사용자 가이드

AWS Ground Station

AWS Ground Station: 사용자 가이드

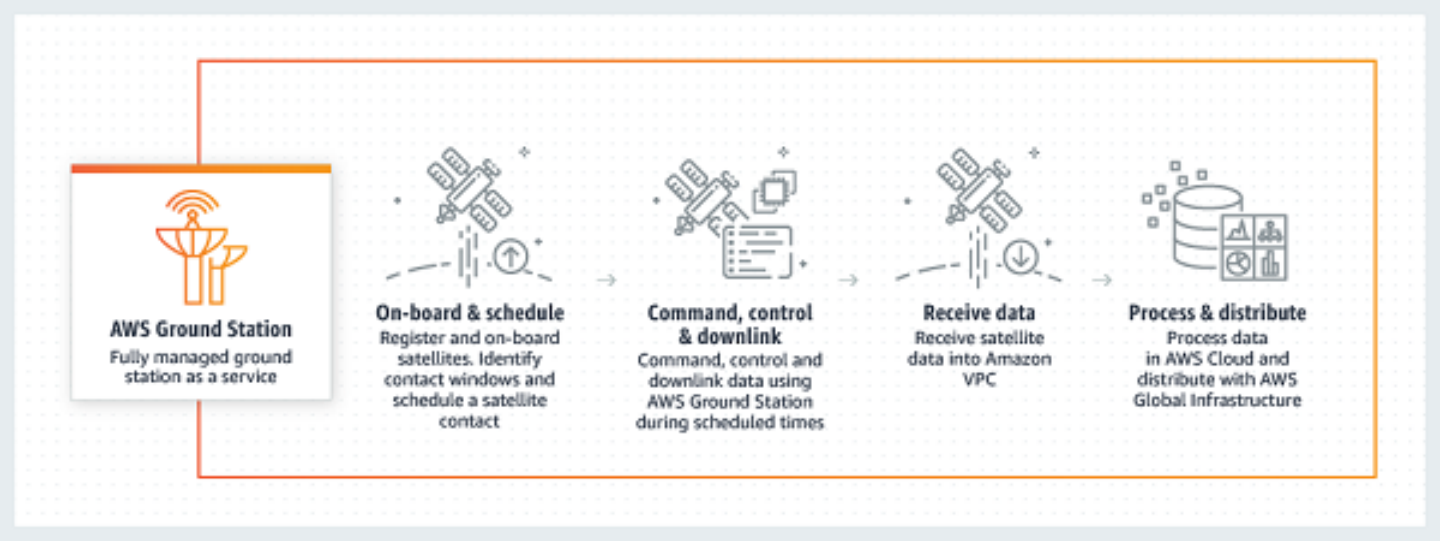
Table of Contents

무엇입니까 AWS Ground Station?

AWS Ground Station 글로벌 인프라 전반에 걸쳐 안전하고 빠르며 예측 가능한 위성 통신을 제공하는 완전 관리형 서비스입니다. 를 사용하면 더 이상 자체 그라운드 스테이션 인프라를 구축, 관리 또는 확장할 필요가 없습니다. AWS Ground Station AWS Ground Station 자체 지상국을 구축, 운영 및 확장하는 데 리소스를 소비하는 대신 위성 데이터를 수집하는 새로운 애플리케이션을 혁신하고 빠르게 실험하는 데 집중할 수 있습니다.

지연 시간이 짧고 대역폭이 높은 글로벌 광섬유 네트워크를 사용하면 AWS 안테나 시스템에서 수신한 지 몇 초 만에 위성 데이터 처리를 시작할 수 있습니다. 이를 통해 몇 초 만에 원시 데이터를 처리된 정보 또는 분석된 지식으로 전환할 수 있습니다.

일반 사용 사례



AWS Ground Station 인공위성과 양방향으로 통신할 수 있으며 다음과 같은 사용 사례를 지원합니다.

- 다운링크 데이터 — 인공위성으로부터 데이터를 수신하여 X-대역 및 S-대역 주파수를 전송하여 Amazon EC2 인스턴스에 실시간 (VITA-49 형식) 으로 전송하거나 사용자 계정의 Amazon S3 버킷으로 직접 전송 (형식) 합니다. PCAP 또한 지원되는 변조 및 인코딩 체계를 사용하는 위성의 경우 복조 및 디코딩된 데이터를 수신하거나 원시 디지털 중간 주파수 (DigiF) 샘플 (-49 형식) 중에서 선택할 수 있습니다. VITA
- 업링크 데이터 — 전송할 DigiF 데이터 VITA (-49 형식) 를 전송하여 S-대역 주파수를 수신하는 위성에 데이터와 명령을 보냅니다. AWS Ground Station

- 업링크 에코 — 전송된 신호를 물리적으로 같은 위치에 있는 안테나로 수신하여 우주선으로 전송된 명령을 검증하고 기타 고급 작업을 수행합니다.
- 소프트웨어 정의 라디오 (SDR) /프런트 엔드 프로세서 (FEP) — Amazon 인스턴스에서 실행 가능한 기존 SDR 및/또는 FEP Amazon EC2 인스턴스를 사용하여 실시간으로 데이터를 처리하여 기존 파형을 전송/수신하고 데이터 제품을 생성합니다.
- 원격 측정, 추적 및 명령 (TT&C) — 앞서 나열한 사용 사례를 조합하여 TT&C를 수행하여 위성 플릿을 관리합니다.
- 지역 간 데이터 전송 — 단일 지역의 글로벌 안테나 네트워크를 사용하여 AWS Ground Station여러 개의 동시 연락처를 운영합니다. AWS
- 디지털 트윈 — 프로덕션 안테나 용량을 사용하지 않고도 저렴한 비용으로 테스트 일정 수립, 구성 검증 및 적절한 오류 처리를 수행할 수 있습니다.

다음 단계

다음 단원을 읽고 시작하면 도움이 됩니다.

- 필수 AWS Ground Station 개념을 알아보려면 을 참조하십시오AWS Ground Station 작동 방식.
- 사용할 계정 및 리소스를 설정하는 방법을 AWS Ground Station알아보려면 을 참조하십시오시작하기.
- 프로그래밍 방식으로 사용하려면 AWS Ground StationAWS Ground Station API참조를 참조하십시오. API레퍼런스는 모든 API 작업을 AWS Ground Station 자세히 설명합니다. 또한 지원되는 웹 서비스 프로토콜에 대한 샘플 요청, 응답 및 오류도 제공합니다. 원하는 언어로 또는 AWS SDKan을 AWS CLI사용하여 상호 작용하는 AWS Ground Station코드를 작성할 수 있습니다.

AWS Ground Station 작동 방식

AWS Ground Station 지상 안테나를 작동시켜 위성과의 통신을 용이하게 합니다. 안테나가 수행할 수 있는 물리적 특성을 추상화하여 이를 성능이라고 합니다. 안테나의 물리적 위치와 현재 기능은 섹션에서 참조할 수 있습니다. 위치 사용 사례에 추가 기능, 추가 위치 제공 또는 더 정확한 안테나 위치가 필요한 경우 <aws-groundstation@amazon.com> 으로 문의하십시오.

AWS Ground Station 안테나 중 하나를 사용하려면 특정 위치에 시간을 예약해야 합니다. 이러한 예약을 연락처라고 합니다. 연락을 성공적으로 예약하려면 성공 여부를 확인하기 위한 추가 데이터가 AWS Ground Station 필요합니다.

- 위성이 하나 이상의 위치에 탑재되어 있어야 합니다. 이렇게 하면 요청된 위치에서 다양한 기능을 운영할 수 있는 승인을 받을 수 있습니다.
- 위성에는 유효한 이피머리스 (ephemeris) 가 있어야 합니다. — 이렇게 하면 안테나가 가시선을 확보하고 접촉 중에 위성을 정확하게 가리킬 수 있습니다.
- 유효한 임무 프로필이 있어야 합니다. 이렇게 하면 위성으로 데이터를 수신하고 전송하는 방법을 포함하여 연락처의 작동 방식을 사용자 지정할 수 있습니다. 동일한 차량에 대해 여러 개의 임무 프로필을 활용하여 다양한 작동 자세나 상황에 맞게 서로 다른 연락처를 만들 수 있습니다.

위성 온보딩

위성 AWS Ground Station 온보딩은 데이터 수집, 기술 검증, 스펙트럼 라이센싱, 통합 및 테스트를 포함하는 다단계 프로세스입니다. 가이드의 Satellite 온보딩 섹션에서는 이 프로세스를 안내합니다.

미션 프로필 구성

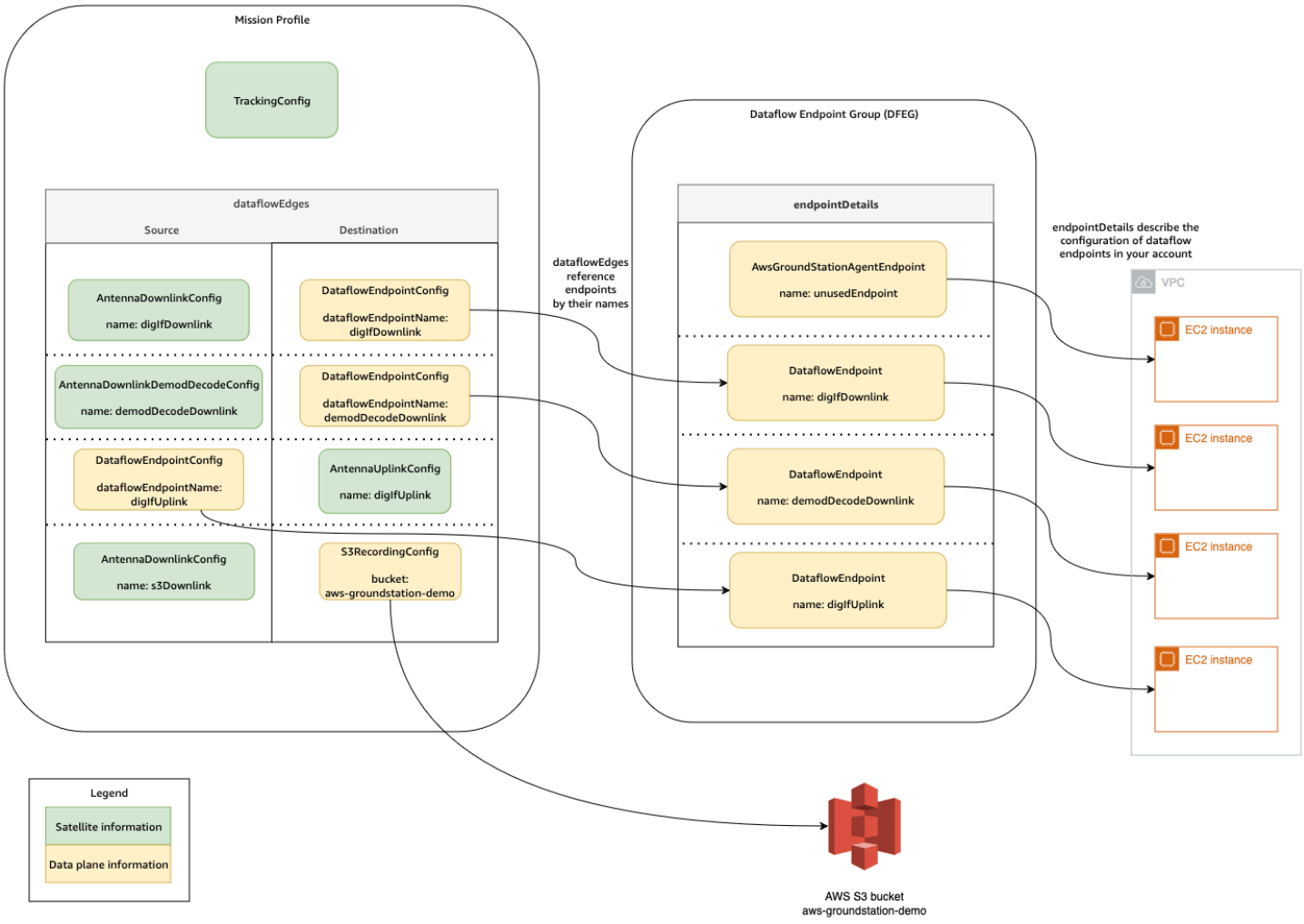
위성 주파수 정보, 데이터 플레인 정보 및 기타 세부 정보가 임무 프로필에 요약되어 있습니다. 미션 프로필은 구성 구성 요소의 모음입니다. 이를 통해 다양한 미션 프로필에서 구성 구성 요소를 사용 사례에 맞게 재사용할 수 있습니다. 임무 프로필은 개별 위성을 직접 참조하지 않고 기술적 능력에 대한 정보만 포함하므로 동일한 구성을 가진 여러 위성에서도 임무 프로필을 재사용할 수 있습니다.

유효한 임무 프로필에는 추적 구성과 하나 이상의 데이터 흐름이 있어야 합니다. 추적 구성에는 연락 중에 추적하기 위한 기본 설정이 지정됩니다. 데이터 흐름 내의 각 구성 쌍은 소스와 대상을 설정합니다. 위성과 작동 모드에 따라 업링크 및 다운링크 통신 경로와 데이터 처리 측면을 나타내는 임무 프로필의 정확한 데이터 흐름 수가 달라집니다.

- 문의 중에 사용할 AmazonVPC, Amazon S3 및 Amazon EC2 리소스를 구성하는 방법에 대한 자세한 내용은 을 참조하십시오데이터 흐름.
- 각 구성의 작동 방식에 대한 자세한 내용은 을 참조하십시오. 구성
- 모든 예상 매개변수에 대한 자세한 내용은 을 참조하십시오. 미션 프로필
- 사용 사례를 지원하기 위해 다양한 임무 프로필을 만드는 방법에 대한 예는 을 참조하십시오미션 프로필 구성 예시.

아래 다이어그램은 미션 프로필 예시와 필요한 추가 리소스를 보여주는 데 사용됩니다. 참고로 이 예시는 유연성을 보여주기 위해 이 임무 프로필에 필요하지 않은 데이터 흐름 엔드포인트 (이름이 지정된 unusedEndpoint) 를 보여줍니다. 이 예시는 다음과 같은 데이터 흐름을 지원합니다.

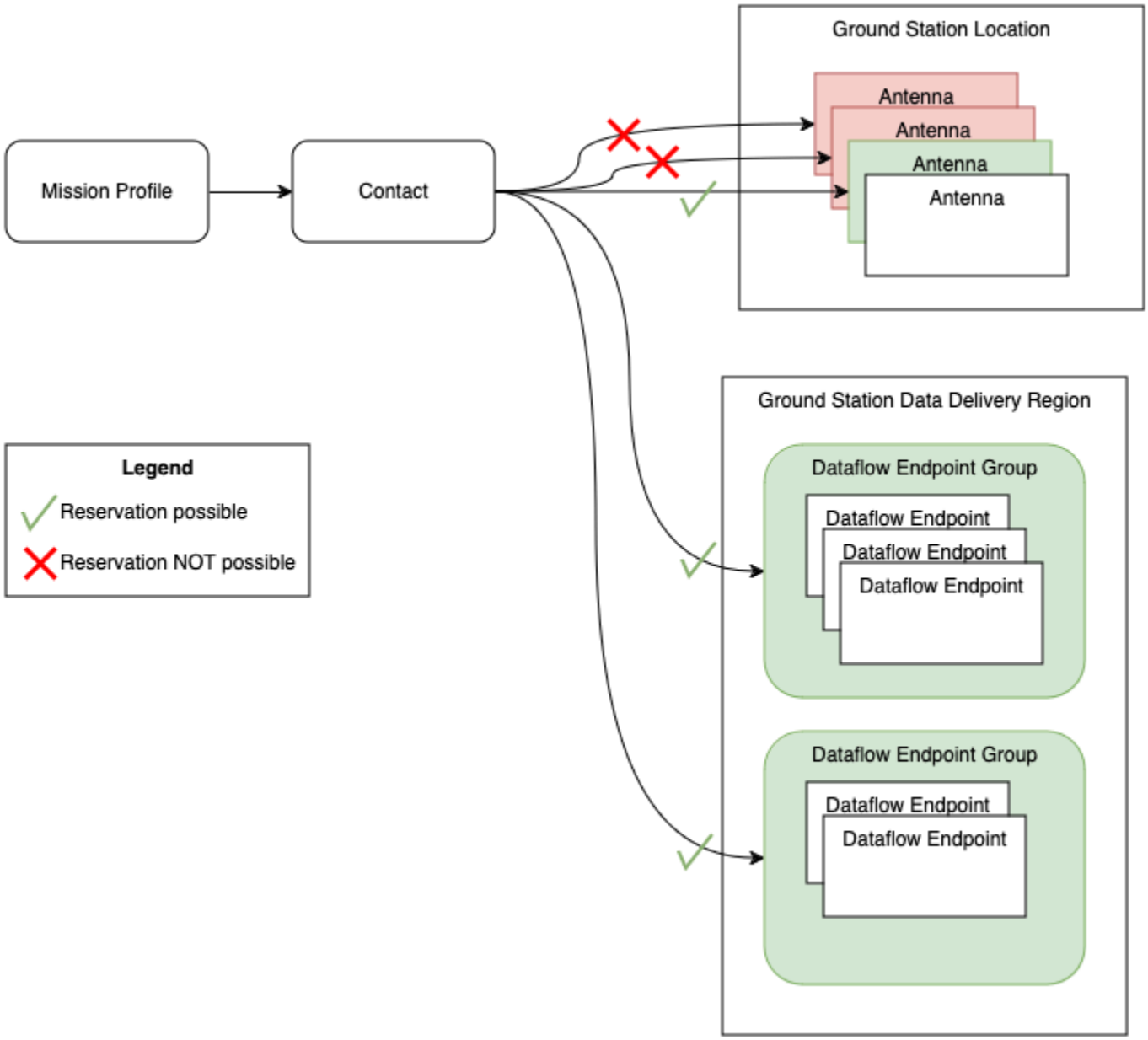
- 관리하는 Amazon EC2 인스턴스로 디지털 중간 주파수 데이터를 동기식으로 다운링크합니다. 이름으로 표시됩니다. digIfDownlink
- Amazon S3 버킷으로 디지털 중간 주파수 데이터를 비동기식으로 다운링크합니다. 버킷 이름으로 표시됩니다. aws-groundstation-demo
- 복조 및 디코딩된 데이터를 관리하는 Amazon EC2 인스턴스로 동기식으로 다운링크합니다. 이름으로 표시됩니다. demodDecodeDownlink
- 관리하는 Amazon EC2 인스턴스의 데이터를 관리형 안테나로 동기식으로 업링크합니다. AWS Ground Station 이름으로 표시됩니다. digIfUplink



연락처 예약

유효한 임무 프로필이 있으면 탑승한 위성과의 연락을 요청할 수 있습니다. 연락처 예약 요청은 비동기로 진행되므로 글로벌 안테나 서비스가 관련된 모든 지역에서 일관된 일정을 맞출 수 있는 시간을 확보할 수 있습니다. AWS 이 과정에서 요청된 지상국 위치에 있는 다양한 안테나를 평가하여 안테나가 사용 가능하고 접촉을 처리할 수 있는지 확인합니다. 이 과정에서 구성된 데이터 흐름 엔드포인트도 평가하여 가용성을 결정합니다. 이 평가가 진행되는 동안에는 연락처 상태가 '켜짐'으로 표시됩니다. SCHEDULING

이 비동기식 예약 프로세스는 요청 후 5분 이내에 완료되지만 일반적으로 1분 이내에 완료됩니다. 예약 시간 중 이벤트 기반 이벤트를 AWS Ground Station 이용한 자동화 모니터링에 대해 검토하십시오.



수행할 수 있고 가용성이 있는 연락처는 연락처로 이어집니다. SCHEDULED 예정된 연락을 통해 연락을 수행하는 데 필요한 자원은 임무 프로필에 정의된 대로 필요한 AWS 지역에 예약되어 있습니다. 연락할 수 없거나 부품을 사용할 수 없는 경우 연락은 FAILEDSCHEDULE_TO_가 됩니다. 디버깅 세부 정보는 FAILED_TO_ 연락처 SCHEDULE 문제 해결 를 참조하십시오.

연락처 실행

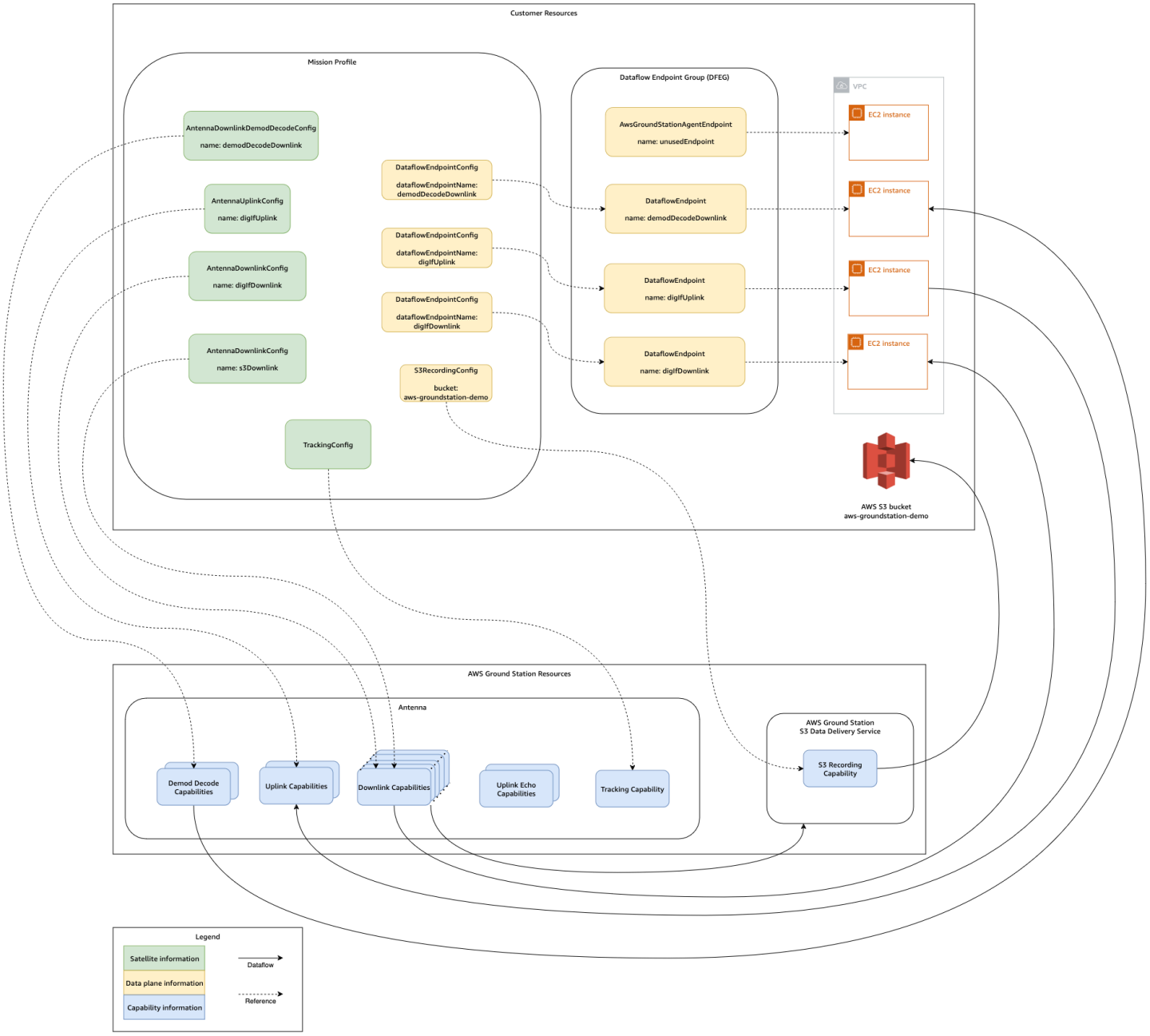
AWS Ground Station 연락처 예약 중에 AWS 관리되는 리소스를 자동으로 조정합니다. 해당하는 경우, 임무 프로필에 정의된 EC2 리소스를 데이터 흐름 엔드포인트로 오케스트레이션할 책임은 귀하에게 있습니다. AWS Ground Station 리소스 오케스트레이션을 자동화하여 비용을 절감하기 위한 AWS

EventBridge 이벤트를 제공합니다. 자세한 내용은 이벤트를 AWS Ground Station 이용한 자동화 섹션을 참조하세요.

연락하는 동안 연락처 성과에 대한 원격 측정이 수신자에게 전달됩니다. AWS CloudWatch 실행 중에 연락처를 모니터링하는 방법에 대한 자세한 내용은 을 참조하십시오모니터링.

다음 다이어그램은 이전 예와 마찬가지로 연락 중에 조정된 리소스와 동일한 리소스를 보여 줍니다.

> **Note**
>
> 이 예제에서는 모든 안테나 기능이 사용된 것은 아닙니다. 예를 들어, 각 안테나에는 다중 주파수와 편파를 지원하는 12개 이상의 안테나 다운링크 기능이 있습니다. AWS Ground Station 안테나에서 사용할 수 있는 각 기능 유형의 수와 지원되는 주파수 및 편파에 대한 자세한 내용은 을 참조하십시오. AWS Ground Station 사이트 기능



연락이 끝나면 연락처의 성과를 평가하고 AWS Ground Station 최종 연락 상태를 결정합니다. 오류가 발견되지 않은 연락처는 COMPLETED연락처 상태가 됩니다. 문의하는 동안 서비스 오류로 인해 데이터 전달 문제가 발생한 연락처는 AWS_ FAILED 상태가 됩니다. 연락처 중에 클라이언트 또는 사용자 오류로 인해 데이터 전달 문제가 발생한 연락처는 FAILED상태가 됩니다. 연락 시간 외의 오류, 즉 사전 통과 또는 사후 통과 중 발생한 오류는 판결 중에 고려되지 않습니다.

자세한 내용은 연락처 라이프사이클 섹션을 참조하세요.

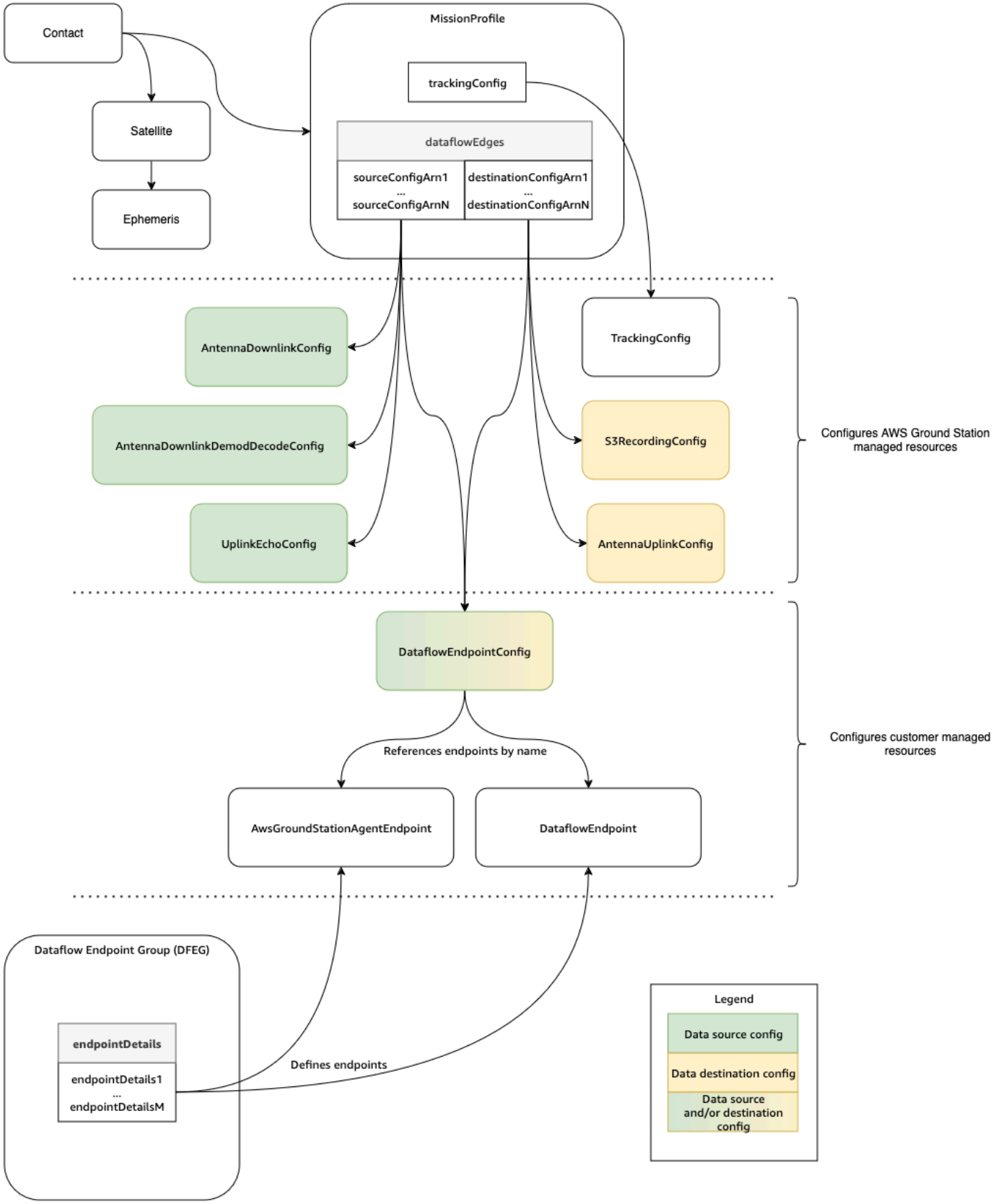
디지털 트윈

의 디지털 트윈 기능을 AWS Ground Station 사용하면 가상 그라운드 스테이션 위치를 기준으로 연락처를 예약할 수 있습니다. 이러한 가상 그라운드 스테이션은 안테나 기능, 사이트 마스크 및 실제 GPS 좌표를 포함하여 프로덕션 그라운드 스테이션을 정확히 복제합니다. 디지털 트윈 기능을 사용하면 프로덕션 그라운드 스테이션에 비해 훨씬 적은 비용으로 접촉 오케스트레이션 워크플로를 테스트할 수 있습니다. 자세한 내용은 AWS Ground Station 디지털 트윈 섹션을 참조하세요.

핵심 구성 요소

이 섹션에서는 AWS Ground Station의 핵심 구성 요소에 대한 자세한 정의를 제공합니다.

다음 다이어그램은 핵심 구성 요소 AWS Ground Station 및 이들 구성 요소가 서로 어떻게 관련되는지를 보여줍니다. 화살표는 구성 요소 간 종속성 방향을 나타내며, 여기서 각 구성 요소는 해당 종속성을 가리킵니다.


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

다음 항목에서는 AWS Ground Station 핵심 구성 요소에 대해 자세히 설명합니다.

주제

미션 프로필

미션 프로파일에는 접촉이 실행되는 방법에 대한 구성과 파라미터가 포함되어 있습니다. 접촉을 예약하거나 이용 가능한 접촉을 검색할 때 사용하려는 미션 프로파일을 제공합니다. 미션 프로파일은 모든 구성을 종합하며 접촉 중에 안테나가 구성되는 방식과 데이터가 이동하는 위치를 정의합니다.

임무 프로필은 동일한 무선 특성을 공유하는 위성 간에 공유할 수 있습니다. 별자리에 대해 수행하려는 최대 동시 접촉을 제한하기 위해 추가 데이터 흐름 엔드포인트 그룹을 생성할 수 있습니다.

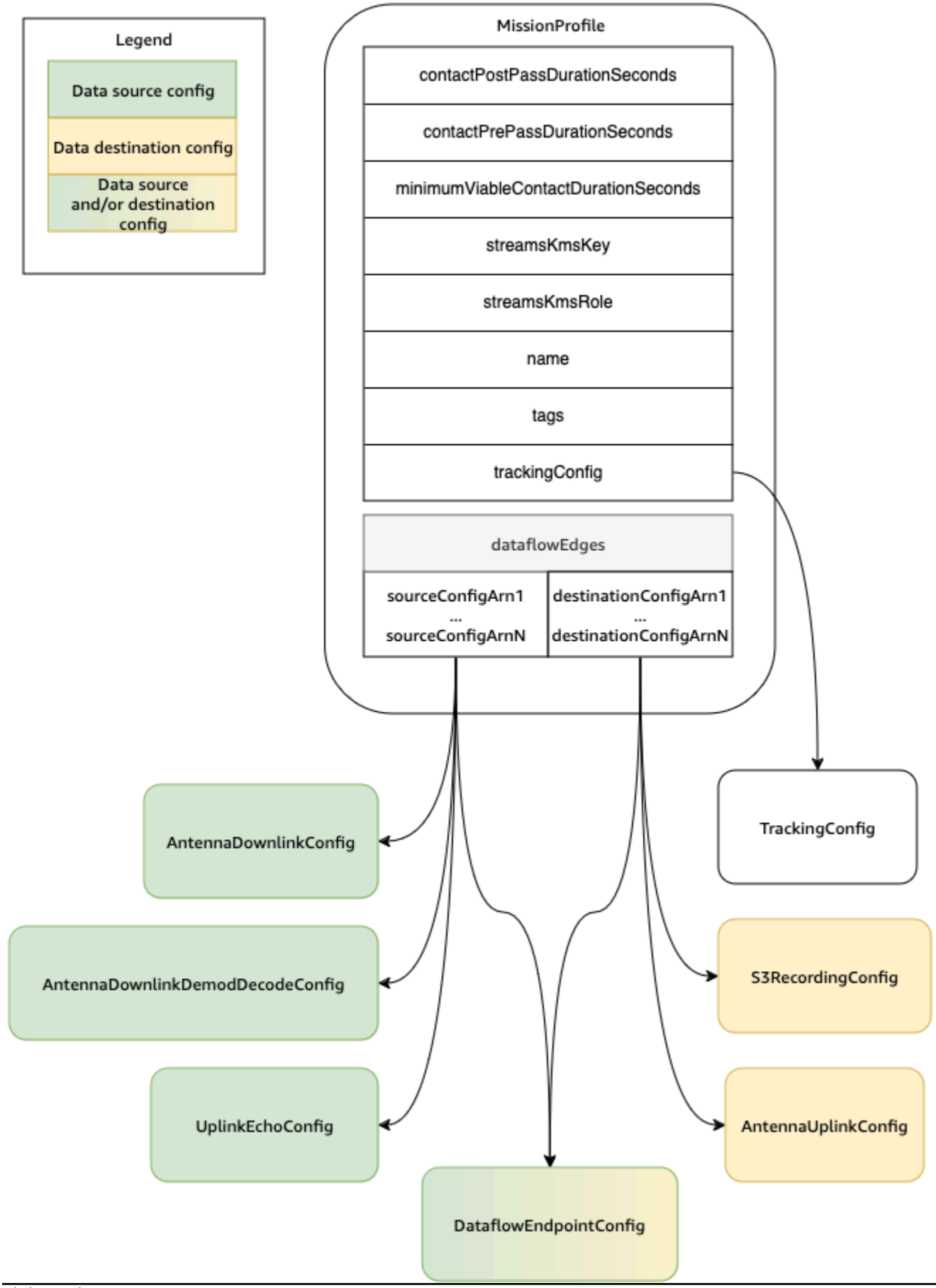
추적 구성은 임무 프로필 내에서 고유한 필드로 지정됩니다. 추적 구성은 연락 중에 프로그램 추적 및 자동 추적 사용에 대한 기본 설정을 지정하는 데 사용됩니다. 자세한 내용은 추적 구성 단원을 참조하십시오.

다른 모든 구성은 미션 프로필 `dataflowEdges` 필드에 포함되어 있습니다. 이러한 구성은 각각 데이터를 보내거나 받을 수 있는 AWS Ground Station 관리형 리소스 및 관련 구성을 나타내는 데이터 흐름 노드로 생각할 수 있습니다. 이 `dataflowEdges` 필드는 필요한 소스 및 대상 데이터 흐름 노드 (구성) 를 정의합니다. 단일 데이터 흐름 엣지는 두 개의 구성 Amazon Resource Names ARNs () 목록으로, 첫 번째는 소스 구성이고 두 번째는 대상 구성입니다. 두 구성 사이에 데이터 흐름 에지를 지정하면 접촉 중에 데이터가 어디로, 어디로 이동해야 하는지 AWS Ground Station 알 수 있습니다. 자세한 내용은 구성 단원을 참조하십시오.

`contactPrePassDurationSeconds`및 를 `contactPostPassDurationSeconds` 사용하면 이벤트 알림을 받을 연락처를 기준으로 시간을 지정할 수 있습니다. CloudWatch 연락처와 관련된 이벤트 일정을 보려면 여기를 읽어보십시오연락처 라이프사이클.

미션 프로파일의 `name` 필드는 생성하는 미션 프로파일 간을 구별하는 데 도움이 됩니다.

`streamsKmsRole`및 `streamsKmsKey` 는 AWS Ground Station 에이전트에 데이터를 전달할 때 사용하는 AWS Ground Station 암호화를 정의하는 데 사용됩니다. 참고하세요전송 중 데이터 암호화 AWS Ground Station.


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

파라미터 및 예제의 전체 목록은 다음 설명서에 포함되어 있습니다.

- AWS::GroundStation:: MissionProfile CloudFormation 리소스 유형

구성

구성은 연락처의 각 측면에 대한 매개변수를 정의하는 데 AWS Ground Station 사용하는 리소스입니다. 원하는 구성을 미션 프로파일에 추가하면 접촉을 실행할 때 해당 미션 프로파일이 사용됩니다. 여러 갖 유형의 구성을 정의할 수 있습니다. 구성을 두 범주로 그룹화할 수 있습니다.

- 추적 구성
- 데이터플로우 구성

TrackingConfigA가 유일한 추적 구성 유형입니다. 접촉 중에 안테나의 자동 추적 설정을 구성하는 데 사용되며 임무 프로필에 필요합니다.

미션 프로필 데이터 흐름에 사용할 수 있는 구성은 각각 데이터를 보내거나 받을 수 있는 AWS Ground Station 관리 리소스를 나타내는 데이터 흐름 노드라고 생각할 수 있습니다. 임무 프로필에는 이러한 구성 쌍이 적어도 한 쌍이 필요합니다. 한 쌍은 데이터 소스를 나타내고 다른 하나는 목적지를 나타냅니다. 이러한 구성은 다음 표에 요약되어 있습니다.

Config 이름	데이터 흐름 소스/대상
AntennaDownlinkConfig	소스
AntennaDownlinkDemodDecodeConfig	소스
UplinkEchoConfig	소스
S3 RecordingConfig	대상
AntennaUplinkConfig	대상
DataflowEndpointConfig	소스 및/또는 대상

AWS CloudFormation AWS Command Line Interface, 또는 를 사용하여 구성 작업을 수행하는 방법에 대한 자세한 내용은 다음 설명서를 참조하십시오. AWS Ground Station API 특정 구성 유형에 대한 설명서 링크도 아래에 제공됩니다.

- AWS::GroundStation: :구성 리소스 CloudFormation 유형
- Config AWS CLI 레퍼런스
- Config API 참조

추적 구성

미션 프로파일에서 추적 구성을 사용하여 접촉 중에 자동 추적을 활성화할지 여부를 결정할 수 있습니다. 이 구성에는 `autotrack`이라는 단일 파라미터가 있습니다. `autotrack` 파라미터에는 다음과 같은 값이 있습니다.

- `REQUIRED` - 자동 추적이 접촉에 필수입니다.
- `PREFERRED` - 자동 추적이 접촉에 선호되지만, 자동 추적이 없더라도 접촉을 실행할 수 있습니다.
- `REMOVED` - 자동 추적을 접촉에 사용하지 않습니다.

AWS Ground Station 자동 추적을 사용하지 않을 때는 임시 데이터를 기반으로 가리키는 프로그래밍 방식 추적을 활용합니다. 에페메리스의 구성 방법에 위성 에페메리스 데이터 대한 자세한 내용은 참조하시기 바랍니다.

Autotrack은 예상 신호를 찾을 때까지 프로그램 추적을 사용합니다. 그런 일이 발생하면 신호 강도에 따라 계속 추적합니다.

AWS CloudFormation AWS Command Line Interface, 또는 를 사용하여 구성 추적 작업을 수행하는 방법에 대한 자세한 내용은 다음 설명서를 참조하십시오. AWS Ground Station API

- AWS::GroundStation: 구성 속성 TrackingConfig CloudFormation
- Config AWS CLI 참조 (섹션 참조) `trackingConfig -> (structure)`
- TrackingConfig API참조

안테나 다운링크 구성

안테나 다운링크 구성을 사용하여 접촉 중에 다운링크를 위한 안테나를 구성할 수 있습니다. 이 구성은 다운링크 접촉 중에 사용해야 하는 주파수, 대역폭 및 편광을 지정하는 스펙트럼 구성으로 이루어집니다.

이 구성은 데이터 흐름의 소스 노드를 나타냅니다. 무선 주파수 데이터를 디지털화하는 역할을 합니다. 이 노드에서 스트리밍되는 데이터는 신호 데이터/IP 형식을 따릅니다. 이 구성으로 데이터 흐름을 구성하는 방법에 대한 자세한 내용은 을 참조하십시오. 데이터 흐름

다운링크 사용 사례에 복조나 디코드가 필요한 경우 안테나 다운링크 복조 디코드 구성 단원을 참조하세요.

AWS CloudFormation, 또는 를 사용하여 안테나 다운링크 구성에서 작업을 수행하는 방법에 대한 자세한 내용은 다음 설명서를 참조하십시오. AWS Command Line Interface AWS Ground Station API

- AWS::GroundStation: 구성 속성 AntennaDownlinkConfig CloudFormation
- Config AWS CLI 참조 (섹션 참조) `antennaDownlinkConfig -> (structure)`
- AntennaDownlinkConfig API참조

안테나 다운링크 복조 디코드 구성

안테나 다운링크 디코딩 컨피그레이션은 복조 및/또는 디코딩을 사용하여 다운링크 컨
택을 실행하는 데 사용할 수 있는 보다 복잡하고 사용자 지정 가능한 구성 유형입니다.
`<### ### #### #### # ### ## ## aws-groundstation@amazon.com ## #### ## ## #####.`
사용 사례에 적합한 구성 및 임무 프로필을 정의할 수 있도록 도와드리겠습니다.

이 구성은 데이터 흐름의 소스 노드를 나타냅니다. 무선 주파수 데이터를 디지털화하고 지정된 대로 복조 및 디코딩을 수행합니다. 이 노드에서 스트리밍되는 데이터는 복조/디코딩된 데이터/IP 형식을 따릅니다. 이 구성으로 데이터 흐름을 구성하는 방법에 대한 자세한 내용은 을 참조하십시오. 데이터 흐름

, 또는 를 사용하여 안테나 다운링크 데모 디코드 구성에서 작업을 수행하는 방법에 대한 자세한 내용은 다음 설명서를 참조하십시오. AWS CloudFormation AWS Command Line Interface AWS Ground Station API

- AWS::GroundStation::Config AntennaDownlinkDemodDecodeConfig CloudFormation 속성
- Config AWS CLI 참조 (섹션 참조) `antennaDownlinkDemodDecodeConfig -> (structure)`
- AntennaDownlinkDemodDecodeConfig API참조

안테나 업링크 구성

안테나 업링크 구성을 사용하여 업링크 접촉 중에 안테나를 구성할 수 있습니다. 주파수, 편광 및 목표 유효 등방성 방사 전력 () 이 포함된 스펙트럼 구성으로 구성됩니다. EIRP 업링크 루프백을 구성하는 방법에 대한 자세한 내용은 안테나 업링크 에코 구성 단원을 참조하세요.

이 구성은 데이터 흐름의 대상 노드를 나타냅니다. 제공된 디지털화된 무선 주파수 데이터 신호를 아날로그 신호로 변환하여 위성이 수신할 수 있도록 방출합니다. 이 노드로 스트리밍되는 데이터는 신호 데

이터/IP 형식을 충족해야 합니다. 이 구성으로 데이터 흐름을 구성하는 방법에 대한 자세한 내용은 을 참조하십시오. 데이터 흐름

, 또는 를 사용하여 AWS CloudFormation안테나 업링크 구성에서 작업을 수행하는 방법에 대한 자세한 내용은 다음 설명서를 참조하십시오. AWS Command Line Interface AWS Ground Station API

- AWS::GroundStation: 구성 속성 AntennaUplinkConfig CloudFormation
- Config AWS CLI 참조 (섹션 참조) `antennaUplinkConfig -> (structure)`
- AntennaUplinkConfig API참조

안테나 업링크 에코 구성

업링크 에코 구성은 업링크 에코를 실행하는 방법을 안테나에 알립니다. 업링크 에코는 우주선으로 전송되는 명령을 검증하고 기타 고급 작업을 수행하는 데 사용할 수 있습니다. 이는 AWS Ground Station 안테나가 전송하는 실제 신호 (예: 업링크) 를 기록함으로써 달성됩니다. 이는 안테나가 데이터 흐름 엔드포인트로 보낸 신호를 반향하므로 전송된 신호와 일치해야 합니다. 업링크 에코 컨피그레이션에는 업링크 컨피그레이션이 포함됩니다. ARN 안테나는 업링크 에코를 실행할 때 에서 가리키는 업링크 구성의 파라미터를 사용합니다. ARN

이 구성은 데이터 흐름의 소스 노드를 나타냅니다. 이 노드에서 스트리밍되는 데이터는 신호 데이터/IP 형식을 충족합니다. 이 구성으로 데이터 흐름을 구성하는 방법에 대한 자세한 내용은 을 참조하십시오. 데이터 흐름

, 또는 를 사용하여 업링크 에코 구성에서 작업을 수행하는 방법에 대한 자세한 내용은 다음 설명서를 참조하십시오. AWS CloudFormation AWS Command Line Interface AWS Ground Station API

- AWS::GroundStation: 구성 속성 UplinkEchoConfig CloudFormation
- Config AWS CLI 참조 (섹션 참조) `uplinkEchoConfig -> (structure)`
- UplinkEchoConfig API참조

데이터 흐름 엔드포인트 구성

> **Note**
>
> Dataflow 엔드포인트 구성은 Amazon으로의 데이터 전송에만 EC2 사용되며 Amazon S3로의 데이터 전송에는 사용되지 않습니다.

데이터 흐름 엔드포인트 구성을 사용하여 데이터 흐름 엔드포인트 그룹 내의 어느 데이터 흐름 엔드포인트를 접촉 중에 어느 곳으로 전송할지 또는 어느 곳으로 데이터를 전송할지 지정할 수 있습니다. 데이터 흐름 엔드포인트 구성의 두 파라미터는 데이터 흐름 엔드포인트의 이름과 영역을 지정합니다. 연락처를 예약할 때 는 지정한 임무 프로필을 AWS Ground Station 분석하고 임무 프로필에 포함된 데이터 흐름 엔드포인트 구성으로 지정된 모든 데이터 흐름 엔드포인트를 포함하는 AWS 지역 내의 데이터 흐름 엔드포인트 그룹을 찾으려고 시도합니다. 적합한 데이터 흐름 엔드포인트 그룹을 찾으면 연락처 상태는 _TO_가 되고 그렇지 않으면 _TO_가 됩니다. SCHEDULED FAILED SCHEDULE 가능한 연락처 상태에 대한 자세한 내용은 을 참조하십시오. AWS Ground Station 연락처 상태

데이터 흐름 엔드포인트 구성의 `dataflowEndpointName` 속성은 데이터 흐름 엔드포인트 그룹의 어느 데이터 흐름 엔드포인트가 접촉 중에 어느 데이터로 또는 어느 데이터로부터 전달되는지를 지정합니다.

`dataflowEndpointRegion` 속성은 데이터플로우 엔드포인트가 위치한 리전을 지정합니다. 데이터 흐름 엔드포인트 구성에 리전이 지정된 경우 지정된 리전에서 데이터 플로우 엔드포인트를 찾아보세요. AWS Ground Station 지역을 지정하지 않은 경우 연락처의 그라운드 AWS Ground Station 스테이션 지역을 기본값으로 사용합니다. 데이터 흐름 엔드포인트의 리전이 접촉의 Ground Station 리전과 동일하지 않은 경우 접촉은 리전 간 데이터 전송 접촉으로 간주됩니다. 지역 간 데이터 흐름에 데이터 흐름 대한 자세한 내용은 을 참조하십시오.

데이터 흐름의 다양한 이름 지정 체계가 사용 사례에 어떻게 도움이 되는지에 데이터플로우 엔드포인트 그룹 대한 팁은 을 참조하십시오.

이 구성으로 데이터 흐름을 구성하는 방법에 대한 자세한 내용은 을 참조하십시오. 데이터 흐름

, 또는 를 사용하여 AWS CloudFormation데이터 흐름 엔드포인트 구성에서 작업을 수행하는 방법에 대한 자세한 내용은 다음 설명서를 참조하십시오. AWS Command Line Interface AWS Ground Station API

- AWS::GroundStation: 구성 속성 DataflowEndpointConfig CloudFormation
- Config AWS CLI 참조 (섹션 참조) `dataflowEndpointConfig -> (structure)`
- DataflowEndpointConfig API참조

아마존 S3 레코딩 구성

> **Note**
>
> Amazon S3 기록 구성은 Amazon S3로 데이터를 전송하는 용도로만 사용되며 Amazon으로의 데이터 전송에는 사용되지 않습니다. EC2

이 구성은 데이터 흐름의 대상 노드를 나타냅니다. 이 노드는 데이터 흐름의 소스 노드에서 들어오는 데이터를 pcap 데이터로 캡슐화합니다. 이 구성으로 데이터 흐름을 구성하는 방법에 대한 자세한 내용은 을 참조하십시오. 데이터 흐름

S3 기록 구성을 사용하여 사용된 명명 규칙과 함께 다운링크된 데이터를 전송할 Amazon S3 버킷을 지정할 수 있습니다. 다음은 이러한 파라미터에 대한 제한 및 세부 정보를 지정합니다.

- Amazon S3 버킷 이름은 `aws-groundstation`로 시작해야 합니다.
- IAM역할에는 `groundstation.amazonaws.com` 서비스 주체가 역할을 맡도록 허용하는 신뢰 정책이 있어야 합니다. 예제는 아래 신뢰 정책 예제를 참조하세요. 구성 생성 시 구성 리소스 ID가 존재하지 않으므로 신뢰 정책에는 별표 () 를 사용해야 합니다.*) 대신 *`your-config-id`* 구성 리소스 ID를 사용하여 생성 후 업데이트할 수 있습니다.

신뢰 정책 예제

역할의 신뢰 정책을 업데이트하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 IAM역할 관리를 참조하십시오.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "groundstation.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "your-account-id"
```

```
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:groundstation:config-region:your-account-id:config/
s3-recording/your-config-id"
        }
      }
    }
  ]
}
```

- 역할에는 IAM 역할이 버킷에서 작업을 수행하고 `s3:PutObject` 버킷 객체에 대한 `s3:GetBucketLocation` 작업을 수행하도록 허용하는 IAM 정책이 있어야 합니다. Amazon S3 버킷에 버킷 정책이 있는 경우, 버킷 정책은 IAM 역할이 이러한 작업을 수행하도록 허용해야 합니다. 예제는 아래 역할 정책 예제를 참조하세요.

역할 정책 예제

역할 정책을 업데이트하거나 연결하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 IAM정책 관리를 참조하십시오.

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

```
    }
  ]
}
```

- 접두사는 S3 데이터 객체의 이름을 지정할 때 사용됩니다. 대체를 위한 선택적 키를 지정할 수 있습니다. 이 값은 연락처 세부 정보의 해당 정보로 대체됩니다. 예를 들어, 접두사가 `{satellite_id}/{year}/{month}/{day}` 바뀌면 다음과 같은 결과가 출력됩니다. `fake_satellite_id/2021/01/10`

  대체를 위한 선택적 키: `{satellite_id}|||{config-name}||{config-id}|{year}|{month} {day}`

AWS CloudFormation AWS Command Line Interface, 또는 를 사용하여 S3 기록 구성에서 작업을 수행하는 방법에 대한 자세한 내용은 다음 설명서를 참조하십시오. AWS Ground Station API

- AWS::GroundStation: :구성 S3 속성 RecordingConfig CloudFormation
- Config AWS CLI 참조 (섹션 참조) `s3RecordingConfig -> (structure)`
- S3 RecordingConfig API 레퍼런스

데이터플로우 엔드포인트 그룹

Dataflow 엔드포인트는 통화 중에 데이터를 동기적으로 스트리밍하거나 주고받을 위치를 정의합니다. 데이터 흐름 엔드포인트는 항상 데이터 흐름 엔드포인트 그룹의 일부로 생성됩니다. 여러 데이터 흐름 엔드포인트를 한 그룹에 포함시키면 지정된 엔드포인트를 단일 접촉 중에 모두 함께 사용할 수 있다고 선언하는 것입니다. 예를 들어, 접촉에서 세 개의 개별 데이터 흐름 엔드포인트에 데이터를 전송해야 하는 경우 미션 프로파일의 데이터 흐름 엔드포인트 구성과 일치하는 세 개의 엔드포인트가 단일 데이터 흐름 엔드포인트 그룹에 있어야 합니다.

> **Tip**
>
> 데이터 흐름 엔드포인트는 연락처를 실행할 때 선택한 이름으로 식별됩니다. 이러한 이름이 계정 전체에서 고유할 필요는 없습니다. 이렇게 하면 서로 다른 위성과 안테나에 있는 여러 연락처를 동일한 임무 프로필을 사용하여 동시에 실행할 수 있습니다. 작동 특성이 동일한 여러 위성이 있는 경우에 유용할 수 있습니다. 위성 집합에 필요한 최대 동시 연락처 수에 맞게 데이터 흐름 엔드포인트 그룹 수를 확장할 수 있습니다.

데이터 흐름 엔드포인트 그룹에 있는 하나 이상의 리소스가 접촉에 사용 중이면 전체 그룹이 해당 접촉의 기간에 예약됩니다. 여러 접촉을 동시에 실행할 수 있지만, 이러한 접촉을 서로 다른 데이터 흐름 엔드포인트 그룹에서 실행해야 합니다.

> **Important**
>
> 데이터 흐름 엔드포인트 그룹은 이를 사용하여 연락을 예약할 수 있는 HEALTHY 상태여야 합니다. 상태가 아닌 데이터 흐름 엔드포인트 그룹의 문제를 해결하는 방법에 대한 자세한 내용은 을 참조하십시오. HEALTHY HEALTHY상태가 DataflowEndpointGroups 아닌 문제 해결

AWS CloudFormation, 또는 를 사용하여 데이터 흐름 엔드포인트 그룹에서 작업을 수행하는 방법에 대한 자세한 내용은 다음 설명서를 참조하십시오. AWS Command Line Interface AWS Ground Station API

- AWS::GroundStation: 리소스 유형 DataflowEndpointGroup CloudFormation
- 데이터플로우 엔드포인트 그룹 참조 AWS CLI
- 데이터 플로우 엔드포인트 그룹 API 참조

데이터 흐름 엔드포인트

데이터 흐름 엔드포인트 그룹의 구성원은 데이터 흐름 엔드포인트입니다. AWS Ground Station 에이전트를 사용하거나 데이터 흐름 엔드포인트 애플리케이션과 함께 작동하도록 Dataflow 엔드포인트를 정의할 수 있습니다. 두 유형의 인스턴스 모두에 대해 데이터 흐름 엔드포인트 그룹을 생성하기 전에 지원 구조 (예: IP 주소) 를 생성해야 합니다. 사용할 데이터 흐름 엔드포인트 유형 및 지원 구조 설정 방법에 데이터 흐름 대한 권장 사항은 을 참조하십시오.

다음 섹션에서는 지원되는 두 엔드포인트 유형에 대해 설명합니다.

AWS Ground Station 에이전트 엔드포인트

AWS Ground Station 에이전트 엔드포인트는 AWS Ground Station 에이전트를 소프트웨어 구성 요소로 활용하여 연결을 종료합니다. 50% 이상의 디지털 신호 데이터를 다운링크하려는 경우 AWS Ground Station 에이전트 데이터 흐름 엔드포인트를 사용하십시오. MHz AWS Ground Station 에이전트 엔드포인트를 구성하려면 의 필드만 채우면 됩니다. AwsGroundStationAgentEndpoint EndpointDetails AWS Ground Station 에이전트에 대한 자세한 내용은 전체 AWS Ground Station 에이전트 사용 설명서를 참조하십시오.

AwsGroundStationAgentEndpoint는 다음 구성 요소로 이루어져 있습니다.

- Name- 데이터 흐름 엔드포인트 이름. 연락처가 이 데이터 흐름 엔드포인트를 사용하려면 이 이름이 데이터 흐름 엔드포인트 구성에 사용된 이름과 일치해야 합니다.
- EgressAddress- 에이전트로부터 데이터를 송신하는 데 사용되는 IP 및 포트 주소.
- IngressAddress- 에이전트로 데이터를 수신하는 데 사용되는 IP 및 포트 주소.

데이터 플로우 엔드포인트

Dataflow 엔드포인트는 네트워킹 애플리케이션을 소프트웨어 구성 요소로 활용하여 연결을 종료합니다. 디지털 신호 데이터를 업링크하거나, 50% MHz 미만의 디지털 신호 데이터를 다운링크하거나, 복조/디코딩된 신호 데이터를 다운링크하려는 경우 Dataflow Endpoint를 사용하십시오. Dataflow 엔드포인트를 구성하려면 의 및 필드를 채웁니다. Endpoint Security Details EndpointDetails

Endpoint는 다음 구성 요소로 이루어져 있습니다.

- Name- 데이터플로우 엔드포인트 이름. 연락처가 이 데이터 흐름 엔드포인트를 사용하려면 이 이름이 이 데이터 흐름 엔드포인트 구성에 사용된 이름과 일치해야 합니다.
- Address- 사용된 IP 및 포트 주소.

SecurityDetails는 다음 구성 요소로 이루어져 있습니다.

- roleArn- 사용자 VPC 내에서 엘라스틱 네트워크 인터페이스 (ARN) 를 생성하는 역할을 맡을 역할의 Amazon 리소스 이름 (ENIs) AWS Ground Station 이들은 ENIs 연락 중에 스트리밍되는 데이터의 수신 및 발신 지점 역할을 합니다.
- securityGroupIds - 탄력적 네트워크 인터페이스에 연결할 보안 그룹입니다.
- subnetIds- 인스턴스로 스트림을 전송하기 위해 엘라스틱 네트워크 인터페이스를 AWS Ground Station 배치하는 서브넷 목록입니다.

전달되는 IAM 역할에는 groundstation.amazonaws.com 서비스 주체가 역할을 맡도록 허용하는 신뢰 정책이 roleArn 있어야 합니다. 예제는 아래 신뢰 정책 예제를 참조하세요. 엔드포인트 생성 중에는 엔드포인트 리소스 ID가 존재하지 않으므로 신뢰 정책에는 별표 () 를 사용해야 합니다.*다음 항목 대신) *your-endpoint-id*. 신뢰 정책의 범위를 특정 데이터 흐름 엔드포인트 그룹으로 제한하기 위해 엔드포인트 리소스 ID를 사용하도록 생성 후 업데이트할 수 있습니다.

IAM역할에는 설정을 허용하는 IAM AWS Ground Station 정책이 있어야 합니다. ENIs 예제는 아래 역할 정책 예제를 참조하세요.

신뢰 정책 예제

역할의 신뢰 정책을 업데이트하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 IAM역할 관리를 참조하십시오.

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

역할 정책 예제

역할 정책을 업데이트하거나 연결하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 IAM정책 관리를 참조하십시오.

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

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

AWS Ground Station 대리인

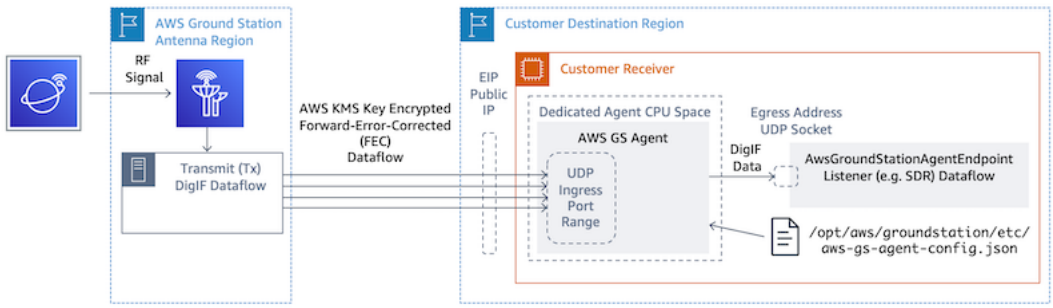
AWS Ground Station 에이전트란 무엇인가요?

AWSGround Station 에이전트를 AWS Ground Station 사용하면 Ground Station에 접속하는 동안 동기식 광대역 디지털 중간 주파수 (DiGif) 데이터 흐름을 수신 (다운링크) 할 수 있습니다. AWS 데이터 전송을 위한 두 가지 옵션을 선택할 수 있습니다.

1. EC2인스턴스로의 데이터 전송 - 소유한 EC2 인스턴스로의 데이터 전송. AWS Ground Station 에이전트를 관리합니다. 이 옵션은 실시간에 가까운 데이터 처리가 필요한 경우에 가장 적합할 수 있습니다. EC2데이터 전송에 대한 자세한 내용은 데이터 흐름 섹션을 참조하십시오.
2. S3 버킷으로의 데이터 전송 - AWS S3 버킷으로의 데이터 전송은 에서 완전히 관리합니다 AWS Ground Station. S3 데이터 전송에 대한 자세한 내용은 시작하기 안내서를 참조하세요.

두 가지 데이터 전송 모드 모두 AWS 리소스 세트를 생성해야 합니다. 신뢰성, 정확성 및 지원 가능성을 CloudFormation 보장하려면 를 사용하여 AWS 리소스를 생성하는 것이 좋습니다. 각 연락처는 EC2 또는 S3에만 데이터를 전송할 수 있으며 두 연락처 모두에 동시에 데이터를 전송할 수는 없습니다.

다음 다이어그램은 소프트웨어 정의 라디오 () 또는 유사한 리스너를 사용하여 AWS Ground Station 안테나 영역에서 EC2 인스턴스로의 DiGif 데이터 흐름을 보여줍니다. SDR



추가 정보

자세한 내용은 전체 에이전트 사용 설명서를 참조하십시오.AWS Ground Station

시작하기

시작하기 전에 의 기본 개념을 숙지해야 합니다. AWS Ground Station자세한 내용은 AWS Ground Station 작동 방식 단원을 참조하십시오.

다음은 AWS Identity and Access Management (IAM) 에 대한 모범 사례와 필요한 권한입니다. 적절한 역할을 설정한 후 나머지 단계를 수행할 수 있습니다.

가입해 주세요. AWS 계정

계정이 없는 경우 다음 단계를 완료하여 계정을 만드세요. AWS 계정

가입하려면 AWS 계정

1. https://portal.aws.amazon.com/billing/등록 열기.
2. 온라인 지시 사항을 따릅니다.

   등록 절차 중 전화를 받고 전화 키패드로 확인 코드를 입력하는 과정이 있습니다.

   에 가입하면 AWS 계정 루트 사용자팬이 생성됩니다. AWS 계정루트 사용자에게는 계정의 모든 AWS 서비스 및 리소스에 액세스할 권한이 있습니다. 보안 모범 사례는 사용자에게 관리 액세스 권한을 할당하고, 루트 사용자만 사용하여 루트 사용자 액세스 권한이 필요한 작업을 수행하는 것입니다.

AWS 가입 절차가 완료된 후 확인 이메일을 보냅니다. 언제든지 https://aws.amazon.com/으로 이동하고 내 계정을 선택하여 현재 계정 활동을 보고 계정을 관리할 수 있습니다.

관리자 액세스 권한이 있는 사용자 생성

등록한 AWS 계정후에는 일상적인 작업에 루트 사용자를 사용하지 않도록 관리 사용자를 보호하고 AWS IAM Identity Center활성화하고 생성하십시오 AWS 계정 루트 사용자.

보안을 유지하세요. AWS 계정 루트 사용자

1. 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 계정 AWS Management Console소유자로 로그인합니다. 다음 페이지에서 비밀번호를 입력합니다.

루트 사용자를 사용하여 로그인하는 데 도움이 필요하면 AWS 로그인 User Guide의 루트 사용자로 로그인을 참조하십시오.

2. 루트 사용자에 대한 다단계 인증 (MFA) 을 켜십시오.

   지침은 사용 설명서의 AWS 계정 IAM루트 사용자 (콘솔) 용 가상 MFA 기기 활성화를 참조하십시오.

관리자 액세스 권한이 있는 사용자 생성

1. IAMID 센터를 활성화합니다.

   지침은 AWS IAM Identity Center 사용 설명서의 AWS IAM Identity Center설정을 참조하세요.

2. IAMID 센터에서 사용자에게 관리 액세스 권한을 부여하십시오.

   를 ID 소스로 사용하는 방법에 대한 자습서는 사용 설명서의 기본값으로 IAM Identity Center 디렉터리AWS IAM Identity Center 사용자 액세스 구성을 참조하십시오. IAM Identity Center 디렉터리

관리 액세스 권한이 있는 사용자로 로그인

- IAMIdentity Center 사용자로 로그인하려면 IAM Identity Center 사용자를 생성할 때 이메일 주소로 전송된 URL 로그인을 사용하십시오.

  IAMIdentity Center 사용자를 사용하여 로그인하는 데 도움이 필요하면 사용 설명서의 AWS 액세스 포털에 로그인을 참조하십시오.AWS 로그인

추가 사용자에게 액세스 권한 할당

1. IAMIdentity Center에서 최소 권한 권한 적용의 모범 사례를 따르는 권한 집합을 생성하십시오.

   지침은AWS IAM Identity Center 사용 설명서의 Create a permission set를 참조하세요.

2. 사용자를 그룹에 할당하고, 그룹에 Single Sign-On 액세스 권한을 할당합니다.

   지침은AWS IAM Identity Center 사용 설명서의 Add groups를 참조하세요.

AWS 계정에 AWS Ground Station 권한 추가

관리자 AWS Ground Station 없이 사용하려면 새 정책을 만들어 AWS 계정에 연결해야 합니다.

1. 에 AWS Management Console 로그인하고 IAM콘솔을 엽니다.
2. 새 정책 생성. 다음 단계를 사용합니다.

   a. 탐색 창에서 정책을 선택한 후 정책 생성을 선택합니다.

   b. JSON탭에서 다음 값 중 하나를 JSON 사용하여 를 편집합니다. 애플리케이션에 가장 JSON 적합한 방법을 사용하십시오.

   - Ground Station 관리자 권한의 경우 Action을 다음과 같이 groundtation: *으로 설정합니다.

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

   - 읽기 전용 권한의 경우 Action을 다음과 같이 groundstation:Get*, groundstation:List* 및 groundstation:Describe*로 설정합니다.

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

```
}
```

- 다단계 인증을 통해 보안을 강화하려면 다음과 같이 액션을 그라운드 스테이션: *로 설정하고 조건/Bool을 aws ::true로 설정하십시오. MultiFactorAuthPresent

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

3. IAM콘솔에서 생성한 정책을 원하는 사용자에게 연결합니다.

IAM사용자 및 연결 정책에 대한 자세한 내용은 IAM사용 설명서를 참조하십시오.

1단계: 새틀라이트 온보딩

위성 AWS Ground Station 온보딩은 데이터 수집, 기술 검증, 스펙트럼 라이센싱, 통합 및 테스트를 포함하는 다단계 프로세스입니다. 비밀 유지 계약 (NDAs) 도 필요합니다.

고객 온보딩 프로세스 개요

Satellite 온보딩은 콘솔 페이지의 Satellite and Resources 섹션에서 찾을 수 있는 수동 프로세스입니다. AWS Ground Station 다음은 전체 프로세스에 대한 설명입니다.

1. 위치섹션을 검토하여 위성이 지리적 및 무선 주파수 특성을 충족하는지 확인하십시오.
2. AWSGround Station에 위성을 온보딩하기 시작하려면 조직 이름, 필요한 주파수, 위성 발사 예정일 또는 발사 시기, 위성의 궤도 유형, 사용 계획 여부 등 임무와 위성 요구 사항에 대한 간략한 요약과 함께 <aws-groundstation@amazon.com> 으로 이메일을 보내주십시오. AWS Ground Station 디지털 트윈

3. 요청이 검토 및 AWS Ground Station 승인되면 사용하려는 특정 위치에서 규제 라이선스를 신청하게 됩니다. 이 단계의 기간은 지역 및 기존 규정에 따라 달라집니다.
4. 승인을 받으면 위성을 볼 수 있게 됩니다. AWS Ground Station 업데이트 성공 알림을 보내드립니다.

(선택 사항) 위성 이름 지정

온보딩 후에는 위성 레코드에 이름을 추가하여 이름을 더 쉽게 알아볼 수 있습니다. AWS Ground Station 콘솔에는 연락처 페이지를 사용할 때 Norad ID와 함께 위성에 대한 사용자 정의 이름을 표시할 수 있는 기능이 있습니다. 위성 이름을 표시하면 일정을 잡을 때 올바른 위성을 훨씬 쉽게 선택할 수 있습니다. 이를 위해 태그를 사용할 수 있습니다.

AWSGround Station Satellites에 태그를 지정하는 작업은 다음 중 하나를 사용하여 태그 리소스를 API 통해 수행할 수 있습니다. AWS CLI AWS SDKs 이 가이드에서는 를 사용하여 공영 방송 위성 Aqua (Norad ID 27424) 에 태그를 지정하는 방법을 설명합니다. AWS Ground Station CLI `us-west-2`

AWS Ground Station CLI

상호 작용하는 데 사용할 AWS CLI 수 있습니다. AWS Ground Station위성에 태그를 지정하는 AWS CLI 데 사용하기 전에 다음 AWS CLI 사전 요구 사항을 충족해야 합니다.

- 설치되어 있는지 확인하세요. AWS CLI AWS CLI설치에 대한 자세한 내용은 AWSCLI버전 2 설치를 참조하십시오.
- 구성되어 AWS CLI 있는지 확인하십시오. 구성에 AWS CLI대한 자세한 내용은 AWSCLI버전 2 구성을 참조하십시오.
- AWS CLI에서 유지 관리되는 파일에 자주 사용되는 구성 설정과 보안 인증을 저장할 수 있습니다. AWS Ground Station 연락처를 예약하고 관리하려면 이러한 설정과 자격 증명이 필요합니다 AWS CLI. 구성 및 자격 증명 설정 저장에 대한 자세한 내용은 구성 및 자격 증명 파일 설정을 참조하십시오.

구성을 AWS CLI 마치고 사용할 준비가 되면 AWSGround Station CLI 명령 참조 페이지를 검토하여 사용 가능한 명령을 숙지하십시오. 이 서비스를 사용할 때는 AWS CLI 명령 구조를 따르고 명령 접두사를 사용하여 사용하려는 AWS Ground Station 서비스로 지정하십시오. `groundstation` AWS CLI 명령 구조에 대한 자세한 내용은 AWSCLI페이지의 명령 구조를 참조하십시오. 예제 명령 구조는 다음과 같습니다.

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

위성 이름 지정하기

먼저 태그를 지정하려는 위성의 코드를 가져와야 합니다. ARN 다음 사이트의 목록 위성을 API 통해 이 작업을 수행할 수 있습니다. AWS CLI

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

위 CLI 명령을 실행하면 다음과 비슷한 출력이 반환됩니다.

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

태그를 지정하려는 위성을 찾아 `satelliteArn`를 메모해 둡니다. 태깅에 대한 한 가지 중요한 주의 사항은 태그 리소스에는 지역이 API 필요하고 리스트 위성이 ARN 반환하는 값은 글로벌 ARN 리소스라는 점입니다. 다음 단계에서는 태그를 추가하려는 지역 (일정을 잡는 지역 등) ARN 으로 태그를 보강해야 합니다. 이 예제에서는 `us-west-2`을 사용합니다. 이번 변경으로 다음과 같이 ARN 변경됩니다.

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

변경 후:

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

콘솔에 위성 이름을 표시하려면 위성에 키로 사용되는 “Name"과 있는 태그가 있어야 합니다. 또한 를 사용하기 때문에 따옴표는 AWS CLI백슬래시를 사용하여 이스케이프 처리해야 합니다. 태그는 다음과 같이 표시됩니다.

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

다음으로 tag-resource를 호출하여 위성에 태그를 지정합니다API. 다음과 AWS CLI 같이 이 작업을 수행할 수 있습니다.

```
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"}'
```

이렇게 하면 설정한 위성 이름을 AWS Ground Station 콘솔에서 확인할 수 있습니다.

위성 이름 변경

위성의 이름을 변경하려는 경우, “Name” 키는 같지만 태그의 값은 다른 상태로 위성을 사용하여 tag-resource를 ARN 다시 호출하면 됩니다. 그러면 기존 태그가 업데이트되고 콘솔에 새 이름이 표시됩니다. 다음은 이에 대한 예제 직접적 호출입니다.

```
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"}'
```

위성 이름 제거

untag-resource를 사용하여 위성에 설정된 이름을 제거할 수 있습니다. API 여기에는 태그가 위치한 지역의 ARN 위성과 태그 키 목록이 API 필요합니다. 이름의 경우 태그 키는 “Name”입니다. 다음과 같은 API 방법을 사용하여 이를 호출하는 예시는 AWS CLI 다음과 같습니다.

```
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
```

공공 방송 위성

자체 위성을 온보딩하는 것 외에도 공개적으로 액세스할 수 있는 다운링크 통신 경로를 제공하는 지원되는 공용 방송 위성에 온보딩하도록 요청할 수 있습니다. 이를 통해 이러한 위성의 데이터를 다운링크하는 데 사용할 AWS Ground Station 수 있습니다.

> **Note**
>
> 이러한 위성에 업링크할 수 없습니다. 공개적으로 액세스할 수 있는 다운링크 통신 경로만 사용할 수 있습니다.

AWS Ground Station 다음 위성의 온보딩을 지원하여 다이렉트 브로드캐스트 데이터를 다운링크할 수 있습니다.

- Aqua
- SNPP
- JPSSNOAA-1/ -20
- Terra

일단 탑승하면 이 위성에 액세스하여 즉시 사용할 수 있습니다. AWS Ground Station 서비스를 더 쉽게 시작할 수 있도록 미리 구성된 여러 AWS CloudFormation 템플릿을 유지 관리합니다. 사용 방법에 미션 프로필 구성 예시 대한 예는 AWS Ground Station 를 참조하십시오.

이러한 위성과 전송하는 데이터 종류에 대한 자세한 내용은 Aqua, JPSS-1/ NOAA -20 및 Terra를 참조하십시오. SNPP

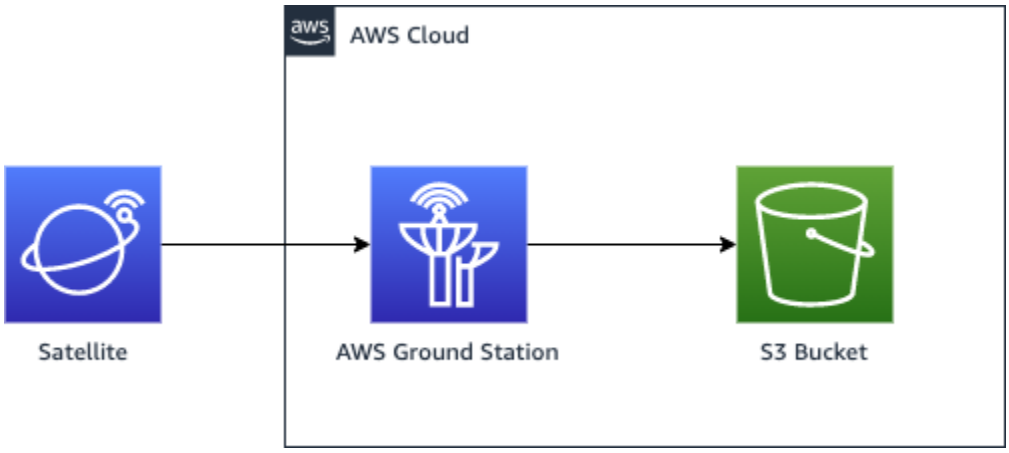
2단계: 데이터 흐름 통신 경로 계획

위성의 각 통신 경로에 대해 동기 통신과 비동기 통신 중에서 선택할 수 있습니다. 위성과 사용 사례에 따라 한 가지 또는 두 가지 유형이 모두 필요할 수 있습니다. 동기식 통신 경로를 통해 협대역 및 광대역 다운링크 작동은 물론 거의 실시간 업링크도 가능합니다. 비동기 통신 경로는 협대역 및 광대역 다운링크 작업만 지원합니다.

비동기 데이터 전송

Amazon S3로 데이터 전송 시 접촉 데이터가 계정의 Amazon S3 버킷에 비동기적으로 전송됩니다. 연락처 데이터는 패킷 캡처 (pcap) 파일로 제공되므로 연락처 데이터를 소프트웨어 정의 라디오 (SDR)로 재생하거나 pcap 파일에서 페이로드 데이터를 추출하여 처리할 수 있습니다. 안테나 하드웨어가 접촉 데이터를 수신할 때마다 pcap 파일이 30초마다 Amazon S3 버킷으로 전송되어 필요한 경우 연락 중에 접촉 데이터를 처리할 수 있습니다. 데이터를 받으면 자체 사후 처리 소프트웨어를 사용하여 처리하거나 Amazon SageMaker 또는 Amazon Rekognition과 같은 다른 AWS 서비스를 사용할 수 있습니

다. Amazon S3로 데이터를 전송하는 것은 위성 데이터를 다운링크하는 경우에만 사용할 수 있습니다. Amazon S3에서 위성으로 데이터를 업링크하는 것은 불가능합니다.



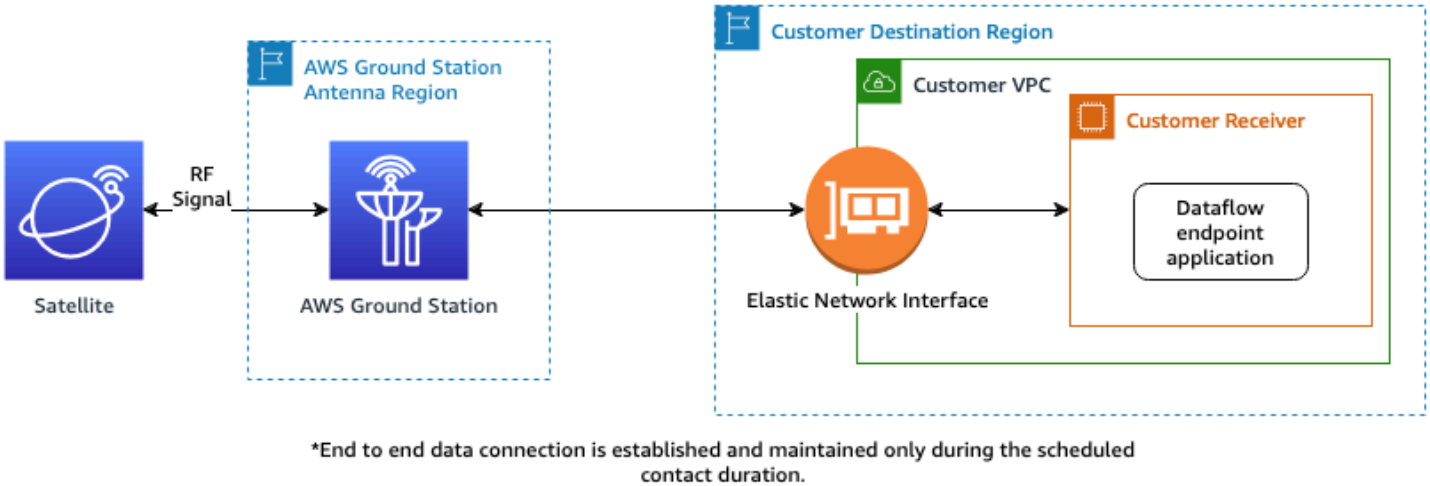
이 경로를 활용하려면 데이터를 전송할 Amazon S3 버킷을 생성해야 합니다. AWS Ground Station 다음 단계에서는 S3 레코딩 구성도 생성해야 합니다. 버킷 이름 지정에 아마존 S3 레코딩 구성 대한 제한 사항 및 파일에 사용되는 이름 지정 규칙을 지정하는 방법은 를 참조하십시오.

동기 데이터 전송

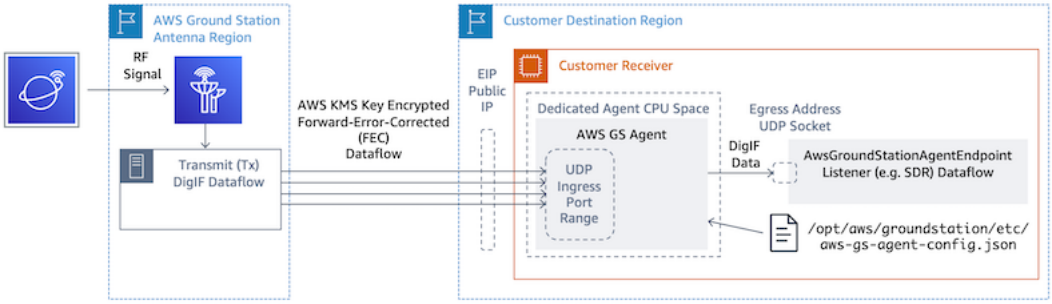
Amazon으로 데이터를 전송하면 연락처 데이터가 Amazon EC2 인스턴스로 스트리밍되고 Amazon EC2 인스턴스에서 전송됩니다. Amazon EC2 인스턴스에서 실시간으로 데이터를 처리하거나 사후 처리를 위해 데이터를 전달할 수 있습니다.

동기 경로를 활용하려면 Amazon EC2 인스턴스를 설정 및 구성하고 Dataflow 엔드포인트 그룹을 하나 이상 생성해야 합니다. Amazon EC2 인스턴스를 구성하려면 를 참조하십시오EC2- 설정 및 구성. Dataflow 엔드포인트 그룹을 생성하려면 를 참조하십시오. 데이터플로우 엔드포인트 그룹

다음은 데이터 흐름 엔드포인트 구성을 사용하는 경우의 통신 경로를 보여줍니다.



다음은 AWS Ground Station 에이전트 구성을 사용하는 경우의 통신 경로를 보여줍니다.



3단계: 구성 생성

이 단계를 통해 필요에 따라 위성, 통신 경로, Amazon 및 Amazon EC2 S3 리소스를 식별했습니다. IAM 이 단계에서는 해당 파라미터를 저장하는 AWS Ground Station 구성을 생성합니다.

데이터 전송 구성

가장 먼저 만들어야 하는 구성은 데이터를 전달하려는 위치 및 방법과 관련이 있습니다. 이전 단계의 정보를 사용하여 다음과 같은 구성 유형을 다양하게 구성할 수 있습니다.

- 아마존 S3 레코딩 구성- Amazon S3 버킷으로 데이터를 전송합니다.
- 데이터 흐름 엔드포인트 구성- Amazon EC2 인스턴스로 데이터를 전송합니다.

위성 구성

위성 구성은 위성과 AWS Ground Station 통신할 수 있는 방법과 관련이 있습니다. 에서 1단계: 새틀라이트 온보딩 수집한 정보를 참조하게 됩니다.

- 추적 구성- 연락 중에 차량을 물리적으로 추적하는 방법에 대한 기본 설정을 설정합니다. 이는 미션 프로파일을 구성하는 데 필요합니다.
- 안테나 다운링크 구성- 디지털화된 무선 주파수 데이터를 제공합니다.
- 안테나 다운링크 복조 디코드 구성 - 복조 및 디코딩된 무선 주파수 데이터를 제공합니다.
- 안테나 업링크 구성- 위성에 데이터를 업링크합니다.
- 안테나 업링크 에코 구성- 업링크 신호 데이터의 에코를 전달합니다.

4단계: 미션 프로필 생성

이전 단계에서 구성한 구성을 통해 위성을 추적하는 방법과 위성과 통신할 수 있는 방법을 식별했습니다. 이 단계에서는 하나 이상의 임무 프로필을 구성해 보겠습니다. 임무 프로필은 가능한 구성을 예상 동작으로 취합한 후 일정을 잡고 운영할 수 있는 상황을 나타냅니다.

최신 파라미터는 리소스 유형을 참조하십시오. AWS::GroundStation::MissionProfile CloudFormation

1. 임무 프로필의 이름을 지정하세요. 이렇게 하면 시스템 내에서의 사용법을 빠르게 이해할 수 있습니다. 예를 들어 satellite-wideband-narrowband-nominal-Operations를 사용하고 비상 작전을 위한 별도의 협대역 통신사가 있는 satellite-narrowband-emergency-operations경우 a를 사용할 수 있습니다.
2. 추적 구성을 설정하세요.
3. 연락 가능한 최소 기간을 설정하세요. 이렇게 하면 잠재적 연락처를 필터링하여 임무에 필요한 사항을 충족할 수 있습니다.
4. 전송 중에 데이터를 암호화하는 데 사용되는 밴드를 설정하세요 streamsKmsKey. streamsKmsRole 이는 모든 AWS Ground Station 에이전트 데이터 흐름에 사용됩니다.
5. 데이터 흐름을 설정합니다. 이전 단계에서 만든 구성을 사용하여 이동통신사 신호와 일치하도록 데이터 흐름을 생성하십시오.
6. [선택 사항] 사전 통과 및 통과 후 연결 지속 시간을 초 단위로 설정합니다. 이는 접촉 전과 후에 각각 연락처별 이벤트를 내보내는 데 사용됩니다. 자세한 내용은 이벤트를 AWS Ground Station 이용한 자동화 섹션을 참조하세요.
7. [선택 사항] 태그를 임무 프로필에 연결할 수 있습니다. 이를 통해 프로그래밍 방식으로 임무 프로필을 차별화할 수 있습니다.

를 참조하여 잠재적 미션 프로필 구성 예시 구성 중 일부만 확인할 수 있습니다.

다음 단계

이제 위성이 탑재되고 유효한 임무 프로필이 준비되었으므로 연락처를 예약하고 위성과 통신할 준비가 되었습니다. AWS Ground Station

다음 방법 중 하나로 연락을 예약할 수 있습니다.

- AWS Ground Station 콘솔.
- AWS CLI예약 연락처 명령.

- AWS SDK그. ReserveContactAPI.

위성의 궤적을 AWS Ground Station 추적하는 방법과 해당 정보가 사용되는 방식에 대한 자세한 내용은 참조하시기 바랍니다. 위성 에페메리스 데이터

AWS Ground Station 서비스를 더 쉽게 시작할 수 있도록 미리 구성된 여러 AWS CloudFormation 템플릿을 유지 관리합니다. 사용 방법에 미션 프로필 구성 예시 대한 예는 AWS Ground Station 를 참조하십시오.

제공된 디지털 중간 주파수 데이터 또는 복조 및 디코딩된 데이터를 처리하는 방법은 특정 사용 AWS Ground Station 사례에 따라 다릅니다. 다음 블로그 게시물은 사용 가능한 몇 가지 옵션을 이해하는 데 도움이 될 수 있습니다.

- AWS Ground Station Amazon S3 데이터 전송 (및 관련 GitHub 리포지토리 aws-groundstation-eos-pipelineawslabs/) 을 사용한 자동 지구 관측
- 위성 지상 세그먼트를 다음과 같이 가상화합니다. AWS
- 사용한 지구 관측 AWS Ground Station: 가이드 방법
- AWS Ground Station WideBand DigiF 및 Amphincy SDR Blink (및 관련 리포지토리 aws-samples/) 를 사용하여 처리량이 높은 위성 데이터 다운링크 아키텍처 구축 GitHub aws-groundstation-wbdigif-snpp

위치

AWS Ground Station 글로벌 AWS 인프라 지역 네트워크와 가까운 거리에 있는 글로벌 그라운드 스테이션 네트워크를 제공합니다. 지원되는 모든 AWS 지역에서 이러한 위치를 사용하도록 구성할 수 있습니다. 여기에는 데이터가 전달되는 AWS 지역이 포함됩니다.

지상국 위치를 위한 AWS 지역 찾기

AWS Ground Station 글로벌 네트워크에는 연결된 AWS지역에 물리적으로 위치하지 않는 지상국 위치가 포함됩니다. 액세스할 수 있는 지상국 목록은 AWS SDK ListGroundStation응답을 통해 검색할 수 있습니다. 지상국 위치의 전체 목록은 아래에 나와 있으며, 곧 더 많은 위치가 제공될 예정입니다. 위성에 대한 사이트 승인을 추가하거나 수정하려면 온보딩 가이드를 참조하십시오.

그라운드 스테이션 이름	그라운드 스테이션 위치	AWS지역 이름	AWS 리전 코드	참고
알래스카 1	알래스카, USA	미국 서부(오레곤)	us-west-2	물리적으로 특정 지역에 위치하지 않음 AWS
바레인 1	바레인	중동(바레인)	me-south-1	
케이프타운 1	케이프타운, 남아프리카	아프리카(케이프타운)	af-south-1	
더보 1	더보, 오스트레일리아	아시아 태평양(시드니)	ap-southeast-2	물리적으로 특정 지역에 위치하지 않음 AWS
하와이 1	하와이, USA	미국 서부(오레곤)	us-west-2	물리적으로 특정 AWS 지역에 위치하지 않음
아일랜드 1	아일랜드	유럽(아일랜드)	eu-west-1	
오하이오 1	오하이오, USA	미국 동부(오하이오)	us-east-2	
오리건 1	오리건, USA	미국 서부(오레곤)	us-west-2	
푼타 아레나스 1	푼타 아레나스, 칠레	남아메리카(상파울루)	sa-east-1	특정 지역에 물리적으로 위치하지 않음 AWS
서울 1	서울, 대한민국	아시아 태평양(서울)	ap-northeast-2	
싱가포르 1	싱가포르	아시아 태평양(싱가포르)	ap-southeast-1	
스톡홀름 1	스톡홀름, 스웨덴	유럽(스톡홀름)	eu-north-1	

AWS Ground Station 지원 지역 AWS

지원 AWS 지역의 AWS SDK 또는 AWS Ground Station 콘솔을 통해 데이터를 전달하고 연락처를 구성할 수 있습니다. 엔드포인트 및 할당량에서 지원 지역 및 관련 엔드포인트를 볼 수 있습니다.AWS Ground Station

디지털 트윈 가용성

AWS Ground Station 디지털 트윈사용 가능한 모든 AWS지역에서 AWS Ground Station 사용할 수 있습니다. 디지털 트윈 그라운드 스테이션은 Ground Station 이름에 “디지털 트윈”이라는 수정 접두사가 붙은 프로덕션 그라운드 스테이션의 정확한 사본입니다. 예를 들어, “디지털 트윈 오하이오 1"은 “오하이오 1" 프로덕션 그라운드 스테이션을 그대로 복사한 디지털 트윈 그라운드 스테이션입니다.

AWS Ground Station 사이트 마스크

각 AWS Ground Station 안테나 위치에는 관련 사이트 마스크가 있습니다. 이 마스크는 특정 방향(일반적으로 수평선 근처)을 가리킬 때 해당 위치의 안테나가 전송하거나 수신하지 못하도록 차단합니다. 마스크에는 다음 사항이 고려될 수 있습니다.

- 안테나 주변의 지리적 지형 특징 — 예를 들어 무선 주파수 (RF) 신호를 차단하거나 전송을 방해하는 산이나 건물 등이 이에 해당합니다.
- 무선 주파수 간섭 (RFI) — 이는 수신 기능 (Ground Station 안테나로의 다운링크 신호에 영향을 미치는 외부 RFI 소스) 과 전송 (AWSGround Station 안테나가 전송하는 RF 신호는 외부 수신기에 부정적인 영향을 미침) 모두에 영향을 미칩니다. AWS
- 법적 승인 — 각 지역에서 Ground AWS Station을 운영하기 위한 현지 사이트 승인에는 전송을 위한 최소 고도 각도와 같은 특정 제한 사항이 포함될 수 있습니다.

이러한 사이트 마스크는 시간이 지남에 따라 변경될 수 있습니다. 예를 들어 안테나 위치 근처에 새 건물을 지을 수 있고, RFI 출처가 변경될 수 있으며, 다른 제한 사항으로 법적 허가를 갱신할 수 있습니다. AWSGround Station 사이트 마스크는 기밀 유지 계약 (NDA) 에 따라 사용할 수 있습니다.

고객 전용 마스크

특정 지역의 위성과 통신할 수 있는 자체 법적 권한에 대한 제한으로 인해 각 사이트의 AWS Ground Station 사이트 마스크 외에도 추가 마스크가 있을 수 있습니다. AWSGround Station을 사용하여 이러한 위성과 통신할 때 규정 준수를 보장하기 위해 AWS Ground Station에서 이러한 마스크를 구성할 수 있습니다. case-by-case 자세한 내용은 AWS Ground Station 팀에 문의하십시오.

사이트 마스크가 연락 가능 시간에 미치는 영향

사이트 마스크에는 업링크(전송) 사이트 마스크와 다운링크(수신) 사이트 마스크의 두 종류가 있습니다.

ListContacts 오퍼레이션을 사용하여 가능한 연락 시간을 나열하면 AWS Ground Station은 위성이 다운링크 마스크 위로 올라가고 다운링크 마스크 아래로 내려가는 시간을 기준으로 가시성 시간을 반환합니다. 이용 가능한 연락 시간은 이 다운링크 마스크 가시성 창을 기준으로 합니다. 이렇게 하면 위성이 다운링크 마스크 아래에 있을 때 시간을 예약하지 않아도 됩니다.

미션 프로파일에 데이터 흐름 엣지에 안테나 업링크 구성이 포함되어 있더라도 업링크 사이트 마스크는 사용 가능한 연락 시간에 적용되지 않습니다. 이렇게 하면 업링크 사이트 마스크로 인해 일부 시간 동안 업링크를 사용할 수 없는 경우에도 사용 가능한 모든 연락 시간을 다운링크에 사용할 수 있습니다. 그러나 위성 연락처용으로 예약된 일부 또는 전체 시간 동안에는 업링크 신호가 전송되지 않을 수 있습니다. 업링크 전송을 예약할 때 제공된 업링크 마스크를 고려해야 할 책임은 귀하에게 있습니다.

접점에서 업링크를 사용할 수 없는 부분은 안테나 위치의 업링크 사이트 마스크를 기준으로 접촉 중의 위성 궤적에 따라 달라집니다. 업링크 사이트 마스크와 다운링크 사이트 마스크가 비슷한 리전에서는 일반적으로 이 지속 시간이 짧습니다. 업링크 마스크가 다운링크 사이트 마스크보다 상당히 높을 수 있는 다른 리전에서는 이로 인해 접속 기간의 상당 부분 또는 전체가 업링크에 사용할 수 없게 될 수 있습니다. 예약된 시간 중 일부를 업링크에 사용할 수 없는 경우에도 전체 연락 시간이 청구됩니다.

AWS Ground Station 사이트 기능

환경을 단순화하기 위해 안테나 유형에 맞는 공통 기능 세트를 AWS Ground Station 결정한 다음 여러 안테나를 그라운드 스테이션 위치에 배치합니다. 온보딩 단계 중 일부는 위성이 특정 위치의 안테나 유형과 호환되도록 합니다. 연락처를 예약하면 사용되는 안테나 유형을 간접적으로 결정합니다. 이렇게 하면 어떤 안테나를 사용하든 관계없이 시간이 지나도 특정 지상국 위치에서의 경험이 동일하게 유지됩니다. 접점의 구체적인 성능은 현장의 날씨와 같은 다양한 환경 문제로 인해 달라질 수 있습니다.

현재 모든 사이트에서 다음 기능을 지원합니다.

> **Note**
>
> 다음 표의 각 행은 달리 명시되지 않는 한 독립적인 통신 경로를 나타냅니다. 여러 통신 경로를 동시에 사용할 수 있는 다중 채널 기능을 반영하기 위해 중복된 행이 존재합니다.

역량 유형	주파수 범위	대역폭 범위	편광	일반 이름	참고
안테나-다운링크	7750 - 8400 MHz	50 - 400 MHz	RHCP	X-밴드 광대역 다운링크	총 대역폭은 400 미만이어야 MHz 하며 사용되는 주파수 범위는 겹치지 않아야 합니다. 푼타 아레나스 최대 값은 167 입니다. MHz GS 에이전트가 필요합니다.
안테나 다운링크	7750 - 8400 MHz	50 - 400 MHz	RHCP		
안테나 다운링크	7750 - 8400 MHz	50 - 400 MHz	RHCP		
안테나 다운링크	7750 - 8400 MHz	50 - 400 MHz	RHCP		
안테나 다운링크	7750 - 8400 MHz	50 - 400 MHz	RHCP		
안테나 다운링크	7750 - 8400 MHz	50 - 400 MHz	LHCP		
안테나 다운링크	7750 - 8400 MHz	50 - 400 MHz	LHCP		
안테나 다운링크	7750 - 8400 MHz	50 - 400 MHz	LHCP		
안테나 다운링크	7750 - 8400 MHz	50 - 400 MHz	LHCP		
안테나 다운링크	7750 - 8400 MHz	50 - 400 MHz	LHCP		
안테나 다운링크	2200 - 2290 MHz	최대 40개 MHz	RHCP	S-밴드 다운링크	한 번에 하나의 편광만 사용할 수 있습니다.
안테나-다운링크	2200 - 2290 MHz	최대 40개 MHz	LHCP		
안테나 다운링크	7750 - 8400 MHz	최대 40개 MHz	RHCP	X-밴드 협대역 다운링크	한 번에 하나의 편광만 사

역량 유형	주파수 범위	대역폭 범위	편광	일반 이름	참고
안테나-다운링크	7750 - 8400 MHz	최대 40개 MHz	LHCP		용할 수 있습니다.
안테나 업링크	2025 - 210 MHz	최대 40개 MHz	RHCP	S-밴드 업링크	한 번에 하나의 편광만 사용할 수 있습니다. EIRP20-53 dBW
안테나 업링크	2025 - 210 MHz	최대 40개 MHz	LHCP		
antenna-uplink-echo	2025 - 2110 MHz	2 MHz	RHCP	업링크 에코	안테나 업링크 제한과 일치합니다.
antenna-uplink-echo	2025 - 210 MHz	2 MHz	LHCP		
antenna-downlink-demod-decode	7750 - 8400 MHz	최대 500개 MHz	RHCP	X-대역 광대역 복조 및 디코딩된 다운링크	
antenna-downlink-demod-decode	7750 - 8400 MHz	최대 500개 MHz	LHCP		
추적	N/A	해당 사항 없음	해당 사항 없음	N/A	자동 추적 및 프로그램 추적 지원

* RHCP = 오른손 원형 편광, LHCP = 왼손 원형 편광. 편광에 대한 자세한 내용은 원형 편광을 참조하십시오.

위성 에페메리스 데이터

복수 에페메리스인 에페메리스는 천체의 궤적을 제공하는 파일 또는 데이터 구조입니다. 과거에는 이 파일이 표 형식의 데이터만 참조했지만 점차 우주선 궤적을 나타내는 다양한 데이터 파일로 이동하게 되었습니다.

AWS Ground Station 임시 데이터를 사용하여 위성에 연락처를 사용할 수 있는 시점을 파악하고 네트워크의 안테나가 위성을 가리키도록 올바르게 명령합니다. AWS Ground Station 기본적으로 위성에 할당된 ID가 AWS Ground Station 있는 경우 에페메리드를 제공하기 위해 별도의 조치를 취하지 않아도 됩니다. NORAD

주제

기본 에페메리스 데이터

기본적으로 은 Space-Track에서 공개적으로 사용 가능한 데이터를 AWS Ground Station 사용하며 이러한 기본 에페메리드를 제공하기 AWS Ground Station 위한 조치는 필요하지 않습니다. 이러한 에페메리드는 위성 ID와 관련된 두 줄의 요소 집합 () 입니다. TLEs NORAD 모든 기본 에페메리스의 우선순위는 0입니다. 따라서 에페메리스를 통해 업로드된 만료되지 않은 커스텀 에페메리드는 항상 오버라이드됩니다. 에페메리스는 항상 우선순위가 1 이상이어야 합니다. API

ID가 없는 위성은 사용자 지정 임시 데이터를 에 업로드해야 합니다. NORAD AWS Ground Station예를 들어 방금 발사되었거나 Space-Track 카탈로그에서 의도적으로 생략한 위성에는 ID가 없으므로 사용자 지정 에페메리드를 업로드해야 합니다. NORAD 사용자 지정 에페메리스 제공에 대한 자세한 내용은 사용자 지정 에페메리스 데이터 제공을 참조하세요.

맞춤형 에페메리스 데이터 제공

> **Important**
>
> 에페메리스는 현재 API 프리뷰 상태입니다.

Ephemeris에 대한 API 액세스는 필요한 경우에만 제공됩니다.
<### ## ##### #### #### # ## ### ### ## aws-groundstation@amazon.com ## #### ###

개요

Ephemeris를 API 사용하면 사용자 지정 에페메리드를 업로드하여 위성과 함께 사용할 수 있습니다. AWS Ground Station 이러한 에페메리드는 Space-Track의 기본 에페메리드보다 우선합니다 (참조:). 기본 에페메리스 데이터 Orbit Epemeris Message () 및 2줄 요소 () 형식의 에페메리스 데이터 수신을 지원합니다. OEM TLE

사용자 지정 에페메리드를 업로드하면 추적 품질이 향상되고, Space-Track 에페메리드를 사용할 수 없는 상황에서도 초기 작전을 처리할 수 있으며 기동성을 고려할 수 있습니다. AWS Ground Station

> **Note**
>
> 위성에 위성 카탈로그 번호가 할당되기 전에 사용자 지정 임시 데이터를 제공하는 경우 의 위성 카탈로그 번호 필드에 00000을 사용하고 TLE 또는 OEM 메타데이터의 국제 지정자 필드 발사 번호 부분에 000을 사용할 수 있습니다 (예: 2024년에 출시된 차량의 경우 24000A). TLE 형식에 대한 자세한 내용은 2줄 요소 집합을 참조하십시오. TLEs 형식에 대한 자세한 내용은 OEMs 을 참조하십시오OEM임시 형식.

OEM임시 형식

AWS Ground Station OEM고객이 제공한 에페메리데스를 표준에 따라 처리하고 몇 가지 추가 제한 사항을 적용합니다. CCSDS OEM파일은 형식이 맞아야 합니다. KVN 다음 표에는 an의 여러 필드와 표준과의 AWS Ground Station 차이점이 OEM 요약되어 있습니다. CCSDS

섹션	필드	CCSDS필수	AWS Ground Station 필수	참고
헤더	CCSDS_OEM_VERS	예	예	필수 값: 2.0
	COMMENT	아니요	아니요	
	CLASSIFICATION	아니요	아니요	
	CREATION_DATE	예	예	
	ORIGINATOR	예	예	
	MESSAGE_아이디	아니요	아니요	
메타데이터	META_START	예	예	
	COMMENT	아니요	아니요	
	OBJECT_NAME	예	예	
	OBJECT_아이디	예	예	
	CENTER_NAME	예	예	필수 값: 지구
	REF_FRAME	예	예	허용되는 값: EME2 000, ITRF2 000
	REF_FRAME_EPOCH	아니요	지원되지 않음*	허용된 REF FRAMEs _에 암시적 에포크가 있으므로 필요하지 않습니다.
	TIME_SYSTEM	예	예	필수 값: UTC

섹션	필드	CCSDS필수	AWS Ground Station 필수	참고
	START_TIME	예	예	
	USEABLE_START_TIME	아니요	아니요	
	USEABLE_STOP_TIME	아니요	아니요	
	STOP_TIME	예	예	
	INTERPOLATION	아니요	예	접점의 정확한 포인팅 AWS Ground Station 각도를 생성하기 위해 필요합니다.
	INTERPOLATION_DEGREES	아니요	예	접점의 정확한 포인팅 AWS Ground Station 각도를 생성하기 위해 필요합니다.
	META_STOP	예	예	
데이터	X	예	예	다음과 같이 표현됩니다. km
	Y	예	예	에서 대표 km
	Z	예	예	에서 대표 km
	X_ DOT	예	예	에 대표 km/s
	Y_ DOT	예	예	에 대표 km/s
	Z_ DOT	예	예	에 대표 km/s

섹션	필드	CCSDS필수	AWS Ground Station 필수	참고
	X_ DDOT	아니요	아니요	에 대표 km/s^2
	Y_ DDOT	아니요	아니요	에 대표 km/s^2
	Z_ DDOT	아니요	아니요	에 대표 km/s^2
공분산 행렬	COVARIANCE_START	아니요	아니요	
	EPOCH	아니요	아니요	
	COV_REF_FRAME	아니요	아니요	
	COVARIANCE_STOP	아니요	아니요	

* 에서 지원되지 않는 행이 제공된 AWS Ground Station OEM 항목에 포함된 경우 검증에 OEM 실패합니다.

에 대한 CCSDS 표준과의 중요한 편차는 AWS Ground Station 다음과 같습니다.

- CCSDSOEM_ VERS _는 필수입니다. `2.0`
- REFFRAME_는 `EME2000` 또는 중 하나여야 `ITRF2000` 합니다.
- REFFRAME_ EPOCH _는 지원되지 않습니다 AWS Ground Station.
- CENTERNAME_는 필수입니다`Earth`.
- TIMESYSTEM_는 필수입니다`UTC`.
- INTERPOLATION와 INTERPOLATION DEGREES _는 모두 AWS Ground Station CPE 필수입니다.

형식의 OEM 이피메리스 예시 KVN

다음은 -1 OEM 공영 방송사 위성의 형식을 잘라낸 예제입니다. KVN JPSS

```
CCSDS_OEM_VERS = 2.0

COMMENT Orbit data are consistent with planetary ephemeris DE-430

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

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

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

사용자 지정 이피머리스 만들기

의 작업을 사용하여 사용자 지정 이피머스를 만들 수 있습니다. CreateEphemeris AWS Ground Station API 이 작업은 요청 본문 또는 지정된 S3 버킷의 데이터를 사용하여 에페메리스를 업로드합니다.

한 가지 주의할 점은 에피메리스를 업로드하면 에피메리스가 VALIDATING로 설정되고 비동기 워크플로가 시작되어 에피메리스를 검증하고 이로부터 잠재적 접촉을 생성하는 비동기 워크플로가 시작된다는 점입니다. 임시 저장소가 이 워크플로를 통과한 후 ENABLED가 된 후에만 접촉에 사용됩니다. 이피머리스 상태를 DescribeEphemeris폴링하거나 CloudWatch 이벤트를 사용하여 이피머리스의 상태 변화를 추적해야 합니다.

잘못된 이페머리스 문제를 해결하려면 다음을 참조하십시오. 잘못된 에페메리데스 문제 해결

예: 다음을 통해 두 줄로 된 요소 () 를 생성하십시오. TLE API

및 는 AWS SDKs 호출을 통해 두 줄로 된 element (TLE) set ephemeris를 업로드하는 데 사용할 CLI 수 있습니다. AWS Ground Station CreateEphemeris 이 에페메리스는 위성의 기본 에페메리스 데이터 대신 사용됩니다(기본 에페메리스 데이터 참조). 이 예제에서는 AWS SDKfor Python (Boto3) 을 사용하여 이 작업을 수행하는 방법을 보여줍니다.

TLE집합은 하나 이상의 문자열을 TLEs 묶어 연속 궤적을 구성하는 JSON 형식이 지정된 객체입니다. TLEs집합의 TLE 집합은 궤적을 구성하는 데 사용할 수 있는 연속 집합을 형성해야 합니다 (즉, 집합 사이에 시간 간격이 없어야 함). TLEs TLE 예제 TLE 세트는 다음과 같습니다.

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

```
        "validTimeRange": {
            "startTime": 12346,
            "endTime": 12347
        }
    }
]
```

> **Note**
>
> 유효하고 연속적인 궤적이 되려면 TLE 세트의 시간 범위가 정확히 일치해야 합니다. TLEs

TLE세트는 다음과 같이 AWS Ground Station boto3 클라이언트를 통해 업로드할 수 있습니다.

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

이 호출은 미래에 에페머리스를 참조하는 데 사용할 수 있는 를 반환합니다. ephemerisId 예를 들어, 위 ephemerisId 호출에서 제공된 정보를 사용하여 이페머리스 상태를 폴링할 수 있습니다.

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

다음은 해당 DescribeEphemeris조치의 응답 예시입니다.

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

DescribeEphemeris경로를 폴링하거나 CloudWatch 이벤트를 사용하여 업로드된 Epemeris의 상태를 추적하는 것이 좋습니다. 업로드된 Epemeris가 설정되고 연락처 예약 ENABLED 및 실행에 사용할 수 있게 되려면 비동기 검증 워크플로를 거쳐야 하기 때문입니다.

참고로 위 예시에서는 TLE 세트의 모든 NORAD TLEs ID가 Space-Track 25994 데이터베이스에서 위성에 할당된 NORAD ID와 일치해야 합니다.

예: S3 버킷에서 이페메리스 데이터 업로드

또한 버킷과 객체 키를 가리키면 S3 버킷에서 직접 ephemeris 파일을 업로드할 수 있습니다. AWS Ground Station 사용자를 대신하여 객체를 검색합니다. 저장된 데이터의 암호화에 대한 자세한 내용은 AWSGround Station의 미사용 데이터 암호화에 자세히 설명되어 AWS Ground Station 있습니다.

다음은 S3 버킷에서 OEM 임시 파일을 업로드하는 예제입니다.

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

```
        }
    })
```

다음은 예제 코드의 이전 블록에 업로드된 OEM 에피메리스에 대해 호출된 DescribeEphemeris작업에서 반환된 데이터의 예제입니다.

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

예: 고객이 제공한 에페메리데스 사용 AWS Ground Station

고객이 제공한 에페메리드를 사용하는 방법에 대한 자세한 지침은 고객 제공 에페메리드 사용 (및 관련 리포지토리 AWS Ground Station aws-samples/) 을 참조하십시오. AWS Ground Station GitHub aws-groundstation-cpe

어떤 에페메리스가 사용됩니까?

에페메리스에는 우선 순위, 만료 시간 및 활성화 플래그가 있습니다. 이 둘을 종합하면 어떤 에페메리스가 위성에 사용되는지가 결정됩니다. 각 위성에 대해 하나의 에페메리스만 활성화할 수 있습니다.

사용할 에페메리스는 우선 순위가 가장 높은 활성화된 에페메리스로, 만료 시간은 미래입니다. 우선 순위 값이 클수록 우선 순위가 높습니다. 에서 ListContacts반환되는 사용 가능한 연락 시간은 이 임시 참조를 기준으로 합니다. 여러 개의 ENABLED 에페메리스의 우선 순위가 동일한 경우 가장 최근에 생성되거나 업데이트된 에페메리스가 사용됩니다.

> **Note**
>
> AWS Ground Station 위성당 ENABLED 고객이 제공한 에페메리데스 수에 대한 서비스 할당량이 있습니다 (참조: Service Quotas). 이 할당량에 도달한 후 에페메리스 데이터를 업로드하려면 우선 순위가 가장 낮거나 가장 먼저 생성된 고객 제공 에페메리스를 (DeleteEphemeris를 사용하여) 삭제하거나 (UpdateEphemeris를 사용하여) 비활성화하십시오.

생성된 이페메리스가 없거나 ENABLED 상태가 지정된 에페메리드가 없는 경우, 가능한 경우 Space-Track에서 제공하는 위성용 기본 이페메리스를 사용합니다. AWS Ground Station 이 기본 에페메리스의 우선순위는 0입니다.

새로운 에페메리데스가 이전에 예정된 접촉에 미치는 영향

활성 가시성 DescribeContact API시간을 반환하여 새 에페메리드가 이전에 예정된 접촉에 미치는 영향을 보려면 를 사용하십시오.

새 에페메리스를 업로드하기 전에 예약된 연락처는 원래 예정된 연락 시간을 유지하지만 안테나 추적에는 활성 에페메리스가 사용됩니다. 활성 에피메리스를 기준으로 한 우주선의 위치가 이전의 에피메리스와 크게 다를 경우, 송수신 사이트 마스크 밖에서 작동하는 우주선으로 인해 안테나와의 위성 접촉 시간이 단축될 수 있습니다. 따라서 이전 임시 연락처와 크게 다른 새 임시 항목을 업로드한 후에는 취소하고 향후 연락처를 다시 예약하는 것이 좋습니다. 를 사용하면 예정된 `startTime` 연락처와 `endTime` 반환된 연락처를 비교하여 전송/수신 사이트 마스크 외부에서 작동하는 우주선으로 인해 향후 접촉 중 사용할 수 없는 부분을 확인할 수 있습니다. DescribeContact API`visibilityStartTime` `visibilityEndTime` 향후 연락을 취소하고 일정을 다시 잡으려면 연락 시간 범위가 공개 시간 범위를 30초 이상 벗어나서는 안 됩니다. 취소된 연락을 연락 시간에 너무 가깝게 취소하면 비용이 발생할 수 있습니다. 취소된 연락처에 대한 자세한 내용은 Ground FAQs Station을 참조하십시오.

인공위성에 대한 현재 속성값 구하기

or 액션을 호출하여 특정 위성에 사용 중인 현재 이페머리스를 AWS Ground Station 검색할 수 있습니다. GetSatelliteListSatellites 이 두 메서드는 모두 현재 사용 중인 에페메리스에 대한 메타데이터를 반환합니다. 이 에페머리스 메타데이터는 업로드된 사용자 지정 에페메리드와 기본 에페메리드의 경우 다릅니다. AWS Ground Station

기본 에페메리스는 `source` 및 `epoch` 필드만 포함합니다. 이 시대는 Space-Track에서 가져온 2줄 요소 집합의 epoch시대이며, 현재는 위성의 궤적을 계산하는 데 사용되고 있습니다.

사용자 지정 에페메리스는 "CUSTOMER_PROVIDED"의 source 값을 가지며 ephemerisId 필드에 고유한 식별자가 포함됩니다. 이 고유 식별자는 액션을 통해 이피메리스를 쿼리하는 데 사용할 수 있습니다. DescribeEphemeris 작업을 통해 업로드하는 동안 에페메리스에 이름이 할당된 경우 선택적 name 필드가 반환됩니다. AWS Ground Station CreateEphemeris

에페메리드는 동적으로 AWS Ground Station 업데이트되므로 를 호출할 때 사용 중인 에페메리스의 스냅샷만 반환된다는 점에 유의하십시오. API

기본 에페메리스를 사용하는 위성의 **GetSatellite** 반환 예시

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

사용자 지정 **GetSatellite** 에페메리스를 사용하는 위성의 예

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

```
}
```

기본 임시 데이터로 되돌리기

사용자 지정 에페메리스 데이터를 업로드하면 해당 위성에 사용되는 기본 에페메리데스가 무시합니다. AWS Ground Station AWS Ground Station 현재 활성화되어 있고 만료되지 않은 고객 제공 에페메리드를 사용할 수 없을 때까지 기본 에페메리스를 다시 사용하지 않습니다. AWS Ground Station 또한 현재 고객이 제공한 임시 메모리의 만료 시간이 지난 연락처를 나열하지 않습니다. 해당 만료 시간 이후에 사용할 수 있는 기본 임시 메모리가 있더라도 마찬가지입니다.

기본 Space-Track 에페메리데스로 되돌리려면 다음 중 하나를 수행해야 합니다.

- 활성화된 고객 제공 에페메리드를 모두 삭제 (사용 DeleteEphemeris) 하거나 비활성화 (사용 UpdateEphemeris) 합니다. 를 사용하여 위성에 대해 고객이 제공한 에페메리드를 나열할 수 있습니다. ListEphemerides
- 고객이 제공한 기존 에페메리스가 모두 만료될 때까지 기다리세요.

전화를 걸어 GetSatellite위성의 현재 이페메리스가 맞는지 확인하면 기본 이피머스가 사용되고 있는지 확인할 수 있습니다. `source` `SPACE_TRACK` 기본 에페메리드에 대한 자세한 내용은 을 참조하십시오기본 에페메리스 데이터.

데이터 흐름

AWS Ground Station 노드와 에지 관계를 사용하여 데이터 흐름을 구성하여 데이터의 스트림 처리를 가능하게 합니다. 각 노드는 예상 처리를 설명하는 구성으로 표시됩니다. 이 개념을 설명하기 위해 a까지의 데이터 흐름을 생각해 보십시오. `antenna-downlink` `s3-recording` `antenna-downlink`노드는 구성에 정의된 파라미터에 따른 무선 주파수 스펙트럼의 아날로그-디지털 변환을 나타냅니다. 는 수신 데이터를 수신하여 S3 버킷에 저장하는 컴퓨팅 노드를 `s3-recording` 나타냅니다. 결과 데이터 흐름은 사양에 따라 S3 버킷으로 디지털화된 RF 데이터를 비동기식으로 전송하는 것입니다.

미션 프로필 내에서 요구 사항에 맞는 다양한 데이터 흐름을 생성할 수 있습니다. 다음 섹션에서는 함께 AWS Ground Station 사용할 다른 AWS 리소스를 설정하는 방법을 설명하고 데이터 흐름 구성을 위한 권장 사항을 제공합니다. 소스 노드로 간주되는지 대상 노드로 간주되는지를 포함하여 각 노드의 작동 방식에 대한 자세한 내용은 을 참조하십시오. 구성

주제

- AWS Ground Station 데이터 플레인 인터페이스
- 지역 간 데이터 전송 사용
- S3 - 설정 및 구성
- VPC- 설정 및 구성
- EC2- 설정 및 구성

AWS Ground Station 데이터 플레인 인터페이스

선택한 데이터 흐름의 결과 데이터 구조는 데이터 흐름의 소스에 따라 달라집니다. 이러한 형식의 세부 정보는 인공위성을 온보딩하는 동안 제공됩니다. 다음은 각 데이터 흐름 유형에 사용되는 형식을 요약한 것입니다.

- 안테나-다운링크
  - (대역폭 54 미만MHz) 데이터는 -49 신호 데이터/IP 형식 패킷으로 VITA 제공됩니다.
  - (대역폭 greater-than-or-equal -54MHz) 데이터는 클래스 2 패킷으로 전달됩니다. AWS Ground Station
- antenna-downlink-demod-decode
  - 데이터는 복조/디코딩된 데이터/IP 형식 패킷으로 전달됩니다.
- 안테나 업링크

  - 데이터는 VITA-49 신호 데이터/IP 형식 패킷으로 전달되어야 합니다.
- antenna-uplink-echo
  - 데이터는 VITA-49 신호 데이터/IP 형식 패킷으로 전달됩니다.

지역 간 데이터 전송 사용

AWS Ground Station 지역 간 데이터 전송 기능을 사용하면 안테나에서 AWS Ground Station 지원되는 AWS 모든 지역으로 데이터를 유연하게 전송할 수 있습니다. 즉, 인프라를 단일 AWS 지역에 유지 관리하고 가입한 모든 지역에서 연락을 AWS Ground Station 위치 예약할 수 있습니다.

Amazon S3 버킷으로 연락처 데이터를 수신하면 현재 AWS Ground Station 지원되는 모든 지역에서 지역 간 데이터 전송이 가능합니다. AWS Ground Station 모든 전송 측면을 대신 관리합니다.

AWS Ground Station 에이전트를 EC2 통해 Amazon으로 지역 간 데이터를 전송하는 것은 모든 antenna-to-destination 지역에서 가능합니다. 이 설정에는 고유한 구성이나 승인이 필요하지 않습니다.

아래 설명된 지역에서는 Dataflow 엔드포인트를 EC2 사용하여 Amazon으로 지역 간 데이터를 전송하는 것이 기본값*으로 제공됩니다. antenna-to-destination

- 미국 동부(오하이오) 리전(us-east-2)- 미국 서부(오레곤) 리전(us-west-2)
- 미국 서부(오레곤) 리전(us-west-2)- 미국 동부(오하이오) 리전(us-east-2)

Amazon EC2 인스턴스로 리전 간 데이터 전송을 사용하려면 현재 지역에 dataflow 엔드포인트를 생성하고 동일한 AWS 지역을 dataflow-endpoint-config지정해야 합니다.

지역 간 데이터 전송을 위해 지원되는 지역 및 전송 방법을 자세히 설명하는 이전 정보가 다음 표에 요약되어 있습니다.

수신 방법	안테나 영역	수신 지역
아마존 S3 데이터 전송	모두 온보딩됨 AWS Ground Station 위치	모든 지역AWS Ground Station
AWS Ground Station 아마존 에이전트 EC2	모두 온보딩 AWS Ground Station 위치	모든 지역AWS Ground Station
Amazon의 데이터 흐름 엔드포인트* EC2	미국 동부(오하이오) 리전(us-east-2)	미국 서부(오레곤) 리전(us-west-2)

수신 방법	안테나 영역	수신 지역
	미국 서부(오레곤) 리전(us-west-2)	미국 동부(오하이오) 리전(us-east-2)

*목록에 없는 추가 antenna-to-destination 지역은 특별한 Amazon EC2 및 소프트웨어 설정이 필요합니다. 온보딩 지침은 <aws-groundstation@amazon.com ##> 문의하십시오.

S3 - 설정 및 구성

Amazon S3 버킷을 사용하여 AWS Ground Station다운링크 신호를 수신할 수 있습니다. 대상 s3-recording-config를 생성하려면 Amazon S3 버킷과 해당 버킷에 파일을 쓸 권한을 부여하는 IAM AWS Ground Station 역할을 지정할 수 있어야 합니다.

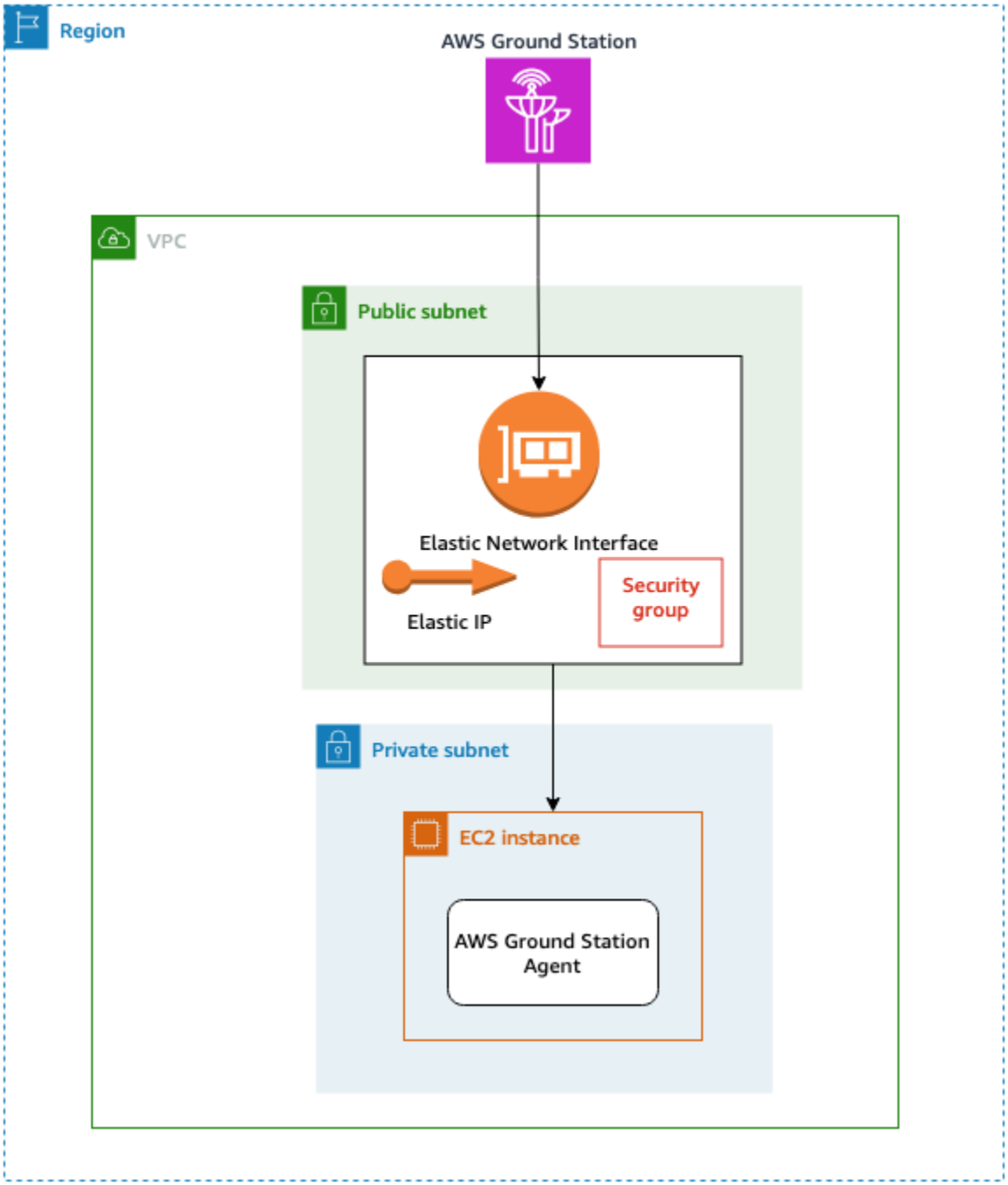
Amazon S3 버킷, IAM 역할 또는 AWS Ground Station 구성 생성에 아마존 S3 레코딩 구성 대한 제한 사항은 을 참조하십시오.

VPC- 설정 및 구성

설정을 위한 전체 가이드는 이 가이드의 범위를 벗어납니다. VPC 자세한 내용은 AWSVPC사용 설명서를 참조하십시오.

이 섹션에서는 Amazon EC2 엔드포인트와 dataflow 엔드포인트가 어떻게 내부에 존재할 수 있는지 설명합니다. VPC AWS Ground Station 특정 데이터 흐름에 대해 여러 전송 지점을 지원하지 않습니다. 각 데이터 흐름은 단일 수신자로 종료될 것으로 예상됩니다. EC2 EC2수신기가 한 개일 것으로 예상되지만 다중 AZ 이중화 구성은 아닙니다. 를 사용하는 전체 예제는 VPC 을 참조하십시오. 미션 프로필 구성 예시

VPC AWS Ground Station 에이전트를 사용한 구성



위성 데이터는 안테나와 가까운 AWS Ground Station 에이전트 인스턴스에 제공됩니다. AWS Ground Station 에이전트는 사용자가 제공한 AWS KMS 키를 사용하여 데이터를 스트라이핑한 다음 암호화합니다. 각 스트라이프는 AWS 네트워크 백본을 통해 소스 안테나에서 Amazon EC2 Elastic IP (EIP) 로 전송됩니다. 데이터는 연결된 Amazon EC2 엘라스틱 네트워크 인터페이스 (ENI) 를 통해 EC2 인스턴스에 도착합니다. EC2인스턴스에 도착하면 설치된 AWS Ground Station 에이전트가 데이터를 해독하

고 정방향 오류 수정 (FEC) 을 수행하여 삭제된 데이터를 복구한 다음 설정에서 지정한 IP 및 포트로 전달합니다.

아래 목록은 AWS Ground Station 에이전트 딜리버리를 설정할 때 고려할 수 있는 고유한 설정 고려 사항을 VPC 나타냅니다.

보안 그룹 - AWS Ground Station 트래픽만 전담하는 보안 그룹을 설정하는 것이 좋습니다. 이 보안 그룹은 Dataflow 엔드포인트 그룹에 지정한 것과 동일한 포트 범위에서 UDP 인그레스 트래픽을 허용해야 합니다. AWS Ground Station 권한을 IP 주소로만 제한하는 AWS 관리형 접두사 목록을 유지 관리합니다. AWS Ground Station 배포 지역에서 를 교체하는 방법에 대한 자세한 내용은 AWS관리형 접두사 목록을 참조하십시오. PrefixListId

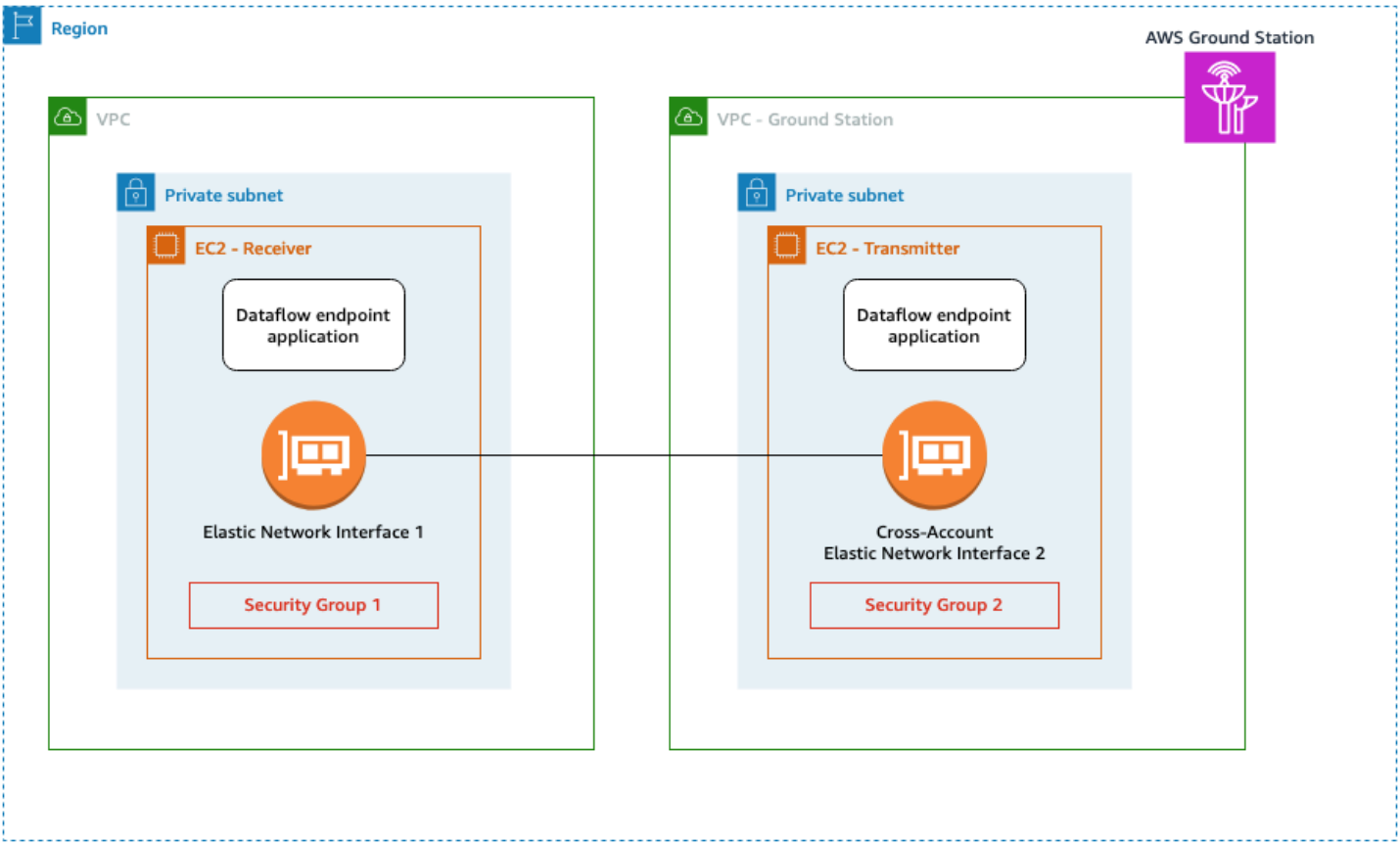
Elastic Network Interface (ENI) - 위의 보안 그룹을 여기에 연결하고 퍼블릭 서브넷에 배치해야 합니다. ENI

다음 CloudFormation 템플릿은 이 섹션에 설명된 인프라를 생성하는 방법을 보여줍니다.

```
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
```

VPC데이터 흐름 엔드포인트를 사용한 구성



위성 데이터는 안테나와 가까운 데이터 흐름 엔드포인트 애플리케이션 인스턴스에 제공됩니다. 그런 다음 VPC 소유자로부터 계정 간 Amazon EC2 Elastic Network Interface (ENI) 를 통해 데이터를 전송합니다. AWS Ground Station그러면 데이터가 ENI 연결된 Amazon EC2 EC2 인스턴스를 통해 인스턴스에 도착합니다. 그러면 설치된 데이터 흐름 엔드포인트 애플리케이션이 설정에서 지정한 IP 및 포트로 데이터를 전달합니다. 업링크 연결의 경우 이 흐름의 반대 현상이 발생합니다.

아래 목록은 데이터 흐름 엔드포인트 전송을 설정할 때 고려할 수 VPC 있는 고유한 설정 고려 사항을 설명합니다.

IAM역할 - IAM 역할은 Dataflow 엔드포인트의 일부이며 다이어그램에 표시되어 있지 않습니다. 교차 계정을 ENI 생성하고 AWS Ground Station Amazon EC2 인스턴스에 연결하는 데 사용되는 IAM 역할입니다.

보안 그룹 1 - 이 보안 그룹은 사용자 계정의 Amazon EC2 인스턴스와 연결될 보안 그룹에 연결됩니다. ENI 사용자 지정 포트를 통해 보안 그룹 2에서 들어오는 UDP 트래픽을 허용해야 dataflow-endpoint-group합니다.

엘라스틱 네트워크 인터페이스 (ENI) 1 - 보안 그룹 1을 여기에 연결하고 서브넷에 배치해야 합니다. ENI

보안 그룹 2 - 이 보안 그룹은 Dataflow 엔드포인트에서 참조됩니다. 이 보안 그룹은 계정에 데이터를 ENI 저장하는 AWS Ground Station 데 사용할 보안 그룹에 연결됩니다.

지역 - 지역 간 연결이 지원되는 지역에 대한 자세한 내용은 을 참조하십시오지역 간 데이터 전송 사용.

다음 CloudFormation 템플릿은 이 섹션에 설명된 인프라를 만드는 방법을 보여줍니다.

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

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

InstanceSecurityGroup:
  Type: AWS::EC2::SecurityGroup
  Properties:
```

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

EC2- 설정 및 구성

에이전트 또는 데이터 흐름 엔드포인트를 통해 VITA -49 신호/IP 데이터 또는 VITA -49 확장 데이터/IP를 동기식으로 전송하려면 EC2 인스턴스를 올바르게 구성해야 합니다. AWS Ground Station 특정 요구 사항에 따라 동일한 인스턴스에서 프런트 엔드 (FE) 프로세서 또는 소프트웨어 정의 라디오 (SDR)를 직접 수행하거나 추가 인스턴스를 사용해야 할 수 있습니다. EC2 FE 또는 FE 선택 및 SDR 설치는 이 사용 설명서의 범위를 벗어납니다. 특정 데이터 형식에 대한 자세한 내용은 을 참조하십시오AWS Ground Station 데이터 플레인 인터페이스.

서비스 약관에 대한 자세한 내용은 서비스 약관을 참조하십시오AWS .

제공된 공통 소프트웨어

AWS Ground Station EC2인스턴스를 쉽게 설정할 수 있는 공통 소프트웨어를 제공합니다.

AWS Ground Station 에이전트

AWS Ground Station 에이전트는 디지털 중간 주파수 (DigiF) 다운링크 데이터를 수신하고 다음을 가능하게 하는 복호화된 데이터를 송신합니다.

- 40에서 MHz MHz 400까지의 대역폭의 DiGif 다운링크 기능을 제공합니다.
- 네트워크 상의 모든 퍼블릭 IP (AWSElastic IP) 로 고속, 저지터 DigiF 데이터 전송 AWS
- 순방향 오류 수정 () 을 사용하여 데이터를 안정적으로 전달합니다. FEC
- 암호화를 위한 고객 관리 AWS KMS 키를 사용하여 데이터를 안전하게 전송합니다.

자세한 내용은 AWS Ground Station 상담원 사용 설명서를 참조하십시오.

Dataflow 엔드포인트 애플리케이션

AWS Ground Station 안테나 위치와 Amazon EC2 인스턴스 간에 데이터를 보내고 받는 AWS Ground Station 데 사용되는 네트워킹 애플리케이션입니다. 데이터의 업링크 및 다운링크에 사용할 수 있습니다.

소프트웨어 정의 라디오 () SDR

위성과 통신하는 데 사용되는 신호를 변조/복조하는 데 사용할 수 있는 소프트웨어 정의 라디오 (SDR) 입니다.

AWS Ground Station 아마존 머신 이미지 (AMIs)

이러한 설치의 빌드 및 구성 시간을 단축하기 위해 사전 AMIs 구성된 AWS Ground Station 서비스도 제공합니다. 온보딩이 AMIs 완료되면 사용자 계정에서 데이터 흐름 엔드포인트 네트워킹 애플리케이션과 소프트웨어 정의 라디오 (SDR) 를 사용할 수 있습니다. Amazon EC2 콘솔에서 비공개 Amazon 머신 이미지 (AMIs) 에서 그라운드 스테이션을 검색하여 찾을 수 있습니다. AMIswith AWS Ground Station Agent는 공개되며 Amazon EC2 콘솔에서 공개 Amazon Machine Images (AMIs) 에서 그라운드 스테이션을 검색하면 찾을 수 있습니다.

연락처

AWS Ground Station 콘솔을 사용하거나 원하는 언어로 위성 데이터를 입력하고, 안테나 위치를 식별하고, 통신하고 AWS CLI, 선택한 위성에 대한 안테나 시간을 예약할 수 있습니다. AWS SDK 연락 시작* 최대 15분 전까지 연락처 예약을 검토, 취소 및 조정할 수 있습니다. 또한, 예약 시간 가격 책정 모델을 사용하는 경우 예약 시간 요금제의 세부 정보를 볼 수 있습니다. AWS Ground Station

AWS Ground Station 지역 간 데이터 전송을 지원합니다. 선택한 미션 프로파일의 일부인 데이터 흐름 엔드포인트 구성에 따라 데이터가 전송되는 리전이 결정됩니다. 지역 간 데이터 전송 사용에 대한 자세한 내용은 을 참조하십시오. 지역 간 데이터 전송 사용

접촉을 예약하려면 리소스를 구성해야 합니다. 리소스를 구성하지 않은 경우 을 참조하십시오시작하기.

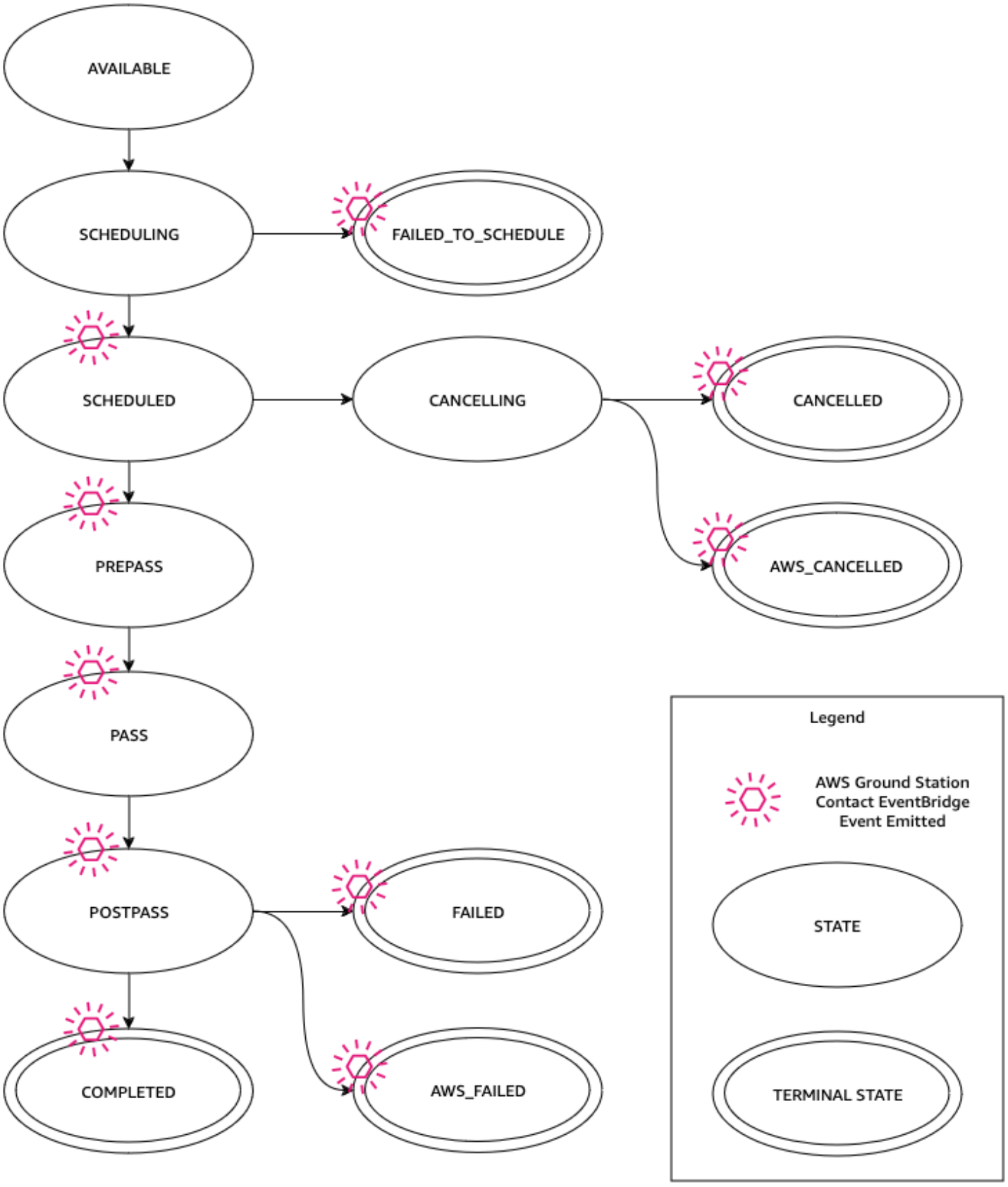
* 취소한 문의는 연락 시간에 너무 가까운 시점에 취소할 경우 비용이 발생할 수 있습니다. 취소된 연락처에 대한 자세한 내용은 Ground FAQs Station을 참조하십시오.

주제

- 연락처 라이프사이클

연락처 라이프사이클

연락처 라이프사이클을 이해하면 자동화를 구성하는 방법과 문제 해결 노력을 결정하는 데 도움이 될 수 있습니다. 다음 다이어그램은 AWS Ground Station 연락처 수명 주기와 수명 주기 동안 발생하는 이벤트 브리지 이벤트를 보여줍니다. 중요한 점은,, FAILED _TO_ COMPLETEDFAILED, _, AWS _ SCHEDULE CANCELLEDCANCELLED, FAILED _가 터미널 상태라는 AWS 점입니다. 연락처는 터미널 상태 밖으로 전환되지 않습니다. 각 상태가 나타내는 내용에 AWS Ground Station 연락처 상태 대한 자세한 내용은 를 참조하십시오.


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 연락처 상태

AWS Ground Station 연락처 상태를 통해 특정 시간에 해당 연락처에 무슨 일이 일어나고 있는지 파악할 수 있습니다.

연락처 상태

다음은 접촉이 가질 수 있는 상태 목록입니다.

- AVAILABLE- 연락처는 예약이 가능합니다.
- SCHEDULING- 연락처 예약 중입니다.
- SCHEDULED- 연락이 성공적으로 예약되었습니다.
- FAILED_TO_ SCHEDULE - 연락을 예약하지 못했습니다.
- PREPASS- 연락이 곧 시작되며 리소스를 준비 중입니다.
- PASS- 현재 연락이 실행 중이며 위성과 통신 중입니다.
- POSTPASS- 통신이 완료되었으며 사용된 리소스를 정리하고 있습니다.
- COMPLETED- 연락이 오류 없이 완료되었습니다.
- FAILED- 리소스 구성 문제 때문에 연락이 실패했습니다.
- AWS_ FAILED - AWS Ground Station 서비스 문제 때문에 연락이 실패했습니다.
- CANCELLING- 연락처가 취소되는 중입니다.
- AWS_ CANCELLED - 서비스에 의해 연락이 취소되었습니다. AWS Ground Station 이러한 상황이 발생할 수 있는 예로는 안테나 또는 사이트 유지 관리, 임시 드리프트 등이 있습니다.
- CANCELLED- 귀하에 의해 연락이 취소되었습니다.

AWS Ground Station 디지털 트윈

의 디지털 트윈 기능은 위성 임무 관리 및 명령 및 제어 소프트웨어를 테스트하고 통합할 수 있는 환경을 AWS Ground Station 제공합니다. 디지털 트윈 기능을 사용하면 프로덕션 안테나 용량을 사용하지 않고도 스케줄링, 구성 검증 및 적절한 오류 처리를 테스트할 수 있습니다. 디지털 트윈 기능과의 AWS Ground Station 통합 테스트를 통해 위성 운영을 원활하게 관리할 수 있는 시스템의 능력에 대한 신뢰도를 높일 수 있습니다. 또한 생산 능력을 사용하거나 스펙트럼 라이선스를 AWS Ground Station APIs 요구하지 않고도 테스트할 수 있습니다.

시작하려면 1단계: 새틀라이트 온보딩 팔로우하고 디지털 트윈 기능에 대한 온보딩을 요청하세요. 위성이 디지털 트윈 기능에 온보딩되면 디지털 트윈 그라운드 스테이션과 연락을 예약할 수 있습니다. 액세스할 수 있는 지상국 목록은 응답을 통해 검색할 수 있습니다. AWS SDK ListGroundStations 디지털 트윈 그라운드 스테이션은 Ground Station 이름 앞에 “디지털 트윈”이라는 수정 접두사가 위치 붙은 상태로 등재된 그라운드 스테이션의 정확한 사본입니다. 여기에는 사이트 마스크와 실제 GPS 좌표를 포함하나 이에 국한되지 않는 메타데이터 및 안테나 기능이 포함됩니다. 현재 디지털 트윈 기능은 에 설명된 데이터 전송을 지원하지 않습니다데이터 흐름.

일단 온보딩되면 디지털 트윈 기능은 에 설명된 프로덕션 서비스와 동일한 Amazon EventBridge 이벤트 및 API 응답을 내보냅니다. 이벤트를 AWS Ground Station 이용한 자동화 이러한 이벤트를 통해 구성 및 데이터 흐름 엔드포인트 그룹을 미세 조정할 수 있습니다.

모니터링

모니터링은 AWS Ground Station의 안정성, 가용성 및 성능을 유지하는 데 중요한 부분입니다. AWS감시, 문제 발생 시 보고 AWS Ground Station, 적절한 경우 자동 조치를 취할 수 있는 다음과 같은 모니터링 도구를 제공합니다.

- AWS EventBridge 이벤트는 AWS 리소스 변경을 설명하는 시스템 이벤트의 스트림을 거의 실시간으로 제공합니다. EventBridge 이벤트를 사용하면 특정 이벤트를 감시하고 이러한 이벤트가 발생할 경우 다른 AWS 서비스에서 자동화된 작업을 트리거하는 규칙을 작성할 수 있으므로 자동화된 이벤트 기반 컴퓨팅이 가능합니다. EventBridge 이벤트에 대한 자세한 내용은 Amazon EventBridge Events 사용 설명서를 참조하십시오.
- AWS CloudTrail사용자 계정에서 또는 AWS 계정을 대신하여 이루어진 API 호출 및 관련 이벤트를 캡처하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 어떤 사용자와 계정이 전화를 걸었는지 AWS, 어떤 소스 IP 주소에서 호출이 이루어졌는지, 언제 호출이 발생했는지 식별할 수 있습니다. 에 대한 AWS CloudTrail자세한 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.
- Amazon CloudWatch Metrics는 예약 연락처의 사용 시 지표를 AWS Ground Station캡처합니다. CloudWatch 지표를 사용하면 채널, 편파 및 위성 ID를 기반으로 데이터를 분석하여 연락처의 신호 강도와 오류를 식별할 수 있습니다. 자세한 내용은 Amazon CloudWatch 지표 사용을 참조하십시오.
- AWS 사용자 알림 AWS Ground Station 이벤트에 대한 알림을 받을 전송 채널을 설정하는 데 사용할 수 있습니다. 이벤트가 지정한 규칙과 일치하면 알림을 받습니다. 이메일, AWS Chatbot 채팅 알림 또는 AWS Console Mobile Application 푸시 알림을 비롯한 여러 채널을 통해 이벤트에 대한 알림을 받을 수 있습니다. AWS 콘솔 알림 센터에서도 알림을 볼 수 있습니다. 사용자 알림 집계를 지원하여 특정 이벤트 중에 받는 알림 수를 줄일 수 있습니다.

다음 항목을 사용하여 AWS Ground Station을 모니터링하십시오.

주제

- 이벤트를 AWS Ground Station 이용한 자동화
- 를 사용하여 AWS Ground Station API 통화 기록하기 AWS CloudTrail
- Amazon을 사용한 메트릭스 CloudWatch

이벤트를 AWS Ground Station 이용한 자동화

> **Note**
>
> 이 문서에서는 전체적으로 “이벤트”라는 용어를 사용합니다. CloudWatch EventBridge 이벤트는 동일한 기본 서비스이며API. 두 서비스를 사용하면 수신 이벤트를 확인한 후 처리 대상으로 라우팅하는 규칙을 생성할 수 있습니다.

이벤트를 사용하면 AWS 서비스를 자동화하고 애플리케이션 가용성 문제나 리소스 변경과 같은 시스템 이벤트에 자동으로 대응할 수 있습니다. AWS 서비스의 이벤트는 거의 실시간으로 전달됩니다. 원하는 이벤트만 표시하도록 간단한 규칙을 작성한 후 규칙과 일치하는 이벤트 발생 시 실행할 자동화 작업을 지정할 수 있습니다. 자동으로 트리거될 수 있는 일부 작업은 다음과 같습니다.

- 함수 호출 AWS Lambda
- 아마존 EC2 실행 커맨드 호출
- Amazon Kinesis Data Streams로 이벤트 릴레이
- 스테이트 머신 활성화 AWS Step Functions
- 아마존 SNS 주제 또는 아마존 대기열에 알림 SQS

이벤트와 함께 AWS Ground Station 사용하는 몇 가지 예는 다음과 같습니다.

- Lambda 함수를 호출하여 이벤트 상태에 따라 EC2 Amazon 인스턴스의 시작 및 중지를 자동화합니다.
- 연락처 상태가 변경될 때마다 Amazon SNS 주제에 게시합니다. 이러한 주제는 접촉의 시작 또는 끝 부분에 이메일 공지를 보내도록 설정할 수 있습니다.

자세한 내용은 Amazon EventBridge Events 사용 설명서를 참조하십시오.

AWS Ground Station 이벤트 유형

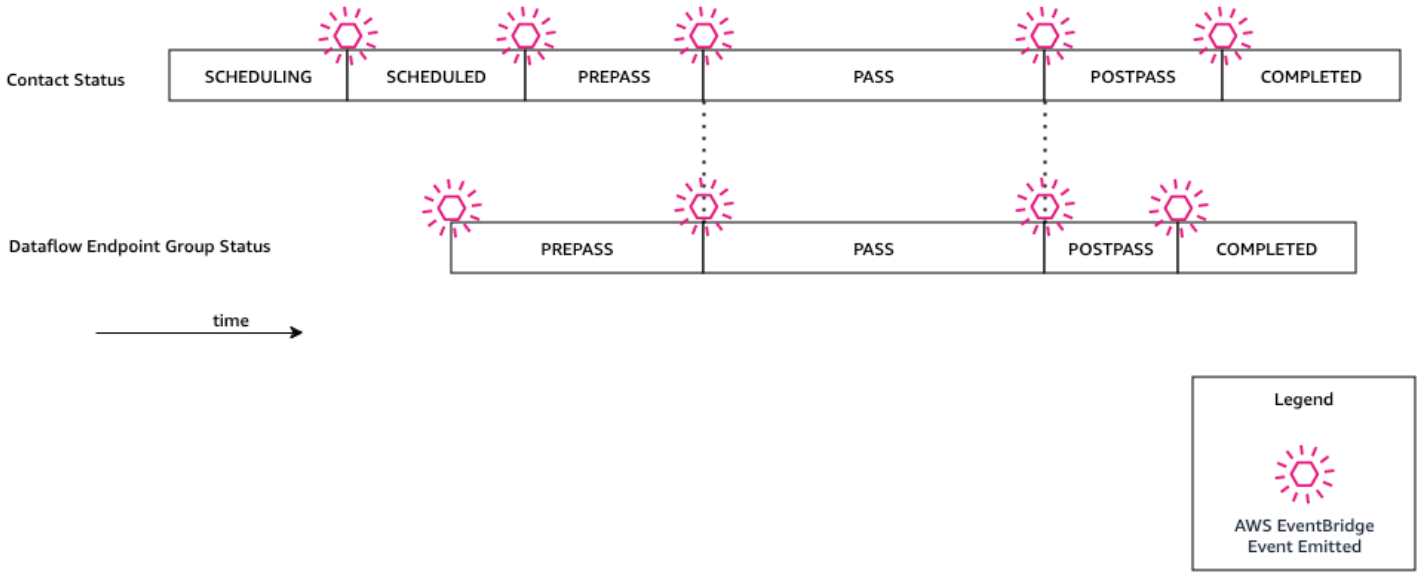
> **Note**
>
> AWSGround Station에서 생성되는 모든 이벤트는 “소스”의 값으로 “aws.groundstation”을 사용합니다.

AWS Ground Station 상태 변경과 관련된 이벤트를 내보내 자동화를 사용자 지정하는 기능을 지원합니다. 현재 연락처 상태 변경 이벤트, 데이터 흐름 엔드포인트 그룹 변경 이벤트 및 임시 상태 변경 이벤트를 AWS Ground Station 지원합니다. 다음 섹션에서는 각 유형에 대한 자세한 정보를 제공합니다.

연락처 이벤트 타임라인

AWS Ground Station 연락처 상태가 변경되면 이벤트를 내보냅니다. 이러한 상태 변경의 정의 및 상태 자체의 의미에 대한 자세한 내용은 을 참조하십시오연락처 라이프사이클. 연락처에서 사용되는 모든 데이터 흐름 엔드포인트 그룹에는 내보내는 독립적인 이벤트 집합이 있습니다. 같은 기간 동안 당사는 데이터 흐름 엔드포인트 그룹을 위한 이벤트도 내보냅니다. 미션 프로필과 데이터 흐름 엔드포인트 그룹을 설정할 때 사전 통과 및 사후 통과 이벤트의 정확한 시간을 구성할 수 있습니다.

다음 다이어그램은 공칭 연락처 및 관련 데이터 흐름 엔드포인트 그룹에 대해 발생하는 상태 및 이벤트를 보여줍니다.



Ground Station 접촉 상태 변경

예정된 연락처의 상태가 변경될 때 특정 작업을 수행하려는 경우 이 작업을 자동화하는 규칙을 설정할 수 있습니다. 이 기능은 접촉의 상태 변경에 대한 알림을 수신하려는 경우에 유용합니다. 이러한 이벤트를 받았을 때 변경하고 싶다면 임무 프로필의 contactPrePassDurationSeconds및 을 수정할 수 contactPostPassDurationSeconds있습니다. 이벤트는 접촉이 예약된 리전으로 전송됩니다.

이벤트 예시는 다음과 같습니다.

```
{
    "version": "0",
    "id": "01234567-0123-0123",
    "account": "123456789012",
    "time": "2019-05-30T17:40:30Z",
    "region": "us-west-2",
    "source": "aws.groundstation",
    "resources": [
        "arn:aws:groundstation:us-
west-2:123456789012:contact/11111111-1111-1111-1111-111111111111"
    ],
    "detailType": "Ground Station Contact State Change",
    "detail": {
        "contactId": "11111111-1111-1111-1111-111111111111",
        "groundstationId": "Ground Station 1",
        "missionProfileArn": "arn:aws:groundstation:us-west-2:123456789012:mission-
profile/11111111-1111-1111-1111-111111111111",
        "satelliteArn":
 "arn:aws:groundstation::123456789012:satellite/11111111-1111-1111-1111-111111111111",
        "contactStatus": "PASS"
    },
    "account": "123456789012"
}
```

contactStatus에 대해 가능한 값은 the section called “AWS Ground Station 연락처 상태”에 정의됩니다.

Ground Station 데이터 흐름 엔드포인트 그룹 상태 변경

데이터 흐름 엔드포인트 그룹이 데이터 수신에 사용 중일 때 작업을 수행하고 싶으면 이 작업을 자동화하도록 규칙을 설정할 수 있습니다. 이렇게 하면 데이터 흐름 엔드포인트 그룹의 상태 변경에 따라 다른 작업을 수행할 수 있습니다. 이러한 이벤트 수신 시기를 변경하려면 다른 contactPrePassDurationSeconds및 를 포함하는 데이터 흐름 엔드포인트 그룹을 사용하십시오. contactPostPassDurationSeconds 이 이벤트는 데이터 흐름 엔드포인트 그룹의 리전으로 전송됩니다.

아래에 예제가 나와 있습니다.

```
{
    "version": "0",
    "id": "01234567-0123-0123",
    "account": "123456789012",
```

```
    "time": "2019-05-30T17:40:30Z",
    "region": "us-west-2",
    "source": "aws.groundstation",
    "resources": [
        "arn:aws:groundstation:us-west-2:123456789012:dataflow-endpoint-group/
bad957a8-1d60-4c45-a92a-39febd98921d",
        "arn:aws:groundstation:us-west-2:123456789012:contact/98ddd10f-f2bc-479c-
bf7d-55644737fb09",
        "arn:aws:groundstation:us-west-2:123456789012:mission-profile/c513c84c-
eb40-4473-88a2-d482648c9234"
    ],
    "detailType": "Ground Station Dataflow Endpoint Group State Change",
    "detail": {
        "dataflowEndpointGroupId": "bad957a8-1d60-4c45-a92a-39febd98921d",
        "groundstationId": "Ground Station 1",
        "contactId": "98ddd10f-f2bc-479c-bf7d-55644737fb09",
        "dataflowEndpointGroupArn": "arn:aws:groundstation:us-
west-2:680367718957:dataflow-endpoint-group/bad957a8-1d60-4c45-a92a-39febd98921d",
        "missionProfileArn": "arn:aws:groundstation:us-west-2:123456789012:mission-
profile/c513c84c-eb40-4473-88a2-d482648c9234",
        "dataflowEndpointGroupState": "PREPASS"
    },
    "account": "123456789012"
}
```

dataflowEndpointGroupState에서 가능한 상태로는 PREPASS, PASS, POSTPASS 및 COMPLETED가 있습니다.

에페메리스 이벤트

Ground Station 에페메리스 상태 변경

에페메리스가 상태를 변경할 때 특정 작업을 수행하려는 경우 이 작업을 자동화하도록 규칙을 설정할 수 있습니다. 이렇게 하면 상태를 변경하는 에페메리스에 따라 다양한 작업을 수행할 수 있습니다. 예를 들어, 에페메리스의 검증이 완료되었는데 지금은 ENABLED일 때 작업을 수행할 수 있습니다. 이 이벤트에 대한 알림은 에페메리스가 업로드된 리전으로 전송됩니다.

아래에 예제가 나와 있습니다.

```
    {
    "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"
    }
    }
```

ephemerisStatus에서 가능한 상태로는 ENABLED, VALIDATING, INVALID, ERROR, DISABLED, EXPIRED가 있습니다.

를 사용하여 AWS Ground Station API 통화 기록하기 AWS CloudTrail

AWS Ground Station 사용자 AWS CloudTrail, 역할 또는 서비스가 수행한 작업의 기록을 제공하는 AWS 서비스와 통합되어 AWS Ground Station있습니다. CloudTrail AWS Ground Station as에 대한 모든 API 호출을 이벤트로 캡처합니다. 캡처된 호출에는 AWS Ground Station 콘솔에서의 호출과 AWS Ground Station API 작업에 대한 코드 호출이 포함됩니다. 트레일을 생성하면 에 대한 이벤트를 포함하여 Amazon S3 버킷으로 CloudTrail 이벤트를 지속적으로 전송할 수 AWS Ground Station있습니다. 트레일을 구성하지 않아도 CloudTrail 콘솔의 이벤트 기록에서 가장 최근 이벤트를 계속 볼 수 있습니다. 에서 수집한 CloudTrail 정보를 사용하여 요청을 받은 사람 AWS Ground Station, 요청한 IP 주소, 요청한 사람, 요청 시기 및 추가 세부 정보를 확인할 수 있습니다.

자세한 CloudTrail 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.

AWS Ground Station 정보: CloudTrail

CloudTrail 계정을 만들면 AWS 계정에서 활성화됩니다. 에서 AWS Ground Station활동이 발생하면 해당 활동이 CloudTrail 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 이벤트에 기록됩니다. AWS

계정에서 최근 이벤트를 보고, 검색하고, 다운로드할 수 있습니다. 자세한 내용은 이벤트 기록으로 CloudTrail 이벤트 보기를 참조하십시오.

에 대한 이벤트를 포함하여 AWS 계정에서 진행 중인 이벤트의 기록을 보려면 AWS Ground Station 트레일을 생성하세요. 트레일을 사용하면 CloudTrail Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 기본적으로 콘솔에서 트레일을 생성하면 트레일이 모든 AWS 지역에 적용됩니다. 트레일은 AWS 파티션에 있는 모든 지역의 이벤트를 기록하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 또한 CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 이에 따라 조치를 취하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음 자료를 참조하십시오.

- 추적 생성 개요
- CloudTrail 지원되는 서비스 및 통합
- 에 대한 Amazon SNS 알림 구성 CloudTrail
- 여러 지역에서 CloudTrail 로그 파일 수신 및 여러 계정으로부터 CloudTrail 로그 파일 수신

모든 AWS Ground Station 작업은 참조에 CloudTrail 기록되며 AWS Ground Station API참조에 문서화되어 있습니다. 예를 들어`ReserveContact`, 에 대한 호출 `CancelContact` 및 `ListConfigs` 작업은 CloudTrail 로그 파일에 항목을 생성합니다.

모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. 보안 인증 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청이 루트 또는 AWS Identity and Access Management (IAM) 사용자 자격 증명으로 이루어졌는지 여부.
- 역할 또는 페더레이션 사용자에 대한 임시 보안 보안 인증을 사용하여 요청이 생성되었는지 여부.
- 다른 AWS 서비스에서 요청했는지 여부.

자세한 내용은 CloudTrail userIdentity요소를 참조하십시오.

AWS Ground Station 로그 파일 항목 이해

트레일은 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 전송할 수 있는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함되어 있습니다. 이벤트는 모든 소스의 단일 요청을 나타내며 요청된 작업, 작업 날짜 및 시간, 요청 매개 변수 등에 대한 정보를 포함합니다. CloudTrail 로그 파일은 공개 API 호출의 정렬된 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

다음 예제는 `ReserveContact` 작업을 보여주는 CloudTrail 로그 항목을 보여줍니다.

예: 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"
}
```

Amazon을 사용한 메트릭스 CloudWatch

연락 중에 AWS Ground Station 자동으로 데이터를 캡처하여 분석을 CloudWatch 위해 전송합니다. Amazon CloudWatch 콘솔에서 데이터를 볼 수 있습니다. 액세스 및 CloudWatch 지표에 대한 자세한 내용은 Amazon CloudWatch 지표 사용을 참조하십시오.

AWS Ground Station 지표 및 차원

사용할 수 있는 지표는 무엇입니까?

에서 사용할 수 있는 지표는 다음과 같습니다 AWS Ground Station.

> **Note**
>
> 생성되는 특정 지표는 사용 중인 AWS Ground Station 기능에 따라 다릅니다. 구성에 따라 아래 지표 중 일부만 내보낼 수 있습니다.

지표	측정치 차원	설명
`AzimuthAngle`	SatelliteId	안테나의 방위각. 진북쪽은 0도이고 동쪽은 90도입니다. 단위: 도
`BitErrorRate`	채널, 편광, SatelliteId	지정된 비트 전송 횟수에서 비트에 대한 오류율입니다. 비트 오류는 노이즈, 왜곡 또

지표	측정치 차원	설명
		는 간섭으로 인해 발생합니다. 단위: 단위 시간당 비트 오류
BlockErrorRate	채널, 편광, SatelliteId	지정된 수신 블록의 수에서 블록의 오류율입니다. 블록 오류는 간섭으로 인해 발생합니다. 단위: 잘못된 블록/총 블록 수
CarrierFrequencyRecovery_Cn0	카테고리, 구성, SatelliteId	단위 대역폭당 캐리어 대 잡음 밀도 비율. 단위: 데시벨-헤르츠(dB-Hz)
CarrierFrequencyRecovery_Locked	카테고리, 구성, SatelliteId	복조기 캐리어 주파수 복구 루프가 잠겨 있으면 1로 설정하고 잠금 해제되면 0으로 설정합니다. 단위: 단위 없음

지표	측정치 차원	설명
CarrierFrequencyRecovery_OffsetFrequency_Hz	카테고리, 구성, SatelliteId	추정된 신호 중심과 이상적인 중심 주파수 사이의 오프셋. 이는 우주선과 안테나 시스템 사이의 도플러 시프트 및 로컬 오실레이터 오프셋으로 인해 발생합니다. 단위: 헤르츠(Hz)
ElevationAngle	SatelliteId	안테나의 고도 각도. 수평선은 0도이고 천정은 90도입니다. 단위: 도
Es/N0	채널, 편광, SatelliteId	심볼당 에너지 대 노이즈 파워 스펙트럼 밀도의 비율. 단위: 데시벨(dB)
ReceivedPower	편광, SatelliteId	복조기/디코더에서 측정된 신호 강도입니다. 단위: 밀리와트 기준 데시벨 () dBm

지표	측정치 차원	설명
SymbolTimingRecovery_ErrorVectorMagnitude	카테고리, 구성, SatelliteId	수신된 심볼과 이상적인 성상점 사이의 오차 벡터 크기. 단위: 백분율
SymbolTimingRecovery_Locked	카테고리, 구성, SatelliteId	복조기 심볼 타이밍 복구 루프가 잠겨 있으면 1로 설정하고, 잠금이 해제되면 0으로 설정합니다. 단위: 단위 없음
SymbolTimingRecovery_OffsetSymbolRate	카테고리, 구성, SatelliteId	추정된 심볼 레이트와 이상적인 신호 심볼 레이트 사이의 오프셋. 이는 우주선과 안테나 시스템 사이의 도플러 시프트 및 로컬 오실레이터 오프셋으로 인해 발생합니다. 단위: 기호/초

어떤 치수가 AWS Ground Station사용되나요?

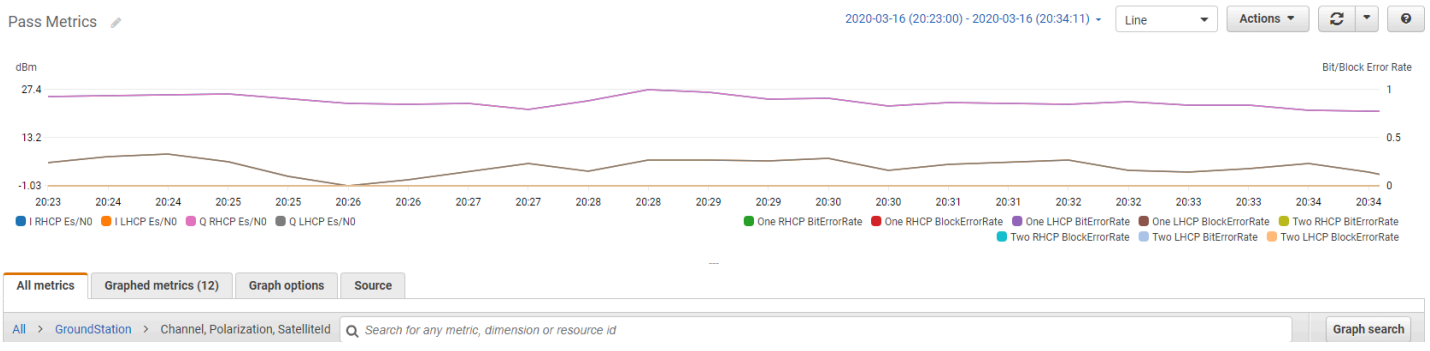
다음 측정기준을 사용하여 AWS Ground Station 데이터를 필터링할 수 있습니다.

측정기준	설명
Category	복조 또는 디코딩.
Channel	각 접촉에 대한 채널에는 1, 2, I(동상) 및 Q(직교)가 포함됩니다.
Config	안테나 다운링크 디모드는 컨피그레이션을 디코딩합니다.
Polarization	각 접점의 편파에는 LHCP (왼손 원형 편파) 또는 RHCP (오른손 원형 편파) 가 포함됩니다.
SatelliteId	위성 ID에는 ARN 연락처의 위성 정보가 들어 있습니다.

지표 보기

그래프로 표시된 지표를 볼 때 집계 창에서 지표가 표시되는 방법이 결정된다는 점에 유의해야 합니다. 접촉의 각 지표는 데이터를 받은 후 3시간 동안 초당 데이터로 표시될 수 있습니다. 3시간이 경과하면 데이터는 CloudWatch Metrics에 의해 분당 데이터로 집계됩니다. 초당 데이터 측정값에 대한 측정치를 확인해야 하는 경우 데이터를 수신한 후 3시간 이내에 데이터를 보거나 측정치 외부에서 데이터를 보관하는 것이 좋습니다. CloudWatch CloudWatch 보존에 대한 자세한 내용은 Amazon CloudWatch 개념 - 지표 보존을 참조하십시오.

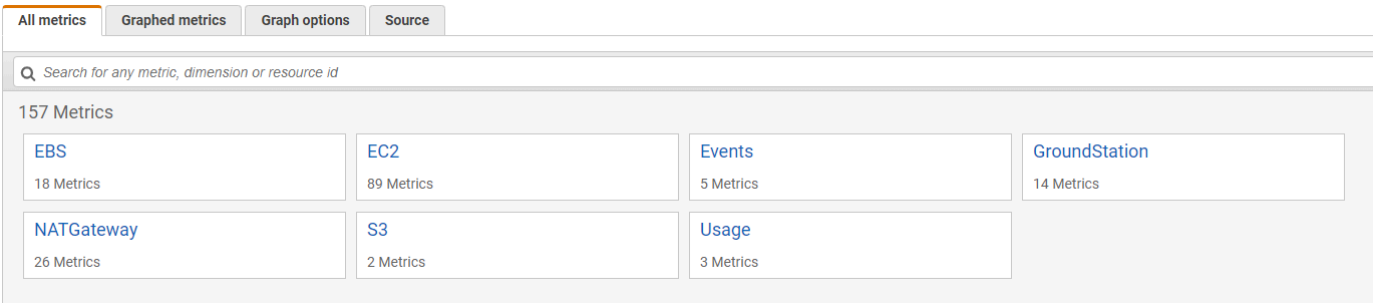
또한 처음 60초 내에 캡처된 데이터에는 의미 있는 지표를 생성하기에 충분한 정보가 포함되지 않으며 표시되지 않을 수 있습니다. 의미 있는 지표를 보려면 60초 후에 데이터를 보는 것이 좋습니다.



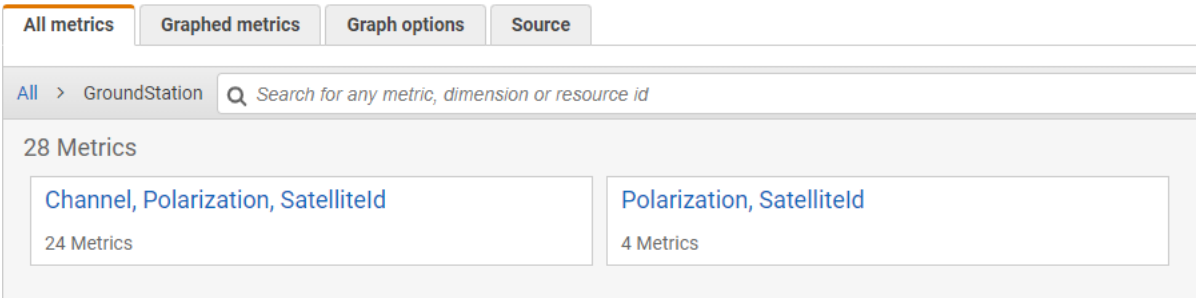
에서 AWS Ground Station CloudWatch 지표를 그래프로 표시하는 방법에 대한 자세한 내용은 그래프 지표를 참조하십시오.

콘솔을 사용한 메트릭 확인

1. 콘솔을 엽니다. CloudWatch
2. 탐색 창에서 지표(Metrics)를 선택합니다.
3. GroundStation 네임스페이스를 선택합니다.



4. 원하는 측정법 치수 (예: 채널, 편광 SatelliteId) 를 선택합니다.



5. 모든 지표 탭에 네임스페이스의 해당 측정기준에 대한 모든 지표가 표시됩니다. 다음을 수행할 수 있습니다.

   a. 테이블을 정렬하려면 열 머리글을 사용합니다.

   b. 지표를 그래프로 표시하려면 지표와 관련된 확인란을 선택합니다. 모든 지표를 선택하려면 표의 제목 행에 있는 확인란을 선택합니다.

   c. 리소스로 필터링하려면 리소스 ID를 선택한 후 검색에 추가를 선택합니다.

   d. 지표로 필터링하려면 지표 이름을 선택한 후 검색에 추가를 선택합니다.

다음을 사용하여 지표를 보려면 AWS CLI

1. 설치되어 AWS CLI 있는지 확인하세요. AWS CLI설치에 대한 자세한 내용은 AWSCLI버전 2 설치를 참조하십시오.

2. 의 get-metric-data메서드를 사용하여 수정할 수 있는 파일을 CloudWatch CLI 생성하여 원하는 메트릭을 지정한 다음 해당 메트릭을 쿼리하는 데 사용할 수 있습니다.

   이렇게 하려면 다음을 `aws cloudwatch get-metric-data --generate-cli-skeleton` 실행하세요. 그러면 다음과 비슷한 출력이 생성됩니다.

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

3. 를 실행하여 사용 가능한 CloudWatch 지표를 `aws cloudwatch list-metrics` 나열합니다.

   최근에 사용한 AWS Ground Station경우 메서드는 다음과 같은 항목이 포함된 출력을 반환해야 합니다.

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

   > **Note**
   >
   > 제한으로 인해 마지막으로 사용한 AWS Ground Station지 2주가 넘으면 사용 가능한 지표 표를 수동으로 검사하여 `AWS/GroundStation` 메트릭 네임스페이스에서 지표 이름과 차원을 찾아야 합니다. CloudWatch CloudWatch 제한에 대한 자세한 내용은 사용 가능한 지표 보기를 참조하십시오.

4. 2단계에서 만든 JSON 파일을 3단계 (예:`SatelliteId`) 및 `Polarization` 지표의 필수 값과 일치하도록 수정하십시오. 또한`StartTime`, 및 `EndTime` 값을 연락처와 일치하도록 업데이트해야 합니다. 예:

```
        {
           "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 지표에 따라 1~60초마다 지표를 게시합니다. `Period`필드 값이 지표의 게시 기간보다 작은 경우 지표가 반환되지 않습니다.

5. 이전 단계에서 만든 구성 파일을 `aws cloudwatch get-metric-data` 사용하여 실행합니다. 아래에 예제가 나와 있습니다.

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

지표는 접촉의 타임스탬프와 함께 제공됩니다. 다음은 AWS Ground Station 지표 출력의 예시입니다.


```
{
   "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": []
}
```

보안 내부 AWS Ground Station

클라우드 AWS 보안이 최우선 과제입니다. AWS 고객은 가장 보안에 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처를 활용할 수 있습니다. AWS보안 목표를 달성하는 데 도움이 되는 보안 관련 도구 및 기능을 제공합니다. 이러한 도구와 기능에는 네트워크 보안, 구성 관리, 액세스 제어 및 데이터 보안이 포함됩니다.

사용할 AWS Ground Station때는 업계 모범 사례를 따르고 암호화를 구현하는 것이 좋습니다. end-to-end AWS암호화와 데이터 보호를 통합할 수 있도록 합니다. APIs 보안에 대한 자세한 내용은 AWS 보안 소개 백서를 참조하십시오. AWS

다음 주제에서 리소스 보안 방법에 대해 알아보십시오.

주제

- Identity 및 Access Management에 대한 AWS Ground Station
- AWS 에 대한 관리형 정책 AWS Ground Station
- Ground Station에 서비스 연결 역할 사용
- 유휴 데이터 암호화 AWS Ground Station
- 전송 중 데이터 암호화 AWS Ground Station

Identity 및 Access Management에 대한 AWS Ground Station

AWS Identity and Access Management (IAM) 는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어할 수 AWS 서비스 있도록 도와줍니다. IAM관리자는 AWS Ground Station 리소스를 사용할 수 있는 인증 (로그인) 및 권한 부여 (권한 보유) 를 받을 수 있는 사용자를 제어합니다. IAM추가 비용 없이 사용할 AWS 서비스 수 있습니다.

주제

- 고객
- ID를 통한 인증
- 정책을 사용한 액세스 관리
- 의 AWS Ground Station 작동 방식 IAM
- 다음과 같은 ID 기반 정책 예제 AWS Ground Station
- AWS Ground Station ID 및 액세스 문제 해결

고객

AWS Identity and Access Management (IAM) 를 사용하는 방법은 수행하는 작업에 따라 다릅니다. AWS Ground Station

서비스 사용자 - AWS Ground Station 서비스를 사용하여 작업을 수행하는 경우 관리자가 필요한 자격 증명과 권한을 제공합니다. 더 많은 AWS Ground Station 기능을 사용하여 작업을 수행함에 따라 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방식을 이해하면 적절한 권한을 관리자에게 요청할 수 있습니다. AWS Ground Station의 기능에 액세스할 수 없는 경우 AWS Ground Station ID 및 액세스 문제 해결을 참조하세요.

서비스 관리자 — 회사에서 AWS Ground Station 리소스를 담당하는 경우 전체 액세스 권한이 있을 수 AWS Ground Station있습니다. 서비스 사용자가 액세스해야 하는 AWS Ground Station 기능과 리소스를 결정하는 것은 여러분의 몫입니다. 그런 다음 IAM 관리자에게 서비스 사용자의 권한을 변경해 달라는 요청을 제출해야 합니다. 이 페이지의 정보를 검토하여 의 기본 개념을 IAM 이해하십시오. 회사에서 사용하는 방법에 대한 자세한 내용은 IAM AWS Ground Station을 참조하십시오의 AWS Ground Station 작동 방식 IAM.

IAM관리자 — IAM 관리자인 경우 액세스 관리를 위한 정책을 작성하는 방법에 대해 자세히 알아보는 것이 좋습니다 AWS Ground Station. 에서 IAM 사용할 수 있는 AWS Ground Station ID 기반 정책의 예를 보려면 을 참조하십시오. 다음과 같은 ID 기반 정책 예제 AWS Ground Station

ID를 통한 인증

인증은 ID 자격 증명을 AWS 사용하여 로그인하는 방법입니다. IAM사용자로서 또는 역할을 위임하여 인증 (로그인 AWS) 을 받아야 합니다. AWS 계정 루트 사용자 IAM

ID 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 ID로 로그인할 수 있습니다. AWS AWS IAM Identity Center (IAMID 센터) 사용자, 회사의 싱글 사인온 인증, Google 또는 Facebook 자격 증명이 페더레이션 ID의 예입니다. 페더레이션 ID로 로그인하는 경우 관리자는 이전에 역할을 사용하여 ID 페더레이션을 설정했습니다. IAM 페더레이션을 AWS 사용하여 액세스하는 경우 간접적으로 역할을 수임하는 것입니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 로그인에 대한 자세한 내용은 AWS 로그인 사용 설명서의 내 로그인 방법을 참조하십시오. AWS AWS 계정

AWS 프로그래밍 방식으로 액세스하는 경우 자격 증명을 사용하여 요청에 암호로 서명할 수 있는 소프트웨어 개발 키트 (SDKCLI) 와 명령줄 인터페이스 () 가 AWS 제공됩니다. AWS 도구를 사용하지 않는 경우 요청에 직접 서명해야 합니다. 권장 방법을 사용하여 직접 요청에 서명하는 방법에 대한 자세한 내용은 사용 IAM설명서의 AWS API요청 서명을 참조하십시오.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어, 계정 보안을 강화하기 위해 다단계 인증 (MFA) 을 사용할 AWS 것을 권장합니다. 자세한 내용은 사용 설명서의 다단계 인증 및 사용 AWS IAM Identity Center 설명서의 다단계 인증 사용 (MFA) 을 IAM 참조하십시오. AWS

AWS 계정 루트 사용자

계정을 AWS 계정만들 때는 먼저 계정의 모든 AWS 서비스 리소스에 대한 완전한 액세스 권한을 가진 하나의 로그인 ID로 시작합니다. 이 ID를 AWS 계정 루트 사용자라고 하며, 계정을 만들 때 사용한 이메일 주소와 비밀번호로 로그인하여 액세스할 수 있습니다. 일상적인 작업에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 보안 인증 정보를 보호하고 루트 사용자만 수행할 수 있는 작업을 수행하는 데 사용합니다. 루트 사용자로 로그인해야 하는 작업의 전체 목록은 사용 설명서의 루트 사용자 자격 증명이 필요한 작업을 참조하십시오. IAM

페더레이션 자격 증명

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 비롯한 수동 AWS 서비스 사용자가 ID 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 액세스하도록 하는 것입니다.

페더레이션 ID는 기업 사용자 디렉토리, 웹 ID 공급자, Identity Center 디렉터리의 사용자 또는 ID 소스를 통해 제공된 자격 증명을 사용하여 액세스하는 AWS 서비스 모든 사용자를 말합니다. AWS Directory Service페더레이션 ID에 AWS 계정액세스하면 이들이 역할을 맡고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center(을)를 사용하는 것이 좋습니다. IAMIdentity Center에서 사용자 및 그룹을 만들거나 자체 ID 소스의 사용자 및 그룹 집합에 연결하고 동기화하여 AWS 계정 모든 사용자 및 애플리케이션에서 사용할 수 있습니다. ID 센터에 대한 자세한 내용은 IAM ID 센터란 IAM 무엇입니까? 를 참조하십시오. AWS IAM Identity Center 사용 설명서에서.

IAM 사용자 및 그룹

IAM사용자란 단일 사용자 또는 애플리케이션에 대한 특정 권한을 가진 사용자 내의 ID입니다. AWS 계정 가능하면 암호 및 액세스 키와 같은 장기 자격 증명을 가진 IAM 사용자를 만드는 대신 임시 자격 증명을 사용하는 것이 좋습니다. 하지만 특정 사용 사례에서 IAM 사용자의 장기 자격 증명이 필요한 경우에는 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 사용 설명서의 장기 자격 증명이 필요한 사용 사례에 대한 정기적인 액세스 키 IAM 교체를 참조하십시오.

IAM그룹은 IAM 사용자 컬렉션을 지정하는 ID입니다. 사용자는 그룹으로 로그인할 수 없습니다. 그룹을 사용하여 여러 사용자의 권한을 한 번에 지정할 수 있습니다. 그룹을 사용하면 대규모 사용자 집합

의 권한을 더 쉽게 관리할 수 있습니다. 예를 들어 이름을 지정한 IAMAdmins그룹을 만들고 해당 그룹에 IAM 리소스를 관리할 권한을 부여할 수 있습니다.

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수임할 수 있습니다. 사용자는 영구적인 장기 보안 인증 정보를 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세히 알아보려면 사용 설명서의 역할 대신 IAM 사용자를 만드는 시기를 참조하십시오. IAM

IAM역할

IAM역할은 특정 권한을 AWS 계정 가진 사용자 내의 ID입니다. IAM사용자와 비슷하지만 특정인과 관련이 있는 것은 아닙니다. 역할을 AWS Management Console 전환하여 에서 일시적으로 IAM 역할을 맡을 수 있습니다. AWS CLI or AWS API 작업을 호출하거나 사용자 지정을 사용하여 역할을 수임할 수 URL 있습니다. 역할 사용 방법에 대한 자세한 내용은 사용 IAM설명서의 IAM역할 사용을 참조하십시오.

IAM임시 자격 증명이 있는 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 ID에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 페더레이션 ID가 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션을 위한 역할에 대한 자세한 내용은 IAM사용 설명서의 타사 ID 제공자를 위한 역할 생성을 참조하십시오. IAMIdentity Center를 사용하는 경우 권한 집합을 구성합니다. ID가 인증된 후 액세스할 수 있는 대상을 제어하기 위해 IAM Identity Center는 권한 집합을 역할의 상관 관계와 연결합니다. IAM 권한 세트에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 세트를 참조하세요.
- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할이 역할을 맡아 특정 작업에 대해 일시적으로 다른 권한을 부여받을 수 있습니다. IAM
- 계정 간 액세스 - IAM 역할을 사용하여 다른 계정의 사용자 (신뢰할 수 있는 사용자) 가 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다. 하지만 일부 AWS 서비스경우에는 역할을 프록시로 사용하는 대신 정책을 리소스에 직접 연결할 수 있습니다. 계정 간 액세스에 대한 역할과 리소스 기반 정책의 차이점을 알아보려면 사용 설명서의 교차 계정 리소스 액세스를 참조하십시오. IAM IAM
- 서비스 간 액세스 — 일부는 다른 기능을 AWS 서비스 사용합니다. AWS 서비스예를 들어, 서비스를 호출하면 해당 서비스가 Amazon에서 애플리케이션을 EC2 실행하거나 Amazon S3에 객체를 저장하는 것이 일반적입니다. 서비스는직접적으로 호출하는 보안 주체의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
  - 전달 액세스 세션 (FAS) — IAM 사용자 또는 역할을 사용하여 작업을 수행하는 AWS경우 보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수

행할 수 있습니다. FAS전화를 거는 주체의 권한을 다운스트림 서비스에 AWS 서비스 요청하라는 요청과 결합하여 사용합니다. AWS 서비스 FAS요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS요청 시 적용되는 정책 세부 정보는 전달 액세스 세션을 참조하십시오.

- 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 간주하는 IAM 역할입니다. IAM관리자는 내부에서 IAM 서비스 역할을 만들고, 수정하고, 삭제할 수 있습니다. 자세한 내용은 사용 설명서의 역할 만들기를 참조하여 권한을 위임하십시오IAM. AWS 서비스
- 서비스 연결 역할 - 서비스 연결 역할은 에 연결된 서비스 역할 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM관리자는 서비스 연결 역할에 대한 권한을 볼 수 있지만 편집할 수는 없습니다.

- Amazon에서 실행 중인 애플리케이션 EC2 — IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 AWS API 요청을 보내는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. AWS CLI EC2인스턴스 내에 액세스 키를 저장하는 것보다 이 방법이 더 좋습니다. EC2인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있게 하려면 인스턴스에 연결된 인스턴스 프로필을 만들어야 합니다. 인스턴스 프로필에는 역할이 포함되며, 이를 통해 EC2 인스턴스에서 실행 중인 프로그램이 임시 자격 증명을 얻을 수 있습니다. 자세한 내용은 사용 설명서의 IAM역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 IAM 참조하십시오.

IAM역할을 사용할지 IAM 사용자를 사용할지 알아보려면 사용 설명서의 IAM 역할 생성 시기 (사용자 대신) 를 IAM참조하십시오.

정책을 사용한 액세스 관리

정책을 만들고 이를 AWS ID 또는 리소스에 AWS 연결하여 액세스를 제어할 수 있습니다. 정책은 ID 또는 리소스와 연결될 때 AWS 해당 권한을 정의하는 객체입니다. AWS 주도자 (사용자, 루트 사용자 또는 역할 세션) 가 요청할 때 이러한 정책을 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는지를 결정합니다. 대부분의 정책은 JSON 문서로 AWS 저장됩니다. JSON정책 문서의 구조 및 내용에 대한 자세한 내용은 IAM사용 설명서의 JSON 정책 개요를 참조하십시오.

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

기본적으로, 사용자와 역할에는 어떠한 권한도 없습니다. IAM관리자는 IAM 정책을 생성하여 필요한 리소스에서 작업을 수행할 수 있는 권한을 사용자에게 부여할 수 있습니다. 그러면 관리자가 역할에 IAM 정책을 추가할 수 있으며, 사용자는 역할을 수임할 수 있습니다.

IAM정책은 작업을 수행하는 데 사용하는 방법에 관계없이 작업에 대한 권한을 정의합니다. 예를 들어, `iam:GetRole` 작업을 허용하는 정책이 있다고 가정합니다. 해당 정책을 사용하는 사용자는 AWS Management Console, AWS CLI, 또는 에서 역할 정보를 가져올 수 AWS API 있습니다.

보안 인증 기반 정책

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. ID 기반 정책을 만드는 방법을 알아보려면 사용 설명서의 IAM정책 생성을 참조하십시오. IAM

보안 인증 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은 내 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립형 정책입니다. AWS 계정관리형 정책에는 AWS 관리형 정책과 고객 관리형 정책이 포함됩니다. 관리형 정책과 인라인 정책 중에서 선택하는 방법을 알아보려면 IAM사용 설명서의 관리형 정책과 인라인 정책 중 선택을 참조하십시오.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 문서입니다. 리소스 기반 정책의 예로는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책이 있습니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. 리소스 기반 IAM 정책에서는 AWS 관리형 정책을 사용할 수 없습니다.

액세스 제어 목록 () ACLs

액세스 제어 목록 (ACLs) 은 리소스에 액세스할 수 있는 권한을 가진 주체 (계정 구성원, 사용자 또는 역할) 를 제어합니다. ACLs정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 JSON 비슷합니다.

지원하는 서비스의 VPC 예로는 Amazon S3와 Amazon이 ACLs 있습니다. AWS WAF자세한 내용은 Amazon 심플 스토리지 서비스 개발자 안내서의 액세스 제어 목록 (ACL) 개요를 참조하십시오. ACLs

기타 정책 타입

AWS 일반적이지 않은 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 유형에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 - 권한 경계는 ID 기반 정책이 IAM 엔티티 (IAM사용자 또는 역할) 에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 객체의 자격 증명 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 내용은 사용 IAM설명서의 IAM 엔티티의 권한 경계를 참조하십시오.
- 서비스 제어 정책 (SCPs) - SCPs 조직 또는 OU (조직 구성 단위) 에 대한 최대 권한을 지정하는 JSON AWS Organizations정책입니다. AWS Organizations 기업이 소유한 여러 AWS 계정 개를 그룹화하고 중앙에서 관리하는 서비스입니다. 조직의 모든 기능을 사용하도록 설정하면 일부 또는 모든 계정에 서비스 제어 정책 (SCPs) 을 적용할 수 있습니다. 각 항목을 포함하여 구성원 계정의 엔티티에 대한 권한을 SCP AWS 계정 루트 사용자제한합니다. Organizations 및 SCPs 에 대한 자세한 내용은 AWS Organizations 사용 설명서의 서비스 제어 정책을 참조하십시오.
- 세션 정책 – 세션 정책은 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할의 보안 인증 기반 정책의 교차와 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 내용은 IAM사용 설명서의 세션 정책을 참조하십시오.

여러 정책 유형

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. 여러 정책 유형이 관련된 경우 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM사용 설명서의 정책 평가 로직을 참조하십시오.

의 AWS Ground Station 작동 방식 IAM

액세스를 관리하는 IAM 데 사용하기 전에 사용할 수 있는 IAM 기능에 대해 알아보십시오 AWS Ground Station. AWS Ground Station

IAM함께 사용할 수 있는 기능 AWS Ground Station

IAM기능	AWS Ground Station 지원
ID 기반 정책	예
리소스 기반 정책	아니요

IAM기능	AWS Ground Station 지원
정책 작업	예
정책 리소스	예
정책 조건 키(서비스별)	예
ACLs	아니요
ABAC(정책의 태그)	예
임시 보안 인증	예
보안 주체 권한	예
서비스 역할	아니요
서비스 링크 역할	예

대부분의 IAM 기능과 함께 작동하는 방식 AWS Ground Station 및 기타 AWS 서비스를 개괄적으로 보려면 IAM사용 IAM 설명서에서 함께 작동하는AWS 서비스를 참조하십시오.

ID 기반 정책은 다음과 같습니다. AWS Ground Station

ID 기반 정책 지원: 예

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. ID 기반 정책을 만드는 방법을 알아보려면 사용 설명서의 IAM정책 생성을 참조하십시오. IAM

IAMID 기반 정책을 사용하면 허용 또는 거부된 작업 및 리소스는 물론 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. 보안 인증 기반 정책에서는 보안 주체가 연결된 사용자 또는 역할에 적용되므로 보안 주체를 지정할 수 없습니다. JSON정책에서 사용할 수 있는 모든 요소에 대해 알아보려면 사용 IAM설명서의 IAM JSON 정책 요소 참조를 참조하십시오.

아이덴티티 기반 정책 예시 AWS Ground Station

AWS Ground Station ID 기반 정책의 예를 보려면 을 참조하십시오. 다음과 같은 ID 기반 정책 예제 AWS Ground Station

내 리소스 기반 정책 AWS Ground Station

리소스 기반 정책 지원: 아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 문서입니다. 리소스 기반 정책의 예로는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책이 있습니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

계정 간 액세스를 활성화하려면 다른 계정의 전체 계정 또는 IAM 엔티티를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하십시오. 보안 주체와 리소스가 다른 AWS 계정경우 신뢰할 수 있는 계정의 IAM 관리자는 보안 주체 (사용자 또는 역할) 에게 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 엔터티에 ID 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 보안 주체에 액세스를 부여하는 경우, 추가 자격 증명 기반 정책이 필요하지 않습니다. 자세한 내용은 IAM사용 설명서의 계정 간 리소스 액세스를 참조하십시오. IAM

에 대한 정책 조치 AWS Ground Station

정책 작업 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

정책 `Action` 요소는 JSON 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 정책 작업은 일반적으로 관련 AWS API 작업과 이름이 같습니다. 일치하는 작업이 없는 권한 전용 작업과 같은 몇 가지 예외가 있습니다. API 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 일컬어 종속 작업이라고 합니다.

연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하십시오.

AWS Ground Station 작업 목록을 보려면 서비스 권한 부여 AWS Ground Station참조에 정의된 작업을 참조하십시오.

정책 조치는 조치 앞에 다음 접두사를 AWS Ground Station 사용합니다.

```
groundstation
```

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

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

AWS Ground Station ID 기반 정책의 예를 보려면 을 참조하십시오. 다음과 같은 ID 기반 정책 예제 AWS Ground Station

에 대한 정책 리소스 AWS Ground Station

정책 리소스 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Resource`JSON정책 요소는 작업이 적용되는 하나 또는 여러 개의 객체를 지정합니다. 문장에는 `Resource`또는 `NotResource`요소가 반드시 추가되어야 합니다. Amazon 리소스 이름 (ARN) 을 사용하여 리소스를 지정하는 것이 가장 좋습니다. 리소스 수준 권한이라고 하는 특정 리소스 유형을 지원하는 작업에 대해 이 태스크를 수행할 수 있습니다.

작업 나열과 같이 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

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

AWS Ground Station 리소스 유형 및 해당 ARNs 유형의 목록을 보려면 서비스 권한 부여 AWS Ground Station참조에 정의된 리소스를 참조하십시오. 각 리소스에 어떤 작업을 지정할 수 있는지 알아보려면 정의된 작업을 참조하십시오 AWS Ground Station. ARN

AWS Ground Station ID 기반 정책의 예를 보려면 을 참조하십시오. 다음과 같은 ID 기반 정책 예제 AWS Ground Station

에 대한 정책 조건 키 AWS Ground Station

서비스별 정책 조건 키 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Condition` 요소(또는 `Condition` 블록)를 사용하면 정책이 발효되는 조건을 지정할 수 있습니다. `Condition` 요소는 옵션입니다. 같거나 작음과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

한 문에서 여러 `Condition` 요소를 지정하거나 단일 `Condition` 요소에서 여러 키를 지정하는 경우, AWS 는 논리적 `AND` 태스크를 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우 는 논리적 `OR` 연산을 사용하여 조건을 AWS 평가합니다. 명문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예를 들어 리소스에 IAM 사용자 이름이 태그가 지정된 경우에만 리소스에 대한 액세스 권한을 IAM 사용자에게 부여할 수 있습니다. 자세한 내용은 IAM사용 설명서의 IAM 정책 요소: 변수 및 태그를 참조하십시오.

AWS 글로벌 조건 키 및 서비스별 조건 키를 지원합니다. 모든 AWS 글로벌 조건 키를 보려면 IAM사용 설명서의AWS 글로벌 조건 컨텍스트 키를 참조하십시오.

AWS Ground Station 조건 키 목록을 보려면 서비스 권한 부여 AWS Ground Station참조의 조건 키를 참조하십시오. 조건 키를 사용할 수 있는 작업 및 리소스에 대해 알아보려면 작업 정의 기준을 참조하십시오 AWS Ground Station.

AWS Ground Station ID 기반 정책의 예를 보려면 을 참조하십시오. 다음과 같은 ID 기반 정책 예제 AWS Ground Station

ACLs에서 AWS Ground Station

지원ACLs: 아니요

액세스 제어 목록 (ACLs) 은 리소스에 액세스할 수 있는 권한을 가진 주체 (계정 구성원, 사용자 또는 역할) 를 제어합니다. ACLs정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 JSON 비슷합니다.

ABAC... 와 AWS Ground Station

지원 ABAC (정책의 태그): 예

속성 기반 액세스 제어 (ABAC) 는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. AWS에서는 이러한 속성을 태그라고 합니다. IAM엔티티 (사용자 또는 역할) 및 여러 AWS 리소스에 태그를 첨부할 수 있습니다. 의 ABAC 첫 번째 단계는 엔티티와 리소스에 태그를 지정하는 것입니다. 그런 다음 보안 주체의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.

ABAC빠르게 성장하는 환경에서 유용하며 정책 관리가 복잡해지는 상황에 도움이 됩니다.

태그에 근거하여 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` 또는 `aws:TagKeys` 조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다.

서비스가 모든 리소스 유형에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 유형에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

에 대한 자세한 내용은 What is ABAC? 를 참조하십시오. ABAC IAM사용 설명서에서. 설정 ABAC 단계가 포함된 자습서를 보려면 사용 IAM설명서의 속성 기반 액세스 제어 사용 (ABAC) 을 참조하십시오.

임시 자격 증명 사용: AWS Ground Station

임시 자격 증명 지원: 예

임시 자격 증명을 사용하여 로그인하면 작동하지 AWS 서비스 않는 것도 있습니다. 임시 자격 증명을 사용하는 AWS 서비스 방법을 비롯한 추가 정보는 IAM사용 설명서의 AWS 서비스 해당 자격 증명을 참조하십시오. IAM

사용자 이름과 암호를 제외한 다른 방법을 AWS Management Console 사용하여 로그인하는 경우 임시 자격 증명을 사용하는 것입니다. 예를 들어 회사의 Single Sign-On (SSO) 링크를 AWS 사용하여 액세스하는 경우 이 프로세스에서 자동으로 임시 자격 증명을 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 보안 인증을 자동으로 생성합니다. 역할 전환에 대한 자세한 내용은 IAM사용 설명서의 역할 전환 (콘솔) 을 참조하십시오.

AWS CLI 또는 를 사용하여 임시 자격 증명을 수동으로 생성할 수 AWS API 있습니다. 그런 다음 해당 임시 자격 증명을 사용하여 액세스할 수 AWS있습니다. AWS 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성할 것을 권장합니다. 자세한 내용은 의 임시 보안 자격 증명을 참조하십시오. IAM

서비스 간 사용자 권한: AWS Ground Station

순방향 액세스 세션 지원 (FAS): 예

에서 IAM 사용자 또는 역할을 사용하여 작업을 수행하는 AWS경우 사용자는 보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS를 호출하는 주체의 권한을 다운스트림 서비스에 AWS 서비스 요청하기 위한 요청과 결합하여 사용합니다. AWS 서비스 FAS요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS요청 시 적용되는 정책 세부 정보는 전달 액세스 세션을 참조하십시오.

AWS Ground Station의 서비스 역할

서비스 역할 지원: 아니요

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 간주하는 IAM역할입니다. IAM관리자는 내부에서 IAM 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 사용 설명서의 역할 만들기를 참조하여 권한을 위임하십시오IAM. AWS 서비스

> **Warning**
>
> 서비스 역할의 권한을 변경하면 AWS Ground Station 기능이 중단될 수 있습니다. 서비스 역할을 편집하기 위한 지침이 AWS Ground Station 제공되는 경우에만 서비스 역할을 편집하십시오.

서비스 연결 역할은 다음과 같습니다. AWS Ground Station

서비스 링크 역할 지원: 예

서비스 연결 역할은 에 연결된 서비스 역할 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM관리자는 서비스 연결 역할에 대한 권한을 볼 수 있지만 편집할 수는 없습니다.

서비스 연결 역할을 만들거나 관리하는 방법에 대한 자세한 내용은 함께 작동하는 AWS 서비스를 참조하십시오. IAM 서비스 연결 역할 열에서 Yes(이)가 포함된 서비스를 테이블에서 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 Yes(네) 링크를 선택합니다.

다음과 같은 ID 기반 정책 예제 AWS Ground Station

기본적으로 사용자 및 역할에는 AWS Ground Station 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console, AWS Command Line Interface (AWS CLI) 또는 를 사용하여 작업을 수행할 수 없습니다. AWS API IAM관리자는 IAM 정책을 생성하여 필요한 리소스에서 작업

을 수행할 수 있는 권한을 사용자에게 부여할 수 있습니다. 그러면 관리자가 역할에 IAM 정책을 추가할 수 있으며, 사용자는 역할을 수임할 수 있습니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 만드는 방법을 알아보려면 사용 IAM설명서에서 IAM 정책 생성을 참조하십시오.

각 리소스 유형의 형식을 포함하여 AWS Ground Station에서 정의한 AWS Ground Station작업 및 리소스 유형에 ARNs 대한 자세한 내용은 서비스 권한 부여 참조의 작업, 리소스 및 조건 키를 참조하십시오.

주제

- 정책 모범 사례
- AWS Ground Station 콘솔 사용
- 사용자가 자신의 고유한 권한을 볼 수 있도록 허용

정책 모범 사례

ID 기반 정책은 누군가가 사용자 계정에서 AWS Ground Station 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부를 결정합니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따릅니다.

- AWS 관리형 정책으로 시작하여 최소 권한 권한으로 이동 — 사용자와 워크로드에 권한을 부여하려면 여러 일반적인 사용 사례에 권한을 부여하는 AWS 관리형 정책을 사용하세요. 에서 사용할 수 있습니다. AWS 계정사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 더 줄이는 것이 좋습니다. 자세한 내용은 IAM사용 설명서의 AWS 관리형 정책 또는 작업 기능에 대한AWS 관리형 정책을 참조하십시오.
- 최소 권한 적용 — IAM 정책으로 권한을 설정하는 경우 작업 수행에 필요한 권한만 부여하십시오. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. 를 사용하여 권한을 IAM 적용하는 방법에 대한 자세한 내용은 사용 설명서의 정책 및 권한을 참조하십시오. IAM IAM
- IAM정책의 조건을 사용하여 액세스를 추가로 제한 - 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어, 를 사용하여 모든 요청을 전송하도록 지정하는 정책 조건을 작성할 수 SSL 있습니다. 예를 AWS 서비스들어 특정 작업을 통해 서비스 작업을 사용하는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 AWS CloudFormation있습니다. 자세한 내용은 IAM사용 설명서의 IAMJSON정책 요소: 조건을 참조하십시오.
- IAMAccess Analyzer를 사용하여 IAM 정책을 검증하여 안전하고 기능적인 권한을 보장합니다. IAM Access Analyzer는 새 정책과 기존 정책을 검증하여 정책이 IAM 정책 언어 (JSON) 및 IAM 모범 사

례를 준수하는지 확인합니다. IAMAccess Analyzer는 안전하고 기능적인 정책을 작성하는 데 도움이 되는 100개 이상의 정책 검사와 실행 가능한 권장 사항을 제공합니다. 자세한 내용은 사용 설명서의 IAMAccess Analyzer 정책 검증을 참조하십시오. IAM

- 다단계 인증 필요 (MFA) - 사용자 또는 루트 IAM 사용자가 필요한 시나리오가 있는 경우 보안을 강화하려면 이 기능을 MFA 켜십시오. AWS 계정 API작업 호출 MFA 시기를 요구하려면 정책에 MFA 조건을 추가하세요. 자세한 내용은 IAM사용 설명서의 MFA -보호된 API 액세스 구성을 참조하십시오.

의 모범 사례에 IAM 대한 자세한 내용은 IAM사용 설명서의 보안 모범 사례를 참조하십시오. IAM

AWS Ground Station 콘솔 사용

AWS Ground Station 콘솔에 액세스하려면 최소 권한 집합이 있어야 합니다. 이러한 권한을 통해 내 AWS Ground Station 리소스의 세부 정보를 나열하고 볼 수 있어야 AWS 계정합니다. 최소 필수 권한보다 더 제한적인 자격 증명 기반 정책을 만들면 콘솔이 해당 정책에 연결된 엔터티(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

AWS CLI 또는 에만 전화를 거는 사용자에게 최소 콘솔 권한을 허용할 필요는 AWS API 없습니다. 대신 수행하려는 작업과 일치하는 API 작업에만 액세스를 허용하세요.

사용자와 역할이 AWS Ground Station 콘솔을 계속 사용할 수 있도록 하려면 AWS Ground Station *ConsoleAccess* 또는 *ReadOnly* AWS 관리형 정책도 엔티티에 연결하세요. 자세한 내용은 사용 설명서의 IAM사용자에게 권한 추가를 참조하십시오.

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예제에서는 IAM 사용자가 자신의 사용자 ID에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 만드는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 OR를 사용하여 프로그래밍 방식으로 이 작업을 완료할 수 있는 AWS CLI 권한이 포함됩니다. AWS API

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
```

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

AWS Ground Station ID 및 액세스 문제 해결

다음 정보를 사용하면 및 를 사용할 때 발생할 수 있는 일반적인 문제를 AWS Ground Station 진단하고 해결하는 데 도움이 IAM 됩니다.

주제

- 다음과 같은 작업을 수행할 권한이 없습니다. AWS Ground Station
- 저는 IAM을 수행할 권한이 없습니다. PassRole
- 외부 사용자가 내 AWS Ground Station 리소스에 액세스할 수 있도록 AWS 계정 허용하고 싶습니다.

다음과 같은 작업을 수행할 권한이 없습니다. AWS Ground Station

작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 작업을 수행할 수 있도록 정책을 업데이트해야 합니다.

다음 예제 오류는 mateojackson IAM 사용자가 콘솔을 사용하여 가상 *my-example-widget* 리소스에 대한 세부 정보를 보려고 하지만 가상 권한이 없는 경우 발생합니다. groundstation:*GetWidget*

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

이 경우 groundstation:*GetWidget*작업을 사용하여 *my-example-widget*리소스에 액세스할 수 있도록 mateojackson사용자 정책을 업데이트해야 합니다.

도움이 필요하면 관리자에게 문의하세요. AWS 관리자는 로그인 자격 증명을 제공한 사람입니다.

저는 IAM을 수행할 권한이 없습니다. PassRole

iam:PassRole 작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 AWS Ground Station에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

일부 AWS 서비스 서비스에서는 새 서비스 역할 또는 서비스 연결 역할을 생성하는 대신 기존 역할을 해당 서비스에 전달할 수 있습니다. 이렇게 하려면 사용자가 서비스에 역할을 전달할 수 있는 권한을 가지고 있어야 합니다.

다음 예제 오류는 라는 IAM 사용자가 콘솔을 사용하여 에서 작업을 marymajor 수행하려고 할 때 발생합니다. AWS Ground Station하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 수 있는 권한을 가지고 있지 않습니다.

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

이 경우, Mary가 iam:PassRole 작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

외부 사용자가 내 AWS Ground Station 리소스에 액세스할 수 있도록 AWS 계정 허용하고 싶습니다.

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제어 목록 (ACLs) 을 지원하는 서비스의 경우 이러한 정책을 사용하여 사용자에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세히 알아보려면 다음을 참조하세요.

- 이러한 기능의 AWS Ground Station 지원 여부를 알아보려면 을 참조하십시오. 의 AWS Ground Station 작동 방식 IAM
- 소유한 리소스에 대한 액세스 권한을 AWS 계정 부여하는 방법을 알아보려면 사용 설명서에서 AWS 계정 자신이 소유한 다른 IAM 사용자의 액세스 권한 제공을 IAM 참조하십시오.
- 제3자에게 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM사용 설명서의 제3자가 AWS 계정 소유한 리소스에 대한 액세스 제공을 참조하십시오. AWS 계정
- ID 페더레이션을 통해 액세스를 제공하는 방법을 알아보려면 사용 설명서의 외부 인증된 사용자에게 액세스 제공 (ID 페더레이션) 을 IAM 참조하십시오.
- 계정 간 액세스에 대한 역할 사용과 리소스 기반 정책의 차이점을 알아보려면 사용 설명서의 계정 간 리소스 액세스를 참조하십시오. IAM IAM

AWS 에 대한 관리형 정책 AWS Ground Station

AWS 관리형 정책은 에서 생성하고 관리하는 독립형 정책입니다. AWS AWS 관리형 정책은 많은 일반 사용 사례에 대한 권한을 제공하도록 설계되었으므로 사용자, 그룹 및 역할에 권한을 할당하기 시작할 수 있습니다.

AWS 관리형 정책은 모든 AWS 고객이 사용할 수 있으므로 특정 사용 사례에 대해 최소 권한 권한을 부여하지 않을 수도 있다는 점에 유의하세요. 사용 사례에 고유한 고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다.

관리형 정책에 정의된 권한은 변경할 수 없습니다. AWS AWS 관리형 정책에 정의된 권한을 업데이트하는 경우 AWS 해당 업데이트는 정책이 연결된 모든 주체 ID (사용자, 그룹, 역할) 에 영향을 미칩니다. AWS 새 정책이 시작되거나 기존 서비스에 새 AWS 서비스 API 작업을 사용할 수 있게 되면 AWS 관리형 정책을 업데이트할 가능성이 가장 높습니다.

자세한 내용은 IAM사용 설명서의 AWS 관리형 정책을 참조하십시오.

AWS 관리형 정책: AWSGroundStationAgentInstancePolicy

AWSGroundStationAgentInstancePolicy정책을 IAM ID에 연결할 수 있습니다.

이 정책은 AWS Ground Station 에이전트에게 Amazon EC2 인스턴스에 Ground Station 연결 중에 인스턴스가 데이터를 보내고 받을 수 있는 권한을 부여합니다. 이 정책의 모든 권한은 Ground Station 서비스에서 부여됩니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- groundstation— 데이터 흐름 엔드포인트 인스턴스가 Ground Station Agent를 호출할 수 있도록 합니다. APIs

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

AWS 관리형 정책: AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy

AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy IAM엔티티에 연결할 수 없습니다. 이 정책은 사용자를 AWS Ground Station 대신하여 작업을 수행할 수 있는 서비스 연결 역할에 연결됩니다. 자세한 내용은 서비스 연결 역할 사용을 참조하십시오.

이 정책은 공용 IPv4 주소를 찾을 수 있는 EC2 권한을 AWS Ground Station 부여합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `ec2:DescribeAddresses`— 사용자를 대신하여 IPs 관련된 EIPs 모든 항목을 나열할 수 있습니다. AWS Ground Station
- `ec2:DescribeNetworkInterfaces`— 사용자를 대신하여 EC2 인스턴스와 연결된 네트워크 인터페이스에 대한 정보를 가져올 수 있습니다. AWS Ground Station

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeAddresses",
                "ec2:DescribeNetworkInterfaces"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS Ground StationAWS 관리형 정책 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 AWS Ground Station 이후의 AWS 관리형 정책 업데이트에 대한 세부 정보를 볼 수 있습니다. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 AWS Ground Station 문서 기록 페이지에서 RSS 피드를 구독하십시오.

변경 사항	설명	날짜
AWSGroundStationAgentInstancePolicy - 새 정책	AWS Ground Station AWSGround Station Agent를 사용할 수 있는 데이터 흐름 엔드포인트 인스턴스 권한을 제공하는 새 정책이 추가되었습니다.	2023년 8월 12일
AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy - 새 정책	AWS Ground Station 인스턴스와 연결된 공용 IPv4 주소 EIPs 및 인스턴스와 연결된 네트워크 인터페이스를 찾을 수 AWS Ground Station 있는 EC2 권한을 부여하는 새 정책이 추가되었습니다. EC2	2022년 11월 2일
AWS Ground Station 변경 내용 추적 시작	AWS Ground Station AWS 관리형 정책의 변경 사항 추적을 시작했습니다.	2021년 3월 1일

Ground Station에 서비스 연결 역할 사용

AWS Ground Station AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 Ground Station에 직접 연결되는 고유한 IAM 역할 유형입니다. 서비스 연결 역할은 Ground Station에서 사전 정의하며 서비스가 사용자를 대신하여 다른 AWS 서비스를 호출하는 데 필요한 모든 권한을 포함합니다.

필요한 권한을 수동으로 추가할 필요가 없으므로 서비스 연결 역할은 Ground Station를 더 쉽게 설정할 수 있습니다. Ground Station에서 서비스 연결 역할의 권한을 정의하므로 다르게 정의되지 않은 한, Ground Station만 해당 역할을 수임할 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며 해당 권한 정책은 다른 엔티티에 연결할 수 없습니다. IAM

서비스 연결 역할을 지원하는 다른 서비스에 대한 자세한 내용은 함께 작동하는AWS 서비스를 IAM 참조하고 서비스 연결 역할 열에서 '예'로 표시된 서비스를 찾아보세요. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다.

Ground Station에 대한 서비스 연결 역할 권한

Ground Station은 AWSServiceRoleForGroundStationDataflowEndpointGroup—라는 서비스 연결 역할을 AWS GroundStation 사용하여 이 서비스 연결 역할을 호출하여 공용 주소를 찾습니다EC2. IPv4

AWSServiceRoleForGroundStationDataflowEndpointGroup 서비스 연결 역할은 다음 서비스를 신뢰하여 역할을 수임합니다.

- `groundstation.amazonaws.com`

이름이 지정된 역할 권한 정책을 AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy 통해 Ground Station은 지정된 리소스에서 다음 작업을 완료할 수 있습니다.

- 작업: `all AWS resources (*)`에 대한 `ec2:DescribeAddresses`

  작업을 통해 Ground Station은 IPs 관련된 모든 항목을 나열할 수 EIPs 있습니다.
- 작업: `all AWS resources (*)`에 대한 `ec2:DescribeNetworkInterfaces`

  작업을 통해 Ground Station은 EC2 인스턴스와 연결된 네트워크 인터페이스에 대한 정보를 가져올 수 있습니다.

IAM엔티티 (예: 사용자, 그룹 또는 역할) 가 서비스 연결 역할을 생성, 편집 또는 삭제할 수 있도록 권한을 구성해야 합니다. 자세한 내용은 사용 설명서의 서비스 연결 역할 권한을 참조하십시오. IAM

Ground Station에 대한 서비스 연결 역할 생성

서비스 링크 역할은 수동으로 생성할 필요가 없습니다. AWS CLI 또는 DataflowEndpointGroup 에서를 생성하면 Ground AWS API Station에서 서비스 연결 역할을 자동으로 생성합니다.

이 서비스 연결 역할을 삭제했다가 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. 를 생성하면 DataflowEndpointGroup Ground Station에서 서비스 연결 역할을 다시 생성합니다.

또한 IAM 콘솔을 사용하여 EC2Amazon으로의 데이터 전송 사용 사례와 함께 서비스 연결 역할을 생성할 수 있습니다. AWS CLI 또는 에서 서비스 AWS API 이름을 사용하여 서비스 연결 역할을 생성합니다. `groundstation.amazonaws.com` 자세한 내용은 사용 설명서의 서비스 연결 역할 만들기를 참조하십시오. IAM 이 서비스 연결 역할을 삭제하면 동일한 프로세스를 사용하여 역할을 다시 생성할 수 있습니다.

Ground Station에 대한 서비스 연결 역할 편집

Ground Station에서는 AWSServiceRoleForGroundStationDataflowEndpointGroup 서비스 연결 역할을 편집할 수 없습니다. 서비스 링크 역할을 생성한 후에는 다양한 개체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 를 사용하여 역할에 대한 설명을 편집할 수 있습니다. IAM 자세한 내용은 사용 IAM설명서의 서비스 연결 역할 편집을 참조하십시오.

Ground Station에 대한 서비스 연결 역할 삭제

서비스 연결 역할이 필요한 기능 또는 서비스가 더 이상 필요 없는 경우에는 해당 역할을 삭제하는 것이 좋습니다. 따라서 적극적으로 모니터링하거나 유지하지 않는 미사용 엔터티가 없도록 합니다.

서비스 연결 역할을 DataflowEndpointGroups 사용하여 서비스 연결 역할을 먼저 삭제한 후에만 서비스 연결 역할을 삭제할 수 있습니다. 이렇게 하면 자신의 권한이 실수로 취소되는 것을 방지할 수 있습니다. DataflowEndpointGroups 서비스 연결 역할을 여러 DataflowEndpointGroups 역할과 함께 사용하는 경우 서비스 연결 역할을 사용하는 모든 DataflowEndpointGroups 역할을 삭제해야 삭제할 수 있습니다.

> **Note**
>
> 리소스를 삭제하려 할 때 Ground Station 서비스가 역할을 사용 중이면 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

에서 사용하는 Ground Station 리소스를 삭제하려면 AWSServiceRoleForGroundStationDataflowEndpointGroup

- AWSCLI또는 DataflowEndpointGroups 를 통해 삭제합니다 AWSAPI.

를 사용하여 서비스 연결 역할을 수동으로 삭제하려면 IAM

IAM콘솔 AWS CLI, 또는 를 AWS API 사용하여 AWSServiceRoleForGroundStationDataflowEndpointGroup 서비스 연결 역할을 삭제합니다. 자세한 내용은 사용 설명서의 서비스 연결 역할 삭제를 참조하십시오. IAM

Ground Station 서비스 연결 역할이 지원되는 리전

Ground Station에서는 서비스를 사용할 수 있는 모든 리전에서 서비스 연결 역할 사용을 지원합니다. 자세한 내용은 리전 표를 참조하세요.

문제 해결

`NOT_AUTHORIZED_TO_CREATE_SLR`- 이는 를 호출하는 데 사용되는 사용자 계정의 역할에 권한이 CreateDataflowEndpointGroup API 없음을 나타냅니다. `iam:CreateServiceLinkedRole` `iam:CreateServiceLinkedRole` 권한이 있는 관리자는 계정의 서비스 연결 역할을 수동으로 생성해야 합니다.

유휴 데이터 암호화 AWS Ground Station

AWS Ground Station 기본적으로 암호화를 제공하여 저장된 민감한 데이터를 AWS 자체 암호화 키를 사용하여 보호합니다.

- AWS소유 키 - 기본적으로 이러한 키를 AWS Ground Station 사용하여 직접 식별 가능한 개인 데이터와 에페메리드를 자동으로 암호화합니다. AWS소유 키를 확인, 관리 또는 사용하거나 사용을 감사할 수는 없습니다. 하지만 데이터를 암호화하는 키를 보호하기 위한 조치를 취하거나 프로그램을 변경할 필요는 없습니다. 자세한 내용은 키 관리 서비스 개발자 AWS 가이드의 -own AWS keys를 참조하십시오.

기본적으로 저장 데이터를 암호화하면 민감한 데이터 보호와 관련된 운영 오버헤드와 복잡성을 줄이는 데 도움이 됩니다. 동시에 엄격한 암호화 규정 준수 및 규제 요구 사항을 충족하는 안전한 애플리케이션을 구축할 수 있습니다.

AWS Ground Station 모든 민감한 미사용 데이터에 암호화를 적용하지만 에페메리데스와 같은 일부 AWS Ground Station 리소스의 경우 기본 관리 키 대신 고객 관리 키를 사용하도록 선택할 수 있습니다. AWS

- 고객 관리 키 -- 사용자가 생성하고 소유하고 관리하는 대칭형 고객 관리 키를 사용하여 기존 소유 암호화에 두 번째 암호화 계층을 추가할 수 있도록 AWS Ground Station 지원합니다. AWS 이 암호화 계층을 완전히 제어할 수 있으므로 다음과 같은 작업을 수행할 수 있습니다.
  - 키 정책 수립 및 유지
  - IAM정책 및 보조금의 수립 및 유지
  - 키 정책 활성화 및 비활성화
  - 키 암호화 자료 교체
  - 태그 추가
  - 키 별칭 생성
  - 삭제를 위한 스케줄 키

자세한 내용은 키 관리 서비스 개발자 가이드의 고객 관리형 AWS 키를 참조하십시오.

다음 표에는 고객 관리 키 사용을 AWS Ground Station 지원하는 리소스가 요약되어 있습니다.

데이터 유형	AWS 소유 키 암호화	고객 관리형 키 암호화 (선택 사항)
위성의 궤적을 계산하는 데 사용되는 Ephemeris 데이터	활성화됨	활성화됨

> **Note**
>
> AWS Ground Station AWS 소유 키를 사용하여 저장된 데이터를 자동으로 암호화하여 개인 식별 데이터를 무료로 보호합니다. 하지만 고객 관리 키 사용에는 AWS KMS 요금이 부과됩니다. 요금에 대한 자세한 내용은 AWS키 관리 서비스 요금을 참조하십시오.
> 에 대한 AWS KMS 자세한 내용은 AWSKMS개발자 안내서를 참조하십시오.

지원금을 AWS Ground Station 사용하는 방법 AWS KMS

AWS Ground Station 고객 관리 키를 사용하려면 키 부여가 필요합니다.

고객 관리 키로 암호화된 Epemeris를 업로드하면 에서 요청을 전송하여 사용자를 대신하여 키 부여를 AWS Ground Station 생성합니다. CreateGrant AWS KMS 권한 AWS KMS 부여는 계정의 KMS 키에 AWS Ground Station 대한 액세스 권한을 부여하는 데 사용됩니다.

AWS Ground Station 다음과 같은 내부 작업에 고객 관리 키를 사용하려면 권한 부여가 필요합니다.

- 고객 관리 키로 암호화된 데이터 키를 AWS KMS 생성해 GenerateDataKey달라는 요청을 보내세요.
- 암호화된 데이터 키를 해독하여 AWS KMS 데이터를 암호화하는 데 사용할 수 있도록 암호 해독 요청을 보내십시오.
- 제공된 데이터를 암호화하도록 AWS KMS 암호화 요청을 보내십시오.

언제든지 권한 부여에 대한 액세스 권한을 취소하거나 고객 관리형 키에 대한 서비스 액세스를 제거할 수 있습니다. 이렇게 하면 고객 관리 키로 암호화된 데이터에 액세스할 수 AWS Ground Station 없게

되며, 이는 해당 데이터에 의존하는 작업에 영향을 미칩니다. 예를 들어, 현재 연락처에 사용 중인 임시 계정에서 키 부여를 AWS Ground Station 삭제하면 제공된 임시 데이터를 사용하여 연락하는 동안 안테나를 가리키는 데 사용할 수 없게 됩니다. 이렇게 하면 연락이 특정 상태에서 종료됩니다. FAILED

고객 관리형 키 생성

관리 콘솔 또는 를 사용하여 대칭적인 고객 AWS 관리 키를 생성할 수 있습니다. AWS KMS APIs

대칭형 고객 관리형 키를 생성하려면

키 관리 서비스 개발자 가이드의 대칭 고객 관리AWS 키 생성 단계를 따르세요.

키 정책

키 정책은 고객 관리형 키에 대한 액세스를 제어합니다. 모든 고객 관리형 키에는 키를 사용할 수 있는 사람과 키를 사용하는 방법을 결정하는 문장이 포함된 정확히 하나의 키 정책이 있어야 합니다. 고객 관리형 키를 생성할 때 키 정책을 지정할 수 있습니다. 자세한 내용은 키 관리 서비스 개발자 가이드의 고객 관리 키에 AWS 대한 액세스 관리를 참조하십시오.

고객 관리 키를 AWS Ground Station 리소스와 함께 사용하려면 키 정책에서 다음 API 작업을 허용해야 합니다.

`kms:CreateGrant` - 고객 관리형 키에 권한 부여를 추가합니다. 지정된 KMS 키에 대한 제어 액세스 권한을 부여하여 권한 부여 작업에 AWS Ground Station 필요한 액세스를 허용합니다. 권한 부여 사용에 대한 자세한 내용은 AWS 키 관리 서비스 개발자 안내서를 참조하십시오.

이를 통해 Amazon은 AWS 다음 작업을 수행할 수 있습니다.

- 암호화하는 GenerateDataKey데 데이터 키가 즉시 사용되지 않으므로 암호화된 데이터 키를 생성하여 저장하려면 호출하십시오.
- 저장된 암호화된 데이터 키를 사용하여 암호화된 데이터에 액세스하려면 Decrypt를 호출하십시오.
- 데이터 키를 사용하여 데이터를 암호화하려면 Encrypt를 호출하십시오.
- 서비스가 `RetireGrant`를 사용할 수 있도록 은퇴하는 보안 주체를 설정하세요.

`kms:DescribeKey`- 제공된 키에 대한 권한 부여를 시도하기 전에 키를 검증할 수 있도록 AWS Ground Station 고객 관리 키 세부 정보를 제공합니다.

다음은 추가할 수 있는 IAM 정책 설명 예제입니다. AWS Ground Station

```
"Statement" : [
```

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

정책에서 권한을 지정하는 방법에 대한 자세한 내용은 AWS 키 관리 서비스 개발자 안내서를 참조하십시오.

키 액세스 문제 해결에 대한 자세한 내용은 AWS 키 관리 서비스 개발자 안내서를 참조하십시오.

고객 관리 키 지정: AWS Ground Station

다음 리소스를 암호화하기 위해 고객 관리형 키를 지정할 수 있습니다.

- Ephemeris

리소스를 생성할 때 다음을 제공하여 데이터 키를 지정할 수 있습니다. kmsKeyArn

- kmsKeyArn- AWS KMS 고객 관리 키의 키 식별자

AWS Ground Station 암호화 컨텍스트

암호화 컨텍스트는 데이터에 대한 추가 컨텍스트 정보를 포함하는 선택적 키-값 페어 세트입니다. AWS KMS암호화 컨텍스트를 인증된 추가 데이터로 사용하여 인증된 암호화를 지원합니다. 데이터 암호화 요청에 암호화 컨텍스트를 포함하면 암호화 컨텍스트를 암호화된 데이터에 AWS KMS 바인딩합니다. 요청에 동일한 암호화 컨텍스트를 포함해야 이 데이터를 해독할 수 있습니다.

AWS Ground Station 암호화 컨텍스트

AWS Ground Station 암호화되는 리소스에 따라 다른 암호화 컨텍스트를 사용하고 생성된 각 키 부여에 대해 특정 암호화 컨텍스트를 지정합니다.

Ephemeris 암호화 컨텍스트:

에페메리스 리소스 암호화를 위한 키 부여는 특정 위성에 바인딩됩니다. ARN

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

> **Note**
>
> 키 부여는 동일한 키-위성 쌍에 재사용됩니다.

모니터링을 위한 암호화 컨텍스트 사용

대칭형 고객 관리형 키를 사용하여 Ephemeris를 암호화하는 경우 감사 레코드 및 로그의 암호화 컨텍스트를 사용하여 고객 관리형 키가 사용되는 방식을 식별할 수도 있습니다. 암호화 컨텍스트는 AWS CloudTrail 또는 Amazon Logs에서 생성한 CloudWatch 로그에도 나타납니다.

암호화 컨텍스트를 사용하여 고객 관리형 키에 대한 액세스 제어

키 정책 및 IAM 정책의 암호화 컨텍스트를 사용하여 대칭 고객 관리 키에 대한 `conditions` 액세스를 제어할 수 있습니다. 또한 권한 부여에서 암호화 컨텍스트 제약 조건을 사용할 수 있습니다.

AWS Ground Station 권한 부여의 암호화 컨텍스트 제약을 사용하여 계정 또는 지역의 고객 관리 키에 대한 액세스를 제어합니다. 권한 부여 제약 조건에 따라 권한 부여가 허용하는 작업은 지정된 암호화 컨텍스트를 사용해야 합니다.

다음은 특정 암호화 컨텍스트에서 고객 관리형 키에 대한 액세스 권한을 부여하는 키 정책 설명의 예입니다. 이 정책 설명의 조건에 따라 권한 부여에는 암호화 컨텍스트를 지정하는 암호화 컨텍스트 제약 조건이 있어야 합니다.

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

암호화 키 모니터링 대상 AWS Ground Station

AWS Ground Station 리소스와 함께 AWS KMS 고객 관리 키를 사용하는 AWS CloudTrail경우 Amazon CloudWatch 로그를 사용하여 로 AWS Ground Station 보내는 요청을 추적할 수 AWS KMS 있습니다. 다음 예는 고객 관리 키로 암호화된 데이터에 `DescribeKey` 액세스하기 위해 AWS Ground Station에서 호출한 `CreateGrant` `GenerateDataKeyDecrypt`,, `Encrypt` 및 모니터링 KMS 작업에 대한 AWS CloudTrail 이벤트입니다.

`CreateGrant` (Cloudtrail)

AWS KMS고객 관리 키를 사용하여 ephemeris 리소스를 암호화하는 경우, 는 사용자 대신 계정의 KMS 키에 `CreateGrant` 액세스하라는 요청을 AWS Ground Station 보냅니다. AWS AWS Ground Station 생성되는 권한 부여는 고객 관리 키와 연결된 리소스에만 적용됩니다. AWS KMS 또한 AWS Ground Station은 리소스를 삭제할 때 이 `RetireGrant` 작업을 사용하여 허가를 제거합니다.

다음 예제 이벤트는 `CreateGrant` 작업을 기록합니다.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AAAAAAAAAAAAAAAAAAAAA:SampleUser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/SampleUser01",
        "accountId": "111122223333",
        "accessKeyId": "ASIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AAAAAAAAAAAAAAAAAAAAA",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-02-22T22:22:22Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2022-02-22T22:22:22Z",
```

```
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "111.11.11.11",
    "userAgent": "ExampleDesktop/1.0 (V1; OS)",
    "requestParameters": {
        "operations": [
            "GenerateDataKeyWithoutPlaintext",
            "Decrypt",
            "Encrypt"
        ],
        "constraints": {
            "encryptionContextSubset": {
                "aws:groundstation:arn":
 "arn:aws:groundstation::111122223333:satellite/00a770b0-082d-45a4-80ed-SAMPLE"
            }
        },
        "granteePrincipal": "groundstation.us-west-2.amazonaws.com",
        "retiringPrincipal": "groundstation.us-west-2.amazonaws.com",
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "responseElements": {
        "grantId":
 "0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE"
    },
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

DescribeKey (Cloudtrail)

AWS KMS고객 관리 키를 사용하여 ephemeris 리소스를 암호화하는 경우 요청된 키가 계정에 존재하는지 DescribeKey 확인하라는 요청을 대신 AWS Ground Station 보냅니다.

다음 예제 이벤트는 DescribeKey 작업을 기록합니다.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AAAAAAAAAAAAAAAAAAAAA:SampleUser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/User/Role",
        "accountId": "111122223333",
        "accessKeyId": "ASIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AAAAAAAAAAAAAAAAAAAAA",
                "arn": "arn:aws:iam::111122223333:role/Role",
                "accountId": "111122223333",
                "userName": "User"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-02-22T22:22:22Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2022-02-22T22:22:22Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DescribeKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
```

```
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

GenerateDataKey (Cloudtrail)

AWS KMS고객 관리 키를 사용하여 ephemeris 리소스를 암호화하는 경우, 는 데이터를 암호화하는 데 KMS 사용할 데이터 키를 생성하기 위해 GenerateDataKey 요청을 로 AWS Ground Station 보냅니다.

다음 예제 이벤트는 GenerateDataKey 작업을 기록합니다.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2022-02-22T22:22:22Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keySpec": "AES_256",
        "encryptionContext": {
            "aws:groundstation:arn":
 "arn:aws:groundstation::111122223333:satellite/00a770b0-082d-45a4-80ed-SAMPLE",
            "aws:s3:arn":
 "arn:aws:s3:::customerephemerisbucket/0034abcd-12ab-34cd-56ef-123456SAMPLE"
```

```
        },
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "sharedEventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventCategory": "Management"
}
```

Decrypt (Cloudtrail)

AWS KMS고객 관리 키를 사용하여 이피메리스 리소스를 암호화하는 경우, 동일한 고객 관리 키로 이미 암호화된 경우, 제공된 에페메리스를 해독하는 `Decrypt` 작업을 AWS Ground Station 사용합니다. 예를 들어 S3 버킷에서 epemeris를 업로드하고 해당 버킷에서 지정된 키를 사용하여 암호화하는 경우를 예로 들 수 있습니다.

다음 예제 이벤트는 `Decrypt` 작업을 기록합니다.

```
{
    "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"
}
```


전송 중 데이터 암호화 AWS Ground Station

AWS Ground Station 전송 중에 민감한 데이터를 보호하기 위해 기본적으로 암호화를 제공합니다. 미션 프로필 구성에 따라 두 가지 방법으로 AWS Ground Station 안테나 위치와 Amazon EC2 인스턴스 간에 데이터를 스트리밍할 수 있습니다.

- AWS Ground Station 에이전트
- 데이터 흐름 엔드포인트

데이터 스트리밍의 각 방법은 전송 데이터 암호화를 다르게 처리합니다. 다음 섹션에서는 각 방법을 설명합니다.

AWS Ground Station 에이전트 스트림

AWS Ground Station 에이전트는 고객 관리 AWS KMS 키를 사용하여 스트림을 암호화합니다. Amazon EC2 인스턴스에서 실행되는 AWS Ground Station 에이전트는 스트림을 자동으로 해독하여 복호화된 데이터를 제공합니다.

스트림을 암호화하는 데 사용되는 AWS KMS 키는 파라미터에서 를 생성할 때 지정됩니다. `MissionProfile` streamsKmsKey 키에 AWS Ground Station 대한 액세스 권한을 부여하는 모든 권한은 연결된 AWS KMS 키 정책을 통해 처리됩니다. `streamsKmsKey`

데이터플로우 엔드포인트 스트림

Dataflow 엔드포인트 스트림은 데이터그램 전송 계층 보안 () 을 사용하여 암호화됩니다. DTLS 이는 자체 서명된 인증서를 사용하여 수행되며 추가 구성이 필요하지 않습니다.

미션 프로필 구성 예시

제공된 예시는 공공 방송 위성을 촬영하고 이를 지원하는 임무 프로필을 만드는 방법을 보여줍니다. 결과 템플릿은 공용 방송 위성과 연락을 취하고 위성에 대한 결정을 내리는 데 도움이 되도록 제공됩니다.

주제

- JPSS-1 - 공용 방송 위성 (PBS) - 평가
- Amazon S3 데이터 전송을 활용하는 공공 방송 위성
- 데이터 흐름 엔드포인트 (협대역) 를 활용하는 공영 방송 위성
- 데이터 흐름 엔드포인트를 활용하는 공영 방송 위성 (복조 및 디코딩)
- AWS Ground Station 에이전트 (광대역) 를 활용한 공영방송 위성

JPSS-1 - 공용 방송 위성 (PBS) - 평가

이 예제 섹션은 과 고객 온보딩 프로세스 개요 일치합니다. 다음 예제에 대한 간략한 호환성 분석을 제공하고 다음 예제를 위한 단계를 설정합니다. AWS Ground Station

공공 방송 위성섹션에서 설명한 것처럼 공개적으로 사용 가능한 일부 위성 또는 위성의 통신 경로를 활용할 수 있습니다. 이 섹션에서는 용어로 JPSS-1을 설명합니다. AWS Ground Station 참고로, 우리는 Joint Polar Satellite System 1 (JPSS-1) 우주선 고속 데이터 (HRD) 에서 직접 방송국에 대한 (DBS) 무선 주파수 (RF) 인터페이스 제어 문서 (ICD) 를 활용하여 예제를 완성합니다. 또한 JPSS -1이 NORAD ID 43013과 연관되어 있다는 점도 주목할 만합니다.

그림 1-1에서 볼 수 있듯이 JPSS -1 위성은 업링크 1개와 다이렉트 다운링크 통신 경로 3개를 제공합니다. ICD 이 네 가지 통신 경로 중 대중이 사용할 수 있는 유일한 High Rate Data (HRD) 다운링크 통신 경로는 단 하나뿐입니다. 이를 바탕으로 보면 이 경로에도 훨씬 더 구체적인 데이터가 연관되어 있음을 알 수 있습니다. 네 가지 경로는 다음과 같습니다.

- MHz중앙 주파수 2067.27의 명령 경로 (업링크), 데이터 전송 속도는 2-128kbps입니다. 이 경로는 공개적으로 액세스할 수 없습니다.
- MHz중앙 주파수 2247.5의 원격 측정 경로 (다운링크), 데이터 전송 속도는 1~524kbps입니다. 이 경로는 공개적으로 액세스할 수 없습니다.
- SMD경로 (다운링크) 는 GHz 중앙 주파수가 26.7034이고 데이터 속도는 150-300Mbps입니다. 이 경로는 공개적으로 액세스할 수 없습니다.

- 데이터 속도가 15Mbps인 7812 MHz 중앙 주파수의 HRD 경로 (다운링크) 용 RF. MHz대역폭은 30이고, 그렇습니다. right-hand-circular-polarized 를 사용하여 JPSS -1을 AWS Ground Station온보딩하면 이 통신 경로를 통해 액세스할 수 있습니다. 이 통신 경로에는 기기 과학 데이터, 기기 엔지니어링 데이터, 기기 원격 측정 데이터 및 실시간 우주선 관리 데이터가 포함됩니다.

잠재적 데이터 경로를 비교해 보면 명령 (업링크), 텔레메트리 (다운링크) 및 HRD (다운링크) 경로가 의 주파수, 대역폭 및 다중 채널 동시 사용 기능을 충족한다는 것을 알 수 있습니다. AWS Ground Station중심 주파수가 기존 수신기 범위를 벗어나므로 SMD 경로가 호환되지 않습니다. 지원되는 기능에 대한 자세한 내용은 을 참조하십시오AWS Ground Station 사이트 기능.

> **Note**
>
> SMD경로가 해당 경로와 호환되지 AWS Ground Station 않으므로 예제 구성에는 표시되지 않습니다.

> **Note**
>
> 명령 (업링크) 및 원격 분석 (다운링크) 경로는 에 정의되어 있지 않으며 공용으로 사용할 수도 없기 때문에 사용 시 제공된 값은 표준입니다. ICD

Amazon S3 데이터 전송을 활용하는 공공 방송 위성

이 예제는 사용 설명서의 JPSS-1 - 공용 방송 위성 (PBS) - 평가 섹션에서 수행한 분석을 기반으로 합니다.

이 예제에서는 HRD 통신 경로를 디지털 중간 주파수로 캡처하여 향후 일괄 처리를 위해 저장하려는 시나리오를 가정해야 합니다. 이렇게 하면 디지털화된 후 원시 무선 주파수 (RF) 동위상 직교 (I/Q) 샘플이 절약됩니다. 데이터가 Amazon S3 버킷에 저장되면 원하는 소프트웨어를 사용하여 데이터를 복조 및 디코딩할 수 있습니다. 처리에 대한 자세한 예는 MathWorks 자습서를 참조하십시오. 이 예제를 사용한 후에는 데이터를 처리하고 전체 처리 비용을 낮추기 위해 Amazon EC2 스팟 요금 구성 요소를 추가하는 것을 고려해 볼 수 있습니다.

통신 경로

이 섹션은 2단계: 데이터 흐름 통신 경로 계획 시작에 대해 설명합니다.

다음 템플릿 스니펫은 모두 템플릿의 AWS CloudFormation 리소스 섹션에 속합니다.

```
Resources:
  # Resources that you would like to create should be placed within the Resources
 section.
```

> **Note**
>
> 템플릿 내용에 대한 자세한 내용은 AWS CloudFormation 템플릿 섹션을 참조하십시오.

Amazon S3에 단일 통신 경로를 전달하는 시나리오를 생각해 보면 단일 비동기 전송 경로를 갖게 된다는 것을 알 수 있습니다. 비동기 데이터 전송섹션에 따라 Amazon S3 버킷을 정의해야 합니다.

```
  # 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]]]]]]
```

또한 버킷 사용을 AWS Ground Station 허용하려면 적절한 역할과 정책을 생성해야 합니다.

```
  # 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 구성

이 섹션에서는 시작하는 3단계: 구성 생성 방법을 설명합니다.

자동 추적 사용에 대한 기본 설정을 지정하려면 추적 구성이 필요합니다. 자동 추적을 선택하면 PREFERRED신호 품질을 개선할 수 있지만 -1 ephemeris 품질이 충분하기 때문에 신호 품질을 반드시 충족할 필요는 없습니다. JPSS

```
  TrackingConfig:
```

```
    Type: AWS::GroundStation::Config
    Properties:
      Name: "JPSS Tracking Config"
      ConfigData:
        TrackingConfig:
          Autotrack: "PREFERRED"
```

통신 경로에 따라 위성 부분을 나타내는 안테나 다운링크 구성과 방금 생성한 Amazon S3 버킷을 참조하는 s3 녹화를 정의해야 합니다.

```
 # 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 미션 프로필

이 섹션은 4단계: 미션 프로필 생성 시작에 대해 설명합니다.

이제 관련 구성이 준비되었으므로 이를 사용하여 데이터 흐름을 구성할 수 있습니다. 나머지 매개변수에는 기본값을 사용하겠습니다.

```
 # 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
```

모두 합치기

위의 리소스를 통해 이제 모든 온보드의 비동기 데이터 전송을 위해 JPSS 1-1개의 연락처를 예약할 수 있습니다. AWS Ground Station 위치

다음은 이 섹션에 설명된 모든 리소스가 에서 직접 사용할 수 있는 단일 템플릿으로 결합된 완전한 AWS CloudFormation 템플릿입니다. AWS CloudFormation

라는 AWS CloudFormation 템플릿에는 Amazon S3 버킷과 연락처를 예약하고 VITA -49 신호/IP 다이렉트 브로드캐스트 데이터를 수신하는 데 필요한 AWS Ground Station 리소스가 `AquaSnppJpss-1TerraDigIfS3DataDelivery.yml` 포함되어 있습니다.

AquaSNPP, JPSS -1/ NOAA -20 및 Terra가 계정에 온보딩되지 않은 경우 을 참조하십시오. 1단계: 새 틀라이트 온보딩

> **Note**
>
> 고객 온보딩 Amazon S3 버킷에 액세스하여 템플릿에 액세스할 수 있습니다. 아래 링크는 리전 Amazon S3 버킷을 사용합니다. AWS CloudFormation 스택을 생성하려는 해당 지역을 나타내도록 지역 코드를 변경하십시오. `us-west-2`

또한 다음 지침에서도 사용합니다YAML. 그러나 템플릿은 두 가지 JSON 형식 YAML 모두에서 사용할 수 있습니다. 사용하려면 JSON 템플릿을 다운로드할 `.json` 때 `.yml` 파일 확장자를 로 바꾸십시오.

를 사용하여 AWS CLI템플릿을 다운로드하려면 다음 명령을 사용합니다.

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

브라우저에서 다음으로 이동하여 콘솔에서 템플릿을 보고 다운로드할 수 있습니다. URL

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

다음 링크를 AWS CloudFormation 사용하여 템플릿을 직접 지정할 수 있습니다.

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

데이터 흐름 엔드포인트 (협대역) 를 활용하는 공영 방송 위성

이 예제는 사용 설명서 JPSS-1 - 공용 방송 위성 (PBS) - 평가 섹션에서 수행한 분석을 기반으로 합니다.

이 예제를 완료하려면 HRD 통신 경로를 디지털 중간 주파수 (DiGif) 로 캡처하고 Amazon EC2 인스턴스의 데이터 흐름 엔드포인트 애플리케이션이 수신한 대로 처리하려는 시나리오를 가정해야 합니다. SDR

통신 경로

이 섹션은 2단계: 데이터 흐름 통신 경로 계획 시작에 대해 설명합니다. 이 예시에서는 AWS CloudFormation 템플릿에 매개변수와 리소스 섹션이라는 두 개의 섹션을 생성합니다.

> **Note**
>
> 템플릿 내용에 대한 자세한 내용은 AWS CloudFormation 템플릿 섹션을 참조하십시오.

매개 변수 섹션에는 다음 매개 변수를 추가할 것입니다. AWS CloudFormation 콘솔을 통해 스택을 생성할 때 이러한 값을 지정해야 합니다.

```
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**
>
> 키 페어를 생성하고 Amazon EC2 **EC2Key** 파라미터의 이름을 제공해야 합니다. Amazon EC2 인스턴스용 키 페어 생성을 참조하십시오.
> 또한 AWS CloudFormation 스택을 생성할 때 올바른 지역별 AMI ID를 제공해야 합니다. AWS Ground Station 아마존 머신 이미지 (AMIs)을 참조하세요.

나머지 템플릿 스니펫은 템플릿의 AWS CloudFormation 리소스 섹션에 속합니다.

```
Resources:
  # Resources that you would like to create should be placed within the resource
 section.
```

EC2인스턴스에 단일 통신 경로를 전달하는 시나리오에서는 단일 동기 전송 경로를 갖게 됩니다. 동기 데이터 전송섹션에 따라 데이터 흐름 엔드포인트 애플리케이션을 사용하여 Amazon EC2 인스턴스를 설정 및 구성하고 데이터 흐름 엔드포인트 그룹을 하나 이상 생성해야 합니다.

```
 # The EC2 instance that will send/receive data to/from your satellite using AWS
Ground Station.
 ReceiverInstance:
   Type: AWS::EC2::Instance
   Properties:
     DisableApiTermination: false
     IamInstanceProfile: !Ref GeneralInstanceProfile
     ImageId: !Ref ReceiverAMI
     InstanceType: m5.4xlarge
     KeyName: !Ref EC2Key
     Monitoring: true
     PlacementGroupName: !Ref ClusterPlacementGroup
     SecurityGroupIds:
       - Ref: InstanceSecurityGroup
     SubnetId: !Ref ReceiverSubnet
     BlockDeviceMappings:
       - DeviceName: /dev/xvda
         Ebs:
           VolumeType: gp2
           VolumeSize: 40
     Tags:
       - Key: Name
         Value: !Join [ "-" , [ "Receiver" , !Ref "AWS::StackName" ] ]
     UserData:
       Fn::Base64:
         |
         #!/bin/bash
         exec > >(tee /var/log/user-data.log|logger -t user-data -s 2>/dev/console)
2>&1
         echo `date +'%F %R:%S'` "INFO: Logging Setup" >&2

         GROUND_STATION_DIR="/opt/aws/groundstation"
         GROUND_STATION_BIN_DIR="${GROUND_STATION_DIR}/bin"
         STREAM_CONFIG_PATH="${GROUND_STATION_DIR}/customer_stream_config.json"

         echo "Creating ${STREAM_CONFIG_PATH}"
         cat << STREAM_CONFIG > "${STREAM_CONFIG_PATH}"
         {
           "ddx_streams": [
             {
               "streamName": "Downlink",
               "maximumWanRate": 4000000000,
               "lanConfigDevice": "lo",
               "lanConfigPort": 50000,
```

```
                "wanConfigDevice": "eth1",
                "wanConfigPort": 55888,
                "isUplink": false
              }
            ]
          }
          STREAM_CONFIG

          echo "Waiting for dataflow endpoint application to start"
          while netstat -lnt | awk '$4 ~ /:80$/ {exit 1}'; do sleep 10; done

          echo "Configuring dataflow endpoint application streams"
          python "${GROUND_STATION_BIN_DIR}/configure_streams.py" --configFileName
"${STREAM_CONFIG_PATH}"
          sleep 2
          python "${GROUND_STATION_BIN_DIR}/save_default_config.py"

          exit 0

  # The AWS Ground Station Dataflow Endpoint Group that defines the endpoints that AWS
Ground
  # Station will use to send/receive data to/from your satellite.
  DataflowEndpointGroup:
    Type: AWS::GroundStation::DataflowEndpointGroup
    Properties:
      ContactPostPassDurationSeconds: 180
      ContactPrePassDurationSeconds: 120
      EndpointDetails:
        - Endpoint:
            Name: !Join [ "-" , [ !Ref "AWS::StackName" , "Downlink" ] ] # needs to
match DataflowEndpointConfig name
            Address:
              Name: !GetAtt ReceiverInstanceNetworkInterface.PrimaryPrivateIpAddress
              Port: 55888
          SecurityDetails:
            SecurityGroupIds:
              - Ref: "DataflowEndpointSecurityGroup"
            SubnetIds:
              - !Ref ReceiverSubnet
            RoleArn: !GetAtt DataDeliveryServiceRole.Arn

  # The security group for your EC2 instance.
  InstanceSecurityGroup:
    Type: AWS::EC2::SecurityGroup
```

```
    Properties:
      GroupDescription: AWS Ground Station receiver instance security group.
      VpcId: !Ref ReceiverVPC
      SecurityGroupIngress:
        # To allow SSH access to the instance, add another rule allowing tcp port 22
from your CidrIp
        - IpProtocol: udp
          FromPort: 55888
          ToPort: 55888
          SourceSecurityGroupId: !Ref DataflowEndpointSecurityGroup
          Description: "AWS Ground Station Downlink Stream"

  # The security group that the ENI created by AWS Ground Station belongs to.
  DataflowEndpointSecurityGroup:
    Type: AWS::EC2::SecurityGroup
    Properties:
      GroupDescription: Security Group for AWS Ground Station registration of Dataflow
Endpoint Groups
      VpcId: !Ref ReceiverVPC
      SecurityGroupEgress:
        - IpProtocol: udp
          FromPort: 55888
          ToPort: 55888
          CidrIp: 10.0.0.0/8
          Description: "AWS Ground Station Downlink Stream To 10/8"
        - IpProtocol: udp
          FromPort: 55888
          ToPort: 55888
          CidrIp: 172.16.0.0/12
          Description: "AWS Ground Station Downlink Stream To 172.16/12"
        - IpProtocol: udp
          FromPort: 55888
          ToPort: 55888
          CidrIp: 192.168.0.0/16
          Description: "AWS Ground Station Downlink Stream To 192.168/16"

  # The placement group in which your EC2 instance is placed.
  ClusterPlacementGroup:
    Type: AWS::EC2::PlacementGroup
    Properties:
      Strategy: cluster

  ReceiverVPC:
    Type: AWS::EC2::VPC
```

```
    Properties:
      CidrBlock: "10.0.0.0/16"
      Tags:
        - Key: "Name"
          Value: "AWS Ground Station - PBS to dataflow endpoint Example VPC"
        - Key: "Description"
          Value: "VPC for EC2 instance receiving AWS Ground Station data"

  ReceiverSubnet:
    Type: AWS::EC2::Subnet
    Properties:
      CidrBlock: "10.0.0.0/24"
      Tags:
        - Key: "Name"
          Value: "AWS Ground Station - PBS to dataflow endpoint Example Subnet"
        - Key: "Description"
          Value: "Subnet for EC2 instance receiving AWS Ground Station data"
      VpcId: !Ref ReceiverVPC

  # An ENI providing a fixed IP address for AWS Ground Station to connect to.
  ReceiverInstanceNetworkInterface:
    Type: AWS::EC2::NetworkInterface
    Properties:
      Description: Floating network interface providing a fixed IP address for AWS
Ground Station to connect to.
      GroupSet:
        - !Ref InstanceSecurityGroup
      SubnetId: !Ref ReceiverSubnet

  # Attach the ENI to the EC2 instance.
  ReceiverInstanceInterfaceAttachment:
    Type: AWS::EC2::NetworkInterfaceAttachment
    Properties:
      DeleteOnTermination: false
      DeviceIndex: "1"
      InstanceId: !Ref ReceiverInstance
      NetworkInterfaceId: !Ref ReceiverInstanceNetworkInterface
```

또한 계정에 Elastic Network Interface (ENI) 를 생성할 수 AWS Ground Station 있도록 적절한 정책과 역할을 만들어야 합니다.

```
 # 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 구성

이 섹션에서는 시작하는 3단계: 구성 생성 방법을 설명합니다.

자동 추적 사용에 대한 기본 설정을 지정하려면 추적 구성이 필요합니다. 자동 추적을 선택하면 PREFERRED신호 품질을 개선할 수 있지만 -1 ephemeris 품질이 충분하기 때문에 신호 품질을 반드시 충족할 필요는 없습니다. JPSS

```
  TrackingConfig:
    Type: AWS::GroundStation::Config
    Properties:
      Name: "JPSS Tracking Config"
      ConfigData:
        TrackingConfig:
          Autotrack: "PREFERRED"
```

통신 경로에 따라 위성 부분을 나타내는 안테나-다운링크 컨피그레이션과 엔드포인트 세부 정보를 정의하는 데이터플로우 엔드포인트 그룹을 참조하는 데이터플로우 엔드포인트 컨피그레이션을 정의해야 합니다.

```
  # 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 미션 프로필

이 섹션은 4단계: 미션 프로필 생성 시작에 대해 설명합니다.

이제 관련 구성이 준비되었으므로 이를 사용하여 데이터 흐름을 구성할 수 있습니다. 나머지 매개변수에는 기본값을 사용하겠습니다.

```
  # 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
```

모두 합치기

위의 리소스를 통해 이제 모든 AWS Ground Station 위치 온보드의 동시 데이터 전송을 위해 JPSS 1-1 개의 연락처를 예약할 수 있습니다.

다음은 이 섹션에 설명된 모든 리소스가 에서 직접 사용할 수 있는 단일 템플릿으로 결합된 완전한 AWS CloudFormation 템플릿입니다. AWS CloudFormation

이름이 지정된 AWS CloudFormation `AquaSnppJpssTerraDigIF.yml` 템플릿은 AquaSNPP, JPSS -1/ NOAA -20 및 Terra 위성에 대한 디지털화된 중간 주파수 (DiGif) 데이터 수신을 빠르게 시작할 수 있도록 설계되었습니다. 여기에는 Amazon EC2 인스턴스와 원본 DigiF 다이렉트 브로드캐스트 데이터를 수신하는 데 필요한 AWS CloudFormation 리소스가 포함되어 있습니다.

AquaSNPP, JPSS -1/ NOAA -20 및 Terra가 계정에 온보딩되지 않은 경우 을 참조하십시오. 1단계: 새 틀라이트 온보딩

> **Note**
>
> 고객 온보딩 Amazon S3 버킷에 액세스하여 템플릿에 액세스할 수 있습니다. 아래 링크는 리전 Amazon S3 버킷을 사용합니다. AWS CloudFormation 스택을 생성하려는 해당 지역을 나타내도록 지역 코드를 변경하십시오. `us-west-2`
> 또한 다음 지침에서도 사용합니다YAML. 그러나 템플릿은 두 가지 JSON 형식 YAML 모두에서 사용할 수 있습니다. 사용하려면 JSON 템플릿을 다운로드할 `.json` 때 `.yml` 파일 확장자를 로 바꾸십시오.

를 사용하여 AWS CLI템플릿을 다운로드하려면 다음 명령을 사용합니다.

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

브라우저에서 다음으로 이동하여 콘솔에서 템플릿을 보고 다운로드할 수 있습니다. URL

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

다음 링크를 AWS CloudFormation 사용하여 템플릿을 직접 지정할 수 있습니다.

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

템플릿은 어떤 추가 리소스를 정의합니까?

`AquaSnppJpssTerraDigIF`템플릿에는 다음과 같은 추가 리소스가 포함됩니다.

- (선택 사항) CloudWatch 이벤트 트리거 - 연락 AWS Ground Station 전후에 보낸 CloudWatch 이벤트를 사용하여 트리거되는 AWS Lambda 함수입니다. AWS Lambda 함수는 Receiver 인스턴스를 시작하고 선택적으로 중지합니다.
- (선택 사항) 연락처 EC2 확인 - Lambda를 사용하여 알림이 있는 연락처에 대해 EC2 Amazon 인스턴스의 확인 시스템을 설정하는 옵션입니다. SNS 이때 현재 사용량에 따라 요금이 부과될 수 있다는 점에 유의하세요.
- Ground Station Amazon 머신 이미지 검색 Lambda - 인스턴스에 설치할 소프트웨어와 원하는 소프트웨어를 선택할 수 있는 옵션입니다. AMI 소프트웨어 옵션에는 `DDX 2.6.2 Only` 및 `DDX 2.6.2 with qRadio 3.6.0`이 포함됩니다. 추가 소프트웨어 업데이트 및 기능이 출시됨에 따라 이러한 옵션은 계속 확장될 것입니다.
- 추가 임무 프로필 - 추가 공공 방송 위성 (Aqua, Terra) 의 임무 프로필. SNPP
- 추가 안테나 다운링크 구성 - 추가 공공 방송 위성 (Aqua, 및 Terra) 을 위한 안테나 다운링크 구성. SNPP

이 템플릿의 위성에 대한 값과 매개 변수가 이미 채워져 있습니다. 이러한 매개변수를 사용하면 이러한 위성과 함께 즉시 쉽게 사용할 수 있습니다. AWS Ground Station 이 템플릿을 사용할 AWS Ground Station 때는 값을 직접 구성하지 않아도 사용할 수 있습니다. 그러나 사용 사례에 맞게 템플릿을 작동하도록 값을 사용자 지정할 수 있습니다.

내 데이터는 어디에서 수신합니까?

데이터 흐름 엔드포인트 그룹은 템플릿의 일부로 생성되는 수신기 인스턴스 네트워크 인터페이스를 사용하도록 설정됩니다. Receiver 인스턴스는 dataflow 엔드포인트 애플리케이션을 사용하여 dataflow 엔드포인트에서 정의한 포트에서 데이터 스트림을 수신합니다. AWS Ground Station 수신된 데이터는 수신기 인스턴스의 루프백 어댑터에 있는 UDP 포트 50000을 통해 사용

할 수 있습니다. 데이터 흐름 엔드포인트 그룹 설정에 대한 자세한 내용은 그룹을 참조하십시오. AWS::GroundStation::DataflowEndpoint

데이터 흐름 엔드포인트를 활용하는 공영 방송 위성 (복조 및 디코딩)

이 예제는 사용 설명서의 JPSS-1 - 공용 방송 위성 (PBS) - 평가 섹션에서 수행한 분석을 기반으로 합니다.

이 예제를 완료하려면 데이터 흐름 엔드포인트를 사용하여 HRD 통신 경로를 복조 및 디코딩된 다이렉트 브로드캐스트 데이터로 캡처하려는 시나리오를 가정해야 합니다. NASADirect Readout Labs 소프트웨어 (RT- 및) 를 사용하여 데이터를 처리하려는 경우 이 예제를 시작하는 것이 좋습니다. STPS IPOPP

통신 경로

이 섹션은 2단계: 데이터 흐름 통신 경로 계획 시작에 대해 설명합니다. 이 예제에서는 AWS CloudFormation 템플릿에 매개변수와 리소스 섹션이라는 두 개의 섹션을 생성합니다.

> **Note**
>
> 템플릿 내용에 대한 자세한 내용은 AWS CloudFormation 템플릿 섹션을 참조하십시오.

매개 변수 섹션에는 다음 매개 변수를 추가할 것입니다. AWS CloudFormation 콘솔을 통해 스택을 생성할 때 이러한 값을 지정해야 합니다.

```
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**
>
> 키 페어를 생성하고 Amazon EC2 **EC2Key** 파라미터의 이름을 제공해야 합니다. Amazon EC2 인스턴스용 키 페어 생성을 참조하십시오.
> 또한 AWS CloudFormation 스택을 생성할 때 올바른 지역별 AMI ID를 제공해야 합니다. AWS Ground Station 아마존 머신 이미지 (AMIs)을 참조하세요.

나머지 템플릿 스니펫은 템플릿의 AWS CloudFormation 리소스 섹션에 속합니다.

```
Resources:
  # Resources that you would like to create should be placed within the resource
 section.
```

EC2인스턴스에 단일 통신 경로를 전달하는 시나리오에서는 단일 동기 전송 경로를 갖게 됩니다. 동기 데이터 전송섹션에 따라 데이터 흐름 엔드포인트 애플리케이션을 사용하여 Amazon EC2 인스턴스를 설정 및 구성하고 데이터 흐름 엔드포인트 그룹을 하나 이상 생성해야 합니다.

```
  # 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
```

또한 계정에 Elastic Network Interface (ENI) AWS Ground Station 를 만들려면 적절한 정책, 역할 및 프로필이 필요합니다.

```
  # 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 구성

이 3단계: 구성 생성 섹션은 사용 설명서를 나타냅니다.

자동 추적 사용에 대한 기본 설정을 지정하려면 추적 구성이 필요합니다. 자동 추적을 선택하면 PREFERRED신호 품질을 개선할 수 있지만 -1 ephemeris 품질이 충분하기 때문에 신호 품질을 반드시 충족할 필요는 없습니다. JPSS

```
TrackingConfig:
  Type: AWS::GroundStation::Config
  Properties:
    Name: "JPSS Tracking Config"
    ConfigData:
      TrackingConfig:
        Autotrack: "PREFERRED"
```

통신 경로에 따라 위성 부분을 나타내는 antenna-downlink-demod-decode컨피그레이션과 엔드포인트 세부 정보를 정의하는 데이터플로우 엔드포인트 그룹을 참조하는 데이터플로우 엔드포인트 컨피그레이션을 정의해야 합니다.

> **Note**
>
> 및 값을 설정하는 방법에 대한 자세한 내용은 을 참조하십시오. `DemodulationConfig` `DecodeConfig` 안테나 다운링크 복조 디코드 구성

```
 # 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 미션 프로필

이 4단계: 미션 프로필 생성 섹션은 사용자 안내서를 나타냅니다.

이제 관련 구성이 준비되었으므로 이를 사용하여 데이터 흐름을 구성할 수 있습니다. 나머지 매개변수에는 기본값을 사용하겠습니다.

```
 # 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
```

모두 합치기

위의 리소스를 통해 이제 모든 AWS Ground Station 위치 온보드의 동시 데이터 전송을 위해 JPSS 1-1 개의 연락처를 예약할 수 있습니다.

다음은 이 섹션에 설명된 모든 리소스가 에서 직접 사용할 수 있는 단일 템플릿으로 결합된 완전한 AWS CloudFormation 템플릿입니다. AWS CloudFormation

이름이 지정된 AWS CloudFormation `AquaSnppJpss.yml` 템플릿은 AquaSNPP, 및 JPSS -1/ NOAA -20 위성에 대한 데이터 수신을 빠르게 시작할 수 있도록 설계되었습니다. 여기에는 Amazon EC2 인스턴스와 연락처를 예약하고 복조 및 디코딩된 다이렉트 브로드캐스트 데이터를 수신하는 데 필요한 AWS Ground Station 리소스가 포함되어 있습니다.

AquaSNPP, JPSS -1/ NOAA -20 및 Terra가 계정에 온보딩되지 않은 경우 을 참조하십시오. 1단계: 새 틀라이트 온보딩

> **Note**
>
> 고객 온보딩 Amazon S3 버킷에 액세스하여 템플릿에 액세스할 수 있습니다. 아래 링크는 리전 Amazon S3 버킷을 사용합니다. AWS CloudFormation 스택을 생성하려는 해당 지역을 나타내도록 지역 코드를 변경하십시오. `us-west-2`
> 또한 다음 지침에서도 사용합니다YAML. 그러나 템플릿은 두 가지 JSON 형식 YAML 모두에서 사용할 수 있습니다. 사용하려면 JSON 템플릿을 다운로드할 `.json` 때 `.yml` 파일 확장자를 로 바꾸십시오.

를 사용하여 AWS CLI템플릿을 다운로드하려면 다음 명령을 사용합니다.

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

브라우저에서 다음으로 이동하여 콘솔에서 템플릿을 보고 다운로드할 수 있습니다. URL

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

다음 링크를 AWS CloudFormation 사용하여 템플릿을 직접 지정할 수 있습니다.

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

템플릿은 어떤 추가 리소스를 정의합니까?

AquaSnppJpss템플릿에는 다음과 같은 추가 리소스가 포함됩니다.

- (선택 사항) CloudWatch 이벤트 트리거 - 연락 AWS Ground Station 전후에 보낸 CloudWatch 이벤트를 사용하여 트리거되는 AWS Lambda 함수입니다. AWS Lambda 함수는 Receiver 인스턴스를 시작하고 선택적으로 중지합니다.
- (선택 사항) 연락처 EC2 확인 - Lambda를 사용하여 알림이 있는 연락처에 대해 EC2 Amazon 인스턴스의 확인 시스템을 설정하는 옵션입니다. SNS 이때 현재 사용량에 따라 요금이 부과될 수 있다는 점에 유의하세요.
- Ground Station Amazon 머신 이미지 검색 Lambda - 인스턴스에 설치할 소프트웨어와 원하는 소프트웨어를 선택할 수 있는 옵션입니다. AMI 소프트웨어 옵션에는 `DDX 2.6.2 Only` 및 `DDX 2.6.2 with qRadio 3.6.0`이 포함됩니다. 광대역 DiGif 데이터 전송 및 AWS Ground Station 에이전트를 사용하려면 을 참조하십시오. AWS Ground Station 에이전트 (광대역) 를 활용한 공영방송 위성 추가 소프트웨어 업데이트 및 기능이 출시됨에 따라 이러한 옵션은 계속 확장될 것입니다.
- 추가 임무 프로필 - 추가 공공 방송 위성 (Aqua, Terra) 의 임무 프로필. SNPP
- 추가 안테나 다운링크 구성 - 추가 공공 방송 위성 (Aqua, 및 Terra) 을 위한 안테나 다운링크 구성. SNPP

이 템플릿의 위성에 대한 값과 매개 변수가 이미 채워져 있습니다. 이러한 매개변수를 사용하면 이러한 위성과 함께 즉시 쉽게 사용할 수 있습니다. AWS Ground Station 이 템플릿을 사용할 AWS Ground Station 때는 값을 직접 구성하지 않아도 사용할 수 있습니다. 그러나 사용 사례에 맞게 템플릿을 작동하도록 값을 사용자 지정할 수 있습니다.

내 데이터는 어디에서 수신합니까?

데이터 흐름 엔드포인트 그룹은 템플릿의 일부로 생성되는 수신기 인스턴스 네트워크 인터페이스를 사용하도록 설정됩니다. Receiver 인스턴스는 dataflow 엔드포인트 애플리케이션을 사용하여 dataflow 엔드포인트에서 정의한 포트에서 데이터 스트림을 수신합니다. AWS Ground Station 수신된 데이터는 수신기 인스턴스의 루프백 어댑터에 있는 UDP 포트 50000을 통해 사용할 수 있습니다. 데이터 흐름 엔드포인트 그룹 설정에 대한 자세한 내용은 그룹을 참조하십시오. AWS::GroundStation::DataflowEndpoint

AWS Ground Station 에이전트 (광대역) 를 활용한 공영방송 위성

이 예제는 사용 설명서의 JPSS-1 - 공용 방송 위성 (PBS) - 평가 섹션에서 수행한 분석을 기반으로 합니다.

이 예제를 완료하려면 HRD 통신 경로를 광대역 디지털 중간 주파수 (DiGif) 로 캡처하고 에이전트가 Amazon AWS Ground Station EC2 인스턴스에서 수신한 대로 처리하려는 시나리오를 가정해야 합니다. SDR

> **Note**
>
> 실제 JPSS HRD 통신 경로 신호의 대역폭은 30이지만MHz, 이 예에서는 AWS Ground Station 에이전트가 수신할 올바른 경로를 통해 전달될 수 있도록 안테나-다운링크 구성을 100 MHz 대역폭의 신호로 처리하도록 구성합니다.

통신 경로

이 섹션은 2단계: 데이터 흐름 통신 경로 계획 시작에 대해 설명합니다. 이 예제의 경우 AWS CloudFormation 템플릿에 다른 예제에서 사용되지 않은 추가 섹션인 매핑 섹션이 필요합니다.

> **Note**
>
> 템플릿 내용에 대한 자세한 내용은 AWS CloudFormation 템플릿 섹션을 참조하십시오.

먼저 AWS CloudFormation 템플릿에서 지역별 AWS Ground Station 접두사 목록을 위한 매핑 섹션을 설정해 보겠습니다. 이렇게 하면 Amazon EC2 인스턴스 보안 그룹에서 접두사 목록을 쉽게 참조할 수 있습니다. 접두사 목록 사용에 대한 자세한 내용은 을 참조하십시오. VPC AWS Ground Station 에이전트를 사용한 구성

```
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
```

매개 변수 섹션의 경우 다음 매개 변수를 추가할 것입니다. AWS CloudFormation 콘솔을 통해 스택을 생성할 때 이러한 값을 지정해야 합니다.

```
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**
>
> 키 페어를 생성하고 Amazon EC2 **EC2Key** 파라미터의 이름을 제공해야 합니다. Amazon EC2 인스턴스용 키 페어 생성을 참조하십시오.
> 또한 AWS CloudFormation 스택을 생성할 때 올바른 지역별 AMI ID를 제공해야 합니다. AWS Ground Station 아마존 머신 이미지 (AMIs)을 참조하세요.

나머지 템플릿 스니펫은 템플릿의 AWS CloudFormation 리소스 섹션에 속합니다.

```
Resources:
  # Resources that you would like to create should be placed within the Resources
 section.
```

Amazon EC2 인스턴스에 단일 통신 경로를 전달하는 시나리오를 생각해 보면 동기식 전송 경로가 하나라는 것을 알 수 있습니다. 동기 데이터 전송섹션에 따라 AWS Ground Station Agent를 사용하여 Amazon EC2 인스턴스를 설정 및 구성하고 데이터 흐름 엔드포인트 그룹을 하나 이상 생성해야 합니다. 먼저 AWS Ground Station 에이전트를 VPC 위해 Amazon을 설정해 보겠습니다.

```
  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**
>
> 에이전트가 지원하는 VPC 구성에 대한 자세한 내용은 AWS Ground Station AWS Ground Station 에이전트 요구 사항 - VPC 다이어그램을 참조하십시오.

다음으로 Receiver Amazon EC2 인스턴스를 설정합니다.

```
 # 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
```

또한 계정에 Elastic network interface (ENI) 를 AWS Ground Station 만들려면 적절한 정책, 역할 및 프로필이 필요합니다.

```
 # 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 구성

이 섹션에서는 시작하는 3단계: 구성 생성 방법을 설명합니다.

자동 추적 사용에 대한 기본 설정을 지정하려면 추적 구성이 필요합니다. 자동 추적을 선택하면 PREFERRED신호 품질을 개선할 수 있지만 -1 ephemeris 품질이 충분하기 때문에 신호 품질을 반드시 충족할 필요는 없습니다. JPSS

```
  TrackingConfig:
    Type: AWS::GroundStation::Config
    Properties:
      Name: "JPSS Tracking Config"
      ConfigData:
        TrackingConfig:
          Autotrack: "PREFERRED"
```

통신 경로에 따라 위성 부분을 나타내는 안테나-다운링크 컨피그레이션과 엔드포인트 세부 정보를 정의하는 데이터플로우 엔드포인트 그룹을 참조하는 데이터플로우 엔드포인트 컨피그레이션을 정의해야 합니다.

```
  # 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 미션 프로필

이 섹션은 4단계: 미션 프로필 생성 시작에 대해 설명합니다.

이제 관련 구성이 준비되었으므로 이를 사용하여 데이터 흐름을 구성할 수 있습니다. 나머지 매개변수에는 기본값을 사용하겠습니다.

```
  # 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
```

모두 합치기

위의 리소스를 통해 이제 모든 AWS Ground Station 위치 온보드의 동시 데이터 전송을 위해 JPSS 1-1 개의 연락처를 예약할 수 있습니다.

다음은 이 섹션에 설명된 모든 리소스가 에서 직접 사용할 수 있는 단일 템플릿으로 결합된 완전한 AWS CloudFormation 템플릿입니다. AWS CloudFormation

이름이 지정된 AWS CloudFormation `DirectBroadcastSatelliteWbDigIfEc2DataDelivery.yml` 템플릿은 AquaSNPP, JPSS -1/ NOAA -20 및 Terra 위성에 대한 디지털화된 중간 주파수 (DiGif) 데이터 수신을 빠르게 시작할 수 있도록 설계되었습니다. Amazon EC2 인스턴스와 에이전트를 사용하여 AWS Ground Station 원본 DiGif 다이렉트 브로드캐스트 데이터를 수신하는 데 필요한 AWS CloudFormation 리소스가 포함되어 있습니다.

AquaSNPP, JPSS -1/ NOAA -20 및 Terra가 계정에 온보딩되지 않은 경우 을 참조하십시오. 1단계: 새틀라이트 온보딩

> **Note**
>
> 고객 온보딩 Amazon S3 버킷에 액세스하여 템플릿에 액세스할 수 있습니다. 아래 링크는 리전 Amazon S3 버킷을 사용합니다. AWS CloudFormation 스택을 생성하려는 해당 지역을 나타내도록 지역 코드를 변경하십시오. `us-west-2`
> 또한 다음 지침에서도 사용합니다YAML. 그러나 템플릿은 두 가지 JSON 형식 YAML 모두에서 사용할 수 있습니다. 사용하려면 JSON 템플릿을 다운로드할 `.json` 때 `.yml` 파일 확장자를 로 바꾸십시오.

를 사용하여 AWS CLI템플릿을 다운로드하려면 다음 명령을 사용합니다.

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

브라우저에서 다음으로 이동하여 콘솔에서 템플릿을 보고 다운로드할 수 있습니다. URL

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

다음 링크를 AWS CloudFormation 사용하여 템플릿을 직접 지정할 수 있습니다.

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

템플릿은 어떤 추가 리소스를 정의합니까?

`DirectBroadcastSatelliteWbDigIfEc2DataDelivery`템플릿에는 다음과 같은 추가 리소스가 포함됩니다.

- Receiver 인스턴스 엘라스틱 네트워크 인터페이스 - (조건부) 제공된 PublicSubnetId경우 에서 지정한 서브넷에 엘라스틱 네트워크 인터페이스가 생성됩니다. 이는 수신기 인스턴스가 프라이빗 서브넷에 있는 경우 필요합니다. Elastic network 인터페이스는 수신자 인스턴스와 EIP 연결되고 수신자 인스턴스에 연결됩니다.
- 수신기 인스턴스 엘라스틱 IP - 연결할 엘라스틱 IP입니다. AWS Ground Station 이는 수신기 인스턴스 또는 Elastic Network 인터페이스에 연결됩니다.
- 다음 엘라스틱 IP 연결 중 하나:
  - 수신기 인스턴스와 엘라스틱 IP 연결 - 엘라스틱 IP와 수신기 인스턴스의 연결 (PublicSubnetId지정되지 않은 경우). 이를 위해서는 퍼블릭 서브넷을 SubnetId참조해야 합니다.
  - Receiver 인스턴스 엘라스틱 네트워크 인터페이스와 엘라스틱 IP 연결 - 엘라스틱 IP를 수신기 인스턴스 엘라스틱 네트워크 인터페이스에 연결하는 것입니다 (지정된 경우 PublicSubnetId).
- (선택 사항) CloudWatch 이벤트 트리거 - 연락 AWS Ground Station 전후에 전송된 CloudWatch 이벤트를 사용하여 트리거되는 AWS Lambda 함수입니다. AWS Lambda 함수는 Receiver 인스턴스를 시작하고 선택적으로 중지합니다.
- (선택 사항) Amazon 연락처 EC2 확인 - Lambda를 사용하여 알림이 있는 연락처에 대해 EC2 Amazon 인스턴스의 확인 시스템을 설정하는 옵션입니다. SNS 이때 현재 사용량에 따라 요금이 부과될 수 있다는 점에 유의하세요.

- 추가 임무 프로필 - 추가 공공 방송 위성 (Aqua, SNPP Terra) 의 임무 프로필.
- 추가 안테나 다운링크 구성 - 추가 공공 방송 위성 (Aqua, 및 Terra) 을 위한 안테나 다운링크 구성. SNPP

이 템플릿의 위성에 대한 값과 매개 변수가 이미 채워져 있습니다. 이러한 매개변수를 사용하면 이러한 위성과 함께 즉시 쉽게 사용할 수 있습니다. AWS Ground Station 이 템플릿을 사용할 AWS Ground Station 때는 값을 직접 구성하지 않아도 사용할 수 있습니다. 그러나 사용 사례에 맞게 템플릿을 작동하도록 값을 사용자 지정할 수 있습니다.

내 데이터는 어디에서 수신합니까?

데이터 흐름 엔드포인트 그룹은 템플릿의 일부로 생성되는 수신기 인스턴스 네트워크 인터페이스를 사용하도록 설정됩니다. Receiver 인스턴스는 AWS Ground Station 에이전트를 사용하여 dataflow AWS Ground Station 엔드포인트에서 정의한 포트에서 데이터 스트림을 수신합니다. 데이터 흐름 엔드포인트 그룹 설정에 대한 자세한 내용은 그룹을 참조하십시오. AWS::GroundStation::DataflowEndpoint AWS Ground Station 에이전트에 대한 자세한 내용은 에이전트란? 을 AWS Ground Station 참조하십시오.

문제 해결

다음 설명서는 사용 중에 발생할 수 있는 문제를 해결하는 데 도움이 될 수 있습니다. AWS Ground Station

주제

Amazon으로 데이터를 전송하는 연락처 문제 해결 EC2

AWS Ground Station 연락을 성공적으로 완료할 수 없는 경우 Amazon EC2 인스턴스가 실행 중인지, 데이터 흐름 엔드포인트 애플리케이션이 실행 중인지, 데이터 흐름 엔드포인트 애플리케이션의 스트림이 제대로 구성되어 있는지 확인해야 합니다.

> **Note**
>
> DataDefender (DDX) 는 에서 현재 지원하는 데이터 흐름 엔드포인트 애플리케이션의 한 예입니다. AWS Ground Station

사전 조건

다음 절차에서는 Amazon EC2 인스턴스가 이미 설정되어 있다고 가정합니다. 에서 AWS Ground Station Amazon EC2 인스턴스를 설정하려면 시작하기를 참조하십시오.

1단계: EC2 인스턴스가 실행 중인지 확인

1. 문제 해결 중인 연락처에 사용된 Amazon EC2 인스턴스를 찾으십시오. 다음 단계를 사용합니다.
   a. AWS CloudFormation대시보드에서 Amazon EC2 인스턴스가 포함된 스택을 선택합니다.

b. 리소스 탭을 선택하고 논리 ID 열에서 Amazon EC2 인스턴스를 찾습니다. 인스턴스가 상태 열에 생성되었는지 확인합니다.

c. 물리적 ID 열에서 Amazon EC2 인스턴스의 링크를 선택합니다. 그러면 Amazon EC2 관리 콘솔로 이동합니다.

2. Amazon EC2 관리 콘솔에서 Amazon EC2 인스턴스 상태가 실행 중인지 확인합니다.

3. 인스턴스가 실행 중이면 다음 단계로 계속합니다. 인스턴스가 실행 중이 아니면 다음 단계를 사용하여 인스턴스를 시작합니다.

   - Amazon EC2 인스턴스를 선택한 상태에서 [작업] > [인스턴스 상태] > [시작] 을 선택합니다.

2단계: 사용되는 데이터 흐름 애플리케이션 유형 결정

에이전트를 데이터 전송에 사용하는 경우 AWS Ground Station 에이전트 문제 해결 섹션으로 리디렉션하십시오. AWS Ground Station 그렇지 않으면 DataDefender (DDX) 응용 프로그램을 사용하는 경우 계속 the section called “3단계: 데이터 흐름 애플리케이션이 실행 중인지 확인” 진행하십시오.

3단계: 데이터 흐름 애플리케이션이 실행 중인지 확인

상태를 확인하려면 EC2 Amazon의 DataDefender 인스턴스에 연결해야 합니다. 인스턴스 연결에 대한 자세한 내용은 Linux 인스턴스에 연결을 참조하십시오.

다음 절차는 SSH 클라이언트에서 명령을 사용하는 문제 해결 단계를 제공합니다.

1. 터미널 또는 명령 프롬프트를 열고 를 사용하여 Amazon EC2 인스턴스에 연결합니다SSH. DataDefender 웹 UI를 보려면 원격 호스트의 포트 80을 전달하십시오. 다음 명령은 포트 포워딩이 활성화된 EC2 배스천을 통해 Amazon 인스턴스에 SSH 연결하는 방법을 보여줍니다.

   > **Note**
   >
   > < SSH KEY >, < > 및 < BASTION HOST HOST >를 특정 ssh 키, 배스천 호스트 이름 및 Amazon EC2 인스턴스 호스트 이름으로 바꿔야 합니다.

   Windows의 경우

   ```
   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>
   ```

Mac의 경우

```
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. 출력에서 ddx라는 DDX 실행 중인 프로세스를 확인 (확인) 하여 실행 중인지 확인하십시오. DataDefender 실행 중인 프로세스를 검사하는 명령과 성공적인 예제 출력은 다음과 같습니다.

```
[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
```

실행 DataDefender 중이면 the section called “4단계: 데이터 흐름 애플리케이션 스트림이 구성되어 있는지 확인” 그렇지 않음으로 건너뛰고 다음 단계로 진행하십시오.

3. 아래 show 명령을 DataDefender 사용해 시작하십시오.

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

명령을 사용한 후 실행 DataDefender 중인 경우 the section called “4단계: 데이터 흐름 애플리케이션 스트림이 구성되어 있는지 확인” 다른 방법으로 건너뛰고 다음 단계로 진행하십시오.

4. 아래 명령을 사용하여 다음 파일을 검사하여 설치 및 구성 DataDefender 중에 오류가 발생했는지 확인하십시오.

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

> **Note**
>
> 이러한 파일을 검사할 때 발견되는 일반적인 문제는 Amazon VPC EC2 인스턴스가 실행되는 Amazon이 설치 파일을 다운로드할 수 있는 Amazon S3에 액세스할 수 없다는 것입니다. 로그에서 이러한 문제가 발견되면 EC2 인스턴스의 Amazon VPC 및 보안 그룹 설정이 Amazon S3에 대한 액세스를 차단하고 있지 않은지 확인하십시오.

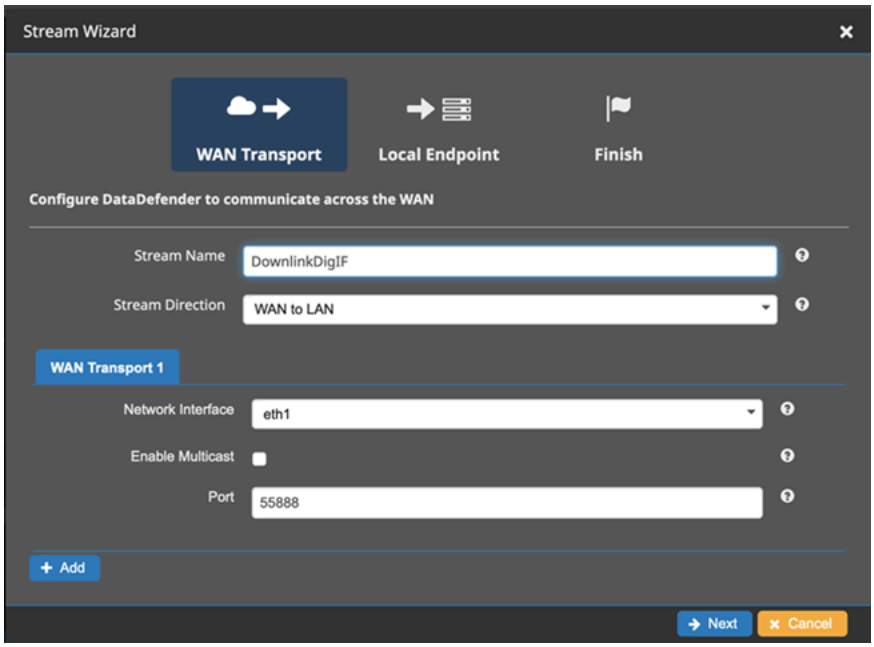
Amazon VPC 설정을 확인한 후 실행 DataDefender 중인 경우 계속 진행하십시오the section called “4단계: 데이터 흐름 애플리케이션 스트림이 구성되어 있는지 확인”. 문제가 지속되면 AWSSupport에 문의하여 문제에 대한 설명이 포함된 로그 파일을 보내십시오.

4단계: 데이터 흐름 애플리케이션 스트림이 구성되어 있는지 확인

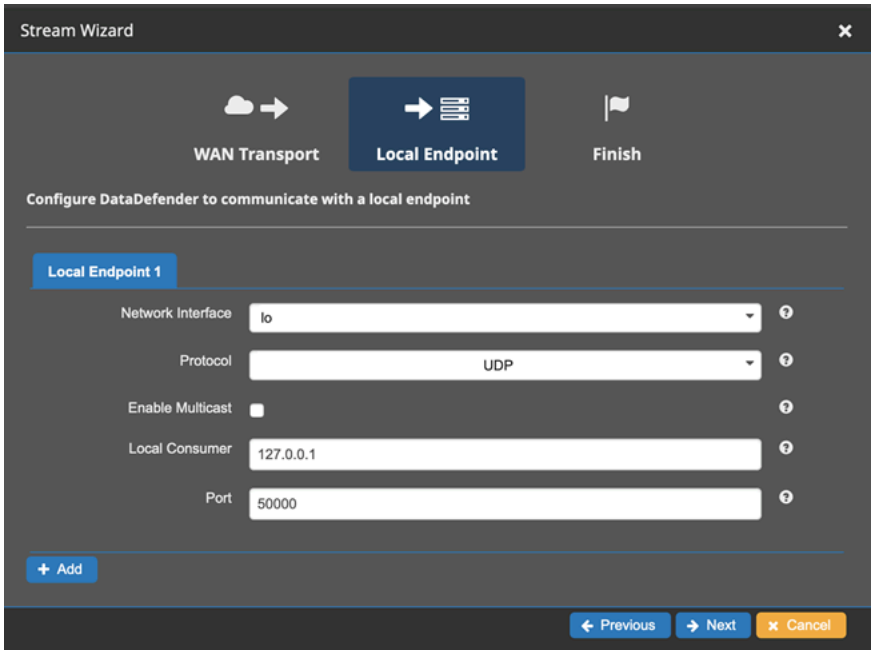
1. 웹 브라우저에서 주소 표시줄에 localhost:8080 주소를 입력하여 DataDefender 웹 사용자 인터페이스에 액세스합니다. 그런 다음 Enter 키를 누릅니다.
2. DataDefender대시보드에서 세부 정보로 이동을 선택합니다.
3. 스트림 목록에서 스트림을 선택하고 스트림 편집을 선택합니다.
4. 스트림 마법사 대화 상자에서 다음을 수행합니다.

   a. WAN전송 패널에서 스트림 방향으로 WAN LAN to가 선택되어 있는지 확인합니다.

   b. 포트 상자에 데이터 흐름 엔드포인트 그룹에 대해 선택한 포트가 있는지 확인합니다. WAN 기본적으로 이 포트는 55888입니다. 그리고 다음을 선택합니다.



   c. 로컬 엔드포인트 창에서 포트 상자에 올바른 포트가 표시되는지 확인합니다. 기본적으로 이 포트는 50000입니다. 이 포트는 서비스로부터 데이터를 수신한 후 DataDefender 데이터를 수신하게 될 포트입니다. AWS Ground Station 그리고 다음을 선택합니다.



d. 값을 변경한 경우 나머지 메뉴에서 완료를 선택합니다. 그렇지 않으면 스트림 마법사 메뉴를 취소할 수 있습니다.

이제 Amazon EC2 인스턴스와 S가 모두 제대로 DataDefender 실행되고 있으며 에서 AWS Ground Station데이터를 수신하도록 구성되어 있는지 확인했습니다. 문제가 계속 발생하는 경우 AWSSupport에 문의하세요.

FAILED연락처 문제 해결

연락처의 터미널 연락처 상태는 리소스 구성과 관련된 문제를 AWS Ground Station 감지한 FAILED시점입니다. FAILED문의가 발생할 수 있는 일반적인 사용 사례와 문제 해결에 도움이 되는 단계가 아래에 나와 있습니다.

> **Note**
>
> 이 가이드는 특히 FAILED연락처 상태를 위한 것으로 AWS_ FAILEDCANCELLED, AWS_ 또는 FAILED _TO_와 같은 다른 장애 상태에는 해당되지 않습니다. SCHEDULE 연락 상태에 대한 자세한 설명은 the section called “AWS Ground Station 연락처 상태” 섹션을 참조하십시오.

데이터플로우 엔드포인트 사용 사례 FAILED

다음은 데이터 흐름 엔드포인트 기반 데이터 흐름에 대한 FAILED연락처 상태로 이어질 수 있는 일반적인 사용 사례 목록입니다.

- Dataflow 엔드포인트가 연결되지 않음 - 하나 이상의 데이터 플로우에 대한 AWS Ground Station 안테나와 Dataflow 엔드포인트 그룹 간의 연결이 설정되지 않았습니다.
- Dataflow 엔드포인트가 늦게 연결됨 - 연결 시작 시간 이후에 하나 이상의 데이터 플로우에 대한 AWS Ground Station 안테나와 Dataflow 엔드포인트 그룹 간의 연결이 설정되었습니다.

모든 데이터 흐름 엔드포인트 장애 사례의 경우 다음을 살펴보는 것이 좋습니다.

- 연락 시작 시간 전에 수신자 Amazon EC2 인스턴스가 성공적으로 시작되었는지 확인합니다.
- 문의하는 동안 데이터 흐름 엔드포인트 소프트웨어가 가동되어 실행 중인지 확인하십시오.

자세한 문제 해결 단계는 Amazon으로 데이터를 전송하는 연락처 문제 해결 EC2 관련 섹션을 참조하십시오.

AWS Ground Station 상담원 사용 사례 FAILED

다음은 에이전트 기반 데이터 흐름의 FAILED연락처 상태를 초래할 수 있는 일반적인 사용 사례 목록입니다.

- AWS Ground Station 상담원이 보고되지 않음 상태 - 상태가 제대로 보고되지 않은 하나 이상의 데이터 흐름에 대해 Dataflow 엔드포인트 그룹에서 데이터 전달을 조율하는 역할을 담당하는 에이전트입니다. AWS Ground Station이 상태 업데이트는 연락 종료 시간으로부터 몇 초 이내에 이루어져야 합니다.
- AWS Ground Station 에이전트가 늦게 시작됨 - 하나 이상의 데이터 플로우에 대해 Dataflow Endpoint Group에서 데이터 전송을 조율하는 역할을 담당하는 에이전트가 연락 시작 시간 이후 늦게 시작되었습니다.

모든 AWS Ground Station 에이전트 데이터 흐름 실패 사례의 경우 다음을 살펴보는 것이 좋습니다.

- 연락 시작 시간 전에 수신자 Amazon EC2 인스턴스가 성공적으로 시작되었는지 확인합니다.
- 시작 시점과 연락 중에 에이전트 애플리케이션이 가동되어 실행 중인지 확인하십시오.

- 문의 종료 후 15초 이내에 에이전트 애플리케이션과 Amazon EC2 인스턴스가 종료되지 않았는지 확인합니다. 이렇게 하면 에이전트가 AWS Ground Station에 상태를 보고할 충분한 시간을 확보할 수 있습니다.

자세한 문제 해결 단계는 Amazon으로 데이터를 전송하는 연락처 문제 해결 EC2 관련 섹션을 참조하십시오.

FAILED_TO_ 연락처 SCHEDULE 문제 해결

리소스 구성 또는 내부 시스템 내에서 문제가 AWS Ground Station 감지되면 연락처는 FAILED_TO_ SCHEDULE 상태로 종료됩니다. FAILED_TO_ SCHEDULE 상태로 끝나는 연락처는 선택적으로 추가 컨텍스트를 제공합니다. `errorMessage` 연락처 설명에 대한 자세한 내용은 를 참조하십시오. DescribeContactAPI

FAILED_TO_ SCHEDULE 문의가 발생할 수 있는 일반적인 사용 사례가 문제 해결에 도움이 되는 단계와 함께 아래에 나와 있습니다.

> **Note**
>
> 이 가이드는 FAILED_TO_ SCHEDULE 연락처 상태를 위한 것으로, _, _ 등과 같은 AWS 다른 장애 상태에는 해당되지 않습니다. FAILED AWS CANCELLED FAILED 연락 상태에 대한 자세한 설명은 the section called “AWS Ground Station 연락처 상태” 섹션을 참조하십시오.

안테나 다운링크 Demod 디코드 컨피그레이션에 지정된 설정은 지원되지 않습니다.

이 연락을 예약하는 데 사용된 임무 프로필의 antenna-downlink-demod-decode 구성이 유효하지 않았습니다.

이전의 기존 구성 AntennaDownlinkDemodDecode

- antenna-downlink-demod-decode 구성이 최근에 변경된 경우 일정을 잡기 전에 이전에 작동하던 버전으로 롤백하세요.
- 기존 구성을 의도적으로 변경했거나 기존 구성이 더 이상 일정에 맞지 않는 경우, 새 구성을 온보딩하는 방법에 대한 다음 단계를 따르세요. AntennaDownlinkDemodDecode

새로 AntennaDownlinkDemodDecode 생성된 구성

새 구성을 온보딩하려면 AWS Ground Station 직접 문의하세요. FAILED_TO_ SCHEDULE 상태로 `contactId` 종료된 사례를 포함하여 AWSSupport에 사례 생성

일반 문제 해결 단계

위의 문제 해결 단계로도 문제가 해결되지 않은 경우:

- 연락 일정을 다시 잡거나 동일한 임무 프로필을 사용하여 다른 연락을 예약해 보십시오. 연락처 예약 방법에 대한 자세한 내용은 을 참조하십시오. ReserveContact
- 이 임무 프로필에 대해 FAILED_TO_ SCHEDULE 등급을 계속 받으면 Support에 문의하세요. AWS

HEALTHY상태가 DataflowEndpointGroups 아닌 문제 해결

다음은 데이터 흐름 엔드포인트 그룹이 특정 `HEALTHY` 상태에 있지 않을 수 있는 이유와 취해야 할 적절한 수정 조치입니다.

- `NO_REGISTERED_AGENT`- EC2 인스턴스를 시작하면 에이전트가 등록됩니다. 단, 이 직접적 호출이 성공하려면 유효한 컨트롤러 구성 파일이 있어야 합니다. 해당 파일 구성에 AWS Ground Station 대리인 대한 자세한 내용은 를 참조하세요.
- `INVALID_IP_OWNERSHIP`- DeleteDataflowEndpointGroup API 를 사용하여 Dataflow 엔드포인트 그룹을 삭제한 다음 를 사용하여 인스턴스와 연결된 IP 주소 및 포트를 사용하여 Dataflow 엔드포인트 그룹을 다시 생성합니다. CreateDataflowEndpointGroup API EC2
- `UNVERIFIED_IP_OWNERSHIP` - IP 주소는 아직 검증되지 않았습니다. 검증은 주기적으로 이루어지므로 이 문제는 저절로 해결될 것입니다.
- `NOT_AUTHORIZED_TO_CREATE_SLR` - 계정에 필요한 서비스 연결 역할을 생성할 권한이 없습니다. Ground Station에 서비스 연결 역할 사용에서 문제 해결 단계를 확인하세요

잘못된 에페메리데스 문제 해결

사용자 지정 에페메리스가 업로드되면 비동기 검증 AWS Ground Station 워크플로우를 거쳐 업로드됩니다. `ENABLED` 이 워크플로는 위성 식별자, 메타데이터 및 궤적이 유효한지 확인합니다.

에페메리스가 검증에 실패하면 에페메리스가 검증에 실패한 이유를 파악할 수 있는 a가 `DescribeEphemeris` EphemerisInvalidReason반환됩니다. 의 잠재적 값은 다음과 같습니다. EphemerisInvalidReason

값	설명	작업 문제 해결
METADATA_INVALID	제공된 우주선 식별자(예: 위성 ID)가 유효하지 않습니다	ephemeris 데이터에 제공된 NORAD ID 또는 기타 식별자를 확인하십시오.
TIME_RANGE_INVALID	제공된 에페메리스의 시작, 종료 또는 만료 시간이 유효하지 않습니다	시작 시간은 '지금' 이전이고(시작 시간은 몇 분 전으로 설정하는 것이 좋습니다), 종료 시간은 시작 시간 이후이고, 종료 시간은 만료 시간 이후여야 합니다
TRAJECTORY_INVALID	에페메리스가 유효하지 않은 우주선 궤적을 정의하는 경우	제공된 궤적이 연속적이고 올바른 위성을 위한 궤적인지 확인하세요.
VALIDATION_ERROR	검증을 위해 임시 항목을 처리하는 동안 내부 서비스 오류가 발생했습니다	업로드 재시도

아래는 `INVALID` 에페메리스에 대한 `DescribeEphemeris` 응답 예시입니다.

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

```
  },
}
```

> **Note**
>
> 에페머리스 상태인 경우 해당 에페머리스는 ERROR 서비스에 문제가 있기 때문이 아닙니다. ENABLED AWS Ground Station 를 통해 에페머리스 제공을 다시 시도해야 합니다. CreateEphemeris 문제가 일시적일 ENABLED 경우 새로운 이피머스가 발생할 수 있습니다.

데이터를 받지 못한 연락처 문제 해결

연락처가 성공한 것처럼 보이지만 여전히 데이터를 받지 못했을 수 있습니다. 즉, S3 데이터 전송을 사용하는 경우 비어 있는 PCAP PCAP 파일을 받거나 파일이 전혀 수신되지 않을 수 있습니다. 이는 여러 이유로 발생할 수 있습니다. 다음은 몇 가지 원인과 해결 방법을 설명합니다.

잘못된 다운링크 구성

위성으로부터 데이터를 수신하는 각 연락처에는 관련 안테나 다운링크 구성 또는 정보가 있습니다. 안테나 다운링크 복조 디코드 구성 지정된 구성이 위성이 전송하는 신호와 일치하지 않는 경우 전송된 신호를 수신할 수 없습니다. AWS Ground Station 그러면 에서 데이터를 수신할 수 없게 됩니다 AWS Ground Station.

이 문제를 해결하려면 사용 중인 구성이 위성이 전송하는 신호와 일치하는지 확인하십시오. 예를 들어, 중앙 주파수, 대역폭, 편파, 필요한 경우 복조 및 디코딩 파라미터를 올바르게 설정했는지 확인하십시오.

위성 기동

위성이 일부 통신 시스템을 일시적으로 비활성화하는 기동을 수행할 수 있는 경우가 있습니다. 이 기동으로 인해 하늘에서 위성의 위치가 크게 바뀔 수도 있습니다. AWS Ground Station 신호를 전송하지 않는 위성으로부터 신호를 수신할 수 없거나, 사용 중인 에페머리스로 인해 AWS Ground Station 안테나가 하늘에서 위성이 없는 위치를 가리키는 경우 신호를 수신할 수 없습니다.

에서 운영하는 NOAA 공공 방송 위성과 통신하려는 경우 위성 경보 메시지 페이지에서 정전 또는 기동을 설명하는 메시지를 찾을 수 있습니다. NOAA 메시지에는 데이터 전송 재개 예상 일정이 포함되거나 후속 메시지에 게시될 수 있습니다.

자체 위성과 통신하는 경우 위성 작동 방식과 이것이 통신에 미치는 영향을 이해하는 것은 귀하의 책임입니다. AWS Ground Station위성 궤적에 영향을 미치는 기동을 수행하는 경우 업데이트된 사용자 지정 임시 데이터 제공이 포함될 수 있습니다. 사용자 지정 임시 데이터 제공에 대한 자세한 내용은 을 참조하십시오. 맞춤형 에페메리스 데이터 제공

AWS Ground Station 정전

연락이 AWS Ground Station 실패하거나 AWS Ground Station 취소되면 연락처 상태가 AWS_ 또는 FAILED AWS _로 설정됩니다. CANCELLED 연락처 수명 주기에 대한 자세한 내용은 을 참조하십시오연락처 라이프사이클. 경우에 따라 데이터가 계정에 전달되지 않지만 연락처가 AWS_ FAILED 또는 AWS_ CANCELLED 상태가 되지 않는 오류가 발생할 수 있습니다. AWS Ground Station 이 경우 AWS Health 대시보드에 계정별 이벤트를 AWS Ground Station 게시해야 합니다. AWS Health 대시보드에 대한 자세한 내용은 AWS Health 사용 설명서를 참조하십시오.

할당량 및 제한

지원되는 지역, 관련 엔드포인트, 엔드포인트 및 할당량의 할당량을 볼 수 있습니다.AWS Ground Station

필요한 경우 Service Quotas 콘솔을 사용하여 할당량 증가를 요청할 수 있습니다. AWS APIAWS CLI

서비스 약관

AWS Ground Station 서비스 약관은 서비스 약관을 AWS 참조하십시오.

AWS Ground Station 사용자 안내서의 문서 기록

다음 표에는 AWS Ground Station 사용 설명서의 각 릴리스에서 변경된 주요 내용이 설명되어 있습니다.

변경 사항	설명	날짜
새 기능	AWS Ground Station 디지털 트윈을 포함하도록 사용자 안내서를 업데이트했습니다.	2024년 8월 6일
설명서 업데이트	새 다이어그램, 예제 등을 포함하여 사용 설명서의 여러 섹션이 업데이트되었습니다.	2024년 7월 18일
설명서 업데이트	사용 설명서에 RSS 피드가 추가되었습니다.	2024년 7월 18일
문서 업데이트	AWS Ground Station 에이전트 사용 설명서를 별도의 사용 설명서로 분할하십시오.	2024년 7월 18일
새 기능	이제 가시성 시간 범위 밖에서 최대 30초까지 연락처를 예약할 수 있습니다. 가시성 시간은 DescribeContact 응답에 포함됩니다.	2024년 3월 26일
문서 업데이트	구성이 개선되고 “EC2인스턴스 선택 및 CPU 계획” 섹션이 추가되었습니다.	2024년 3월 6일
설명서 업데이트	에이전트와 함께 서비스 및 프로세스를 실행하기 위한 새로운 모범 사례를 AWS Ground Station AWS Ground Station 에이전트 사용 설명서에 추가했습니다.	2024년 2월 23일

설명서 업데이트	에이전트 릴리스 노트 페이지가 추가되었습니다.	2024년 2월 21일
템플릿 업데이트	DirectBroadcastSatelliteWbDigIfEc2 DataDelivery 템플릿에 별도의 퍼블릭 서브넷에 대한 지원이 추가되었습니다.	2024년 2월 14일
설명서 업데이트	모니터링 AWS 사용자 알림 문서에 참조를 추가했습니다.	2023년 8월 6일
설명서 업데이트	콘솔에 표시할 이름을 위성에 태깅하기 위한 지침이 추가되었습니다. AWS Ground Station	2023년 7월 26일
새 기능	광대역 DiGif 데이터 전송 릴리스를 위한 AWS Ground Station 에이전트 사용 설명서가 추가되었습니다.	2023년 8월 12일
새 관리형 정책 AWS	AWS Ground Station 라는 새 정책을 추가했습니다 AWSGroundStationAgentInstancePolicy.	2023년 8월 12일
새 기능	CPEPreview 릴리스를 위한 사용 설명서가 업데이트되었습니다.	2022년 11월 9일
새 AWS 관리형 정책	AWS Ground Station 라는 새 정책이 포함된 AWSServiceRoleForGroundStationDataflowEndpointGroup service-linked-role (SLR) 가 추가되었습니다 AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy.	2022년 11월 2일

새 기능	와의 통합을 포함하도록 사용 설명서를 AWS CLI업데이트했습니다.	2020년 4월 17일
새 기능	CloudWatch Metrics와의 통합을 포함하도록 사용 설명서를 업데이트했습니다.	2020년 2월 24일
새 템플릿	공용 방송 위성 (AquaSnpp Jpss 템플릿) 이 AWS Ground Station 사용 설명서에 추가되었습니다.	2020년 2월 19일
새 기능	교차 리전 데이터 전송을 포함하도록 사용 설명서가 업데이트되었습니다.	2020년 2월 5일
문서 업데이트	CloudWatch 이벤트 AWS Ground Station 모니터링에 대한 예제와 설명이 업데이트되었습니다.	2020년 2월 4일
설명서 업데이트	템플릿 위치가 업데이트되었으며, 시작하기 및 문제 해결 섹션이 수정되었습니다.	2019년 12월 19일
새 문제 해결 섹션	문제 해결 섹션이 에 추가되었습니다.	2019년 11월 7일
새 시작 주제	최신 AWS CloudFormation 템플릿이 포함된 시작하기 항목이 업데이트되었습니다.	2019년 7월 1일
킨들 버전	AWS Ground Station 사용 설명서의 공개된 Kindle 버전입니다.	2019년 6월 20일

새로운 서비스 및 가이드	이 버전은 의 첫 번째 AWS Ground Station 릴리스이자 AWS Ground Station 사용 설명서입니다.	2019년 5월 23일

AWS 용어집

최신 AWS 용어는 AWS 용어집 참조서의 AWS 용어집을 참조하세요.

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.