Benutzer-Leitfaden

AWS Ground Station

AWS Ground Station: Benutzer-Leitfaden

Table of Contents

Was ist AWS Ground Station? 1
Häufige Anwendungsfälle 1
Nächste Schritte 2
Wie AWS Ground Station funktioniert 3
Onboarding per Satellit 3
Zusammensetzung des Missionsprofils 3
Kontaktplanung 5
Ausführung des Kontakts 7
Digitaler Zwilling 9
AWS Ground Station Kernkomponenten verstehen 9
Missionsprofil 11
Configs 14
Dataflow-Endpunktgruppen 24
AWS Ground Station Agent 32
Erste Schritte 34
Melden Sie sich an für ein AWS-Konto 34
Erstellen eines Benutzers mit Administratorzugriff 34
Fügen Sie Ihrem AWS Konto AWS Ground Station Berechtigungen hinzu 36
Satellit an Bord 38
Überblick über den Onboarding-Prozess für Kunden 38
(Optional) Benennen von Satelliten 39
Öffentliche Rundfunksatelliten 42
Planen Sie Ihre Datenfluss-Kommunikationspfade 42
Asynchrone Datenübermittlung 43
Synchrone Datenübermittlung 44
Planen Sie Ihre Telemetrie 45
Konfigurationen erstellen 46
Konfigurationen für die Datenlieferung 46
Telemetriekonfiguration (optional) 46
Satelliten-Konfigurationen 46
Missionsprofil erstellen 47
Verstehen Sie die nächsten Schritte 48
AWS Ground Station Standorte 49
Suche nach der AWS-Region für einen Standort für eine Bodenstation 49

AWS Ground Station unterstützte AWS-Regionen 51
Verfügbarkeit digitaler Zwillinge 51
AWS Ground Station Seitenmasken 51
Kundenspezifische Masken 52
Auswirkung von Seitenmasken auf die verfügbaren Kontaktzeiten 52
AWS Ground Station Funktionen der Website 53
Verstehe, wie AWS Ground Station Ephemeriden verwendet werden 57
Standard-Ephemeridendaten 58
Stellen Sie benutzerdefinierte Ephemeridendaten bereit 58
-Übersicht 58
Beispiel: Verwendung von vom Kunden bereitgestellten Ephemeriden mit AWS Ground Station 59
Stellen Sie TLE-Ephemeridendaten bereit 59
Stellen Sie OEM-Ephemeridendaten bereit 66
Geben Sie Azimut-Elevations-Ephemeridendaten an 74
Reservieren Sie Kontakte mit benutzerdefinierten Ephemeriden 85
-Übersicht 85
Workflows für Kontaktreservierungen 86
Arbeitsablauf 1: Verfügbare Kontakte auflisten und dann reservieren 86
Workflow 2: Direkte Kontaktreservierung 91
Überwachung von Änderungen des Kontaktstatus 94
Bewährte Methoden und Überlegungen 96
Verstehe, welche Ephemeride verwendet wird 97
TLE- und OEM-Ephemeriden 98
Azimut-Elevations-Ephemeriden 98
Auswirkung neuer Ephemeriden auf zuvor geplante Kontakte 99
Ruft die aktuelle Ephemeride für einen Satelliten ab 100
Beispiel für eine GetSatelliteRückgabe für einen Satelliten, der eine Standard-Ephemeride verwendet 100
Beispiel GetSatellitefür einen Satelliten, der eine benutzerdefinierte Ephemeride verwendet 101
Auflisten von Azimut-Elevations-Ephemeriden 101
Kehren Sie zu den Standard-Ephemeridendaten zurück 102
Rückgängigmachen von TLE- und OEM-Ephemeriden 103
Verwaltung von Azimut-Elevations-Ephemeriden 103
Mit Datenflüssen arbeiten 105

AWS Ground Station Schnittstellen auf Datenebene 105
Verwenden Sie die regionsübergreifende Datenbereitstellung 106
Amazon S3 einrichten und konfigurieren 106
Amazon VPC einrichten und konfigurieren 107
VPC-Konfiguration mit Agent AWS Ground Station 108
VPC-Konfiguration mit einem Datenfluss-Endpunkt 111
Amazon einrichten und konfigurieren EC2 113
Im Lieferumfang enthaltene Standardsoftware 114
AWS Ground Station Amazon-Maschinenbilder (AMIs) 114
Arbeiten Sie mit Telemetrie 116
Wie funktioniert Telemetrie 116
Verfügbare Telemetriearten 116
Regionale Verfügbarkeit 117
Telemetrie einrichten 117
Schritt 1: Erstellen Sie die erforderlichen Ressourcen AWS 118
Schritt 2: Erstellen Sie ein TelemetrySinkConfig 120
Schritt 3: Fügen Sie Ihrem Missionsprofil Telemetrie hinzu 120
Schritt 4: Einen Kontakt vereinbaren 120
Nächste Schritte 121
Verstehen Sie Telemetriedaten 121
Überblick über das Datenformat 121
Zeigetelemetrie 122
Telemetrie verfolgen 124
Daten aus dem Kinesis Data Streams Streams-Stream lesen 126
Versionierung und Weiterentwicklung von Schemas 127
Arbeiten Sie mit Kontakten 128
Verstehen Sie den Lebenszyklus von Kontakten 128
AWS Ground Station Status der Kontakte 131
Aufbewahrung von Kontaktdaten 132
Verstehen Sie die Abrechnung mit Kontakten 133
Bandbreitendefinitionen 133
Modi für die Terminplanung 133
CancelContact 133
Szenario 1: Ein einziger Ansprechpartner 134
Szenario 2: Einzelner abgebrochener Kontakt 135
Szenario 3: Einzelnes Duplikat 135

Szenario 4: Kurzes Duplikat 136
Szenario 5: Mehrere Duplikate 137
Szenario 6: Mehrere Stopps 139
Szenario 7: Bodenstation mit mehreren Antennen ohne Duplikat 140
Szenario 8: Bodenstation mit mehreren Antennen und doppelten Kontakten 141
AWS Ground Station digitaler Zwilling 143
Überwachen 144
Automatisieren Sie mit Ereignissen 145
AWS Ground Station Arten von Ereignissen 146
Event-Zeitplan kontaktieren 146
Ephemeriden-Ereignisse 149
API-Aufrufe protokollieren mit CloudTrail 150
AWS Ground Station Informationen in CloudTrail 150
Grundlegendes zu AWS Ground Station Protokolldateieinträgen 151
Metriken mit Amazon anzeigen CloudWatch 153
AWS Ground Station Metriken und Dimensionen 153
Anzeigen von -Metriken 159
Sicherheit 166
Identitäts- und Zugriffsverwaltung 166
Zielgruppe 167
Authentifizierung mit Identitäten 167
Verwalten des Zugriffs mit Richtlinien 169
Wie AWS Ground Station funktioniert mit IAM 170
Beispiele für identitätsbasierte Richtlinien 176
Fehlerbehebung 179
AWS verwaltete Richtlinien 181
AWSGroundStationAgentInstancePolicy 182
AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy 182
Richtlinienaktualisierungen 183
Serviceverknüpfte Rollen verwenden 184
Dienstbezogene Rollenberechtigungen für Ground Station 185
Eine serviceverknüpfte Rolle für Ground Station erstellen 186
Bearbeiten einer serviceverknüpften Rolle für Ground Station 186
Löschen einer serviceverknüpften Rolle für Ground Station 186
Unterstützte Regionen für dienstbezogene Rollen an der Ground Station 187
Fehlerbehebung 187

Datenverschlüsselung im Ruhezustand für AWS Ground Station ... 187
Erstellen eines kundenseitig verwalteten Schlüssels ... 189
Angabe eines vom Kunden verwalteten Schlüssels für AWS Ground Station ... 191
AWS Ground Station Verschlüsselungskontext ... 191
Verschlüsselung im Ruhezustand für TLE- und OEM-Ephemeridendaten ... 191
Verschlüsselung im Ruhezustand für Azimuthöhen-Ephemeriden ... 201
Datenverschlüsselung während der Übertragung für AWS Ground Station ... 210
AWS Ground Station Agenten-Streams ... 211
Datenfluss-Endpunktstreams ... 211
Beispielkonfigurationen von Missionsprofilen ... 212
JPSS-1 — Öffentlicher Rundfunksatellit (PBS) — Evaluierung ... 212
Öffentlicher Rundfunksatellit, der Amazon S3 S3-Datenlieferung nutzt ... 213
Kommunikationswege ... 214
AWS Ground Station Konfigurationen ... 216
AWS Ground Station Missionsprofil ... 217
Es zusammensetzen ... 218
Öffentlicher Rundfunksatellit, der einen Datenflussendpunkt nutzt (Schmalband) ... 219
Kommunikationspfade ... 219
AWS Ground Station Konfigurationen ... 226
AWS Ground Station Missionsprofil ... 227
Es zusammensetzen ... 228
Öffentlicher Rundfunksatellit, der einen Datenflussendpunkt verwendet (demoduliert und dekodiert) ... 230
Kommunikationswege ... 230
AWS Ground Station Konfigurationen ... 237
AWS Ground Station Missionsprofil ... 241
Es zusammensetzen ... 241
Öffentlicher Rundfunksatellit mit AWS Ground Station Agent (Breitband) ... 243
Kommunikationspfade ... 244
AWS Ground Station Konfigurationen ... 255
AWS Ground Station Missionsprofil ... 256
Es zusammensetzen ... 257
Fehlerbehebung ... 260
Problembehandlung bei Kontakten, die Daten an Amazon EC2 liefern ... 260
Schritt 1: Stellen Sie sicher, dass Ihre EC2-Instance läuft ... 261
Schritt 2: Ermitteln Sie den Typ der verwendeten Datenflussanwendung ... 261

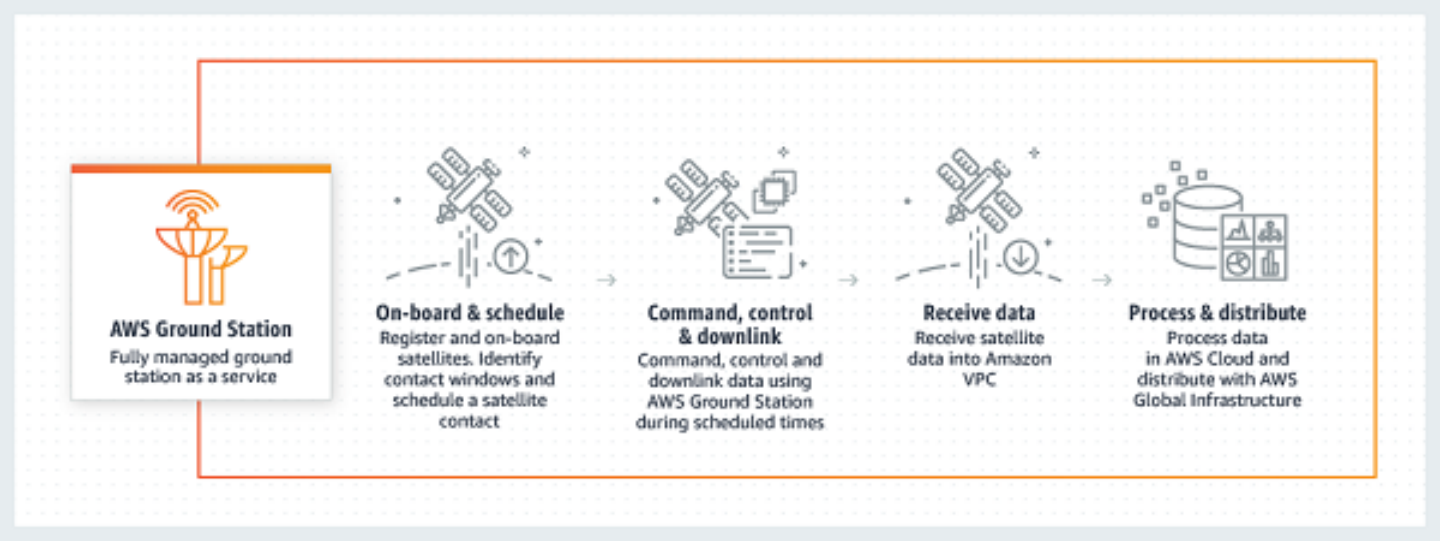
Schritt 3: Stellen Sie sicher, dass die Dataflow-Anwendung ausgeführt wird 261
Schritt 4: Stellen Sie sicher, dass Ihr Dataflow-Anwendungsstream konfiguriert ist 263
Schritt 5: Stellen Sie sicher, dass Sie über genügend verfügbare IP-Adressen im Subnetz Ihrer Empfänger-Instance (en) verfügen 265
Fehlerbehebung bei FEHLGESCHLAGENEN Kontakten 266
Anwendungsfälle von Dataflow Endpoint FAILED 267
AWS Ground Station Anwendungsfälle von Agent FAILED 268
Fehlerbehebung bei FAILED_TO_SCHEDULE-Kontakten 268
Die in Ihrer Antenna Downlink Demod Decode Config angegebenen Einstellungen werden nicht unterstützt 269
Allgemeine Fehlerbehebungsschritte 269
Problembehandlung DataflowEndpointGroups nicht im Zustand GESUND 270
Fehlerbehebung bei ungültigen Ephemeriden 270
Fehler bei der Validierung von Ephemeriden verstehen 270
Häufige Validierungsfehler für TLE-Ephemeriden 271
Häufige Validierungsfehler für OEM-Ephemeriden 272
Häufige Validierungsfehler für Azimut-Elevations-Ephemeriden 272
Fehlerbehebungsschritte 274
Vollständige Fehlercode-Referenz 274
Problembehandlung bei Kontakten, die keine Daten erhalten haben 279
Falsche Downlink-Konfiguration 279
Satellitenmanöver 279
AWS Ground Station Ausfall 280
Fehlerbehebung bei Telemetrie 280
Häufig auftretende Probleme bei der Einrichtung 280
Probleme bei der Telemetrieübertragung 283
Probleme mit dem Datenformat 285
Hilfe erhalten 286
Kontingente und -Einschränkungen 287
Bedingungen für den Service 288
Dokumentverlauf 289
AWS Glossar 295
..... ccxcvi

Was ist AWS Ground Station?

AWS Ground Station ist ein vollständig verwalteter Service, der sichere, schnelle und vorhersehbare Satellitenkommunikation in einer globalen Infrastruktur bietet. Damit AWS Ground Station müssen Sie Ihre eigene Bodenstationsinfrastruktur nicht mehr aufbauen, verwalten oder skalieren. AWS Ground Station ermöglicht es Ihnen, sich auf Innovationen zu konzentrieren und schnell mit neuen Anwendungen zu experimentieren, die Satellitendaten aufnehmen, anstatt Ressourcen für den Bau, Betrieb und die Skalierung Ihrer eigenen Bodenstationen aufzuwenden.

Mithilfe des globalen Glasfasernetzes von AWS mit niedriger Latenz und hoher Bandbreite können Sie innerhalb von Sekunden nach Empfang am Antennensystem mit der Verarbeitung Ihrer Satellitendaten beginnen. Auf diese Weise können Sie Rohdaten innerhalb von Sekunden in verarbeitete Informationen oder analysiertes Wissen umwandeln.

Häufige Anwendungsfälle



AWS Ground Station ermöglicht Ihnen die bidirektionale Kommunikation mit Ihren Satelliten und unterstützt die folgenden Anwendungsfälle:

- Downlink-Daten — Empfangen Sie Daten von Ihren Satelliten, die X-Band- und S-Band-Frequenzen übertragen und in Echtzeit an eine EC2 Amazon-Instance (VITA-49-Format) oder direkt an einen Amazon S3-Bucket in Ihrem Konto (PCAP-Format) gesendet werden. Darüber hinaus können Sie bei Satelliten, die ein unterstütztes Modulations- und Kodierungsschema

verwenden, zwischen dem Empfang von demodulierten und dekodierten Daten oder den Rohdaten der digitalen Zwischenfrequenz (DigIF) (VITA-49-Format) wählen.

- Uplink-Daten — Senden Sie Daten und Befehle an Ihre Satelliten, die S-Band-Frequenzen empfangen, indem Sie DigiF-Daten (VITA-49-Format) zur Übertragung von senden. AWS Ground Station
- Uplink-Echo — Validieren Sie Befehle, die an Ihr Raumschiff gesendet werden, und führen Sie andere fortgeschrittene Aufgaben durch, indem Sie Ihr übertragenes Signal über eine Antenne empfangen, die sich physisch am selben Ort befindet.
- Software Defined Radio (SDR)/Front End Processor (FEP) — Verwenden Sie Ihr vorhandenes SDR, Ihre vorhandenen Wellenformen und generieren and/or FEP, that's capable of running on an Amazon EC2 instance, to process your data in real-time to send/receive Sie Ihre Datenprodukte.
- Telemetrie, Tracking and Command (TT&C) — Führen Sie TT&C mithilfe einer Kombination der zuvor aufgeführten Anwendungsfälle durch, um Ihre Satellitenflotte zu verwalten.
- Regionsübergreifende Datenbereitstellung — Betreiben Sie mehrere gleichzeitige Kontakte mithilfe AWS Ground Station des globalen Antennennetzwerks von einer einzigen AWS-Region aus.
- Digitaler Zwilling — Testplanung, Überprüfung von Konfigurationen und korrekte Fehlerbehandlung zu reduzierten Kosten, ohne die Kapazität der Produktionsantennen zu beanspruchen.

Nächste Schritte

Wir empfehlen, zuerst die folgenden Abschnitte zu lesen:

- Grundlegende AWS Ground Station Konzepte finden Sie unterWie AWS Ground Station funktioniert.
- Informationen zur Einrichtung Ihres Kontos und der zu AWS Ground Station verwendenden Ressourcen finden Sie unterErste Schritte.
- Informationen zur programmgesteuerten Verwendung AWS Ground Station finden Sie in der AWS Ground Station API-Referenz. Die API-Referenz beschreibt alle API-Operationen für AWS Ground Station im Detail. Sie enthält auch Beispiele für Anfragen, Antworten und Fehler für die unterstützten Webdienstprotokolle. Sie können die AWS CLI oder ein AWS SDK in der Sprache Ihrer Wahl verwenden, um Code zu schreiben, der mit AWS Ground Station interagiert.

Wie AWS Ground Station funktioniert

AWS Ground Station betreibt bodengestützte Antennen, um die Kommunikation mit Ihrem Satelliten zu erleichtern. Die physikalischen Eigenschaften der Antennen sind abstrakt und werden als Fähigkeiten bezeichnet. Der physische Standort der Antenne sowie ihre aktuellen Fähigkeiten können in AWS Ground Station Standorte diesem Abschnitt beschrieben werden. Bitte kontaktieren Sie uns über den, AWS Support Center Consolefalls Ihr Anwendungsfall zusätzliche Funktionen, zusätzliche Standortangebote oder genauere Antennenstandorte erfordert.

Um eine der AWS Ground Station Antennen verwenden zu können, müssen Sie einen Termin an einem bestimmten Standort reservieren. Diese Reservierung wird als Kontakt bezeichnet. Um einen Kontakt erfolgreich zu vereinbaren, AWS Ground Station sind zusätzliche Daten erforderlich, um den Erfolg sicherzustellen.

- Ihr Satellit muss an einem oder mehreren Standorten installiert sein. Dadurch wird sichergestellt, dass Sie über die Genehmigung verfügen, die verschiedenen Funktionen am gewünschten Standort zu betreiben.
- Ihr Satellit muss über eine gültige Ephemeride verfügen. Dadurch wird sichergestellt, dass die Antennen eine Sichtlinie haben und während des Kontakts genau auf Ihren Satelliten zeigen können.
- Sie müssen über ein gültiges Missionsprofil verfügen. Auf diese Weise können Sie das Verhalten dieses Kontakts anpassen, einschließlich der Art und Weise, wie Sie Daten an Ihren Satelliten empfangen und an diesen senden. Sie können mehrere Missionsprofile für dasselbe Fahrzeug verwenden, um verschiedene Kontakte zu erstellen, die sich an unterschiedliche Betriebspositionen oder Szenarien anpassen, denen Sie begegnen.

Onboarding per Satellit

Das Onboarding eines Satelliten AWS Ground Station ist ein mehrstufiger Prozess, der Datenerfassung, technische Validierung, Frequenzlizenzierung sowie Integration und Tests umfasst. Der Abschnitt „Satelliten-Onboarding“ des Leitfadens führt Sie durch diesen Prozess.

Zusammensetzung des Missionsprofils

Die Satellitenfrequenzinformationen, Informationen zur Datenebene und andere Details sind in einem Missionsprofil zusammengefasst. Das Missionsprofil ist eine Sammlung von

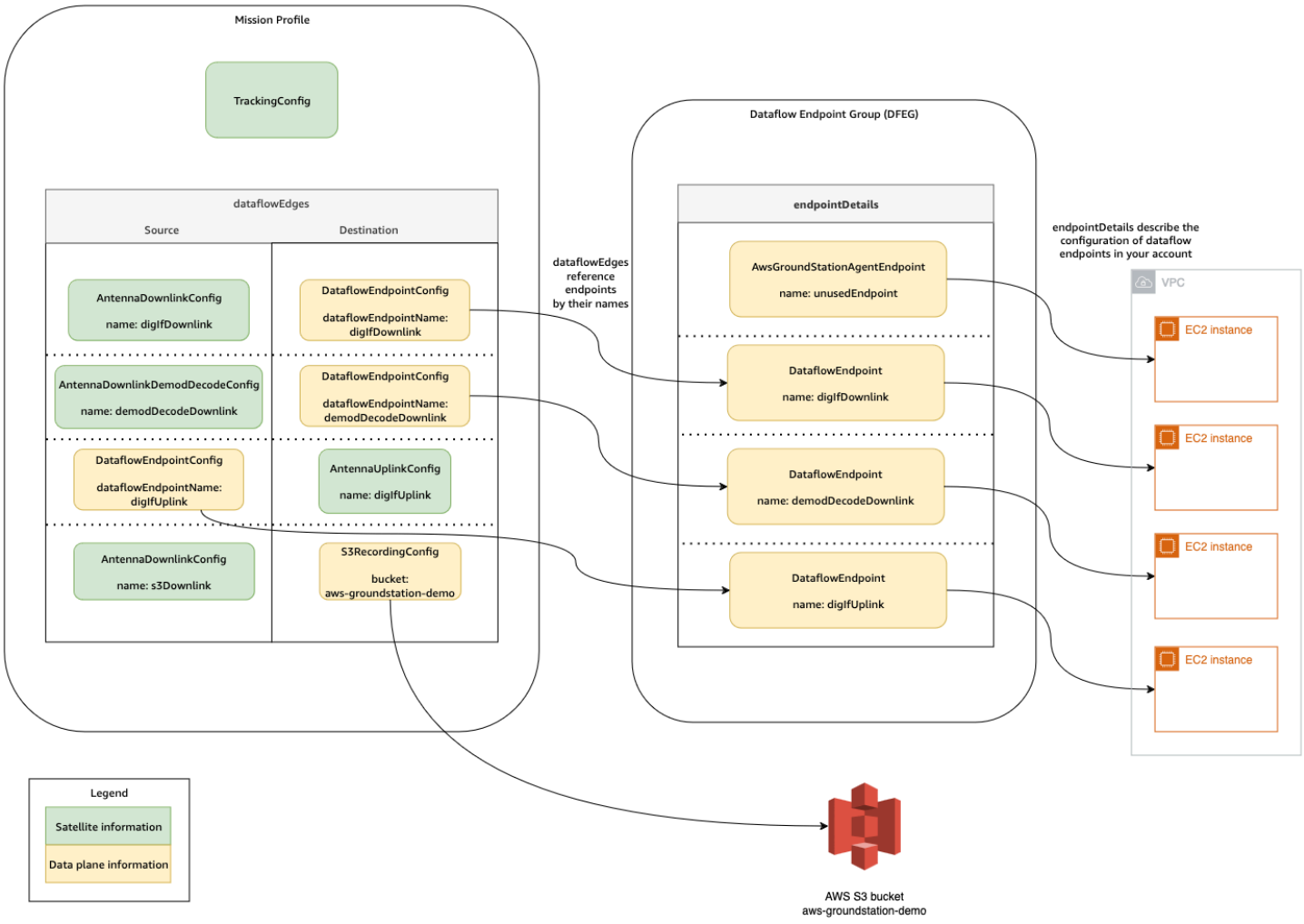
Konfigurationskomponenten. Auf diese Weise können Sie Konfigurationskomponenten je nach Anwendungsfall in verschiedenen Missionsprofilen wiederverwenden. Da Missionsprofile nicht direkt auf einzelne Satelliten verweisen, sondern nur Informationen über ihre technischen Fähigkeiten enthalten, können Missionsprofile auch von mehreren Satelliten mit derselben Konfiguration wiederverwendet werden.

Ein gültiges Missionsprofil verfügt über eine Tracking-Konfiguration und einen oder mehrere Datenflüsse. In der Tracking-Konfiguration wird Ihre Präferenz für die Nachverfolgung während eines Kontakts angegeben. Jedes Konfigurationspaar innerhalb eines Datenflusses legt eine Quelle und ein Ziel fest. Abhängig von Ihrem Satelliten und seinen Betriebsmodi variiert die genaue Anzahl der Datenflüsse in einem Missionsprofil, um Ihre Uplink- und Downlink-Kommunikationspfade sowie alle Aspekte der Datenverarbeitung darzustellen.

- Weitere Informationen zur Konfiguration Ihrer Amazon VPC-, Amazon S3- und EC2 Amazon-Ressourcen, die während eines Kontakts verwendet werden, finden Sie unterMit Datenflüssen arbeiten.
- Einzelheiten zum Verhalten der einzelnen Konfigurationen finden Sie unter. AWS Ground Station Konfigurationen verwenden
- Spezifische Informationen zu allen erwarteten Parametern finden Sie unterAWS Ground Station Missionsprofile verwenden.
- Beispiele dafür, wie verschiedene Missionsprofile zur Unterstützung Ihres Anwendungsfalls erstellt werden können, finden Sie unterBeispielkonfigurationen von Missionsprofilen.

Das folgende Diagramm zeigt ein Beispiel für ein Missionsprofil und die benötigten zusätzlichen Ressourcen. Beachten Sie, dass das Beispiel einen Datenflussendpunkt mit dem Namen UnusedEndpoint zeigt, der für dieses Missionsprofil nicht benötigt wird, um die Flexibilität zu demonstrieren. Das Beispiel unterstützt die folgenden Datenflüsse:

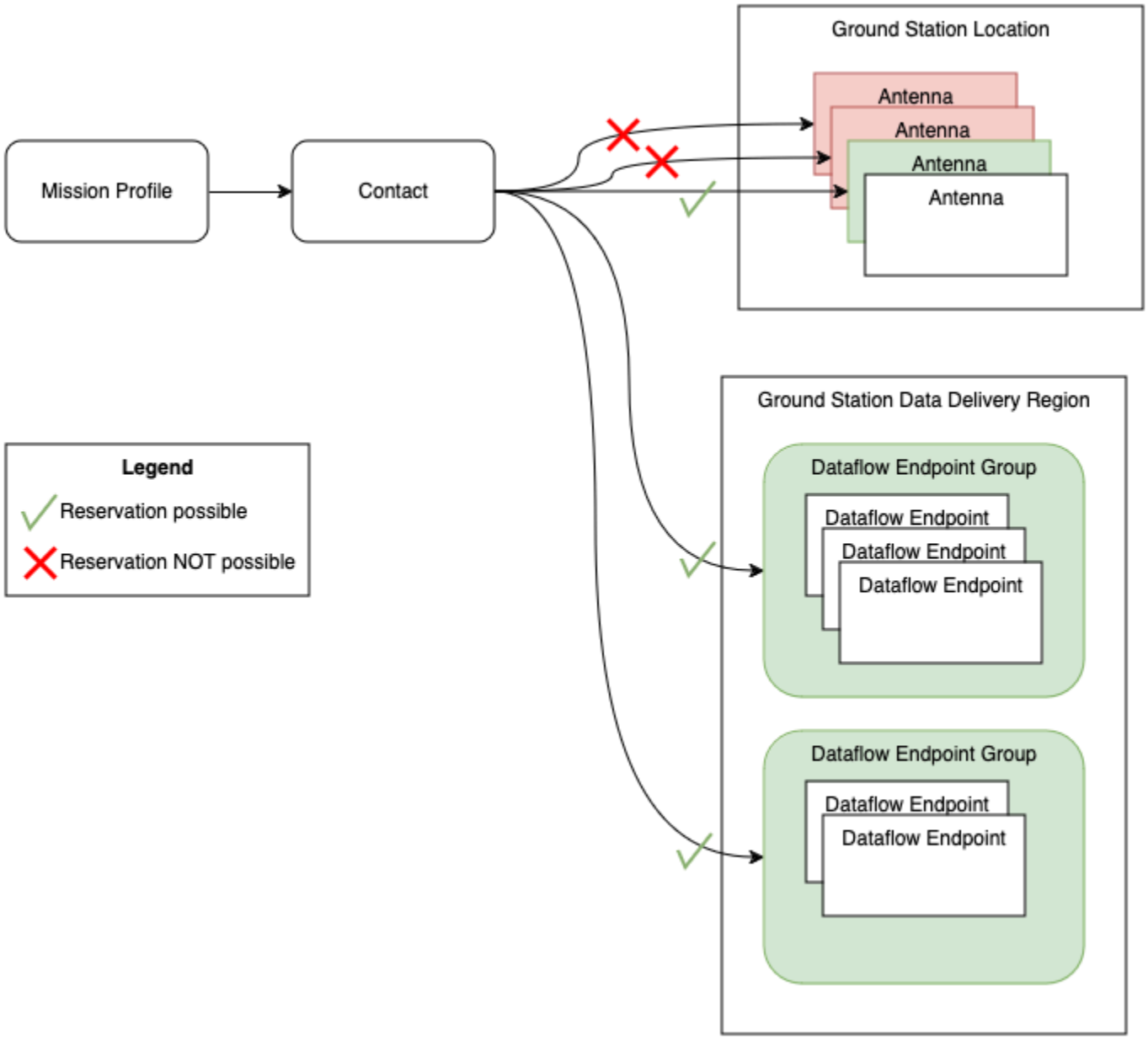
- Synchroner Downlink von digitalen Zwischenfrequenzdaten zu einer EC2 Amazon-Instance, die Sie verwalten. Wird durch den Namen bezeichnet. digIfDownlink
- Asynchroner Downlink von digitalen Zwischenfrequenzdaten zu einem Amazon S3 S3-Bucket. Wird durch den Bucket-Namen bezeichnet. aws-groundstation-demo
- Synchroner Downlink von demodulierten und dekodierten Daten zu einer EC2 Amazon-Instance, die Sie verwalten. Wird durch den Namen bezeichnet. demodDecodeDownlink
- Synchroner Uplink von Daten von einer EC2 Amazon-Instance, die Sie verwalten, zu einer AWS Ground Station verwalteten Antenne. Wird durch den Namen bezeichnet. digIfUplink



Kontaktplanung

Mit einem gültigen Missionsprofil können Sie einen Kontakt zu Ihren an Bord befindlichen Satelliten anfordern. Die Kontaktreservierungsanfrage erfolgt asynchron, damit der globale Antennendienst genügend Zeit hat, um einen einheitlichen Zeitplan für alle AWS beteiligten Regionen einzuhalten. Während dieses Vorgangs werden verschiedene Antennen am gewünschten Standort der Bodenstation überprüft, um festzustellen, ob sie verfügbar und in der Lage sind, den Kontakt zu verarbeiten. Während dieses Vorgangs werden auch Ihre konfigurierten Datenflussendpunkte bewertet, um ihre Verfügbarkeit zu ermitteln. Während dieser Evaluierung wird der Kontaktstatus in SCHEDULING angezeigt.

Dieser asynchrone Planungsprozess wird innerhalb von fünf Minuten nach der Anfrage abgeschlossen, in der Regel jedoch innerhalb einer Minute. Bitte überprüfen Sie Automatisieren Sie AWS Ground Station mit Ereignissen die ereignisbasierte Überwachung während der Terminplanung.



Kontakte, die durchgeführt werden können und verfügbar sind, führen zu geplanten Kontakten. Bei einem geplanten Kontakt wurden die Ressourcen, die für die Durchführung Ihres Kontakts benötigt werden, für die erforderlichen AWS-Regionen reserviert, wie in Ihrem Missionsprofil definiert. Kontakte, die nicht ausgeführt werden können oder bei denen Teile nicht verfügbar sind, führen zu FAILED_TO_SCHEDULE-Kontakten. Einzelheiten zum Debuggen finden Sie unter. Fehlerbehebung bei FAILED_TO_SCHEDULE-Kontakten

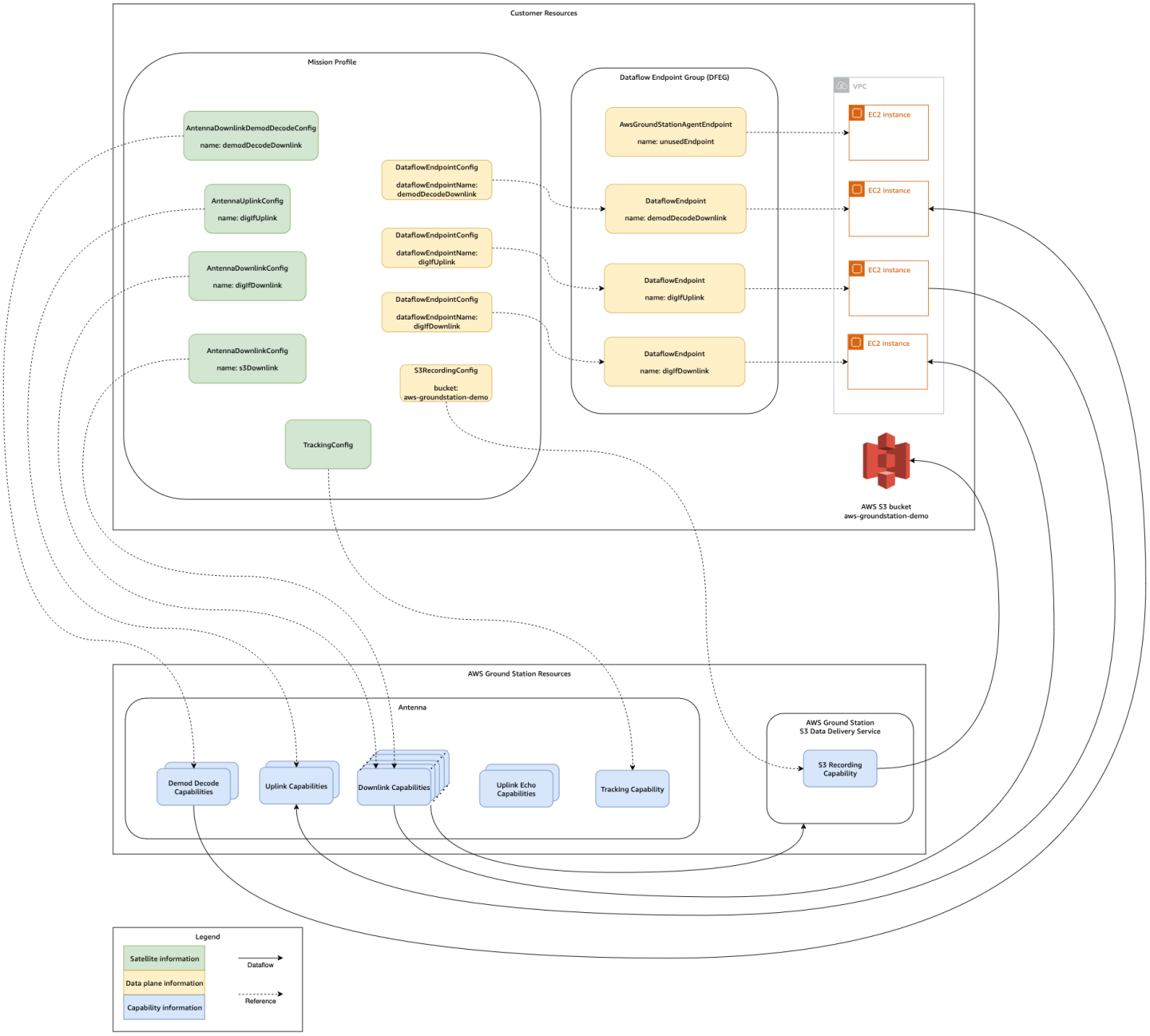
Ausführung des Kontakts

AWS Ground Station orchestriert Ihre von AWS verwalteten Ressourcen während Ihrer Kontaktreservierung automatisch. Falls zutreffend, sind Sie für die Orchestrierung von EC2 Ressourcen verantwortlich, die in Ihrem Missionsprofil als Datenfluss-Endpunkte definiert sind. AWS Ground Station bietet EventBridge AWS-Events zur Automatisierung der Orchestrierung Ihrer Ressourcen zur Kostensenkung. Weitere Details finden Sie unter Automatisieren Sie AWS Ground Station mit Ereignissen.

Während des Kontakts werden Telemetriedaten über Ihre Kontaktleistung an AWS CloudWatch übermittelt. Informationen darüber, wie Sie Ihren Kontakt während der Ausführung überwachen können, finden Sie unterVerstehen Sie die Überwachung mit AWS Ground Station.

Das folgende Diagramm setzt das vorherige Beispiel fort und zeigt dieselben Ressourcen, die während des Kontakts orchestriert wurden.

> **Note**
>
> In diesem Beispiel wurden nicht alle Antennenfunktionen verwendet. Beispielsweise stehen an jeder Antenne mehr als ein Dutzend Antennen-Downlink-Funktionen zur Verfügung, die mehrere Frequenzen und Polarisationen unterstützen. Weitere Informationen zur Anzahl der von AWS Ground Station Antennen verfügbaren Funktionstypen sowie zu den unterstützten Frequenzen und Polarisationen finden Sie unter. AWS Ground Station Funktionen der Website



Am Ende Ihres Kontakts AWS Ground Station wird die Leistung Ihres Kontakts bewertet und der endgültige Kontaktstatus festgelegt. Bei Kontakten, bei denen keine Fehler festgestellt wurden, wird der Kontaktstatus ABGESCHLOSSEN angezeigt. Kontakte, bei denen Servicefehler während des Kontakts zu Problemen bei der Datenübermittlung geführt haben, AWS_FAILEDerhalten einen Status. Kontakte, bei denen Kunden- oder Benutzerfehler während des Kontakts zu Problemen bei der Datenübermittlung geführt haben, erhalten den Status FEHLGESCHLAGEN. Fehler außerhalb der Kontaktzeit, also während des Pre-Passes oder Post-Passes, werden bei der Entscheidung nicht berücksichtigt.

Weitere Informationen finden Sie unter Verstehen Sie den Lebenszyklus von Kontakten.

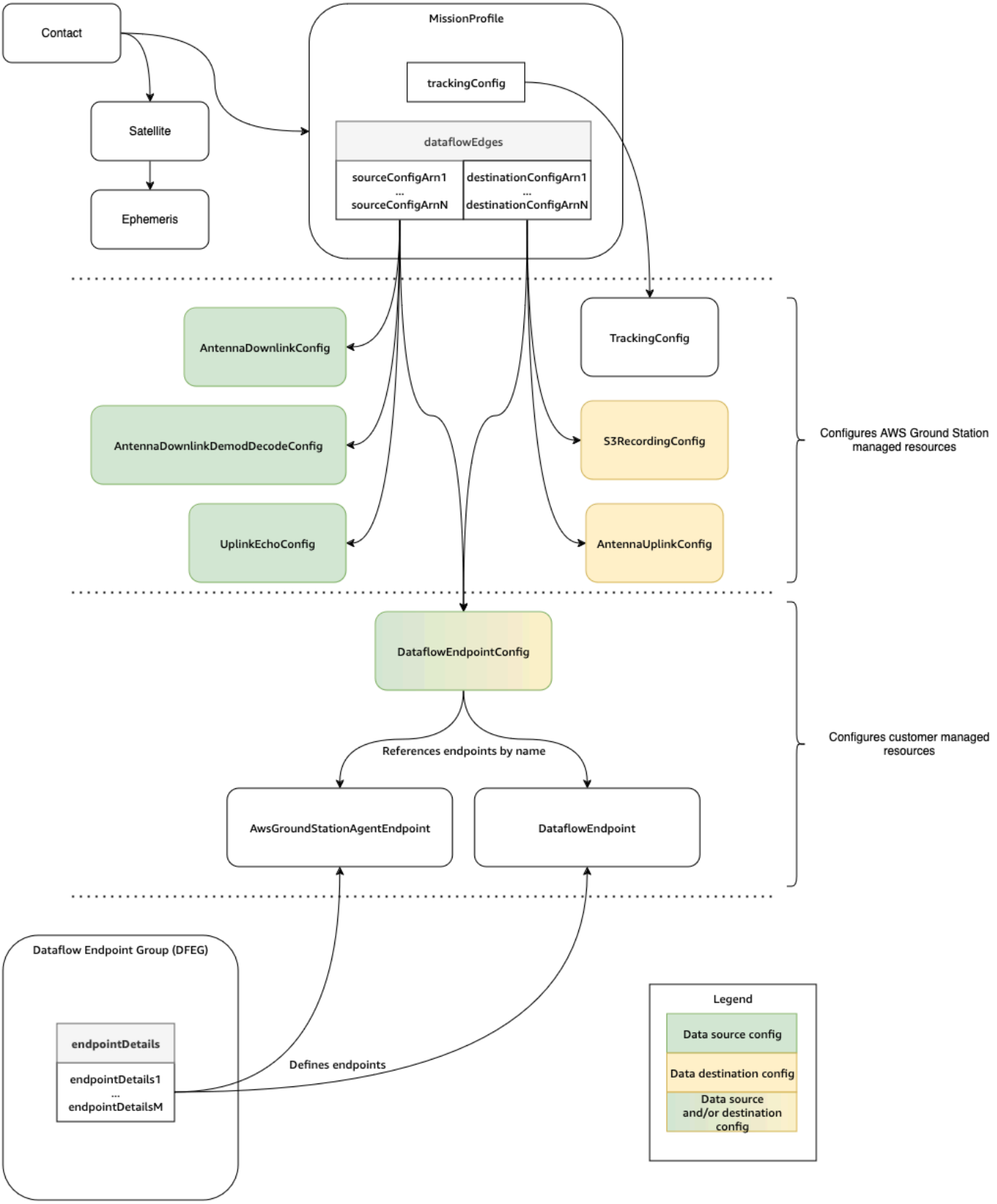
Digitaler Zwilling

Mit der digitalen Zwillingsfunktion für AWS Ground Station können Sie Kontakte für virtuelle Bodenstationen planen. Diese virtuellen Bodenstationen sind exakte Nachbildungen von Bodenstationen in der Produktion, einschließlich Antennenkapazitäten, Standortmasken und tatsächlichen GPS-Koordinaten. Mit der digitalen Zwillingsfunktion können Sie Ihren Workflow zur Kontaktorchestrierung zu einem Bruchteil der Kosten testen, die im Vergleich zu Bodenstationen in der Produktion anfallen. Weitere Informationen finden Sie unter Verwenden Sie die AWS Ground Station digitale Zwillingsfunktion.

AWS Ground Station Kernkomponenten verstehen

Dieser Abschnitt enthält detaillierte Definitionen für die Kernkomponenten von AWS Ground Station.

Das folgende Diagramm zeigt die Kernkomponenten von AWS Ground Station und wie sie zueinander in Beziehung stehen. Die Pfeile geben die Richtung der Abhängigkeiten zwischen den Komponenten an, wobei jede Komponente auf ihre Abhängigkeiten verweist.


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

In den folgenden Themen werden die AWS Ground Station Kernkomponenten detailliert beschrieben.

Themen

- AWS Ground Station Missionsprofile verwenden
- AWS Ground Station Konfigurationen verwenden
- AWS Ground Station Dataflow-Endpunktgruppen verwenden
- AWS Ground Station Agent verwenden

AWS Ground Station Missionsprofile verwenden

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

Missionsprofile können von allen Satelliten gemeinsam genutzt werden, die dieselben Funkeigenschaften aufweisen. Sie können zusätzliche Datenfluss-Endpunktgruppen erstellen, um die maximale Anzahl gleichzeitiger Kontakte zu begrenzen, die Sie für Ihre Konstellation herstellen möchten.

Tracking-Konfigurationen werden als eindeutiges Feld innerhalb des Missionsprofils angegeben. Tracking-Konfigurationen werden verwendet, um Ihre Präferenz für die Verwendung von Programm-Tracking und Auto-Tracking während Ihres Kontakts anzugeben. Weitere Informationen finden Sie unter Nachverfolgungs-Config.

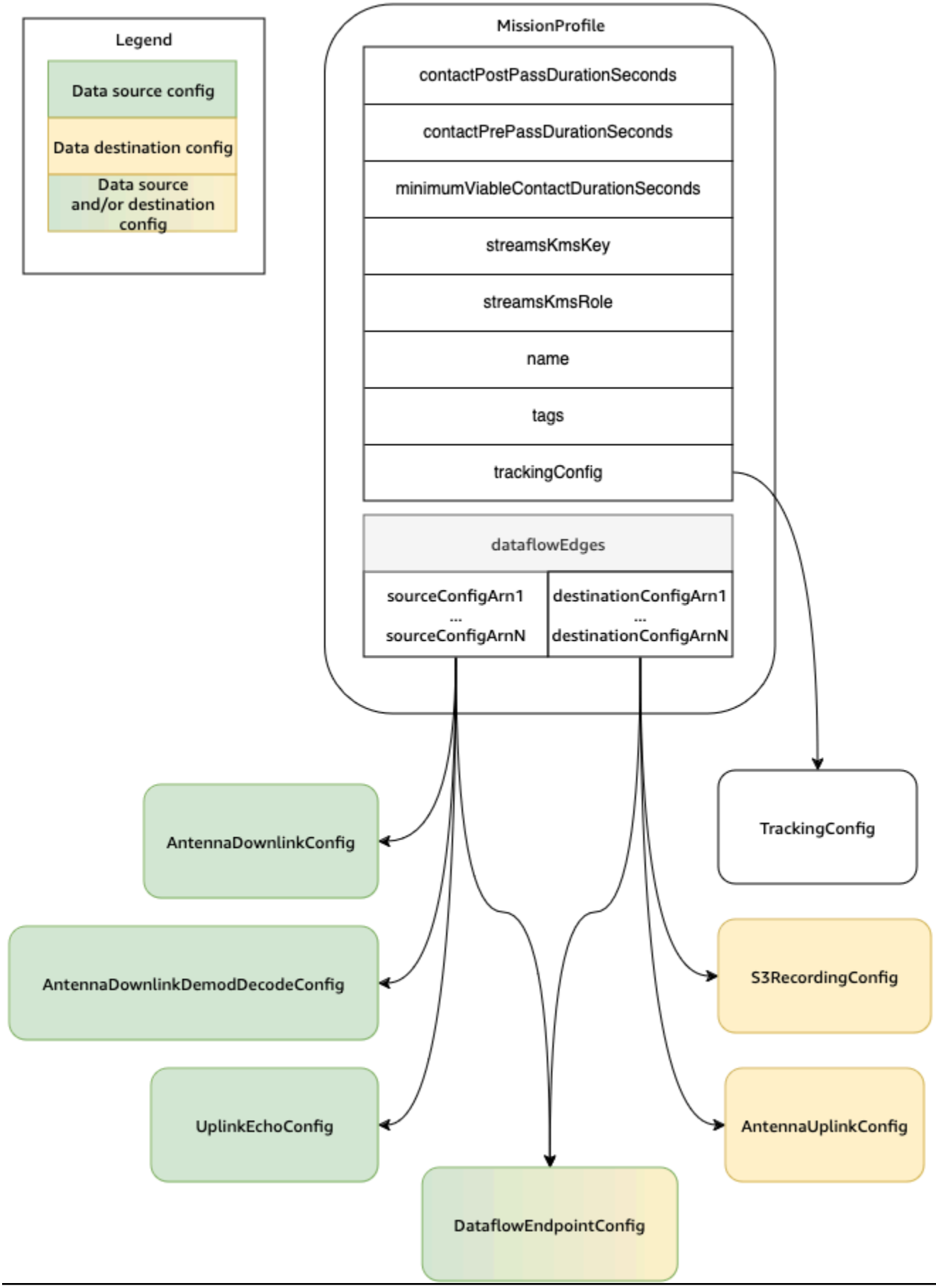
Alle anderen Konfigurationen sind im `dataflowEdges` Feld des Missionsprofils enthalten. Diese Konfigurationen können als Datenflussknoten betrachtet werden, die jeweils eine AWS Ground Station verwaltete Ressource darstellen, die Daten senden oder empfangen kann, und die zugehörige Konfiguration. Das `dataflowEdges` Feld definiert, welche Quell- und Zieldatenflussknoten (Konfigurationen) benötigt werden. Ein einzelner Datenflussrand ist eine Liste von zwei konfigurierten Amazon-Ressourcennamen (ARNs) — der erste ist die Quellkonfiguration und der zweite ist die Zielkonfiguration. Indem Sie eine Datenfluss-Kante zwischen zwei Konfigurationen angeben, geben Sie an, AWS Ground Station von wo und wohin Daten während eines Kontakts fließen sollen. Weitere Informationen finden Sie unter AWS Ground Station Konfigurationen verwenden.

`contactPostPassDurationSeconds`Mit `contactPrePassDurationSeconds` und können Sie im Verhältnis zum Kontakt die Zeiten angeben, zu denen Sie eine CloudWatch Ereignisbenachrichtigung erhalten. Eine Zeitleiste der Ereignisse im Zusammenhang mit Ihrem Kontakt finden Sie unterVerstehen Sie den Lebenszyklus von Kontakten.

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

Die `streamsKmsRole` und `streamsKmsKey` werden verwendet, um die Verschlüsselung zu definieren, die AWS Ground Station für Ihre Datenübermittlung mit AWS Ground Station Agent verwendet wird. Weitere Informationen finden Sie unter Datenverschlüsselung während der Übertragung für AWS Ground Station.

Das `telemetrySinkConfigArn` Feld ist optional und ermöglicht es Ihnen, AWS Ground Station Telemetrie bei Kontakten zu aktivieren. Wenn angegeben, werden während der Ausführung Ihrer Kontakte Telemetriedaten nahezu in Echtzeit an Ihr Konto AWS Ground Station gestreamt. Weitere Informationen zur Konfiguration und Verwendung von Telemetrie finden Sie unter. Arbeiten Sie mit Telemetrie


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

Eine vollständige Liste der Parameter und Beispiele finden Sie in der folgenden Dokumentation.

- AWS::GroundStation::MissionProfile CloudFormation Ressourcentyp

AWS Ground Station Konfigurationen verwenden

Konfigurationen sind Ressourcen, mit denen AWS Ground Station Sie die Parameter für jeden Aspekt Ihres Kontakts 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. Die Konfigurationen können in drei Kategorien eingeteilt werden:

- Konfigurationen nachverfolgen
- Dataflow-Konfigurationen
- Telemetriekonfigurationen

A TrackingConfigist die einzige Art von Tracking-Konfiguration. Sie wird verwendet, um die Autotrack-Einstellung der Antenne während eines Kontakts zu konfigurieren, und ist in einem Missionsprofil erforderlich.

Die Konfigurationen, die in einem Missionsprofil-Datenfluss verwendet werden können, können als Datenflussknoten betrachtet werden, die jeweils eine AWS Ground Station verwaltete Ressource darstellen, die Daten senden oder empfangen kann. Ein Missionsprofil erfordert mindestens ein Paar dieser Konfigurationen, wobei eine für eine Datenquelle und eine für ein Ziel steht. Diese Konfigurationen sind in der folgenden Tabelle zusammengefasst.

Name der Config	Quelle/Ziel des Datenflusses
AntennaDownlinkConfig	Quelle
AntennaDownlinkDemodDecodeConfig	Quelle
UplinkEchoConfig	Quelle
S3 RecordingConfig	Ziel
AntennaUplinkConfig	Ziel

Name der Config	Quelle/Ziel des Datenflusses
DataflowEndpointConfig	and/or Quellziel

A TelemetrySinkConfigist die einzige Art der Telemetriekonfiguration. Sie wird verwendet, um zu konfigurieren, wohin Telemetriedaten während eines Kontakts übermittelt werden, und ist in einem Missionsprofil optional. Falls enthalten, werden Telemetriedaten während der Ausführung Ihrer Kontakte nahezu in Echtzeit an Ihr Konto AWS Ground Station gestreamt.

In der folgenden Dokumentation finden Sie weitere Informationen dazu, wie Sie Operationen an Konfigurationen mithilfe CloudFormation der oder der AWS Command Line Interface AWS Ground Station API ausführen. Links zur Dokumentation für bestimmte Konfigurationstypen finden Sie ebenfalls unten.

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

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.

AWS Ground Station verwendet programmatisches Tracking, das auf der Grundlage Ihrer Ephemeride anzeigt, wenn Autotrack nicht verwendet wird. Einzelheiten Verstehe, wie AWS Ground Station Ephemeriden verwendet werden zur Konstruktion von Ephemeriden finden Sie unter.

Autotrack verwendet die Programmverfolgung, bis das erwartete Signal gefunden wird. Sobald dies der Fall ist, wird die Überwachung auf der Grundlage der Signalstärke fortgesetzt.

In der folgenden Dokumentation finden Sie weitere Informationen zur Durchführung von Vorgängen zur Überwachung von Konfigurationen mithilfe CloudFormation der AWS Command Line Interface 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 Antennen-Downlink-Konfigurationen verwenden, um die Antenne während Ihres Kontakts für den Downlink zu konfigurieren. Sie bestehen aus einer Frequenzkonfiguration, die die Frequenz, Bandbreite und Polarisation festlegt, die während Ihres Downlink-Kontakts verwendet werden sollen.

Diese Konfiguration stellt einen Quellknoten in einem Datenfluss dar. Es ist für die Digitalisierung von Hochfrequenzdaten verantwortlich. Daten, die von diesem Knoten gestreamt werden, folgen dem Data/IP Signalformat. Ausführlichere Informationen zum Konstruieren von Datenflüssen mit dieser Konfiguration finden Sie unter Mit Datenflüssen arbeiten

Wenn Ihr Downlink-Anwendungsfall eine Demodulation oder Dekodierung erfordert, finden Sie weitere Informationen unter. Antennen-Downlink-Demod-Decode-Config

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

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

Antennen-Downlink-Demod-Decode-Config

Antennen-Downlink-Demod-Dekodierungskonfigurationen sind ein komplexerer und anpassbarer Konfigurationstyp, mit dem Sie Downlink-Kontakte mit Demodulationsdekodierung ausführen können. and/or Wenn Sie daran interessiert sind, diese Art von Kontakten auszuführen, öffnen Sie bitte ein

Ticket über die. AWS Support AWS Support Center Console Wir helfen Ihnen, die richtige Config und das richtige Missionsprofil für Ihren Anwendungsfall zu definieren.

Diese Konfiguration stellt einen Quellknoten in einem Datenfluss dar. Es ist verantwortlich für die Digitalisierung von Hochfrequenzdaten und die Durchführung der Demodulation und Decodierung wie angegeben. Daten, die von diesem Knoten gestreamt werden, folgen dem Daten-/IP-Format. Demodulated/Decoded Ausführlichere Informationen zum Erstellen von Datenflüssen mit dieser Konfiguration finden Sie unter Mit Datenflüssen arbeiten

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

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

Antennen-Uplink-Config

Sie können die Antennen-Uplink-Konfigurationen verwenden, um die Antenne während Ihres Kontakts für den Uplink zu konfigurieren. Sie bestehen aus einer Frequenzkonfiguration mit Frequenz, Polarisation und effektiver isotroper Zielstrahlungsleistung (EIRP). Hinweise zur Konfiguration eines Kontakts für Uplink-Loopback finden Sie unter. Antennen-Uplink-Echo-Config

Diese Konfiguration stellt einen Zielknoten in einem Datenfluss dar. Es wandelt das bereitgestellte digitalisierte Hochfrequenzdatensignal in ein analoges Signal um und sendet es an Ihren Satelliten zum Empfang aus. Es wird erwartet, dass Daten, die zu diesem Knoten gestreamt werden, das Data/IP Signalformat erfüllen. Ausführlichere Informationen zum Erstellen von Datenflüssen mit dieser Konfiguration finden Sie unter Mit Datenflüssen arbeiten

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

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

Antennen-Uplink-Echo-Config

Uplink-Echo-Configs teilen der Antenne mit, wie ein Uplink-Echo ausgeführt werden soll. Ein Uplink-Echo kann verwendet werden, um Befehle, die an Ihr Raumschiff gesendet werden, zu validieren und andere fortgeschrittene Aufgaben auszuführen. Dies wird erreicht, indem das von der AWS Ground Station Antenne (d. h. dem Uplink) tatsächlich übertragene Signal aufgezeichnet wird. Dadurch wird das von der Antenne an Ihren Datenflussendpunkt gesendete Signal als Echo wiedergegeben und sollte mit dem übertragenen Signal übereinstimmen. 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.

Diese Konfiguration stellt einen Quellknoten in einem Datenfluss dar. Daten, die von diesem Knoten gestreamt werden, entsprechen dem Signalformat. Data/IP Ausführlichere Informationen zum Konstruieren von Datenflüssen mit dieser Konfiguration finden Sie unter Mit Datenflüssen arbeiten

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

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

Datenflussendpunkt-Config

> **Note**
>
> Dataflow-Endpunktkonfigurationen werden nur für die Datenlieferung an Amazon EC2 und nicht für die Datenlieferung an Amazon S3 verwendet.

Sie können Datenfluss-Endpunktkonfigurationen verwenden, um anzugeben, welcher Datenflussendpunkt in einer Datenfluss-Endpunktgruppe von welchem oder zu welchem Datenfluss Sie während eines Kontakts möchten. Die beiden Parameter einer Datenflussendpunktkonfiguration geben den Namen und die Region des Datenflussendpunkts an. AWS Ground Station Analysiert bei der Reservierung eines Kontakts das von Ihnen angegebene Missionsprofil und versucht, eine Datenfluss-Endpunktgruppe innerhalb der AWS Region zu finden, die alle Datenfluss-Endpunkte

enthält, die in den Datenfluss-Endpunktkonfigurationen in Ihrem Missionsprofil angegeben sind. Wenn eine geeignete Datenfluss-Endpunktgruppe gefunden wird, erhält der Kontakt den Status SCHEDULED, andernfalls erhält er den Status FAILED_TO_SCHEDULE. Weitere Informationen zu den möglichen Status eines Kontakts finden Sie unter. AWS Ground Station Status der Kontakte

Die `dataflowEndpointName` Eigenschaft einer Datenfluss-Endpunktkonfiguration gibt an, welcher Datenflussendpunkt in einer Datenfluss-Endpunktgruppe zu welchem oder von welchem Datenfluss während eines Kontakts übertragen wird.

Die `dataflowEndpointRegion` Eigenschaft gibt an, in welcher Region sich der Datenflussendpunkt befindet. Wenn in Ihrer Datenfluss-Endpunktkonfiguration eine Region angegeben ist, AWS Ground Station wird nach einem Datenfluss-Endpunkt in der angegebenen Region gesucht. Wenn keine Region angegeben ist, AWS Ground Station wird standardmäßig die Region der Bodenstation des Kontakts verwendet. Ein Kontakt gilt als regionsübergreifender Datenlieferkontakt, wenn die Region Ihres Datenflussendpunkts nicht mit der Region der Bodenstation des Kontakts übereinstimmt. Weitere Informationen Mit Datenflüssen arbeiten zu regionsübergreifenden Datenflüssen finden Sie unter.

Tipps dazu, wie unterschiedliche Benennungsschemas für Ihre Datenflüsse Ihrem Anwendungsfall zugute kommen können, finden AWS Ground Station Dataflow-Endpunktgruppen verwenden Sie unter.

Ausführlichere Informationen zum Erstellen von Datenflüssen mit dieser Konfiguration finden Sie unter Mit Datenflüssen arbeiten

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

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

Amazon S3 S3-Aufnahmekonfiguration

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

Diese Konfiguration stellt einen Zielknoten in einem Datenfluss dar. Dieser Knoten kapselt eingehende Daten vom Quellknoten des Datenflusses in PCAP-Daten ein. Ausführlichere Informationen zum Konstruieren von Datenflüssen mit dieser Konfiguration finden Sie unter Mit Datenflüssen arbeiten

Sie können S3-Aufzeichnungskonfigurationen verwenden, um einen Amazon S3 S3-Bucket anzugeben, an den herunterverknüpfte Daten zusammen mit der verwendeten Namenskonvention geliefert werden sollen. Im Folgenden werden Einschränkungen und Einzelheiten zu diesen Parametern angegeben:

- Der Name des Amazon S3 S3-Buckets muss mit beginnen`aws-groundstation`.
- Die IAM-Rolle muss über eine Vertrauensrichtlinie verfügen, die es dem `groundstation.amazonaws.com` Dienstprinzipal ermöglicht, die Rolle zu übernehmen. Ein Beispiel finden Sie im Abschnitt „Beispiel für eine Vertrauensrichtlinie“ weiter unten. Während der Konfigurationserstellung ist die Konfigurationsressourcen-ID nicht vorhanden. Die Vertrauensrichtlinie muss stattdessen ein Sternchen (`*`) verwenden *`your-config-id`* und kann nach der Erstellung mit der Konfigurationsressourcen-ID aktualisiert werden.

Beispiel für eine Vertrauensrichtlinie

Weitere Informationen zur Aktualisierung der Vertrauensrichtlinie einer Rolle finden Sie unter Verwaltung von IAM-Rollen im IAM-Benutzerhandbuch.

JSON

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

```
            "Principal": {
                "Service": "groundstation.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "999999999999"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:groundstation:us-
east-1:999999999999:config/s3-recording/your-config-id"
                }
            }
        }
    ]
}
```

- Die IAM-Rolle muss über eine IAM-Richtlinie verfügen, die es der Rolle ermöglicht, die Aktion für den Bucket und `s3:PutObject` die `s3:GetBucketLocation` Aktion für die Objekte des Buckets auszuführen. Wenn der Amazon S3 S3-Bucket über eine Bucket-Richtlinie verfügt, muss die Bucket-Richtlinie auch der IAM-Rolle die Ausführung dieser Aktionen ermöglichen. Ein Beispiel finden Sie im Abschnitt „Beispiel für eine Rollenrichtlinie“ weiter unten.

Beispiel für eine Rollenrichtlinie

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

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation"
      ],
      "Resource": [
```

```
        "arn:aws:s3:::your-bucket-name"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3:::your-bucket-name/*"
      ]
    }
  ]
}
```

- Das Präfix wird bei der Benennung des S3-Datenobjekts verwendet. Sie können optionale Schlüssel zur Ersetzung angeben. Diese Werte werden durch die entsprechenden Informationen aus Ihren Kontaktdaten ersetzt. Zum Beispiel `{satellite_id}/{year}/{month}/{day}` wird das Präfix von ersetzt und würde zu einer Ausgabe wie `fake_satellite_id/2021/01/10`

  Optionale Schlüssel für die Ersetzung: `{satellite_id}` `{config-name}` || `{config-id}` | `{year}` | `{month}` | `{day}`

In der folgenden Dokumentation finden Sie weitere Informationen zur Ausführung von Vorgängen an S3-Aufzeichnungskonfigurationen mithilfe CloudFormation der AWS Command Line Interface oder der AWS Ground Station API.

- AWS::GroundStation::Config S3-Eigenschaft RecordingConfig CloudFormation
- AWS CLI Konfigurationsreferenz (siehe `s3RecordingConfig -> (structure)` Abschnitt)
- RecordingConfig S3-API-Referenz

Telemetrie Sink Config

Mithilfe von Telemetriesenkkonfigurationen können Sie angeben, wohin die Telemetriedaten bei Satellitenkontakten übertragen werden sollen. Eine Konfiguration für Telemetrieempfänger ist optional und wird Ihrem Missionsprofil hinzugefügt, um telemetriefähige Kontakte zu planen. Im Folgenden werden Einschränkungen und Einzelheiten zu diesen Parametern festgelegt:

- Die IAM-Rolle muss über eine Vertrauensrichtlinie verfügen, die es dem `groundstation.amazonaws.com` Dienstprinzipal ermöglicht, die Rolle zu übernehmen. Ein Beispiel finden Sie im Abschnitt „Beispiel für eine Vertrauensrichtlinie“ weiter unten.

Beispiel für eine Vertrauensrichtlinie

Weitere Informationen zur Aktualisierung der Vertrauensrichtlinie einer Rolle finden Sie unter Verwaltung von IAM-Rollen im IAM-Benutzerhandbuch.

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

- Die IAM-Rolle muss über eine IAM-Richtlinie verfügen, die es der Rolle ermöglicht`kinesis:DescribeStream`, die `kinesis:PutRecord` und `kinesis:PutRecords` Aktionen im Stream auszuführen. Ein Beispiel finden Sie im Abschnitt „Beispiel für eine Rollenrichtlinie“ weiter unten.

Beispiel für eine Rollenrichtlinie

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

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kinesis:DescribeStream",
        "kinesis:PutRecord",
```

```
        "kinesis:PutRecords"
      ],
      "Resource": "arn:aws:kinesis:us-east-2:999999999999:stream/your-stream-name"
    }
  ]
}
```

Wenn Sie Ihrem Missionsprofil eine Telemetrie-Senkenkonfiguration hinzufügen, AWS Ground Station werden bei Kontakten Telemetriedaten an Ihr Konto gestreamt. Weitere Informationen zu Telemetriearten, zum Datenformat und zur Einrichtung der erforderlichen AWS Ressourcen finden Sie unter. Arbeiten Sie mit Telemetrie

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

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

AWS Ground Station Dataflow-Endpunktgruppen verwenden

Datenfluss-Endpunkte definieren den Ort, an den die Daten bei Kontakten synchron gestreamt oder von dort gestreamt werden sollen. 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.

Gruppenversionen von Dataflow-Endpunkten

AWS Ground Station unterstützt zwei Versionen von Datenfluss-Endpunktgruppen:

- DataflowEndpointGroup- Die ursprüngliche Implementierung, die Uplink und Downlink über einen Datenfluss-Endpunkt und nur Downlink für einen Agent-Endpunkt unterstützt AWS Ground Station

- DataflowEndpointGroupV2 — Aktualisierte Version, die sowohl Uplink- als auch Downlink-Datenflüsse für Agenten-Endpunkte mit verbesserter Übersichtlichkeit und Funktionalität unterstützt AWS Ground Station

Vergleich der Dataflow-Endpunktgruppen

Feature	DataflowEndpointGroup	DataflowEndpointGroupV2
Unterstützte Endpunkttypen	DataflowEndpoint, AwsGroundStationAgentEndpoint	DownlinkAwsGroundStationAgentEndpoint, UplinkAwsGroundStationAgentEndpoint
Endpunkte, die Uplink unterstützen	DataflowEndpoint	UplinkAwsGroundStationAgentEndpoint
Endpunkte, die Downlink unterstützen	DataflowEndpoint, AwsGroundStationAgentEndpoint	DownlinkAwsGroundStationAgentEndpoint

DataflowEndpointGroupV2 wurde entwickelt, um Uplink-Datenflüsse zu unterstützen und die Sprache, die Datenfluss-Endpunktgruppen umgibt, klarer zu gestalten. Wir empfehlen für alle neuen UplinkAwsGroundStationAgentEndpointAnwendungsfälle die Verwendung von DownlinkAwsGroundStationAgentEndpointEndpunkten mit V2. DataflowEndpointGroup DataflowEndpointGroup wird aus Gründen der Abwärtskompatibilität weiterhin unterstützt, aber DataflowEndpointGroup V2 bietet erweiterte Funktionen und klarere Konfigurationsoptionen.

> **Tip**
>
> Die Datenfluss-Endpunkte werden bei der Ausführung von Kontakten durch einen Namen Ihrer Wahl identifiziert. Diese Namen müssen nicht für das gesamte Konto eindeutig sein. Auf diese Weise können mehrere Kontakte über verschiedene Satelliten und Antennen gleichzeitig mit demselben Missionsprofil ausgeführt werden. Dies kann nützlich sein, wenn Sie über eine Konstellation von Satelliten verfügen, die dieselben Betriebseigenschaften aufweisen. Sie können die Anzahl der Datenfluss-Endpunktgruppen so skalieren, dass sie der maximalen Anzahl gleichzeitiger Kontakte entspricht, die Ihre Satellitenkonstellation benötigt.

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 unterschiedlichen Datenfluss-Endpunktgruppen ausgeführt werden.

> **Important**
>
> Dataflow-Endpunktgruppen müssen in der HEALTHY Lage sein, Kontakte mithilfe dieser Gruppen zu planen. Informationen zur Fehlerbehebung bei Dataflow-Endpunktgruppen, die sich nicht in einem HEALTHY bestimmten Status befinden, finden Sie unter. Problembehandlung DataflowEndpointGroups nicht im Zustand GESUND

In der folgenden Dokumentation finden Sie weitere Informationen zur Ausführung von Vorgängen an Datenfluss-Endpunktgruppen mithilfe CloudFormation der oder der API AWS Command Line Interface. AWS Ground Station

- AWS::GroundStation::DataflowEndpointGroup CloudFormation Ressourcentyp
- Referenz zur Dataflow-Endpunktgruppe AWS CLI
- API-Referenz für Dataflow Endpoint Group

Datenflussendpunkte

Die Mitglieder einer Datenfluss-Endpunktgruppe sind Datenfluss-Endpunkte. Die unterstützten Endpunkttypen hängen davon ab, welche Version der Datenfluss-Endpunktgruppe Sie verwenden.

DataflowEndpointGroup Endpunkte

DataflowEndpointGroup unterstützt Uplink und Downlink unter Verwendung eines Datenfluss-Endpunkts und nur Downlink für einen Agent-Endpunkt.AWS Ground Station Für beide Arten von Endpunkten erstellen Sie die unterstützenden Konstrukte (z. B. IP-Adressen), bevor Sie die Datenfluss-Endpunktgruppe erstellen. Empfehlungen dazu, welcher Datenfluss-Endpunkttyp verwendet werden soll und wie die unterstützenden Konstrukte eingerichtet werden, finden Mit Datenflüssen arbeiten Sie unter.

In den folgenden Abschnitten werden beide unterstützten Endpunkttypen beschrieben.

> **Important**
>
> Alle Datenfluss-Endpunkte innerhalb einer einzelnen Datenfluss-Endpunktgruppe müssen vom gleichen Typ sein. Sie können AWS Ground Station Agent-Endpunkte nicht mit Dataflow-Endpunkten in derselben Gruppe kombinieren. Wenn Ihr Anwendungsfall beide Arten von Endpunkten erfordert, müssen Sie für jeden Typ separate Datenfluss-Endpunktgruppen erstellen.
> Für DataflowEndpointGroup V2 können Sie beides mischen UplinkAwsGroundStationAgentEndpointund DownlinkAwsGroundStationAgentEndpointin derselben Gruppe befinden.

AWS Ground Station Agenten-Endpunkt

Der AWS Ground Station Agenten-Endpunkt verwendet den AWS Ground Station Agenten als Softwarekomponente, um Verbindungen zu beenden. Um einen AWS Ground Station Agenten-Endpunkt zu erstellen, füllen Sie nur das `AwsGroundStationAgentEndpoint` Feld von aus. EndpointDetails Weitere Informationen zum AWS Ground Station Agenten finden Sie im vollständigen AWS Ground Station Agent-Benutzerhandbuch.

Der `AwsGroundStationAgentEndpoint` enthält die folgenden Elemente:

- `Name`— Der Name des Datenfluss-Endpunkts. Damit der Kontakt diesen Datenflussendpunkt verwenden kann, muss dieser Name mit dem Namen übereinstimmen, der in Ihrer Datenfluss-Endpunktkonfiguration verwendet wurde.
- `EgressAddress`— Die IP- und Portadresse, die für den Datenaustausch vom Agenten verwendet werden.
- `IngressAddress`- Die IP- und Portadresse, die für den Dateneingang an den Agenten verwendet werden.

Datenfluss-Endpunkt

Der Dataflow-Endpunkt verwendet eine Netzwerkanwendung als Softwarekomponente, um Verbindungen zu beenden. Verwenden Sie Dataflow Endpoint, wenn Sie digitale Signaldaten per Uplink verknüpfen, weniger als 50 MHz digitale Signaldaten herunterverknüpfen oder Signaldaten herabsetzen möchten. Demodulated/Decoded Um einen Datenfluss-Endpunkt zu erstellen, füllen Sie die Felder und von. `Endpoint` `Security Details` EndpointDetails

Der `Endpoint` enthält die folgenden Elemente:

- `Name`- Der Name des Datenfluss-Endpunkts. Damit der Kontakt diesen Datenflussendpunkt verwenden kann, muss dieser Name mit dem Namen übereinstimmen, der in Ihrer Datenfluss-Endpunktkonfiguration verwendet wurde.
- `Address`— Die verwendete IP- und Portadresse.

Der `SecurityDetails` enthält die folgenden Elemente:

- `roleArn`— Der Amazon-Ressourcenname (ARN) einer Rolle, die AWS Ground Station die Erstellung von Elastic Network Interfaces (ENIs) in Ihrer VPC übernimmt. Diese ENIs dienen als Eingangs- und Ausgangspunkte für 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 elastische Netzwerkschnittstellen platziert werden AWS Ground Station können, um Streams an Ihre Instances zu senden. Wenn mehrere Subnetze angegeben sind, müssen sie untereinander routbar sein. Wenn sich die Subnetze in unterschiedlichen Availability Zones (AZs) befinden, können AZ-übergreifende Datenübertragungsgebühren anfallen.

Die übergebene IAM-Rolle `roleArn` muss über eine Vertrauensrichtlinie verfügen, die es dem `groundstation.amazonaws.com` Dienstprinzipal ermöglicht, die Rolle zu übernehmen. Ein Beispiel finden Sie unten im Abschnitt „Beispiel für eine Vertrauensrichtlinie“. Während der Endpunkterstellung ist die Ressourcen-ID des Endpunkts nicht vorhanden, daher muss die Vertrauensrichtlinie anstelle von *`your-endpoint-id`* ein Sternchen (`*`) verwenden. Dies kann nach der Erstellung aktualisiert werden, sodass die Endpunkt-Ressourcen-ID verwendet wird, um die Vertrauensrichtlinie auf diese spezifische Datenfluss-Endpunktgruppe auszudehnen.

Die IAM-Rolle muss über eine IAM-Richtlinie verfügen, die die Einrichtung von AWS Ground Station ermöglicht. ENIs Ein Beispiel finden Sie im Abschnitt „Beispiel für eine Rollenrichtlinie“ weiter unten.

Beispiel für eine Vertrauensrichtlinie

Weitere Informationen zur Aktualisierung der Vertrauensrichtlinie einer Rolle finden Sie unter Verwaltung von IAM-Rollen im IAM-Benutzerhandbuch.

JSON

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

Beispiel für eine Rollenrichtlinie

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

JSON

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

```
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource": "*"
    }
  ]
}
```

DataflowEndpointGroupV2-Endpunkte

DataflowEndpointGroupV2 führt spezielle Endpunkttypen ein, die eine klarere Konfiguration und erweiterte Funktionen bieten:

- UplinkAwsGroundStationAgentEndpoint- Optimiert für Uplink-Datenflüsse
- DownlinkAwsGroundStationAgentEndpoint- Optimiert für Downlink-Datenflüsse

Diese spezialisierten Endpunkte ersetzen die generischen AwsGroundStationAgentEndpointdurch richtungsspezifische Konfigurationen, die die Einrichtung und Verwaltung Ihrer Datenflüsse erleichtern.

AWS Ground Station Uplink-Agent-Endpunkt

Der UplinkAwsGroundStationAgentEndpointwurde speziell für Uplink-Datenflüsse entwickelt und bietet klarere Konfigurationsoptionen. Verwenden Sie diesen Endpunkttyp, wenn Sie Daten bereitstellen müssen, die auf Ihren Satelliten AWS Ground Station übertragen werden sollen.

Der `UplinkAwsGroundStationAgentEndpoint` enthält die folgenden Elemente:

- `Name`— Der Name des Datenfluss-Endpunkts. Damit der Kontakt diesen Datenflussendpunkt verwenden kann, muss dieser Name mit dem Namen übereinstimmen, der in Ihrer Datenfluss-Endpunktkonfiguration verwendet wurde.
- `IngressAddressAndPort`- Eine einzige IP- und Port-Adresse für die Dateneingabe an den Agenten
- `AgentIpAndPortAddress`- Portbereich für die Agentenkommunikation

AWS Ground Station Downlink-Agent-Endpunkt

Der DownlinkAwsGroundStationAgentEndpointist für Downlink-Datenflüsse optimiert, einschließlich Schmalband-Downlink-, Breitband-Demodulation/-dekodierung und Uplink-Echo-Szenarien.

Der `DownlinkAwsGroundStationAgentEndpoint` enthält die folgenden Elemente:

- `Name`— Der Name des Datenfluss-Endpunkts. Damit der Kontakt diesen Datenflussendpunkt verwenden kann, muss dieser Name mit dem Namen übereinstimmen, der in Ihrer Datenfluss-Endpunktkonfiguration verwendet wurde.
- `EgressAddressAndPort`- Eine einzige IP- und Port-Adresse für die Datenausgabe vom Agenten
- `AgentIpAndPortAddress`- Portbereich für die Agentenkommunikation

Datenfluss-Endpunktgruppen erstellen

Sie können Datenfluss-Endpunktgruppen mit beiden Versionen erstellen:

CreateDataflowEndpointGroup

Verwenden Sie diese CreateDataflowEndpointGroupOption aus Gründen der Abwärtskompatibilität oder wenn Sie die generischen AwsGroundStationAgentEndpointTypen oder verwenden müssen. DataflowEndpoint

CreateDataflowEndpointGroupV2

Verwenden Sie CreateDataflowEndpointGroupV2 für neue Implementierungen, um die Vorteile spezialisierter Endpunkttypen zu nutzen, die sowohl Uplink- als auch Downlink-Datenflüsse unterstützen. Diese API unterstützt nur und. UplinkAwsGroundStationAgentEndpointDownlinkAwsGroundStationAgentEndpoint

Überlegungen zur Migration

Wenn Sie derzeit verwenden DataflowEndpointGroup, können Sie Ihre bestehende Konfiguration ohne Änderungen weiter verwenden. AWS Ground Station behält die volle Abwärtskompatibilität bei.

Wenn Sie auf die neue DataflowEndpointGroup Version 2 migrieren möchten und derzeit eine Anwendung DataflowEndpointmit einer Dataflow-Endpunktanwendung verwenden, um Ihre Daten zu empfangen, müssen Sie stattdessen migrieren, um den AWS Ground Station Agenten zu verwenden. Wenn Sie bereits einen AWS Ground Station Agenten für den Downlink verwenden,

können Sie dieselbe Agenteninstanz auch für den Uplink verwenden — es sind keine zusätzlichen Agenteninstanzen erforderlich.

Um auf V2 zu migrieren: DataflowEndpointGroup

1. Wenn Sie von migrieren DataflowEndpoint, richten Sie den AWS Ground Station Agenten gemäß dem AWS Ground Station Agent-Benutzerhandbuch ein
2. Identifizieren Sie Ihre Datenflussrichtung und erstellen Sie den entsprechenden Endpunkttyp (oder) UplinkAwsGroundStationAgentEndpointDownlinkAwsGroundStationAgentEndpoint
3. Erstellen Sie die DataflowEndpointGroupV2, die auf diese Endpunkte verweist
4. Erstellen Sie eine neue Datenfluss-Endpunktkonfiguration, die namentlich auf die neue V2 verweist DataflowEndpointGroup
5. Erstellen Sie ein neues Missionsprofil, das auf die Datenfluss-Endpunktkonfiguration als Datenfluss-Edge verweist
6. Verwenden Sie das neue Missionsprofil, um Kontakte zu planen
7. Testen Sie Ihre Konfiguration, bevor Sie sie in der Produktion einsetzen

Weitere Informationen zum vollständigen Workflow finden Sie unter AWS Ground Station Kernkomponenten verstehen undKonfigurationen erstellen.

AWS Ground Station Agent verwenden

Der AWS Ground Station Agent ermöglicht es Ihnen, synchrone Wideband Digital Intermediate Frequency (DigIF) -Datenflüsse während Kontakten mit der AWS Ground Station zu empfangen (Downlink).

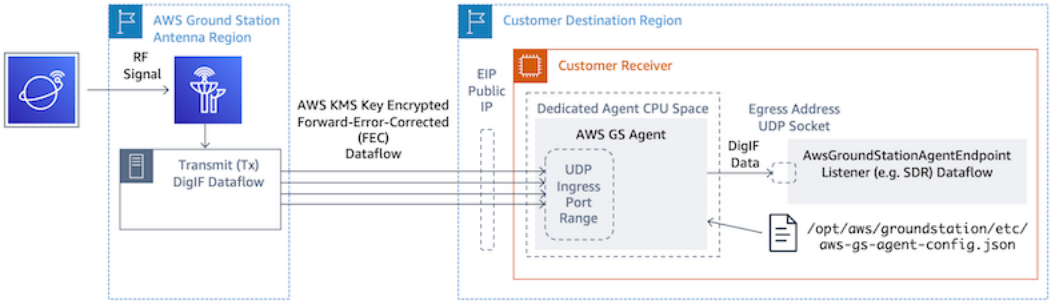
Funktionsweise

Sie können zwei Optionen für die Datenübermittlung wählen:

1. Datenlieferung an eine EC2 Instanz — Datenlieferung an eine EC2 Instanz, die Sie besitzen. Sie 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 Datenlieferung finden Sie im Mit Datenflüssen arbeiten Abschnitt.
2. Datenlieferung an einen S3-Bucket — Die Datenlieferung an Ihren AWS S3-Bucket wird vollständig von verwaltet AWS Ground Station. Informationen zur S3-Datenlieferung finden Sie im Erste Schritte Leitfaden.

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

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



Zusätzliche Informationen

Ausführlichere Informationen finden Sie im vollständigen Agent-Benutzerhandbuch.AWS Ground Station

Erste Schritte

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

Im Folgenden finden Sie die bewährten Methoden für AWS Identity and Access Management (IAM) und die erforderlichen Berechtigungen. Nachdem Sie die entsprechenden Rollen eingerichtet haben, können Sie mit den restlichen Schritten beginnen.

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/die Anmeldung.
2. Folgen Sie den Online-Anweisungen.

   Während der Anmeldung erhalten Sie einen Telefonanruf oder eine Textnachricht und müssen 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 Benutzer 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. Du kannst jederzeit deine aktuellen Kontoaktivitäten einsehen und dein Konto verwalten, indem du zu https://aws.amazon.com/gehst und Mein Konto auswählst.

Erstellen eines Benutzers mit Administratorzugriff

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-Managementkonsoleals 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 Benutzers mit Administratorzugriff

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 Benutzerzugriff.

   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.

Weiteren Benutzern Zugriff zuweisen

1. Erstellen Sie im IAM-Identity-Center einen Berechtigungssatz, der den bewährten Vorgehensweisen für die Anwendung von geringsten Berechtigungen folgt.

Anweisungen hierzu finden Sie unter Berechtigungssatz erstellen im AWS IAM Identity Center - Benutzerhandbuch.

2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

   Eine genaue Anleitung finden Sie unter Gruppen hinzufügen im AWS IAM Identity Center - Benutzerhandbuch.

Fügen Sie Ihrem AWS Konto AWS Ground Station Berechtigungen hinzu

Für die Nutzung, AWS Ground Station ohne dass ein Administratorbenutzer erforderlich ist, müssen Sie eine neue Richtlinie erstellen und sie Ihrem AWS Konto hinzufügen.

1. Melden Sie sich bei der an AWS-Managementkonsole 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:

        JSON

```
{
  "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:

  JSON

```
{
  "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

  JSON

```
{
    "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.

Satellit an Bord

Das Onboarding eines Satelliten AWS Ground Station ist ein mehrstufiger Prozess, der Datenerfassung, technische Validierung, Frequenzlizenzierung sowie Integration und Tests umfasst. Es sind auch Geheimhaltungsvereinbarungen () NDAs erforderlich.

Überblick über den Onboarding-Prozess für Kunden

Das Onboarding per Satellit ist ein manueller Prozess, der auf der AWS Ground Station Konsolenseite im Bereich Satelliten und Ressourcen zu finden ist. Im Folgenden wird der Gesamtprozess beschrieben.

1. Lesen Sie den AWS Ground Station Standorte Abschnitt, um festzustellen, ob Ihr Satellit die geografischen Eigenschaften und die Hochfrequenzeigenschaften erfüllt.
2. Um mit dem Onboarding Ihres Satelliten zu beginnen AWS Ground Station, reichen Sie bitte im Bereich Satelliten und Ressourcen auf der AWS Ground Station Konsolenseite einen Fragebogen zum Onboarding von Satelliten ein. Bitte fügen Sie eine kurze Zusammenfassung Ihrer Mission und Ihres Satellitenbedarfs bei, einschließlich des Namens Ihrer Organisation, der benötigten Frequenzen, des Starts oder Starts der Satelliten, der Art der Umlaufbahn des Satelliten und ob Sie ihn einsetzen möchten. Verwenden Sie die AWS Ground Station digitale Zwillingsfunktion
3. Sobald Ihr Antrag geprüft und genehmigt wurde, beantragen AWS Ground Station wir für die jeweiligen Standorte, die Sie nutzen möchten, eine behördliche Genehmigung. Die Dauer dieses Schritts hängt von den Standorten und den bestehenden Vorschriften ab.
4. Sobald diese Genehmigung eingeholt wurde, ist Ihr Satellit für Sie sichtbar und kann verwendet werden. AWS Ground Station sendet Ihnen eine Benachrichtigung über das erfolgreiche Update.

(Optional) Benennen von Satelliten

Nach dem Onboarding möchten Sie Ihrem Satellitendatensatz vielleicht einen Namen hinzufügen, um ihn leichter erkennen zu können. Die AWS Ground Station Konsole bietet die Möglichkeit, einen benutzerdefinierten Namen für einen Satelliten zusammen mit der Norad-ID anzuzeigen, wenn Sie die Kontaktseite verwenden. 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 einer der AWS erfolgen. SDKs 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 Ihrer Konfiguration und der Einstellungen für die Anmeldeinformationsdatei finden Sie unter Einstellungen für die Konfiguration und die Anmeldeinformationsdatei.

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
```

Öffentliche Rundfunksatelliten

Zusätzlich zum Onboarding Ihrer eigenen Satelliten können Sie das Onboarding unterstützter öffentlicher Rundfunksatelliten beantragen, die einen öffentlich zugänglichen Downlink-Kommunikationspfad bereitstellen. Auf diese Weise können Sie Daten von AWS Ground Station diesen Satelliten herunterladen.

> **Note**
>
> Sie können keine Uplinks zu diesen Satelliten herstellen. Sie können nur die öffentlich zugänglichen Downlink-Kommunikationspfade verwenden.

AWS Ground Station unterstützt das Onboarding der folgenden Satelliten für den Downlink von Direktübertragungsdaten:

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

Sobald sie an Bord sind, kann auf diese Satelliten zugegriffen werden, sodass sie sofort verwendet werden können. AWS Ground Station verwaltet eine Reihe vorkonfigurierter CloudFormation Vorlagen, um den Einstieg in den Service zu erleichtern. Beispiele Beispielkonfigurationen von Missionsprofilen dafür, wie es verwendet werden AWS Ground Station kann, finden Sie unter.

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.

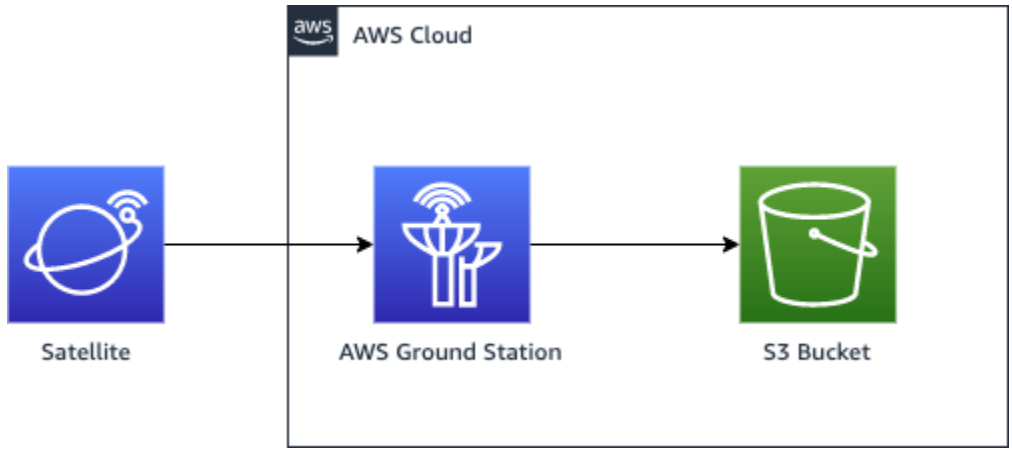
Planen Sie Ihre Datenfluss-Kommunikationspfade

Sie haben die Wahl zwischen synchroner und asynchroner Kommunikation für jeden Kommunikationspfad auf Ihrem Satelliten. Abhängig von Ihrem Satelliten und Ihrem Anwendungsfall

benötigen Sie möglicherweise einen oder beide Typen. Synchrone Kommunikationspfade ermöglichen Uplink- sowie Schmalband- und Breitband-Downlink-Operationen nahezu in Echtzeit. Asynchrone Kommunikationspfade unterstützen nur Schmalband- und Breitband-Downlink-Operationen.

Asynchrone Datenübermittlung

Bei der Datenlieferung an Amazon S3 werden Ihre Kontaktdaten asynchron an einen Amazon S3 S3-Bucket in Ihrem Konto übermittelt. Ihre Kontaktdaten werden als Paketerfassungsdateien (Pcap) geliefert, um die Wiedergabe der Kontaktdaten in einem Software Defined Radio (SDR) zu ermöglichen oder um die Nutzdaten zur Verarbeitung aus den PCAP-Dateien zu extrahieren. Die PCAP-Dateien werden alle 30 Sekunden an Ihren Amazon S3 S3-Bucket gesendet, sobald die Kontaktdaten von der Antennenhardware empfangen werden, um die Verarbeitung der Kontaktdaten während des Kontakts zu ermöglichen, falls gewünscht. Nach Erhalt können Sie die Daten mit Ihrer eigenen Nachbearbeitungssoftware verarbeiten oder andere AWS-Services wie Amazon SageMaker AI oder Amazon Rekognition nutzen. Die Datenübermittlung an Amazon S3 ist nur für das Downlinken von Daten von Ihrem Satelliten verfügbar. Es ist nicht möglich, Daten von Amazon S3 auf Ihren Satelliten hochzuladen.



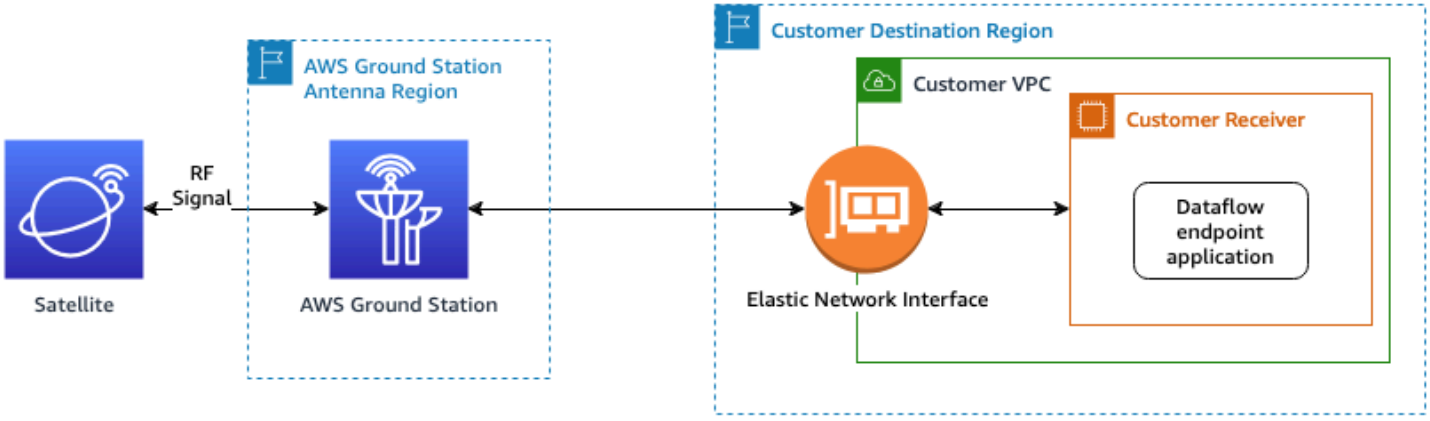
Um diesen Pfad nutzen zu können, müssen Sie einen Amazon S3 S3-Bucket erstellen, in AWS Ground Station den die Daten übertragen werden sollen. Im nächsten Schritt müssen Sie im nächsten Schritt auch eine S3-Aufnahmekonfiguration erstellen. Informationen zu Einschränkungen bei der Amazon S3 S3-Aufnahmekonfiguration Benennung von Buckets und zur Angabe der für Ihre Dateien verwendeten Benennungskonventionen finden Sie unter.

Synchrone Datenübermittlung

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

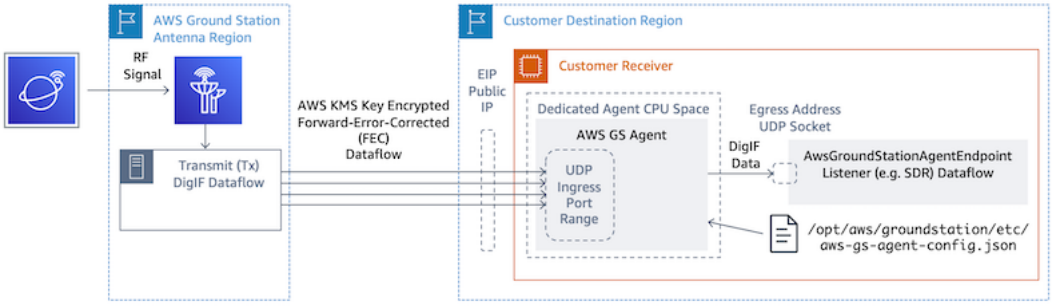
Um einen synchronen Pfad zu verwenden, müssen Sie Ihre EC2 Amazon-Instances einrichten und konfigurieren und eine oder mehrere Dataflow-Endpunktgruppen erstellen. Um Ihre EC2 Amazon-Instance zu konfigurieren, verweisen Sie aufAmazon einrichten und konfigurieren EC2. Um Ihre Dataflow-Endpunktgruppe zu erstellen, verweisen Sie bitte auf die. AWS Ground Station Dataflow-Endpunktgruppen verwenden

Im Folgenden wird der Kommunikationspfad angezeigt, wenn Sie die Dataflow-Endpunktkonfiguration verwenden.



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

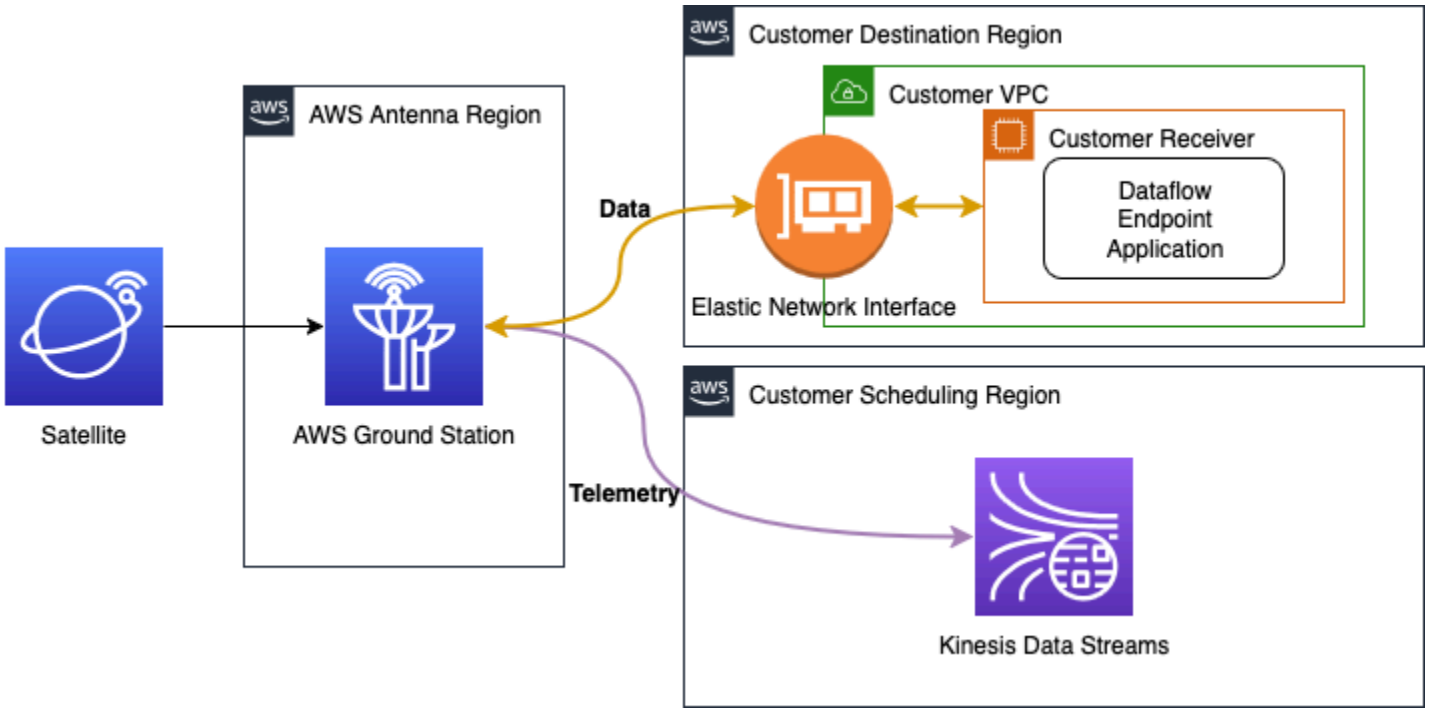
Im Folgenden wird der Kommunikationspfad angezeigt, wenn Sie die AWS Ground Station Agentenkonfiguration verwenden.



Planen Sie Ihre Telemetrie

AWS Ground Station Telemetrie ist eine optionale Funktion, die bei Satellitenkontakten Messwerte von AWS Ground Station Antennen zu Ihrem AWS Konto streamt. Auf diese Weise können Sie die Kontaktleistung nahezu in Echtzeit überwachen und maßgeschneiderte Überwachungslösungen entwickeln.

Mit AWS Ground Station Telemetrie werden Messwerte von AWS Ground Station Antennen direkt auf Ihr Konto gestreamt. Das Streamen der Telemetriedaten beginnt zu Beginn des Kontakts und wird während der gesamten Kontaktdauer fortgesetzt. Die Telemetriedaten werden nahezu in Echtzeit an Ihr Konto übermittelt, da sie von der Antennenhardware abgetastet werden. Nach Erhalt können Sie die Daten mit Ihrer eigenen Nachbearbeitungssoftware verarbeiten oder andere AWS-Services wie Amazon Data Firehose oder verwenden. AWS Lambda



Im nächsten Schritt erstellen Sie die Konfigurationen, die für Ihr Missionsprofil erforderlich sind. Wenn Sie Telemetrie aktivieren möchten, erstellen Sie zusätzlich zu Ihrer Tracking-Konfiguration und Ihren Datenflusskonfigurationen eine Telemetry Sink Config. Eine ausführliche Anleitung zur Einrichtung finden Sie unter. Telemetrie einrichten

Weitere Informationen zu finden TelemetrySinkConfig Sie unterTelemetrie Sink Config.

Konfigurationen erstellen

In diesem Schritt haben Sie den Satelliten, die Kommunikationspfade und die benötigten IAM-, Amazon EC2- und Amazon S3 S3-Ressourcen identifiziert. In diesem Schritt erstellen Sie AWS Ground Station Konfigurationen, die ihre jeweiligen Parameter speichern.

Konfigurationen für die Datenlieferung

Die ersten zu erstellenden Konfigurationen beziehen sich darauf, wo und wie die Daten geliefert werden sollen. Anhand der Informationen aus dem vorherigen Schritt werden Sie viele der folgenden Konfigurationstypen erstellen.

- Amazon S3 S3-Aufnahmekonfiguration- Liefern Sie Daten an Ihren Amazon S3 S3-Bucket.
- Datenflussendpunkt-Config- Liefern Sie Daten an Ihre Amazon EC2 EC2-Instance.

Telemetriekonfiguration (optional)

Wenn Sie während Ihrer Kontakte Telemetriedaten nahezu in Echtzeit empfangen möchten, können Sie eine erstellen. TelemetrySinkConfig Diese Konfiguration ist optional und gibt an, wohin die Telemetriedaten geliefert AWS Ground Station werden.

- Telemetrie Sink Config- Stellen Sie Telemetriedaten an Ihr Konto bereit.

Eine ausführliche Anleitung zur Einrichtung finden Sie unterTelemetrie einrichten.

Satelliten-Konfigurationen

Die Satellitenkonfigurationen geben an, wie AWS Ground Station Sie mit Ihrem Satelliten kommunizieren können. Sie werden auf die Informationen verweisen, die Sie gesammelt haben. Satellit an Bord

- Nachverfolgungs-Config- Legt fest, wie Ihr Fahrzeug während eines Kontakts physisch verfolgt wird. Dies ist für die Erstellung von Missionsprofilen erforderlich.
- Antennen-Downlink-Config- Liefern Sie digitalisierte Hochfrequenzdaten.
- Antennen-Downlink-Demod-Decode-Config- Liefern Sie demodulierte und dekodierte Hochfrequenzdaten.
- Antennen-Uplink-Config- Uplink-Daten zu Ihrem Satelliten.

- Antennen-Uplink-Echo-Config- Liefert ein Echo Ihrer Uplink-Signaldaten.

Missionsprofil erstellen

Mit den im vorherigen Schritt erstellten Konfigurationen haben Sie herausgefunden, wie Sie Ihren Satelliten verfolgen können, wie Sie mit Ihrem Satelliten kommunizieren können und wie Sie Telemetrie nahezu in Echtzeit während der Kontaktausführung aktivieren können. In diesem Schritt erstellen Sie ein oder mehrere Missionsprofile. Ein Missionsprofil stellt die Zusammenfassung der möglichen Konfigurationen zu einem erwarteten Verhalten dar, das dann geplant und ausgeführt werden kann.

Die neuesten Parameter finden Sie unter dem Ressourcentyp AWS::GroundStation::MissionProfile CloudFormation

1. Nennen Sie Ihr Missionsprofil. Auf diese Weise können Sie schnell verstehen, wie es in Ihrem System verwendet wird. Zum Beispiel haben Sie möglicherweise einen satellite-wideband-narrowband-nominal-Betrieb und einen, satellite-narrowband-emergency-operationsob Sie einen separaten Schmalband-Netzbetreiber für Notoperationen haben.
2. Stellen Sie Ihre Tracking-Konfiguration ein.
3. Lege deine Mindestdauer für brauchbare Kontakte fest. Auf diese Weise können Sie potenzielle Kontakte filtern, um sie an Ihre Missionsanforderungen anzupassen.
4. Stellen Sie Ihre streamsKmsKeyDaten ein streamsKmsRole, die zur Verschlüsselung Ihrer Daten während der Übertragung verwendet werden. Dies wird für alle AWS Ground Station Agent-Datenflüsse verwendet.
5. Stellen Sie Ihre Datenflüsse ein. Erstellen Sie Ihre Datenflüsse so, dass sie Ihren Trägersignalen entsprechen, indem Sie die Konfigurationen verwenden, die Sie im vorherigen Schritt erstellt haben.
6. [Optional] Lege deine Kontaktdauer vor und nach dem Pass in Sekunden fest. Dies wird verwendet, um Ereignisse pro Kontakt vor bzw. nach dem Kontakt auszusenden. Weitere Informationen finden Sie unter Automatisieren Sie AWS Ground Station mit Ereignissen.
7. [Optional] Stellen Sie Ihren telemetrySinkConfigARN so ein, dass Telemetrie bei Kontakten aktiviert wird. Auf diese Weise können Sie Telemetriedaten nahezu in Echtzeit direkt in Ihrem Konto zur Überwachung und Analyse empfangen. Weitere Informationen finden Sie unter Arbeiten Sie mit Telemetrie.
8. [Optional] Sie können Ihrem Missionsprofil Tags zuordnen. Diese können verwendet werden, um Ihre Missionsprofile programmatisch zu differenzieren.

Sie können auf die verweisenBeispielkonfigurationen von Missionsprofilen, um nur einige der möglichen Konfigurationen zu sehen.

Verstehen Sie die nächsten Schritte

Da Sie nun über einen Satelliten an Bord und ein gültiges Missionsprofil verfügen, können Sie Kontakte planen und mit Ihrem Satelliten kommunizieren. AWS Ground Station

Sie können einen Kontakt auf eine der folgenden Arten planen:

- Die AWS Ground Station Konsole.
- Der AWS CLI-Befehl reserve-contact.
- Das AWS SDK. ReserveContact API.

Informationen darüber, wie die Flugbahn Ihres Satelliten AWS Ground Station verfolgt wird und wie diese Informationen verwendet werden, finden Sie unter. Verstehe, wie AWS Ground Station Ephemeriden verwendet werden

AWS Ground Station verwaltet eine Reihe von vorkonfigurierten CloudFormation Vorlagen, um den Einstieg in den Service zu erleichtern. Beispiele Beispielkonfigurationen von Missionsprofilen dafür, wie es verwendet werden AWS Ground Station kann, finden Sie unter.

Die Verarbeitung der digitalen Zwischenfrequenzdaten oder der demodulierten und dekodierten Daten, die Ihnen zur Verfügung gestellt AWS Ground Station werden, hängt von Ihrem spezifischen Anwendungsfall ab. Die folgenden Blogbeiträge können Ihnen helfen, einige der Optionen zu verstehen, die Ihnen zur Verfügung stehen:

- Automatisierte Erdbeobachtung mit AWS Ground Station Amazon S3 S3-Datenlieferung (und dem zugehörigen GitHub Repository awslabs/ aws-groundstation-eos-pipeline)
- Virtualisierung des Satelliten-Bodensegments mit AWS
- Erdbeobachtung mithilfe von AWS Ground Station: Eine Anleitung
- Aufbau von Downlink-Architekturen für Satellitendaten mit hohem Durchsatz mit AWS Ground Station WideBand DigIF und Amphinicy Blink SDR (und dem zugehörigen Repository aws-samples/) GitHub aws-groundstation-wbdigif-snpp

AWS Ground Station Standorte

AWS Ground Station bietet ein globales Netzwerk von Bodenstationen in unmittelbarer Nähe zu unserem globalen Netzwerk von AWS-Infrastrukturregionen. Sie können Ihre Nutzung dieser Standorte von jeder unterstützten AWS-Region aus konfigurieren. Dies schließt die AWS-Region ein, in der Daten geliefert werden.

Finden Sie die AWS Region für einen Standort für eine Bodenstation

Das AWS Ground Station globale Netzwerk umfasst Bodenstationen, die sich nicht physisch in der AWS-Region befinden, mit der sie verbunden sind. Die Liste der Bodenstationen, auf die Sie Zugriff haben, kann über die ListGroundStationAWS-SDK-Antwort abgerufen werden. Die vollständige Liste der Standorte der Bodenstationen ist unten aufgeführt. Weitere werden in Kürze folgen. Informationen zum Hinzufügen oder Ändern von Standortgenehmigungen für Ihre Satelliten finden Sie im Onboarding-Leitfaden.

Name der Ground Station	Standort der Ground Station	Name der AWS-Region	AWS-Regionalcode	Hinweise
Alaska 1	Alaska, Vereinigte Staaten	USA West (Oregon)	us-west-2	Nicht physisch in einer AWS Region gelegen
Bahrain 1	Bahrain	Naher Osten (Bahrain)	me-south-1	
Kapstadt 1	Cape Town, Südafrika	Afrika (Kapstadt)	af-south-1	
Dubbo 1	Dubbo, Australien	Asien-Pazifik (Sydney)	ap-southeast-2	Nicht physisch in einer AWS Region gelegen
Hawaii 1	Hawaii, Vereinigte Staaten	USA West (Oregon)	us-west-2	Nicht physisch in einer AWS Region ansässig
Irland 1	Irland	Europa (Irland)	eu-west-1	
Ohio 1	Ohio, Vereinigte Staaten	USA Ost (Ohio)	us-east-2	
Oregon 1	Oregon, Vereinigte Staaten	USA West (Oregon)	us-west-2	
Punta Arenas 1	Punta Arenas, Chile	Südamerika (São Paulo)	sa-east-1	Nicht physisch in einer AWS Region gelegen
Seoul 1	Seoul, Südkorea	Asien-Pazifik (Seoul)	ap-northeast-2	
Singapur 1	Singapur	Asien-Pazifik (Singapur)	ap-southeast-1	

Name der Ground Station	Standort der Ground Station	Name der AWS-Region	AWS-Regionalcode	Hinweise
Stockholm 1	Stockholm, Schweden	Europa (Stockholm)	eu-north-1	

AWS Ground Station unterstützte AWS-Regionen

Sie können Daten bereitstellen und Ihre Kontakte über das AWS-SDK oder die AWS Ground Station Konsole aus unterstützten AWS-Regionen konfigurieren. Sie können die unterstützten Regionen und die zugehörigen Endpunkte unter den AWS Ground Station Endpunkten und Kontingenten einsehen.

Verfügbarkeit digitaler Zwillinge

Verwenden Sie die AWS Ground Station digitale Zwillingsfunktionist in allen AWS-Regionen verfügbar, in denen AWS Ground Station es verfügbar ist. Digitale Zwillingsbodenstationen sind exakte Kopien von Bodenstationen aus der Produktion mit dem modifizierenden Präfix „Digitaler Zwilling“ für den Namen der Ground Station. Bei „Digital Twin Ohio 1" handelt es sich beispielsweise um eine digitale Doppelbodenstation, die eine exakte Kopie der Produktionsbodenstation „Ohio 1" ist.

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 geografischen Geländes, das die Antenne umgibt — 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, wie 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 Ihnen im Rahmen einer Geheimhaltungsvereinbarung (NDA) zur Verfügung.

Kundenspezifische Masken

Zusätzlich zu den Masken der AWS Ground Station an jedem Standort verfügen Sie möglicherweise über zusätzliche Masken, da Ihre eigene gesetzliche Genehmigung zur Kommunikation mit Ihren 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 Seitenmasken 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 Sie keine Zeit reservieren, 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 Sie die gesamte verfügbare Kontaktzeit für den Downlink verwenden, 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 für einen Teil oder die gesamte Zeit, die für einen Satellitenkontakt reserviert ist, nicht übertragen wird. Sie 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 Ihnen in Rechnung gestellt, auch wenn Teile der reservierten Zeit für den Uplink nicht verfügbar sind.

AWS Ground Station Funktionen der Website

Um Ihnen die Bedienung zu erleichtern, AWS Ground Station wird ein einheitlicher Funktionsumfang für einen Antennentyp ermittelt und anschließend mehrere Antennen an einer Bodenstation installiert. Ein Teil der Onboarding-Schritte stellt sicher, dass Ihr Satellit mit den Antennentypen an einem bestimmten Standort kompatibel ist. Wenn Sie einen Kontakt reservieren, bestimmen Sie indirekt den verwendeten Antennentyp. Dadurch wird sichergestellt, dass Ihr Erlebnis an einem bestimmten Standort der Bodenstation im Laufe der Zeit gleich bleibt, unabhängig davon, welche Antennen verwendet werden. Die spezifische Leistung Ihres Kontakts wird aufgrund einer Vielzahl von Umweltproblemen, wie z. B. dem Wetter am Standort, variieren.

Derzeit unterstützen alle Websites die folgenden Funktionen:

> **Note**
>
> Jede Zeile in der folgenden Tabelle gibt einen unabhängigen Kommunikationspfad an, sofern nicht anders angegeben. Doppelte Zeilen sind vorhanden, um unsere Mehrkanalfunktionen widerzuspiegeln, die die gleichzeitige Nutzung mehrerer Kommunikationspfade ermöglichen.

Art der Fähigkeit	Frequenzbereich	Bandbreitenbereich	Polarisierung	Common Name	Hinweise
Antennen-Downlink	7750 - 8500 MHz	50 - 400 MHz	RHCP	X-Band-Breitband-Downlink	Diese Funktion erfordert die Verwendung des Agenten.A
Antennen-Downlink	7750 - 8500 MHz	50 - 400 MHz	RHCP		

Art der Fähigkeit	Frequenzbereich	Bandbreitenbereich	Polarisierung	Common Name	Hinweise
Antennen-Downlink	7750 - 8500 MHz	50 - 400 MHz	RHCP		WS Ground Station
Antennen-Downlink	7750 - 8500 MHz	50 - 400 MHz	RHCP		Diese Funktion wird in Alaska 1 oder Punta Arenas 1 nicht unterstützt.
Antennen-Downlink	7750 - 8500 MHz	50 - 400 MHz	RHCP		
Antennen-Downlink	7750 - 8500 MHz	50 - 400 MHz	LHCP		
Antennen-Downlink	7750 - 8500 MHz	50 - 400 MHz	LHCP		Die Gesamtbandbreite darf 400 MHz pro Polarisation an jedem Standort nicht überschreiten.
Antennen-Downlink	7750 - 8500 MHz	50 - 400 MHz	LHCP		
Antennen-Downlink	7750 - 8500 MHz	50 - 400 MHz	LHCP		
Antennen-Downlink	7750 - 8500 MHz	50 - 400 MHz	LHCP		Alle verwendeten Frequenzbereiche dürfen sich nicht überlappen.
Antennen-Downlink	2200 - 290 MHz	Bis zu 40 MHz	RHCP	S-Band-Downlink	Es kann jeweils nur eine Polarisation verwendet werden
Antennen-Downlink	2200 - 290 MHz	Bis zu 40 MHz	LHCP		

Art der Fähigkeit	Frequenzbereich	Bandbreitenbereich	Polarisierung	Common Name	Hinweise
Antennen-Downlink	7750 - 8500 MHz	Bis zu 40 MHz	RHCP	X-Band-Schmalband-Downlink	Es kann jeweils nur eine Polarisation verwendet werden
Antennen-Downlink	7750 - 8500 MHz	Bis zu 40 MHz	LHCP		
Antennen-Uplink	2025 - 2110 MHz	Bis zu 40 MHz	RHCP	S-Band-Uplink	Es kann jeweils nur eine Polarisation verwendet werden EIRP 20-50 dBW
Antennen-Uplink	2025 - 2110 MHz	Bis zu 40 MHz	LHCP		
antenna-uplink-echo	2025 - 2110 MHz	2 MHz	RHCP	Uplink-Echo	Entspricht den Antennen-Uplink-Einschränkungen
antenna-uplink-echo	2025-2110 MHz	2 MHz	LHCP		
antenna-downlink-demod-decode	750 - 8500 MHz	Bis zu 500 MHz	RHCP	Demodulierter und dekodierter X-Band-Downlink	
antenna-downlink-demod-decode	7750 - 8500 MHz	Bis zu 500 MHz	LHCP		
Nachverfolgung	N/A	–	–	N/A	Support für Auto-Tracking und Programm-Tracking

* RHCP = zirkulare Polarisation für Rechtshänder und LHCP = zirkulare Polarisation für Linkshänder. Weitere Informationen zur Polarisation finden Sie unter Zirkulare Polarisation.

Verstehe, wie AWS Ground Station Ephemeriden verwendet werden

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.

Die Ephemeriden-API ermöglicht das Hochladen benutzerdefinierter Ephemeriden zur Verwendung mit einem Satelliten. AWS Ground Station Diese Ephemeriden überschreiben die Standard-Ephemeriden von Space-Track (siehe:). Standard-Ephemeridendaten Wir unterstützen den Empfang von Ephemeridendaten in den Formaten Orbit Ephemeris Message (OEM), Two-Line Element (TLE) und Azimut-Elevation.

AWS Ground Station verwendet Ephemeridendaten, um anhand der bereitgestellten Ephemeridendaten zu ermitteln, wann Kontakte verfügbar werden, und steuert die Antennen im Netzwerk korrekt an. AWS Ground Station Standardmäßig sind keine Maßnahmen zur Bereitstellung AWS Ground Station von Ephemeriden erforderlich, wenn Ihrem Satelliten eine NORAD-ID zugewiesen wurde.

Das Hochladen benutzerdefinierter Ephemeriden kann die Qualität der Ortung verbessern, frühe Operationen durchführen, für die keine Space-Track-Ephemeriden verfügbar sind, und Manöver berücksichtigen. AWS Ground Station

AWS Ground Station Unterstützt alternativ ein Azimut-Höhenformat, mit dem Sie die Ausrichtung der Antenne direkt angeben können, ohne Informationen zur Satellitenbahn bereitzustellen. Dies ist nützlich für Szenarien, in denen eine genaue Ausrichtung der Antenne erforderlich ist, da die Flugbahninformationen von Satelliten ungenau oder unbekannt sind.

Themen

- Standard-Ephemeridendaten
- Stellen Sie benutzerdefinierte Ephemeridendaten bereit
- Reservieren Sie Kontakte mit benutzerdefinierten Ephemeriden
- Verstehe, welche Ephemeride verwendet wird
- Ruft die aktuelle Ephemeride für einen Satelliten ab

- Kehren Sie zu den Standard-Ephemeridendaten zurück

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. Diese Ephemeriden sind zweizeilige Elementsätze (TLEs), 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 oder höher haben. 1

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 benutzerdefinierter Ephemeridendaten finden Sie unter: Bereitstellung benutzerdefinierter Ephemeridendaten.

Stellen Sie benutzerdefinierte Ephemeridendaten bereit

> **Important**
>
> Die Ephemeriden-API befindet sich derzeit im Vorschaustatus

Der Zugriff auf die Ephemeris-API wird nur bei Bedarf gewährt. Wenn Sie die Möglichkeit benötigen, benutzerdefinierte Ephemeridendaten hochzuladen, öffnen Sie bitte ein Ticket über. AWS Support AWS Support Center Console Unser Team wird mit Ihnen zusammenarbeiten, um diese Funktion für Ihre spezifischen Anforderungen zu aktivieren.

-Übersicht

Die Ephemeris-API ermöglicht das Hochladen benutzerdefinierter Ephemeriden zur Verwendung mit AWS Ground Station einem Satelliten. Diese Ephemeriden überschreiben die Standard-Ephemeriden von Space-Track (siehe:). Standard-Ephemeridendaten Wir unterstützen den Empfang von Ephemeridendaten in den Formaten Orbit Ephemeris Message (OEM), Two-Line Element (TLE) und Azimut-Elevation.

AWS Ground Station behandelt Ephemeriden als individualisierte Nutzungsdaten. Wenn Sie diese optionale Funktion verwenden, verwendet AWS Ihre Ephemeridendaten, um Unterstützung bei der Fehlerbehebung bereitzustellen.

Durch das Hochladen benutzerdefinierter Ephemeriden kann die Qualität der Ortung verbessert, Operationen abgewickelt werden, für die keine Space-Track-Ephemeriden verfügbar sind, und Manöver können berücksichtigt werden. AWS Ground Station

Informationen zur Behebung einer ungültigen Ephemeride findest du unter: Fehlerbehebung bei ungültigen Ephemeriden

Beispiel: Verwendung von vom Kunden bereitgestellten Ephemeriden mit AWS Ground Station

Eine detailliertere Anleitung zur Verwendung von vom Kunden bereitgestellten Ephemeriden mit finden Sie unter Vom Kunden bereitgestellte Ephemeriden verwenden mit AWS Ground Station und dem zugehörigen Repository aws-samples/. AWS Ground Station GitHub aws-groundstation-cpe

Stellen Sie TLE-Ephemeridendaten bereit

> **Important**
>
> Die Ephemeriden-API befindet sich derzeit im Vorschaustatus

Der Zugriff auf die Ephemeris-API wird nur bei Bedarf gewährt. Wenn Sie die Möglichkeit benötigen, benutzerdefinierte Ephemeridendaten hochzuladen, öffnen Sie bitte ein Ticket über. AWS Support AWS Support Center Console Unser Team wird mit Ihnen zusammenarbeiten, um diese Funktion für Ihre spezifischen Anforderungen zu aktivieren.

-Übersicht

Two-Line Element (TLE) -Sets sind ein standardisiertes Format zur Beschreibung von Satellitenbahnen. Die Ephemeris-API ermöglicht das Hochladen von TLE-Ephemeriden zur Verwendung mit einem Satelliten. AWS Ground Station Diese Ephemeriden überschreiben die Standard-Ephemeriden von Space-Track (siehe:). Standard-Ephemeridendaten

AWS Ground Station behandelt Ephemeriden als individualisierte Nutzungsdaten. Wenn Sie diese optionale Funktion verwenden, verwendet AWS Ihre Ephemeridendaten, um Unterstützung bei der Fehlerbehebung bereitzustellen.

Das Hochladen benutzerdefinierter TLE-Ephemeriden kann die Qualität der Ortung verbessern, frühe Operationen abwickeln, für die keine Space-Track-Ephemeriden verfügbar sind, und Manöver berücksichtigen. AWS Ground Station

> **Note**
>
> Wenn Sie benutzerdefinierte Ephemeriden angeben, bevor Ihrem Satelliten eine Satellitenkatalognummer zugewiesen wird, können Sie dies für das Feld `00000` für die Satellitenkatalognummer des TLE und für den Teil mit der Startnummer des internationalen Kennzeichnungsfeldes des TLE verwenden (z. B. `000` für ein Fahrzeug, das 2024 auf den Markt gebracht wurde). `24000A`
> Weitere Informationen zum Format von finden Sie unter Zweizeiliger TLEs Elementsatz.

Eine TLE-Ephemeride erstellen

Eine TLE-Ephemeride kann mithilfe der CreateEphemerisAktion in der API erstellt werden. AWS Ground Station Bei dieser Aktion wird eine Ephemeride mithilfe von Daten hochgeladen, die entweder im Anfragetext oder aus einem bestimmten S3-Bucket enthalten sind.

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 Status der Ephemeriden DescribeEphemerisabfragen oder CloudWatch Ereignisse verwenden, um die Statusänderungen der Ephemeriden nachzuverfolgen.

Informationen zur Fehlerbehebung bei einer ungültigen Ephemeride finden Sie unter: Fehlerbehebung bei ungültigen Ephemeriden

Beispiel: Erstellen Sie eine Ephemeride mit zweizeiligen Elementen (TLE) über die API

Die CLI und kann verwendet werden AWS SDKs, um AWS Ground Station über den Aufruf ein Two-Line-Element (TLE) -Set-Ephemeriden CreateEphemerishochzuladen. Diese Ephemeride wird anstelle der standardmäßigen Ephemeridendaten für einen Satelliten verwendet (siehe). Standard-Ephemeridendaten Dieses Beispiel zeigt, wie das mit dem AWS SDK for Python (Boto3) gemacht wird.

Ein TLE-Set ist ein Objekt im JSON-Format, das eines oder mehrere Objekte TLEs aneinanderreiht, um eine kontinuierliche Trajektorie zu erstellen. Das TLEs im TLE-Set enthaltene Objekt muss einen kontinuierlichen Satz bilden, den wir verwenden können, um eine Trajektorie zu konstruieren (d. h. keine zeitlichen Lücken dazwischen TLEs in einem TLE-Set). Ein Beispiel für ein TLE-Set ist unten dargestellt:

```
[
    {
        "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 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:

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

# Create AWS Ground Station client
```

```
ground_station_client = boto3.client("groundstation")

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

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

Dieser Aufruf gibt eine EphemerisId zurück, mit der in future auf die Ephemeride verwiesen werden kann. Zum Beispiel können wir die bereitgestellte EphemerisID aus dem obigen Aufruf verwenden, um den Status der Ephemeride abzufragen:

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

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

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

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

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

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

response = ground_station_client.describe_ephemeris(ephemerisId=ephemeris_id)

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

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 DescribeEphemerisRoute abzufragen oder CloudWatch Ereignisse zu verwenden, um den Status der hochgeladenen Ephemeriden zu verfolgen, da sie einen asynchronen Validierungsworkflow durchlaufen muss, bevor sie auf gesetzt wird `ENABLED` und für die Planung und Ausführung von Kontakten verwendet werden kann.

Beachten Sie, dass die gesamte NORAD-ID im TLE-Set TLEs in den obigen Beispielen mit der NORAD-ID übereinstimmen muss, die Ihrem Satelliten 25994 in der Space-Track-Datenbank zugewiesen wurde.

Beispiel: Hochladen von TLE-Ephemeridendaten aus einem S3-Bucket

Es ist auch möglich, eine TLE-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 in AWS Ground Station finden Sie in:Datenverschlüsselung im Ruhezustand für AWS Ground Station.

Im Folgenden finden Sie ein Beispiel für das Hochladen einer TLE-Ephemeriden-Datei aus einem S3-Bucket

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

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

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

```
# Create sample TLE set data
# Note: For actual satellites, use real TLE data from sources like Space-Track
tle_set_data = [
    {
        "tleLine1": "1 25994U 99068A   20318.54719794  .00000075  00000-0  26688-4 0
 9997",
        "tleLine2": "2 25994  98.2007  30.6589 0001234  89.2782  18.9934
 14.57114995111906",
        "validTimeRange": {
            "startTime": datetime.now(timezone.utc),
            "endTime": datetime.now(timezone.utc) + timedelta(days=3),
        },
    },
    {
        "tleLine1": "1 25994U 99068A   20321.54719794  .00000075  00000-0  26688-4 0
 9998",
        "tleLine2": "2 25994  98.2007  33.6589 0001234  89.2782  18.9934
 14.57114995112342",
        "validTimeRange": {
            "startTime": datetime.now(timezone.utc) + timedelta(days=3),
            "endTime": datetime.now(timezone.utc) + timedelta(days=7),
        },
    },
]

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

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

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

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

s3_tle_ephemeris = ground_station_client.create_ephemeris(
    name="2022-11-05 S3 TLE Upload",
    satelliteId="fde41049-14f7-413e-bd7b-EXAMPLE01",
```

```
    enabled=True,
    expirationTime=datetime.now(timezone.utc) + timedelta(days=5),
    priority=2,
    ephemeris={"tle": {"s3Object": {"bucket": bucket_name, "key": object_key}}},
)

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

Stellen Sie OEM-Ephemeridendaten bereit

> **Important**
>
> Die Ephemeriden-API befindet sich derzeit im Vorschaustatus

Der Zugriff auf die Ephemeris-API wird nur bei Bedarf gewährt. Wenn Sie die Möglichkeit benötigen, benutzerdefinierte Ephemeridendaten hochzuladen, öffnen Sie bitte ein Ticket über. AWS Support AWS Support Center Console Unser Team wird mit Ihnen zusammenarbeiten, um diese Funktion für Ihre spezifischen Anforderungen zu aktivieren.

-Übersicht

Orbit Ephemeris Message (OEM) ist ein standardisiertes Format zur Darstellung von Flugbahndaten von Raumfahrzeugen. Die Ephemeris-API ermöglicht das Hochladen von OEM-Ephemeriden zur Verwendung mit einem Satelliten. AWS Ground Station Diese Ephemeriden überschreiben die Standard-Ephemeriden von Space-Track (siehe:). Standard-Ephemeridendaten

AWS Ground Station behandelt Ephemeriden als individualisierte Nutzungsdaten. Wenn Sie diese optionale Funktion verwenden, AWS werden Ihre Ephemeridendaten verwendet, um Unterstützung bei der Fehlerbehebung zu bieten.

Durch das Hochladen benutzerdefinierter OEM-Ephemeriden kann die Qualität der Ortung verbessert, frühe Einsätze, für die keine Space-Track-Ephemeriden verfügbar sind, durchgeführt und Manöver berücksichtigt werden. AWS Ground Station

> **Note**
>
> Wenn Sie benutzerdefinierte Ephemeriden bereitstellen, bevor Ihrem Satelliten eine Satellitenkatalognummer zugewiesen wird, können Sie diese für den Teil des OEM verwenden. `satelliteId` `OBJECT_ID`

Weitere Informationen zum Format von OEMs finden Sie unter. OEM-Format für Ephemeriden

OEM-Format für Ephemeriden

AWS Ground Station verarbeitet vom OEM-Kunden bereitgestellte Ephemeriden gemäß dem CCSDS-Standard mit einigen zusätzlichen Einschränkungen. OEM-Dateien sollten im KVN-Format vorliegen. In der folgenden Tabelle werden die verschiedenen Felder in einem OEM und die AWS Ground Station Unterschiede zum CCSDS-Standard beschrieben.

Abschnitt	Feld	CCSDS erforderlich	AWS Ground Station erforderlich	Hinweise
Header	CCSDS_OEM_VERS	Ja	Ja	Erforderlicher Wert: 2,0
	COMMENT	Nein	Nein	
	EINSTUFUNG	Nein	Nein	
	ERSTELLUNGSDATUM	Ja	Ja	
	URHEBER	Ja	Ja	
	NACHRICHTEN-ID	Nein	Nein	
Metadaten	META_START	Ja	Ja	
	COMMENT	Nein	Nein	
	OBJEKTNAME	Ja	Ja	
	OBJEKT-ID	Ja	Ja	
	NAME DES ZENTRUMS	Ja	Ja	Erforderlicher Wert: Erde

Abschnitt	Feld	CCSDS erforderlich	AWS Ground Station erforderlich	Hinweise
	REF_FRAME	Ja	Ja	Zulässige Werte:, EME2000 ITRF2000
	REF_FRAME_EPOCH	Nein	Nicht unterstützt*	Nicht erforderlich, da die akzeptierten REF_ FRAMEs eine implizite Epoche haben
	TIME_SYSTEM	Ja	Ja	Erforderlicher Wert: UTC
	START_TIME	Ja	Ja	
	VERWENDBARE_STARTZEIT	Nein	Nein	
	VERWENDBARE STOPPZEIT	Nein	Nein	
	STOPPZEIT	Ja	Ja	
	INTERPOLATION	Nein	Ja	Erforderlich, AWS Ground Station damit genaue Zeigewinkel für Kontakte generiert werden können.

Abschnitt	Feld	CCSDS erforderlich	AWS Ground Station erforderlich	Hinweise
	INTERPOLATION_DEGREE	Nein	Ja	Erforderlich, damit genaue Zeigewinkel für Kontakte generiert werden AWS Ground Station können.
	META_STOP	Ja	Ja	
Daten	X	Ja	Ja	Vertreten in `km`
	Y	Ja	Ja	Vertreten in `km`
	Z	Ja	Ja	Vertreten in `km`
	X_DOT	Ja	Ja	Vertreten in `km/s`
	Y_DOT	Ja	Ja	Vertreten in `km/s`
	Z_DOT	Ja	Ja	Vertreten in `km/s`
	X_DOT	Nein	Nein	Vertreten in `km/s^2`
	Y_DDOT	Nein	Nein	Vertreten in `km/s^2`
	Z_DDOT	Nein	Nein	Vertreten in `km/s^2`

Abschnitt	Feld	CCSDS erforderlich	AWS Ground Station erforderlich	Hinweise
Kovarianzmatrix	KOVARIANZ_START	Nein	Nein	
	EPOCHE	Nein	Nein	
	COV_REF_FRAME	Nein	Nein	
	KOVARIANZ STOPP	Nein	Nein	

* Wenn Zeilen, die von nicht unterstützt werden, im bereitgestellten OEM enthalten AWS Ground Station sind, schlägt der OEM die Validierung fehl.

Die wichtigsten Abweichungen vom CCSDS-Standard für AWS Ground Station sind:

- `CCSDS_OEM_VERS`muss sein. `2.0`
- `REF_FRAME`muss entweder `EME2000` oder sein `ITRF2000`.
- `REF_FRAME_EPOCH`wird nicht unterstützt von AWS Ground Station.
- `CENTER_NAME`muss sein`Earth`.
- `TIME_SYSTEM`muss sein`UTC`.
- `INTERPOLATION`und `INTERPOLATION_DEGREE` sind beide für vom AWS Ground Station Kunden bereitgestellte Ephemeriden erforderlich.

Beispiel für eine OEM-Ephemeride im KVN-Format

Im Folgenden finden Sie ein gekürztes Beispiel für eine OEM-Ephemeride im KVN-Format für den öffentlichen Rundfunksatelliten JPSS-1.

```
CCSDS_OEM_VERS = 2.0

COMMENT Orbit data are consistent with planetary ephemeris DE-430
```

```
CREATION_DATE  = 2024-07-22T05:20:59
ORIGINATOR     = Raytheon-JPSS/CGS

META_START
OBJECT_NAME          = J1
OBJECT_ID            = 2017-073A
CENTER_NAME          = Earth
REF_FRAME            = EME2000
TIME_SYSTEM          = UTC
START_TIME           = 2024-07-22T00:00:00.000000
STOP_TIME            = 2024-07-22T00:06:00.000000
INTERPOLATION        = Lagrange
INTERPOLATION_DEGREE = 5
META_STOP

2024-07-22T00:00:00.000000   5.905147360000000e+02  -1.860082793999999e+03
  -6.944807075000000e+03  -5.784245796000000e+00   4.347501391999999e+00
 -1.657256863000000e+00
2024-07-22T00:01:00.000000   2.425572045154201e+02  -1.595860765983339e+03
  -7.030938457373539e+03  -5.810660250794190e+00   4.457103652219009e+00
 -1.212889340333023e+00
2024-07-22T00:02:00.000000  -1.063224256538050e+02  -1.325569732497146e+03
  -7.090262617183503e+03  -5.814973972202444e+00   4.549739160042560e+00
 -7.639633689161465e-01
2024-07-22T00:03:00.000000  -4.547973959231161e+02  -1.050238305712201e+03
  -7.122556683227951e+03  -5.797176562437553e+00   4.625064829516728e+00
 -3.121687831090774e-01
2024-07-22T00:04:00.000000  -8.015427368657785e+02  -7.709137891269565e+02
  -7.127699477194810e+03  -5.757338007808417e+00   4.682800822515077e+00
 1.407953645161997e-01
2024-07-22T00:05:00.000000  -1.145240083085062e+03  -4.886583601179489e+02
  -7.105671911254255e+03  -5.695608435738609e+00   4.722731329786999e+00
 5.932259682105052e-01
2024-07-22T00:06:00.000000  -1.484582479061495e+03  -2.045451985605701e+02
  -7.056557069672793e+03  -5.612218005854990e+00   4.744705579872771e+00
 1.043421397392599e+00
```

Erstellen einer OEM-Ephemeride

Eine OEM-Ephemeride kann mithilfe der CreateEphemerisAktion in der API erstellt werden. AWS Ground Station Bei dieser Aktion wird eine Ephemeride mithilfe von Daten hochgeladen, die entweder im Anfragetext oder aus einem bestimmten S3-Bucket enthalten sind.

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 Status der Ephemeriden DescribeEphemerisabfragen oder CloudWatch Ereignisse verwenden, um die Statusänderungen der Ephemeriden nachzuverfolgen.

Informationen zur Fehlerbehebung bei einer ungültigen Ephemeride finden Sie unter: Fehlerbehebung bei ungültigen Ephemeriden

Beispiel: OEM-Ephemeridendaten aus einem S3-Bucket hochladen

Es ist auch möglich, eine OEM-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 in AWS Ground Station finden Sie in:Datenverschlüsselung im Ruhezustand für AWS Ground Station.

Im Folgenden finden Sie ein Beispiel für das Hochladen einer OEM-Ephemeridendatei aus einem S3-Bucket

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

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

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

# Create sample OEM data in KVN format
oem_data = """CCSDS_OEM_VERS = 2.0

COMMENT Orbit data are consistent with planetary ephemeris DE-430

CREATION_DATE  = 2024-07-22T05:20:59
ORIGINATOR     = Raytheon-JPSS/CGS

META_START
OBJECT_NAME          = J1
OBJECT_ID            = 2017-073A
```

```
CENTER_NAME          = Earth
REF_FRAME            = EME2000
TIME_SYSTEM          = UTC
START_TIME           = 2024-07-22T00:00:00.000000
STOP_TIME            = 2024-07-22T00:06:00.000000
INTERPOLATION        = Lagrange
INTERPOLATION_DEGREE = 5
META_STOP

2024-07-22T00:00:00.000000   5.905147360000000e+02  -1.860082793999999e+03
  -6.944807075000000e+03  -5.784245796000000e+00   4.347501391999999e+00
 -1.657256863000000e+00
2024-07-22T00:01:00.000000   2.425572045154201e+02  -1.595860765983339e+03
  -7.030938457373539e+03  -5.810660250794190e+00   4.457103652219009e+00
 -1.212889340333023e+00
2024-07-22T00:02:00.000000  -1.063224256538050e+02  -1.325569732497146e+03
  -7.090262617183503e+03  -5.814973972202444e+00   4.549739160042560e+00
 -7.639633689161465e-01
2024-07-22T00:03:00.000000  -4.547973959231161e+02  -1.050238305712201e+03
  -7.122556683227951e+03  -5.797176562437553e+00   4.625064829516728e+00
 -3.121687831090774e-01
2024-07-22T00:04:00.000000  -8.015427368657785e+02  -7.709137891269565e+02
  -7.127699477194810e+03  -5.757338007808417e+00   4.682800822515077e+00
 1.407953645161997e-01
2024-07-22T00:05:00.000000  -1.145240083085062e+03  -4.886583601179489e+02
  -7.105671911254255e+03  -5.695608435738609e+00   4.722731329786999e+00
 5.932259682105052e-01
2024-07-22T00:06:00.000000  -1.484582479061495e+03  -2.045451985605701e+02
  -7.056557069672793e+03  -5.612218005854990e+00   4.744705579872771e+00
 1.043421397392599e+00
"""

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

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

print("OEM data uploaded successfully to S3")

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

```
s3_oem_ephemeris = ground_station_client.create_ephemeris(
    name="2024-07-22 S3 OEM Upload",
    satelliteId="fde41049-14f7-413e-bd7b-EXAMPLE01",
    enabled=True,
    expirationTime=datetime.now(timezone.utc) + timedelta(days=5),
    priority=2,
    ephemeris={"oem": {"s3Object": {"bucket": bucket_name, "key": object_key}}},
)

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

Im Folgenden finden Sie ein Beispiel für zurückgegebene Daten aus der DescribeEphemerisAktion, 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"
      }
    }
  }
}
```

Geben Sie Azimut-Elevations-Ephemeridendaten an

Important

Die Funktion „Azimut-Elevation-Ephemeride“ befindet sich derzeit im Vorschaustatus und erfordert eine explizite Einführung.
Die Azimut-Elevation-Ephemeridenfunktion unterliegt einer strengen Zugriffskontrolle für eine begrenzte Anzahl von vorab festgelegten, speziellen Anwendungsfällen. Der Zugriff ist deutlich restriktiver als bei standardmäßigen, vom Kunden bereitgestellten

Ephemeridenfunktionen. Für weitere Informationen über zugelassene Anwendungsfälle und den Prozess der Zugriffsanforderung öffnen Sie bitte ein AWS Support Ticket über die. AWS Support Center Console Unser Team führt Sie durch den Genehmigungsprozess für spezielle Anwendungsfälle.

-Übersicht

Die Azimut-Elevations-Ephemeride bietet die Möglichkeit, die Richtung der Antennenausrichtung direkt zu spezifizieren, ohne Informationen über die Umlaufbahn des Satelliten bereitzustellen. Anstatt Ephemeridendaten hochzuladen, die die Umlaufbahn eines Satelliten beschreiben, geben Sie Azimut- und Elevationswinkel mit Zeitmarkierungen an, die der Antenne genau sagen, wohin sie während eines Kontakts zeigen soll.

AWS Ground Station behandelt Ephemeriden als individualisierte Nutzungsdaten. Wenn Sie diese optionale Funktion verwenden, verwendet AWS Ihre Ephemeridendaten, um Unterstützung bei der Fehlerbehebung bereitzustellen.

Dieser Ansatz ist besonders nützlich für die folgenden Szenarien:

- Unterstützung in der Anfangsphase des Betriebs: Während der Start- und Early-Orbit-Phase (LEOP), wenn keine genauen Orbitaldaten verfügbar sind oder sich die Bahnparameter schnell ändern.
- Benutzerdefinierte Zeigemuster: Implementierung spezifischer Zeigesequenzen für Antennentests oder für nicht standardmäßige Operationen.

Note

Bei Verwendung der Azimut-Elevations-Ephemeride kann der Satelliten-ARN in der Kontaktreservierungsanfrage weggelassen werden. Wenn das Satelliten-ARN nicht weggelassen wird, wird es trotzdem als Teil der Kontaktdaten aufgenommen, aber die Azimuthöhen-Ephemeride wird für die Antennenausrichtung verwendet, anstatt die Ephemeriden-Prioritätsauflösung durchzuführen. Die Azimuthöhen-Ephemeride ist einer bestimmten Bodenstation zugeordnet und definiert die Richtungsrichtungen der Antenne für diesen Standort.

Datenformat der Azimut-Elevations-Ephemeride

Ephemeridendaten zur Azimut-Höhe bestehen aus Azimut- und Höhenwerten mit Zeitangabe, die in Segmenten angeordnet sind. Jedes Segment enthält eine Reihe von Azimut- und Höhenwinkeln, die einen bestimmten Zeitraum abdecken.

Die wichtigsten Komponenten der Azimut-Elevations-Ephemeridendaten sind:

- Ground Station: Die spezifische Bodenstation, an der diese Azimuthöhen-Ephemeride verwendet wird.
- Winkeleinheit: Die Maßeinheit für Winkel (oder). `DEGREE_ANGLE` `RADIAN`
- Segmente: Eine oder mehrere zeitlich begrenzte Sammlungen von Azimut- und Elevationswinkeln.
- Winkel mit Zeitangabe: Einzelne Azimut- und Höhenwerte mit zugehörigen Zeitstempeln.

Für jedes Segment ist Folgendes erforderlich:

- Eine Referenzepoche (die Basiszeit für das Segment)
- Ein gültiger Zeitraum (Start- und Endzeit für das Segment)
- Mindestens 5 Paare mit Zeitangaben azimuth/elevation

Einschränkungen der Azimut-Elevation:

- Azimut in Grad: -180° bis 360°
- Azimut im Bogenmaß: -π bis 2π
- Höhe in Grad: -90° bis 90°
- Höhe im Bogenmaß: -π /2 bis π /2
- Die Zeitwerte müssen innerhalb jedes Segments in aufsteigender Reihenfolge angegeben werden
- Segmente dürfen sich zeitlich nicht überlappen

Weitere Informationen finden Sie in der CreateEphemerisAPI-Dokumentation und zum TimeAzElDatentyp.

Eine Azimut-Elevations-Ephemeride erstellen

Die Azimut-Elevation-Ephemeride wird mit derselben CreateEphemerisAPI-Aktion erstellt, jedoch mit dem Ephemeridentyp. `azEl` Die wichtigsten Unterschiede zu TLE- und OEM-Ephemeriden sind:

- Sie müssen einen Parameter angeben `groundStation`
- Der `satelliteId` Parameter muss in der Anfrage weggelassen werden
- Die Prioritätseinstellungen gelten nicht (jede Azimut-Elevations-Ephemeride ist spezifisch für eine Bodenstation)
- Jedes Segment muss mindestens 5 azimuth/elevation Punkte enthalten, um die Lagrange-Interpolation 4. Ordnung zu unterstützen
- Zusätzliche Beschränkungen und Anforderungen sind in der API-Dokumentation detailliert beschrieben CreateEphemeris

Es ist wichtig zu beachten, dass durch das Hochladen einer Ephemeride die Ephemeride in einen asynchronen Workflow umgewandelt `VALIDATING` und gestartet wird, der potenzielle Kontakte anhand Ihrer Ephemeride validiert und generiert. Eine Ephemeride wird erst dann für Kontakte verwendet, wenn sie diesen Workflow bestanden hat und ihr Status lautet. `ENABLED` Sie sollten den Ephemeridenstatus DescribeEphemerisabfragen oder CloudWatch Ereignisse verwenden, um die Statusänderungen der Ephemeriden nachzuverfolgen.

Informationen zur Fehlerbehebung bei einer ungültigen Ephemeride finden Sie unter: Fehlerbehebung bei ungültigen Ephemeriden

Beispiel: Eine Azimut-Elevations-Ephemeride per API erstellen

Das folgende Beispiel zeigt, wie Sie mit dem AWS SDK for Python (Boto3) eine Azimut-Elevations-Ephemeride erstellen:

```
import boto3

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

# Create azimuth elevation ephemeris
azimuth_elevation_ephemeris = ground_station_client.create_ephemeris(
    name="Azimuth Elevation for Ohio Ground Station",
    ephemeris={
        "azEl": {
            "groundStation": "Ohio 1",
            "data": {
                "azElData": {
                    "angleUnit": "DEGREE_ANGLE",
                    "azElSegmentList": [
```

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

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

In diesem Beispiel:

- Die Azimut-Höhendaten sind der Bodenstation „Ohio 1" zugeordnet
- Winkel werden in Grad angegeben
- Das Segment deckt einen Zeitraum von 15 Minuten ab
- Die `dt` Werte sind Atomsekunden, die von der Referenzepoche abweichen
- Es stehen sechs azimuth/elevation Paare zur Verfügung (mindestens 5)

Beispiel: Laden Sie Azimut-Höhendaten von S3 hoch

Für größere Datensätze können Sie Azimut-Höhendaten aus einem S3-Bucket hochladen:

```
import boto3
import json

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

```
ground_station_client = boto3.client("groundstation")

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

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

# Upload sample data to S3
```

```
print(f"Uploading azimuth elevation data to s3://{bucket_name}/{object_key}")

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

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

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

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

Das S3-Objekt sollte eine JSON-Struktur mit den Azimut-Höhendaten im gleichen Format enthalten, wie im direkten Upload-Beispiel gezeigt.

Kontakte mit Azimut-Elevations-Ephemeriden reservieren

Bei der Verwendung einer Azimut-Elevations-Ephemeride zur Reservierung eines Kontakts unterscheidet sich das Verfahren von TLE- und OEM-Ephemeriden:

1. Erstellen Sie die Azimut-Elevations-Ephemeride mit CreateEphemeris
2. Warten Sie, bis die Ephemeride den Status erreicht hat `ENABLED`
3. Reservieren Sie den Kontakt mithilfe von ReserveContactTracking-Overrides

Beispiel für die Reservierung eines Kontakts mit einer Azimut-Elevations-Ephemeride:

```
import boto3
from datetime import datetime
```

```
import time

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

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

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

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

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

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

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

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

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

> **Note**
>
> Der `satelliteArn` Parameter kann weggelassen werden, wenn ein Kontakt mit einer Azimut-Elevations-Ephemeride reserviert wird. Die Antenne folgt während des Kontakts den angegebenen Azimut- und Elevationswinkeln.

Verfügbare Kontakte auflisten

Bei der Verwendung von Azimut-Elevation-Ephemeriden benötigt die ListContactsAPI bestimmte Parameter:

- Der `satelliteArn` Parameter kann in der Anfrage weggelassen werden

- Sie müssen einen `ephemeris` Parameter mit der Azimut-Elevation-Ephemeriden-ID angeben, um anzugeben, welche Ephemeride verwendet werden soll
- Verfügbare Kontaktfenster zeigen an, wann der angegebene Azimut- und Elevationswinkel über der Standortmaske der angeforderten Bodenstation liegt
- Sie müssen immer noch angeben und `groundStation` `missionProfileArn`

Beispiel für die Erstellung einer Azimut-Elevations-Ephemeride und die damit verbundene Auflistung verfügbarer Kontakte:

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

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

# Step 1: Create azimuth elevation ephemeris
print("Creating azimuth elevation ephemeris...")
ephemeris_response = ground_station_client.create_ephemeris(
    name="Stockholm AzEl Ephemeris",
    ephemeris={
        "azEl": {
            "groundStation": "Stockholm 1",
            "data": {
                "azElData": {
                    "angleUnit": "DEGREE_ANGLE",
                    "azElSegmentList": [
                        {
                            "referenceEpoch": "2024-04-01T12:00:00Z",
                            "validTimeRange": {
                                "startTime": "2024-04-01T12:00:00Z",
                                "endTime": "2024-04-01T12:30:00Z",
                            },
                            "azElList": [
                                {"dt": 0.0, "az": 30.0, "el": 15.0},
                                {"dt": 360.0, "az": 45.0, "el": 30.0},
                                {"dt": 720.0, "az": 60.0, "el": 45.0},
                                {"dt": 1080.0, "az": 75.0, "el": 35.0},
                                {"dt": 1440.0, "az": 90.0, "el": 20.0},
                                {"dt": 1800.0, "az": 105.0, "el": 10.0},
                            ],
```

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

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

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

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

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

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

# Convert epoch timestamps to datetime objects
start_time = datetime.fromtimestamp(1760710513, tz=timezone.utc)
end_time = datetime.fromtimestamp(1760883313, tz=timezone.utc)

contacts_response = ground_station_client.list_contacts(
    startTime=start_time,
    endTime=end_time,
    groundStation="Stockholm 1",
    statusList=["AVAILABLE"],
    ephemeris={"azEl": {"id": ephemeris_id}},
```

```
    # satelliteArn is optional
    satelliteArn="arn:aws:groundstation::111122223333:satellite/a88611b0-f755-404e-
b60d-57d8aEXAMPLE",
    missionProfileArn="arn:aws:groundstation:eu-north-1:111122223333:mission-
profile/966b72f6-6d82-4e7e-b072-f8240EXAMPLE",
)

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

> **Note**
>
> Der `ephemeris` Parameter mit der Azimut-Elevation-ID muss beim Auflisten von Kontakten angegeben werden, um anzugeben, welche Azimut-Elevation-Ephemeride für die Bestimmung von Kontaktfenstern verwendet werden soll. Wenn das angegeben `satelliteArn` ist, wird es mit den Kontaktdaten verknüpft, aber die Azimut-Elevations-Ephemeride wird für die Antennenausrichtung verwendet, anstatt die Ephemeriden-Prioritätsauflösung durchzuführen.

Reservieren Sie Kontakte mit benutzerdefinierten Ephemeriden

-Übersicht

Wenn Sie benutzerdefinierte Ephemeriden (TLE, OEM oder Azimut-Elevation) verwenden, können Sie Kontakte über die API reservieren. ReserveContact In diesem Abschnitt werden zwei gängige Workflows für die Reservierung von Kontakten sowie wichtige Überlegungen zur Sicherstellung einer erfolgreichen Kontaktplanung beschrieben.

AWS Ground Station Antennen sind Ressourcen, die von mehreren Kunden gemeinsam genutzt werden. Das bedeutet, dass selbst wenn ein Kontaktfenster verfügbar erscheint, wenn Sie

Kontakte auflisten, ein anderer Kunde es möglicherweise vor Ihnen reserviert. Daher ist es wichtig, sicherzustellen, dass Ihr Kontakt den `SCHEDULED` Status nach der Reservierung erreicht hat, und für eine angemessene Überwachung bei Änderungen des Kontaktstatus zu sorgen.

> **Important**
>
> Bei azimutalen Elevations-Ephemeriden kann der `satelliteArn` Parameter in der `ReserveContact` Anfrage weggelassen werden und Sie müssen die Ephemeriden-ID angeben`trackingOverrides`. Für TLE- und OEM-Ephemeriden müssen Sie dennoch die angeben. `satelliteArn`

Workflows für Kontaktreservierungen

Es gibt zwei Hauptworkflows für die Reservierung von Kontakten mit benutzerdefinierten Ephemeriden:

1. List-then-reserve Arbeitsablauf: Zuerst die verfügbaren Kontaktfenster mithilfe auflisten ListContacts, dann ein bestimmtes Fenster auswählen und reservieren. Dieser Ansatz ist nützlich, wenn Sie alle verfügbaren Möglichkeiten sehen möchten, bevor Sie eine Auswahl treffen.
2. Direkter Reservierungsablauf: Reservieren Sie einen Kontakt direkt für ein bestimmtes Zeitfenster, ohne zuerst die verfügbaren Kontakte aufzulisten. Dieser Ansatz ist nützlich, wenn Sie Ihre gewünschte Kontaktzeit bereits kennen oder mit festgelegten Zeitplänen arbeiten.

Beide Workflows sind gültig und die Wahl hängt von Ihren betrieblichen Anforderungen ab. Die folgenden Abschnitte enthalten Beispiele für jeden Ansatz.

Arbeitsablauf 1: Verfügbare Kontakte auflisten und dann reservieren

Dieser Workflow fragt zuerst nach verfügbaren Kontaktfenstern und reserviert dann ein bestimmtes Fenster. Dies ist nützlich, wenn Sie alle verfügbaren Opportunities sehen möchten, bevor Sie eine Auswahl treffen.

Beispiel: Ephemeriden mit Azimut-Elevation auflisten und reservieren

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

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

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

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

# Wait for ephemeris to become ENABLED
while True:
    status = ground_station_client.describe_ephemeris(ephemerisId=ephemeris_id)[
        "status"
    ]
```

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

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

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

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

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

Beispiel: Mit TLE-Ephemeriden auflisten und reservieren

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

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

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

# Create TLE ephemeris
print("Creating TLE ephemeris...")
ephemeris_response = ground_station_client.create_ephemeris(
    name="TLE Ephemeris for Contact",
    satelliteId=satellite_id,
    enabled=True,
    expirationTime=datetime.now(timezone.utc) + timedelta(days=7),
    priority=1,  # Higher priority than default ephemeris
    ephemeris={
        "tle": {
            "tleData": [
                {
                    "tleLine1": "1 25994U 99068A   24075.54719794  .00000075  00000-0
 26688-4 0  9997",
                    "tleLine2": "2 25994  98.2007  30.6589 0001234  89.2782  18.9934
 14.57114995111906",
                    "validTimeRange": {
                        "startTime": datetime.now(timezone.utc),
                        "endTime": datetime.now(timezone.utc) + timedelta(days=7),
                    },
                }
            ]
        }
    },
)

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

# Wait for ephemeris to become ENABLED
while True:
```

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

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

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

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

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

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

```
    print("No available contacts found")
```

Workflow 2: Direkte Kontaktreservierung

Dieser Workflow reserviert direkt einen Kontakt, ohne zuerst die verfügbaren Fenster aufzulisten. Dieser Ansatz ist nützlich, wenn Sie Ihre gewünschte Kontaktzeit bereits kennen oder eine automatisierte Terminplanung implementieren.

Beispiel: Direkte Reservierung mit azimutaler Elevations-Ephemeride

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

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

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

# Create azimuth elevation ephemeris for the specific contact time
print("Creating azimuth elevation ephemeris...")
ephemeris_response = ground_station_client.create_ephemeris(
    name="Direct Contact AzEl Ephemeris",
    ephemeris={
        "azEl": {
            "groundStation": "Ohio 1",
            "data": {
                "azElData": {
                    "angleUnit": "DEGREE_ANGLE",
                    "azElSegmentList": [
                        {
                            "referenceEpoch": contact_start.isoformat(),
                            "validTimeRange": {
                                "startTime": contact_start.isoformat(),
                                "endTime": contact_end.isoformat(),
                            },
                            "azElList": [
                                {"dt": 0.0, "az": 45.0, "el": 10.0},
                                {"dt": 180.0, "az": 50.0, "el": 15.0},
                                {"dt": 360.0, "az": 55.0, "el": 20.0},
                                {"dt": 540.0, "az": 60.0, "el": 25.0},
```

```
                                {"dt": 720.0, "az": 65.0, "el": 30.0},
                                {"dt": 900.0, "az": 70.0, "el": 35.0},
                            ],
                        }
                    ],
                }
            },
        }
    },
)

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

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

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

reservation = ground_station_client.reserve_contact(
    # Note: satelliteArn is omitted for azimuth elevation
    missionProfileArn="arn:aws:groundstation:us-east-2:111122223333:mission-profile/
example-profile",
    groundStation="Ohio 1",
    startTime=contact_start,
    endTime=contact_end,
    trackingOverrides={"programTrackSettings": {"azEl": {"ephemerisId":
 ephemeris_id}}},
)

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

Beispiel: Direktreservierung mit TLE-Ephemeriden

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

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

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

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

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

ephemeris_id = ephemeris_response["ephemerisId"]
```

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

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

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

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

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

Überwachung von Änderungen des Kontaktstatus

Nach der Reservierung eines Kontakts ist es wichtig, seinen Status zu überwachen, um sicherzustellen, dass der Übergang erfolgreich ist, `SCHEDULED` und um bei Problemen benachrichtigt zu werden. AWS Ground Station sendet Ereignisse an Amazon EventBridge für alle Änderungen des Kontaktstatus.

Kontaktstatus folgen diesem Lebenszyklus:

- `SCHEDULING`- Der Kontakt wird zur Terminplanung bearbeitet
- `SCHEDULED`- Der Kontakt wurde erfolgreich geplant und wird ausgeführt
- `FAILED_TO_SCHEDULE`- Der Kontakt konnte nicht geplant werden (Terminalstatus)

Weitere Informationen zu Kontaktstatus und Lebenszyklus finden Sie unterVerstehen Sie den Lebenszyklus von Kontakten.

Implementierung der Kontaktstatusüberwachung mit EventBridge

Um Änderungen des Kontaktstatus in Echtzeit zu überwachen, können Sie eine EventBridge Amazon-Regel einrichten, die eine Lambda-Funktion auslöst, wenn sich der Status eines Bodenstationskontakts ändert. Dieser Ansatz ist effizienter und skalierbarer als die Abfrage des Kontaktstatus.

Implementierungsschritte

1. Erstellen Sie eine Lambda-Funktion zur Verarbeitung von Ereignissen zur Änderung des Kontaktstatus
2. Erstellen Sie eine EventBridge Regel, die den Ereignissen zur Änderung des Kontaktstatus der Ground Station entspricht
3. Fügen Sie die Lambda-Funktion als Ziel für die Regel hinzu

Beispiel für einen Lambda-Funktionshandler

Ein vollständiges Beispiel für eine Lambda-Funktion, die Ereignisse zur Änderung des Kontaktstatus verarbeitet, finden Sie in der `GroundStationCloudWatchEventHandlerLambda` Ressource in der `AquaSnppJpssTerraDigIF.yml` CloudFormation Vorlage. Diese Vorlage ist im Amazon S3 S3-Bucket für AWS Ground Station Kunden verfügbar. Anweisungen zum Zugriff auf diese Vorlage finden Sie im Es zusammensetzen Abschnitt des Beispiels für einen Datenfluss-Endpunkt.

EventBridge Konfiguration der Regeln

Die EventBridge Regel sollte das folgende Ereignismuster verwenden, um allen Änderungen des Kontaktstatus der Ground Station Rechnung zu tragen:

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

Um nur nach bestimmten Zuständen zu filtern (z. B. nach Ausfällen), können Sie einen Detailfilter hinzufügen:

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

Ausführliche Anweisungen zum Erstellen von EventBridge Regeln mit Lambda-Zielen finden Sie unter Erstellen von Regeln, die auf Ereignisse reagieren im EventBridge Amazon-Benutzerhandbuch.

EventBridge Regeln für die Automatisierung einrichten

Sie können EventBridge Regeln erstellen, um automatisch auf Änderungen des Kontaktstatus zu reagieren. Beispiel:

- Senden Sie Benachrichtigungen, wenn ein Kontakt den Terminplan nicht einhält
- Lambda-Funktionen auslösen, um Ressourcen vorzubereiten, wenn ein Kontakt eintritt `PREPASS`
- Protokollieren Sie den Abschluss von Kontakten zu Prüfungszwecken

Ausführliche Informationen zum Einrichten von EventBridge Regeln für AWS Ground Station Ereignisse finden Sie unterAutomatisieren Sie AWS Ground Station mit Ereignissen.

Bewährte Methoden und Überlegungen

Umgang mit Terminkonflikten

Da es sich bei AWS Ground Station Antennen um gemeinsam genutzte Ressourcen handelt, wurde ein Kontaktfenster, das unter verfügbar angezeigt wird, `ListContacts` möglicherweise von einem anderen Kunden reserviert, bevor Sie es reservieren können. Um das zu handhaben:

1. Überprüfen Sie nach der Reservierung immer den Kontaktstatus
2. Implementieren Sie die Wiederholungslogik mit alternativen Zeitfenstern

3. Erwägen Sie, Kontakte möglichst weit im Voraus zu reservieren
4. Verwenden Sie EventBridge Ereignisse, um nach Staaten Ausschau zu halten `FAILED_TO_SCHEDULE`

Zeitplan für die Validierung von Ephemeriden

Denken Sie daran, dass die Ephemeride aktiviert sein muss, bevor `ENABLED` Sie sie zum Reservieren von Kontakten verwenden können. Der Validierungsprozess dauert je nach Art und Größe der Ephemeriden in der Regel einige Sekunden bis einige Minuten. Überprüfen Sie immer den Status der Ephemeriden, bevor Sie versuchen, Kontakte zu reservieren.

Überlegungen zum Zeitpunkt der Kontaktaufnahme

Wenn Sie benutzerdefinierte Ephemeriden verwenden:

- Stellen Sie sicher, dass Ihre Ephemeride die gesamte Kontaktdauer abdeckt
- Stellen Sie bei Azimut-Ephemeriden sicher, dass die Antenne aufgrund der Winkel während des gesamten Kontakts über der Ortsmaske bleibt
- Berücksichtigen Sie bei der Planung future Kontakte die Ablaufzeiten von Ephemeriden

API-Unterschiede je nach Ephemeridentyp

Die `ReserveContact` API verhält sich je nach Ephemeridentyp unterschiedlich:

Ephemeriden-Typ	SatellitARN erforderlich	TrackingOverrides erforderlich
TEL	Ja	Nein (optional)
OEM	Ja	Nein (optional)
Azimut-Elevation	Nein (optional)	Ja

Verstehe, welche Ephemeride verwendet wird

Ephemeriden haben eine Priorität, eine Ablaufzeit und eine Aktivierungskennzeichnung. Zusammen bestimmen sie, welche Ephemeride für die Nachverfolgung während eines Kontakts verwendet wird.

TLE- und OEM-Ephemeriden

Bei OEM- und TLE-Ephemeriden kann für jeden Satelliten nur eine Ephemeride aktiv sein. Die Ephemeride, die verwendet wird, ist die aktivierte Ephemeride mit der höchsten Priorität, deren Ablaufzeit in der future liegt. Ein höherer Prioritätswert weist auf eine höhere Priorität hin. Die von zurückgegebenen verfügbaren Kontaktzeiten ListContactsbasieren auf dieser Ephemeride. Wenn mehrere `ENABLED` Ephemeriden dieselbe Priorität haben, wird die zuletzt erstellte oder aktualisierte Ephemeride verwendet.

> **Note**
>
> AWS Ground Station hat eine Servicequote 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 UpdateEphemerisEphemeriden.

Wenn keine Ephemeriden erstellt wurden oder keine Ephemeriden einen `ENABLED` Status haben, wird eine Standard-Ephemeride für den Satelliten (von Space-Track) verwendet, AWS Ground Station sofern verfügbar. Diese Standard-Ephemeride hat Priorität 0.

Azimut-Elevations-Ephemeriden

Azimut-Elevation-Ephemeriden funktionieren anders als OEM- und TLE-Ephemeriden. Jede Azimuthöhen-Ephemeride ist einer bestimmten Bodenstation zugeordnet und hat keine Priorität. Wenn Sie einen Kontakt mit Azimut-Elevation-Ephemeriden reservieren, geben Sie über den Parameter explizit an, welche Azimut-Elevation-Ephemeride verwendet werden soll. `tracking0verrides`

Hauptunterschiede bei Azimut-Elevations-Ephemeriden:

- Kein Prioritätssystem — Sie wählen die Ephemeriden für jeden Kontakt explizit aus
- Bodenstationsspezifisch — jede Ephemeride ist einer bestimmten Bodenstation zugeordnet
- Kein automatischer Fallback — wenn die angegebene Ephemeride nicht verfügbar ist, schlägt der Kontakt fehl

> **Note**
>
> Azimut-Elevations-Ephemeriden konkurrieren nicht mit OEM- und TLE-Ephemeriden. Sie werden bei der Reservierung eines Kontakts explizit ausgewählt und nur verwendet, wenn Tracking-Overrides angegeben sind.

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.

Bei OEM- und TLE-Ephemeriden behalten Kontakte, die vor dem Hochladen einer neuen Ephemeride geplant wurden, die ursprünglich geplante Kontaktzeit bei, während für die Antennenverfolgung die aktive Ephemeride verwendet wird. Wenn die Position des Raumfahrzeugs, basierend auf der aktiven Ephemeride, stark von der vorherigen Ephemeride abweicht, kann dies zu einer kürzeren Kontaktzeit des Satelliten mit der Antenne führen, da das Raumfahrzeug außerhalb der Ortsmaske operiert. transmit/receive 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 transmit/receive Standortmaske operiert, indem Sie Ihren geplanten Kontakt `endTime` mit dem zurückgegebenen `startTime` `visibilityStartTime` und vergleichen. `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: Ground Station FAQs.

Für Ephemeriden mit Azimut-Elevation verwenden geplante Kontakte die spezifische Ephemeride, die bei der Reservierung des Kontakts ausgewählt wurde. Wenn Sie die Azimut-Höhendaten für einen geplanten Kontakt aktualisieren müssen, können Sie den Kontakt stornieren und mit einer neuen Ephemeride verschieben.

Ruft die aktuelle Ephemeride für einen Satelliten ab

Die aktuelle Ephemeride, die von AWS Ground Station einem bestimmten Satelliten verwendet wird, kann durch Aufrufen der Aktionen oder abgerufen werden. GetSatelliteListSatellites 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

> **Note**
>
> Azimut-Elevations-Ephemeriden sind nicht mit Satelliten verknüpft und werden daher nicht von oder zurückgegeben. GetSatelliteListSatellites Um Informationen über Azimuthöhen-Ephemeriden abzurufen, verwenden Sie die DescribeEphemerisAPI mit der spezifischen Ephemeriden-ID oder verwenden Sie, um alle verfügbaren Ephemeriden für Ihr Konto anzuzeigen. ListEphemerides

`sourceepoch`Standard-Ephemeriden enthalten nur Felder und. Dies `epoch` ist die Epoche des aus Space-Track stammenden Elementsatzes mit zwei Linien, 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 Upload 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 GetSatelliteRückgabe für einen Satelliten, der eine Standard-Ephemeride verwendet

```
{
    "satelliteId": "e1cfe0c7-67f9-4d98-bad2-EXAMPLE",
    "satelliteArn": "arn:aws:groundstation::111122223333:satellite/e1cfe0c7-67f9-4d98-
bad2-EXAMPLE",
```

```
    "noradSatelliteID": 25994,
    "groundStations": [
        "Ohio 1",
        "Oregon 1"
    ],
    "currentEphemeris": {
        "source": "SPACE_TRACK",
        "epoch": 1528245583.619
    }
}
```

Beispiel GetSatellitefür einen Satelliten, der eine benutzerdefinierte Ephemeride verwendet

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

Auflisten von Azimut-Elevations-Ephemeriden

Da Azimut-Elevations-Ephemeriden nicht mit Satelliten in Verbindung gebracht werden, müssen Sie verschiedene Optionen verwenden, um Informationen über sie zu finden und abzurufen: APIs

1. Verwenden Sie diese Option ListEphemerides, um alle Ephemeriden in Ihrem Konto aufzulisten, einschließlich Azimut-Elevations-Ephemeriden. Sie können nach Status und Ephemeridentyp filtern.
2. Verwenden Sie es DescribeEphemeriszusammen mit einer bestimmten Ephemeriden-ID, um detaillierte Informationen über eine Azimuthöhen-Ephemeride zu erhalten.

3. Verwenden Sie diese DescribeContactOption zusammen mit einer bestimmten Kontakt-ID, um detaillierte Informationen zu einer Ephemeride zu erhalten, die für den Kontakt verwendet wurde.

Beispiel für eine ListEphemeridesAntwort mit einer Ephemeride mit Azimut-Elevation:

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

> **Note**
>
> In der ListEphemeridesAntwort haben Azimut-Elevations-Ephemeriden ein `groundStation` Feld statt eines Feldes, sodass sie leicht zu identifizieren sind. `satelliteId`

Kehren Sie zu den Standard-Ephemeridendaten zurück

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 die Ablaufzeit der aktuellen, vom Kunden bereitgestellten Ephemeride überschritten haben, auch wenn nach dieser Ablaufzeit eine Standard-Ephemeride verfügbar ist.

> **Note**
>
> Azimut-Elevations-Ephemeriden haben keine Standardwerte und überschreiben keine Satelliten-Ephemeriden. Sie werden explizit ausgewählt, wenn ein Kontakt mithilfe des Parameters reserviert wird. `trackingOverrides` Wenn Sie die Azimut-Elevation-Ephemeride nicht mehr verwenden möchten, reservieren Sie einfach Kontakte ohne Angabe von Tracking-Overrides. Das System verwendet dann stattdessen die aktive Satelliten-Ephemeride.

Rückgängigmachen von TLE- und OEM-Ephemeriden

Um zu den Standard-Space-Track-Ephemeriden für einen Satelliten 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 GetSatelliteund überprüfen, ob die aktuelle Ephemeride für den Satelliten `source` verwendet wird. `SPACE_TRACK` Weitere Informationen zu Standard-Ephemeridendaten Standard-Ephemeriden finden Sie unter.

Verwaltung von Azimut-Elevations-Ephemeriden

Da Azimut-Elevation-Ephemeriden explizit für jeden Kontakt ausgewählt werden und nicht mit Satelliten verknüpft sind, gibt es kein Konzept, zu einer Standardeinstellung zurückzukehren. Stattdessen können Sie Azimut-Elevation-Ephemeriden wie folgt verwalten:

- Um die Verwendung von Azimut-Elevation-Ephemeriden zu beenden: Reservieren Sie einfach neue Kontakte, ohne a anzugeben und anzugeben. `trackingOverrides` `satelliteArn` Der Kontakt verwendet stattdessen die aktive Ephemeride für den angegebenen Satelliten.
- Um ungenutzte Azimut-Elevation-Ephemeriden zu entfernen: Dient DeleteEphemeriszum Löschen von Azimut-Elevation-Ephemeriden, die nicht mehr benötigt werden. Beachten Sie, dass Sie keine Ephemeride löschen können, die gerade von einem geplanten Kontakt verwendet wird.

Um alle Azimut-Elevations-Ephemeriden in Ihrem Konto aufzulisten, verwenden Sie. ListEphemerides Azimut-Elevations-Ephemeriden können anhand des Felds oder anhand des Vorhandenseins eines `ephemerisType` Feldes anstelle eines Feldes in der Antwort identifiziert werden. `groundStation` `satelliteId`

Mit Datenflüssen arbeiten

AWS Ground Station verwendet eine Knoten - und Kantenbeziehung, um Datenflüsse zu erstellen, die die Stream-Verarbeitung Ihrer Daten ermöglichen. Jeder Knoten wird durch eine Konfiguration repräsentiert, die die erwartete Verarbeitung beschreibt. Stellen Sie sich zur Veranschaulichung dieses Konzepts einen Datenfluss von `antenna-downlink` bis a vor. `s3-recording` Der `antenna-downlink` Knoten stellt die Analog-Digital-Transformation des Funkfrequenzspektrums gemäß den in der Konfiguration definierten Parametern dar. Der `s3-recording` steht für einen Rechenknoten, der eingehende Daten empfängt und sie in Ihrem S3-Bucket speichert. Der resultierende Datenfluss ist eine asynchrone Datenlieferung von digitalisierten HF-Daten an einen S3-Bucket auf der Grundlage Ihrer Spezifikationen.

In Ihrem Missionsprofil können Sie viele Datenflüsse erstellen, die Ihren Anforderungen entsprechen. In den folgenden Abschnitten wird beschrieben, wie Sie Ihre anderen AWS-Ressourcen für die Verwendung mit diesen einrichten, AWS Ground Station und es werden Empfehlungen für die Erstellung von Datenflüssen gegeben. Detaillierte Informationen zum Verhalten der einzelnen Knoten, einschließlich der Frage, ob sie als Quell- oder Zielknoten betrachtet werden, finden Sie unter. AWS Ground Station Konfigurationen verwenden

Themen

- AWS Ground Station Schnittstellen auf Datenebene
- Verwenden Sie die regionsübergreifende Datenbereitstellung
- Amazon S3 einrichten und konfigurieren
- Amazon VPC einrichten und konfigurieren
- Amazon einrichten und konfigurieren EC2

AWS Ground Station Schnittstellen auf Datenebene

Die resultierende Datenstruktur des ausgewählten Datenflusses hängt von der Quelle des Datenflusses ab. Einzelheiten zu diesen Formaten erhalten Sie beim Onboarding Ihrer Satelliten. Im Folgenden werden die Formate zusammengefasst, die für die einzelnen Datenflusstypen verwendet werden.

- Antennen-Downlink

  - (Bandbreite less-than-or-equal bis 40MHz) Daten werden als VITA-49-Signaldaten-/IP-Format-Pakete geliefert.
  - (Bandbreite größer als 40MHz) Daten werden als Pakete der Klasse 2 geliefert. AWS Ground Station
- antenna-downlink-demod-decode
  - Daten werden als Pakete im Demodulated/Decoded Daten-/IP-Format geliefert.
- Antennen-Uplink
  - Daten müssen als Pakete im VITA-49-Signaldaten-/IP-Format geliefert werden.
- antenna-uplink-echo
  - Daten werden als Pakete im VITA-49-Signaldaten-/IP-Format geliefert.

Verwenden Sie die regionsübergreifende Datenbereitstellung

Die Funktion zur AWS Ground Station regionsübergreifenden Datenübermittlung bietet Ihnen die Flexibilität, Ihre Daten von einer Antenne in jede AWS Ground Station unterstützte AWS Region zu senden. Das bedeutet, dass Sie Ihre Infrastruktur in einer einzigen AWS-Region verwalten und Kontakte für jede Region planen können, in der AWS Ground Station Standorte Sie angemeldet sind.

Wenn Sie Ihre Kontaktdaten in einem Amazon S3 S3-Bucket AWS Ground Station erhalten, verwaltet er alle Lieferaspekte für Sie.

Um die regionsübergreifende Datenübermittlung an eine EC2 Amazon-Instance zu verwenden (entweder mit dem AWS Ground Station Agenten oder einem Datenfluss-Endpunkt), muss der Datenfluss-Endpunkt in Ihrer aktuellen AWS-Region erstellt werden und Sie müssen dieselbe Region angeben. dataflow-endpoint-config AWS Ground Station kümmert sich für Sie um die regionsübergreifende Bereitstellung der Daten.

Amazon S3 einrichten und konfigurieren

Sie können einen Amazon S3 S3-Bucket verwenden, um Ihre Downlink-Signale mit AWS Ground Station zu empfangen. Um das Ziel s3-recording-config zu erstellen, müssen Sie in der Lage sein, einen Amazon S3 S3-Bucket und eine IAM-Rolle anzugeben, die das Schreiben von Dateien in den Bucket autorisiert AWS Ground Station .

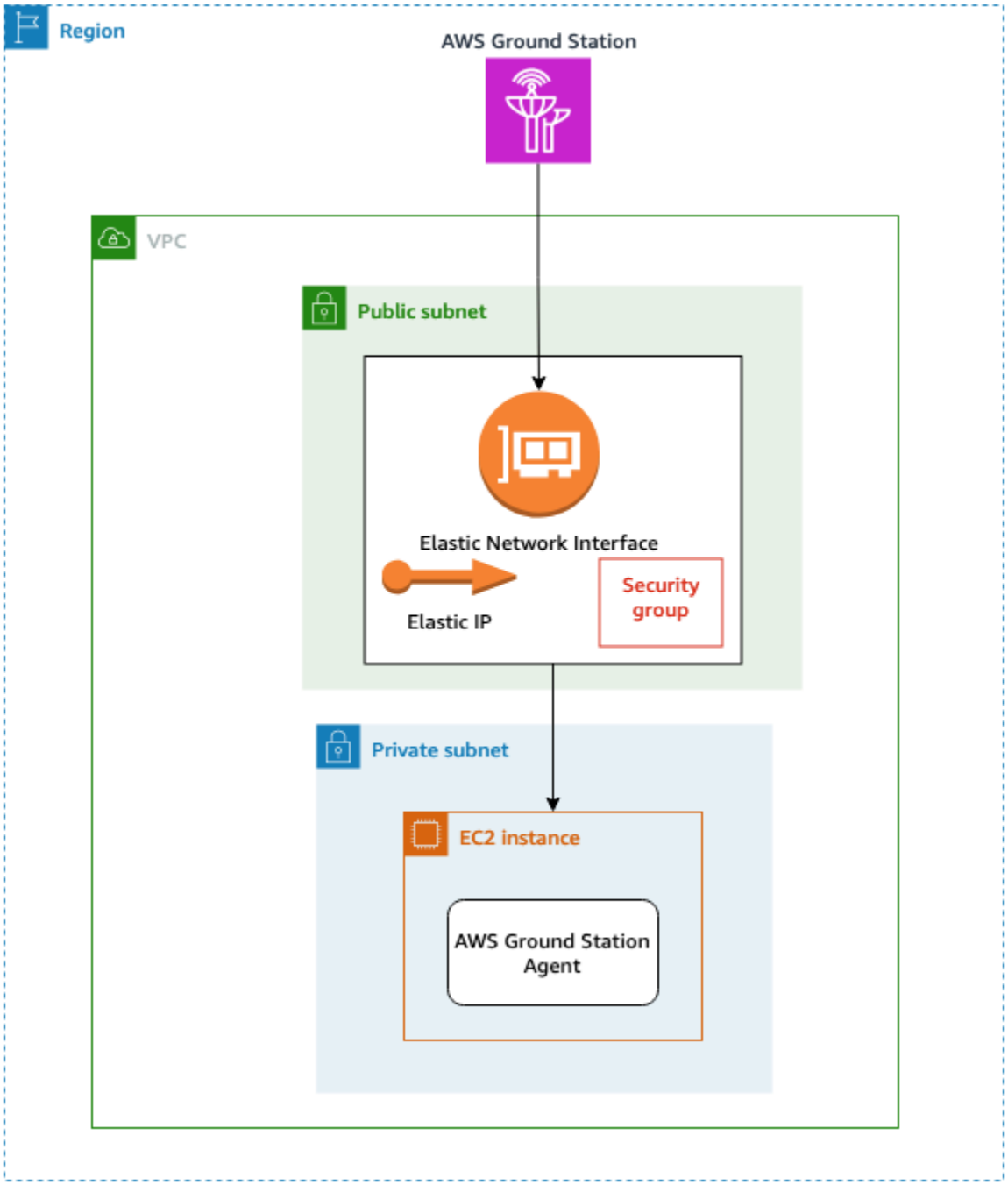
Einschränkungen Amazon S3 S3-Aufnahmekonfiguration für den Amazon S3 S3-Bucket, die IAM-Rolle oder die AWS Ground Station Konfigurationserstellung finden Sie unter.

Amazon VPC einrichten und konfigurieren

Eine vollständige Anleitung zur Einrichtung einer VPC würde den Rahmen dieses Handbuchs sprengen. Ein detailliertes Verständnis finden Sie im Amazon VPC-Benutzerhandbuch.

In diesem Abschnitt wird beschrieben, wie Ihr Amazon EC2 - und Dataflow-Endpunkt in einer VPC existieren können. AWS Ground Station unterstützt nicht mehrere Lieferpunkte für einen bestimmten Datenfluss — es wird erwartet, dass jeder Datenfluss zu einem einzelnen Empfänger endet. EC2 Da wir einen einzelnen EC2 Empfänger erwarten, ist die Konfiguration nicht Multi-AZ-redundant. Vollständige Beispiele, für die Ihre VPC verwendet wird, finden Sie unterBeispielkonfigurationen von Missionsprofilen.

VPC-Konfiguration mit Agent AWS Ground Station



Ihre Satellitendaten werden einer AWS Ground Station Agent-Instanz zur Verfügung gestellt, die sich in der Nähe der Antenne befindet. Der AWS Ground Station Agent verschlüsselt Ihre Daten per Stripe und verschlüsselt sie anschließend mit dem von Ihnen AWS KMS bereitgestellten Schlüssel. Jeder Stripe wird von der Quellantenne über den AWS-Netzwerk-Backbone an Ihre Amazon EC2 Elastic IP (EIP) gesendet. Die Daten kommen über das angehängte Amazon EC2 Elastic Network Interface

(ENI) an Ihre EC2 Instance an. Sobald Sie sich auf Ihrer EC2 Instance befinden, entschlüsselt der installierte AWS Ground Station Agent Ihre Daten und führt eine Forward-Fehlerkorrektur (FEC) durch, um verloren gegangene Daten wiederherzustellen. Anschließend leitet er sie an die IP und den Port weiter, die Sie in Ihrem Setup angegeben haben.

In der folgenden Liste werden spezielle Überlegungen zur Einrichtung aufgeführt, die bei der Einrichtung Ihrer VPC für die AWS Ground Station Agentenzustellung zu berücksichtigen sind.

Sicherheitsgruppe — Es wird empfohlen, eine Sicherheitsgruppe einzurichten, die ausschließlich dem AWS Ground Station Datenverkehr gewidmet ist. Diese Sicherheitsgruppe sollte eingehenden UDP-Verkehr über denselben Portbereich zulassen, den Sie in Ihrer Dataflow-Endpunktgruppe angeben. AWS Ground Station verwaltet eine von AWS verwaltete Präfixliste, um Ihre Berechtigungen nur auf AWS Ground Station IP-Adressen zu beschränken. Einzelheiten dazu, wie Sie die PrefixListIdfür Ihre Bereitstellungsregionen ersetzen können, finden Sie in den AWS Managed Prefix Lists.

Elastic Network Interface (ENI) — Sie müssen die oben genannte Sicherheitsgruppe mit dieser ENI verknüpfen und sie in Ihrem öffentlichen Subnetz platzieren.

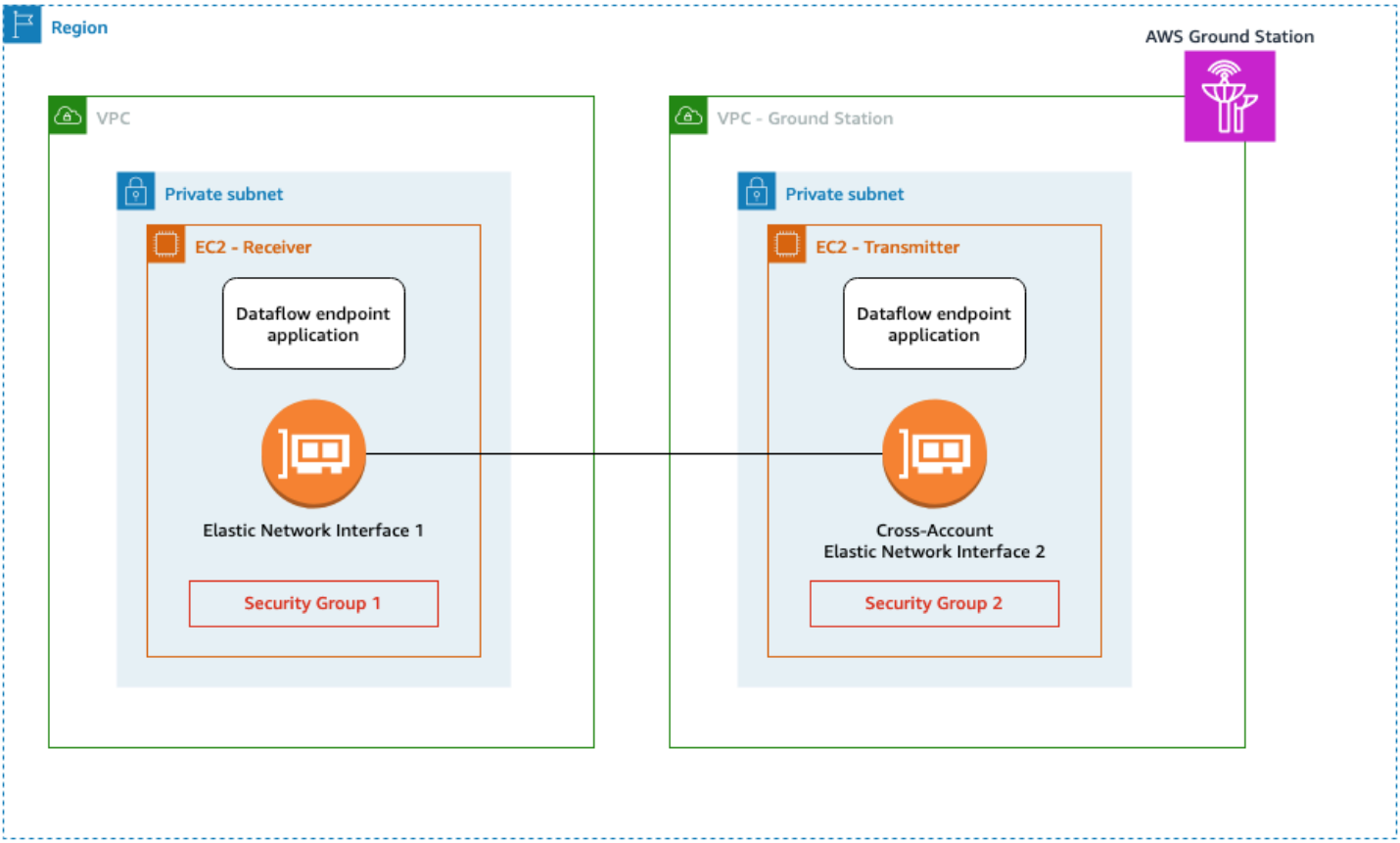
> **Note**
>
> Das Standardkontingent für die Anzahl der pro ENI angehängten Sicherheitsgruppen ist 5. Dies ist ein einstellbares Limit von bis zu 16, siehe Amazon VPC-Kontingente.

Die folgende CloudFormation Vorlage zeigt, wie die in diesem Abschnitt beschriebene Infrastruktur erstellt wird.

```
ReceiveInstanceEIP:
  Type: AWS::EC2::EIP
  Properties:
    Domain: 'vpc'

InstanceSecurityGroup:
  Type: AWS::EC2::SecurityGroup
  Properties:
    GroupDescription: AWS Ground Station receiver instance security group.
    VpcId:YourVpcId
    SecurityGroupIngress:
      # Add additional items here.
      - IpProtocol: udp
        FromPort: your-port-start-range
```

```
        ToPort: your-port-end-range
        PrefixListIds:
          - PrefixListId: com.amazonaws.global.groundstation
        Description: "Allow AWS Ground Station Downlink ingress."

InstanceNetworkInterface:
  Type: AWS::EC2::NetworkInterface
  Properties:
    Description: ENI for AWS Ground Station to connect to.
    GroupSet:
      - !Ref InstanceSecurityGroup
    SubnetId: A Public Subnet

ReceiveInstanceEIPAllocation:
  Type: AWS::EC2::EIPAssociation
  Properties:
    AllocationId:
      Fn::GetAtt: [ ReceiveInstanceEIP, AllocationId ]
    NetworkInterfaceId:
      Ref: InstanceNetworkInterface
```

VPC-Konfiguration mit einem Datenfluss-Endpunkt



Ihre Satellitendaten werden einer Dataflow-Endpunkt-Anwendungsinstanz bereitgestellt, die sich in der Nähe der Antenne befindet. Die Daten werden dann über das kontoübergreifende Amazon EC2 Elastic Network Interface (ENI) von einer VPC gesendet, deren Eigentümer ist. AWS Ground Station Die Daten kommen dann über die ENI, die an Ihre EC2 Amazon-Instance angehängt ist, bei Ihrer EC2 Instance an. Die installierte Dataflow-Endpunktanwendung leitet sie dann an die IP und den Port weiter, die Sie in Ihrem Setup angegeben haben. Die Umkehrung dieses Flusses erfolgt bei Uplink-Verbindungen.

In der folgenden Liste werden spezielle Überlegungen zur Einrichtung aufgeführt, die bei der Einrichtung Ihrer VPC für die Datenflussendpunktbereitstellung zu berücksichtigen sind.

> **Note**
>
> Das Standardkontingent für die Anzahl der pro ENI angehängten Sicherheitsgruppen ist 5. Dies ist ein einstellbares Limit von bis zu 16, siehe Amazon VPC-Kontingente.

IAM-Rolle — Die IAM-Rolle ist Teil des Dataflow-Endpunkts und wird im Diagramm nicht dargestellt. Die IAM-Rolle, die zum Erstellen und Anhängen der kontoübergreifenden ENI an die AWS Ground Station EC2 Amazon-Instance verwendet wird.

Sicherheitsgruppe 1 — Diese Sicherheitsgruppe ist mit der ENI verknüpft, die der EC2 Amazon-Instance in Ihrem Konto zugeordnet wird. Sie muss UDP-Verkehr von Sicherheitsgruppe 2 an den in Ihrem angegebenen Port zulassen dataflow-endpoint-group.

Elastic Network Interface (ENI) 1 — Sie müssen dieser ENI Sicherheitsgruppe 1 zuordnen und sie in einem Subnetz platzieren.

Subnetz — Sie müssen sicherstellen, dass in Ihrem Konto mindestens eine verfügbare IP-Adresse pro Datenfluss für die EC2 Amazon-Instance verfügbar ist. Weitere Informationen zur Subnetzdimensionierung finden Sie unter Subnetz-CIDR-Blöcke

Sicherheitsgruppe 2 — Auf diese Sicherheitsgruppe wird im Dataflow-Endpunkt verwiesen. Diese Sicherheitsgruppe wird mit der ENI verknüpft, über die Daten in Ihrem Konto gespeichert AWS Ground Station werden.

Region — Weitere Informationen zu den unterstützten Regionen für regionsübergreifende Verbindungen finden Sie unterVerwenden Sie die regionsübergreifende Datenbereitstellung.

Die folgende CloudFormation Vorlage zeigt, wie die in diesem Abschnitt beschriebene Infrastruktur erstellt wird.

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

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

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

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

Amazon einrichten und konfigurieren EC2

Die korrekte Konfiguration Ihrer EC2 Amazon-Instance ist erforderlich, damit die synchrone Lieferung von VITA-49 Signal/IP data or VITA-49 Extension data/IP über den AWS Ground Station Agenten oder einen Datenflussendpunkt erfolgen kann. Je nach Ihren spezifischen Anforderungen können Sie den Front-End-Prozessor (FE) oder den Software Defined Radio (SDR) direkt auf derselben Instance ausführen, oder Sie müssen möglicherweise zusätzliche Instances verwenden. EC2 Die Auswahl und Installation Ihres FE oder SDR würde den Rahmen dieses Benutzerhandbuchs sprengen. Weitere Informationen zu den spezifischen Datenformaten finden Sie unterAWS Ground Station Schnittstellen auf Datenebene.

Informationen zu unseren Servicebedingungen finden Sie unter AWS Servicebedingungen.

Im Lieferumfang enthaltene Standardsoftware

AWS Ground Station bietet gängige Software, um die Einrichtung Ihrer EC2 Amazon-Instance zu vereinfachen.

AWS Ground Station Agent

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 Datenübermittlung mit Forward Error Correction (FEC).
- Sichere Datenübermittlung mit einem vom Kunden verwalteten AWS KMS Schlüssel zur Verschlüsselung.

Weitere Informationen finden Sie im AWS Ground Station Agent-Benutzerhandbuch.

Dataflow-Endpunktanwendung

Eine Netzwerkanwendung, die von AWS Ground Station zum Senden und Empfangen von Daten zwischen den AWS Ground Station Antennenstandorten und Ihren EC2 Amazon-Instances verwendet wird. Sie kann für den Uplink und Downlink von Daten verwendet werden.

Softwaredefiniertes Radio (SDR)

Ein softwaredefiniertes Radio (SDR), mit dem das für die Kommunikation mit Ihrem Satelliten verwendete Signal moduliert/demoduliert werden kann.

AWS Ground Station Amazon-Maschinenbilder (AMIs)

Um die Bau- und Konfigurationszeiten dieser Installationen zu verkürzen, bietet es AWS Ground Station auch vorkonfigurierte AMIs Angebote. Die AMIs mit einem Datenfluss ausgestattete Netzwerkanwendung für Endgeräte und ein softwaredefiniertes Radio (SDR) werden Ihrem Konto nach Abschluss des Onboardings zur Verfügung gestellt. Sie können in der EC2 Amazon-Konsole

gefunden werden, indem Sie in privaten Amazon Machine Images (AMIs) nach Groundstation suchen. Die AMIs mit AWS Ground Station Agent sind öffentlich und können in der EC2 Amazon-Konsole gefunden werden, indem Sie in den öffentlichen Amazon Machine Images (AMIs) nach Groundstation suchen.

Arbeiten Sie mit Telemetrie

AWS Ground Station Telemetrie liefert während Ihrer Satellitenkontakte nahezu in Echtzeit Messdaten von AWS Ground Station Antennen. Sie können Telemetriedaten verwenden, um die Kontaktleistung zu überwachen, Anomalien zu erkennen und fundierte Entscheidungen über Ihre Satellitenkommunikation zu treffen.

Wie funktioniert Telemetrie

Um Telemetrie zu verwenden, konfigurieren Sie eine, TelemetrySinkConfigdie festlegt, wohin Telemetriedaten geliefert AWS Ground Station werden sollen. Anschließend fügen Sie diese Konfiguration mithilfe des Felds zu Ihrem Missionsprofil hinzu. `telemetrySinkConfigArn` Bei Kontakten, die ein telemetrisches Missionsprofil verwenden, werden Telemetriedaten an AWS Ground Station Ihr Konto gestreamt.

Der Telemetriebereitstellungsprozess funktioniert wie folgt:

1. Sie erstellen in Ihrem AWS Konto einen Kinesis Data Streams Streams-Stream, um Telemetriedaten zu empfangen. Der Stream muss in demselben Konto und in derselben Region erstellt werden, von der aus Sie Ihre Kontakte planen.
2. Sie erstellen eine IAM-Rolle, die Ihnen die AWS Ground Station Erlaubnis erteilt, Daten in Ihren Stream zu schreiben.
3. Sie erstellen eine TelemetrySinkConfig , die auf Ihren Stream und Ihre IAM-Rolle verweist.
4. Sie fügen das TelemetrySinkConfig zu Ihrem Missionsprofil hinzu.
5. Sie listen Kontakte auf und reservieren sie mithilfe des neuen Telemetrie-fähigen Missionsprofils.
6. Bei Kontakten, die dieses Missionsprofil verwenden, AWS Ground Station werden Telemetriedaten nahezu in Echtzeit an Ihren Kinesis Data Streams-Stream gestreamt.
7. Sie nutzen und verarbeiten die Telemetriedaten aus Ihrem Stream mithilfe von AWS Diensten oder Ihren eigenen Anwendungen.

Verfügbare Telemetriearten

AWS Ground Station bietet die folgenden Telemetriearten bei Kontakten:

> **Note**
>
> AWS Ground Station arbeitet daran, die Anzahl der unterstützten Telemetriearten zu erweitern

Zeigetelemetrie

Liefert Informationen zur Ausrichtung der Antenne bei Satellitenkontakten. Dieser Telemetrie-Typ wird immer während eines Kontakts gesendet und umfasst tatsächliche und angeforderte Azimut- und Elevationswinkel. Weitere Informationen finden Sie unter Zeigetelemetrie.

Telemetrie zur Nachverfolgung

Bietet Informationen zum Status der Antennenverfolgung und zu Tracking-Fehlern. Dieser Telemetrie-Typ wird gesendet, wenn Autotracking in Ihrer Tracking-Konfiguration aktiviert ist. Weitere Informationen finden Sie unter Telemetrie verfolgen.

Regionale Verfügbarkeit

Telemetrie ist in allen AWS Regionen verfügbar, in denen AWS Ground Station wir tätig sind. Während der Ausführung des Kontakts wird die Telemetrie von der AWS Ground Station Antenne an die Region gesendet, von der aus Sie Ihren Kontakt vereinbart haben, sodass ein regionsübergreifender Support gewährleistet ist.

Eine vollständige Liste der AWS Ground Station Regionen und Standorte der Bodenstationen finden Sie unter. AWS Ground Station Standorte

Themen

- Telemetrie einrichten
- Verstehen Sie Telemetriedaten

Telemetrie einrichten

Gehen Sie wie folgt vor, um die Telemetrie für Ihre AWS Ground Station Kontakte zu konfigurieren. Nach Abschluss dieser Einrichtung werden Telemetriedaten bei Kontakten, die ein telemetriefähiges Missionsprofil verwenden, an Ihren Kinesis Data Streams Streams-Stream übermittelt. Ein

detailliertes Verständnis von Kinesis Data Streams finden Sie im Kinesis Data Streams Streams-Benutzerhandbuch.

Schritt 1: Erstellen Sie die erforderlichen Ressourcen AWS

Der folgende CloudFormation Ausschnitt zeigt, wie Sie die erforderlichen AWS Ressourcen für die Telemetriebereitstellung erstellen. Dieses Snippet erstellt einen Kinesis Data Streams Streams-Stream und eine IAM-Rolle, die die AWS Ground Station Erlaubnis erteilt, Telemetriedaten in den Stream zu schreiben.

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

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

In der folgenden Liste werden spezielle Überlegungen zur Einrichtung bei der Konfiguration der Telemetriebereitstellung für aufgeführt. AWS Ground Station

Kinesis Data Streams Streams-Stream — Der Stream verwendet den On-Demand-Kapazitätsmodus, der automatisch auf der Grundlage des Durchsatzes skaliert wird. Dies wird für die meisten Anwendungsfälle empfohlen. Der Stream ist so konfiguriert, dass er Daten 24 Stunden lang aufbewahrt. Standardmäßig verwendet der Stream AWS verwaltete Verschlüsselung. Um die vom Kunden verwaltete Verschlüsselung mit zu verwenden AWS Key Management Service, fügen Sie die `StreamEncryption` Eigenschaft hinzu und aktualisieren Sie die IAM-Rollenrichtlinie, sodass sie auch Berechtigungen enthältkms:GenerateDataKey. Weitere Informationen finden Sie unter Datenschutz in Amazon Kinesis Data Streams.

IAM-Rolle — Die IAM-Rolle ermöglicht es dem `groundstation.amazonaws.com` Service Principal, die Rolle zu übernehmen und Telemetriedaten in Ihren Kinesis Data Streams Streams-Stream zu schreiben. Die Rollenrichtlinie gewährt Berechtigungen für `kinesis:DescribeStreamkinesis:PutRecord`, und `kinesis:PutRecords` Aktionen im Stream. Anleitungen Telemetrie Sink Config zur Einrichtung der Vertrauens- und Rollenrichtlinie finden Sie unter.

Zusätzliche Konfiguration — Fügen Sie dem IAM-Benutzer oder der IAM-Rolle, die Sie für AWS Ground Station API-Aufrufe verwenden, `iam:PassRole` Berechtigungen hinzu. Auf diese Weise können Sie die Telemetriefunktion AWS Ground Station beim Erstellen eines übergeben. TelemetrySinkConfig

Beispiel für PassRole eine Richtlinie

Weitere Informationen zum Aktualisieren oder Anhängen einer Rollenrichtlinie finden Sie unter Verwaltung von IAM-Richtlinien im IAM-Benutzerhandbuch. Weitere Informationen zur `iam:PassRole` Berechtigung finden Sie unter Erteilen von Benutzerberechtigungen zur Übergabe einer Rolle an einen AWS-Service

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

```
    }
  ]
}
```

Schritt 2: Erstellen Sie ein TelemetrySinkConfig

Erstellen Sie eine TelemetrySinkConfig, die definiert, wie AWS Ground Station Telemetriedaten an Ihren Kinesis Data Streams Streams-Stream geliefert werden. Verwenden Sie den Stream-ARN und den Rollen-ARN aus den CloudFormation Stack-Ausgaben in Schritt 1.

> **Note**
>
> Wenn Sie einen erstellen TelemetrySinkConfig, AWS Ground Station wird der Zugriff auf Ihren Kinesis Data Streams Streams-Stream überprüft, indem ein leerer Testdatensatz mit dem Partitionsschlüssel von `test` bereitgestellt wird.

Weitere Informationen zum Erstellen eines finden Sie TelemetrySinkConfigunterTelemetrie Sink Config.

Schritt 3: Fügen Sie Ihrem Missionsprofil Telemetrie hinzu

Erstellen Sie ein Missionsprofil. Weitere Informationen zum Erstellen von Missionsprofilen finden Sie unterAWS Ground Station Missionsprofile verwenden. Fügen Sie das `telemetrySinkConfigArn` zu Ihrem Missionsprofil hinzu, um die Telemetrieübertragung bei Kontakten zu aktivieren. Verwenden Sie den in Schritt 2 TelemetrySinkConfigerstellten ARN.

Schritt 4: Einen Kontakt vereinbaren

Planen Sie einen Kontakt mithilfe Ihres telemetriefähigen Missionsprofils. Während des Kontakts AWS Ground Station werden Telemetriedaten in Ihren Kinesis Data Streams-Stream gestreamt.

Was ist bei Kontakten zu erwarten

- Telemetriestart — Die Daten werden gestreamt, sobald der Kontakt beginnt.
- Lieferung nahezu in Echtzeit — Telemetrie geht nahezu in Echtzeit in Ihren Kinesis Data Streams Streams-Stream ein.
- Kontaktdauer — Die Daten bleiben während des gesamten Kontakts erhalten.
- Automatischer Stopp — Die Telemetrie stoppt das Streaming, wenn der Kontakt endet.

Überwachung der Lieferung

Sie können die Telemetrieübertragung wie folgt überwachen:

- Kinesis Data Streams Streams-Streams-Streams-Metriken — Checken Sie eingehende Datensätze ein. CloudWatch Weitere Informationen finden Sie unter Amazon Kinesis Data Streams überwachen.
- Anwendungsprotokolle — Überprüfen Sie die Datenverarbeitung in Ihren Anwendungen, die Daten aus dem Stream verarbeiten.
- Kinesis Data Viewer — Verwenden Sie die Kinesis Data Streams Streams-Stream-Konsole, um Beispieldatensätze aus Ihrem Stream anzuzeigen.

Nächste Schritte

Nach Abschluss der Einrichtung können Sie:

- Erfahren Sie mehr über das Telemetriedatenformat und die verfügbaren Telemetriearten. Siehe Verstehen Sie Telemetriedaten.
- Erstellen Sie Anwendungen zur Verarbeitung von Telemetriedaten aus Ihrem Kinesis Data Streams Streams-Stream. Weitere Informationen finden Sie unter Building Consumers for Amazon Kinesis Data Streams.
- Erstellen Sie Dashboards und Benachrichtigungen mithilfe von CloudWatch und anderen AWS Diensten.
- Lesen Sie die Anleitungen zur Fehlerbehebung, falls Sie auf Probleme stoßen. Siehe Fehlerbehebung bei Telemetrie.

Verstehen Sie Telemetriedaten

Telemetriedaten werden als Base64-kodierte JSON-Datensätze an Ihren Kinesis Data Streams Streams-Stream übermittelt. Jeder Datensatz enthält Informationen, die während Ihres Satellitenkontakts gesammelt wurden, einschließlich Metadaten über den Kontakt und die gesammelten Telemetriemessungen.

Überblick über das Datenformat

Jeder Telemetriedatensatz enthält die folgenden Komponenten:

Typ und Version der Telemetrie

Identifiziert den spezifischen Typ von Telemetriedaten und dessen Schemaversion. Auf diese Weise können Sie verschiedene Telemetriearten entsprechend analysieren. Weitere Informationen zur Schemaversionierung finden Sie unter. Versionierung und Weiterentwicklung von Schemas

Bereichs-ID

Eine eindeutige Kennung für den Umfang der Telemetrie. Auf diese Weise können Sie Telemetriedaten mit bestimmten Kontakten korrelieren.

Metadaten

Kontextinformationen zur Telemetrie.

Daten

Die ausgewählten Telemetriemessungen, die für den jeweiligen Telemetrietyp spezifisch sind.

Partitionsschlüssel

Telemetriedatensätze werden mit einem Partitionsschlüssel im folgenden Format an Ihren Kinesis Data Streams Streams-Stream übermittelt:

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

Dieser Partitionsschlüssel stellt sicher, dass die gesamte Telemetrie eines bestimmten Typs für einen einzelnen Kontakt an denselben Shard in Ihrem Kinesis Data Streams Streams-Stream übertragen wird, sodass Sie den Telemetriestream dieses Kontakts bestmöglich bestellen können.

Zeigetelemetrie

Die Zeigetelemetrie liefert Informationen über die Ausrichtung der Antenne bei Satellitenkontakten. Dieser Telemetrie-Typ wird immer während eines Kontakts gesendet.

Datenfelder

Beispiel für einen Zeitstempel

Zeitpunkt, zu dem die Telemetriedaten abgetastet wurden, im ISO-8601-Format in UTC mit Millisekundengenauigkeit.

Azimut

Tatsächlicher Azimutwinkel der Antenne in Grad.

Höhenlage

Tatsächlicher Höhenwinkel der Antenne in Grad.

Hat Azimuth befohlen

Befehlsmäßiger Azimutwinkel in Grad. Dies ist der Zielazimutwinkel, den die Antenne zu erreichen versucht.

Befehlte Höhe

Befohlener Höhenwinkel in Grad. Dies ist der Zielhöhenwinkel, den die Antenne zu erreichen versucht.

> **Note**
>
> Die tatsächliche Antennenposition kann aufgrund von physikalischen Einschränkungen oder mechanischen Verzögerungen während des Kontakts von der angegebenen Position abweichen.

Metadaten-Felder

Bodenstation

Name der Bodenstation (z. B. „Ohio 1").

Satelliten-ID

Kennung der Satellitenressource in. AWS Ground Station

contactId

Kennung des Kontakts.

Beispiel JSON

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

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

Telemetrie verfolgen

Die Tracking-Telemetrie liefert Informationen zum Status der Antennenverfolgung und zu Tracking-Fehlern. Dieser Telemetrie-Typ wird gesendet, wenn Autotracking in Ihrer Tracking-Konfiguration aktiviert ist und wenn die Antenne Autotrack aktiv verwendet.

> **Note**
>
> Wenn der `autotrack` Parameter in Ihrem auf eingestellt TrackingConfig ist`REMOVED`, wird keine Tracking-Telemetrie übermittelt. Weitere Informationen zu Tracking-Konfigurationen finden Sie unter. Nachverfolgungs-Config

Datenfelder

Beispiel für einen Zeitstempel

Zeitpunkt, zu dem die Telemetriedaten abgetastet wurden, im ISO-8601-Format in UTC mit Millisekundengenauigkeit.

Status der Nachverfolgung

Aktueller Tracking-Status der Antenne. Zu den möglichen Werten gehören `TRACKING`, `ACQUIRING` und `MASKED`.

trackingErrorAzimuth

Tracking-Fehler in der Azimutachse, gemessen in Grad.

trackingErrorElevation

Spurfehler auf der Höhenachse, gemessen in Grad.

> **Note**
>
> Bei den Tracking-Fehlerwerten handelt es sich um Anpassungen aus dem auf Ephemeriden basierenden Programmtrack, der beim Autotracking AWS Ground Station angewendet wird, um die Signalstärke zu maximieren.

Metadaten-Felder

Die Tracking-Telemetrie umfasst dieselben Metadatenfelder wie die Zeigetelemetrie: `groundStationsatelliteId`, und. `contactId`

JSON-Beispiel

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

Daten aus dem Kinesis Data Streams Streams-Stream lesen

Telemetriedaten werden an Ihren Kinesis Data Streams Streams-Stream übermittelt und können mithilfe von Standard-Stream-Verbrauchsmustern genutzt werden. Beachten Sie beim Lesen von Daten aus Ihrem Stream die folgenden Überlegungen.

Base64-Decodierung

Daten im Kinesis Data Streams Streams-Stream sind Base64-codiert. Sie müssen die Daten dekodieren, bevor Sie sie als JSON analysieren können. Weitere Informationen finden Sie unter Arbeiten mit Amazon Kinesis Data Streams.

Verwenden des Kinesis Data Viewers

Für den schnellen Zugriff auf Ihre Telemetriedaten bietet die Kinesis Data Streams Streams-Stream-Konsole eine Data Viewer-Funktion. Wenn Sie diese Funktion verwenden:

- Die Telemetrieübertragung kann an jeden Shard in Ihrem Stream erfolgen.
- Die Standard-Startposition liest aus den neuesten Datensätzen im Shard.
- Möglicherweise müssen Sie den ausgewählten Shard anpassen und die Startposition „Am Zeitstempel“ verwenden, um die empfangenen Datensätze anzuzeigen.

Verwenden der Kinesis Client Library

Die Kinesis Client Library (KCL) bewältigt viele der komplexen Aufgaben, die mit der Nutzung von Daten aus dem Kinesis Data Streams Streams-Stream verbunden sind, einschließlich Shard-Management, Checkpointing und Load Balancing. Wir empfehlen die Verwendung von KCL für Anwendungen zur Nutzung von Telemetrie in der Produktion.

Weitere Informationen finden Sie unter Developing Consumer Using the Kinesis Client Library.

Bewährte Methoden für den Konsum

- Latenz minimieren — Verwenden Sie Enhanced Fan-Out, um aus dem Kinesis Data Streams Streams-Stream mit dediziertem Durchsatz und geringerer Latenz im Vergleich zu Polling zu lesen. Weitere Informationen finden Sie unter Entwickeln erweiterter Fan-Out-Nutzer.
- Dedizierter Stream — Verwenden Sie einen dedizierten Kinesis Data Streams Streams-Stream für Ihre AWS Ground Station Telemetrieintegration. Die gemeinsame Nutzung eines Streams mit

anderen Anwendungen kann zu einer Überlastung des Schreibdurchsatzes und zu Fehlern bei der Telemetrieübertragung führen.

- Kapazität auf Abruf — Stellen Sie Ihren Kinesis Data Streams Streams-Stream im On-Demand-Bereitstellungsmodus bereit, um eine automatische Skalierung von Shards basierend auf dem Durchsatz zu ermöglichen.
- Durchsatz überwachen — Überwachen Sie Ihren Stream anhand von Metriken auf Drosselung. CloudWatch Weitere Informationen finden Sie unter Amazon Kinesis Data Streams überwachen.

Versionierung und Weiterentwicklung von Schemas

Telemetrieschemas werden versioniert, um die Entwicklung im Laufe der Zeit zu unterstützen. Das `telemetryVersion` Feld in jedem Datensatz gibt die Schemaversion an.

Umgang mit Schemaänderungen

- In future könnten neue Telemetriearten eingeführt werden.
- Bestehende Telemetriearten erhalten möglicherweise neue Versionen mit grundlegenden Änderungen.
- Ihre Anwendungen sollten gegenüber unbekannten Telemetriearten und -versionen tolerant sein.
- Analysieren Sie die `telemetryVersion` Felder`telemetryTypeAndVersion`, und`telemetryType`, um zu bestimmen, wie die einzelnen Datensätze verarbeitet werden sollen.

Wir empfehlen die Implementierung einer versionsabhängigen Payload-Serialisierung, die mehrere Schemaversionen problemlos verarbeiten kann, sodass Ihre Anwendungen auch bei der Einführung neuer Versionen weiter funktionieren können.

Arbeiten Sie mit Kontakten

Sie können mithilfe der AWS Ground Station Konsole oder des AWS SDK in der Sprache Ihrer Wahl Satellitendaten eingeben, Antennenstandorte identifizieren AWS CLI, kommunizieren und die Antennenzeit für ausgewählte Satelliten planen. Sie können Kontaktreservierungen bis zu 15 Minuten vor Kontaktbeginn überprüfen, stornieren und verschieben. 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 Hinweise zur Verwendung der regionsübergreifenden Datenübermittlung finden Sie unter. Verwenden Sie die regionsübergreifende Datenbereitstellung

Um Kontakte zu planen, müssen Ihre Ressourcen konfiguriert sein. Wenn Sie Ihre Ressourcen nicht konfiguriert haben, finden Sie weitere Informationen unterErste Schritte. Wenn aufgerufen ReserveContactwird, erstellt eine AWS Ground Station Momentaufnahme des Missionsprofils und konfiguriert Ressourcen für die Nutzung während des gesamten Lebenszyklus des Kontakts. Änderungen an diesen Ressourcen mithilfe von UpdateMissionProfileund wirken UpdateConfig APIs sich nicht auf Kontakte aus, die vor den Aktualisierungen reserviert wurden. Wenn Sie möchten, dass die Ressourcenänderungen auf einen bereits geplanten Kontakt angewendet werden, müssen Sie zuerst den Kontakt mit CancelContactstornieren und ihn dann mit ReserveContactneu planen.

* Stornierte Kontakte können Kosten verursachen, wenn sie zu kurz vor dem Kontaktzeitpunkt storniert werden. Weitere Informationen zu stornierten Kontakten finden Sie unter: Ground Station FAQs.

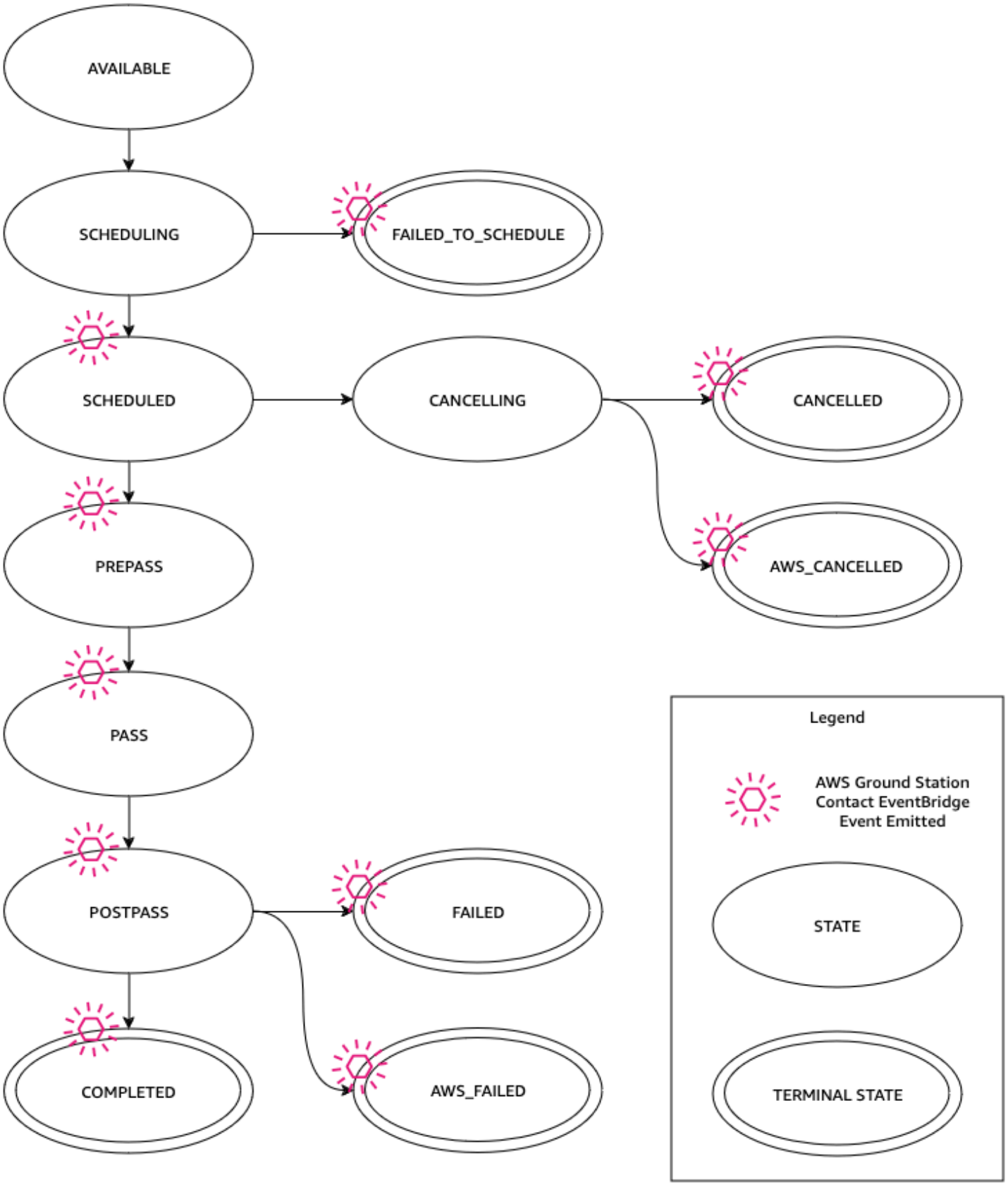
Themen

- Verstehen Sie den Lebenszyklus von Kontakten
- Verstehen Sie die Abrechnung mit Kontakten

Verstehen Sie den Lebenszyklus von Kontakten

Wenn Sie den Kontaktlebenszyklus verstehen, können Sie verschiedene Probleme bei der Nutzung automatisieren und beheben AWS Ground Station. Das folgende Diagramm zeigt den AWS Ground Station Kontaktlebenszyklus sowie die während des Lebenszyklus ausgelösten

Event Bridge-Ereignisse. Es ist wichtig zu beachten, dass es sich bei den Werten COMPLETED, FAILED, FAILED_TO_SCHEDULE AWS_CANCELLED, CANCELLED und um Endstatus handelt. AWS_FAILED Kontakte verlassen den Terminalstatus nicht. AWS Ground Station Status der KontakteWeitere Informationen darüber, was die einzelnen Status bedeuten und ob sie beendet oder storniert werden können, finden Sie unter. CancelContact


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

AWS Ground Station Status der Kontakte

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

Status der Kontakte

In der folgenden Tabelle werden die Status beschrieben, die ein Kontakt haben kann:

Status	Description	Terminal	Stornierbar	Aufhaltbar
VERFÜGBAR	Der Kontakt kann reserviert werden.	Nein	–	–
TERMINPLANUNG	Der Kontakt ist gerade dabei, einen Termin zu vereinbaren.	Nein	Ja	Nein
GEPLANT	Der Kontakt wurde erfolgreich geplant.	Nein	Ja	Nein
FAILED_TO_SCHEDULE	Der Kontakt konnte nicht geplant werden.	Ja	Nein	Nein
PREPASS	Der Kontakt beginnt bald und die Ressourcen werden vorbereitet.	Nein	Ja	Nein
PASS	Der Kontakt wird gerade ausgeführt und es wird mit dem Satelliten kommuniziert.	Nein	Nein	Ja
POSTPASS	Die Kommunikation ist abgeschlossen und die verwendeten Ressourcen werden bereinigt.	Nein	Nein	Nein
COMPLETED	Der Kontakt wurde ohne Fehler abgeschlossen.	Ja	Nein	Nein
FEHLGESCHLAGEN	Der Kontakt ist aufgrund eines Problems mit Ihrer Ressourcenkonfiguration fehlgeschlagen.	Ja	Nein	Nein

Status	Description	Terminal	Stornierbar	Aufhaltbar
AWS_FAILED	Der Kontakt ist aufgrund eines Problems mit dem AWS Ground Station Dienst fehlgeschlagen.	Ja	Nein	Nein
CANCELLING	Der Kontakt wird gerade storniert.	Nein	Nein	Nein
AWS_CANCELLED	Der Kontakt wurde vom AWS Ground Station Dienst storniert . Wartung von Antennen oder Standorten und Ephemeridendrift sind Beispiele dafür, wann dies passieren könnte.	Ja	Nein	Nein
CANCELLED	Der Kontakt wurde von Ihnen storniert.	Ja	Nein	Nein

> **Note**
>
> Informationen zu den Auswirkungen stornierter oder gekündigter Kontakte auf die Abrechnung finden Sie unterVerstehen Sie die Abrechnung mit Kontakten.

Aufbewahrung von Kontaktdaten

AWS Ground Station speichert Kontaktdaten für ein Jahr, nachdem eine ReserveContactAnfrage zur Reservierung eines Kontakts gestellt wurde. Nach Ablauf des Zeitraums von 1 Jahr werden die Kontaktdaten gelöscht.

Wenn Sie Kontaktdaten länger als ein Jahr aufbewahren müssen, wird empfohlen, Ihre Daten vor Ablauf der Aufbewahrungsfrist zu exportieren. Weitere Informationen zum Zugriff auf und Exportieren von Kontaktdaten finden Sie unter:

- AWS Ground Station API Reference
- AWS Ground Station CLI-Befehlsreferenz

Verstehen Sie die Abrechnung mit Kontakten

Mit AWS Ground Station zahlen Sie nur für die Antennenzeit, die Sie nutzen. AWS Ground Station Messgeräte kontaktieren die Nutzung auf Minutenbasis. Für jeden Kontakt berechnet der Service die Kontaktdauer von der Start- bis zur Endzeit und rundet sie auf die nächste Minute auf. Diese gemessene Dauer bestimmt Ihre Gebühren für diesen Kontakt.

Ihr Tarif hängt von zwei Hauptfaktoren ab:

- Bandbreite — Die für den Kontakt reservierte Bandbreite (Schmalband oder Breitband)
- Standort der Bodenstation — Die Preise variieren je nach Standort der Bodenstation

Bandbreitendefinitionen

AWS Ground Station unterteilt Kontakte auf der Grundlage der aktuellen Bandbreite in zwei Bandbreitenkategorien:

- Schmalband — Jeder Kontakt, bei dem die aktuelle Bandbreite kleiner oder gleich 40 ist MHz
- Breitband — Jeder Kontakt, bei dem die Momentanbandbreite größer als 40 ist MHz

Modi für die Terminplanung

AWS Ground Station bietet zwei Planungsmodi:

- Auf Abruf — Zahlen Sie für den Antennenanschluss ohne langfristige Verpflichtungen
- Reserviert — Bietet einen vergünstigten Tarif und eine verbesserte Terminplanung im Vergleich zu On-Demand-Diensten mit monatlichem Abonnement. Für Kunden, die sich zu einer monatlichen Nutzung für einen bestimmten Zeitraum verpflichten, ist der Preis für reservierte Minuten verfügbar.

Für spezifische Preisinformationen für Ihr Konto oder um mehr über den Reserved Scheduling Mode zu erfahren, wenden Sie sich an Ihren AWS-Ansprechpartner.

CancelContact

Die Verwendung der CancelContactAPI hängt vom Status des Kontakts ab, in dem Sie sie aufrufen:

- Vor Beginn des Kontakts — Bricht den Kontakt vollständig ab

- Nach dem Beginn des Kontakts und vor dem Ende des Kontakts — Beendet den laufenden Kontakt

Wenn du einen Kontakt stornierst, hängt die Abrechnung von deinem Terminplanungsmodus und dem Zeitpunkt ab, zu dem du kündigst. Weitere Informationen erhalten Sie von Ihrem AWS-Mitarbeiter.

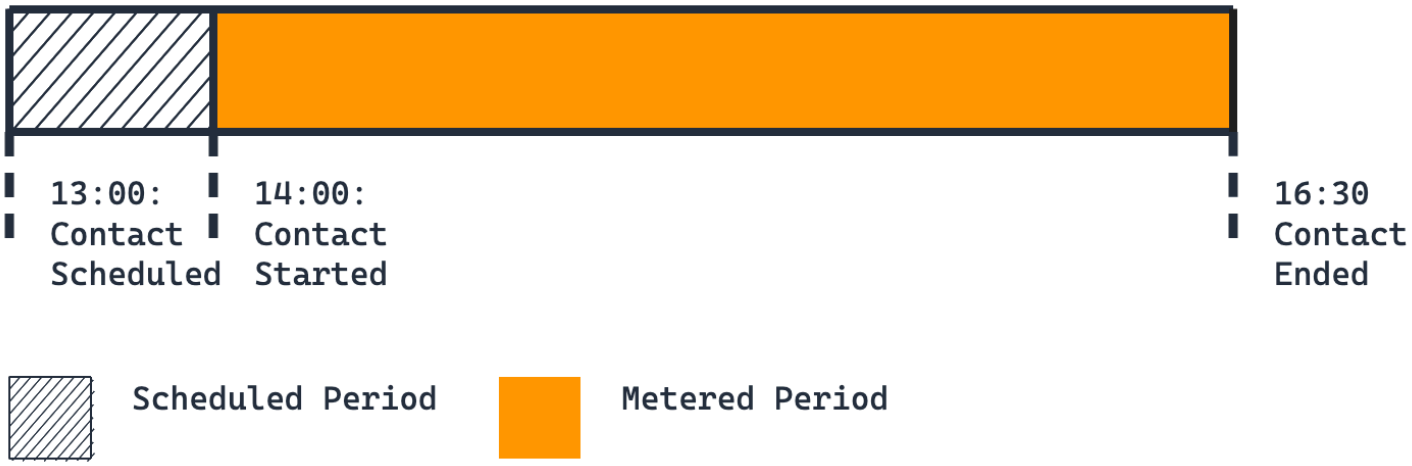
Wenn Sie einen Kontakt beenden, wird Ihnen der Teil des Kontakts, der ausgeführt wurde, und die verbleibende Zeit, die nicht durch doppelte Kontakte abgedeckt ist, in Rechnung gestellt. Ein doppelter Kontakt in diesem Zusammenhang war:

- Es wurde für dieselbe Bodenstation geplant wie der ursprünglich abgebrochene Kontakt
- Geplant mit derselben AWS-Konto-ID wie der ursprünglich unterbrochene Kontakt
- Reserviert, nachdem der Befehl ausgegeben wurde, den ursprünglichen Kontakt zu beenden

Die folgenden Szenarien zeigen, wie diese Messung in der Praxis funktioniert.

Szenario 1: Ein einziger Ansprechpartner

Sie planen einen 150-minütigen Kontakt auf der Ground Station Anytown 1, der um 14:00 Uhr beginnt und um 16:30 Uhr endet.



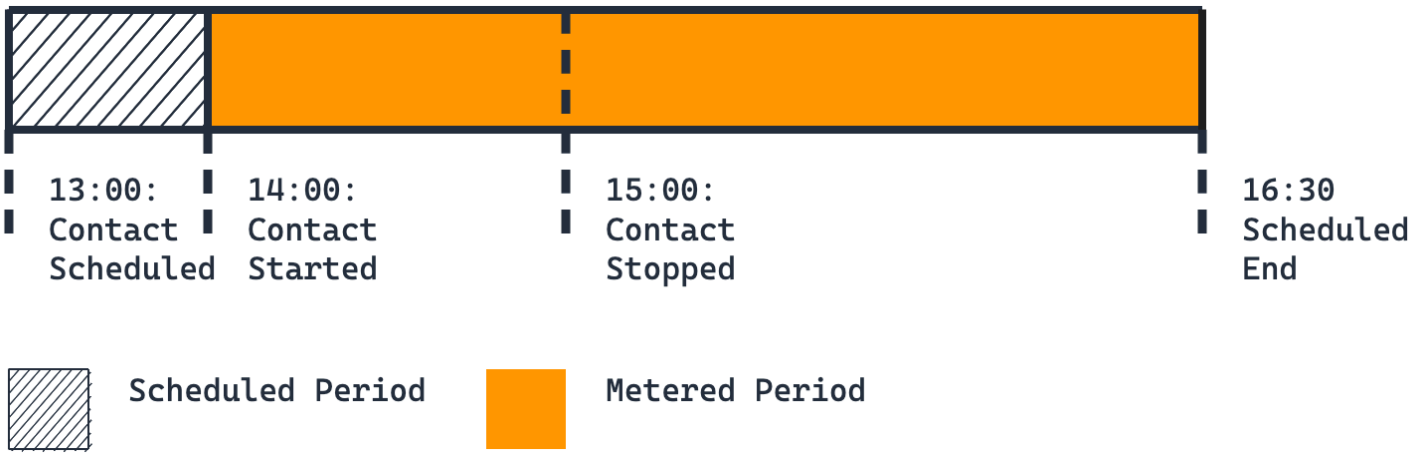
Aufschlüsselung der Abrechnung:

- Erster Kontakt: 150 Minuten (volle Dauer)

Ihnen werden 150 Minuten in Rechnung gestellt. Dies ist das Basisszenario, in dem ein Kontakt seinen geplanten Abschluss ohne Unterbrechungen oder Stornierungen erreicht.

Szenario 2: Einzelner abgebrochener Kontakt

Sie planen einen 150-minütigen Kontakt auf der Ground Station Anytown 1, der um 14:00 Uhr beginnt und um 16:30 Uhr endet. Um 15:00 Uhr rufen Sie die CancelContact API auf, um Ihren Kontakt zu beenden.



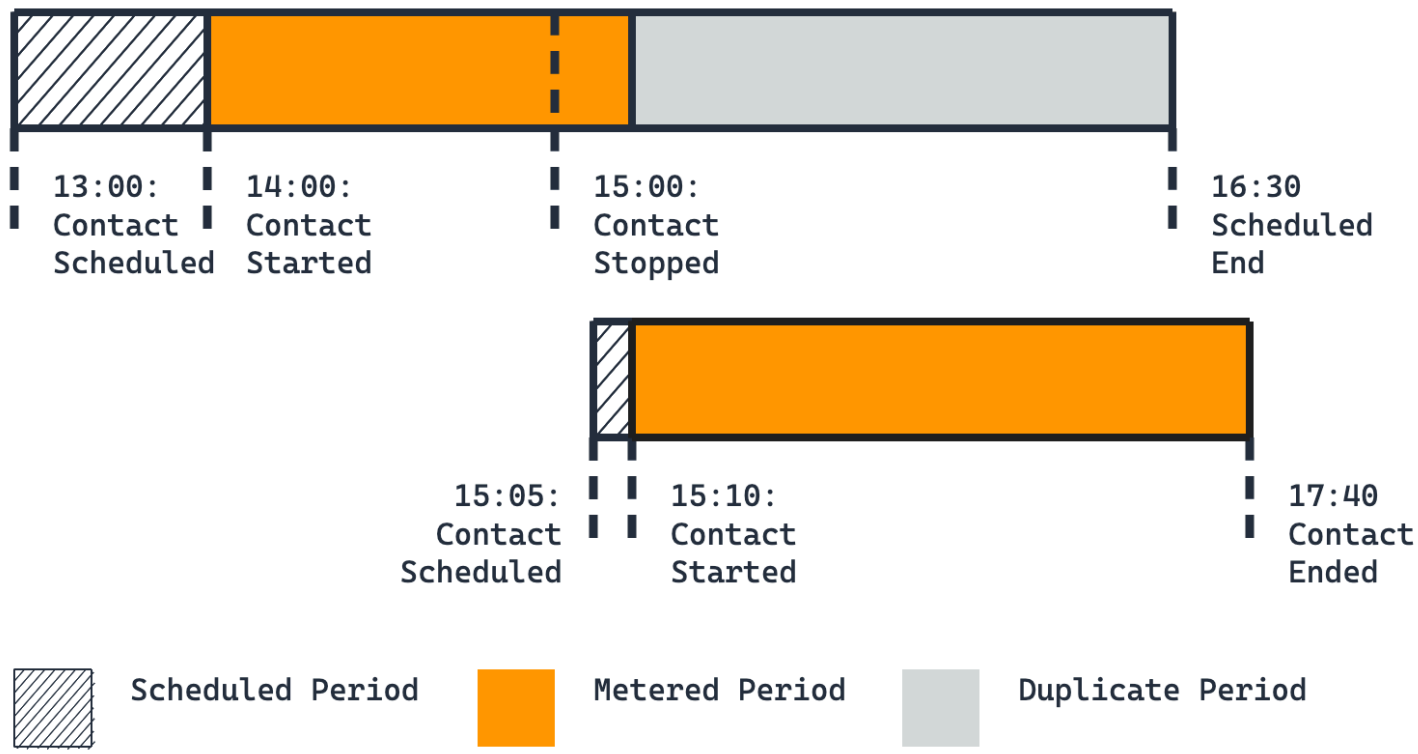
Aufschlüsselung der Abrechnung:

- Erster Kontakt: 150 Minuten (volle ursprüngliche Dauer)

Ihnen werden die vollen 150 Minuten in Rechnung gestellt, weil Sie den Kontakt beendet haben, aber keine doppelten Kontakte für die verbleibende Zeit (15:00-16:30) geplant haben. Wenn Sie einen Kontakt beenden, ohne Duplikate zu planen, bleiben Sie für die gesamte ursprünglich geplante Dauer verantwortlich.

Szenario 3: Einzelnes Duplikat

Sie planen einen 150-minütigen Kontakt auf der Ground Station Anytown 1, der um 14:00 Uhr beginnt und um 16:30 Uhr endet. Um 15:00 Uhr rufen Sie die CancelContact API auf, um Ihren ersten Kontakt zu beenden. Nach dem Anruf CancelContact vereinbaren Sie einen weiteren Kontakt auf derselben Ground Station ab 15:10 Uhr für 150 Minuten.



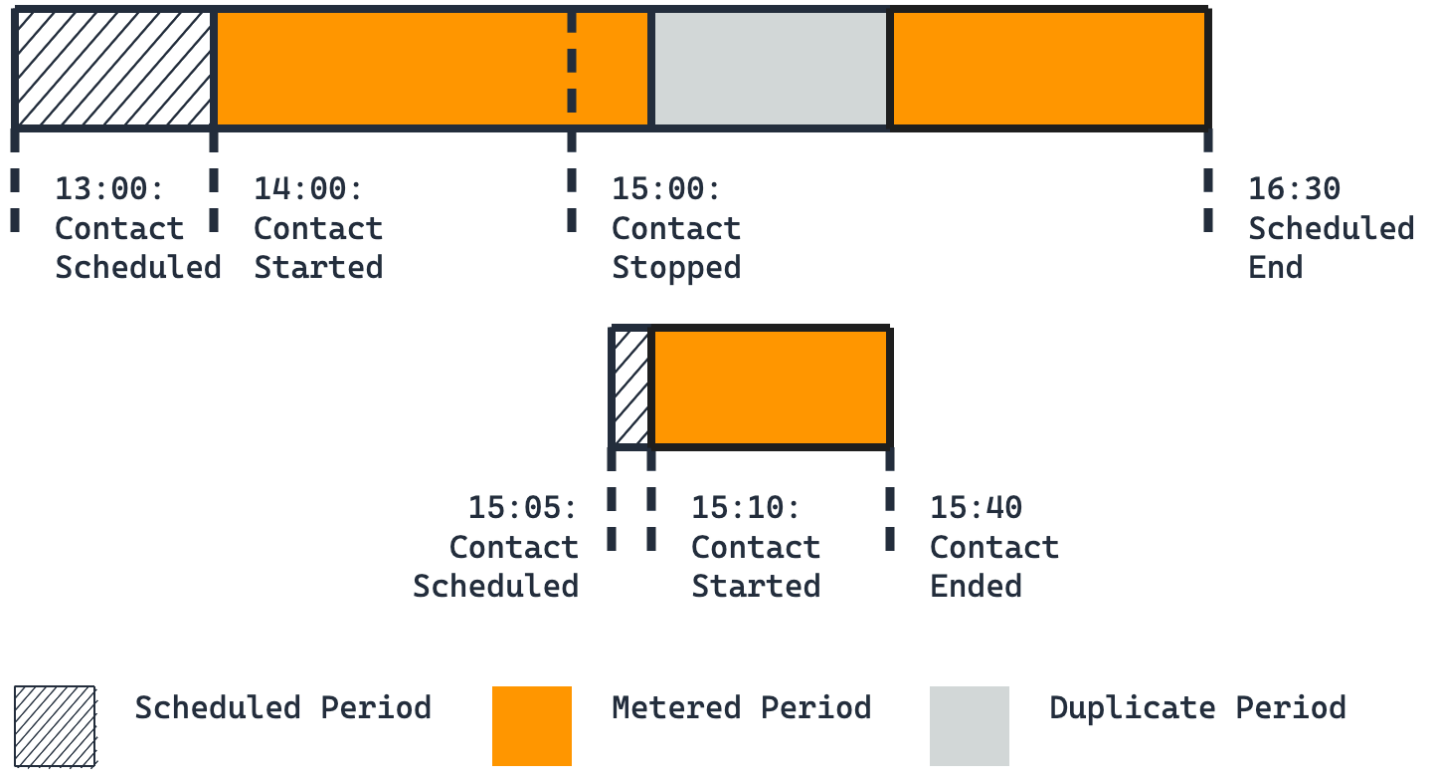
Aufschlüsselung der Abrechnung:

- Erster Kontakt: 70 Minuten (60 Minuten Bearbeitung plus 10 Minuten Ausfallzeit, bevor der zweite Kontakt beginnt)
- Zweiter Kontakt: 150 Minuten (volle Dauer)

Der zweite Kontakt ist ein Duplikat, da Sie ihn geplant haben, nachdem Sie den ersten Kontakt beendet haben. Das Duplikat deckt die verbleibende Zeit von 15:10 bis 16:30 Uhr ab. Ihnen wird also nur die Zeit in Rechnung gestellt, in der der erste Kontakt tatsächlich ausgeführt wurde, zuzüglich der Zeitspanne von 10 Minuten zwischen dem Stoppen und Neustarten.

Szenario 4: Kurzes Duplikat

Sie planen einen 150-minütigen Kontakt auf der Ground Station Anytown 1, der um 14:00 Uhr beginnt und um 16:30 Uhr endet. Um 15:00 Uhr rufen Sie die CancelContact API auf, um Ihren ersten Kontakt zu beenden. Nach dem Anruf CancelContact vereinbaren Sie ab 15:10 Uhr einen 30-minütigen Kontakt an derselben Ground Station.



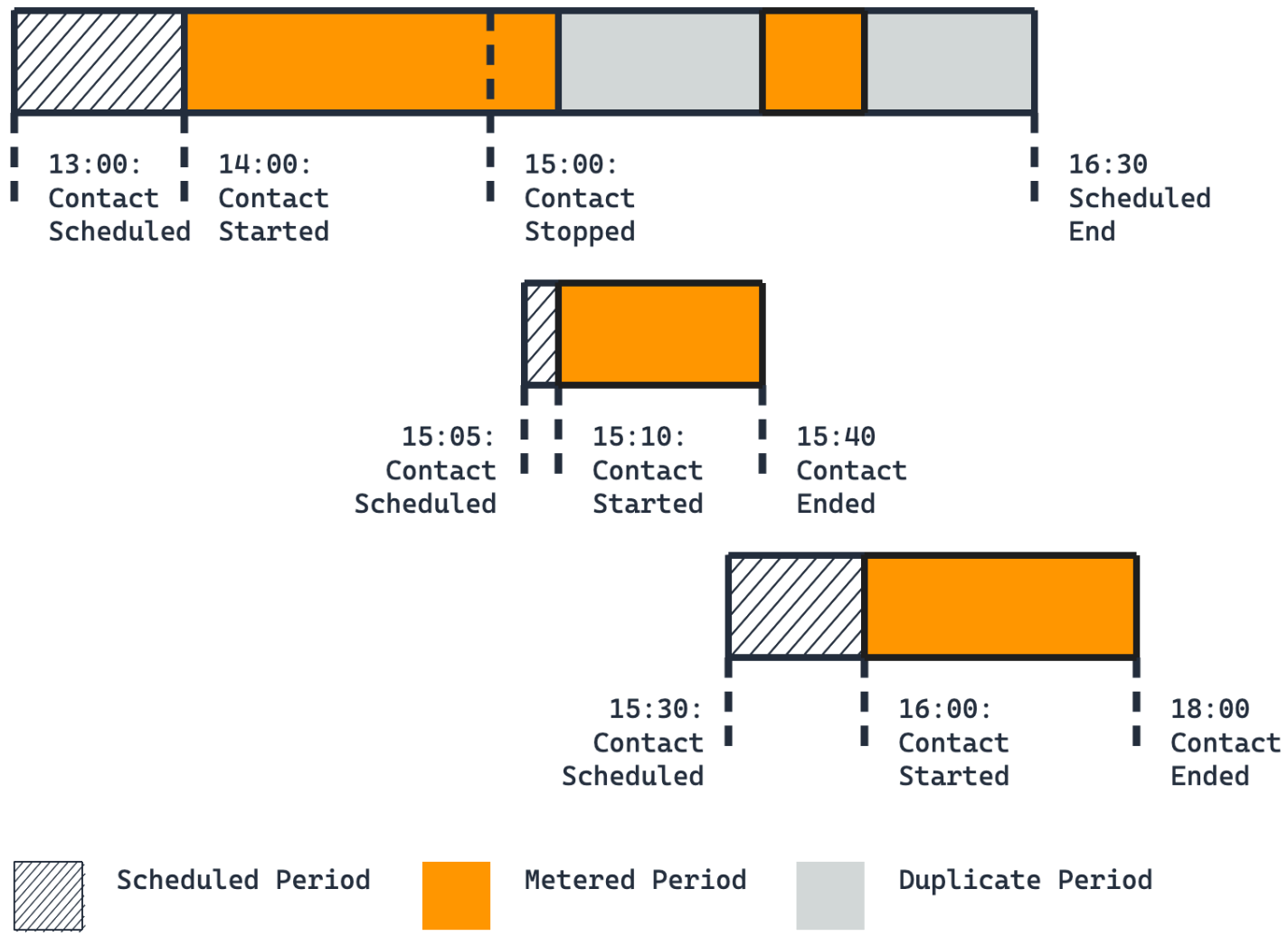
Aufschlüsselung der Abrechnung:

- Erster Kontakt: 120 Minuten (60 Minuten Bearbeitung + 10 Minuten Ausfallzeit vor Beginn des zweiten Kontakts + 50 Minuten Restzeit, die das Duplikat nicht abdeckte)
- Zweiter Kontakt: 30 Minuten (volle Dauer)

Der doppelte Kontakt deckt nur 30 Minuten (15:10-15:40) der 90 Minuten ab, die nach dem Beenden des ersten Kontakts verbleiben. Ihnen werden sowohl die 10-minütige Pause vor Beginn des Duplikats als auch die 50 Minuten aufgedeckter Zeit nach dem Ende des Duplikats (15:40-16:30) in Rechnung gestellt.

Szenario 5: Mehrere Duplikate

Sie planen einen 150-minütigen Kontakt auf der Ground Station Anytown 1, der um 14:00 Uhr beginnt und um 16:30 Uhr endet. Um 15:00 Uhr rufen Sie die CancelContact API auf, um Ihren ersten Kontakt zu beenden. Nach dem Anruf CancelContact vereinbaren Sie ab 15:10 Uhr einen 30-minütigen Kontakt an derselben Ground Station. Später, um 15:30 Uhr, vereinbaren Sie einen weiteren Kontakt ab 16:00 Uhr für 120 Minuten.



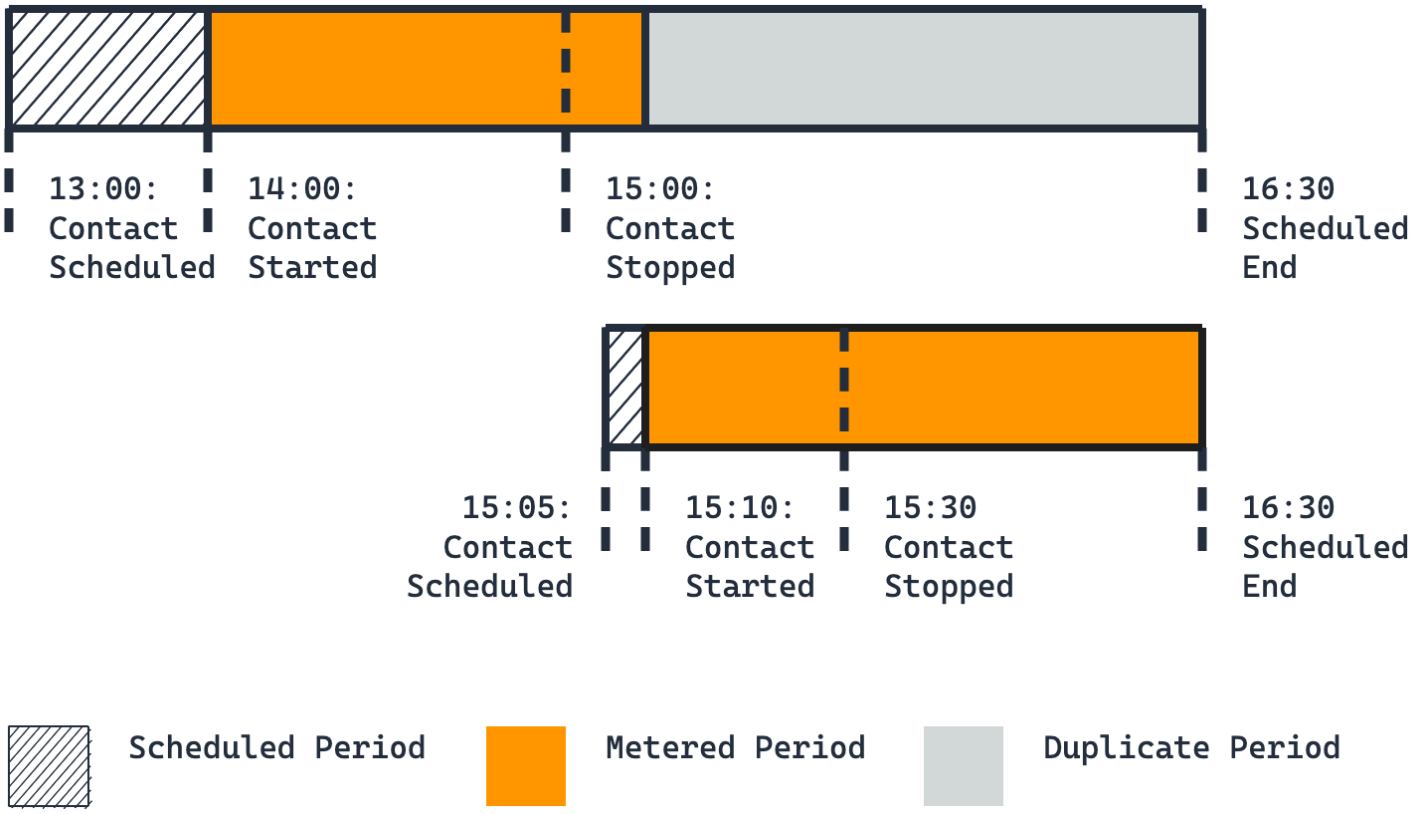
Aufschlüsselung der Abrechnung:

- Erster Kontakt: 90 Minuten (60 Minuten Ausführung + 10 Minuten Ausfallzeit vor Beginn des zweiten Kontakts + 20 Minuten Ausfallzeit zwischen dem zweiten und dem dritten Kontakt)
- Zweiter Kontakt: 30 Minuten (volle Dauer)
- Dritter Kontakt: 120 Minuten (volle Dauer)

Sowohl der zweite als auch der dritte Kontakt gelten als Duplikate, da Sie sie nach dem Beenden des ersten Kontakts geplant haben. Ihnen werden jedoch weiterhin die Lücken zwischen den Kontakten in Rechnung gestellt: 10 Minuten zwischen dem ersten Stopp (15:00) und dem zweiten Start (15:10) und 20 Minuten zwischen dem zweiten Ende (15:40) und dem dritten Start (16:00).

Szenario 6: Mehrere Stopps

Sie planen einen 150-minütigen Kontakt auf der Ground Station Anytown 1, der um 14:00 Uhr beginnt und um 16:30 Uhr endet. Um 15:00 Uhr rufen Sie die CancelContact API auf, um Ihren ersten Kontakt zu beenden. Nach dem Anruf CancelContact vereinbaren Sie einen 80-minütigen Kontakt auf der Ground Station Anytown 1, der um 15:10 Uhr beginnt und um 16:30 Uhr endet. Um 15:30 Uhr rufen Sie die CancelContact API erneut auf und beenden so Ihren doppelten Kontakt.



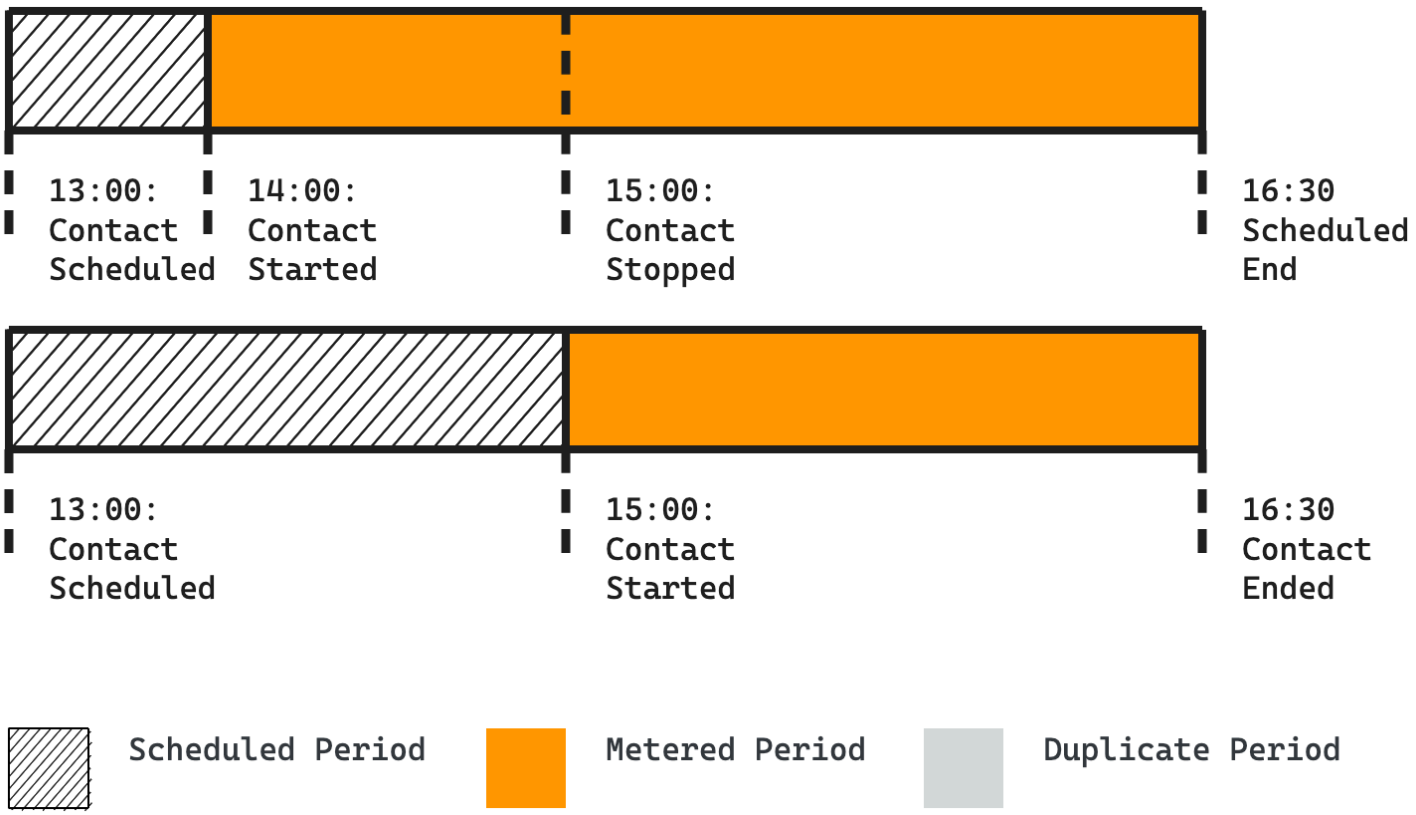
Aufschlüsselung der Abrechnung:

- Erster Kontakt: 70 Minuten (60 Minuten Bearbeitung plus 10 Minuten Ausfallzeit, bevor der zweite Kontakt beginnt)
- Zweiter Kontakt: 80 Minuten (volle ursprüngliche Dauer)

Der zweite Kontakt wird für die gesamte Dauer von 80 Minuten in Rechnung gestellt, da Sie ihn um 15:30 Uhr unterbrochen haben und somit 60 Minuten der ursprünglich geplanten Zeit (15:30-16:30) unbesetzt geblieben sind. Sofern Sie nicht einen weiteren doppelten Kontakt für die verbleibende Zeit planen, sind Sie für die gesamte Dauer eines unterbrochenen Kontakts verantwortlich.

Szenario 7: Bodenstation mit mehreren Antennen ohne Duplikat

Um 13:00 Uhr vereinbaren Sie zwei Kontakte auf der Ground Station Anytown 1. Der erste ist ein 150-minütiger Kontakt, der um 14:00 Uhr beginnt und um 16:30 Uhr endet. Der zweite ist ein 90-minütiger Kontakt, der um 15:00 Uhr beginnt und um 16:30 Uhr endet. Um 15:00 Uhr rufen Sie die CancelContact API auf, um Ihren ersten Kontakt zu beenden. Ground Station Anytown 1 ist eine Bodenstation mit mehreren Antennen, mit der beide Kontakte gleichzeitig betrieben werden können.



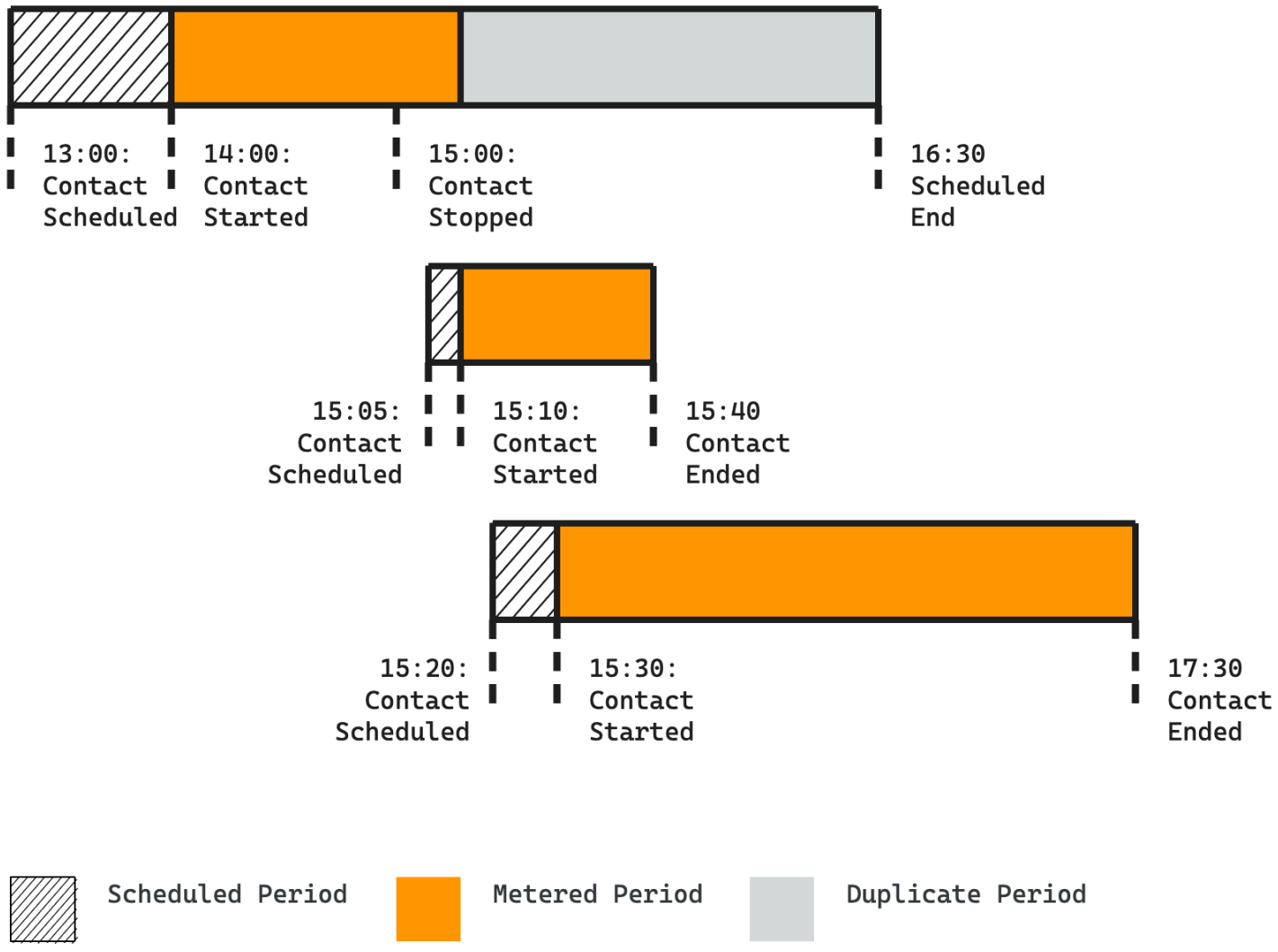
Aufschlüsselung der Abrechnung:

- Erster Kontakt: 150 Minuten (volle ursprüngliche Dauer)
- Zweiter Kontakt: 90 Minuten (volle Dauer)

Der zweite Kontakt überschneidet sich zwar mit dem unterbrochenen Teil des ersten Kontakts, zählt aber nicht als Duplikat. Der zweite Kontakt erfüllt nicht das erste Kriterium für Duplikate: Er war für 13:00 Uhr geplant, bevor Sie den ersten Kontakt um 15:00 Uhr beendet haben. Da es sich nicht um ein Duplikat handelt, wird Ihnen die gesamte ursprüngliche Dauer des ersten Kontakts in Rechnung gestellt, unabhängig davon, wann Sie ihn beendet haben.

Szenario 8: Bodenstation mit mehreren Antennen und doppelten Kontakten

Sie planen einen 150-minütigen Kontakt auf der Ground Station Anytown 1, der um 14:00 Uhr beginnt und um 16:30 Uhr endet. Um 15:00 Uhr rufen Sie die CancelContact API auf, um Ihren ersten Kontakt zu beenden. Nach dem Anruf CancelContact vereinbaren Sie einen 30-minütigen Kontakt auf der Ground Station Anytown 1, der um 15:10 Uhr beginnt und um 15:40 Uhr endet. Später vereinbaren Sie einen weiteren 90-minütigen Kontakt auf der Ground Station Anytown 1, der um 15:30 Uhr beginnt und um 17:00 Uhr endet. Ground Station Anytown 1 ist eine Bodenstation mit mehreren Antennen, die es ermöglicht, beide doppelten Kontakte gleichzeitig mit überlappenden Zeiten zu betreiben.



Aufschlüsselung der Abrechnung:

- Erster Kontakt: 70 Minuten (60 Minuten Bearbeitung plus 10 Minuten Ausfallzeit, bevor der zweite Kontakt beginnt)
- Zweiter Kontakt: 30 Minuten (volle Dauer)
- Dritter Kontakt: 90 Minuten (volle Dauer)

Sowohl der zweite als auch der dritte Kontakt gelten als Duplikate, da Sie sie nach dem Beenden des ersten Kontakts geplant haben. Der Abstand von 10 Minuten zwischen dem Beenden des ersten Kontakts (15:00 Uhr) und dem Starten des zweiten Kontakts (15:10) stellt eine Ausfallzeit dar, die Ihnen gegenüber dem ursprünglichen Kontakt in Rechnung gestellt wird.

Verwenden Sie die AWS Ground Station digitale Zwillingsfunktion

Die digitale Zwillingsfunktion für AWS Ground Station bietet Ihnen eine Umgebung, in der Sie Ihre Software für die Verwaltung und Steuerung von Satellitenmissionen testen und integrieren können. Mit der Funktion für den digitalen Zwilling können Sie die Testplanung, die Überprüfung der Konfigurationen und die korrekte Fehlerbehandlung durchführen, ohne die Kapazität der Produktionsantenne zu beanspruchen. Wenn Sie Ihre AWS Ground Station Integration mit der digitalen Zwillingsfunktion testen, können Sie mehr Vertrauen in die Fähigkeit Ihres Systems haben, Ihren Satellitenbetrieb reibungslos zu verwalten. Außerdem können Sie damit testen, AWS Ground Station APIs ohne Produktionskapazität zu beanspruchen oder Frequenzlizenzen zu benötigen.

Um loszulegen, folgen Sie dem Formular Satellit an Bord und fordern Sie an, in die digitale Zwillingsfunktion integriert zu werden. Sobald Ihr Satellit in die digitale Zwillingsfunktion integriert ist, können Sie Kontakte mit Bodenstationen für digitale Zwillinge planen. Die Liste der Bodenstationen, auf die Sie Zugriff haben, kann über die ListGroundStationsAWS-SDK-Antwort abgerufen werden. Digitale Zwillingsbodenstationen sind exakte Kopien der in aufgeführten Bodenstationen AWS Ground Station Standorte mit dem modifizierenden Präfix „Name der Ground Station“ von „Digital Twin“. Dazu gehören ihre Antennenfunktionen und Metadaten, einschließlich, aber nicht beschränkt auf die Standortmaske und die tatsächlichen GPS-Koordinaten. Derzeit unterstützt die Funktion für den digitalen Zwilling keine Datenübermittlung, wie unter beschriebenMit Datenflüssen arbeiten.

Nach dem Onboarding sendet die digitale Zwillingsfunktion dieselben EventBridge Amazon-Ereignisse und API-Antworten aus wie der Produktionsservice, wie unter beschrieben. Automatisieren Sie AWS Ground Station mit Ereignissen Diese Ereignisse ermöglichen Ihnen die Feinabstimmung Ihrer Konfigurationen und Datenfluss-Endpunktgruppen.

Verstehen Sie die Überwachung mit 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 EventBridge Events bietet einen Stream von Systemereignissen, die Änderungen an AWS Ressourcen beschreiben, nahezu in Echtzeit. EventBridge 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 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 feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Aufrufe erfolgten. Weitere Informationen zu AWS CloudTrail finden Sie im AWS CloudTrail Benutzerhandbuch.
- Amazon CloudWatch Metrics erfasst bei der Nutzung Metriken 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 Verwenden von CloudWatch Amazon-Metriken.
- 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, darunter E-Mail, Amazon Q Developer in Chat-Anwendungen, Chat-Benachrichtigungen oder AWS Console Mobile ApplicationPush-Benachrichtigungen. Sie können Benachrichtigungen auch im Benachrichtigungscenter der AWS Konsole sehen. Benutzerbenachrichtigungen unterstützt die Aggregation, wodurch die Anzahl der Benachrichtigungen, die Sie bei bestimmten Ereignissen erhalten, reduziert werden kann.

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

Themen

- Automatisieren Sie AWS Ground Station mit Ereignissen
- AWS Ground Station API-Aufrufe protokollieren mit AWS CloudTrail
- Metriken mit Amazon anzeigen CloudWatch

Automatisieren Sie 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. Zu den Aktionen, die automatisch ausgelöst werden können, gehören die folgenden:

- 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
- Benachrichtigen eines Amazon SNS-Themas oder einer Amazon SQS-Warteschlange

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 EventBridge Events-Benutzerhandbuch.

AWS Ground Station Arten von Ereignissen

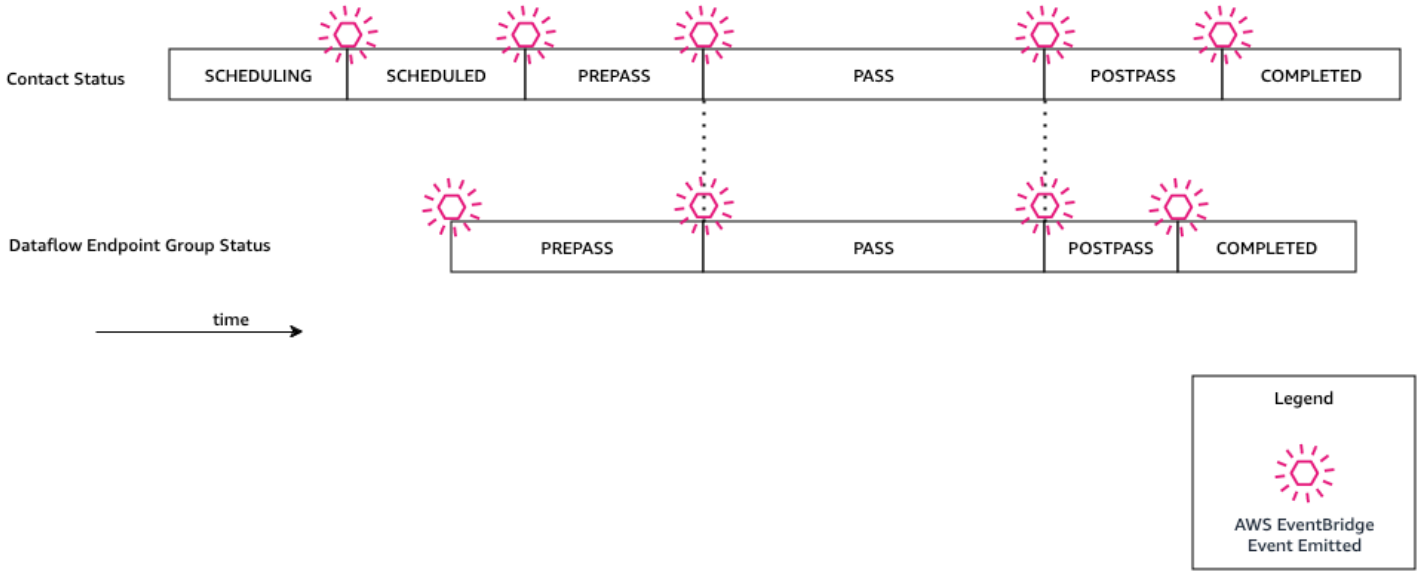
> **Note**
>
> Alle von AWS Ground Station generierten Ereignisse haben „aws.groundstation“ als Wert für „source“.

AWS Ground Station gibt Ereignisse aus, die sich auf Statusänderungen beziehen, um Sie bei der Anpassung Ihrer Automatisierung zu unterstützen. AWS Ground Station Unterstützt derzeit Kontaktstatusänderungsereignisse, Datenfluss-Endpunktgruppen-Änderungsereignisse und kurzlebige Statusänderungsereignisse. Die folgenden Abschnitte enthalten detaillierte Informationen zu den einzelnen Typen.

Event-Zeitplan kontaktieren

AWS Ground Station sendet Ereignisse aus, wenn Ihr Kontakt den Status ändert. Weitere Informationen darüber, was diese Statusänderungen sind und was die Staaten selbst bedeuten, finden Sie unterVerstehen Sie den Lebenszyklus von Kontakten. Alle Datenfluss-Endpunktgruppen, die in Ihrem Kontakt verwendet werden, verfügen über einen unabhängigen Satz von Ereignissen, die ebenfalls ausgelöst werden. Im gleichen Zeitraum senden wir auch Ereignisse für Ihre Datenfluss-Endpunktgruppe aus. Die genaue Uhrzeit der Pre-Pass- und Post-Pass-Ereignisse können Sie bei der Einrichtung Ihres Missionsprofils und der Dataflow-Endpunktgruppe konfigurieren.

Das folgende Diagramm zeigt die Status und Ereignisse, die für einen nominellen Kontakt und die zugehörige Datenfluss-Endpunktgruppe ausgegeben wurden.



Änderung des Ground Station-Kontaktzustands

Wenn Sie eine bestimmte Aktion ausführen möchten, wenn sich der Status eines bevorstehenden Kontakts 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 contactPrePassDurationSecondsund in Ihrem Missionsprofil ändern contactPostPassDurationSeconds. Die Ereignisse werden in die Region gesendet, in der der Kontakt geplant wurde.

Ein Beispiel für ein Ereignis finden Sie unten.

```
{
    "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"
    }
}
```

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

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"
    }
}
```

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

Ephemeriden-Ereignisse

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"
    }
}
```

Mögliche Zustände dafür `ephemerisStatus` sind`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 CloudTrail userIdentity-Element.

Grundlegendes zu AWS Ground Station Protokolldateieinträgen

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_PRINCIPAL_ID",
        "arn": "arn:aws:sts::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2019-05-15T21:11:59Z"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EX_PRINCIPAL_ID",
                "arn": "arn:aws:iam::123456789012:role/Alice",
                "accountId": "123456789012",
                "userName": "Alice"
            }
        }
    },
    "eventTime": "2019-05-15T21:14:37Z",
    "eventSource": "groundstation.amazonaws.com",
    "eventName": "ReserveContact",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "127.0.0.1",
    "userAgent": "Mozilla/5.0 Gecko/20100101 Firefox/123.0",
    "requestParameters": {
        "satelliteArn":
 "arn:aws:groundstation::123456789012:satellite/11111111-2222-3333-4444-555555555555",
        "groundStation": "Ohio 1",
        "startTime": 1558356107,
        "missionProfileArn": "arn:aws:groundstation:us-east-2:123456789012:mission-
profile/11111111-2222-3333-4444-555555555555",
        "endTime": 1558356886
    },
    "responseElements": {
        "contactId": "11111111-2222-3333-4444-555555555555"
    },
    "requestID": "11111111-2222-3333-4444-555555555555",
```

```
    "eventID": "11111111-2222-3333-4444-555555555555",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "11111111-2222-3333-4444-555555555555"
}
```

Metriken mit Amazon anzeigen CloudWatch

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

Die AWS Ground Station Telemetriefunktion kann auch verwendet werden, um bei Kontakten Metriken nahezu in Echtzeit zu erhalten. CloudWatch Metriken sind nicht nahezu in Echtzeit verfügbar und es kann zu Verzögerungen bei der Lieferung kommen. CloudWatch aggregiert außerdem Metriken über einen Zeitraum von einer Sekunde, wodurch die Datengranularität möglicherweise reduziert wird. Die Telemetriefunktion stellt die einzelnen Metriken bereit und übermittelt sie nahezu in Echtzeit direkt an Ihr Konto. AWS Weitere Informationen finden Sie unter Arbeiten Sie mit Telemetrie.

> **Important**
>
> AWS Ground Station sendet CloudWatch Messwerte an die AWS Region, die mit dem Standort der Bodenstation des Kontakts verknüpft ist, und nicht an die AWS Region, von der aus der Kontakt geplant wurde. Um die Messwerte für einen Kontakt anzuzeigen, müssen Sie CloudWatch in der Region der Bodenstation darauf zugreifen. Informationen darüber, welche AWS Region mit den einzelnen Standorten der Bodenstation verknüpft ist, finden Sie unterFinden Sie die AWS Region für einen Standort für eine Bodenstation. Um Telemetriedaten in der Region zu empfangen, von der aus Sie Ihre Kontakte planen, können Sie die AWS Ground Station Telemetriefunktion verwenden. Weitere Details finden Sie unter Arbeiten Sie mit Telemetrie.

AWS Ground Station Metriken und Dimensionen

Welche Metriken sind verfügbar?

Die folgenden Metriken sind bei erhältlich AWS Ground Station.

> **Note**
>
> Die spezifischen ausgegebenen Metriken hängen von den verwendeten AWS Ground Station Funktionen ab. Abhängig von Ihrer Konfiguration kann nur eine Teilmenge der folgenden Metriken ausgegeben werden.

Metrik	Metrikdimensionen	Description
`AzimuthAngle`	SatelliteId	Der Azimutwinkel der Antenne. Der wahre Norden ist 0 Grad und der Osten ist 90 Grad. Einheiten: Grad
`BitErrorRate`	Kanal, Polarisation, SatelliteId	Die Fehlerrate bei Bits bei einer bestimmten Anzahl von Bitübertragungen. Bitfehler werden durch Rauschen, Verzerrungen oder Störungen verursacht Einheiten: Bitfehler pro Zeiteinheit
`BlockErrorRate`	Kanal, Polarisation, SatelliteId	Die Fehlerquote von Blöcken in einer bestimmte

Metrik	Metrikdimensionen	Description
		n Anzahl empfangener Blöcke. Blockfehler werden durch Störungen verursacht. Einheiten: Fehlerhafte Blöcke/Gesamtzahl der Blöcke
`CarrierFrequencyRecovery_Cn0`	Kategorie, Config, SatelliteId	Verhältnis zwischen Träger und Rauschdichte pro Bandbreiteneinheit. Einheiten: Dezibel-Hertz (dB-Hz)
`CarrierFrequencyRecovery_Locked`	Kategorie, Config, SatelliteId	Wird auf 1 gesetzt, wenn die Trägerfrequenz-Wiederherstellungsschleife des Demodulators gesperrt ist, und auf 0, wenn sie entsperrt ist. Einheiten: ohne Einheit

Metrik	Metrikdimensionen	Description
`CarrierFrequencyRecovery_OffsetFrequency_Hz`	Kategorie, Config, SatelliteId	Der Offset zwischen dem geschätzten Signalzentrum und der idealen Mittenfrequenz. Dies wird durch die Dopplerverschiebung und den Offset des Lokaloszillators zwischen Raumfahrzeug und Antennensystem verursacht. Einheiten: Hertz (Hz)
`ElevationAngle`	SatelliteId	Der Höhenwinkel der Antenne. Der Horizont ist 0 Grad und der Zenit ist 90 Grad. Einheiten: Grad

Metrik	Metrikdimensionen	Description
`Es/N0`	Kanal, Polarisation, SatelliteId	Das Verhältnis von Energie pro Symbol zur spektralen Leistungsdichte des Rauschens. Einheiten: Dezibel (dB)
`ReceivedPower`	Polarisierung, SatelliteId	Die gemessene Signalstärke im Demodulator/Decoder. Einheiten: Dezibel relativ zu Milliwatt (dBm)
`SymbolTimingRecovery_ErrorVectorMagnitude`	Kategorie, Config, SatelliteId	Die Größe des Fehlervektors zwischen empfangenen Symbolen und idealen Konstellationspunkten. Einheiten: Prozent

Metrik	Metrikdimensionen	Description
SymbolTimingRecovery_Locked	Kategorie, Config, SatelliteId	Auf 1 setzen, wenn die Zeitwiederherstellungsschleife des Demodulatorsymbols gesperrt ist, und auf 0, wenn sie entsperrt ist Einheiten: ohne Einheit
SymbolTimingRecovery_OffsetSymbolRate	Kategorie, Config, SatelliteId	Der Offset zwischen der geschätzten Symbolrate und der idealen Signalsymbolrate. Dies wird durch die Dopplerverschiebung und den Offset des Lokaloszillators zwischen Raumfahrzeug und Antennensystem verursacht. Einheiten: Symbole/Sekunde

Wofür werden Dimensionen verwendet? AWS Ground Station

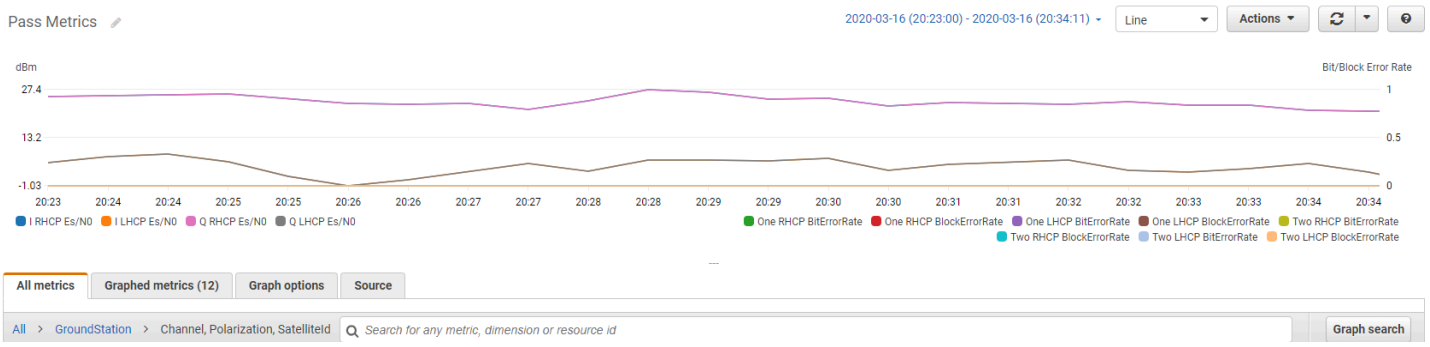
Sie können AWS Ground Station Daten anhand der folgenden Dimensionen filtern.

Dimension	Description
`Category`	Demodulation oder Decodierung.
`Channel`	Die Kanäle für jeden Kontakt umfassen One, Two, I (In-Phase) und Q (Quadrature).
`Config`	Ein Antennen-Downlink-Demod-Decoder-Konf igurations-ARN.
`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 zusammengefasst. 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 Weitere Informationen zur CloudWatch Aufbewahrung finden Sie unter CloudWatch Amazon-Konzepte — Aufbewahrung metrischer Daten.

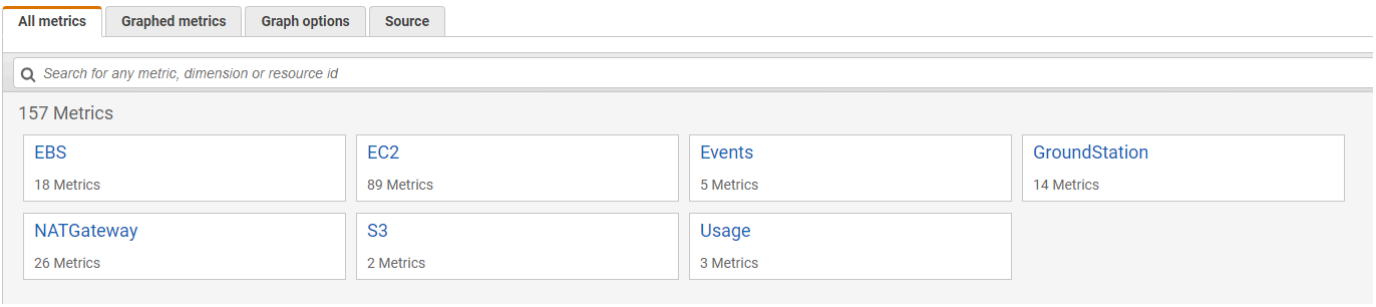
Darüber hinaus enthalten alle innerhalb der ersten 60 Sekunden erfassten Daten nicht genügend Informationen, um aussagekräftige Metriken zu erzeugen, und werden wahrscheinlich nicht angezeigt. Um aussagekräftige Metriken anzuzeigen, empfiehlt es sich, Ihre Daten nach 60 Sekunden anzuzeigen.



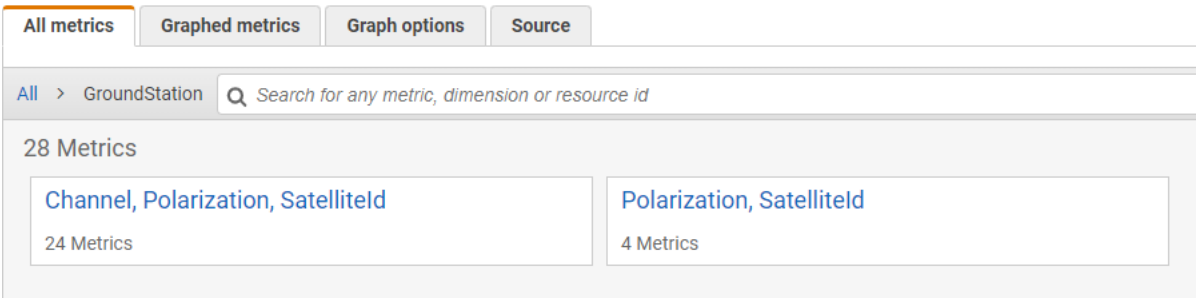
Weitere Informationen zur grafischen Darstellung von AWS Ground Station Metriken finden Sie unter [Metriken grafisch darstellen. CloudWatch]

So zeigen Sie Metriken mithilfe der -Konsole an

1. Ermitteln Sie die AWS Region, die mit dem Standort Ihrer Bodenstation verknüpft ist. AWS Ground Station sendet CloudWatch Messwerte in der Region aus, die mit dem Standort der Bodenstation Ihres Kontakts verknüpft ist. Eine Liste der Standorte der Bodenstationen und der zugehörigen AWS Regionen finden Sie unter[Finden Sie die AWS Region für einen Standort für eine Bodenstation].
2. Öffnen Sie die [CloudWatch -Konsole].
3. Wählen Sie im Navigationsbereich Metriken aus.
4. Wählen Sie den GroundStation-Namespace.



5. Wählen Sie die gewünschten metrischen Abmessungen aus (z. B. Kanal, Polarisation, SatelliteId).



6. 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 Überschriftenzeile 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

AWS Ground Station sendet CloudWatch Metriken in der Region aus, die dem Standort der Bodenstation Ihres Kontakts zugeordnet ist. Für die Liste der Standorte der Bodenstationen und deren zugehörige AWS Regionen,Finden Sie die AWS Region für einen Standort für eine Bodenstation. *`ground-station-region-code`*Ersetzen Sie es durch den AWS Regionalcode für den Standort Ihrer Bodenstation (z. B. `us-west-2` für Oregon 1, Hawaii 1 oder Alaska 1). Alle nachfolgenden AWS CLI Befehle in diesem Verfahren müssen dieselbe Region verwenden.

1. Stellen Sie sicher, dass AWS CLI das installiert ist. Informationen zur Installation AWS CLI finden Sie unter Installation der AWS-CLI Version 2.
2. Identifizieren Sie die AWS Region, die mit dem Standort Ihrer Bodenstation verknüpft ist.
3. Verwenden Sie die get-metric-dataMethode der CloudWatch CLI, um eine Datei zu generieren, die geändert werden kann, um die Metriken anzugeben, an denen Sie interessiert sind, und die dann zur Abfrage dieser Metriken verwendet werden kann.

Führen Sie dazu den folgenden Befehl aus:`aws cloudwatch get-metric-data --region` *`ground-station-region-code`* `--generate-cli-skeleton`. Dadurch wird eine Ausgabe generiert, die der folgenden ähnelt:

```
{
   "MetricDataQueries": [
      {
         "Id": "",
         "MetricStat": {
            "Metric": {
               "Namespace": "",
               "MetricName": "",
               "Dimensions": [
                  {
                     "Name": "",
                     "Value": ""
                  }
               ]
            },
            "Period": 0,
            "Stat": "",
            "Unit": "Seconds"
         },
         "Expression": "",
         "Label": "",
         "ReturnData": true,
         "Period": 0,
         "AccountId": ""
      } ],
   "StartTime": "1970-01-01T00:00:00",
   "EndTime": "1970-01-01T00:00:00",
   "NextToken": "",
   "ScanBy": "TimestampDescending",
   "MaxDatapoints": 0,
   "LabelOptions": {
      "Timezone": ""
   }
}
```

4. Listet die verfügbaren CloudWatch Metriken auf, indem Sie den Befehl ausführen`aws cloudwatch list-metrics --region` *`ground-station-region-code`*.

   Wenn Sie die Methode kürzlich verwendet haben AWS Ground Station, sollte sie eine Ausgabe zurückgeben, die Einträge wie die folgenden enthält:

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

   > **Note**
   >
   > Wenn seit Ihrer letzten Verwendung mehr als 2 Wochen vergangen sind AWS Ground Station, müssen Sie die Tabelle der verfügbaren Metriken manuell überprüfen, um die Namen und Dimensionen der Metriken im Metrik-Namespace zu finden. `AWS/GroundStation` Weitere Informationen zu CloudWatch Einschränkungen finden Sie unter: Verfügbare Metriken anzeigen

5. Ändern Sie die JSON-Datei, die Sie in Schritt 2 erstellt haben, sodass sie mit den erforderlichen Werten aus Schritt 3 und `Polarization` Ihren Metriken übereinstimmt. `SatelliteId` Achten Sie außerdem darauf`StartTime`, die `EndTime` Werte und so zu aktualisieren, dass sie mit Ihrem Kontakt übereinstimmen. Beispiel:

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

> **Note**
>
> AWS Ground Station veröffentlicht Metriken je nach Metrik alle 1 bis 60 Sekunden. Metriken werden nicht zurückgegeben, wenn das `Period` Feld einen Wert hat, der unter dem Veröffentlichungszeitraum für die Metrik liegt.

6. Führen Sie es `aws cloudwatch get-metric-data` mit der in den vorherigen Schritten erstellten Konfigurationsdatei aus. Nachstehend finden Sie ein Beispiel.

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

Metriken werden mit Zeitstempel von Ihrem Kontakt zur Verfügung gestellt. Ein Beispiel für die Ausgabe von AWS Ground Station -Metriken finden Sie unten.


```
{
   "MetricDataResults": [
      {
         "Id": "receivedPowerExample",
         "Label": "ReceivedPowerExample",
         "Timestamps": [
            "2024-04-08T18:35:00+00:00",
            "2024-04-08T18:30:00+00:00",
            "2024-04-08T18:25:00+00:00"
         ],
         "Values": [
            -33.30191555023193,
            -31.46100273132324,
            -32.13915576934814
         ],
         "StatusCode": "Complete"
      }
   ],
   "Messages": []
}
```

Sicherheit in AWS Ground Station

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die auf die Anforderungen der sicherheitssensibelsten Unternehmen zugeschnitten sind. AWS bietet sicherheitsspezifische Tools und Funktionen, mit denen Sie Ihre Sicherheitsziele erreichen können. Zu diesen Tools und Funktionen gehören Netzwerksicherheit, Konfigurationsverwaltung, Zugriffskontrolle und Datensicherheit.

Wir empfehlen Ihnen AWS Ground Station, bei der Verwendung branchenweit bewährte Verfahren zu befolgen und Verschlüsselung zu implementieren end-to-end. AWS bietet Ihnen APIs die Möglichkeit, Verschlüsselung und Datenschutz zu integrieren. Weitere Informationen zur AWS Sicherheit finden Sie im Whitepaper Einführung in die AWS-Sicherheit.

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

Topics

- Identity and Access Management für AWS Ground Station
- AWS verwaltete Richtlinien für AWS Ground Station
- Verwenden Sie serviceverknüpfte Rollen für die Ground Station
- Datenverschlüsselung im Ruhezustand für AWS Ground Station
- Datenverschlüsselung während der Übertragung für AWS Ground Station

Identity and Access Management für AWS Ground Station

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu AWS kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Ressourcen zu verwenden. AWS Ground Station IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

- Zielgruppe
- Authentifizierung mit Identitäten
- Verwalten des Zugriffs mit Richtlinien

- Wie AWS Ground Station funktioniert mit IAM
- Beispiele für identitätsbasierte Richtlinien für AWS Ground Station
- Problembehandlung bei AWS Ground Station Identität und Zugriff

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von Ihrer Rolle ab:

- Servicebenutzer – Fordern Sie von Ihrem Administrator Berechtigungen an, wenn Sie nicht auf Features zugreifen können (siehe Problembehandlung bei AWS Ground Station Identität und Zugriff).
- Serviceadministrator – Bestimmen Sie den Benutzerzugriff und stellen Sie Berechtigungsanfragen (siehe Wie AWS Ground Station funktioniert mit IAM).
- IAM-Administrator – Schreiben Sie Richtlinien zur Zugriffsverwaltung (siehe Beispiele für identitätsbasierte Richtlinien für AWS Ground Station).

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen sich als IAM-Benutzer authentifizieren oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich als föderierte Identität anmelden, indem Sie Anmeldeinformationen aus einer Identitätsquelle wie AWS IAM Identity Center (IAM Identity Center), Single Sign-On-Authentifizierung oder Anmeldeinformationen verwenden. Google/Facebook Weitere Informationen zum Anmelden finden Sie unter So melden Sie sich bei Ihrem AWS-Konto an im Benutzerhandbuch für AWS-Anmeldung .

AWS Bietet für den programmatischen Zugriff ein SDK und eine CLI zum kryptografischen Signieren von Anfragen. Weitere Informationen finden Sie unter AWS Signature Version 4 for API requests im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, dem sogenannten AWS-Konto Root-Benutzer, der vollständigen Zugriff auf alle AWS-Services Ressourcen hat. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Eine Liste der

Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Tasks that require root user credentials im IAM-Benutzerhandbuch.

Verbundidentität

Als bewährte Methode sollten menschliche Benutzer für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen einen Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensverzeichnis, Ihrem Directory Service Web-Identitätsanbieter oder der AWS-Services mithilfe von Anmeldeinformationen aus einer Identitätsquelle zugreift. Verbundene Identitäten übernehmen Rollen, die temporäre Anmeldeinformationen bereitstellen.

Für die zentrale Zugriffsverwaltung empfehlen wir AWS IAM Identity Center. Weitere Informationen finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center -Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität mit bestimmten Berechtigungen für eine einzelne Person oder Anwendung. Wir empfehlen die Verwendung temporärer Anmeldeinformationen anstelle von IAM-Benutzern mit langfristigen Anmeldeinformationen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Erfordern, dass menschliche Benutzer den Verbund mit einem Identitätsanbieter verwenden müssen, um AWS mithilfe temporärer Anmeldeinformationen darauf zugreifen zu können.

Eine IAM-Gruppe spezifiziert eine Sammlung von IAM-Benutzern und erleichtert die Verwaltung von Berechtigungen für große Gruppen von Benutzern. Weitere Informationen finden Sie unter Anwendungsfälle für IAM-Benutzer im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität mit spezifischen Berechtigungen, die temporäre Anmeldeinformationen bereitstellt. Sie können eine Rolle übernehmen, indem Sie von einer Benutzer- zu einer IAM-Rolle (Konsole) wechseln AWS CLI oder einen AWS API-Vorgang aufrufen. Weitere Informationen finden Sie unter Methoden, um eine Rolle zu übernehmen im IAM-Benutzerhandbuch.

IAM-Rollen sind nützlich für den Verbundbenutzer-Zugriff, temporäre IAM-Benutzerberechtigungen, kontoübergreifenden Zugriff, serviceübergreifenden Zugriff und Anwendungen, die auf Amazon EC2 laufen. Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie definiert Berechtigungen, wenn sie mit einer Identität oder Ressource verknüpft sind. AWS bewertet diese Richtlinien, wenn ein Principal eine Anfrage stellt. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Mit Hilfe von Richtlinien legen Administratoren fest, wer Zugriff auf was hat, indem sie definieren, welches Prinzipal welche Aktionen auf welchen Ressourcenund unter welchen Bedingungendurchführen darf.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator erstellt IAM-Richtlinien und fügt sie zu Rollen hinzu, die die Benutzer dann übernehmen können. IAM-Richtlinien definieren Berechtigungen unabhängig von der Methode, die zur Ausführung der Operation verwendet wird.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität (Benutzer, Gruppe oder Rolle) anfügen können. Diese Richtlinien steuern, welche Aktionen Identitäten für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können Inline-Richtlinien (direkt in eine einzelne Identität eingebettet) oder verwaltete Richtlinien (eigenständige Richtlinien, die mit mehreren Identitäten verbunden sind) sein. Informationen dazu, wie Sie zwischen verwalteten und Inline-Richtlinien wählen, finden Sie unter Choose between managed policies and inline policies im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele hierfür sind Vertrauensrichtlinien für IAM-Rollen 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. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben.

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

Weitere Richtlinientypen

AWS unterstützt zusätzliche Richtlinientypen, mit denen die maximalen Berechtigungen festgelegt werden können, die durch gängigere Richtlinientypen gewährt werden:

- Berechtigungsgrenzen – Eine Berechtigungsgrenze legt die maximalen Berechtigungen fest, die eine identitätsbasierte Richtlinie einer IAM-Entität erteilen kann. Weitere Informationen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im -IAM-Benutzerhandbuch.
- Richtlinien zur Dienstkontrolle (SCPs) — Geben Sie die maximalen Berechtigungen für eine Organisation oder Organisationseinheit in an AWS Organizations. Weitere Informationen finden Sie unter Service-Kontrollrichtlinien im AWS Organizations -Benutzerhandbuch.
- Richtlinien zur Ressourcenkontrolle (RCPs) — Legen Sie die maximal verfügbaren Berechtigungen für Ressourcen in Ihren Konten fest. Weitere Informationen finden Sie im AWS Organizations Benutzerhandbuch unter Richtlinien zur Ressourcenkontrolle (RCPs).
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die als Parameter übergeben werden, wenn Sie eine temporäre Sitzung für eine Rolle oder einen Verbundbenutzer erstellen. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn für eine Anfrage mehrere Arten von Richtlinien gelten, sind die daraus resultierenden Berechtigungen schwieriger zu verstehen. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie unter Bewertungslogik für Richtlinien im IAM-Benutzerhandbuch.

Wie AWS Ground Station funktioniert mit IAM

Bevor Sie IAM zur Verwaltung des Zugriffs auf verwenden, sollten Sie sich darüber informieren AWS Ground Station, mit welchen IAM-Funktionen Sie arbeiten können. AWS Ground Station

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

IAM-Feature	AWS Ground Station Unterstützung
Identitätsbasierte Richtlinien	Ja

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

Einen allgemeinen Überblick darüber, wie AWS Ground Station und andere AWS Dienste mit den meisten IAM-Funktionen funktionieren, finden Sie im IAM-Benutzerhandbuch unter AWS Dienste, die mit IAM funktionieren.

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 Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten 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. 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 AWS Ground Station identitätsbasierte Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS Ground Station

Ressourcenbasierte Richtlinien finden Sie 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. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Richtlinienaktionen für AWS Ground Station

Unterstützt Richtlinienaktionen: Ja

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

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Nehmen Sie Aktionen in eine Richtlinie auf, um Berechtigungen zur Ausführung des zugehörigen Vorgangs zu erteilen.

Eine Liste der AWS Ground Station Aktionen finden Sie unter Aktionen definiert von AWS Ground Station in der Serviceautorisierungsreferenz.

Bei Richtlinienaktionen wird vor der Aktion das folgende Präfix AWS Ground Station verwendet:

```
groundstation
```

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

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

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

Politische Ressourcen für AWS Ground Station

Unterstützt Richtlinienressourcen: Ja

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

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Als Best Practice geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

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

Eine Liste der AWS Ground Station Ressourcentypen und ihrer ARNs Eigenschaften finden Sie unter Resources defined by AWS Ground Station in der Service Authorization Reference. Informationen zu den Aktionen, mit denen Sie den ARN einzelner Ressourcen angeben können, finden Sie unter Von AWS Ground Station definierte Aktionen.

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

Bedingungsschlüssel für Richtlinien für AWS Ground Station

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

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

Das Element `Condition` gibt an, wann Anweisungen auf der Grundlage definierter Kriterien ausgeführt werden. 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. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Eine Liste der AWS Ground Station Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für AWS Ground Station in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Aktionen definiert von AWS Ground Station.

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

ACLs in AWS Ground Station

Unterstützt ACLs: Nein

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten 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, auch als Tags bezeichnet, definiert werden. Sie können Tags an IAM-Entitäten und AWS -Ressourcen anhängen und dann ABAC-Richtlinien entwerfen, die Operationen zulassen, wenn das Tag des Prinzipals mit dem Tag auf der Ressource übereinstimmt.

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 Bedingung `aws:TagKeys` 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 Definieren von Berechtigungen mit ABAC-Autorisierung 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

Temporäre Anmeldeinformationen ermöglichen kurzfristigen Zugriff auf AWS Ressourcen und werden automatisch erstellt, wenn Sie einen Verbund verwenden oder die Rollen wechseln. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Anmeldeinformationen in IAM und AWS-Services , die mit IAM funktionieren im IAM-Benutzerhandbuch.

Serviceübergreifende Prinzipalberechtigungen für AWS Ground Station

Unterstützt Forward Access Sessions (FAS): Ja

Forward Access Sessions (FAS) verwenden die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. Einzelheiten zu den Richtlinien für FAS-Anforderungen 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**
>
> Durch das Ändern der Berechtigungen für eine Servicerolle kann die AWS Ground Station Funktionalität beeinträchtigt werden. Bearbeiten Sie Servicerollen nur, AWS Ground Station wenn Sie dazu eine Anleitung erhalten.

Dienstbezogene Rollen für AWS Ground Station

Unterstützt serviceverknüpfte Rollen: Ja

Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte 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. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen.

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

Einzelheiten zu Aktionen und Ressourcentypen, die von definiert wurden AWS Ground Station, einschließlich des Formats von ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS Ground Station in der Referenz zur Serviceautorisierung.

Themen

- Best Practices für Richtlinien
- Verwenden der Konsole AWS Ground Station

- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

Best Practices 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. Beachten Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Richtlinien und Empfehlungen:

- Erste Schritte mit AWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um damit zu beginnen, Ihren Benutzern und Workloads Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien oder Von 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 Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. CloudFormation B. 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 mit IAM Access Analyzer im IAM-Benutzerhandbuch.

- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, 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 Sicherer API-Zugriff mit MFA im IAM-Benutzerhandbuch.

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

Verwenden der Konsole AWS Ground Station

Um auf die AWS Ground Station Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den AWS Ground Station Ressourcen in Ihrem aufzulisten und anzuzeigen AWS-Konto. 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.

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. 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 umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der AWS CLI AWS OR-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": "*"
        }
    ]
}
```

Problembehandlung bei AWS Ground Station Identität und Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit AWS Ground Station und IAM auftreten können.

Themen

- Ich bin nicht berechtigt, eine Aktion durchzuführen in AWS Ground Station
- Ich bin nicht berechtigt, iam auszuführen: PassRole
- Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine AWS Ground Station Ressourcen ermöglichen

Ich bin nicht berechtigt, eine Aktion durchzuführen in AWS Ground Station

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.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. 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 Stationübergeben zu können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. 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.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine AWS Ground Station Ressourcen ermöglichen

Sie können eine Rolle erstellen, mit der Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation auf Ihre Ressourcen zugreifen können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Für Dienste, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) unterstützen, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob diese Funktionen AWS Ground Station unterstützt werden, finden Sie unter. Wie AWS Ground Station funktioniert mit IAM
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs auf einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- 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 Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

AWS verwaltete Richtlinien für AWS Ground Station

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. AWS Verwaltete Richtlinien sind so konzipiert, dass sie Berechtigungen für viele gängige Anwendungsfälle bereitstellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie allen AWS Kunden zur Verfügung stehen. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

AWS verwaltete Richtlinie: AWSGround StationAgentInstancePolicy

Sie können die `AWSGroundStationAgentInstancePolicy`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt AWS Ground Station Agentenberechtigungen für Ihre Amazon EC2 EC2-Instance, die es der Instance ermöglichen, Daten bei Kontakten mit der Ground Station zu senden und zu empfangen. Alle Genehmigungen in dieser Richtlinie stammen vom Bodenstationsdienst.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `groundstation`— Ermöglicht Datenfluss-Endpunktinstanzen, den Ground Station Agent aufzurufen. APIs

Die neueste Version des JSON-Richtliniendokuments finden Sie AWSGroundStationAgentInstancePolicyim AWS Managed Policy Reference Guide.

AWS verwaltete Richtlinie: AWSService RoleForGroundStationDataflowEndpointGroupPolicy

Sie können keine Verbindungen AWSService RoleForGroundStationDataflowEndpointGroupPolicy zu Ihren IAM-Entitäten herstellen. Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, mit der Sie Aktionen AWS Ground Station in Ihrem Namen ausführen können. Weitere Informationen finden Sie unter Verwenden von dienstverknüpften Rollen.

Diese Richtlinie gewährt EC2-Berechtigungen, die es ermöglichen, öffentliche IPv4 Adressen AWS Ground Station zu finden.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `ec2:DescribeAddresses`— Ermöglicht AWS Ground Station die Auflistung aller Dateien, die mit in EIPs Ihrem Namen IPs verknüpft sind.
- `ec2:DescribeNetworkInterfaces`— Ermöglicht AWS Ground Station das Abrufen von Informationen zu den Netzwerkschnittstellen, die EC2-Instances in Ihrem Namen zugeordnet sind.

Die neueste Version des JSON-Richtliniendokuments finden Sie AWSServiceRoleForGroundStationDataflowEndpointGroupPolicyim AWS Managed Policy Reference Guide.

AWS Ground Station Aktualisierungen der AWS verwalteten Richtlinien

Hier finden Sie Informationen zu Aktualisierungen AWS verwalteter Richtlinien, die AWS Ground Station seit Beginn der Nachverfolgung dieser Änderungen durch diesen Dienst vorgenommen wurden. Abonnieren Sie den RSS-Feed auf der Seite AWS Ground Station Dokumentenverlauf, um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten.

Änderungen	Beschreibung	Datum
AWSGroundStationAgentInstancePolicy – Aktualisi	AWS Ground Station Es wurden neue Berechtig	13. November 2025

Änderungen	Beschreibung	Datum
erung auf eine bestehende Richtlinie	ungen hinzugefügt, mit denen Agenten die Antwort auf Aufgaben abrufen können, um URLs den Betrieb der Ground Station zu verbessern.	
AWSGroundStationAgentInstancePolicy – Neue Richtlinie	AWS Ground Station hat eine neue Richtlinie hinzugefügt, um den Dataflow-Endpunkt-Instance-Berechtigungen zur Verwendung des AWS Ground Station Agent bereitzustellen.	12. April 2023
AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy – Neue Richtlinie	AWS Ground Station hat eine neue Richtlinie hinzugefügt, die EC2-Berechtigungen gewährt, um öffentliche IPv4-Adressen, die AWS Ground Station mit EIPs verknüpft sind, und Netzwerkschnittstellen, die mit EC2-Instances verknüpft sind, zu finden.	02. November 2022
AWS Ground Station hat begonnen, Änderungen zu verfolgen	AWS Ground Station hat mit der Nachverfolgung von Änderungen für AWS verwaltete Richtlinien begonnen.	01. März 2021

Verwenden Sie serviceverknüpfte Rollen für die Ground Station

AWS Ground Station verwendet AWS Identity and Access Management (IAM) serviceverknüpfte Rollen. Eine serviceverknüpfte Rolle ist eine einzigartige Art von IAM-Rolle, die direkt mit der Ground Station verknüpft ist. Dienstbezogene Rollen sind von Ground Station vordefiniert und beinhalten alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

Eine serviceverknüpfte Rolle erleichtert die Einrichtung der Ground Station, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Ground Station definiert die Berechtigungen seiner dienstbezogenen Rollen, und sofern nicht anders definiert, kann nur Ground Station ihre Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Informationen zu anderen Diensten, die dienstverknüpfte Rollen unterstützen, finden Sie unter AWS Dienste, die mit IAM funktionieren. Suchen Sie in der Spalte Dienstverknüpfte Rollen nach den Diensten, für die Ja steht. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Dienstbezogene Rollenberechtigungen für Ground Station

Ground Station verwendet die serviceverknüpfte Rolle mit dem Namen AWSServiceRoleForGroundStationDataflowEndpointGroup— AWS GroundStation verwendet diese serviceverknüpfte Rolle, um EC2 aufzurufen, um öffentliche Adressen zu finden. IPv4

Die AWSService RoleForGroundStationDataflowEndpointGroup serviceverknüpfte Rolle vertraut darauf, dass die folgenden Services die Rolle übernehmen:

- `groundstation.amazonaws.com`

Die genannte Rollenberechtigungsrichtlinie AWSService RoleForGroundStationDataflowEndpointGroupPolicy ermöglicht es Ground Station, die folgenden Aktionen für die angegebenen Ressourcen durchzuführen:

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

  Aktion ermöglicht es Ground Station, alle IPs zugehörigen Objekte aufzulisten EIPs.
- Aktion: `ec2:DescribeNetworkInterfaces` für `all AWS resources (*)`

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

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

Eine serviceverknüpfte Rolle für Ground Station erstellen

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie eine DataflowEndpointGroup in der AWS CLI oder der AWS 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 erneut für Sie.

Sie können die IAM-Konsole auch 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 serviceverknüpfte Rolle mit dem Dienstnamen. `groundstation.amazonaws.com` Weitere Informationen finden Sie unter Erstellen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch. Wenn Sie diese serviceverknüpfte Rolle löschen, können Sie mit demselben Verfahren die Rolle erneut erstellen.

Bearbeiten einer serviceverknüpften Rolle für Ground Station

Ground Station erlaubt es Ihnen nicht, die AWSService RoleForGroundStationDataflowEndpointGroup serviceverknüpfte Rolle zu bearbeiten. 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 Rolle für Ground Station

Wenn Sie ein Feature oder einen Dienst, die bzw. der eine serviceverknüpften 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 dienstverknüpfte Rolle erst löschen, nachdem Sie zuerst die DataflowEndpointGroups mit dem Dienst verknüpfte Rolle gelöscht haben. Dies schützt Sie vor dem versehentlichen Widerruf von Berechtigungen für Ihre. DataflowEndpointGroups Wenn eine dienstverknüpfte Rolle mit mehreren verwendet wird, müssen Sie alle löschen DataflowEndpointGroups, die die dienstverknüpfte Rolle verwenden DataflowEndpointGroups , bevor Sie sie löschen können.

> **Note**
>
> Wenn der Bodenstationsdienst die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Um Bodenstationsressourcen zu löschen, die von der AWSService RoleForGroundStationDataflowEndpointGroup

- Löschen Sie DataflowEndpointGroups über die AWS-CLI oder die AWS-API.

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM-Konsole, die oder die AWS API AWS CLI, um die mit dem AWSService RoleForGroundStationDataflowEndpointGroup Service verknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Unterstützte Regionen für dienstbezogene Rollen an der Ground Station

Ground Station unterstützt die Verwendung von dienstbezogenen Rollen in allen Regionen, in denen der Service verfügbar ist. Weitere Informationen finden Sie in der Regionstabelle.

Fehlerbehebung

`NOT_AUTHORIZED_TO_CREATE_SLR`- Dies weist darauf hin, dass die Rolle in Ihrem Konto, die zum Aufrufen der CreateDataflowEndpointGroup API verwendet wird, nicht über die `iam:CreateServiceLinkedRole` entsprechende Berechtigung verfügt. Ein Administrator mit der entsprechenden `iam:CreateServiceLinkedRole` Berechtigung muss die serviceverknüpfte Rolle für Ihr Konto manuell erstellen.

Datenverschlüsselung im Ruhezustand für AWS Ground Station

AWS Ground Station bietet standardmäßig Verschlüsselung, um Ihre vertraulichen Daten 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. AWS

Eigene Schlüssel können nicht angezeigt, verwaltet oder verwendet oder deren Verwendung überwacht werden. 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 Schlüssel mit AWS eigenem Eigentum im Entwicklerhandbuch.AWS Key Management Service

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 erstellen, besitzen und verwalten, anstelle der vorhandenen Verschlüsselung. 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
  - Schlüssel für das Löschen von Schlüsseln planen

  Weitere Informationen finden Sie unter Vom Kunden verwalteter Schlüssel im AWS Key Management Service Entwicklerhandbuch.

In der folgenden Tabelle sind Ressourcen zusammengefasst, für die die Verwendung von vom Kunden verwalteten Schlüsseln AWS Ground Station unterstützt wird

Datentyp	AWS Verschlüsselung mit eigenem Schlüssel	Vom Kunden verwaltete Schlüsselverschlüsselung (optional)
Ephemeridendaten, die zur Berechnung der Flugbahn eines Satelliten verwendet werden	Aktiviert	Aktiviert
Azimut-Elevations-Ephemeriden, die zur Steuerung von Antennen verwendet werden	Aktiviert	Aktiviert

> **Note**
>
> AWS Ground Station aktiviert automatisch die Verschlüsselung im Ruhezustand AWS-eigene 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 Preisgestaltung.
> Weitere Informationen zu AWS KMS finden Sie im AWS Key Management Service Entwicklerhandbuch.

Spezifische Informationen zu den einzelnen Ressourcentypen finden Sie unter:

- Verschlüsselung im Ruhezustand für TLE- und OEM-Ephemeridendaten
- Verschlüsselung im Ruhezustand für Azimuthöhen-Ephemeriden

Erstellen eines kundenseitig verwalteten Schlüssels

Sie können einen symmetrischen, vom Kunden verwalteten Schlüssel erstellen, indem Sie den AWS-Managementkonsole, oder den AWS KMS APIs verwenden.

Einen symmetrischen kundenverwalteten Schlüssel erstellen

Folgen Sie den Schritten zur Erstellung eines symmetrischen, vom Kunden verwalteten Schlüssels im AWS Key Management Service Entwicklerhandbuch.

Überblick über die wichtigsten Richtlinien

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 kundenseitig 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 Entwicklerhandbuch.

Um Ihren vom Kunden verwalteten Schlüssel mit AWS Ground Station Ressourcen zu verwenden, müssen Sie die Schlüsselrichtlinie so konfigurieren, dass dem AWS Ground Station Dienst die entsprechenden Berechtigungen erteilt werden. Die spezifischen Berechtigungen und die Richtlinienkonfiguration hängen von der Art der Ressource ab, die Sie verschlüsseln:

- Informationen zu LTE- und OEM-Ephemeridendaten finden Sie unter Verschlüsselung im Ruhezustand für TLE- und OEM-Ephemeridendaten Spezifische wichtige Richtlinienanforderungen und Beispiele.
- Informationen zu Ephemeridendaten zur Azimuthöhe finden Sie unter Spezifische wichtige politische Anforderungen und Verschlüsselung im Ruhezustand für Azimuthöhen-Ephemeriden Beispiele.

> **Note**
>
> Die Konfiguration der wichtigsten Richtlinien unterscheidet sich je nach Ephemeriden-Typ. Für TLE- und OEM-Ephemeridendaten werden Zuschüsse für den Schlüsselzugriff verwendet, während bei Ephemeridendaten mit Azimut-Elevation direkte Schlüsselberechtigungen verwendet werden. Stellen Sie sicher, dass Sie Ihre Schlüsselrichtlinie entsprechend dem spezifischen Ressourcentyp konfigurieren, den Sie verschlüsseln.

Weitere Informationen zur Angabe von Berechtigungen in einer Richtlinie und zur Fehlerbehebung beim Schlüsselzugriff finden Sie im AWS Key Management Service Entwicklerhandbuch.

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 (TLE, OEM und Azimuthöhe)

Wenn Sie eine Ressource erstellen, können Sie den Datenschlüssel angeben, indem Sie ein kmsKeyArn

- kmsKeyArn- Eine Schlüssel-ID für einen vom AWS KMS Kunden verwalteten 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 zum Verschlüsseln von Daten einbeziehen, wird der Verschlüsselungskontext AWS KMS an die verschlüsselten Daten gebunden. Zur Entschlüsselung von Daten müssen Sie denselben Verschlüsselungskontext in der Anfrage übergeben.

AWS Ground Station verwendet je nach der zu verschlüsselnden Ressource einen anderen Verschlüsselungskontext und gibt für jede erstellte Schlüsselzuweisung einen bestimmten Verschlüsselungskontext an.

Einzelheiten zum ressourcenspezifischen Verschlüsselungskontext finden Sie unter:

- Verschlüsselung im Ruhezustand für TLE- und OEM-Ephemeridendaten
- Verschlüsselung im Ruhezustand für Azimuthöhen-Ephemeriden

Verschlüsselung im Ruhezustand für TLE- und OEM-Ephemeridendaten

Wichtige politische Anforderungen für TLE- und OEM-Ephemeriden

Um einen vom Kunden verwalteten Schlüssel mit Ephemeridendaten zu verwenden, muss Ihre Schlüsselrichtlinie dem Service die folgenden Berechtigungen gewähren: AWS Ground Station

- `kms:CreateGrant`- Erzeugt eine Zugriffsgewährung für einen vom Kunden verwalteten Schlüssel. Gewährt AWS Ground Station Zugriff auf den vom Kunden verwalteten Schlüssel zum Lesen und Speichern verschlüsselter Daten zur Ausführung von Zugriffsberechtigungen.
- `kms:DescribeKey`- Stellt dem Kunden die vom Kunden verwalteten Schlüssel zur Verfügung, damit AWS Ground Station der Schlüssel validiert werden kann, bevor versucht wird, den bereitgestellten Schlüssel zu verwenden.

Weitere Informationen zur Verwendung von Zuschüssen finden Sie im AWS Key Management Service Entwicklerhandbuch.

IAM-Benutzerberechtigungen für die Erstellung von Ephemeriden mit vom Kunden verwalteten Schlüsseln

Wenn ein vom Kunden verwalteter Schlüssel für kryptografische Operationen AWS Ground Station verwendet wird, handelt er im Namen des Benutzers, der die Ephemeridenressource erstellt.

Um eine Ephemeridenressource mithilfe eines vom Kunden verwalteten Schlüssels zu erstellen, muss ein Benutzer über die erforderlichen Berechtigungen verfügen, um die folgenden Operationen mit dem vom Kunden verwalteten Schlüssel aufzurufen:

- `kms:CreateGrant`- Ermöglicht dem Benutzer, im Namen von Grants für den vom Kunden verwalteten Schlüssel zu erstellen. AWS Ground Station
- `kms:DescribeKey`- Ermöglicht dem Benutzer, die vom Kunden verwalteten Schlüsseldetails einzusehen, um den Schlüssel zu validieren.

Sie können diese erforderlichen Berechtigungen in einer Schlüsselrichtlinie oder in einer IAM-Richtlinie angeben, wenn die Schlüsselrichtlinie dies zulässt. Diese Berechtigungen stellen sicher, dass Benutzer autorisieren können AWS Ground Station , den vom Kunden verwalteten Schlüssel für Verschlüsselungsvorgänge in ihrem Namen zu verwenden.

Wie werden AWS Ground Station Zuschüsse AWS KMS für Ephemeriden verwendet

AWS Ground Station erfordert einen Schlüsselzuschuss, 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 in Ihrem Namen eine Schlüsselzuweisung, indem es

eine CreateGrantAnfrage an sendet. AWS KMS Grants in AWS KMS werden verwendet, um AWS Ground Station Zugriff auf einen AWS KMS Schlüssel in Ihrem Konto zu gewähren.

Auf diese Weise können AWS Ground Station Sie Folgendes tun:

- GenerateDataKey aufrufen, um einen verschlüsselten Datenschlüssel zu generieren und zu speichern, da der Datenschlüssel nicht sofort zum Verschlüsseln verwendet wird.
- Rufen Sie Decrypt auf, um den gespeicherten verschlüsselten Datenschlüssel für den Zugriff auf verschlüsselte Daten zu verwenden.
- Rufen Sie Encrypt auf, um den Datenschlüssel zum Verschlüsseln von Daten zu verwenden.
- Einen Prinzipal für die Außerbetriebnahme einrichten, damit der Service in den Status RetireGrant wechseln kann.

Sie können den Zugriff auf den Zuschuss jederzeit widerrufen. 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.

Ephemeriden-Verschlüsselungskontext

Wichtige Zuschüsse für die Verschlüsselung von Ephemeridenressourcen sind an einen bestimmten Satelliten-ARN gebunden.

```
"encryptionContext": {
    "aws:groundstation:arn":
 "arn:aws:groundstation::111122223333:satellite/00a770b0-082d-45a4-80ed-SAMPLE",
    "aws:s3:arn":
 "arn:aws:s3:::customerephemerisbucket/0034abcd-12ab-34cd-56ef-123456SAMPLE"
}
```

> **Note**
>
> Schlüsselzuschüsse 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 kundenseitig 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.

Das folgende Beispiel zeigt eine wichtige Richtlinie für Ephemeridendaten, die an einen Satelliten gebunden sind:

JSON

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

```
            "Resource": "*"
        },
        {
            "Sid": "Allow AWS Ground Station to Create Grant on key",
            "Effect": "Allow",
            "Principal": {
                "Service": "groundstation.us-east-1.amazonaws.com"
            },
            "Action": "kms:CreateGrant",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:EncryptionContext:aws:groundstation:arn":
 "arn:aws:groundstation::123456789012:satellite/satellite-id"
                }
            }
        }
    ]
}
```

Überwachen Sie Ihre Verschlüsselungsschlüssel auf Ephemeriden

Wenn Sie einen vom AWS Key Management Service Kunden verwalteten Schlüssel mit Ihren Ephemeridenressourcen verwenden, können Sie AWS CloudTrailoder CloudWatch Amazon-Protokolle verwenden, um Anfragen zu verfolgen, die AWS Ground Station an gesendet werden. AWS KMS Die folgenden Beispiele sind CloudTrail Ereignisse für CreateGrant, GenerateDataKey, Decrypt und zur Überwachung von AWS KMS Vorgängen, die aufgerufen werden, DescribeKey AWS Ground Station um auf Daten zuzugreifen, die mit Ihrem vom Kunden verwalteten Schlüssel verschlüsselt wurden.

CreateGrant

Wenn Sie einen vom AWS KMS Kunden verwalteten Schlüssel verwenden, um Ihre Ephemeridenressourcen zu verschlüsseln, AWS Ground Station sendet er in Ihrem Namen eine CreateGrantAnfrage, um auf den AWS KMS Schlüssel in Ihrem Konto zuzugreifen. AWS Der gewährte Zuschuss AWS Ground Station ist spezifisch für die Ressource, die dem vom AWS KMS Kunden verwalteten Schlüssel zugeordnet ist. AWS Ground Station Verwendet außerdem den RetireGrantVorgang, um einen Zuschuss zu entfernen, wenn Sie eine Ressource löschen.

Das folgende Beispielereignis zeichnet den CreateGrantVorgang für eine Ephemeride auf:

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "ASIAIOSFODNN7EXAMPLE",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/SampleUser01",
        "accountId": "111122223333",
        "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "ASIAIOSFODNN7EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-02-22T22:22:22Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2022-02-22T22:22:22Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "ExampleDesktop/1.0 (V1; OS)",
    "requestParameters": {
        "operations": [
            "GenerateDataKeyWithoutPlaintext",
            "Decrypt",
            "Encrypt"
        ],
        "constraints": {
            "encryptionContextSubset": {
                "aws:groundstation:arn":
 "arn:aws:groundstation::111122223333:satellite/00a770b0-082d-45a4-80ed-SAMPLE"
            }
        },
        "granteePrincipal": "groundstation.us-west-2.amazonaws.com",
```

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

DescribeKey

Wenn Sie einen vom AWS KMS Kunden verwalteten Schlüssel zur Verschlüsselung Ihrer Ephemeridenressourcen verwenden, AWS Ground Station sendet er in Ihrem Namen eine DescribeKeyAnfrage, 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": "ASIAIOSFODNN7EXAMPLE",
        "arn": "arn:aws:sts::111122223333:assumed-role/User/Role",
        "accountId": "111122223333",
        "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
        "sessionContext": {
```

```
            "sessionIssuer": {
                "type": "Role",
                "principalId": "ASIAIOSFODNN7EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Role",
                "accountId": "111122223333",
                "userName": "User"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-02-22T22:22:22Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2022-02-22T22:22:22Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DescribeKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

GenerateDataKey

Wenn Sie einen vom AWS KMS Kunden verwalteten Schlüssel zur Verschlüsselung Ihrer Ephemeridenressourcen verwenden, AWS Ground Station sendet er eine GenerateDataKeyAnfrage an, um einen Datenschlüssel zu generieren, mit dem Sie Ihre Daten verschlüsseln können.

Das folgende Beispielereignis zeichnet den GenerateDataKeyVorgang für eine Ephemeride 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

Wenn Sie einen vom AWS KMS Kunden verwalteten Schlüssel zum Verschlüsseln Ihrer Ephemeridenressourcen verwenden, AWS Ground Station verwendet es den Vorgang Decrypt, um die bereitgestellte Ephemeride zu entschlüsseln, sofern sie bereits mit demselben vom Kunden verwalteten Schlüssel verschlüsselt wurde. 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 Decrypt-Vorgang für eine Ephemeride 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"
}
```

Verschlüsselung im Ruhezustand für Azimuthöhen-Ephemeriden

Wichtige politische Anforderungen für Azimut-Ephemeriden

Um einen vom Kunden verwalteten Schlüssel mit Azimut-Elevation-Ephemeridendaten zu verwenden, muss Ihre Schlüsselrichtlinie dem Service die folgenden Berechtigungen gewähren. AWS Ground Station Im Gegensatz zu TLE- und OEM-Ephemeridendaten, für die Zuschüsse verwendet werden, verwendet Azimut-Elevation-Ephemeride direkte Schlüsselrichtlinienberechtigungen für Verschlüsselungsvorgänge. Dies ist eine einfachere Methode zur Verwaltung der Berechtigungen und zur Verwendung Ihrer Schlüssel.

- `kms:GenerateDataKey`- Generiert Datenschlüssel zur Verschlüsselung Ihrer Azimuthöhen-Ephemeridendaten.
- `kms:Decrypt`- Entschlüsselt die verschlüsselten Datenschlüssel beim Zugriff auf Ihre Azimuthöhen-Ephemeridendaten.

Beispiel für eine Schlüsselrichtlinie, die AWS Ground Station Zugriff auf einen vom Kunden verwalteten Schlüssel gewährt

> **Note**
>
> Bei Azimut-Elevation-Ephemeriden müssen Sie diese Berechtigungen direkt in der Schlüsselrichtlinie konfigurieren. Diese Berechtigungen müssen dem Regional AWS Ground

Station Service Principal (z. B.`groundstation.`*`region`*`.amazonaws.com`) in Ihren wichtigsten Richtlinienerklärungen erteilt werden. Ohne diese Angaben in der Hauptrichtlinie AWS Ground Station kann Ihre benutzerdefinierte Azimut-Ephemeride weder gespeichert noch darauf zugegriffen werden.

JSON

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

IAM-Benutzerberechtigungen für die Erstellung von Azimut-Elevation-Ephemeriden mit vom Kunden verwalteten Schlüsseln

Wenn ein vom Kunden verwalteter Schlüssel für kryptografische Operationen AWS Ground Station verwendet wird, handelt er im Namen des Benutzers, der die Azimut-Elevation-Ephemeridenressource erstellt.

Um mithilfe eines vom Kunden verwalteten Schlüssels eine Azimut-Elevation-Ephemeridenressource zu erstellen, muss ein Benutzer berechtigt sein, die folgenden Operationen mit dem vom Kunden verwalteten Schlüssel aufzurufen:

- `kms:GenerateDataKey`— Ermöglicht dem Benutzer die Generierung von Datenschlüsseln zur Verschlüsselung der Azimuthöhen-Ephemeridendaten.
- `kms:Decrypt`- Ermöglicht dem Benutzer, Datenschlüssel zu entschlüsseln, wenn er auf die Azimuthöhen-Ephemeridendaten zugreift.
- `kms:DescribeKey`- Ermöglicht dem Benutzer, die vom Kunden verwalteten Schlüsseldetails einzusehen, um den Schlüssel zu validieren.

Sie können diese erforderlichen Berechtigungen in einer Schlüsselrichtlinie oder in einer IAM-Richtlinie angeben, wenn die Schlüsselrichtlinie dies zulässt. Diese Berechtigungen stellen sicher, dass Benutzer autorisieren können AWS Ground Station , den vom Kunden verwalteten Schlüssel für Verschlüsselungsvorgänge in ihrem Namen zu verwenden.

Wie AWS Ground Station werden wichtige Richtlinien für Azimut-Ephemeriden verwendet

Wenn Sie Azimut-Elevation-Ephemeridendaten mit einem vom Kunden verwalteten Schlüssel bereitstellen, AWS Ground Station verwendet Schlüsselrichtlinien für den Zugriff auf Ihren Verschlüsselungsschlüssel. Die Berechtigungen werden direkt AWS Ground Station durch wichtige Grundsatzerklärungen und nicht durch Zuschüsse wie bei TLE- oder OEM-Ephemeridendaten erteilt.

Wenn Sie den Zugriff auf den vom Kunden verwalteten Schlüssel entfernen AWS Ground Station, können Sie auf AWS Ground Station keine der mit diesem Schlüssel verschlüsselten Daten zugreifen, was sich auf Vorgänge auswirkt, die von diesen Daten abhängig sind. Wenn Sie beispielsweise wichtige Richtlinienberechtigungen für Azimuthöhen-Ephemeriden entfernen, die derzeit für einen Kontakt verwendet AWS Ground Station werden, können Sie die bereitgestellten Azimut-Höhendaten nicht für die Steuerung der Antenne während des Kontakts verwenden. Dadurch endet der Kontakt im Status FEHLGESCHLAGEN.

Kontext für die Verschlüsselung von Ephemeriden mit Azimut und Elevation

Wenn der Dienst Ihren AWS KMS Schlüssel zur Verschlüsselung von Azimut-Elevation-Ephemeridendaten AWS Ground Station verwendet, gibt der Dienst einen Verschlüsselungskontext an. Der Verschlüsselungskontext besteht aus zusätzlichen authentifizierten Daten (AAD), die zur Sicherstellung der Datenintegrität verwendet werden. AWS KMS Wenn für eine Verschlüsselungsoperation ein Verschlüsselungskontext angegeben wird, muss der Service denselben Verschlüsselungskontext auch für die Entschlüsselungsoperation angeben. Andernfalls schlägt die Entschlüsselung fehl. Der Verschlüsselungskontext wird auch in Ihre CloudTrail Protokolle geschrieben, damit Sie nachvollziehen können, warum ein bestimmter AWS KMS Schlüssel verwendet wurde. Ihre CloudTrail Protokolle können viele Einträge enthalten, die die Verwendung eines AWS KMS Schlüssels beschreiben, aber der Verschlüsselungskontext in jedem Protokolleintrag kann Ihnen helfen, den Grund für diese bestimmte Verwendung zu ermitteln.

AWS Ground Station gibt den folgenden Verschlüsselungskontext an, wenn kryptografische Operationen mit Ihrem vom Kunden verwalteten Schlüssel auf einer Azimut-Ephemeride ausgeführt werden:

```
{
    "encryptionContext": {
        "aws:groundstation:ground-station-id": "Ohio 1",
        "aws:groundstation:arn": "arn:aws:groundstation:us-
east-2:111122223333:ephemeris/00a770b0-082d-45a4-80ed-SAMPLE",
        "aws:s3:arn": "arn:aws:s3:::customerephemerisbucket/00a770b0-082d-45a4-80ed-
SAMPLE/raw"
    }
}
```

Der Verschlüsselungskontext umfasst:

`aws:groundstation:ground-station-id`

Der Name der Bodenstation, die mit der Azimuthöhen-Ephemeride verknüpft ist.

aws:groundstation:arn

Der ARN der Ephemeridenressource.

aws:s3:arn

Der ARN der in Amazon S3 gespeicherten Ephemeride.

Verwendung des Verschlüsselungskontextes zur Steuerung des Zugriffs auf den kundenseitig verwalteten Schlüssel

Sie können IAM-Zustandsanweisungen verwenden, um den AWS Ground Station Zugriff auf Ihren vom Kunden verwalteten Schlüssel zu kontrollieren. Das Hinzufügen einer Zustandserklärung zu den `kms:Decrypt` Aktionen `kms:GenerateDataKey` und schränkt ein, für welche Bodenstationen a verwendet werden AWS KMS können.

Im Folgenden finden Sie Beispiele für wichtige Richtlinienerklärungen, mit denen Sie einer bestimmten Bodenstation AWS Ground Station Zugriff auf Ihren vom Kunden verwalteten Schlüssel in einer bestimmten Region gewähren können. Die Bedingung in dieser Richtlinienerklärung erfordert, dass alle den Zugriff auf den Schlüssel verschlüsseln und entschlüsseln, der einen Verschlüsselungskontext angibt, der der Bedingung in der Schlüsselrichtlinie entspricht.

Beispiel für eine Schlüsselrichtlinie, die AWS Ground Station Zugriff auf einen vom Kunden verwalteten Schlüssel für eine bestimmte Bodenstation gewährt

JSON

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

```
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:EncryptionContext:aws:groundstation:ground-station-id":
 "specific-ground-station-name"
                }
            }
        }
    ]
}
```

Beispiel für eine Schlüsselrichtlinie, die AWS Ground Station den Zugriff auf einen vom Kunden verwalteten Schlüssel für mehrere Bodenstationen gewährt

JSON

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

```
                    "kms:EncryptionContext:aws:groundstation:ground-station-id":
 [
                        "specific-ground-station-name-1",
                        "specific-ground-station-name-2"
                    ]
                }
            }
        }
    ]
}
```

Überwachen Sie Ihre Verschlüsselungsschlüssel auf Azimut-Ephemeriden

Wenn Sie einen vom AWS KMS Kunden verwalteten Schlüssel mit Ihren Azimut-Elevation-Ephemeriden-Ressourcen verwenden, können Sie OR-Protokolle verwenden CloudTrail, um Anfragen nachzuverfolgen, die an gesendet werden. CloudWatch AWS Ground Station AWS KMS Bei den folgenden Beispielen handelt es sich um CloudTrail Ereignisse für GenerateDataKeyund Decrypt zur Überwachung von AWS KMS Vorgängen, die aufgerufen werden, um auf Daten zuzugreifen AWS Ground Station , die mit Ihrem vom Kunden verwalteten Schlüssel verschlüsselt wurden.

GenerateDataKey

Wenn Sie einen vom AWS KMS Kunden verwalteten Schlüssel verwenden, um Ihre Azimut-Ephemeridenressourcen zu verschlüsseln, AWS Ground Station sendet eine GenerateDataKeyAnfrage an, um einen Datenschlüssel zu AWS KMS generieren, mit dem Sie Ihre Daten verschlüsseln können.

Das folgende Beispielereignis zeichnet den Vorgang für Azimut-Elevation-Ephemeriden auf GenerateDataKey:

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

```
                "type": "Role",
                "principalId": "ASIAIOSFODNN7EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "attributes": {
                "creationDate": "2025-08-25T14:45:48Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2025-08-25T14:52:02Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keySpec": "AES_256",
        "encryptionContext": {
            "aws:groundstation:arn": "arn:aws:groundstation:us-
west-2:111122223333:ephemeris/bb650670-7a4b-4152-bd60-SAMPLE",
            "aws:groundstation:ground-station-id": "Ohio 1",
            "aws:s3:arn": "arn:aws:s3:::customerephemerisbucket/bb650670-7a4b-4152-
bd60-SAMPLE/raw"
        },
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "responseElements": null,
    "requestID": "ef6f9a8f-8ef6-46a1-bdcb-123456SAMPLE",
    "eventID": "952842d4-1389-3232-b885-123456SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
```

```
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "sharedEventID": "8424f6b6-2280-4d1d-b9fd-0348b1546cba",
    "eventCategory": "Management"
}
```

Decrypt

Wenn Sie einen vom AWS KMS Kunden verwalteten Schlüssel verwenden, um Ihre Azimut-Elevation-Ephemeriden-Ressourcen zu verschlüsseln, AWS Ground Station verwendet die Operation Decrypt, um die bereitgestellten Azimut-Elevation-Ephemeridendaten zu entschlüsseln, sofern sie bereits mit demselben vom Kunden verwalteten Schlüssel verschlüsselt sind.

Das folgende Beispielereignis zeichnet den Decrypt-Vorgang für Azimut-Elevation-Ephemeriden auf:

```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "ASIAIOSFODNN7EXAMPLE",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/SampleUser01",
        "accountId": "111122223333",
        "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "ASIAIOSFODNN7EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            }
        },
        "attributes": {
            "creationDate": "2025-08-25T14:45:48Z",
            "mfaAuthenticated": "false"
        }
    },
    "invokedBy": "AWS Internal",
    "eventTime": "2025-08-25T14:54:01Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-west-2",
```

```
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "encryptionContext": {
            "aws:groundstation:arn": "arn:aws:groundstation:us-
west-2:111122223333:ephemeris/bb650670-7a4b-4152-bd60-SAMPLE",
            "aws:groundstation:ground-station-id": "Ohio 1",
            "aws:s3:arn": "arn:aws:s3:::customerephemerisbucket/bb650670-7a4b-4152-
bd60-SAMPLE/raw"
        },
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
    },
    "responseElements": null,
    "requestID": "a2f46066-49fb-461a-93cb-123456SAMPLE",
    "eventID": "e997b426-e3ad-31c7-a308-123456SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "sharedEventID": "477b568e-7f56-4f04-905c-623ff146f30d",
    "eventCategory": "Management"
}
```


Datenverschlüsselung während der Übertragung für AWS Ground Station

AWS Ground Station bietet standardmäßig Verschlüsselung, um Ihre vertraulichen Daten während der Übertragung zu schützen. Daten können je nach Konfiguration des Missionsprofils auf zwei Arten zwischen AWS Ground Station Antennenstandorten und Ihren Amazon EC2 EC2-Instances gestreamt werden.

- AWS Ground Station Agent

- Datenfluss-Endpunkt

Jede Methode zum Streamen von Daten behandelt die Verschlüsselung von Daten während der Übertragung unterschiedlich. In den folgenden Abschnitten werden beide Methoden beschrieben.

AWS Ground Station Agenten-Streams

AWS Ground Station Der Agent verschlüsselt seine Streams mit vom Kunden verwalteten AWS KMS Schlüsseln. Der AWS Ground Station Agent, der auf Ihrer Amazon EC2 EC2-Instance ausgeführt wird, entschlüsselt den Stream automatisch, um entschlüsselte Daten bereitzustellen.

Der AWS KMS Schlüssel, der für die Verschlüsselung eines Streams verwendet wird, wird bei der Erstellung eines `MissionProfile` im Parameter angegeben. streamsKmsKey Alle Berechtigungen, die AWS Ground Station Zugriff auf die Schlüssel gewähren, werden über die beigefügte AWS KMS Schlüsselrichtlinie verwaltet. `streamsKmsKey`

Datenfluss-Endpunktstreams

Dataflow-Endpoint-Streams werden mit Datagram Transport Layer Security (DTLS) verschlüsselt. Dies erfolgt mithilfe selbstsignierter Zertifikate und erfordert keine zusätzliche Konfiguration.

Beispielkonfigurationen von Missionsprofilen

Die bereitgestellten Beispiele zeigen, wie man anhand eines öffentlich-rechtlichen Rundfunksatelliten ein Missionsprofil erstellt, das ihn unterstützt. Die daraus resultierenden Vorlagen sollen Ihnen dabei helfen, einen öffentlich-rechtlichen Satellitenkontakt herzustellen und Entscheidungen über Ihre Satelliten zu treffen.

Themen

- JPSS-1 — Öffentlicher Rundfunksatellit (PBS) — Evaluierung
- Öffentlicher Rundfunksatellit, der Amazon S3 S3-Datenlieferung nutzt
- Öffentlicher Rundfunksatellit, der einen Datenflussendpunkt nutzt (Schmalband)
- Öffentlicher Rundfunksatellit, der einen Datenflussendpunkt verwendet (demoduliert und dekodiert)
- Öffentlicher Rundfunksatellit mit AWS Ground Station Agent (Breitband)

JPSS-1 — Öffentlicher Rundfunksatellit (PBS) — Evaluierung

Dieser Beispielabschnitt entspricht dem. Überblick über den Onboarding-Prozess für Kunden Es enthält eine kurze Kompatibilitätsanalyse mit den folgenden spezifischen Beispielen AWS Ground Station und schafft die Voraussetzungen für diese.

Wie im Öffentliche Rundfunksatelliten Abschnitt erwähnt, können Sie ausgewählte Satelliten oder Kommunikationspfade eines Satelliten verwenden, die öffentlich verfügbar sind. In diesem Abschnitt beschreiben wir JPSS-1 in den AWS Ground Station folgenden Begriffen. Als Referenz verwenden wir das Joint Polar Satellite System 1 (JPSS-1) Spacecraft High Rate Data (HRD) to Direct Broadcast Stations (DBS) Radio Frequency (RF) Interface Control Document (ICD), um das Beispiel zu vervollständigen. Bemerkenswert ist auch, dass JPSS-1 mit der NORAD-ID 43013 verknüpft ist.

Der JPSS-1-Satellit bietet einen Uplink- und drei direkte Downlink-Kommunikationspfade, wie in Abbildung 1-1 des ICD dargestellt. Von diesen vier Kommunikationspfaden steht nur der einzige Downlink-Kommunikationspfad für High Rate Data (HRD) für den öffentlichen Gebrauch zur Verfügung. Auf dieser Grundlage werden Sie feststellen, dass diesem Pfad auch viel spezifischere Daten zugeordnet sein werden. Die vier Pfade lauten wie folgt:

- Befehlspfad (Uplink) mit einer MHz Mittenfrequenz von 2067,27 und einer Datenrate von 2-128 kbit/s. Dieser Pfad ist nicht öffentlich zugänglich.

- Telemetriepfad (Downlink) mit einer MHz Mittenfrequenz von 2247,5 und einer Datenrate von 1-524 kbit/s. Dieser Pfad ist nicht öffentlich zugänglich.
- SMD-Pfad (Downlink) mit einer GHz Mittenfrequenz von 26,7034 und einer Datenrate von 150-300 Mbit/s. Dieser Pfad ist nicht öffentlich zugänglich.
- Der RF für den HRD-Pfad (Downlink) mit einer MHz Mittenfrequenz von 7812 und einer Datenrate von 15 Mbit/s. Es hat eine MHz Bandbreite von 30 und ist. right-hand-circular-polarized Wenn Sie JPSS-1 mit einbinden AWS Ground Station, ist dies der Kommunikationspfad, auf den Sie Zugriff erhalten. Dieser Kommunikationspfad enthält Daten zur Instrumentenwissenschaft, zur Instrumententechnik, zur Instrumententelemetrie und zur Verwaltung von Raumfahrzeugen in Echtzeit.

Beim Vergleich der potenziellen Datenpfade stellen wir fest, dass die Befehlspfade (Uplink), Telemetrie- (Downlink) und HRD-Pfade (Downlink) die Frequenz-, Bandbreite- und Mehrkanal-Funktionen zur gleichzeitigen Nutzung von erfüllen. AWS Ground Station Der SMD-Pfad ist nicht kompatibel, da die Mittenfrequenz außerhalb des Bereichs der vorhandenen Empfänger liegt. Weitere Informationen zu den unterstützten Funktionen finden Sie unterAWS Ground Station Funktionen der Website.

> **Note**
>
> Da der SMD-Pfad damit nicht kompatibel AWS Ground Station ist, wird er in den Beispielkonfigurationen nicht dargestellt.

> **Note**
>
> Da der Befehlspfad (Uplink) und der Telemetriepfad (Downlink) nicht im ICD definiert sind und auch nicht öffentlich zugänglich sind, handelt es sich bei den angegebenen Werten um fiktive Werte.

Öffentlicher Rundfunksatellit, der Amazon S3 S3-Datenlieferung nutzt

Dieses Beispiel baut auf der Analyse auf, die im JPSS-1 — Öffentlicher Rundfunksatellit (PBS) — Evaluierung Abschnitt des Benutzerhandbuchs durchgeführt wurde.

In diesem Beispiel müssen Sie von einem Szenario ausgehen: Sie möchten den HRD-Kommunikationspfad als digitale Zwischenfrequenz erfassen und für die future Stapelverarbeitung speichern. Auf diese Weise werden die Rohdaten der Hochfrequenz- (RF) -Inphase-Quadratur- (I/Q) -Proben nach der Digitalisierung eingespart. Sobald sich die Daten in Ihrem Amazon S3 S3-Bucket befinden, können Sie die Daten mit jeder beliebigen Software demodulieren und dekodieren. Ein detailliertes Beispiel für die Verarbeitung finden Sie im MathWorks Tutorial. Nachdem Sie dieses Beispiel verwendet haben, können Sie erwägen, Amazon EC2 Spot-Pricing-Komponenten hinzuzufügen, um die Daten zu verarbeiten und Ihre Gesamtverarbeitungskosten zu senken.

Kommunikationswege

Dieser Abschnitt beschreibt Planen Sie Ihre Datenfluss-Kommunikationspfade die ersten Schritte.

Alle folgenden Vorlagenausschnitte gehören zum Abschnitt Ressourcen der CloudFormation Vorlage.

```
Resources:
  # Resources that you would like to create should be placed within the Resources
 section.
```

> **Note**
>
> Weitere Informationen zum Inhalt einer CloudFormation Vorlage finden Sie unter Abschnitte mit Vorlagen.

Angesichts unseres Szenarios, einen einzigen Kommunikationspfad für Amazon S3 bereitzustellen, wissen Sie, dass Sie einen einzigen asynchronen Lieferpfad haben werden. Gemäß Asynchrone Datenübermittlung diesem Abschnitt müssen Sie einen Amazon S3 S3-Bucket definieren.

```
  # The S3 bucket where AWS Ground Station will deliver the downlinked data.
  GroundStationS3DataDeliveryBucket:
    Type: AWS::S3::Bucket
    DeletionPolicy: Retain
    UpdateReplacePolicy: Retain
    Properties:
      # Results in a bucket name formatted like: aws-groundstation-data-{account id}-
{region}-{random 8 character string}
```

```
      BucketName: !Join ["-", ["aws-groundstation-data", !Ref AWS::AccountId, !Ref
 AWS::Region, !Select [0, !Split ["-", !Select [2, !Split ["/", !Ref AWS::StackId]]]]]]
```

Darüber hinaus müssen Sie die entsprechenden Rollen und Richtlinien erstellen, um den Bucket verwenden AWS Ground Station zu können.

```
  # The IAM role that AWS Ground Station will assume to have permission find and write
  # data to your S3 bucket.
  GroundStationS3DataDeliveryRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Statement:
          - Action:
              - 'sts:AssumeRole'
            Effect: Allow
            Principal:
              Service:
                - groundstation.amazonaws.com
            Condition:
              StringEquals:
                "aws:SourceAccount": !Ref AWS::AccountId
              ArnLike:
                "aws:SourceArn": !Sub "arn:aws:groundstation:${AWS::Region}:
${AWS::AccountId}:config/s3-recording/*"

  # The S3 bucket policy that defines what actions AWS Ground Station can perform on
 your S3 bucket.
  GroundStationS3DataDeliveryBucketPolicy:
    Type: AWS::IAM::Policy
    Properties:
      PolicyDocument:
        Statement:
          - Action:
              - 's3:GetBucketLocation'
            Effect: Allow
            Resource:
              - !GetAtt GroundStationS3DataDeliveryBucket.Arn
          - Action:
              - 's3:PutObject'
            Effect: Allow
```

```
            Resource:
              - !Join [ "/", [ !GetAtt GroundStationS3DataDeliveryBucket.Arn, "*" ] ]
      PolicyName: GroundStationS3DataDeliveryPolicy
      Roles:
        - !Ref GroundStationS3DataDeliveryRole
```

AWS Ground Station Konfigurationen

Dieser Abschnitt beschreibt Konfigurationen erstellen die ersten Schritte.

Sie benötigen eine Tracking-Konfiguration, um Ihre Präferenz für die Verwendung von Autotrack festzulegen. Die Auswahl von PREFERRED als Autotrack kann die Signalqualität verbessern, ist aber aufgrund der ausreichenden JPSS-1-Ephemeridenqualität nicht erforderlich, um die Signalqualität zu gewährleisten.

```
 TrackingConfig:
   Type: AWS::GroundStation::Config
   Properties:
     Name: "JPSS Tracking Config"
     ConfigData:
       TrackingConfig:
         Autotrack: "PREFERRED"
```

Basierend auf dem Kommunikationspfad müssen Sie eine Antennen-Downlink-Konfiguration definieren, die den Satellitenanteil darstellt, sowie eine S3-Aufzeichnung, die sich auf den Amazon S3-Bucket bezieht, den Sie gerade erstellt haben.

```
 # The AWS Ground Station Antenna Downlink Config that defines the frequency spectrum
used to
 # downlink data from your satellite.
 JpssDownlinkDigIfAntennaConfig:
   Type: AWS::GroundStation::Config
   Properties:
     Name: "JPSS Downlink DigIF Antenna Config"
     ConfigData:
       AntennaDownlinkConfig:
         SpectrumConfig:
```

```
            Bandwidth:
              Units: "MHz"
              Value: 30
            CenterFrequency:
              Units: "MHz"
              Value: 7812
            Polarization: "RIGHT_HAND"

 # The AWS Ground Station S3 Recording Config that defines the S3 bucket and IAM role
to use
 # when AWS Ground Station delivers the downlink data.
 S3RecordingConfig:
   Type: AWS::GroundStation::Config
   DependsOn: GroundStationS3DataDeliveryBucketPolicy
   Properties:
     Name: "JPSS S3 Recording Config"
     ConfigData:
       S3RecordingConfig:
         BucketArn: !GetAtt GroundStationS3DataDeliveryBucket.Arn
         RoleArn: !GetAtt GroundStationS3DataDeliveryRole.Arn
```

AWS Ground Station Missionsprofil

Dieser Abschnitt beschreibt Missionsprofil erstellen die ersten Schritte.

Da Sie nun über die zugehörigen Konfigurationen verfügen, können Sie sie verwenden, um den Datenfluss zu erstellen. Für die übrigen Parameter verwenden Sie die Standardwerte.

```
 # The AWS Ground Station Mission Profile that groups the above configurations to
define how to downlink data.
 JpssAsynchMissionProfile:
   Type: AWS::GroundStation::MissionProfile
   Properties:
     Name: "43013 JPSS Asynchronous Data"
     MinimumViableContactDurationSeconds: 180
     TrackingConfigArn: !Ref TrackingConfig
     DataflowEdges:
       - Source: !Ref JpssDownlinkDigIfAntennaConfig
         Destination: !Ref S3RecordingConfig
```

Es zusammensetzen

Mit den oben genannten Ressourcen haben Sie jetzt die Möglichkeit, JPSS-1-Kontakte für die asynchrone Datenübermittlung von jedem Ihrer Onboardanbieter aus zu planen. AWS Ground Station [AWS Ground Station Standorte]

Im Folgenden finden Sie eine vollständige CloudFormation Vorlage, die alle in diesem Abschnitt beschriebenen Ressourcen in einer einzigen Vorlage zusammenfasst, die direkt verwendet werden kann. CloudFormation

Die genannte CloudFormation Vorlage `AquaSnppJpss-1TerraDigIfS3DataDelivery.yml` enthält einen Amazon S3 S3-Bucket und die erforderlichen AWS Ground Station Ressourcen, um Kontakte zu planen und VITA-49-Signal-/IP-Direktübertragungsdaten zu empfangen.

Falls Aqua, SNPP, JPSS-1/NOAA-20 und Terra nicht in Ihr Konto integriert sind, finden Sie weitere Informationen unter. [Satellit an Bord]

> **Note**
>
> Sie können auf die Vorlage zugreifen, indem Sie mit gültigen AWS Anmeldeinformationen auf den Amazon S3 S3-Bucket des Kunden zugreifen. Die folgenden Links verwenden einen regionalen Amazon S3 S3-Bucket. Ändern Sie den `us-west-2` Regionalcode so, dass er die entsprechende Region darstellt, in der Sie den CloudFormation Stack erstellen möchten. Darüber hinaus verwenden die folgenden Anweisungen YAML. Die Vorlagen sind jedoch sowohl im YAML- als auch im JSON-Format verfügbar. Um JSON zu verwenden, ersetzen Sie `.json` beim Herunterladen der Vorlage die `.yml` Dateierweiterung durch.

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 direkt CloudFormation über den folgenden Link angeben:

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

Öffentlicher Rundfunksatellit, der einen Datenflussendpunkt nutzt (Schmalband)

Dieses Beispiel baut auf der Analyse auf, die im JPSS-1 — Öffentlicher Rundfunksatellit (PBS) — Evaluierung Abschnitt des Benutzerhandbuchs durchgeführt wurde.

Um dieses Beispiel zu vervollständigen, müssen Sie von einem Szenario ausgehen: Sie möchten den HRD-Kommunikationspfad als digitale Zwischenfrequenz (DigIF) erfassen und ihn so verarbeiten, wie er von einer Datenfluss-Endpunktanwendung auf einer EC2 Amazon-Instance mithilfe eines SDR empfangen wird.

Kommunikationspfade

Dieser Abschnitt beschreibt Planen Sie Ihre Datenfluss-Kommunikationspfade die ersten Schritte. In diesem Beispiel werden Sie zwei Abschnitte in Ihrer CloudFormation Vorlage erstellen: die Abschnitte Parameter und Ressourcen.

> **Note**
>
> Weitere Informationen zum Inhalt einer CloudFormation Vorlage finden Sie unter Abschnitte mit Vorlagen.

Für den Abschnitt Parameter werden Sie die folgenden Parameter hinzufügen. Sie geben Werte für diese an, wenn Sie den Stack über die CloudFormation Konsole erstellen.

```
Parameters:
  EC2Key:
    Description: The SSH key used to access the EC2 receiver instance. Choose any
 SSH key if you are not creating an EC2 receiver instance. For instructions on how to
 create an SSH key see https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/create-
key-pairs.html
    Type: AWS::EC2::KeyPair::KeyName
```

```
    ConstraintDescription: must be the name of an existing EC2 KeyPair.

  ReceiverAMI:
    Description: The Ground Station DDX AMI ID you want to use. Please note
  that AMIs are region specific. For instructions on how to retrieve an AMI
  see https://docs.aws.amazon.com/ground-station/latest/ug/dataflows.ec2-
configuration.html#dataflows.ec2-configuration.amis
    Type: AWS::EC2::Image::Id
```

> **Note**
>
> Sie müssen ein key pair erstellen und den Namen für den EC2 EC2Key Amazon-Parameter angeben. Weitere Informationen finden Sie unter Erstellen eines key pair für Ihre EC2 Amazon-Instance.
> Darüber hinaus müssen Sie bei der Erstellung des CloudFormation Stacks die richtige regionsspezifische AMI-ID angeben. Siehe AWS Ground Station Amazon-Maschinenbilder (AMIs).

Die verbleibenden Vorlagenausschnitte gehören in den Abschnitt Ressourcen der CloudFormation Vorlage.

```
Resources:
  # Resources that you would like to create should be placed within the resource
  section.
```

Angesichts unseres Szenarios, einer EC2 Instanz einen einzigen Kommunikationspfad bereitzustellen, verfügen Sie über einen einzigen synchronen Bereitstellungspfad. Gemäß Synchrone Datenübermittlung diesem Abschnitt müssen Sie eine EC2 Amazon-Instance mit einer Dataflow-Endpoint-Anwendung einrichten und konfigurieren und eine oder mehrere Datenfluss-Endpunktgruppen erstellen.

```
  # The EC2 instance that will send/receive data to/from your satellite using AWS
 Ground Station.
  ReceiverInstance:
    Type: AWS::EC2::Instance
    Properties:
      DisableApiTermination: false
```

```
      IamInstanceProfile: !Ref GeneralInstanceProfile
      ImageId: !Ref ReceiverAMI
      InstanceType: m5.4xlarge
      KeyName: !Ref EC2Key
      Monitoring: true
      PlacementGroupName: !Ref ClusterPlacementGroup
      SecurityGroupIds:
        - Ref: InstanceSecurityGroup
      SubnetId: !Ref ReceiverSubnet
      BlockDeviceMappings:
        - DeviceName: /dev/xvda
          Ebs:
            VolumeType: gp2
            VolumeSize: 40
      Tags:
        - Key: Name
          Value: !Join [ "-" , [ "Receiver" , !Ref "AWS::StackName" ] ]
      UserData:
        Fn::Base64:
          |
          #!/bin/bash
          exec > >(tee /var/log/user-data.log|logger -t user-data -s 2>/dev/console)
2>&1
          echo `date +'%F %R:%S'` "INFO: Logging Setup" >&2

          GROUND_STATION_DIR="/opt/aws/groundstation"
          GROUND_STATION_BIN_DIR="${GROUND_STATION_DIR}/bin"
          STREAM_CONFIG_PATH="${GROUND_STATION_DIR}/customer_stream_config.json"

          echo "Creating ${STREAM_CONFIG_PATH}"
          cat << STREAM_CONFIG > "${STREAM_CONFIG_PATH}"
          {
            "ddx_streams": [
              {
                "streamName": "Downlink",
                "maximumWanRate": 4000000000,
                "lanConfigDevice": "lo",
                "lanConfigPort": 50000,
                "wanConfigDevice": "eth1",
                "wanConfigPort": 55888,
                "isUplink": false
              }
            ]
          }
```

```
          STREAM_CONFIG

          echo "Waiting for dataflow endpoint application to start"
          while netstat -lnt | awk '$4 ~ /:80$/ {exit 1}'; do sleep 10; done

          echo "Configuring dataflow endpoint application streams"
          python "${GROUND_STATION_BIN_DIR}/configure_streams.py" --configFileName
"${STREAM_CONFIG_PATH}"
          sleep 2
          python "${GROUND_STATION_BIN_DIR}/save_default_config.py"

          exit 0

 # The AWS Ground Station Dataflow Endpoint Group that defines the endpoints that AWS
Ground
 # Station will use to send/receive data to/from your satellite.
 DataflowEndpointGroup:
   Type: AWS::GroundStation::DataflowEndpointGroup
   Properties:
     ContactPostPassDurationSeconds: 180
     ContactPrePassDurationSeconds: 120
     EndpointDetails:
       - Endpoint:
           Name: !Join [ "-" , [ !Ref "AWS::StackName" , "Downlink" ] ] # needs to
match DataflowEndpointConfig name
           Address:
             Name: !GetAtt ReceiverInstanceNetworkInterface.PrimaryPrivateIpAddress
             Port: 55888
         SecurityDetails:
           SecurityGroupIds:
             - Ref: "DataflowEndpointSecurityGroup"
           SubnetIds:
             - !Ref ReceiverSubnet
           RoleArn: !GetAtt DataDeliveryServiceRole.Arn

 # The security group for your EC2 instance.
 InstanceSecurityGroup:
   Type: AWS::EC2::SecurityGroup
   Properties:
     GroupDescription: AWS Ground Station receiver instance security group.
     VpcId: !Ref ReceiverVPC
     SecurityGroupIngress:
       # To allow SSH access to the instance, add another rule allowing tcp port 22
from your CidrIp
```

```
        - IpProtocol: udp
          FromPort: 55888
          ToPort: 55888
          SourceSecurityGroupId: !Ref DataflowEndpointSecurityGroup
          Description: "AWS Ground Station Downlink Stream"

  # The security group that the ENI created by AWS Ground Station belongs to.
  DataflowEndpointSecurityGroup:
    Type: AWS::EC2::SecurityGroup
    Properties:
      GroupDescription: Security Group for AWS Ground Station registration of Dataflow
Endpoint Groups
      VpcId: !Ref ReceiverVPC
      SecurityGroupEgress:
        - IpProtocol: udp
          FromPort: 55888
          ToPort: 55888
          CidrIp: 10.0.0.0/8
          Description: "AWS Ground Station Downlink Stream To 10/8"
        - IpProtocol: udp
          FromPort: 55888
          ToPort: 55888
          CidrIp: 172.16.0.0/12
          Description: "AWS Ground Station Downlink Stream To 172.16/12"
        - IpProtocol: udp
          FromPort: 55888
          ToPort: 55888
          CidrIp: 192.168.0.0/16
          Description: "AWS Ground Station Downlink Stream To 192.168/16"

  # The placement group in which your EC2 instance is placed.
  ClusterPlacementGroup:
    Type: AWS::EC2::PlacementGroup
    Properties:
      Strategy: cluster

  ReceiverVPC:
    Type: AWS::EC2::VPC
    Properties:
      CidrBlock: "10.0.0.0/16"
      Tags:
        - Key: "Name"
          Value: "AWS Ground Station - PBS to dataflow endpoint Example VPC"
        - Key: "Description"
```

```
          Value: "VPC for EC2 instance receiving AWS Ground Station data"

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

 # An ENI providing a fixed IP address for AWS Ground Station to connect to.
 ReceiverInstanceNetworkInterface:
   Type: AWS::EC2::NetworkInterface
   Properties:
     Description: Floating network interface providing a fixed IP address for AWS
Ground Station to connect to.
     GroupSet:
       - !Ref InstanceSecurityGroup
     SubnetId: !Ref ReceiverSubnet

 # Attach the ENI to the EC2 instance.
 ReceiverInstanceInterfaceAttachment:
   Type: AWS::EC2::NetworkInterfaceAttachment
   Properties:
     DeleteOnTermination: false
     DeviceIndex: "1"
     InstanceId: !Ref ReceiverInstance
     NetworkInterfaceId: !Ref ReceiverInstanceNetworkInterface
```

Darüber hinaus müssen Sie die entsprechenden Richtlinien und Rollen erstellen, damit AWS Ground Station Sie in Ihrem Konto ein elastic network interface (ENI) einrichten können.

```
 # AWS Ground Station assumes this role to create/delete ENIs in your account in order
to stream data.
```

```
  DataDeliveryServiceRole:
    Type: AWS::IAM::Role
    Properties:
      Policies:
        - PolicyDocument:
            Statement:
              - Action:
                  - ec2:CreateNetworkInterface
                  - ec2:DeleteNetworkInterface
                  - ec2:CreateNetworkInterfacePermission
                  - ec2:DeleteNetworkInterfacePermission
                  - ec2:DescribeSubnets
                  - ec2:DescribeVpcs
                  - ec2:DescribeSecurityGroups
                Effect: Allow
                Resource: '*'
            Version: '2012-10-17'
          PolicyName: DataDeliveryServicePolicy
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service:
              - groundstation.amazonaws.com
            Action:
            - sts:AssumeRole

  # The EC2 instance assumes this role.
  InstanceRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: "Allow"
            Principal:
              Service:
                - "ec2.amazonaws.com"
            Action:
              - "sts:AssumeRole"
      Path: "/"
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess
```

```
        - arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceforEC2Role
        - arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy
        - arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforSSM

  # The instance profile for your EC2 instance.
  GeneralInstanceProfile:
    Type: AWS::IAM::InstanceProfile
    Properties:
      Roles:
        - !Ref InstanceRole
```

AWS Ground Station Konfigurationen

Dieser Abschnitt beschreibt Konfigurationen erstellen die ersten Schritte.

Sie benötigen eine Tracking-Konfiguration, um Ihre Präferenz für die Verwendung von Autotrack festzulegen. Die Auswahl von PREFERRED als Autotrack kann die Signalqualität verbessern, ist aber aufgrund der ausreichenden JPSS-1-Ephemeridenqualität nicht erforderlich, um die Signalqualität zu gewährleisten.

```
  TrackingConfig:
    Type: AWS::GroundStation::Config
    Properties:
      Name: "JPSS Tracking Config"
      ConfigData:
        TrackingConfig:
          Autotrack: "PREFERRED"
```

Basierend auf dem Kommunikationspfad müssen Sie eine Antennen-Downlink-Konfiguration definieren, die den Satellitenanteil repräsentiert, sowie eine Datenfluss-Endpunktkonfiguration, um auf die Datenfluss-Endpunktgruppe zu verweisen, die die Endpunktdetails definiert.

```
  # The AWS Ground Station Antenna Downlink Config that defines the frequency spectrum
used to
  # downlink data from your satellite.
  SnppJpssDownlinkDigIfAntennaConfig:
    Type: AWS::GroundStation::Config
```

```
    Properties:
      Name: "SNPP JPSS Downlink DigIF Antenna Config"
      ConfigData:
        AntennaDownlinkConfig:
          SpectrumConfig:
            Bandwidth:
              Units: "MHz"
              Value: 30
            CenterFrequency:
              Units: "MHz"
              Value: 7812
            Polarization: "RIGHT_HAND"

  # The AWS Ground Station Dataflow Endpoint Config that defines the endpoint used to
downlink data
  # from your satellite.
  DownlinkDigIfEndpointConfig:
    Type: AWS::GroundStation::Config
    Properties:
      Name: "Aqua SNPP JPSS Downlink DigIF Endpoint Config"
      ConfigData:
        DataflowEndpointConfig:
          DataflowEndpointName: !Join [ "-" , [ !Ref "AWS::StackName" , "Downlink" ] ]
          DataflowEndpointRegion: !Ref AWS::Region
```

AWS Ground Station Missionsprofil

Dieser Abschnitt beschreibt Missionsprofil erstellen die ersten Schritte.

Da Sie nun über die zugehörigen Konfigurationen verfügen, können Sie sie verwenden, um den Datenfluss zu erstellen. Für die übrigen Parameter verwenden Sie die Standardwerte.

```
  # The AWS Ground Station Mission Profile that groups the above configurations to
define how to
  # uplink and downlink data to your satellite.
  SnppJpssMissionProfile:
    Type: AWS::GroundStation::MissionProfile
    Properties:
      Name: "37849 SNPP And 43013 JPSS"
      ContactPrePassDurationSeconds: 120
      ContactPostPassDurationSeconds: 60
```

```
      MinimumViableContactDurationSeconds: 180
      TrackingConfigArn: !Ref TrackingConfig
      DataflowEdges:
        - Source: !Ref SnppJpssDownlinkDigIfAntennaConfig
          Destination: !Ref DownlinkDigIfEndpointConfig
```

Es zusammensetzen

Mit den oben genannten Ressourcen haben Sie jetzt die Möglichkeit, JPSS-1-Kontakte für die synchrone Datenübermittlung von jedem Ihrer Onboardanbieter aus zu planen. AWS Ground Station AWS Ground Station Standorte

Im Folgenden finden Sie eine vollständige CloudFormation Vorlage, die alle in diesem Abschnitt beschriebenen Ressourcen in einer einzigen Vorlage zusammenfasst, die direkt verwendet werden kann. CloudFormation

Die genannte 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 EC2 Amazon-Instance und die erforderlichen CloudFormation Ressourcen, um DigiF-Direktübertragungs-Rohdaten zu empfangen.

Falls Aqua, SNPP, JPSS-1/NOAA-20 und Terra nicht in Ihr Konto integriert sind, finden Sie weitere Informationen unter. Satellit an Bord

> **Note**
>
> Sie können auf die Vorlage zugreifen, indem Sie mit gültigen AWS Anmeldeinformationen auf den Amazon S3 S3-Bucket des Kunden zugreifen. Die folgenden Links verwenden einen regionalen Amazon S3 S3-Bucket. Ändern Sie den `us-west-2` Regionalcode so, dass er die entsprechende Region darstellt, in der Sie den CloudFormation Stack erstellen möchten. Darüber hinaus verwenden die folgenden Anweisungen YAML. Die Vorlagen sind jedoch sowohl im YAML- als auch im JSON-Format verfügbar. Um JSON zu verwenden, ersetzen Sie `.json` beim Herunterladen der Vorlage die `.yml` Dateierweiterung durch.

Verwenden Sie den folgenden Befehl AWS CLI, um die Vorlage mit 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 CloudFormation über den folgenden Link angeben:

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

Welche zusätzlichen Ressourcen definiert die Vorlage?

Die `AquaSnppJpssTerraDigIF` Vorlage enthält die folgenden zusätzlichen Ressourcen:

- (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 Überprüfung von Kontakten — Die Option, Lambda zu verwenden, um ein Überprüfungssystem für Ihre EC2 Amazon-Instance (s) für Kontakte mit SNS-Benachrichtigung einzurichten. Bitte beachten Sie, dass hierfür je nach Ihrer aktuellen Nutzung Gebühren anfallen können.
- 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.
- Zusätzliche Missionsprofile — Missionsprofile für zusätzliche öffentlich-rechtliche Rundfunksatelliten (Aqua, SNPP und Terra).
- Zusätzliche Antennen-Downlink-Konfigurationen — Antennen-Downlink-Konfigurationen für zusätzliche öffentlich-rechtliche Rundfunksatelliten (Aqua, SNPP und 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 eine Datenfluss-Endpunktanwendung, 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 Hinweise zum Einrichten einer Datenfluss-Endpunktgruppe finden Sie unter. AWS::GroundStation::DataflowEndpointGroup

Öffentlicher Rundfunksatellit, der einen Datenflussendpunkt verwendet (demoduliert und dekodiert)

Dieses Beispiel baut auf der Analyse auf, die im JPSS-1 — Öffentlicher Rundfunksatellit (PBS) — Evaluierung Abschnitt des Benutzerhandbuchs durchgeführt wurde.

Um dieses Beispiel zu vervollständigen, müssen Sie von einem Szenario ausgehen: Sie möchten den HRD-Kommunikationspfad als demodulierte und dekodierte Direktübertragungsdaten mithilfe eines Datenflussendpunkts erfassen. Dieses Beispiel ist ein guter Ausgangspunkt, wenn Sie planen, die Daten mit der NASA Direct Readout Labs-Software (RT-STPS und IPOPP) zu verarbeiten.

Kommunikationswege

Dieser Abschnitt beschreibt Planen Sie Ihre Datenfluss-Kommunikationspfade die ersten Schritte. In diesem Beispiel werden Sie zwei Abschnitte in Ihrer CloudFormation Vorlage erstellen: die Abschnitte Parameter und Ressourcen.

> **Note**
>
> Weitere Informationen zum Inhalt einer CloudFormation Vorlage finden Sie unter Abschnitte mit Vorlagen.

Für den Abschnitt Parameter werden Sie die folgenden Parameter hinzufügen. Sie geben Werte für diese an, wenn Sie den Stack über die CloudFormation Konsole erstellen.

```
Parameters:
  EC2Key:
    Description: The SSH key used to access the EC2 receiver instance. Choose any
 SSH key if you are not creating an EC2 receiver instance. For instructions on how to
 create an SSH key see https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/create-
key-pairs.html
    Type: AWS::EC2::KeyPair::KeyName
    ConstraintDescription: must be the name of an existing EC2 KeyPair.

  ReceiverAMI:
    Description: The Ground Station DDX AMI ID you want to use. Please note
 that AMIs are region specific. For instructions on how to retrieve an AMI
 see https://docs.aws.amazon.com/ground-station/latest/ug/dataflows.ec2-
configuration.html#dataflows.ec2-configuration.amis
    Type: AWS::EC2::Image::Id
```

> **Note**
>
> Sie müssen ein key pair erstellen und den Namen für den EC2 EC2Key Amazon-Parameter angeben. Weitere Informationen finden Sie unter Erstellen eines key pair für Ihre EC2 Amazon-Instance.
>
> Darüber hinaus müssen Sie bei der Erstellung des CloudFormation Stacks die richtige regionsspezifische AMI-ID angeben. Siehe AWS Ground Station Amazon-Maschinenbilder (AMIs).

Die verbleibenden Vorlagenausschnitte gehören in den Abschnitt Ressourcen der CloudFormation Vorlage.

```
Resources:
  # Resources that you would like to create should be placed within the resource
 section.
```

Angesichts unseres Szenarios, einer EC2 Instanz einen einzigen Kommunikationspfad bereitzustellen, verfügen Sie über einen einzigen synchronen Bereitstellungspfad. Gemäß Synchrone Datenübermittlung diesem Abschnitt müssen Sie eine EC2 Amazon-Instance mit einer

Dataflow-Endpoint-Anwendung einrichten und konfigurieren und eine oder mehrere Datenfluss-Endpunktgruppen erstellen.

```
 # The EC2 instance that will send/receive data to/from your satellite using AWS
Ground Station.
 ReceiverInstance:
   Type: AWS::EC2::Instance
   Properties:
     DisableApiTermination: false
     IamInstanceProfile: !Ref GeneralInstanceProfile
     ImageId: !Ref ReceiverAMI
     InstanceType: m5.4xlarge
     KeyName: !Ref EC2Key
     Monitoring: true
     PlacementGroupName: !Ref ClusterPlacementGroup
     SecurityGroupIds:
       - Ref: InstanceSecurityGroup
     SubnetId: !Ref ReceiverSubnet
     BlockDeviceMappings:
       - DeviceName: /dev/xvda
         Ebs:
           VolumeType: gp2
           VolumeSize: 40
     Tags:
       - Key: Name
         Value: !Join [ "-" , [ "Receiver" , !Ref "AWS::StackName" ] ]
     UserData:
       Fn::Base64:
         |
         #!/bin/bash
         exec > >(tee /var/log/user-data.log|logger -t user-data -s 2>/dev/console)
2>&1
         echo `date +'%F %R:%S'` "INFO: Logging Setup" >&2

         GROUND_STATION_DIR="/opt/aws/groundstation"
         GROUND_STATION_BIN_DIR="${GROUND_STATION_DIR}/bin"
         STREAM_CONFIG_PATH="${GROUND_STATION_DIR}/customer_stream_config.json"

         echo "Creating ${STREAM_CONFIG_PATH}"
         cat << STREAM_CONFIG > "${STREAM_CONFIG_PATH}"
         {
           "ddx_streams": [
```

```
            {
              "streamName": "Downlink",
              "maximumWanRate": 4000000000,
              "lanConfigDevice": "lo",
              "lanConfigPort": 50000,
              "wanConfigDevice": "eth1",
              "wanConfigPort": 55888,
              "isUplink": false
            }
          ]
        }
        STREAM_CONFIG

        echo "Waiting for dataflow endpoint application to start"
        while netstat -lnt | awk '$4 ~ /:80$/ {exit 1}'; do sleep 10; done

        echo "Configuring dataflow endpoint application streams"
        python "${GROUND_STATION_BIN_DIR}/configure_streams.py" --configFileName
"${STREAM_CONFIG_PATH}"
        sleep 2
        python "${GROUND_STATION_BIN_DIR}/save_default_config.py"

        exit 0
```

```
 # The AWS Ground Station Dataflow Endpoint Group that defines the endpoints that AWS
Ground
 # Station will use to send/receive data to/from your satellite.
 DataflowEndpointGroup:
   Type: AWS::GroundStation::DataflowEndpointGroup
   Properties:
     ContactPostPassDurationSeconds: 180
     ContactPrePassDurationSeconds: 120
     EndpointDetails:
       - Endpoint:
           Name: !Join [ "-" , [ !Ref "AWS::StackName" , "Downlink" ] ] # needs to
match DataflowEndpointConfig name
           Address:
             Name: !GetAtt ReceiverInstanceNetworkInterface.PrimaryPrivateIpAddress
             Port: 55888
         SecurityDetails:
           SecurityGroupIds:
             - Ref: "DataflowEndpointSecurityGroup"
```

```
            SubnetIds:
              - !Ref ReceiverSubnet
            RoleArn: !GetAtt DataDeliveryServiceRole.Arn

  # The security group that the ENI created by AWS Ground Station belongs to.
  DataflowEndpointSecurityGroup:
    Type: AWS::EC2::SecurityGroup
    Properties:
      GroupDescription: Security Group for AWS Ground Station registration of Dataflow
Endpoint Groups
      VpcId: !Ref ReceiverVPC
      SecurityGroupEgress:
        - IpProtocol: udp
          FromPort: 55888
          ToPort: 55888
          CidrIp: 10.0.0.0/8
          Description: "AWS Ground Station Downlink Stream To 10/8"
        - IpProtocol: udp
          FromPort: 55888
          ToPort: 55888
          CidrIp: 172.16.0.0/12
          Description: "AWS Ground Station Downlink Stream To 172.16/12"
        - IpProtocol: udp
          FromPort: 55888
          ToPort: 55888
          CidrIp: 192.168.0.0/16
          Description: "AWS Ground Station Downlink Stream To 192.168/16"

  # The placement group in which your EC2 instance is placed.
  ClusterPlacementGroup:
    Type: AWS::EC2::PlacementGroup
    Properties:
      Strategy: cluster

  # The security group for your EC2 instance.
  InstanceSecurityGroup:
    Type: AWS::EC2::SecurityGroup
    Properties:
      GroupDescription: AWS Ground Station receiver instance security group.
      VpcId: !Ref ReceiverVPC
      SecurityGroupIngress:
        # To allow SSH access to the instance, add another rule allowing tcp port 22
from your CidrIp
        - IpProtocol: udp
```

```
          FromPort: 55888
          ToPort: 55888
          SourceSecurityGroupId: !Ref DataflowEndpointSecurityGroup
          Description: "AWS Ground Station Downlink Stream"

  ReceiverVPC:
    Type: AWS::EC2::VPC
    Properties:
      CidrBlock: "10.0.0.0/16"
      Tags:
        - Key: "Name"
          Value: "AWS Ground Station - PBS to dataflow endpoint Demod Decode Example
VPC"
        - Key: "Description"
          Value: "VPC for EC2 instance receiving AWS Ground Station data"

  ReceiverSubnet:
    Type: AWS::EC2::Subnet
    Properties:
      CidrBlock: "10.0.0.0/24"
      Tags:
        - Key: "Name"
          Value: "AWS Ground Station - PBS to dataflow endpoint Demod Decode Example
Subnet"
        - Key: "Description"
          Value: "Subnet for EC2 instance receiving AWS Ground Station data"
      VpcId: !Ref ReceiverVPC

  # An ENI providing a fixed IP address for AWS Ground Station to connect to.
  ReceiverInstanceNetworkInterface:
    Type: AWS::EC2::NetworkInterface
    Properties:
      Description: Floating network interface providing a fixed IP address for AWS
Ground Station to connect to.
      GroupSet:
        - !Ref InstanceSecurityGroup
      SubnetId: !Ref ReceiverSubnet

  # Attach the ENI to the EC2 instance.
  ReceiverInstanceInterfaceAttachment:
    Type: AWS::EC2::NetworkInterfaceAttachment
    Properties:
      DeleteOnTermination: false
      DeviceIndex: "1"
```

```
      InstanceId: !Ref ReceiverInstance
      NetworkInterfaceId: !Ref ReceiverInstanceNetworkInterface

  # The instance profile for your EC2 instance.
  GeneralInstanceProfile:
    Type: AWS::IAM::InstanceProfile
    Properties:
      Roles:
        - !Ref InstanceRole
```

Sie benötigen außerdem die entsprechenden Richtlinien, Rollen und Profile, um ein elastic network interface (ENI) in Ihrem Konto erstellen AWS Ground Station zu können.

```
  # AWS Ground Station assumes this role to create/delete ENIs in your account in order
to stream data.
  DataDeliveryServiceRole:
    Type: AWS::IAM::Role
    Properties:
      Policies:
        - PolicyDocument:
            Statement:
              - Action:
                  - ec2:CreateNetworkInterface
                  - ec2:DeleteNetworkInterface
                  - ec2:CreateNetworkInterfacePermission
                  - ec2:DeleteNetworkInterfacePermission
                  - ec2:DescribeSubnets
                  - ec2:DescribeVpcs
                  - ec2:DescribeSecurityGroups
                Effect: Allow
                Resource: '*'
            Version: '2012-10-17'
          PolicyName: DataDeliveryServicePolicy
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service:
              - groundstation.amazonaws.com
            Action:
```

```
          - sts:AssumeRole

# The EC2 instance assumes this role.
InstanceRole:
  Type: AWS::IAM::Role
  Properties:
    AssumeRolePolicyDocument:
      Version: "2012-10-17"
      Statement:
        - Effect: "Allow"
          Principal:
            Service:
              - "ec2.amazonaws.com"
          Action:
            - "sts:AssumeRole"
    Path: "/"
    ManagedPolicyArns:
      - arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess
      - arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceforEC2Role
      - arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy
      - arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforSSM
```

AWS Ground Station Konfigurationen

Dieser Abschnitt stellt Konfigurationen erstellen das Benutzerhandbuch dar.

Sie benötigen eine Tracking-Konfiguration, um Ihre Präferenz für die Verwendung von Autotrack festzulegen. Die Auswahl von PREFERRED als Autotrack kann die Signalqualität verbessern, ist aber aufgrund der ausreichenden JPSS-1-Ephemeridenqualität nicht erforderlich, um die Signalqualität zu gewährleisten.

```
TrackingConfig:
  Type: AWS::GroundStation::Config
  Properties:
    Name: "JPSS Tracking Config"
    ConfigData:
      TrackingConfig:
        Autotrack: "PREFERRED"
```

Basierend auf dem Kommunikationspfad müssen Sie eine antenna-downlink-demod-decodeKonfiguration definieren, die den Satellitenanteil repräsentiert, sowie eine Datenfluss-Endpunktkonfiguration, um auf die Datenfluss-Endpunktgruppe zu verweisen, die die Endpunktdetails definiert.

> **Note**
>
> Einzelheiten zum Einstellen der Werte für und finden Sie `DemodulationConfig` unter. `DecodeConfig` Antennen-Downlink-Demod-Decode-Config

```
 # The AWS Ground Station Antenna Downlink Config that defines the frequency spectrum
used to
 # downlink data from your satellite.
 JpssDownlinkDemodDecodeAntennaConfig:
   Type: AWS::GroundStation::Config
   Properties:
     Name: "JPSS Downlink Demod Decode Antenna Config"
     ConfigData:
       AntennaDownlinkDemodDecodeConfig:
         SpectrumConfig:
           CenterFrequency:
             Value: 7812
             Units: "MHz"
           Polarization: "RIGHT_HAND"
           Bandwidth:
             Value: 30
             Units: "MHz"
         DemodulationConfig:
           UnvalidatedJSON: '{
             "type":"QPSK",
             "qpsk":{
               "carrierFrequencyRecovery":{
                 "centerFrequency":{
                   "value":7812,
                   "units":"MHz"
                 },
                 "range":{
                   "value":250,
                   "units":"kHz"
                 }
```

```
            },
            "symbolTimingRecovery":{
              "symbolRate":{
                "value":15,
                "units":"Msps"
              },
              "range":{
                "value":0.75,
                "units":"ksps"
              },
              "matchedFilter":{
                "type":"ROOT_RAISED_COSINE",
                "rolloffFactor":0.5
              }
            }
          }
        }'
      DecodeConfig:
        UnvalidatedJSON: '{
          "edges":[
            {
              "from":"I-Ingress",
              "to":"IQ-Recombiner"
            },
            {
              "from":"Q-Ingress",
              "to":"IQ-Recombiner"
            },
            {
              "from":"IQ-Recombiner",
              "to":"CcsdsViterbiDecoder"
            },
            {
              "from":"CcsdsViterbiDecoder",
              "to":"NrzmDecoder"
            },
            {
              "from":"NrzmDecoder",
              "to":"UncodedFramesEgress"
            }
          ],
          "nodeConfigs":{
            "I-Ingress":{
              "type":"CODED_SYMBOLS_INGRESS",
```

```
                "codedSymbolsIngress":{
                  "source":"I"
                }
              },
              "Q-Ingress":{
                "type":"CODED_SYMBOLS_INGRESS",
                "codedSymbolsIngress":{
                  "source":"Q"
                }
              },
              "IQ-Recombiner":{
                "type":"IQ_RECOMBINER"
              },
              "CcsdsViterbiDecoder":{
                "type":"CCSDS_171_133_VITERBI_DECODER",
                "ccsds171133ViterbiDecoder":{
                  "codeRate":"ONE_HALF"
                }
              },
              "NrzmDecoder":{
                "type":"NRZ_M_DECODER"
              },
              "UncodedFramesEgress":{
                "type":"UNCODED_FRAMES_EGRESS"
              }
            }
          }'
```

```
 # The AWS Ground Station Dataflow Endpoint Config that defines the endpoint used to
downlink data
 # from your satellite.
 DownlinkDemodDecodeEndpointConfig:
   Type: AWS::GroundStation::Config
   Properties:
     Name: "Aqua SNPP JPSS Downlink Demod Decode Endpoint Config"
     ConfigData:
       DataflowEndpointConfig:
         DataflowEndpointName: !Join [ "-" , [ !Ref "AWS::StackName" , "Downlink" ] ]
         DataflowEndpointRegion: !Ref AWS::Region
```

AWS Ground Station Missionsprofil

Dieser Abschnitt stellt Missionsprofil erstellen das Benutzerhandbuch dar.

Da Sie nun über die zugehörigen Konfigurationen verfügen, können Sie sie verwenden, um den Datenfluss zu erstellen. Für die übrigen Parameter verwenden Sie die Standardwerte.

```
 # The AWS Ground Station Mission Profile that groups the above configurations to
define how to
 # uplink and downlink data to your satellite.
 SnppJpssMissionProfile:
   Type: AWS::GroundStation::MissionProfile
   Properties:
     Name: "37849 SNPP And 43013 JPSS"
     ContactPrePassDurationSeconds: 120
     ContactPostPassDurationSeconds: 60
     MinimumViableContactDurationSeconds: 180
     TrackingConfigArn: !Ref TrackingConfig
     DataflowEdges:
       - Source: !Join [ "/", [ !Ref JpssDownlinkDemodDecodeAntennaConfig,
"UncodedFramesEgress" ] ]
         Destination: !Ref DownlinkDemodDecodeEndpointConfig
```

Es zusammensetzen

Mit den oben genannten Ressourcen haben Sie jetzt die Möglichkeit, JPSS-1-Kontakte für die synchrone Datenübermittlung von jedem Ihrer Onboardanbieter aus zu planen. AWS Ground Station AWS Ground Station Standorte

Im Folgenden finden Sie eine vollständige CloudFormation Vorlage, die alle in diesem Abschnitt beschriebenen Ressourcen in einer einzigen Vorlage zusammenfasst, die direkt verwendet werden kann. CloudFormation

Die genannte 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 EC2 Amazon-Instance und die erforderlichen AWS Ground Station Ressourcen, um Kontakte zu planen und demodulierte und dekodierte Direktübertragungsdaten zu empfangen.

Falls Aqua, SNPP, JPSS-1/NOAA-20 und Terra nicht in Ihr Konto integriert sind, finden Sie weitere Informationen unter. Satellit an Bord

> **Note**
>
> Sie können auf die Vorlage zugreifen, indem Sie mit gültigen AWS Anmeldeinformationen auf den Amazon S3 S3-Bucket des Kunden zugreifen. Die folgenden Links verwenden einen regionalen Amazon S3 S3-Bucket. Ändern Sie den `us-west-2` Regionalcode so, dass er die entsprechende Region darstellt, in der Sie den CloudFormation Stack erstellen möchten. Darüber hinaus verwenden die folgenden Anweisungen YAML. Die Vorlagen sind jedoch sowohl im YAML- als auch im JSON-Format verfügbar. Um JSON zu verwenden, ersetzen Sie `.json` beim Herunterladen der Vorlage die `.yml` Dateierweiterung durch.

Verwenden Sie den folgenden Befehl AWS CLI, um die Vorlage mit 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 CloudFormation über den folgenden Link angeben:

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

Welche zusätzlichen Ressourcen definiert die Vorlage?

Die `AquaSnppJpss` Vorlage enthält die folgenden zusätzlichen Ressourcen:

- (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 Überprüfung von Kontakten — Die Option, Lambda zu verwenden, um ein Überprüfungssystem für Ihre EC2 Amazon-Instance (s) für Kontakte mit SNS-Benachrichtigung

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

- 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, finden Sie weitere Informationen unter. Öffentlicher Rundfunksatellit mit AWS Ground Station Agent (Breitband) Diese Optionen werden mit der Veröffentlichung zusätzlicher Softwareupdates und Funktionen weiter ausgebaut.
- Zusätzliche Missionsprofile — Missionsprofile für zusätzliche öffentlich-rechtliche Rundfunksatelliten (Aqua, SNPP und Terra).
- Zusätzliche Antennen-Downlink-Konfigurationen — Antennen-Downlink-Konfigurationen für zusätzliche öffentlich-rechtliche Rundfunksatelliten (Aqua, SNPP und 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 eine Datenfluss-Endpunktanwendung, 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 Hinweise zum Einrichten einer Datenfluss-Endpunktgruppe finden Sie unter. AWS::GroundStation::DataflowEndpointGroup

Öffentlicher Rundfunksatellit mit AWS Ground Station Agent (Breitband)

Dieses Beispiel baut auf der Analyse auf, die im JPSS-1 — Öffentlicher Rundfunksatellit (PBS) — Evaluierung Abschnitt des Benutzerhandbuchs durchgeführt wurde.

Um dieses Beispiel zu vervollständigen, müssen Sie von einem Szenario ausgehen: Sie möchten den HRD-Kommunikationspfad als digitale Breitband-Zwischenfrequenz (DigIF) erfassen und ihn so

verarbeiten, wie er vom AWS Ground Station Agenten auf einer EC2 Amazon-Instance mithilfe eines SDR empfangen wird.

> **Note**
>
> Das eigentliche JPSS HRD-Kommunikationspfadsignal hat eine Bandbreite von 30 MHz, aber Sie werden die Antennen-Downlink-Konfiguration so konfigurieren, dass es als Signal mit einer MHz Bandbreite von 100 behandelt wird, sodass es in diesem Beispiel über den richtigen Pfad fließen kann, um vom AWS Ground Station Agenten empfangen zu werden.

Kommunikationspfade

Dieser Abschnitt beschreibt Planen Sie Ihre Datenfluss-Kommunikationspfade die ersten Schritte. Für dieses Beispiel benötigen Sie einen zusätzlichen Abschnitt in Ihrer CloudFormation Vorlage, der in den anderen Beispielen nicht verwendet wurde, den Abschnitt Zuordnungen.

> **Note**
>
> Weitere Informationen zum Inhalt einer CloudFormation Vorlage finden Sie unter Abschnitte mit Vorlagen.

Zunächst richten Sie in Ihrer CloudFormation Vorlage einen Abschnitt „Zuordnungen“ für die AWS Ground Station Präfixlisten nach Regionen ein. Dadurch können die Präfixlisten von der EC2 Amazon-Instance-Sicherheitsgruppe einfach referenziert werden. Weitere Informationen zur Verwendung einer Präfixliste finden Sie unterVPC-Konfiguration mit Agent AWS Ground Station.

```
Mappings:
  PrefixListId:
    us-east-2:
      groundstation: pl-087f83ba4f34e3bea
    us-west-2:
      groundstation: pl-0cc36273da754ebdc
    us-east-1:
      groundstation: pl-0e5696d987d033653
    eu-central-1:
      groundstation: pl-03743f81267c0a85e
```

```
    sa-east-1:
      groundstation: pl-098248765e9effc20
    ap-northeast-2:
      groundstation: pl-059b3e0b02af70e4d
    ap-southeast-1:
      groundstation: pl-0d9b804fe014a6a99
    ap-southeast-2:
      groundstation: pl-08d24302b8c4d2b73
    me-south-1:
      groundstation: pl-02781422c4c792145
    eu-west-1:
      groundstation: pl-03fa6b266557b0d4f
    eu-north-1:
      groundstation: pl-033e44023025215c0
    af-south-1:
      groundstation: pl-0382d923a9d555425
```

Für den Abschnitt Parameter werden Sie die folgenden Parameter hinzufügen. Sie geben Werte für diese an, wenn Sie den Stack über die CloudFormation Konsole erstellen.

```
Parameters:
  EC2Key:
    Description: The SSH key used to access the EC2 receiver instance. Choose any
 SSH key if you are not creating an EC2 receiver instance. For instructions on how to
 create an SSH key see https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/create-
key-pairs.html
    Type: AWS::EC2::KeyPair::KeyName
    ConstraintDescription: must be the name of an existing EC2 KeyPair.

  AZ:
    Description: "The AvailabilityZone that the resources of this stack will be created
 in. (e.g. us-east-2a)"
    Type: AWS::EC2::AvailabilityZone::Name

  ReceiverAMI:
    Description: The Ground Station Agent AMI ID you want to use. Please note
 that AMIs are region specific. For instructions on how to retrieve an AMI
 see https://docs.aws.amazon.com/ground-station/latest/ug/dataflows.ec2-
configuration.html#dataflows.ec2-configuration.amis
    Type: AWS::EC2::Image::Id
```

> **Note**
>
> Sie müssen ein key pair erstellen und den Namen für den EC2 `EC2Key` Amazon-Parameter angeben. Weitere Informationen finden Sie unter Erstellen eines key pair für Ihre EC2 Amazon-Instance.
> Darüber hinaus müssen Sie bei der Erstellung des CloudFormation Stacks die richtige regionsspezifische AMI-ID angeben. Siehe AWS Ground Station Amazon-Maschinenbilder (AMIs).

Die verbleibenden Vorlagenausschnitte gehören in den Abschnitt Ressourcen der CloudFormation Vorlage.

```
Resources:
  # Resources that you would like to create should be placed within the Resources
 section.
```

Angesichts unseres Szenarios, einen einzigen Kommunikationspfad für eine EC2 Amazon-Instance bereitzustellen, wissen Sie, dass Sie einen einzigen synchronen Lieferpfad haben werden. Gemäß Synchrone Datenübermittlung diesem Abschnitt müssen Sie eine EC2 Amazon-Instance mit AWS Ground Station Agent einrichten und konfigurieren und eine oder mehrere Datenfluss-Endpunktgruppen erstellen. Zunächst richten Sie die Amazon VPC für den AWS Ground Station Agenten ein.

```
  ReceiverVPC:
    Type: AWS::EC2::VPC
    Properties:
      EnableDnsSupport: 'true'
      EnableDnsHostnames: 'true'
      CidrBlock: 10.0.0.0/16
      Tags:
      - Key: "Name"
        Value: "AWS Ground Station Example - PBS to AWS Ground Station Agent VPC"
      - Key: "Description"
        Value: "VPC for EC2 instance receiving AWS Ground Station data"

  PublicSubnet:
    Type: AWS::EC2::Subnet
```

```
    Properties:
      VpcId: !Ref ReceiverVPC
      MapPublicIpOnLaunch: 'true'
      AvailabilityZone: !Ref AZ
      CidrBlock: 10.0.0.0/20
      Tags:
      - Key: "Name"
        Value: "AWS Ground Station Example - PBS to AWS Ground Station Agent Public
 Subnet"
      - Key: "Description"
        Value: "Subnet for EC2 instance receiving AWS Ground Station data"

  RouteTable:
    Type: AWS::EC2::RouteTable
    Properties:
      VpcId: !Ref ReceiverVPC
      Tags:
        - Key: Name
          Value: AWS Ground Station Example - RouteTable

  RouteTableAssociation:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref RouteTable
      SubnetId: !Ref PublicSubnet

  Route:
    Type: AWS::EC2::Route
    DependsOn: InternetGateway
    Properties:
      RouteTableId: !Ref RouteTable
      DestinationCidrBlock: '0.0.0.0/0'
      GatewayId: !Ref InternetGateway

  InternetGateway:
    Type: AWS::EC2::InternetGateway
    Properties:
      Tags:
        - Key: Name
          Value: AWS Ground Station Example - Internet Gateway

  GatewayAttachment:
    Type: AWS::EC2::VPCGatewayAttachment
    Properties:
```

```
      VpcId: !Ref ReceiverVPC
      InternetGatewayId: !Ref InternetGateway
```

> **Note**
>
> Weitere Informationen zu den vom Agenten unterstützten VPC-Konfigurationen finden Sie unter AWS Ground Station [AWS Ground Station Agentenanforderungen — VPC-Diagramme](#).

Als Nächstes richten Sie die EC2 Receiver-Amazon-Instance ein.

```
 # The placement group in which your EC2 instance is placed.
 ClusterPlacementGroup:
   Type: AWS::EC2::PlacementGroup
   Properties:
     Strategy: cluster

 # This is required for the EIP if the receiver EC2 instance is in a private subnet.
 # This ENI must exist in a public subnet, be attached to the receiver and be
associated with the EIP.
 ReceiverInstanceNetworkInterface:
   Type: AWS::EC2::NetworkInterface
   Properties:
     Description: Floating network interface
     GroupSet:
       - !Ref InstanceSecurityGroup
     SubnetId: !Ref PublicSubnet

 # An EIP providing a fixed IP address for AWS Ground Station to connect to. Attach it
to the receiver instance created in the stack.
 ReceiverInstanceElasticIp:
   Type: AWS::EC2::EIP
   Properties:
     Tags:
       - Key: Name
         Value: !Join [ "-" , [ "EIP" , !Ref "AWS::StackName" ] ]

 # Attach the ENI to the EC2 instance if using a separate public subnet.
 # Requires the receiver instance to be in a public subnet (SubnetId should be the id
of a public subnet)
 ReceiverNetworkInterfaceAttachment:
```

```
    Type: AWS::EC2::NetworkInterfaceAttachment
    Properties:
      DeleteOnTermination: false
      DeviceIndex: 1
      InstanceId: !Ref ReceiverInstance
      NetworkInterfaceId: !Ref ReceiverInstanceNetworkInterface

  # Associate EIP with the ENI if using a separate public subnet for the ENI.
  ReceiverNetworkInterfaceElasticIpAssociation:
    Type: AWS::EC2::EIPAssociation
    Properties:
      AllocationId: !GetAtt [ReceiverInstanceElasticIp, AllocationId]
      NetworkInterfaceId: !Ref ReceiverInstanceNetworkInterface

  # The EC2 instance that will send/receive data to/from your satellite using AWS
 Ground Station.
  ReceiverInstance:
    Type: AWS::EC2::Instance
    DependsOn: PublicSubnet
    Properties:
      DisableApiTermination: false
      IamInstanceProfile: !Ref GeneralInstanceProfile
      ImageId: !Ref ReceiverAMI
      AvailabilityZone: !Ref AZ
      InstanceType: c5.24xlarge
      KeyName: !Ref EC2Key
      Monitoring: true
      PlacementGroupName: !Ref ClusterPlacementGroup
      SecurityGroupIds:
        - Ref: InstanceSecurityGroup
      SubnetId: !Ref PublicSubnet
      Tags:
        - Key: Name
          Value: !Join [ "-" , [ "Receiver" , !Ref "AWS::StackName" ] ]
      # agentCpuCores list in the AGENT_CONFIG below defines the cores that the AWS
 Ground Station Agent is allowed to run on. This list can be changed to suit your use-
case, however if the agent isn't supplied with enough cores data loss may occur.
      UserData:
        Fn::Base64:
          Fn::Sub:
            - |
              #!/bin/bash
              yum -y update
```

```
              AGENT_CONFIG_PATH="/opt/aws/groundstation/etc/aws-gs-agent-config.json"
              cat << AGENT_CONFIG > "$AGENT_CONFIG_PATH"
              {
                "capabilities": [
                  "arn:aws:groundstation:${AWS::Region}:${AWS::AccountId}:dataflow-
endpoint-group/${DataflowEndpointGroupId}"
                ],
                "device": {
                  "privateIps": [
                    "127.0.0.1"
                  ],
                  "publicIps": [
                    "${EIP}"
                  ],
                  "agentCpuCores": [

 24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,72,73,74,75,76,77,78,79,80,81,8
                  ]
                }
              }
              AGENT_CONFIG

              systemctl start aws-groundstation-agent
              systemctl enable aws-groundstation-agent

              # <Tuning Section Start>
              # Visit the AWS Ground Station Agent Documentation in the User Guide for
 more details and guidance updates

              # Set IRQ affinity with list of CPU cores and Receive Side Scaling mask
              # Core list should be the first two cores (and hyperthreads) on each
 socket
              # Mask set to everything currently
              # https://github.com/torvalds/linux/blob/v4.11/Documentation/networking/
scaling.txt#L80-L96
              echo "@reboot sudo /opt/aws/groundstation/bin/set_irq_affinity.sh '0 1 48
 49' 'ffffffff,ffffffff,ffffffff' >>/var/log/user-data.log 2>&1" >>/var/spool/cron/root

              # Reserving the port range defined in the GS agent ingress address in
 the Dataflow Endpoint Group so the kernel doesn't steal any of them from the GS agent.
 These ports are the ports that the GS agent will ingress data
              # across, so if the kernel steals one it could cause problems ingressing
 data onto the instance.
              echo net.ipv4.ip_local_reserved_ports="42000-50000" >> /etc/sysctl.conf
```

```
              # </Tuning Section End>

              # We have to reboot for linux kernel settings to apply
              shutdown -r now

            - DataflowEndpointGroupId: !Ref DataflowEndpointGroup
              EIP: !Ref ReceiverInstanceElasticIp
```

```
 # The AWS Ground Station Dataflow Endpoint Group that defines the endpoints that AWS
Ground
 # Station will use to send/receive data to/from your satellite.
 DataflowEndpointGroup:
   Type: AWS::GroundStation::DataflowEndpointGroup
   Properties:
     ContactPostPassDurationSeconds: 180
     ContactPrePassDurationSeconds: 120
     EndpointDetails:
       - AwsGroundStationAgentEndpoint:
           Name: !Join [ "-" , [ !Ref "AWS::StackName" , "Downlink" ] ] # needs to
match DataflowEndpointConfig name
           EgressAddress:
             SocketAddress:
               Name: 127.0.0.1
               Port: 55000
           IngressAddress:
             SocketAddress:
               Name: !Ref ReceiverInstanceElasticIp
               PortRange:
                 Minimum: 42000
                 Maximum: 55000
```

Sie benötigen außerdem die entsprechenden Richtlinien, Rollen und Profile, um das elastic network interface (ENI) in Ihrem Konto erstellen AWS Ground Station zu können.

```
 # The security group for your EC2 instance.
 InstanceSecurityGroup:
   Type: AWS::EC2::SecurityGroup
   Properties:
     GroupDescription: AWS Ground Station receiver instance security group.
```

```
      VpcId: !Ref ReceiverVPC
      SecurityGroupEgress:
        - CidrIp: 0.0.0.0/0
          Description: Allow all outbound traffic by default
          IpProtocol: "-1"
      SecurityGroupIngress:
        # To allow SSH access to the instance, add another rule allowing tcp port 22
from your CidrIp
        - IpProtocol: udp
          Description: Allow AWS Ground Station Incoming Dataflows
          ToPort: 50000
          FromPort: 42000
          SourcePrefixListId:
            Fn::FindInMap:
              - PrefixListId
              - Ref: AWS::Region
              - groundstation

  # The EC2 instance assumes this role.
 InstanceRole:
   Type: AWS::IAM::Role
   Properties:
     AssumeRolePolicyDocument:
       Version: "2012-10-17"
       Statement:
         - Effect: "Allow"
           Principal:
             Service:
               - "ec2.amazonaws.com"
           Action:
             - "sts:AssumeRole"
     Path: "/"
     ManagedPolicyArns:
       - arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess
       - arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceforEC2Role
       - arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy
       - arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforSSM
       - arn:aws:iam::aws:policy/AWSGroundStationAgentInstancePolicy
     Policies:
       - PolicyDocument:
           Statement:
             - Action:
                 - sts:AssumeRole
               Effect: Allow
```

```
                Resource: !GetAtt GroundStationKmsKeyRole.Arn
            Version: "2012-10-17"
          PolicyName: InstanceGroundStationApiAccessPolicy

  # The instance profile for your EC2 instance.
  GeneralInstanceProfile:
    Type: AWS::IAM::InstanceProfile
    Properties:
      Roles:
        - !Ref InstanceRole

  # The IAM role that AWS Ground Station will assume to access and use the KMS Key for
 data delivery
  GroundStationKmsKeyRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Statement:
          - Action: sts:AssumeRole
            Effect: Allow
            Principal:
              Service:
                - groundstation.amazonaws.com
            Condition:
              StringEquals:
                "aws:SourceAccount": !Ref AWS::AccountId
              ArnLike:
                "aws:SourceArn": !Sub "arn:${AWS::Partition}:groundstation:
${AWS::Region}:${AWS::AccountId}:mission-profile/*"
          - Action: sts:AssumeRole
            Effect: Allow
            Principal:
              AWS: !Sub "arn:${AWS::Partition}:iam::${AWS::AccountId}:root"

  GroundStationKmsKeyAccessPolicy:
    Type: AWS::IAM::Policy
    Properties:
      PolicyDocument:
        Statement:
          - Action:
              - kms:Decrypt
            Effect: Allow
            Resource: !GetAtt GroundStationDataDeliveryKmsKey.Arn
      PolicyName: GroundStationKmsKeyAccessPolicy
```

```
      Roles:
        - Ref: GroundStationKmsKeyRole

  GroundStationDataDeliveryKmsKey:
    Type: AWS::KMS::Key
    Properties:
      KeyPolicy:
        Statement:
          - Action:
              - kms:CreateAlias
              - kms:Describe*
              - kms:Enable*
              - kms:List*
              - kms:Put*
              - kms:Update*
              - kms:Revoke*
              - kms:Disable*
              - kms:Get*
              - kms:Delete*
              - kms:ScheduleKeyDeletion
              - kms:CancelKeyDeletion
              - kms:GenerateDataKey
              - kms:TagResource
              - kms:UntagResource
            Effect: Allow
            Principal:
              AWS: !Sub "arn:${AWS::Partition}:iam::${AWS::AccountId}:root"
            Resource: "*"
          - Action:
              - kms:Decrypt
              - kms:GenerateDataKeyWithoutPlaintext
            Effect: Allow
            Principal:
              AWS: !GetAtt GroundStationKmsKeyRole.Arn
            Resource: "*"
            Condition:
              StringEquals:
                "kms:EncryptionContext:sourceAccount": !Ref AWS::AccountId
              ArnLike:
                "kms:EncryptionContext:sourceArn": !Sub "arn:
${AWS::Partition}:groundstation:${AWS::Region}:${AWS::AccountId}:mission-profile/*"
          - Action:
              - kms:CreateGrant
            Effect: Allow
```

```
            Principal:
              AWS: !Sub "arn:${AWS::Partition}:iam::${AWS::AccountId}:root"
            Resource: "*"
            Condition:
              ForAllValues:StringEquals:
                "kms:GrantOperations":
                  - Decrypt
                  - GenerateDataKeyWithoutPlaintext
                "kms:EncryptionContextKeys":
                  - sourceArn
                  - sourceAccount
              ArnLike:
                "kms:EncryptionContext:sourceArn": !Sub "arn:
${AWS::Partition}:groundstation:${AWS::Region}:${AWS::AccountId}:mission-profile/*"
              StringEquals:
                "kms:EncryptionContext:sourceAccount": !Ref AWS::AccountId
        Version: "2012-10-17"
      EnableKeyRotation: true
```

AWS Ground Station Konfigurationen

Dieser Abschnitt beschreibt Konfigurationen erstellen die ersten Schritte.

Sie benötigen eine Tracking-Konfiguration, um Ihre Präferenz für die Verwendung von Autotrack festzulegen. Die Auswahl von PREFERRED als Autotrack kann die Signalqualität verbessern, ist aber aufgrund der ausreichenden JPSS-1-Ephemeridenqualität nicht erforderlich, um die Signalqualität zu gewährleisten.

```
  TrackingConfig:
    Type: AWS::GroundStation::Config
    Properties:
      Name: "JPSS Tracking Config"
      ConfigData:
        TrackingConfig:
          Autotrack: "PREFERRED"
```

Basierend auf dem Kommunikationspfad müssen Sie eine Antennen-Downlink-Konfiguration definieren, die den Satellitenanteil repräsentiert, sowie eine Datenfluss-Endpunktkonfiguration, um auf die Datenfluss-Endpunktgruppe zu verweisen, die die Endpunktdetails definiert.

```
 # The AWS Ground Station Antenna Downlink Config that defines the frequency spectrum
used to
 # downlink data from your satellite.
 SnppJpssDownlinkDigIfAntennaConfig:
   Type: AWS::GroundStation::Config
   Properties:
     Name: "SNPP JPSS Downlink WBDigIF Antenna Config"
     ConfigData:
       AntennaDownlinkConfig:
         SpectrumConfig:
           Bandwidth:
             Units: "MHz"
             Value: 100
           CenterFrequency:
             Units: "MHz"
             Value: 7812
           Polarization: "RIGHT_HAND"

 # The AWS Ground Station Dataflow Endpoint Config that defines the endpoint used to
downlink data
 # from your satellite.
 DownlinkDigIfEndpointConfig:
   Type: AWS::GroundStation::Config
   Properties:
     Name: "Aqua SNPP JPSS Terra Downlink DigIF Endpoint Config"
     ConfigData:
       DataflowEndpointConfig:
         DataflowEndpointName: !Join [ "-" , [ !Ref "AWS::StackName" , "Downlink" ] ]
         DataflowEndpointRegion: !Ref AWS::Region
```

AWS Ground Station Missionsprofil

Dieser Abschnitt beschreibt Missionsprofil erstellen die ersten Schritte.

Da Sie nun über die zugehörigen Konfigurationen verfügen, können Sie sie verwenden, um den Datenfluss zu erstellen. Für die übrigen Parameter verwenden Sie die Standardwerte.

```
 # The AWS Ground Station Mission Profile that groups the above configurations to
define how to
```

```
  # uplink and downlink data to your satellite.
  SnppJpssMissionProfile:
    Type: AWS::GroundStation::MissionProfile
    Properties:
      Name: !Sub 'JPSS WBDigIF gs-agent EC2 Delivery'
      ContactPrePassDurationSeconds: 120
      ContactPostPassDurationSeconds: 120
      MinimumViableContactDurationSeconds: 180
      TrackingConfigArn: !Ref TrackingConfig
      DataflowEdges:
        - Source: !Ref SnppJpssDownlinkDigIfAntennaConfig
          Destination: !Ref DownlinkDigIfEndpointConfig
      StreamsKmsKey:
        KmsKeyArn: !GetAtt GroundStationDataDeliveryKmsKey.Arn
      StreamsKmsRole: !GetAtt GroundStationKmsKeyRole.Arn
```

Es zusammensetzen

Mit den oben genannten Ressourcen haben Sie jetzt die Möglichkeit, JPSS-1-Kontakte für die synchrone Datenübermittlung von jedem Ihrer Onboardanbieter aus zu planen. AWS Ground Station AWS Ground Station Standorte

Im Folgenden finden Sie eine vollständige CloudFormation Vorlage, die alle in diesem Abschnitt beschriebenen Ressourcen in einer einzigen Vorlage zusammenfasst, die direkt verwendet werden kann. CloudFormation

Die genannte 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 EC2 Amazon-Instance und die erforderlichen CloudFormation Ressourcen, um DigiF-Direktübertragungs-Rohdaten mit AWS Ground Station Agent zu empfangen.

Falls Aqua, SNPP, JPSS-1/NOAA-20 und Terra nicht in Ihr Konto integriert sind, finden Sie weitere Informationen unter. Satellit an Bord

> **Note**
>
> Sie können auf die Vorlage zugreifen, indem Sie mit gültigen AWS Anmeldeinformationen auf den Amazon S3 S3-Bucket des Kunden zugreifen. Die folgenden Links verwenden einen

regionalen Amazon S3 S3-Bucket. Ändern Sie den `us-west-2` Regionalcode so, dass er die entsprechende Region darstellt, in der Sie den CloudFormation Stack erstellen möchten. Darüber hinaus verwenden die folgenden Anweisungen YAML. Die Vorlagen sind jedoch sowohl im YAML- als auch im JSON-Format verfügbar. Um JSON zu verwenden, ersetzen Sie `.json` beim Herunterladen der Vorlage die `.yml` Dateierweiterung durch.

Verwenden Sie den folgenden Befehl AWS CLI, um die Vorlage mit 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 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 zusätzlichen Ressourcen definiert die Vorlage?

Die `DirectBroadcastSatelliteWbDigIfEc2DataDelivery` Vorlage enthält die folgenden zusätzlichen Ressourcen:

- 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. Dies erfordert, dass SubnetIdauf ein öffentliches Subnetz verwiesen wird.
  - 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 Amazon-Verifizierung für Kontakte — Die Option, Lambda zu verwenden, um ein Überprüfungssystem für Ihre EC2 Amazon-Instance (s) für Kontakte mit SNS-Benachrichtigung einzurichten. Bitte beachten Sie, dass hierfür je nach Ihrer aktuellen Nutzung Gebühren anfallen können.
- Zusätzliche Missionsprofile — Missionsprofile für zusätzliche öffentlich-rechtliche Rundfunksatelliten (Aqua, SNPP und Terra).
- Zusätzliche Antennen-Downlink-Konfigurationen — Antennen-Downlink-Konfigurationen für zusätzliche öffentlich-rechtliche Rundfunksatelliten (Aqua, SNPP und 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 Port zu empfangen, der durch den Datenflussendpunkt definiert ist. Weitere Informationen zum Einrichten einer Datenfluss-Endpunktgruppe finden Sie unter AWS::GroundStation::DataflowEndpointGroup Weitere Informationen zum AWS Ground Station Agenten finden Sie unter Was ist der AWS Ground Station Agent?

Fehlerbehebung

Die folgende Dokumentation kann Ihnen bei der Behebung von Problemen helfen, die bei der Verwendung auftreten können AWS Ground Station.

Themen

- Problembehandlung bei Kontakten, die Daten an Amazon EC2 liefern
- Fehlerbehebung bei FEHLGESCHLAGENEN Kontakten
- Fehlerbehebung bei FAILED_TO_SCHEDULE-Kontakten
- Problembehandlung DataflowEndpointGroups nicht im Zustand GESUND
- Fehlerbehebung bei ungültigen Ephemeriden
- Problembehandlung bei Kontakten, die keine Daten erhalten haben
- Fehlerbehebung bei Telemetrie

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 Ihre Datenfluss-Endpunktanwendung läuft und ob der Stream Ihrer Datenfluss-Endpunktanwendung ordnungsgemäß konfiguriert ist.

> **Note**
>
> DataDefender (DDX) ist ein Beispiel für eine Dataflow-Endpunktanwendung, die derzeit unterstützt wird von AWS Ground Station

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: Stellen Sie sicher, dass Ihre EC2-Instance läuft

Das folgende Verfahren zeigt, wie Sie Ihre Amazon EC2 EC2-Instance in der Konsole finden und sie starten, falls sie nicht läuft.

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 Datenflussanwendung

Wenn Sie den AWS Ground Station Agenten für die Datenübermittlung verwenden, leiten Sie bitte zum Abschnitt AWS Ground Station Troubleshooting-Agent weiter. Andernfalls, wenn Sie die DataDefender (DDX) -Anwendung verwenden, fahren Sie fortthe section called “Schritt 3: Stellen Sie sicher, dass die Dataflow-Anwendung ausgeführt wird”.

Schritt 3: Stellen Sie sicher, dass die Dataflow-Anwendung ausgeführt wird

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

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 DataDefender Weboberfläche aufzurufen. 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. Stellen Sie sicher, dass DataDefender (auch DDX genannt) läuft, indem Sie in der Ausgabe nach einem laufenden Prozess namens ddx suchen. 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
   ```

   Falls ausgeführt DataDefender wird, fahren Sie mit the section called “Schritt 4: Stellen Sie sicher, dass Ihr Dataflow-Anwendungsstream konfiguriert ist” Andernfalls fort und fahren Sie mit dem nächsten Schritt fort.

3. Beginnen Sie DataDefender mit dem unten gezeigten Befehl.

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

Wenn DataDefender es nach der Verwendung des Befehls ausgeführt wird, fahren Sie mit the section called “Schritt 4: Stellen Sie sicher, dass Ihr Dataflow-Anwendungsstream konfiguriert ist” Andernfalls fort und fahren Sie mit dem nächsten Schritt fort.

4. Überprüfen Sie die folgenden Dateien mithilfe der folgenden Befehle, um festzustellen, ob bei der Installation und Konfiguration Fehler aufgetreten sind DataDefender.

```
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 nach DataDefender der Überprüfung Ihrer Amazon VPC-Einstellungen ausgeführt wird, fahren Sie fortthe section called “Schritt 4: Stellen Sie sicher, dass Ihr Dataflow-Anwendungsstream konfiguriert ist”. Wenn das Problem weiterhin besteht, wenden Sie sich an den AWS Support und senden Sie Ihre Protokolldateien mit einer Beschreibung Ihres Problems.

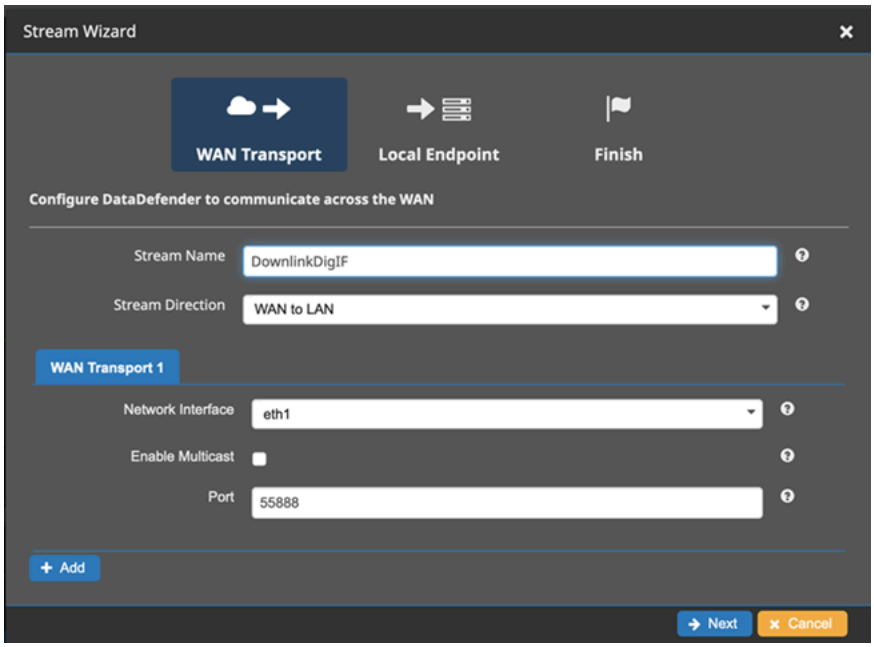
Schritt 4: Stellen Sie sicher, dass Ihr Dataflow-Anwendungsstream konfiguriert ist

1. Greifen Sie in einem Webbrowser auf Ihre DataDefender Weboberfläche zu, indem Sie die folgende Adresse in die Adressleiste eingeben: localhost:8080. Drücken Sie anschließend die Eingabetaste.
2. Wählen Sie im DataDefenderDashboard „Gehe zu Details“.

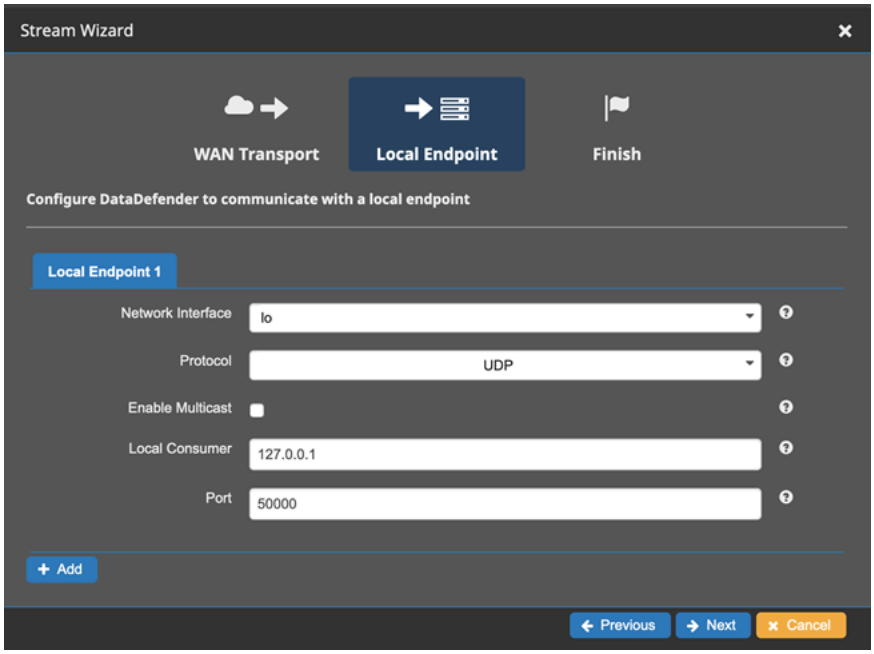
3. Wählen Sie Ihren Stream aus der Liste der Streams aus und wählen Sie Edit Stream (Stream bearbeiten) aus.
4. Führen Sie im Dialogfeld Stream-Assistent die folgenden Schritte aus:

   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, über den Sie Ihre Daten erhalten, DataDefender nachdem Sie sie vom AWS Ground Station Dienst erhalten haben. 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 Ihre Amazon EC2-Instance ordnungsgemäß ausgeführt und konfiguriert DataDefender sind, um Daten von AWS Ground Station zu empfangen. Fahren Sie fort mit the section called “Schritt 5: Stellen Sie sicher, dass Sie über genügend verfügbare IP-Adressen im Subnetz Ihrer Empfänger-Instance (en) verfügen”.

Schritt 5: Stellen Sie sicher, dass Sie über genügend verfügbare IP-Adressen im Subnetz Ihrer Empfänger-Instance (en) verfügen

Das folgende Verfahren zeigt, wie Sie die Anzahl der verfügbaren IP-Adressen in einer Amazon EC2 EC2-Empfängerinstanz in der Konsole ermitteln.

1. Für jede Amazon EC2 EC2-Empfängerinstanz, die für den Kontakt verwendet wurde, den Sie beheben. 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. Suchen Sie in der Amazon EC2-Managementkonsole in der Instance-Zusammenfassung Ihrer Amazon EC2 EC2-Empfänger-Instance nach dem Link Subnet ID und klicken Sie darauf. Dadurch gelangen Sie zur entsprechenden Amazon VPC-Managementkonsole.

3. Wählen Sie das passende Subnetz in der Amazon VPC-Managementkonsole aus und überprüfen Sie die Details Ihres Subnetzes auf Verfügbare Adressen. IPv4 Wenn diese Anzahl nicht mindestens so viele ist wie Datenfluss-Endpunkte, die diese Amazon EC2 EC2-Empfänger-Instance verwenden, gehen Sie wie folgt vor:

   a. Aktualisieren Sie das entsprechende Subnetz Ihrer CloudFormation Vorlage, sodass es die richtige Größe CidrBlockhat. Weitere Informationen zur Subnetzdimensionierung finden Sie unter Subnetz-CIDR-Blöcke.

   b. Stellen Sie Ihren Stack mit Ihrer aktualisierten Vorlage erneut bereit. CloudFormation

Wenn Sie weiterhin Probleme haben, wenden Sie sich an den AWS-Support.

Fehlerbehebung bei FEHLGESCHLAGENEN Kontakten

Ein Kontakt hat den Terminal-Kontaktstatus FAILED, wenn er ein Problem mit Ihrer Ressourcenkonfiguration AWS Ground Station feststellt. Nachfolgend finden Sie die häufigsten Anwendungsfälle, die zu FEHLGESCHLAGENEN Kontakten führen können, sowie Schritte zur Problembehebung.

> **Note**
>
> Diese Anleitung bezieht sich speziell auf den Kontaktstatus FAILED und ist nicht für andere Fehlerstatus wie,, oder AWS_FAILEDAWS_CANCELLEDFAILED_TO_SCHEDULE vorgesehen. Weitere Informationen zum Kontaktstatus finden Sie unter the section called “AWS Ground Station Status der Kontakte”

Anwendungsfälle von Dataflow Endpoint FAILED

Im Folgenden finden Sie eine Liste der häufigsten Anwendungsfälle, die zu einem Kontaktstatus FAILED für Datenflüsse, die auf Datenflussendpunkten basieren, führen können:

- Der Datenfluss-Endpunkt stellt nie eine Verbindung her — Die Verbindung zwischen AWS Ground Station Antenna und Ihrer Dataflow-Endpunktgruppe für einen oder mehrere Datenflüsse wurde nie hergestellt.
- Der Datenfluss-Endpunkt stellt eine verspätete Verbindung her — Die Verbindung zwischen AWS Ground Station Antenna und Ihrer Dataflow-Endpunktgruppe für einen oder mehrere Datenflüsse wurde nach der Startzeit des Kontakts hergestellt.
- Das Subnetz des Dataflow-Endpunkts hat keine verfügbaren IP-Adressen. Die Datenlieferungslösung kann kein ENI in Ihrem privaten Netzwerk erstellen, da im Subnetz der Empfängerinstanz keine IP-Adresse verfügbar ist. AWS Ground Station
- Das Subnetz des Dataflow-Endpunkts ist ungültig — AWS Ground Station die Datenlieferungslösung kann kein ENI in Ihrem privaten Netzwerk erstellen, da nicht auf das bereitgestellte Subnetz zugegriffen werden kann, das in der Dataflow-Endpunktgruppe angegeben ist.

Bei Ausfällen von Datenfluss-Endpunkten 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 Dataflow-Endpunktsoftware während des Kontakts aktiv war und ausgeführt wurde.
- Stellen Sie sicher, dass Sie mindestens eine verfügbare IP-Adresse pro Datenfluss-Endpunkt pro Subnetz der Empfängerinstanz haben.
- Stellen Sie sicher, dass Subnetze, die Ihrer Dataflow-Endpunktgruppe über die in konfigurierten Datenflüsse zugeordnet sind, aktiv und verfügbar bleiben. Amazon VPC einrichten und konfigurieren AWS Ground Station

Spezifischere Schritte zur Fehlerbehebung finden Sie im Abschnitt überProblembehandlung bei Kontakten, die Daten an Amazon EC2 liefern.

AWS Ground Station Anwendungsfälle von Agent FAILED

Im Folgenden finden Sie eine Liste der häufigsten Anwendungsfälle, die zu einem Kontaktstatus FEHLGESCHLAGEN für agentenbasierte Datenflüsse führen können:

- AWS Ground Station Status „Agent nie gemeldet“ — Der Agent, der für die Orchestrierung der Datenübermittlung in Ihrer Dataflow-Endpunktgruppe für einen oder mehrere Datenflüsse verantwortlich ist, hat den Status nie erfolgreich gemeldet. AWS Ground Station Diese Statusaktualisierung sollte innerhalb weniger Sekunden nach dem Ende des Kontakts erfolgen.
- AWS Ground Station Der Agent wurde spät gestartet — Der Agent, der für die Orchestrierung der Datenübermittlung auf Ihrer 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 Agent-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. Problembehandlung bei Kontakten, die Daten an Amazon EC2 liefern

Fehlerbehebung bei FAILED_TO_SCHEDULE-Kontakten

Ein Kontakt endet im Status FAILED_TO_SCHEDULE, wenn ein Problem mit Ihrer Ressourcenkonfiguration oder innerhalb AWS Ground Station des internen Systems festgestellt wird. Ein Kontakt, der im Status FAILED_TO_SCHEDULE endet, bietet optional einen zusätzlichen Kontext. `errorMessage` Informationen zur Beschreibung von Kontakten finden Sie in der API. DescribeContact

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,, oder FAILED vorgesehen. AWS_FAILEDAWS_CANCELLED Weitere Informationen zum Kontaktstatus finden Sie unter the section called “AWS Ground Station Status der Kontakte”

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 existierende 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. Informationen zum Reservieren eines Kontakts finden Sie unter ReserveContact.
- Wenn Sie weiterhin den Status FAILED_TO_SCHEDULE für dieses Missionsprofil erhalten, wenden Sie sich an den AWS-Support

Problembehandlung DataflowEndpointGroups nicht im Zustand GESUND

Im Folgenden sind die Gründe aufgeführt, warum sich Ihre Datenfluss-Endpunktgruppen möglicherweise nicht in einem bestimmten HEALTHY Zustand befinden, sowie die entsprechenden Korrekturmaßnahmen, die Sie ergreifen müssen.

- 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 AWS Ground Station Agent verwenden zur Konfiguration dieser Datei finden Sie in.
- INVALID_IP_OWNERSHIP- Verwenden Sie die DeleteDataflowEndpointGroup API, um die Dataflow-Endpunktgruppe zu löschen, und verwenden Sie dann die CreateDataflowEndpointGroup API, um die Dataflow-Endpunktgruppe mithilfe der IP-Adressen und Ports, die der EC2-Instance zugeordnet sind, neu zu erstellen.
- UNVERIFIED_IP_OWNERSHIP— Die IP-Adresse wurde noch nicht validiert. Die Überprüfung erfolgt regelmäßig, sodass sich das Problem von selbst lösen sollte.
- NOT_AUTHORIZED_TO_CREATE_SLR— Das Konto ist nicht autorisiert, die erforderliche serviceverknüpfte Rolle zu erstellen. Die Schritte zur Fehlerbehebung finden Sie unter Verwenden Sie serviceverknüpfte Rollen für die Ground Station

Fehlerbehebung bei ungültigen Ephemeriden

Wenn Sie Ephemeridendaten auf hochladen AWS Ground Station, durchlaufen sie einen asynchronen Validierungs-Workflow. Wenn die Validierung fehlschlägt, ändert sich der Ephemeridenstatus auf. INVALID Die Fehlermeldung in der DescribeEphemerisAntwort enthält detaillierte Informationen, die Ihnen helfen, das Problem zu identifizieren und zu lösen.

Fehler bei der Validierung von Ephemeriden verstehen

Wenn die Validierung einer Ephemeride fehlschlägt, enthält die DescribeEphemerisAPI-Antwort zwei Felder, die bei der Diagnose des Problems helfen:

errorCode

Ein maschinenlesbarer Code, der den spezifischen Validierungsfehler identifiziert. Dies kann für die programmatische Fehlerbehandlung verwendet werden.

errorMessage

Eine für Menschen lesbare Beschreibung des Validierungsfehlers mit spezifischen Details darüber, was schief gelaufen ist, und Anleitungen zur Behebung des Fehlers.

DescribeEphemerisBeispielantwort für eine ungültige Ephemeride:

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

Häufige Validierungsfehler für TLE-Ephemeriden

Im Folgenden sind häufig Validierungsfehler aufgeführt, die beim Hochladen von TLE-Ephemeriden auftreten:

Die Satelliten-Katalognummer stimmt nicht überein

Fehler: „Die in der Ephemeride enthaltene Satellitenkatalognummer stimmt nicht mit der Satellitenkatalognummer des zugehörigen Satelliten überein“

Lösung: Stellen Sie sicher, dass die ID/satellite NORAD-Katalognummer in Ihren TLE-Leitungen mit der Satellitenkatalognummer Ihres Satelliten übereinstimmt. Verwenden Sie es `00000` für Satelliten ohne zugewiesene Katalognummer.

Ungültiger Mittelwert der Bewegung

Fehler: „Die mittlere Bewegung der bereitgestellten Ephemeride weicht zu stark von der neuesten Referenz-Ephemeride ab“

Lösung: Stellen Sie sicher, dass Ihre TLE-Daten korrekt sind und eine gültige Umlaufbahn darstellen. Die Ground Station verwendet Space-Track-Ephemeriden als Referenz bei der Validierung.

Häufige Validierungsfehler für OEM-Ephemeriden

Im Folgenden sind häufig Validierungsfehler aufgeführt, die beim Hochladen von OEM-Ephemeriden auftreten:

Ungültiger Referenzrahmen

Fehler: „Der REF_FRAME wird nicht unterstützt“

Lösung: Aktualisieren Sie Ihre OEM-Datei, sodass sie einen der unterstützten Referenzrahmen verwendet: EME2000 oder. ITRF2000

Fehlende Pflichtfelder

Fehler: „Metadatenfeld fehlt: INTERPOLATION“

Lösung: Fügen Sie die Felder INTERPOLATION und INTERPOLATION_DEGREE zu Ihrem OEM-Metadatenbereich hinzu. Diese sind erforderlich, um genaue Antennenausrichtungswinkel AWS Ground Station zu erzeugen.

Das Zeitsystem wird nicht unterstützt

Fehler: „Das TIME_SYSTEM wird nicht unterstützt“

Lösung: Stellen Sie sicher, dass Ihre OEM-Datei UTC als Zeitsystem verwendet.

OEM-Version wird nicht unterstützt

Fehler: „Das CCSDS_OEM_VERS wird nicht unterstützt“

Lösung: Stellen Sie sicher, dass Ihre OEM-Datei CCSDS OEM Version 2.0 verwendet.

Häufige Validierungsfehler für Azimut-Elevations-Ephemeriden

Im Folgenden sind häufig Validierungsfehler aufgeführt, die beim Hochladen von Azimut-Elevations-Ephemeriden auftreten:

Fehlende Daten azimuth/elevation

Fehler: „In mindestens einem waren keine TimeAzEl Felder vorhanden AzElSegment“

Lösung: Stellen Sie sicher, dass jedes Segment in Ihren Azimut-Höhendaten mindestens ein Paar mit azimuth/elevation Zeitmarkierungen enthält.

Ungültiger Azimutwinkelbereich (Grad)

Fehler: "AzEl az muss größer oder gleich -180 und kleiner oder gleich 360 Grad sein“

Lösung: Stellen Sie sicher, dass die Azimutwinkel innerhalb von [-180, 360] Grad liegen.

Ungültiger Höhenwinkelbereich (Grad)

Fehler: "AzEl el muss größer oder gleich -90 und kleiner als oder gleich 90 Grad sein“

Lösung: Stellen Sie sicher, dass die Höhenwinkel innerhalb von [-90, 90] Grad liegen.

Ungültiger Azimutwinkelbereich (Radiant)

Fehler: "AzEl az muss größer oder gleich -pi und kleiner oder gleich 2pi Radiant sein“

Lösung: Stellen Sie sicher, dass die Azimutwinkel innerhalb von [-π, 2π] Radiant liegen.

Ungültiger Höhenwinkelbereich (Radiant)

Fehler: "AzEl el muss größer oder gleich -pi/2 und kleiner oder gleich pi/2 Radiant sein“

Lösung: Stellen Sie sicher, dass die Höhenwinkel innerhalb von [-π /2, π /2] Radiant liegen.

Nichtmonotone Zeitwerte

Fehler: „Die TimeAzEl Elemente in a AzElSegment müssen zeitlich in Ordnung sein“

Lösung: Stellen Sie sicher, dass die Zeitwerte in jedem Segment strikt ansteigen.

Segmente sind nicht in der richtigen Reihenfolge

Fehler: "AzElSegments muss vorübergehend in der richtigen Reihenfolge sein“

Lösung: Stellen Sie sicher, dass die Segmente in chronologischer Reihenfolge angeordnet sind.

Überlappende Segmente

Fehler: „Der Zeitbereich mindestens eines Segments überschneidet sich mit anderen Segmentzeitbereichen“

Lösung: Stellen Sie sicher, dass jedes Segment einen eindeutigen, sich nicht überschneidenden Zeitbereich hat. Der Wert `endTime` eines Segments sollte den `startTime` des nächsten Segments nicht überschreiten.

Fehlerbehebungsschritte

Wenn Ihre Ephemeride nicht validiert werden kann, gehen Sie wie folgt vor, um das Problem zu beheben:

1. Rufen Sie DescribeEphemerismit Ihrer Ephemeriden-ID an, um das und abzurufen. `errorCode` `errorMessage`
2. In der Fehlermeldung finden Sie genaue Informationen darüber, welche Validierungsprüfung fehlgeschlagen ist.
3. Korrigieren Sie die festgestellten Probleme in Ihren Ephemeridendaten.
4. Laden Sie eine neue Ephemeride mit den korrigierten Daten hoch mit. CreateEphemeris
5. Überwachen Sie den Status der neuen Ephemeride, bis er den Status erreicht hat. `ENABLED`
6. Löschen Sie die ungültige Ephemeride mit, DeleteEphemeriswenn sie nicht mehr benötigt wird.

Vollständige Fehlercode-Referenz

Die folgenden Abschnitte bieten eine umfassende Zuordnung aller `errorCode` Werte, die zurückgegeben werden können, wenn die Ephemeridenvalidierung fehlschlägt, geordnet nach Kategorien auf hoher Ebene`invalidReason`.

Ungültiger Grund: **`METADATA_INVALID`**

Diese Fehler treten auf, wenn erforderliche Metadatenfelder fehlen, falsch formatiert sind oder Werte in den Ephemeridendaten enthalten, die nicht unterstützt werden.

Fehlercode	Fehlermeldung
MISMATCHED_SATCAT_ID	Die in der TLE-Ephemeride enthaltene Satellitenkatalognummer stimmt nicht mit der Satellitenkatalognummer des zugehörigen Satelliten überein

Fehlercode	Fehlermeldung
OEM_VERSION_UNSUPPORTED	Die `CCSDS_OEM_VERS` im OEM enthaltene Ephemeride wird nicht unterstützt. Unterstützte Werte: [] `2.0`
ORIGINATOR_FEHLT	Das `ORIGINATOR` Header-Feld fehlt in der OEM-Ephemeride
CREATION_DATE_MISSING	Das `CREATION_DATE` Header-Feld fehlt in der OEM-Ephemeride
OBJECT_NAME_MISSING	Das `OBJECT_NAME` Metadatenfeld fehlt in der OEM-Ephemeride
OBJECT_ID_MISSING	Das `OBJECT_ID` Metadatenfeld fehlt in der OEM-Ephemeride
REF_FRAME_UNSUPPORTED	Die `REF_FRAME` im OEM enthaltene Ephemeride wird nicht unterstützt. Unterstützte Werte: [`EME2000`,] `ITRF2000`
REF_FRAME_EPOCH_UNSUPPORTED	Das `REF_FRAME_EPOCH` Metadatenfeld in der OEM-Ephemeride wird nicht unterstützt. Bitte entfernen Sie dieses Feld aus der Ephemeride
TIME_SYSTEM_UNSUPPORTED	Die `TIME_SYSTEM` im OEM enthaltene Ephemeride wird nicht unterstützt. Unterstützte Werte: [] `UTC`
CENTER_BODY_UNSUPPORTED	Die `CENTER_BODY` im OEM enthaltene Ephemeride wird nicht unterstützt. Unterstützte Werte: [] `Earth`
INTERPOLATION_FEHLT	Das `INTERPOLATION` Metadatenfeld fehlt in der OEM-Ephemeride
INTERPOLATION_DEGREE_INVALID	Der Interpolationsgrad in der OEM-Ephemeride muss für die Interpolationsmethode größer als 0 sein
AZ_EL_SEGMENT_LIST_MISSING	Das Feld fehlt `azElSegmentList`

Fehlercode	Fehlermeldung
INSUFFICIENT_TIME_AZ_EL	In mindestens einem waren keine Felder vorhanden `TimeAzElazElSegmentList`

Ungültiger Grund: **`TIME_RANGE_INVALID`**

Diese Fehler treten auf, wenn die Ephemeride ungültige Zeitbereiche enthält, einschließlich Problemen mit start/end Zeiten, Segmentreihenfolge, überlappenden Segmenten oder zeitlichen Inkonsistenzen.

Fehlercode	Fehlermeldung
START_TIME_IN_FUTURE	Die Startzeit der Ephemeride liegt in der future, muss aber in der Vergangenheit liegen
END_TIME_IN_PAST	Die Endzeit von Ephemeride liegt in der Vergangenheit, muss aber in der future liegen
EXPIRATION_TIME_TOO_EARLY	Die angegebene Ablaufzeit liegt vor der Endzeit der Ephemeride
START_TIME_METADAT A_TOO_EARLY	Der `START_TIME` Metadatenwert liegt vor dem frühesten Zeitpunkt in den OEM-Ephemeridendaten
STOP_TIME_METADATA _TOO_LATE	Der `STOP_TIME` Metadatenwert liegt nach dem letzten Zeitpunkt in den OEM-Ephemeridendaten
AZ_EL_SEGMENT_END_ TIME_BEFORE_START_TIME	Der Wert von mindestens einem Datensegment liegt vor dem des Segments `endTimestartTime`
AZ_EL_SEGMENT_TIME S_OVERLAP	Der Zeitbereich mindestens eines Segments überschne idet sich mit anderen Segmentzeitbereichen
AZ_EL_SEGMENTS_OUT _OF_ORDER	Die Segmente sind nicht zeitlich geordnet

Fehlercode	Fehlermeldung
TIME_AZ_EL_ITEMS_OUT_OF_ORDER	Die Artikel innerhalb von müssen zeitlich in Ordnung `TimeAzEl`sein `AzElSegment`
AZ_EL_SEGMENT_REFERENCE_EPOCH_INVALID	Die Referenzepoche für ein Segment ist ungültig oder falsch formatiert
AZ_EL_SEGMENT_START_TIME_INVALID	Die Startzeit im gültigen Zeitbereich eines Segments beginnt nicht nach dem ersten Segment
AZ_EL_SEGMENT_END_TIME_INVALID	Die Endzeit im gültigen Zeitbereich eines Segments endet nicht nach dem letzten Segment
AZ_EL_SEGMENT_VALID_TIME_RANGE_INVALID	Der gültige Zeitbereich für ein Segment ist ungültig
AZ_EL_SEGMENT_END_TIME_TOO_LATE	Die Endzeit eines Segments überschreitet die maximal zulässige Dauer aus der Referenzepoche
AZ_EL_TOTAL_DURATION_EXCEEDED	Die Gesamtdauer aller Segmente überschreitet die maximal zulässige Zeigewinkeldauer

Ungültiger Grund: **`TRAJECTORY_INVALID`**

Diese Fehler treten auf, wenn die Ephemeride ungültige Flugbahndaten enthält, einschließlich Problemen mit Bahnparametern, Winkelbereichen oder Einheiten.

Fehlercode	Fehlermeldung
MEAN_MOTION_INVALID	Die mittlere Bewegung der bereitgestellten TLE-Ephemeride unterscheidet sich zu stark von der neuesten Referenz-Ephemeride. Hinweis: Die Ground Station verwendet Space-Track-Ephemeriden als Referenz bei der Validierung
TIME_AZ_EL_AZ_RADIAN_RANGE_INVALID	AzEl `az`muss größer oder gleich -π und kleiner oder gleich 2π Radiant sein

Fehlercode	Fehlermeldung
TIME_AZ_EL_EL_RADIAN_RANGE_INVALID	AzEl `el`muss größer oder gleich -π /2 und kleiner oder gleich π /2 Radiant sein
TIME_AZ_EL_AZ_DEGREE_RANGE_INVALID	AzEl `az`muss größer oder gleich -180 und kleiner oder gleich 360 Grad sein
TIME_AZ_EL_EL_DEGREE_RANGE_INVALID	AzEl `el`muss größer oder gleich -90 Grad und kleiner oder gleich 90 Grad sein
TIME_AZ_EL_ANGLE_UNITS_INVALID	Ungültige Winkeleinheiten AzEl

Ungültiger Grund: **KMS_KEY_INVALID**

Diese Fehler treten auf, wenn Probleme mit dem AWS Key Management Service (KMS) -Schlüssel auftreten, der zur Verschlüsselung der Ephemeridendaten verwendet wird.

Fehlercode	Fehlermeldung
INSUFFIZIENTE_KMS_PERMISSIONS	Die Ground Station verfügt nicht über ausreichende Berechtigungen, um auf den KMS-Schlüssel dieser Ephemeride zuzugreifen

Ungültiger Grund: **VALIDATION_ERROR**

Diese Fehler treten auf, wenn allgemeine Validierungsprobleme mit den Ephemeridendaten auftreten, die nicht in die anderen spezifischen Kategorien fallen.

Fehlercode	Fehlermeldung
INTERNAL_ERROR	Bei der Ephemeridenvalidierung ist ein interner Fehler aufgetreten

Fehlercode	Fehlermeldung
FILE_FORMAT_INVALID	Das Ephemeridendateiformat ist ungültig oder beschädigt. Stellen Sie sicher, dass die Datei dem erwarteten Format für den Ephemeridentyp entspricht

Problembehandlung bei Kontakten, die keine Daten erhalten haben

Es ist möglich, dass ein Kontakt erfolgreich erscheint, aber dennoch keine Daten erhalten hat. Dies kann bedeuten, dass Sie leere PCAP-Dateien oder gar keine PCAP-Dateien erhalten, wenn Sie die S3-Datenübermittlung verwenden. Dies kann aus einer Reihe von Gründen geschehen. Im Folgenden werden einige der Ursachen und ihre Behebung erläutert.

Falsche Downlink-Konfiguration

Jedem Kontakt, der Daten von einem Satelliten empfängt, ist ein Antennen-Downlink-Config oder Antennen-Downlink-Demod-Decode-Config zugeordnet. Wenn die angegebene Konfiguration nicht mit dem Signal übereinstimmt, das von einem Satelliten übertragen AWS Ground Station wird, kann das übertragene Signal nicht empfangen werden. Dies führt dazu, dass keine Daten von empfangen werden AWS Ground Station.

Um dieses Problem zu beheben, stellen Sie bitte sicher, dass die von Ihnen verwendeten Konfigurationen mit dem von Ihrem Satelliten übertragenen Signal übereinstimmen. Stellen Sie beispielsweise sicher, dass Sie die richtigen Mittenfrequenz, Bandbreite, Polarisation und, falls erforderlich, die Demodulations- und Decodierungsparameter eingestellt haben.

Satellitenmanöver

Es kann vorkommen, dass ein Satellit ein Manöver durchführt, bei dem einige seiner Kommunikationssysteme vorübergehend deaktiviert werden. Das Manöver kann auch die Position des Satelliten am Himmel erheblich verändern. AWS Ground Station kann kein Signal von einem Satelliten empfangen, der kein Signal sendet, oder wenn die verwendete Ephemeride dazu führt, dass die AWS Ground Station Antenne auf eine Stelle am Himmel zeigt, an der der Satellit nicht präsent ist.

Wenn Sie versuchen, mit einem von der NOAA betriebenen öffentlichen Rundfunksatelliten zu kommunizieren, finden Sie möglicherweise auf der Seite mit den NOAA-Satellitenwarnmeldungen

eine Meldung, die einen Ausfall oder ein Manöver beschreibt. Die Nachricht kann einen Zeitplan enthalten, wann die Datenübertragung voraussichtlich wieder aufgenommen wird, oder dieser kann in einer nachfolgenden Nachricht veröffentlicht werden.

Wenn Sie mit Ihren eigenen Satelliten kommunizieren, liegt es in Ihrer Verantwortung, Ihren Satellitenbetrieb zu verstehen und zu verstehen, wie sich dies auf die Kommunikation mit Ihnen auswirken könnte AWS Ground Station. Wenn Sie ein Manöver durchführen, das sich auf die Flugbahn des Satelliten auswirkt, kann dies die Bereitstellung aktualisierter benutzerdefinierter Ephemeridendaten beinhalten. Weitere Informationen zur Bereitstellung benutzerdefinierter Ephemeridendaten finden Sie unter. Verstehe, wie AWS Ground Station Ephemeriden verwendet werden

AWS Ground Station Ausfall

Wenn AWS Ground Station ein Kontakt fehlschlägt oder storniert AWS Ground Station wird, wird der Kontaktstatus auf AWS_FAILED, oder gesetzt. AWS_CANCELLED Weitere Informationen zum Kontaktlebenszyklus finden Sie unterVerstehen Sie den Lebenszyklus von Kontakten. In einigen Fällen AWS Ground Station kann ein Fehler auftreten, der verhindert, dass Daten an Ihr Konto übermittelt werden, der Kontakt jedoch nicht den AWS_CANCELLEDStatus AWS_FAILEDOder hat. In diesem Fall AWS Ground Station sollten Sie ein kontospezifisches Ereignis in Ihrem AWS Health-Dashboard veröffentlichen. Weitere Informationen zum AWS Health-Dashboard finden Sie im AWS Health-Benutzerhandbuch.

Fehlerbehebung bei Telemetrie

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme mit Telemetrie zu beheben.

Häufig auftretende Probleme bei der Einrichtung

IAM-Berechtigungsfehler

Symptome

Wenn Sie aufrufen`CreateConfig`, um eine zu erstellen TelemetrySinkConfig, erhalten Sie eine Fehlermeldung:

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

Ursachen

- Die in der angegebene IAM-Rolle TelemetrySinkConfig verfügt nicht über die erforderlichen Berechtigungen, um in den Kinesis Data Streams Streams-Stream zu schreiben.
- Die Vertrauensrichtlinie für die IAM-Rolle erlaubt es nicht, die Rolle AWS Ground Station zu übernehmen.
- Der Kinesis Data Streams Streams-Stream-ARN in der TelemetrySinkConfig ist falsch oder der Stream ist nicht vorhanden.

Lösungen

1. Stellen Sie sicher, dass die IAM-Rolle existiert und über die richtigen Berechtigungen verfügt. Überprüfen Sie Schritt 2: Erstellen Sie ein TelemetrySinkConfig und stellen Sie sicher, dass alle Schritte befolgt wurden.
2. Prüfen Sie, ob das Ihre IAM-Rolle übernehmen AWS Ground Station kann:

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

   Vergewissern Sie sich, dass die Vertrauensrichtlinie einen vertrauenswürdigen Dienstprinzipal beinhaltet`groundstation.amazonaws.com`.
3. Stellen Sie sicher, dass die IAM-Rolle über die erforderlichen Kinesis-Berechtigungen verfügt:

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

   Stellen Sie sicher, dass die Richtlinie`kinesis:DescribeStream`,`kinesis:PutRecord`, und `kinesis:PutRecords` Berechtigungen für Ihren Stream beinhaltet.
4. Stellen Sie sicher, dass der Kinesis Data Streams Streams-Stream vorhanden ist und der ARN korrekt ist:

   ```
   aws kinesis describe-stream \
       --stream-name your-stream-name \
       --region us-east-2
   ```
5. Wenn Sie eine vom Kunden verwaltete Verschlüsselung verwenden, stellen Sie sicher, dass die IAM-Rolle über die `kms:GenerateDataKey` Berechtigung für Ihren Schlüssel verfügt. AWS KMS

PassRole Berechtigungsfehler

Symptome

Wenn Sie anrufen`CreateConfig`, erhalten Sie die Fehlermeldung, dass Sie nicht berechtigt sind, die IAM-Rolle weiterzugeben.

Lösung

Stellen Sie sicher, dass Ihr IAM-Benutzer oder Ihre IAM-Rolle über die `iam:PassRole` Berechtigung für die Telemetrie-IAM-Rolle verfügt. Fügen Sie Ihrem Benutzer oder Ihrer Rolle die folgende Richtlinie hinzu:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetRole",
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::99999999999:role/your-stream-name"
    }
  ]
}
```

Probleme mit der Kinesis Data Streams Streams-Stream-Konfiguration

Symptome

Die Telemetrieübertragung schlägt fehl oder ist unterbrochen.

Ursachen

- Der Kinesis Data Streams Streams-Stream hat nicht genügend Kapazität für den Telemetriedurchsatz.
- Der Stream wird von anderen Anwendungen verwendet, was zu einer Schreibdrosselung führt.

Lösungen

1. Überprüfen Sie den Stream-Status:

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

2. Überwachen Sie mithilfe CloudWatch von Metriken die Schreibdrosselung:

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

3. Wenn eine Drosselung erkannt wird, sollten Sie Folgendes berücksichtigen:

   - Umschalten in den On-Demand-Kapazitätsmodus für die automatische Skalierung.
   - Verwendung eines dedizierten Streams für die AWS Ground Station Telemetrie.
   - Wenn Sie den Bereitstellungsmodus verwenden, erhöhen Sie die Anzahl der Shards.

Probleme bei der Telemetrieübertragung

Es werden keine Telemetriedaten angezeigt

Symptome

Nachdem Sie einen Kontakt mit einem telemetriefähigen Missionsprofil geplant haben, werden keine Telemetriedaten in Ihrem Kinesis Data Streams Streams-Stream angezeigt.

Mögliche Ursachen und Lösungen

Für das Missionsprofil ist Telemetrie nicht aktiviert

Stellen Sie sicher, dass das für den Kontakt verwendete Missionsprofil Folgendes enthält: `telemetrySinkConfigArn`

```
aws groundstation get-mission-profile \
```

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

Überprüfen Sie die Ausgabe für das `telemetrySinkConfigArn` Feld. Wenn es nicht vorhanden ist, ist Telemetrie im Missionsprofil nicht aktiviert.

Problem mit den IAM-Rollenberechtigungen

Lesen Sie die Schritte zur Fehlerbehebung bei IAM-Berechtigungen unter. IAM-Berechtigungsfehler

Der Kinesis Data Streams Streams-Stream ist nicht vorhanden oder befindet sich in der falschen Region

Stellen Sie sicher, dass der Stream in der richtigen Region vorhanden ist:

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

Der Kontakt hat noch nicht begonnen

Die Telemetrieübertragung beginnt mit der Startzeit des Kontakts. Überprüfen Sie, ob der Kontakt gestartet wurde, indem Sie den Kontaktstatus überprüfen:

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

Intermittierende Telemetriedaten

Symptome

Telemetriedaten werden uneinheitlich mit Lücken oder fehlenden Datensätzen geliefert.

Mögliche Ursachen

- Probleme mit der Stream-Kapazität oder Drosselung von Kinesis Data Streams. Siehe Probleme mit der Kinesis Data Streams Streams-Stream-Konfiguration.
- Probleme mit der Netzwerkverbindung zwischen AWS Ground Station und Ihrem Kinesis Data Streams Streams-Stream.

Lösungen

- Überwachen Sie die Stream-Metriken von Kinesis Data Streams auf CloudWatch Drosselung oder Fehler.
- Stellen Sie sicher, dass Ihr Stream den On-Demand-Kapazitätsmodus verwendet oder über ausreichend bereitgestellte Kapazität verfügt.
- Verwenden Sie einen dedizierten Stream für die AWS Ground Station Telemetrie, um Konflikte mit anderen Anwendungen zu vermeiden.

Probleme mit dem Datenformat

Fehler bei der JSON-Analyse

Symptome

In Ihrer Anwendung treten Fehler auf, wenn Telemetriedatensätze als JSON analysiert werden.

Lösungen

- Überprüfen Sie die Base64-Dekodierung — Daten im Kinesis Data Streams Streams-Stream sind Base64-codiert. Stellen Sie sicher, dass Sie die Daten dekodieren, bevor Sie sie als JSON analysieren. Weitere Informationen finden Sie unter Daten aus dem Kinesis Data Streams Streams-Stream lesen.
- Auf leere Datensätze prüfen — beim Erstellen eines AWS Ground Station werden möglicherweise leere Validierungsdatensätze gesendet. TelemetrySinkConfig Ihre Anwendung sollte leere oder falsch formatierte Datensätze ordnungsgemäß behandeln.
- Implementieren Sie versionsbewusstes Parsing — Analysieren Sie zuerst die `telemetryVersion` Felder, und `telemetryTypeAndVersiontelemetryType`, um das passende Schema für jeden Datensatz zu ermitteln.

Unbekannte Telemetrietypen oder Versionen

Symptome

Ihre Anwendung stößt auf Telemetrietypen oder Versionen, die sie nicht erkennt.

Lösung

Dieses Verhalten ist zu erwarten, da im Laufe der Zeit möglicherweise neue Telemetrietypen und Schemaversionen eingeführt werden. Ihre Bewerbung sollte:

- Protokollieren Sie unbekannte Typen und Versionen zur Überwachung.
- Setzen Sie die Verarbeitung bekannter Typen und Versionen fort.
- Implementieren Sie eine elegante Behandlung für unbekannte Schemas.

Weitere Hinweise zur Schemaversionierung finden Sie unter. Versionierung und Weiterentwicklung von Schemas

Hilfe erhalten

Wenn Sie nach dem Ausführen der Schritte zur Fehlerbehebung weiterhin Probleme haben, wenden Sie sich an den AWS Support.

Informationen, die Sie bereitstellen müssen

Wenn Sie sich an den Support wenden, geben Sie die folgenden Informationen an:

- Kontakt, bei dem IDs Probleme aufgetreten sind
- Verwendete Missionsprofil-ID
- TelemetrySinkConfig ARN
- Kinesis Data Streams Streams-Stream-ARN
- ARN der IAM-Rolle und angehängte Richtlinien
- Fehlermeldungen aus CloudWatch Logs oder Ihrer Anwendung
- Zeitstempel, wann Probleme aufgetreten sind
- Schritte zur Fehlerbehebung wurden bereits unternommen

Allgemeine AWS Ground Station Unterstützung finden Sie im AWS Ground Station Benutzerhandbuch.

Kontingente und -Einschränkungen

Sie können die unterstützten Regionen, die zugehörigen Endpunkte und Kontingente unter Endpunkte und Kontingente einsehen AWS Ground Station .

Sie können die Service-Quotas-Konsole, die AWS -API und die AWS -CLI verwenden, um Kontingenterhöhungen anzufordern, wenn erforderlich.

Bedingungen für den Service

Die AWS Ground Station Servicebedingungen finden Sie in den AWS-Servicebedingungen.

Dokumentenverlauf für das AWS Ground Station Benutzerhandbuch

In der folgenden Tabelle werden die wichtigen Änderungen in den einzelnen Versionen des AWS Ground Station Benutzerhandbuchs beschrieben.

Änderung	Beschreibung	Datum
Aktualisierung der Dokumentation	Der CancelContact API wurden zusätzliche Funktionen hinzugefügt, die Informationen zu diesen Funktionen und den Auswirkungen auf die Messung enthalten. Weitere Informationen finden Sie unter Grundlegendes zur Kontaktmessung.	10. Dezember 2025
Aktualisierung der Dokumentation	Es wurde klargestellt, dass CloudWatch Messwerte in der Region gesendet werden, die der Bodenstation des Kontakts zugeordnet ist. Fehlerhafte Links wurden behoben.	2. Dezember 2025
Die AWS verwaltete Richtlinie wurde aktualisiert	AWS Ground Station hat die verwaltete Richtlinie `AWSGroundStationAgentInstancePolicy` aktualisiert und enthält nun zusätzliche Berechtigungen für das Abrufen von Aufgabenantworten URLs. Weitere Informationen finden Sie unter AWS Ground Station	13. November 2025

	Aktualisierungen der AWS verwalteten Richtlinien.	
Neue Funktion	Das Benutzerhandbuch wurde aktualisiert und enthält nun auch Azimut-Elevations-Ephemeriden. Weitere Informationen finden Sie unter Bereitstellen von Azimut-Elevations-Ephemeridendaten	22. Oktober 2025
Aktualisierung der Dokumentation	Für die regionsübergreifende Datenbereitstellung sind keine speziellen Konfigurationen oder Genehmigungen mehr erforderlich. Weitere Informationen finden Sie unter Verwenden Sie die regionsübergreifende Datenübermittlung.	11. September 2025
Aktualisierung der Dokumentation	Es wurde eine Klarstellung zur Kontaktnutzung konfigurierter Ressourcen hinzugefügt.	4. April 2025
Neue Funktion	Das Benutzerhandbuch wurde um einen AWS Ground Station digitalen Zwilling erweitert.	6. August 2024
Aktualisierung der Dokumentation	Viele Abschnitte des Benutzerhandbuchs wurden aktualisiert, darunter neue Diagramme, Beispiele und mehr.	18. Juli 2024
Aktualisierung der Dokumentation	RSS-Feed zum Benutzerhandbuch hinzugefügt.	18. Juli 2024

Aktualisierung der Dokumentation	Teilen Sie das AWS Ground Station Agent-Benutzerhandbuch in ein separates Benutzerhandbuch auf.	18. Juli 2024
Neue Funktion	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 den Agenten wurde hinzugefügt.	21. Februar 2024
Vorlagen-Update	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 in der AWS Ground Station Konsole angezeigt werden soll.	26. Juli 2023
Neue Funktion	Das AWS Ground Station Agenten-Benutzerhandbuch für die Veröffentlichung von Wideband DigIF Data Delivery wurde hinzugefügt.	12. April 2023
Neue verwaltete Richtlinie AWS	AWS Ground Station hat eine neue Richtlinie mit dem Namen hinzugefügt AWSGroundStationAgentInstancePolicy.	12. April 2023
Neue Funktion	Das Benutzerhandbuch für die Veröffentlichung von CPE Preview wurde aktualisiert.	9. November 2022
Neue AWS verwaltete Richtlinie	AWS Ground Station hat die AWSService RoleForGroundStationDataflowEndpointGroup service-linked-role (SLR) hinzugefügt, die eine neue Richtlinie mit dem Namen AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy enthält.	02. November 2022

Neue Funktion	Das Benutzerhandbuch wurde aktualisiert und umfasst nun auch die Integration mit AWS CLI.	17. April 2020
Neue Funktion	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
Neue Funktion	Das Benutzerhandbuch wurde aktualisiert, um die regionsübergreifende Datenzustellung einzuschließen.	5. Februar 2020
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 zur 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 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.