheiten dazu kennen, wie Sie Richtlinien zur Verwaltung des Zugriffs auf AWS Ground Station verfassen können. Beispiele für identitätsbasierte AWS Ground Station-Richtlinien, die Sie in IAM verwenden können, finden Sie unter Beispiele für identitätsbasierte Richtlinien für AWS Ground Station.

Authentifizierung mit Identitäten

Authentifizierung ist die Art, wie Sie sich mit Ihren Anmeldeinformationen bei AWS anmelden. Die Authentifizierung (Anmeldung bei AWS) muss als Root-Benutzer des AWS-Kontos, als IAM-Benutzer oder durch Übernahme einer IAM-Rolle erfolgen.

Sie können sich bei AWS als Verbundidentität mit Anmeldeinformationen anmelden, die über eine Identitätsquelle bereitgestellt werden. Benutzer von AWS IAM Identity Center. (IAM Identity Center), die Single-Sign-on-Authentifizierung Ihres Unternehmens und Anmeldeinformationen für Google oder

Facebook sind Beispiele für Verbundidentitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie auf AWS mithilfe des Verbunds zugreifen, übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich bei der AWS Management Console oder beim AWS-Zugriffsportal anmelden. Weitere Informationen zum Anmelden bei AWS finden Sie unter So melden Sie sich bei Ihrem AWS-Konto an im Benutzerhandbuch von AWS-Anmeldung.

Bei programmgesteuerten Zugriff auf AWS bietet AWS ein Software Development Kit (SDK) und eine Command Line Interface (CLI, Befehlszeilenschnittstelle) zum kryptographischen Signieren Ihrer Anforderungen mit Ihren Anmeldeinformationen. Wenn Sie keine AWS-Tools verwenden, müssen Sie Anforderungen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode zum eigenen Signieren von Anforderungen finden Sie unter Signieren von AWS-API-Anforderungen im IAM-Benutzerhandbuch.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. AWS empfiehlt beispielsweise die Verwendung von Multi-Faktor Authentifizierung (MFA), um die Sicherheit Ihres Kontos zu verbessern. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center-Benutzerhandbuch und Verwenden der Multi-Faktor-Authentifizierung (MFA) in AWS im IAM-Benutzerhandbuch.

AWS-Konto-Root-Benutzer

Wenn Sie ein AWS-Konto neu erstellen, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services und Ressourcen des Kontos hat. Diese Identität wird als AWS-Konto-Root-Benutzer bezeichnet. Für den Zugriff auf den Root-Benutzer müssen Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, die zur Erstellung des Kontos verwendet wurden. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Verbundidentität

Als bewährte Methode empfiehlt es sich, menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, aufzufordern, den Verbund mit einem Identitätsanbieter zu verwenden, um auf AWS-Services mit temporären Anmeldeinformationen zuzugreifen.

Eine Verbundidentität ist ein Benutzer aus dem Benutzerverzeichnis Ihres Unternehmens, ein Web Identity Provider, AWS Directory Service, das Identity-Center-Verzeichnis oder jeder Benutzer, der mit Anmeldeinformationen, die über eine Identitätsquelle bereitgestellt werden, auf AWS-Services zugreift. Wenn Verbundidentitäten auf AWS-Konten zugreifen, übernehmen sie Rollen und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen im IAM Identity Center erstellen oder Sie können eine Verbindung mit einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und synchronisieren, um sie in allen AWS-Konten und Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center-Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität in Ihrem AWS-Konto mit bestimmten Berechtigungen für eine einzelne Person oder eine einzelne Anwendung. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Eine IAM-Gruppe ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Erstellen eines IAM-Benutzers (anstatt einer Rolle) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität in Ihrem AWS-Konto mit spezifischen Berechtigungen. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der AWS Management Console übernehmen, indem Sie Rollen wechseln. Sie können eine Rolle annehmen, indem Sie eine AWS CLI oder AWS-API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter Verwenden von IAM-Rollen im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center-Benutzerhandbuch.
- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. In einigen AWS-Services können Sie jedoch eine Richtlinie direkt an eine Ressource anfügen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff – Einige AWS-Services verwenden Features in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon EC2 aus oder speichert Objekte in Amazon S3. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward access sessions (FAS) – Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle zum Ausführen von Aktionen in AWS verwenden, gelten Sie als Prinzipal. Bei einigen Services

könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen AWS-Service aufruft, in Kombination mit der Anforderung an den AWS-Service, Anforderungen an nachgelagerte Services zu stellen. FAS-Anforderungen werden nur dann gestellt, wenn ein Dienst eine Anforderung erhält, die Interaktionen mit anderen AWS-Services oder Ressourcen erfordert, um abgeschlossen werden zu können. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

- Servicerolle – Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
- Serviceverknüpfte Rolle – Eine serviceverknüpfte Rolle ist ein Typ von Servicerolle, die mit einem AWS-Service verknüpft ist. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem AWS-Konto angezeigt und gehören zum Service. Ein IAM-Administrator kann die Berechtigungen für serviceverbundene Rollen anzeigen, aber nicht bearbeiten.

- Anwendungen in Amazon EC2 – Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und AWS CLI- oder AWS-API-Anforderungen durchführen. Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Erstellen Sie ein Instance-Profil, das an die Instance angefügt ist, um eine AWS-Rolle einer EC2-Instance zuzuweisen und die Rolle für sämtliche Anwendungen der Instance bereitzustellen. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter Erstellen einer IAM-Rolle (anstatt eines Benutzers) im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Für die Zugriffssteuerung in AWS erstellen Sie Richtlinien und weisen diese den AWS-Identitäten oder -Ressourcen zu. Eine Richtlinie ist ein Objekt in AWS, das, wenn es einer Identität oder Ressource zugeordnet wird, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn

ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anforderung stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden in AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Administratoren können mithilfe von AWS-JSON-Richtlinien festlegen, wer zum Zugriff auf was berechtigt ist. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Benutzerinformationen über die AWS Management Console, die AWS CLI oder die AWS -API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem AWS-Konto anfügen können. Verwaltete Richtlinien umfassen von AWS verwaltete und von Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer eingebundenen Richtlinie wählen, finden Sie unter Auswahl zwischen verwalteten und eingebundenen Richtlinien im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder AWS-Services umfassen.

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können verwaltete AWS-Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Zugriffssteuerungslisten (ACLs)

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3, AWS WAF und Amazon VPC sind Beispiele für Dienste, die ACLs unterstützen. Weitere Informationen“ zu ACLs finden Sie unter Zugriffskontrollliste (ACL) – Übersicht (Access Control List) im Amazon-Simple-Storage-Service-Entwicklerhandbuch.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger häufig verwendete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Ein ausdrückliches Ablehnen in einer dieser Richtlinien setzt das Zulassen außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.

- Service-Kontrollrichtlinien (SCPs) – SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OE) in AWS Organizations angeben. AWS Organizations ist ein Dienst für die Gruppierung und zentrale Verwaltung mehrerer AWS-Konten Ihres Unternehmens. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. SCPs schränken Berechtigungen für Entitäten in Mitgliedskonten einschließlich des jeweiligen Root-Benutzer des AWS-Kontos ein. Weitere Informationen zu Organisationen und SCPs finden Sie unter Funktionsweise von SCPs im AWS Organizations-Benutzerhandbuch.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen dazu, wie AWS die Zulässigkeit einer Anforderung ermittelt, wenn mehrere Richtlinientypen beteiligt sind, finden Sie unter Logik für die Richtlinienauswertung im IAM-Benutzerhandbuch.

Featuresweise von AWS Ground Station mit IAM

Bevor Sie IAM zum Verwalten des Zugriffs auf AWS Ground Station verwenden, erfahren Sie, welche IAM-Funktionen Sie mit AWS Ground Station verwenden können.

IAM-Funktionen, die Sie mit AWS Ground Station verwenden können

IAM-Feature	AWS Ground Station-Support
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja

IAM-Feature	AWS Ground Station-Support
Richtlinienressourcen	Ja
Richtlinienbedingungsschlüssel (services pezifisch)	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Ja
Temporäre Anmeldeinformationen	Ja
Hauptberechtigungen	Ja
Servicerollen	Nein
Serviceverknüpfte Rollen	Ja

Einen Überblick über das Zusammenwirken von AWS Ground Station und anderen AWS-Services mit den meisten IAM-Featureen finden Sie unter AWS-Services, die mit IAM Featureieren im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien für AWS Ground Station

Unterstützt Richtlinien auf Identitätsbasis.	Ja

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet

ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für AWS Ground Station

Beispiele für identitätsbasierte AWS Ground Station-Richtlinien finden Sie unter Beispiele für identitätsbasierte Richtlinien für AWS Ground Station.

Ressourcenbasierte Richtlinien in AWS Ground Station

Unterstützt ressourcenbasierte Richtlinien	Nein

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder AWS-Services umfassen.

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource in unterschiedlichen AWS-Konten befinden, muss ein IAM-Administrator im vertrauenswürdigen Konto auch der Prinzipalentität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource erteilen. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie unter Wie sich IAM-Rollen von ressourcenbasierten Richtlinien unterscheiden im IAM-Benutzerhandbuch.

Richtlinienaktionen für AWS Ground Station

Unterstützt Richtlinienaktionen	Ja

Administratoren können mithilfe von AWS-JSON-Richtlinien festlegen, wer zum Zugriff auf was berechtigt ist. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie die zugehörige AWS-API-Operation. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keine passende API-Operation gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Eine Liste der AWS Ground Station-Aktionen finden Sie unter Von AWS Ground Station definierte Aktionen in der Service-Autorisierungs-Referenz.

Richtlinienaktionen in AWS Ground Station verwenden das folgende Präfix vor der Aktion:

```
groundstation
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

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

Beispiele für identitätsbasierte AWS Ground Station-Richtlinien finden Sie unter Beispiele für identitätsbasierte Richtlinien für AWS Ground Station.

Richtlinienressourcen für AWS Ground Station

Unterstützt Richtlinienressourcen	Ja

Administratoren können mithilfe von AWS-JSON-Richtlinien festlegen, wer zum Zugriff auf was berechtigt ist. Das bedeutet die Festlegung, welcher Prinzipal Aktionen für welche Ressourcen unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

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

Eine Liste der AWS Ground Station-Ressourcentypen und ihrer ARNs finden Sie unter Von AWS Ground Station definierte Ressourcen in der Service-Autorisierungs-Referenz. Informationen zu den Aktionen, mit denen Sie den ARN einzelner Ressourcen angeben können, finden Sie unter Von AWS Ground Station definierte Aktionen.

Beispiele für identitätsbasierte AWS Ground Station-Richtlinien finden Sie unter Beispiele für identitätsbasierte Richtlinien für AWS Ground Station.

Richtlinien-Bedingungsschlüssel für AWS Ground Station

Unterstützt servicespezifische Richtlinienbedingungsschlüssel	Ja

Administratoren können mithilfe von AWS-JSON-Richtlinien festlegen, wer zum Zugriff auf was berechtigt ist. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte

Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen AND-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, wertet AWS die Bedingung mittels einer logischen OR-Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und servicespezifische Bedingungsschlüssel. Eine Liste aller globalen AWS-Bedingungsschlüssel finden Sie unter Globale AWS-Bedingungskontextschlüssel im IAM-Benutzerhandbuch.

Eine Liste von AWS Ground Station-Bedingungsschlüsseln finden Sie unter Bedingungsschlüssel für AWS Ground Station in der Service-Autorisierungs-Referenz. Informationen dazu, mit welchen Aktionen und Ressourcen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von AWS Ground Station definierte Aktionen.

Beispiele für identitätsbasierte AWS Ground Station-Richtlinien finden Sie unter Beispiele für identitätsbasierte Richtlinien für AWS Ground Station.

ACLs in AWS Ground Station

Unterstützt ACLs	Nein

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

ABAC mit AWS Ground Station

Unterstützt ABAC (Tags in Richtlinien)	Ja

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In AWS werden diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und mehrere AWS-Ressourcen anfügen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, oder `aws:TagKeys`Bedingung verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Was ist ABAC? im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Verwenden temporärer Anmeldeinformationen mit AWS Ground Station

Unterstützt temporäre Anmeldeinformationen	Ja

Einige AWS-Services Featureieren nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, darunter welche AWS-Services mit temporären Anmeldeinformationen Featureieren, finden Sie unter AWS-Services, die mit IAM Featureieren im IAM-Benutzerhandbuch.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen Methode als einem Benutzernamen und einem Passwort bei der AWS Management Console anmelden. Wenn Sie beispielsweise über den Single Sign-On (SSO)-Link Ihres Unternehmens auf AWS zugreifen, erstellt dieser Prozess automatisch temporäre Anmeldeinformationen. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter Wechseln zu einer Rolle (Konsole) im IAM-Benutzerhandbuch.

Sie können mithilfe der AWS CLI- oder AWS-API manuell temporäre Anmeldeinformationen erstellen. Sie können dann diese temporären Anmeldeinformationen verwenden, um auf AWS zuzugreifen. AWS empfiehlt, dass Sie temporäre Anmeldeinformationen dynamisch generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Serviceübergreifende Prinzipal-Berechtigungen für AWS Ground Station

Unterstützt Forward Access Sessions (FAS)	Ja

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle zum Ausführen von Aktionen in AWS verwenden, gelten Sie als Prinzipal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen AWS-Service aufruft, in Kombination mit der Anforderung an den AWS-Service, Anforderungen an nachgelagerte Services zu stellen. FAS-Anforderungen werden nur dann gestellt, wenn ein Dienst eine Anforderung erhält, die Interaktionen mit anderen AWS-Services oder Ressourcen erfordert, um abgeschlossen werden zu können. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für AWS Ground Station

Unterstützt Servicerollen	Nein

Eine Servicerolle ist eine IAM-Rolle, die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

> **Warning**
>
> Die Änderung der Berechtigungen für eine Servicerolle kann die Funktionalität von AWS Ground Station beeinträchtigen. Bearbeiten Sie Servicerollen nur, wenn AWS Ground Station eine Anleitung dazu gibt.

Serviceverknüpfte Rollen für AWS Ground Station

Unterstützt serviceverknüpfte Rollen	Ja

Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einem AWS-Service verknüpft ist. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem AWS-Konto angezeigt und gehören zum Service. Ein IAM-Administrator kann die Berechtigungen für serviceverbundene Rollen anzeigen, aber nicht bearbeiten.

Details zum Erstellen oder Verwalten von serviceverknüpften Rollen finden Sie unter AWS-Services, die mit IAM funktionieren. Suchen Sie in der Tabelle nach einem Service mit einem `Yes` in der Spalte Service-linked role (Serviceverknüpfte Rolle). Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

Beispiele für identitätsbasierte Richtlinien für AWS Ground Station

Benutzer und Rollen haben standardmäßig nicht die Berechtigung, AWS Ground Station-Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben über die AWS Management Console, die AWS Command Line Interface (AWS CLI) oder die AWS-API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Einzelheiten zu den von AWS Ground Station definierten Aktionen und Ressourcentypen, einschließlich des Formats der ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS Ground Station in der Service-Autorisierungs-Referenz.

Themen

- Bewährte Methoden für Richtlinien
- Verwenden der AWS Ground Station-Konsole
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand AWS Ground Station-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Erste Schritte mit AWS-verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen – Um Ihren Benutzern und Workloads Berechtigungen zu gewähren, verwenden Sie die AWS-verwaltete Richtlinien die Berechtigungen für viele allgemeine Anwendungsfälle gewähren. Sie sind in Ihrem AWS-Konto verfügbar. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie AWS-kundenverwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS-verwaltete Richtlinien oder AWS-verwaltete Richtlinien für Auftragsfunktionen im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Service-Aktionen zu gewähren, wenn diese durch ein bestimmtes AWS-Service, wie beispielsweise AWS CloudFormation, verwendet werden. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung zum IAM Access Analyzer im IAM-Benutzerhandbuch.

- Bedarf einer Multi-Faktor-Authentifizierung (MFA) – Wenn Sie ein Szenario haben, das IAM-Benutzer oder Root-Benutzer in Ihrem AWS-Konto erfordert, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Konfigurieren eines MFA-geschützten API-Zugriffs im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Verwenden der AWS Ground Station-Konsole

Um auf die AWS Ground Station-Konsole zuzugreifen, müssen Sie über einen Mindestsatz von Berechtigungen verfügen. Diese Berechtigungen müssen Ihnen das Auflisten und Anzeigen von Details zu den AWS Ground Station-Ressourcen in Ihrem AWS-Konto gestatten. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Für Benutzer, die nur Aufrufe an die AWS CLI oder AWS-API durchführen, müssen Sie keine Mindestberechtigungen in der Konsole erteilen. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

Um sicherzustellen, dass Benutzer und Rollen die AWS Ground Station Konsole weiterhin verwenden können, fügen Sie den Entitäten auch die AWS Ground Station *ConsoleAccess* oder die *ReadOnly* AWS verwaltete Richtlinie hinzu. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie enthält Berechtigungen für die Ausführung dieser Aktion auf der Konsole oder für die programmgesteuerte Ausführung über die AWS CLI oder die AWS-API.

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

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

Fehlerbehebung für AWS Ground Station-Identität und -Zugriff

Verwenden Sie die folgenden Informationen, um häufige Probleme zu diagnostizieren und zu beheben, die beim Arbeiten mit AWS Ground Station und IAM auftreten könnten.

Themen

- Ich bin nicht autorisiert, eine Aktion in AWS Ground Station auszuführen.
- Ich bin nicht berechtigt, iam auszuführen: PassRole
- Ich möchte Personen außerhalb meines AWS-Konto Zugriff auf meine AWS Ground Station-Ressourcen gewähren

Ich bin nicht autorisiert, eine Aktion in AWS Ground Station auszuführen.

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der IAM-Benutzer `mateojackson` versucht, über die Konsole Details zu einer fiktiven *`my-example-widget`*-Ressource anzuzeigen, jedoch nicht über `groundstation:`*`GetWidget`*-Berechtigungen verfügt.

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

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `groundstation:`*`GetWidget`*-Aktion auf die *`my-example-widget`*-Ressource zugreifen kann.

Wenden Sie sich an Ihren AWS-Administrator, falls Sie weitere Unterstützung benötigen. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zum Durchführen der `iam:PassRole`-Aktion autorisiert sind, müssen Ihre Richtlinien aktualisiert werden, um eine Rolle an AWS Ground Station übergeben zu können.

Einige AWS-Services erlauben die Übergabe einer vorhandenen Rolle an diesen Dienst, sodass keine neue Servicerolle oder serviceverknüpfte Rolle erstellt werden muss. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in AWS Ground Station auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

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

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenden Sie sich an Ihren AWS-Administrator, falls Sie weitere Unterstützung benötigen. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb meines AWS-Konto Zugriff auf meine AWS Ground Station-Ressourcen gewähren

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Im Fall von Diensten, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen dazu, ob AWS Ground Station diese Funktionen unterstützt, finden Sie unter Featuresweise von AWS Ground Station mit IAM.
- Informationen zum Gewähren des Zugriffs auf Ihre Ressourcen für alle Ihre AWS-Konten finden Sie unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen Ihrer AWS-Konto im IAM-Benutzerhandbuch.
- Informationen dazu, wie Sie AWS-Konten-Drittanbieter Zugriff auf Ihre Ressourcen bereitstellen, finden Sie unter Gewähren des Zugriffs auf AWS-Konten von externen Benutzern im IAM-Benutzerhandbuch.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.

Verwenden von serviceverknüpften Ground Station

AWS Ground Station verwendet serviceverknüpfte Rollen von AWS Identity and Access Management (IAM). Eine serviceverknüpfte Rolle ist ein spezieller Typ einer serviceverknüpften Rolle, die direkt mit Ground Station verknüpft ist. Serviceverknüpfte Rollen werden von Ground Station vordefiniert und schließen alle Berechtigungen ein, die der Service zum Aufrufen andererAWS -Services in Ihrem Namen erfordert.

Eine serviceverknüpfte Rolle vereinfacht das Einrichten von Ground Station, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Ground Station definiert die Berechtigungen seiner serviceverknüpfte Rollen. Sofern keine andere Konfiguration festgelegt wurde, kann nur Ground Station die Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Informationen zu anderen Services, die serviceorientierte Rollen unterstützen, finden Sie unter AWS services that work with IAM (-Services, die mit IAM funktionieren). Suchen Sie nach den Services, für die Yes (Ja) in der Spalte Service-linked roles (Serviceorientierte Rollen) angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer servicegebundenen Rolle für diesen Service anzuzeigen.

Berechtigungen von serviceverknüpften Ground Station

Ground Station verwendet die serviceverknüpfte Rolle namens AWSServiceRoleForGroundStationDataflowEndpointGroup— AWS GroundStation verwendet diese serviceverknüpfte Rolle, um EC2.

Die AWSServiceRoleForGroundStationDataflowEndpointGroup serviceverknüpfte Rolle vertraut, dass die folgenden Services die Rolle übernehmen:

- `groundstation.amazonaws.com`

Die AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy Ground Station Richtlinie für

- Aktion: `ec2:DescribeAddresses` für `all AWS resources (*)`

  Action ermöglicht es Ground Station, alle IPs aufzulisten, die EIPs zugeordnet sind.
- Aktion: `ec2:DescribeNetworkInterfaces` für `all AWS resources (*)`

  Action ermöglicht es Ground Station, Informationen über die Netzwerkschnittstellen abzurufen, die EC2-Instances zugeordnet sind

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine servicegebundene Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter Serviceverknüpfte Rollenberechtigung im IAM-Benutzerhandbuch.

Erstellen einer serviceverknüpften Ground Station

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie eine DataflowEndpointGroup in derAWS CLI oder derAWS -API erstellen, erstellt Ground Station die serviceverknüpfte Rolle für Sie.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie eine erstellen DataflowEndpointGroup, erstellt Ground Station die serviceverknüpfte Rolle wieder für Sie.

Sie können auch die IAM-Konsole verwenden, um eine serviceverknüpfte Rolle mit dem Anwendungsfall Data Delivery to Amazon EC2 zu erstellen. Erstellen Sie in der AWS CLI oder der AWS-API eine servicegebundene Rolle mit dem Servicenamen `groundstation.amazonaws.com`. Weitere Informationen finden Sie unter Erstellen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch. Wenn Sie diese servicegebundene Rolle löschen, können Sie mit demselben Verfahren die Rolle erneut erstellen.

Bearbeiten einer serviceverknüpften Ground Station

Ground Station berechtigt Sie nicht zum Bearbeiten der AWSServiceRoleForGroundStationDataflowEndpointGroup serviceverknüpften Rolle. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Ground Station

Wenn Sie eine Funktion oder einen Service, die bzw. der eine servicegebundene Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird.

Sie können eine serviceverknüpfte Rolle nur löschen, nachdem Sie zuvor die DataflowEndpointGroups serviceverknüpfte Rolle gelöscht haben. Dies schützt Sie vor dem versehentlichen Entzug von -Regionen DataflowEndpointGroups. Wenn eine serviceverknüpfte Rolle mit mehreren verwendet wird DataflowEndpointGroups, müssen Sie alle löschen DataflowEndpointGroups , die die serviceverknüpfte Rolle verwenden.

> **Note**
>
> Verwendet der Bodenstationsservice die Rolle beim Versuch, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Um die Ressourcen der Ground Station zu löschen, die von AWSServiceRoleForGroundStationDataflowEndpointGroup

- Löschen Sie DataflowEndpointGroups über die AWS-CLI oder die AWS-API.

So löschen Sie die servicegebundene Rolle mit IAM

Verwenden Sie die IAM-Konsole, AWS CLI- oder AWS-API, um die AWSServiceRoleForGroundStationDataflowEndpointGroup serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Unterstützte Regionen für

Ground Station unterstützt die Verwendung von serviceverknüpften Rollen in allen Regionen, in denen der Service verfügbar ist. Weitere Informationen finden Sie unter Regionstabelle.

Fehlerbehebung

`NOT_AUTHORIZED_TO_CREATE_SLR`— Dies bedeutet, dass die Rolle in Ihrem Konto, die zum Aufrufen der CreateDataflowEndpointGroup API verwendet wird, nicht über die entsprechende`iam:CreateServiceLinkedRole` Berechtigung verfügt. Ein Administrator mit der entsprechende`iam:CreateServiceLinkedRole` Berechtigung muss die Service-Linked Role für Ihr Konto manuell erstellen.

AWS Von verwaltete Richtlinien für AWS Ground Station

EinAWSEine verwaltete Richtlinie ist eine eigenständige Richtlinie, die erstellt und verwaltet wird vonAWS.AWSverwaltete Richtlinien sind so konzipiert, dass sie Berechtigungen für viele gängige

Anwendungsfälle bereitstellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Denken Sie daran, dassAWSverwaltete Richtlinien gewähren möglicherweise keine Berechtigungen mit den geringsten Rechten für Ihre spezifischen Anwendungsfälle, da sie für alle verfügbar sindAWSKunden zur Nutzung. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sievom Kunden verwaltete Richtliniendie spezifisch für Ihre Anwendungsfälle sind.

Die Berechtigungen, die in den von AWS verwalteten Richtlinien definiert sind, können nicht geändert werden. WennAWSaktualisiert die in einer definierten BerechtigungenAWSverwaltete Richtlinie, das Update wirkt sich auf alle Hauptidentitäten (Benutzer, Gruppen und Rollen) aus, an die die Richtlinie angehängt ist.AWSaktualisiert am wahrscheinlichsten eineAWSverwaltete Richtlinie, wenn eine neueAWS-Servicewird gestartet oder neue API-Operationen werden für bestehende Dienste verfügbar.

Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

AWS verwaltete Richtlinie: AWSGroundStationAgentInstancePolicy

Sie können die `AWSGroundStationAgentInstancePolicy`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt AWS Ground Station Agent-Berechtigungen für eine Kundeninstanz, die es der Instance ermöglichen, während der Bodenstationskontakte Daten zu senden und zu empfangen. Alle in dieser Richtlinie enthaltenen Berechtigungen stammen vom Ground Station-Dienst.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `groundstation`— Ermöglicht Datenfluss-Endpunktinstanzen, die Ground Station Agent-APIs aufzurufen.

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

AWS verwaltete Richtlinie: AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy

Sie können AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy nicht an Ihre IAM-Entitäten anhängen. Diese Richtlinie ist an eine servicegebundene Rolle angehängt, die AWS Ground Station die Durchführung von Aktionen in Ihrem Namen ermöglicht. Weitere Informationen finden Sie unterVerwendung von dienstverknüpften Rollen.

Diese Richtlinie gewährt EC2-Berechtigungen, die Folgendes ermöglichenAWS Ground Stationum öffentliche IPv4-Adressen zu finden.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `ec2:DescribeAddresses`— ErmöglichtAWS Ground Stationum in Ihrem Namen alle IPs aufzulisten, die EIPs zugeordnet sind.
- `ec2:DescribeNetworkInterfaces`— ErmöglichtAWS Ground Stationum in Ihrem Namen Informationen zu den Netzwerkschnittstellen zu erhalten, die EC2-Instances zugeordnet sind.

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

AWS Ground Station-Aktualisierungen für AWS verwaltete Richtlinien

Anzeigen von Details zu Aktualisierungen für AWS-verwaltete Richtlinien für AWS Ground Station, seit dieser Dienst mit der Verfolgung dieser Änderungen begonnen hat. Um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten, abonnieren Sie den RSS-Feed auf der Seite AWS Ground Station-Dokumentverlauf.

Änderung	Beschreibung	Datum
AWSGroundStationAgentInstancePolicy – Neue Richtlinie.	AWS Ground Stationhat eine neue Richtlinie hinzugefügt, um der Dataflow-Endpoint-Instance Berechtigungen zur Nutzung des AWS Ground Station Agents zu gewähren.	12. April 2023
AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy – Neue Richtlinie.	AWS Ground Stationhat eine neue Richtlinie hinzugefügt, die EC2-Berechtigungen zum Zulassen gewährtAWS	02. November 2022

Änderung	Beschreibung	Datum
	Ground Stationum öffentlic he IPv4-Adressen zu finden, die EIPs zugeordnet sind, und Netzwerkschnittstellen, die EC2-Instances zugeordnet sind.	
AWS Ground Station hat die Änderungsverfolgung gestartet	AWS Ground Station hat mit der Verfolgung von Änderungen an AWS-verwa lteten Richtlinien begonnen.	01. März 2021

Datenverschlüsselung im Ruhezustand für AWS Ground Station

AWS Ground Station bietet standardmäßig Verschlüsselung, um vertrauliche Kundendaten im Speicher mithilfe AWS eigener Verschlüsselungsschlüssel zu schützen.

- AWS-eigene Schlüssel — AWS Ground Station verwendet diese Schlüssel standardmäßig, um persönliche, direkt identifizierbare Daten und Ephemeriden automatisch zu verschlüsseln. Sie können AWS-eigene Schlüssel nicht anzeigen, verwalten oder verwenden oder deren Verwendung überwachen. Es ist jedoch nicht erforderlich, Maßnahmen zu ergreifen oder Programme zu ändern, um die Schlüssel, die Daten verschlüsseln, zu schützen. Weitere Informationen finden Sie unter AWS-eigene Schlüssel im AWS Key Management Service Developer Guide.

Die standardmäßige Verschlüsselung von Daten im Ruhezustand trägt dazu bei, den betrieblichen Aufwand und die Komplexität beim Schutz sensibler Daten zu reduzieren. Gleichzeitig ermöglicht es die Entwicklung sicherer Anwendungen, die die strikte Einhaltung der Verschlüsselungsvorschriften sowie die gesetzlichen Anforderungen erfüllen.

AWS Ground Station erzwingt die Verschlüsselung aller sensiblen Daten, die sich im Speicher befinden. Für einige AWS Ground Station Ressourcen, wie z. B. Ephemeriden, können Sie jedoch einen vom Kunden verwalteten Schlüssel anstelle der standardmäßigen verwalteten Schlüssel verwenden. AWS

- Vom Kunden verwaltete Schlüssel — AWS Ground Station unterstützt die Verwendung eines symmetrischen, vom Kunden verwalteten Schlüssels, den Sie selbst erstellen, besitzen und verwalten, um eine zweite Verschlüsselungsebene zur bestehenden Verschlüsselung hinzuzufügen. AWS Da Sie die volle Kontrolle über diese Verschlüsselungsebene haben, können Sie beispielsweise folgende Aufgaben ausführen:
  - Festlegung und Pflege wichtiger Richtlinien
  - Festlegung und Aufrechterhaltung von IAM-Richtlinien und -Zuschüssen
  - Aktivieren und Deaktivieren wichtiger Richtlinien
  - Kryptographisches Material mit rotierendem Schlüssel
  - Hinzufügen von Tags
  - Erstellen von Schlüsselaliasen
  - Planen von Schlüsseln für das Löschen

Weitere Informationen finden Sie unter vom Kunden verwalteter Schlüssel im AWS Key Management Service Developer Guide.

In der folgenden Tabelle sind Ressourcen zusammengefasst, für die die Verwendung von Customer Managed Keys AWS Ground Station unterstützt wird

Datentyp	AWS-eigene Schlüssel verschlüsselung	Vom Kunden verwaltete Schlüsselverschlüsselung (optional)
Ephemeridendaten, die zur Berechnung der Flugbahn eines Satelliten verwendet werden	Aktiviert	Aktiviert

> **Note**
>
> AWS Ground Station aktiviert automatisch die Verschlüsselung im Ruhezustand mithilfe AWS eigener Schlüssel, um personenbezogene Daten kostenlos zu schützen. Für die Verwendung eines vom Kunden verwalteten Schlüssels fallen jedoch AWS KMS-Gebühren an. Weitere Informationen zur Preisgestaltung finden Sie unter AWS Key Management Service – Preise. Weitere Informationen zu AWS KMS finden Sie im AWS KMS Developer Guide.

Wie AWS Ground Station werden Zuschüsse in AWS KMS verwendet

AWS Ground Station erfordert eine Schlüsselzuweisung, um Ihren vom Kunden verwalteten Schlüssel verwenden zu können.

Wenn Sie eine Ephemeride hochladen, die mit einem vom Kunden verwalteten Schlüssel verschlüsselt ist, AWS Ground Station erstellt das System in Ihrem Namen eine Schlüsselzuweisung, indem es eine CreateGrant Anfrage an KMS sendet. AWS Grants in AWS KMS werden verwendet, um AWS Ground Station Zugriff auf einen KMS-Schlüssel in einem Kundenkonto zu gewähren.

AWS Ground Station erfordert, dass der Zuschuss Ihren vom Kunden verwalteten Schlüssel für die folgenden internen Operationen verwendet:

- Senden Sie `GenerateDataKey` Anfragen an AWS KMS, um Datenschlüssel zu generieren, die mit Ihrem vom Kunden verwalteten Schlüssel verschlüsselt werden.
- Senden Sie `Decrypt` Anfragen an AWS KMS, um die verschlüsselten Datenschlüssel zu entschlüsseln, sodass sie zur Verschlüsselung Ihrer Daten verwendet werden können.
- Senden Sie `Encrypt` Anfragen an AWS KMS, um die bereitgestellten Daten zu verschlüsseln.

Sie können den Zugriff auf die Genehmigung jederzeit widerrufen oder den Zugriff des Services auf den vom Kunden verwalteten Schlüssel entfernen. Wenn Sie dies tun, können Sie auf AWS Ground Station keine der mit dem vom Kunden verwalteten Schlüssel verschlüsselten Daten zugreifen, was sich auf Vorgänge auswirkt, die von diesen Daten abhängig sind. Wenn Sie beispielsweise einer Ephemeride, die derzeit für einen Kontakt verwendet wird, eine Schlüsselzuweisung entziehen, können Sie AWS Ground Station die bereitgestellten Ephemeridendaten nicht verwenden, um die Antenne während des Kontakts auszurichten. Dies führt dazu, dass der Kontakt im Status FAILED endet.

Einen kundenverwalteten Schlüssel erstellen

Sie können mithilfe der AWS Management Console oder der AWS KMS-APIs einen symmetrischen, vom Kunden verwalteten Schlüssel erstellen.

Einen symmetrischen kundenverwalteten Schlüssel erstellen

Folgen Sie den Schritten zur Erstellung eines symmetrischen, vom Kunden verwalteten Schlüssels im AWS Key Management Service Developer Guide.

Schlüsselrichtlinie

Schlüsselrichtlinien steuern den Zugriff auf den vom Kunden verwalteten Schlüssel. Jeder vom Kunden verwaltete Schlüssel muss über genau eine Schlüsselrichtlinie verfügen, die aussagt, wer den Schlüssel wie verwenden kann. Wenn Sie Ihren vom Kunden verwalteten Schlüssel erstellen, können Sie eine Schlüsselrichtlinie angeben. Weitere Informationen finden Sie unter Verwaltung des Zugriffs auf vom Kunden verwaltete Schlüssel im AWS Key Management Service Developer Guide.

Um Ihren vom Kunden verwalteten Schlüssel mit Ihren AWS Ground Station Ressourcen zu verwenden, müssen die folgenden API-Operationen in der Schlüsselrichtlinie zulässig sein:

`kms:CreateGrant`- Fügt einem vom Kunden verwalteten Schlüssel einen Zuschuss hinzu. Gewährt Kontrollzugriff auf einen bestimmten KMS-Schlüssel, der den Zugriff für Grant-Operationen AWS Ground Station erfordert. Weitere Informationen zur Verwendung von Grants finden Sie im AWS Key Management Service Developer Guide.

Dadurch kann Amazon AWS Folgendes tun:

- `GenerateDataKey` aufrufen, um einen verschlüsselten Datenschlüssel zu generieren und zu speichern, da der Datenschlüssel nicht sofort zum Verschlüsseln verwendet wird.
- `Decrypt` aufrufen, um den gespeicherten verschlüsselten Datenschlüssel für den Zugriff auf verschlüsselte Daten zu verwenden.
- Rufen Sie `Encrypt` an, um den Datenschlüssel zum Verschlüsseln von Daten zu verwenden.
- Richten Sie einen Principal ein, der in den Ruhestand geht, damit der Dienst dies tun kann. `RetireGrant`

`kms:DescribeKey`- Stellt dem Kunden verwaltete Schlüsselinformationen zur Verfügung, damit AWS Ground Station der Schlüssel validiert werden kann, bevor versucht wird, einen Zuschuss für den bereitgestellten Schlüssel zu erhalten.

Im Folgenden finden Sie Beispiele für IAM-Richtlinienerklärungen, die Sie hinzufügen können 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" : "*"
  }
]
```

Weitere Informationen zur Angabe von Berechtigungen in einer Richtlinie finden Sie im AWS Key Management Service Developer Guide.

Weitere Informationen zur Fehlerbehebung beim Schlüsselzugriff finden Sie im AWS Key Management Service Developer Guide.

Angabe eines vom Kunden verwalteten Schlüssels für AWS Ground Station

Sie können einen vom Kunden verwalteten Schlüssel angeben, um die folgenden Ressourcen zu verschlüsseln:

- Ephemeride

Wenn Sie eine Ressource erstellen, können Sie den Datenschlüssel angeben, indem Sie ein kmsKeyArn

- kmsKeyArn- Eine Schlüssel-ID für einen AWS vom Kunden verwalteten KMS-Schlüssel

AWS Ground Station Verschlüsselungskontext

Ein Verschlüsselungskontext ist ein optionaler Satz von Schlüssel-Wert-Paaren, die zusätzliche kontextbezogene Informationen zu den Daten enthalten. AWS KMS verwendet den Verschlüsselungskontext als zusätzliche authentifizierte Daten, um die authentifizierte Verschlüsselung zu unterstützen. Wenn Sie einen Verschlüsselungskontext in eine Anforderung zur Datenverschlüsselung aufnehmen, bindet AWS KMS den Verschlüsselungskontext an die verschlüsselten Daten. Zur Entschlüsselung von Daten müssen Sie denselben Verschlüsselungskontext in der Anfrage übergeben.

AWS Ground Station Verschlüsselungskontext

AWS Ground Station verwendet je nach der zu verschlüsselnden Ressource einen anderen Verschlüsselungskontext und gibt für jede erstellte Schlüsselzuweisung einen bestimmten Verschlüsselungskontext an.

Ephemeriden-Verschlüsselungskontext:

Key Grant für die Verschlüsselung von Ephemeridenressourcen ist an einen bestimmten Satelliten-ARN gebunden

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

> **Note**
>
> Key Grants werden für dasselbe Schlüssel-Satellitenpaar wiederverwendet.

Verwenden des Verschlüsselungskontexts für die Überwachung

Wenn Sie einen symmetrischen, vom Kunden verwalteten Schlüssel zur Verschlüsselung Ihrer Ephemeriden verwenden, können Sie den Verschlüsselungskontext auch in Prüfaufzeichnungen und Protokollen verwenden, um festzustellen, wie der vom Kunden verwaltete Schlüssel verwendet

wird. Der Verschlüsselungskontext erscheint auch in [Protokollen, die von Amazon CloudWatch Logs generiert wurden AWS CloudTrail].

Verwendung des Verschlüsselungskontextes zur Steuerung des Zugriffs auf den vom Kunden verwalteten Schlüssel

Sie können den Verschlüsselungskontext in Schlüsselrichtlinien und IAM-Richtlinien als `conditions` verwenden, um den Zugriff auf Ihren symmetrischen, kundenverwalteten Schlüssel zu kontrollieren. Sie können Verschlüsselungskontext-Einschränkungen auch in einer Genehmigung verwenden.

AWS Ground Station verwendet bei Zuschüssen eine Einschränkung des Verschlüsselungskontextes, um den Zugriff auf den vom Kunden verwalteten Schlüssel in Ihrem Konto oder Ihrer Region zu kontrollieren. Eine Genehmigungseinschränkung erfordert, dass durch die Genehmigung ermöglichte Vorgänge den angegebenen Verschlüsselungskontext verwenden.

Im Folgenden finden Sie Beispiele für Schlüsselrichtlinienanweisungen zur Gewährung des Zugriffs auf einen vom Kunden verwalteten Schlüssel für einen bestimmten Verschlüsselungskontext. Die Bedingung in dieser Richtlinienanweisung setzt voraus, dass die Genehmigungen eine Einschränkung des Verschlüsselungskontextes haben, die den Verschlüsselungskontext spezifiziert.

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

Überwachen Sie Ihre Verschlüsselungsschlüssel für AWS Ground Station

Wenn Sie einen AWS vom Kunden verwalteten KMS-Schlüssel mit Ihren AWS Ground Station Ressourcen verwenden, können Sie unsere CloudWatch Amazon-Protokolle verwenden AWS CloudTrail, um Anfragen zu verfolgen, die AWS Ground Station an AWS KMS gesendet werden. Die folgenden Beispiele sind AWS CloudTrail Ereignisse für`CreateGrant`,`GenerateDataKey`, `Encrypt` und `DescribeKey` zur Überwachung von KMS-Vorgängen`Decrypt`, die von der AWS Ground Station aufgerufen werden, um auf Daten zuzugreifen, die mit Ihrem vom Kunden verwalteten Schlüssel verschlüsselt wurden.

`CreateGrant`(Cloudtrail)

Wenn Sie einen AWS vom Kunden verwalteten KMS-Schlüssel zur Verschlüsselung Ihrer Ephemeridenressourcen verwenden, AWS Ground Station sendet er in Ihrem Namen eine `CreateGrant` Anfrage, um auf den KMS-Schlüssel in Ihrem Konto zuzugreifen. AWS Die gewährten Zuschüsse sind AWS Ground Station spezifisch für die Ressource, die dem vom Kunden verwalteten AWS KMS-Schlüssel zugeordnet ist. Darüber hinaus verwendet AWS Ground Station den `RetireGrant` Vorgang, um einen Zuschuss zu entfernen, wenn Sie eine Ressource löschen.

Das folgende Beispielereignis zeichnet den Vorgang `CreateGrant` auf:


```
{
    "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)

Wenn Sie einen AWS vom Kunden verwalteten KMS-Schlüssel zur Verschlüsselung Ihrer Ephemeridenressourcen verwenden, AWS Ground Station sendet er in Ihrem Namen eine `DescribeKey` Anfrage, um zu überprüfen, ob der angeforderte Schlüssel in Ihrem Konto vorhanden ist.

Das folgende Beispielereignis zeichnet den Vorgang `DescribeKey` auf:

```
{
    "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)

Wenn Sie einen AWS vom Kunden verwalteten KMS-Schlüssel zur Verschlüsselung Ihrer Ephemeridenressourcen verwenden, AWS Ground Station sendet er eine `GenerateDataKey` Anfrage an KMS, um einen Datenschlüssel zu generieren, mit dem Ihre Daten verschlüsselt werden können.

Das folgende Beispielereignis zeichnet den Vorgang `GenerateDataKey` auf:

```
{
    "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)

Wenn Sie einen AWS vom Kunden verwalteten KMS-Schlüssel zum Verschlüsseln Ihrer Ephemeridenressourcen verwenden, wird der `Decrypt` Vorgang zur Entschlüsselung der bereitgestellten Ephemeriden AWS Ground Station verwendet, sofern sie bereits mit demselben vom Kunden verwalteten Schlüssel verschlüsselt ist. Zum Beispiel, wenn eine Ephemeride aus einem S3-Bucket hochgeladen und in diesem Bucket mit einem bestimmten Schlüssel verschlüsselt wird.

Das folgende Beispielereignis zeichnet den Vorgang `Decrypt` auf:

```
{
    "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"
}
```

Satelliten-Ephemeridendaten

Eine Ephemeride, mehrere Ephemeriden, ist eine Datei oder Datenstruktur, die die Flugbahn astronomischer Objekte angibt. In der Vergangenheit bezog sich diese Datei nur auf tabellarische Daten, aber nach und nach hat sie sich zu einer Vielzahl von Datendateien entwickelt, die die Flugbahn eines Raumfahrzeugs angeben.

AWS Ground Station verwendet Ephemeridendaten, um festzustellen, wann Kontakte für Ihren Satelliten verfügbar werden, und ordnet Antennen im AWS Ground Station Netzwerk korrekt an, auf Ihren Satelliten zu zeigen. Standardmäßig ist keine Aktion erforderlich, um AWS Ground Station Ephemeriden bereitzustellen.

Themen

Standard-Ephemeridendaten

AWS Ground Station Verwendet standardmäßig öffentlich verfügbare Daten von Space-Track, und es sind keine Maßnahmen erforderlich, um diese Standard-Ephemeriden AWS Ground Station bereitzustellen. Bei diesen Ephemeriden handelt es sich um zweizeilige Elementsätze, die der NORAD-ID Ihres Satelliten zugeordnet sind. Alle Standard-Ephemeriden haben eine Priorität von 0. Daher werden sie immer von allen nicht abgelaufenen, benutzerdefinierten Ephemeriden überschrieben, die über die Ephemeriden-API hochgeladen wurden. Diese API muss immer eine Priorität von 1 oder höher haben.

Satelliten ohne NORAD-ID müssen benutzerdefinierte Ephemeridendaten auf hochladen. AWS Ground Station Zum Beispiel hätten Satelliten, die gerade gestartet wurden oder die bewusst nicht im Space-Track-Katalog aufgeführt sind, keine NORAD-ID und es müssten benutzerdefinierte Ephemeriden hochgeladen werden. Weitere Informationen zur Bereitstellung

einer benutzerdefinierten Ephemeride finden Sie unter: Bereitstellung benutzerdefinierter Ephemeridendaten.

Welche Ephemeride wird verwendet

Ephemeriden haben eine Prioritäts -, Ablaufzeit - und Aktivierungskennzeichnung. Zusammen bestimmen sie, welche Ephemeride für einen Satelliten verwendet wird. Für jeden Satelliten kann nur eine Ephemeride aktiv sein.

Die Ephemeride, die verwendet wird, ist die aktivierte Ephemeride mit der höchsten Priorität, deren Ablaufzeit in der future liegt. Die verfügbaren Kontaktzeiten, die von ListContactszurückgegeben werden, basieren auf dieser Ephemeride. Wenn mehrere `ENABLED` Ephemeriden dieselbe Priorität haben, wird die zuletzt erstellte oder aktualisierte Ephemeride verwendet.

> **Note**
>
> AWS Ground Station hat ein Servicekontingent für die Anzahl der `ENABLED` vom Kunden bereitgestellten Ephemeriden pro Satellit (siehe: Service Quotas). Um Ephemeridendaten nach Erreichen dieses Kontingents hochzuladen, löschen (verwenden`DeleteEphemeris`) oder deaktivieren (verwenden) Sie die Ephemeriden mit der niedrigsten Priorität/den frühesten erstellten, vom Kunden bereitgestellten `UpdateEphemeris` Ephemeriden.

Wenn keine Ephemeriden erstellt wurden oder keine Ephemeriden einen `ENABLED` Status haben, wird eine Standard-Ephemeride für den Satelliten (von Space Track) verwendet, sofern AWS Ground Station verfügbar. Diese Standard-Ephemeride hat Priorität 0.

Auswirkung neuer Ephemeriden auf zuvor geplante Kontakte

Verwenden Sie die DescribeContact API, um die Auswirkungen neuer Ephemeriden auf zuvor geplante Kontakte anzuzeigen, indem Sie die aktiven Sichtbarkeitszeiten anzeigen.

Kontakte, die vor dem Hochladen einer neuen Ephemeride geplant wurden, behalten die ursprünglich geplante Kontaktzeit bei, während das Antennen-Tracking die aktiven Ephemeriden verwendet. Wenn die Position des Raumfahrzeugs, basierend auf der aktiven Ephemeride, stark von der Position der vorherigen Ephemeride abweicht, kann dies zu einer kürzeren Kontaktzeit des Satelliten mit der Antenne führen, da das Raumfahrzeug außerhalb der Maske des Sende-/Empfangsorts operiert. Daher empfehlen wir Ihnen, Ihre future Kontakte zu stornieren und zu verschieben, nachdem Sie eine neue Ephemeride hochgeladen haben, die sich stark von den vorherigen Ephemeriden unterscheidet.

Mit der DescribeContact API können Sie den Teil Ihres future Kontakts ermitteln, der unbrauchbar ist, weil das Raumschiff außerhalb der Maske für den Sende-/Empfangsort operiert, indem Sie Ihren geplanten Kontakt `endTime` mit dem zurückgegebenen `startTime` und vergleichen. `visibilityStartTime` `visibilityEndTime` Wenn Sie sich dafür entscheiden, Ihre future Kontakte zu stornieren und zu verschieben, darf der Kontaktzeitbereich nicht länger als 30 Sekunden außerhalb des Sichtbarkeitszeitbereichs liegen. Stornierte Kontakte können Kosten verursachen, wenn sie zu kurz vor dem Zeitpunkt des Kontakts storniert werden. Weitere Informationen zu stornierten Kontakten finden Sie unter: Häufig gestellte Fragen zur Ground Station.

Die aktuelle Ephemeride für einen Satelliten abrufen

Die aktuelle Ephemeride, die von AWS Ground Station einem bestimmten Satelliten verwendet wird, kann durch Aufrufen der Aktionen oder abgerufen werden. `GetSatellite` `ListSatellites` Beide Methoden geben Metadaten für die aktuell verwendete Ephemeride zurück. Diese Ephemeriden-Metadaten unterscheiden sich für benutzerdefinierte Ephemeriden, die auf Standard-Ephemeriden hochgeladen wurden, und für Standard-Ephemeriden. AWS Ground Station

Standard-Ephemeriden enthalten nur Felder und. `source` `epoch` Dies `epoch` ist die Epoche des aus Space Track stammenden Elementsatzes mit zwei Linien AWS Ground Station, der derzeit zur Berechnung der Flugbahn des Satelliten verwendet wird.

Eine benutzerdefinierte Ephemeride hat den `source` Wert `"CUSTOMER_PROVIDED"` und enthält eine eindeutige Kennung im Feld. `ephemerisId` Diese eindeutige Kennung kann verwendet werden, um über die Aktion nach der Ephemeride abzufragen. `DescribeEphemeris` Ein optionales `name` Feld wird zurückgegeben, wenn der Ephemeride beim Hochladen über die Aktion ein Name zugewiesen wurde. AWS Ground Station `CreateEphemeris`

Es ist wichtig zu beachten, dass Ephemeriden dynamisch aktualisiert werden, AWS Ground Station sodass die zurückgegebenen Daten nur eine Momentaufnahme der Ephemeriden sind, die zum Zeitpunkt des API-Aufrufs verwendet wurden.

Beispiel für eine **`GetSatellite`** Rückgabe für einen Satelliten, der eine Standard-Ephemeride verwendet

```
{
    "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
    }
}
```

Beispiel **`GetSatellite`** für einen Satelliten, der eine benutzerdefinierte Ephemeride verwendet

```
{
      "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"
      }
  }
```

Bereitstellung benutzerdefinierter Ephemeridendaten

> **Warning**
>
> Die Ephemeriden-API befindet sich derzeit im Vorschaustatus

Der Zugriff auf die Ephemeris-API wird nur bei Bedarf gewährt. Kunden, die die Möglichkeit benötigen, benutzerdefinierte Ephemeridendaten hochzuladen, wenden sich bitte an aws-groundstation@amazon.com.

Übersicht

Die Ephemeriden-API ermöglicht das Hochladen benutzerdefinierter Ephemeriden zur Verwendung mit einem Satelliten. AWS Ground Station Diese Ephemeriden überschreiben die Standard-Ephemeriden aus Space Track (siehe: Standard-Ephemeridendaten).

Das Hochladen von Ephemeriden von Kunden kann die Qualität der Ortung verbessern, frühe Operationen abwickeln, für die keine Space Track-Ephemeriden verfügbar sind, und um Manöver zu berücksichtigen. AWS Ground Station

Eine benutzerdefinierte Ephemeride erstellen

Eine benutzerdefinierte Ephemeride kann mithilfe der `CreateEphemeris` Aktion in der API erstellt werden. AWS Ground Station Diese Aktion lädt eine Ephemeride hoch, wobei Daten entweder im Anfragetext oder aus einem bestimmten S3-Bucket verwendet werden.

Es ist wichtig zu beachten, dass beim Hochladen einer Ephemeride die Ephemeride in einen asynchronen Workflow umgewandelt `VALIDATING` und gestartet wird, der potenzielle Kontakte anhand Ihrer Ephemeride validiert und generiert. Erst wenn eine Ephemeride diesen Workflow bestanden hat und geworden ist, wird sie für Kontakte verwendet. `ENABLED` Sie sollten den Ephemeridenstatus `DescribeEphemeris` abfragen oder Cloudwatch-Ereignisse verwenden, um die Statusänderungen der Ephemeriden zu verfolgen.

Informationen zur Fehlerbehebung bei ungültigen Ephemeriden finden Sie unter: Fehlerbehebung bei ungültigen Ephemeriden

Erstellen Sie eine TLE-Set-Ephemeride über die API

Der AWS Ground Station Boto3-Client kann verwendet werden, um eine TLE-Ephemeride (TWO Line Element) über den Aufruf hochzuladen. AWS Ground Station `CreateEphemeris` Diese Ephemeride wird anstelle der Standard-Ephemeridendaten für einen Satelliten verwendet (siehe Standard-Ephemeridendaten).

Ein TLE-Set ist ein Objekt im JSON-Format, das eine oder mehrere TLEs aneinanderreiht, um eine kontinuierliche Flugbahn zu erstellen. Die TLEs im TLE-Set müssen einen kontinuierlichen Satz bilden, den wir verwenden können, um eine Trajektorie zu konstruieren (d. h. keine Zeitlücken zwischen den TLEs in einem TLE-Set). Ein Beispiel für ein TLE-Set ist unten dargestellt:

```
# 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**
>
> Die Zeitbereiche der TLEs in einem TLE-Set müssen exakt übereinstimmen, damit es sich um eine gültige, kontinuierliche Trajektorie handelt.

Ein TLE-Set kann wie folgt über den AWS Ground Station boto3-Client hochgeladen werden:

```
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)
                }
            }
        ]
      }
    })
```

Dieser Aufruf gibt eine Ephemeriden-ID zurück, mit der in future auf die Ephemeride verwiesen werden kann. Zum Beispiel können wir die angegebene Ephemeriden-ID aus dem obigen Aufruf verwenden, um den Status der Ephemeriden abzufragen:

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

Im Folgenden finden Sie ein Beispiel für eine Antwort aus der Aktion `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}}]"
    }
  }
}
```

Es wird empfohlen, die `DescribeEphemeris` Route abzufragen oder Cloudwatch-Ereignisse zu verwenden, um den Status der hochgeladenen Ephemeriden zu verfolgen, da sie einen asynchronen Validierungsworkflow durchlaufen muss, bevor sie auf eingestellt wird `ENABLED` und für die Planung und Ausführung von Kontakten verwendet werden kann.

Beachten Sie, dass die NORAD-ID in allen TLEs im TLE-Set 25994 in den obigen Beispielen mit der NORAD-ID übereinstimmen muss, die Ihrem Satelliten in der Space Track-Datenbank zugewiesen wurde.

Ephemeridendaten aus einem S3-Bucket hochladen

Es ist auch möglich, eine Ephemeriden-Datei direkt aus einem S3-Bucket hochzuladen, indem Sie auf den Bucket und den Objektschlüssel zeigen. AWS Ground Station ruft das Objekt in Ihrem Namen ab. Informationen zur Verschlüsselung ruhender Daten finden Sie unter: Datenverschlüsselung im Ruhezustand für AWS Ground Station AWS Ground Station

Im Folgenden finden Sie ein Beispiel für das Hochladen einer OEM-Ephemeriden-Datei aus einem S3-Bucket

```
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",
            }
        }
    })
```

Im Folgenden finden Sie ein Beispiel für zurückgegebene Daten aus der `DescribeEphemeris` Aktion, die für die OEM-Ephemeride aufgerufen wurde, die im vorherigen Beispielcodeblock hochgeladen wurde.

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

Fehlerbehebung für „Ungültige Ephemeriden“

Wenn eine benutzerdefinierte Ephemeride hochgeladen wird, durchläuftAWS Ground Station sie einen asynchronen Validierungsworkflow, bevor sie wird`ENABLED`. Dieser Arbeitsablauf stellt sicher, dass die Satellitenkennungen, Metadaten und Flugbahn gültig sind.

Wenn eine Ephemeride die Validierung nicht bestanden hat,`DescribeEphemeris` wird an zurückgegeben EphemerisInvalidReason, was Aufschluss darüber gibt, warum die Ephemeride die Validierung nicht bestanden hat. Die potenziellen Werte von EphemerisInvalidReasonsind wie folgt:

Wert	Beschreibung	Aktion zur Fehlerbehebung
METADATEN_UNGÜLTIG	Angegebene Raumfahrz eugkennungen wie die Satelliten-ID sind ungültig	Überprüfen Sie die NORAD-ID oder andere Identifikatoren, die in den Ephemeridendaten angegeben sind
TIME_RANGE_UNGÜLTIG	Start-, End- oder Ablaufzeit (n) sind für die angegebene Ephemeride ungültig	Stellen Sie sicher, dass die Startzeit vor `jetzt` liegt (es wird empfohlen, die Startzeit einige Minuten in der Vergangenheit einzustel len), dass die Endzeit nach der Startzeit liegt und dass die Endzeit nach der Ablaufzeit liegt
TRAJECTORY_INVALID	Vorausgesetzt, Ephemerid e definiert eine ungültige Flugbahn des Raumfahrzeugs	Vergewissern Sie sich, dass die angegebene Flugbahn kontinuierlich ist und für den richtigen Satelliten bestimmt ist.
VALIDIERUNG_FEHLER	Bei der Verarbeitung von Ephemeriden zur Validierung ist ein interner Dienstfehler aufgetreten	Wiederholen des Uploads

Im Folgenden finden Sie ein Beispiel für eine`DescribeEphemeris` Antwort auf eine`INVALID` Ephemeride:

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

Zu Standard-Ephemeridendaten zurückkehren

Wenn Sie benutzerdefinierte Ephemeridendaten hochladen, überschreiben diese die standardmäßigen AWS Ground Station Ephemeridendaten, die für diesen bestimmten Satelliten verwendet werden. AWS Ground Station verwendet die Standard-Ephemeriden erst wieder, wenn keine derzeit aktivierten, noch nicht abgelaufenen, vom Kunden bereitgestellten Ephemeriden zur Verfügung stehen. AWS Ground Station listet auch keine Kontakte auf, die nach Ablauf der aktuellen vom Kunden bereitgestellten Ephemeride abgelaufen sind, auch wenn nach dieser Ablaufzeit eine Standard-Ephemeride verfügbar ist.

Um zu den standardmäßigen Space Track-Ephemeriden zurückzukehren, müssen Sie einen der folgenden Schritte ausführen:

- Alle aktivierten, vom Kunden bereitgestellten Ephemeriden löschen (verwenden`DeleteEphemeris`) oder deaktivieren (verwenden`UpdateEphemeris`). Sie können die vom Kunden bereitgestellten Ephemeriden für einen Satelliten auflisten, der sie verwendet. `ListEphemerides`
- Warten Sie, bis alle vorhandenen, vom Kunden bereitgestellten Ephemeriden abgelaufen sind.

Sie können überprüfen, ob die Standard-Ephemeride verwendet wird, indem Sie anrufen `GetSatellite` und überprüfen, ob die aktuelle Ephemeride für den Satelliten `source` verwendet wird. `SPACE_TRACK` Weitere Informationen zu Standard-Ephemeriden finden Sie unter Standard-Ephemeridendaten.

AWS Ground Station Seitenmasken

Jedem AWS Ground Station Antennenstandort sind Standortmasken zugeordnet. Diese Masken verhindern, dass Antennen an diesem Standort senden oder empfangen, wenn sie in bestimmte Richtungen zeigen, normalerweise in der Nähe des Horizonts. Die Masken können Folgendes berücksichtigen:

- Merkmale des die Antenne umgebenden geografischen Geländes. Dazu gehören beispielsweise Dinge wie Berge oder Gebäude, die ein Hochfrequenzsignal (HF) blockieren oder die Übertragung verhindern würden.
- Hochfrequenzinterferenz (RFI) Dies beeinträchtigt sowohl die Empfangsfähigkeit (externe RFI-Quellen beeinflussen ein Downlink-Signal in die AWS-Bodenstation-Antennen) als auch die Übertragungsfähigkeit (das von AWS-Bodenstationsantennen übertragene HF-Signal beeinträchtigt externe Empfänger).
- Rechtliche Genehmigungen. Lokale Standortgenehmigungen für den Betrieb von AWS Ground Station in jeder Region können spezifische Einschränkungen beinhalten, z. B. einen Mindesthöhenwinkel für die Übertragung.

Diese Seitenmasken können sich im Laufe der Zeit ändern. Beispielsweise könnten neue Gebäude in der Nähe eines Antennenstandorts errichtet werden, RFI-Quellen könnten sich ändern oder gesetzliche Genehmigungen könnten mit anderen Einschränkungen erneuert werden. Die AWS Ground Station Station-Standortmasken stehen Kunden im Rahmen einer Geheimhaltungsvereinbarung (NDA) zur Verfügung.

Kundenspezifische Masken

Zusätzlich zu den Masken der AWS Ground Station an jedem Standort kann jeder Kunde zusätzliche Masken verwenden, da seine eigene gesetzliche Autorisierung zur Kommunikation mit seinen Satelliten in einer bestimmten Region eingeschränkt ist. Solche Masken können in AWS Ground Station so konfiguriert werden, dass die Einhaltung case-by-case der Vorschriften gewährleistet ist, wenn AWS Ground Station für die Kommunikation mit diesen Satelliten verwendet wird. Weitere Informationen erhalten Sie vom AWS Ground Station Station-Team.

Auswirkung von Website-Masken auf die verfügbaren Kontaktzeiten

Es gibt zwei Arten von Seitenmasken: Seitenmasken für Uplinks (Übertragung) und Seitenmasken für Downlinks (Empfang).

Bei der Auflistung verfügbarer Kontaktzeiten mithilfe des ListContacts Vorgangs gibt AWS Ground Station Sichtbarkeitszeiten zurück, die darauf basieren, wann Ihr Satellit über und unter der Downlink-Maske steht. Die verfügbaren Kontaktzeiten basieren auf diesem Sichtbarkeitsfenster für die Downlink-Maske. Dadurch wird sichergestellt, dass Kunden keine Zeit reservieren oder dafür bezahlen, wenn sich ihr Satellit unter der Downlink-Maske befindet.

Uplink-Site-Masken werden nicht auf die verfügbaren Kontaktzeiten angewendet, auch wenn das Missionsprofil eine Antennen-Uplink-Konfiguration in einem Datenfluss-Edge enthält. Auf diese Weise können Kunden die gesamte verfügbare Kontaktzeit für den Downlink nutzen, auch wenn der Uplink aufgrund der Uplink-Site-Maske für Teile dieser Zeit möglicherweise nicht verfügbar ist. Es kann jedoch sein, dass das Uplink-Signal während eines Teils oder der gesamten Zeit, die für einen Satellitenkontakt reserviert ist, nicht übertragen wird. Die Kunden sind dafür verantwortlich, die bereitgestellte Uplink-Maske bei der Planung von Uplink-Übertragungen zu berücksichtigen.

Der Teil eines Kontakts, der für den Uplink nicht verfügbar ist, hängt von der Flugbahn des Satelliten während des Kontakts im Verhältnis zur Uplink-Standortmaske an der Antennenposition ab. In Regionen, in denen die Uplink- und Downlink-Seitenmasken ähnlich sind, ist diese Dauer in der Regel kurz. In anderen Regionen, in denen die Uplink-Maske erheblich höher sein kann als die Maske der Downlink-Seite, kann dies dazu führen, dass erhebliche Teile oder sogar die gesamte Kontaktdauer für den Uplink nicht verfügbar sind. Die gesamte Kontaktzeit wird dem Kunden in Rechnung gestellt, auch wenn Teile der reservierten Zeit für den Uplink nicht verfügbar sind.

Dokumentenverlauf für das AWS Ground Station Benutzerhandbuch

In der folgenden Tabelle werden die wichtigen Änderungen an der Dokumentation seit der letzten Version von beschrieben AWS Ground Station.

Änderung	Beschreibung	Veröffentlichungsdatum
Neues Feature	Kontakte können jetzt für bis zu 30 Sekunden außerhalb der Sichtbarkeitszeit geplant werden. Sichtbarkeitszeiten sind in den DescribeContact Antworten enthalten.	26. März 2024
Aktualisierung der Dokumentation	Die Organisation wurde verbessert und der Abschnitt „EC2-Instanzauswahl und CPU-Planung“ hinzugefügt.	6. März 2024
Aktualisierung der Dokumentation	Dem AWS Ground Station Agent-Benutzerhandbuch wurden neue bewährte Methoden für die Ausführung von Diensten und Prozessen neben dem AWS Ground Station Agenten hinzugefügt.	23. Februar 2024
Aktualisierung der Dokumentation	Die Seite mit den Versionshinweisen für Agenten wurde hinzugefügt.	21. Februar 2024
Aktualisierung der Vorlage	Unterstützung für ein separates öffentliches Subnetz in der DirectBroadcastSatelliteWbDigIfEc DataDelivery 2-Vorlage hinzugefügt.	14. Februar 2024
Aktualisierung der Dokumentation	In der Monitoring-Dokumentation wurde ein Verweis Benutzerbenachrichtigungen auf AWS hinzugefügt.	6. August 2023
Aktualisierung der Dokumentation	Es wurden Anweisungen zum Markieren von Satelliten mit einem Namen hinzugefügt, der	26. Juli 2023

Änderung	Beschreibung	Veröffentlichungsdatum
	in der AWS Ground Station Konsole angezeigt werden soll.	
Neues Feature	Das AWS Ground Station Agenten-Benutzerhandbuch für die Veröffentlichung von Wideband DigIF Data Delivery wurde hinzugefügt	12. April 2023
Aktualisierungen der verwalteten AWS-Richtlinien — Neue AWS verwaltete Richtlinien	AWS Ground Station hat eine neue Richtlinie mit dem Namen hinzugefügt AWSGroundStationAgentInstancePolicy.	12. April 2023
Neues Feature	Das Benutzerhandbuch für die Veröffentlichung von CPE Preview wurde aktualisiert.	9. November 2022
Aktualisierungen der verwalteten AWS-Richtlinien — Neue AWS verwaltete Richtlinien	AWS Ground Station hat die AWSServiceRoleForGroundStationDataflowEndpointGroup service-linked-role (SLR) hinzugefügt, die eine neue Richtlinie mit dem Namen AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy enthält.	02. November 2022
Neues Feature	Das Benutzerhandbuch wurde aktualisiert und umfasst nun auch die Integration mit AWS CLI.	17. April 2020
Neues Feature	Das Benutzerhandbuch wurde um die Integration mit CloudWatch Metrics aktualisiert.	24. Februar 2020
Neue Vorlage	Öffentliche Rundfunksatelliten (AquaSnppJpss Vorlage) wurden dem AWS Ground Station Benutzerhandbuch hinzugefügt.	19. Februar 2020
Neues Feature	Das Benutzerhandbuch wurde aktualisiert, um die regionsübergreifende Datenzustellung einzuschließen.	5. Februar 2020

Änderung	Beschreibung	Veröffentlichungsdatum
Aktualisierung der Dokumentation	Beispiele und Beschreibungen für die Überwachung AWS Ground Station mit CloudWatch Ereignissen wurden aktualisiert.	4. Februar 2020
Aktualisierung der Dokumentation	Die Speicherorte der Vorlagen wurden aktualisiert und die Abschnitte „Erste Schritte“ und „Fehlerbehebung“ wurden überarbeitet.	19. Dezember 2019
Neuer Abschnitt für Fehlerbehebung	Der Abschnitt zur Fehlerbehebung wurde dem AWS Ground Station Benutzerhandbuch hinzugefügt.	7. November 2019
Neues Thema „Erste Schritte“	Das Thema Erste Schritte wurde aktualisiert, das die aktuellsten AWS CloudFormation Vorlagen enthält.	1. Juli 2019
Kindle-Version	Veröffentlichte Kindle-Version des AWS Ground Station Benutzerhandbuchs.	20. Juni 2019
Neuer Dienst mit dazugehörigem Handbuch	Dies ist die erste Version von AWS Ground Station und das AWS Ground Station Benutzerhandbuch.	23. Mai 2019

AWS-Glossar

Die neueste AWS-Terminologie finden Sie im AWS-Glossar in der AWS-Glossar-Referenz.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.