Guide de l’utilisateur

AWS Ground Station

AWS Ground Station: Guide de l’utilisateur

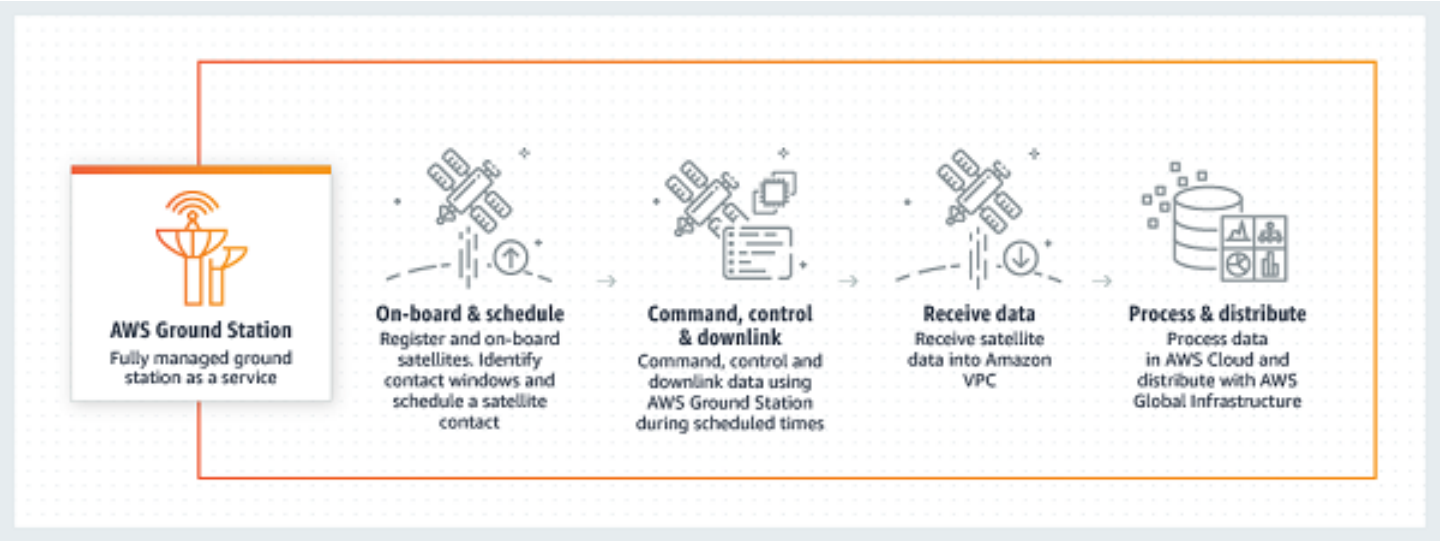
Table of Contents

Qu'est-ce que c'est AWS Ground Station ?

AWS Ground Station est un service entièrement géré qui fournit des communications par satellite sécurisées, rapides et prévisibles au sein d'une infrastructure mondiale. Ainsi AWS Ground Station, vous n'avez plus besoin de construire, de gérer ou de faire évoluer votre propre infrastructure de station au sol. AWS Ground Station vous permet de vous concentrer sur l'innovation et d'expérimenter rapidement de nouvelles applications qui ingèrent des données satellites, plutôt que de consacrer des ressources à la construction, à l'exploitation et à la mise à l'échelle de vos propres stations au sol.

Grâce au réseau mondial AWS de fibre optique à faible latence et à large bande passante, vous pouvez commencer à traiter vos données satellites quelques secondes après réception par le système d'antenne. Cela vous permet de transformer les données brutes en informations traitées ou en connaissances analysées en quelques secondes.

Cas d'utilisation courants



AWS Ground Station vous permet de communiquer avec vos satellites de manière bidirectionnelle et prend en charge les cas d'utilisation suivants :

- Données en liaison descendante : recevez des données de vos satellites, en transmettant des fréquences en bande X et en bande S, transmises à une EC2 instance Amazon en temps réel (format VITA -49) ou directement vers un compartiment Amazon S3 de votre compte (format). PCAP En outre, pour les satellites qui utilisent un schéma de modulation et de codage pris

en charge, vous pouvez choisir entre recevoir des données démodulées et décodées ou des échantillons bruts de fréquence intermédiaire numérique (DigIF) (format -49). VITA

- Données en liaison montante : envoyez des données et des commandes à vos satellites recevant des fréquences en bande S en envoyant des données DigIF (format VITA -49) à transmettre par. AWS Ground Station
- Echo Uplink : validez les commandes envoyées à votre vaisseau spatial et effectuez d'autres tâches avancées en recevant le signal transmis sur une antenne physiquement colocalisée.
- Radio définie par logiciel (SDR) /processeur frontal (FEP) — Utilisez votre processeur existant SDR et/ou FEP capable de fonctionner sur une EC2 instance Amazon pour traiter vos données en temps réel afin d'envoyer/recevoir vos formes d'onde existantes et de générer vos produits de données.
- Télémétrie, suivi et commande (TT&C) — Effectuez le TT&C en utilisant une combinaison des cas d'utilisation répertoriés précédemment pour gérer votre flotte de satellites.
- Livraison de données entre régions — Gérez plusieurs contacts simultanés à l'aide AWS Ground Station du réseau d'antennes mondial d'une seule AWS région.
- Jumeau numérique — Planification des tests, vérification des configurations et gestion appropriée des erreurs à un coût réduit sans utiliser la capacité de production de l'antenne.

Étapes suivantes

Nous vous recommandons de commencer par lire les sections suivantes :

- Pour en savoir plus sur AWS Ground Station les concepts essentiels, voirComment AWS Ground Station fonctionne.
- Pour savoir comment configurer votre compte et les ressources à utiliser AWS Ground Station, consultezMise en route.
- Pour une utilisation par programmation AWS Ground Station, veuillez vous référer à la AWS Ground Station API référence. La API référence décrit AWS Ground Station en détail toutes les API opérations. Il fournit également des exemples de demandes, de réponses et d'erreurs pour les protocoles de service Web pris en charge. Vous pouvez utiliser le AWS CLI, ou un AWS SDK, dans le langage de votre choix, pour écrire du code qui interagit avec AWS Ground Station.

Comment AWS Ground Station fonctionne

AWS Ground Station utilise des antennes au sol pour faciliter la communication avec votre satellite. Les caractéristiques physiques de ce que les antennes peuvent faire sont abstraites et sont appelées capacités. L'emplacement physique de l'antenne ainsi que ses capacités actuelles peuvent être référencés dans Emplacements cette section. Veuillez nous contacter à l'<adresse aws-groundstation@amazon.com> si votre cas d'utilisation nécessite des fonctionnalités supplémentaires, des offres de localisation supplémentaires ou des emplacements d'antennes plus précis.

Pour utiliser l'une des AWS Ground Station antennes, vous devez réserver une heure à un endroit précis. Cette réservation est considérée comme un contact. Pour planifier un contact avec succès, AWS Ground Station des données supplémentaires sont nécessaires pour garantir son succès.

- Votre satellite doit être embarqué sur un ou plusieurs sites. Cela garantit que vous êtes autorisé à utiliser les différentes capacités à l'endroit demandé.
- Votre satellite doit avoir une éphéméride valide. Cela garantit que les antennes ont une ligne de visée et peuvent pointer avec précision votre satellite pendant le contact.
- Vous devez avoir un profil de mission valide. Cela vous permet de personnaliser le comportement de ce contact, notamment la manière dont vous recevrez et enverrez des données à votre satellite. Vous pouvez utiliser plusieurs profils de mission pour le même véhicule afin de créer différents contacts adaptés aux différentes postures opérationnelles ou aux différents scénarios que vous rencontrez.

Intégration par satellite

L'intégration d'un satellite AWS Ground Station est un processus en plusieurs étapes impliquant la collecte de données, la validation technique, l'octroi de licences de spectre, ainsi que l'intégration et les tests. La section du guide consacrée à l'intégration par satellite vous guidera tout au long de ce processus.

Composition du profil de mission

Les informations de fréquence du satellite, les informations du plan de données et d'autres détails sont encapsulés dans un profil de mission. Le profil de mission est un ensemble de composants de

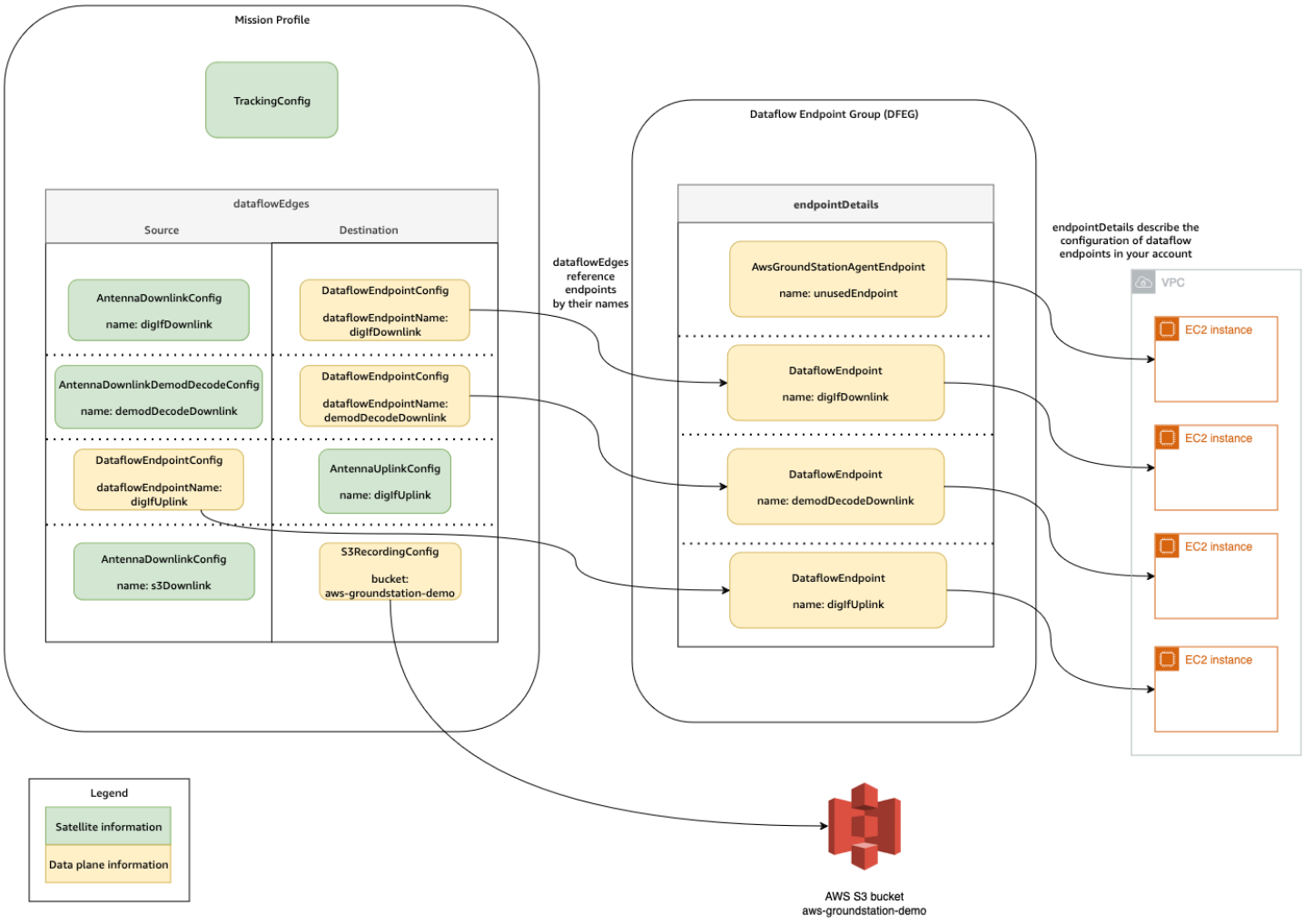
configuration. Cela vous permet de réutiliser les composants de configuration dans différents profils de mission en fonction de votre cas d'utilisation. Étant donné que les profils de mission ne font pas directement référence à des satellites individuels, mais contiennent uniquement des informations sur leurs capacités techniques, les profils de mission peuvent également être réutilisés par plusieurs satellites ayant la même configuration.

Un profil de mission valide comportera une configuration de suivi et un ou plusieurs flux de données. La configuration de suivi indiquera vos préférences en matière de suivi lors d'un contact. Chaque paire de configurations au sein d'un flux de données établit une source et une destination. En fonction de votre satellite et de ses modes de fonctionnement, le nombre exact de flux de données variera dans le profil de mission pour représenter vos voies de communication montantes et descendantes ainsi que les éventuels aspects liés au traitement des données.

- Pour plus d'informations sur la configuration de vos EC2 ressources AmazonVPC, Amazon S3 et Amazon qui seront utilisées lors d'un contact, consultezFlux de données.
- Pour plus de détails sur le comportement de chaque configuration, consultezConfig.
- Pour plus de détails sur tous les paramètres attendus, voirProfil de mission.
- Pour des exemples sur la manière dont différents profils de mission peuvent être créés pour répondre à votre cas d'utilisation, consultezExemples de configurations de profil de mission.

Le schéma ci-dessous est utilisé pour montrer un exemple de profil de mission et les ressources supplémentaires nécessaires. Notez que l'exemple montre un point de terminaison de flux de données qui n'est pas nécessaire pour ce profil de mission, nommé unusedEndpoint, afin de démontrer la flexibilité. L'exemple prend en charge les flux de données suivants :

- Liaison descendante synchrone des données numériques à fréquence intermédiaire vers une EC2 instance Amazon que vous gérez. Désigné par le nom digIfDownlink.
- Liaison descendante asynchrone des données numériques à fréquence intermédiaire vers un compartiment Amazon S3. Désigné par le nom aws-groundstation-demodu compartiment.
- Liaison descendante synchrone des données démodulées et décodées vers une instance Amazon EC2 que vous gérez. Désigné par le nom demodDecodeDownlink.
- Liaison montante synchrone entre les données d'une EC2 instance Amazon que vous gérez et une antenne AWS Ground Station gérée. Désigné par le nom digIfUplink.

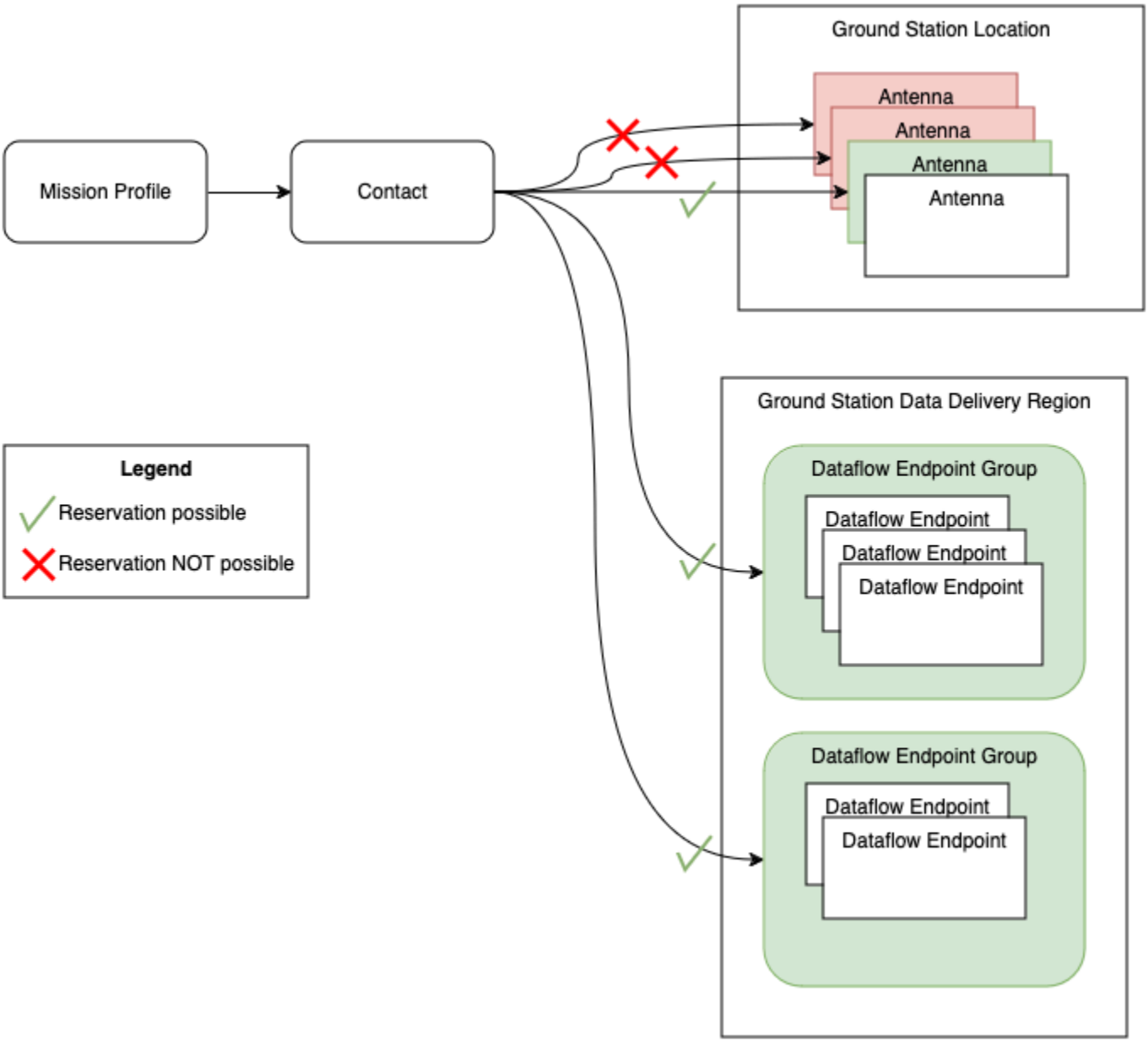


Planification des contacts

Avec un profil de mission valide, vous pouvez demander un contact avec vos satellites embarqués. La demande de réservation de contact est asynchrone afin de laisser le temps au service d'antenne mondial d'établir un calendrier cohérent dans toutes les AWS régions concernées. Au cours de ce processus, diverses antennes situées à l'emplacement de la station au sol demandé sont évaluées afin de déterminer si elles sont disponibles et capables de traiter le contact. Au cours de ce processus, les points de terminaison de votre flux de données configurés sont également évalués afin de déterminer leur disponibilité. Pendant cette évaluation, le statut du contact sera activéSCHEDULING.

Ce processus de planification asynchrone se termine dans les cinq minutes suivant la demande, mais se termine généralement dans la minute qui suit. Veuillez vérifier l'existence [Automatisation]

AWS Ground Station grâce aux événements d'une surveillance basée sur les événements lors de la planification.



Les contacts qui peuvent être effectués et qui sont disponibles donnent lieu à SCHEDULEDdes contacts. Dans le cas d'un contact planifié, les ressources nécessaires pour effectuer votre contact ont été réservées dans les AWS régions requises, telles que définies par le profil de votre mission. Les contacts qui ne peuvent pas être exécutés ou dont les pièces ne sont pas disponibles se traduiront par des contacts FAILED_À_ SCHEDULE. Consultez Résolution des problèmes liés aux FAILED contacts _TO_ SCHEDULE pour plus de détails sur le débogage.

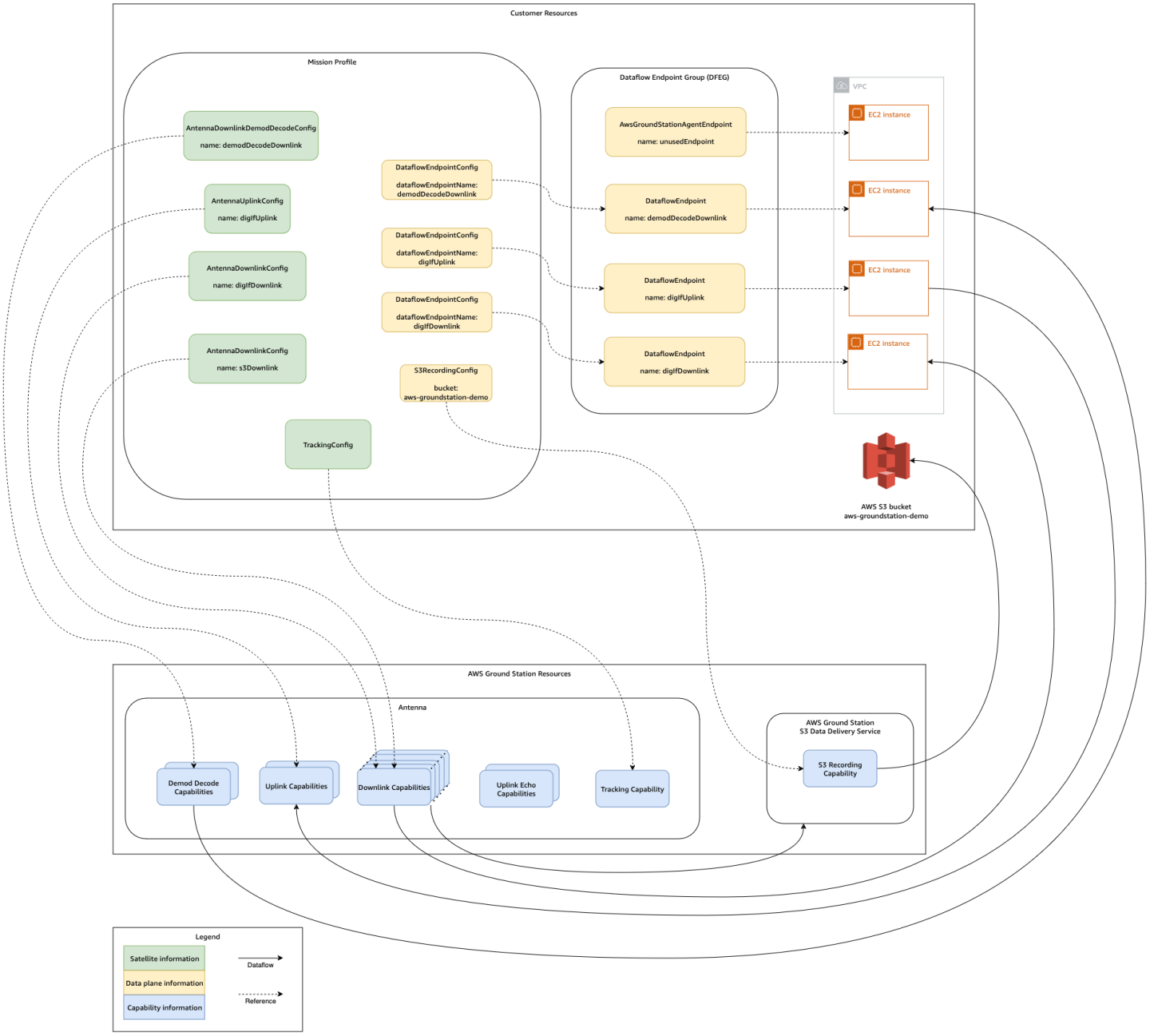
Exécution du contact

AWS Ground Station orchestrera automatiquement vos ressources AWS gérées lors de votre réservation de contact. Le cas échéant, vous êtes responsable de l'orchestration des EC2 ressources définies par votre profil de mission en tant que points de terminaison de flux de données. AWS Ground Station propose des AWS EventBridge événements pour automatiser l'orchestration de vos ressources afin de réduire les coûts. Pour plus d'informations, consultez Automatisation AWS Ground Station grâce aux événements.

Pendant le contact, la télémétrie concernant les performances de votre contact est transmise à. AWS CloudWatch Pour plus d'informations sur la façon de surveiller votre contact pendant l'exécution, veuillez consulterSurveillance.

Le schéma suivant poursuit l'exemple précédent en montrant les mêmes ressources orchestrées lors du contact.

> **Note**
>
> Les capacités de l'antenne n'ont pas toutes été utilisées dans cet exemple. Par exemple, il existe plus d'une douzaine de capacités de liaison descendante disponibles sur chaque antenne qui prennent en charge plusieurs fréquences et polarisations. Pour plus de détails sur le nombre de chaque type de capacité disponible sur les AWS Ground Station antennes, ainsi que sur leurs fréquences et polarisations prises en charge, voir. AWS Ground Station Fonctionnalités du site



À la fin de votre contact, nous AWS Ground Station évaluerons les performances de votre contact et déterminerons le statut final du contact. Les contacts pour lesquels aucune erreur n'est détectée se traduiront par un statut de COMPLETEDcontact. Les contacts pour lesquels des erreurs de service ont causé des problèmes de transmission des données pendant le contact se traduiront par un FAILED statut AWS_. Les contacts pour lesquels des erreurs du client ou de l'utilisateur ont causé des problèmes de livraison des données lors du contact se traduiront par un FAILEDstatut. Les erreurs commises en dehors de l'heure de contact, c'est-à-dire pendant le pré-passage ou après le passage, ne sont pas prises en compte lors de la sélection.

Pour plus d'informations, consultez Cycle de vie des contacts.

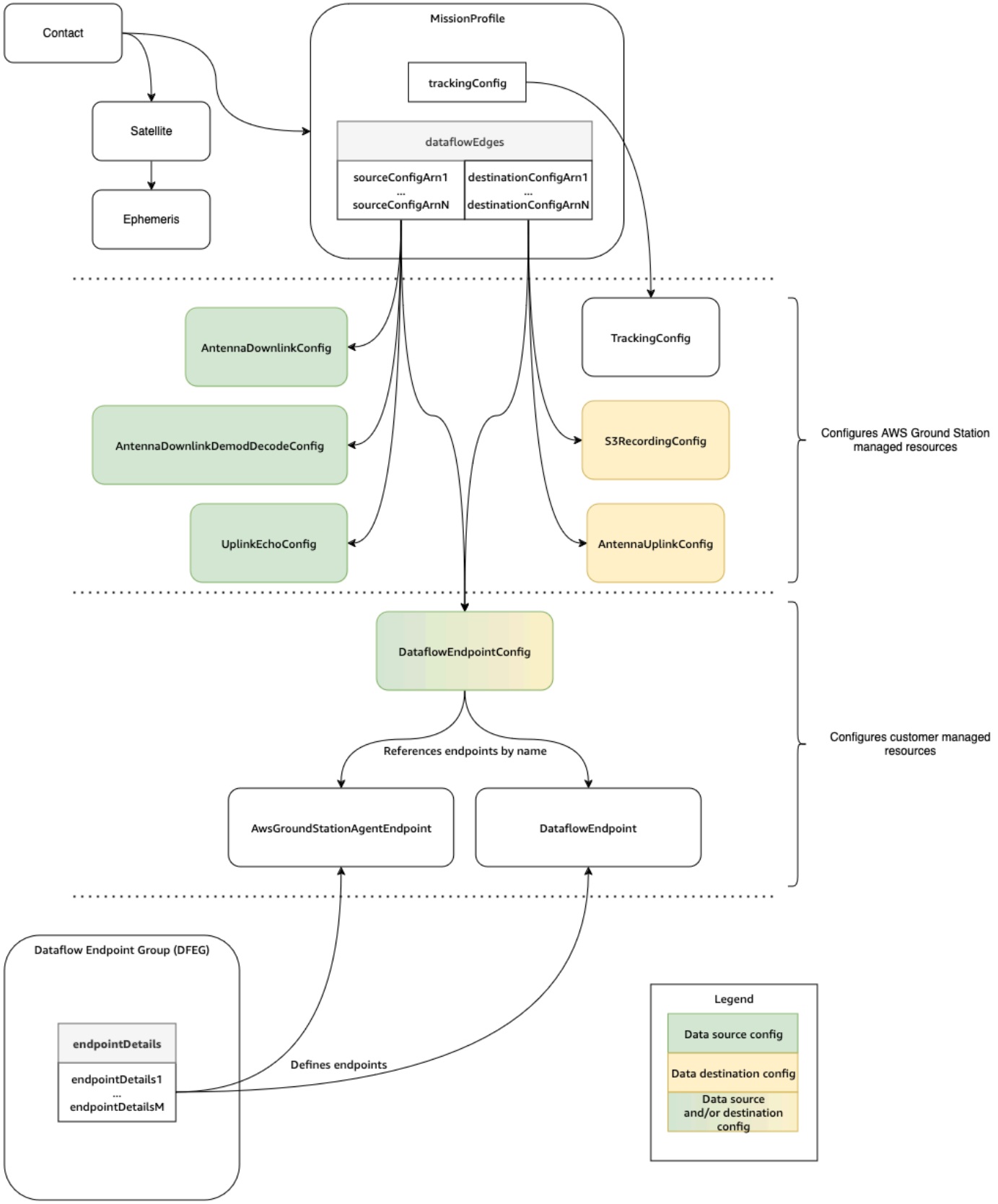
Jumeau numérique

La fonction de jumelage numérique vous AWS Ground Station permet de planifier des contacts en fonction de l'emplacement virtuel des stations au sol. Ces stations terrestres virtuelles sont des répliques exactes des stations terrestres de production, y compris les capacités des antennes, les masques de site et les GPS coordonnées réelles. La fonction de jumelage numérique vous permet de tester votre flux de travail d'orchestration des contacts pour une fraction du coût par rapport aux stations terrestres de production. Pour plus d'informations, consultez AWS Ground Station jumeau numérique.

Composants de base

Cette section fournit des définitions détaillées des principaux composants de AWS Ground Station.

Le schéma suivant montre les composants principaux AWS Ground Station et la manière dont ils sont liés les uns aux autres. Les flèches indiquent le sens des dépendances entre les composants, chaque composant pointant vers ses dépendances.


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

Les rubriques suivantes décrivent les AWS Ground Station principaux composants en détail.

Rubriques

Profil de mission

Les profils de mission contiennent des configurations et des paramètres concernant la façon dont les contacts sont exécutés. Lorsque vous réservez un contact ou recherchez des contacts disponibles, vous fournissez le profil de mission que vous avez l'intention d'utiliser. Les profils de mission rassemblent toutes vos configurations et définissent comment l'antenne sera configurée et où les données seront acheminées lors de votre contact.

Les profils de mission peuvent être partagés entre des satellites partageant les mêmes caractéristiques radio. Vous pouvez créer des groupes de points de terminaison de flux de données supplémentaires pour limiter le maximum de contacts simultanés que vous souhaitez effectuer pour votre constellation.

Les configurations de suivi sont spécifiées sous forme de champ unique dans le profil de mission. Les configurations de suivi sont utilisées pour spécifier vos préférences en matière de suivi des programmes et de suivi automatique lors de votre contact. Pour plus d'informations, consultez Suivi de Config.

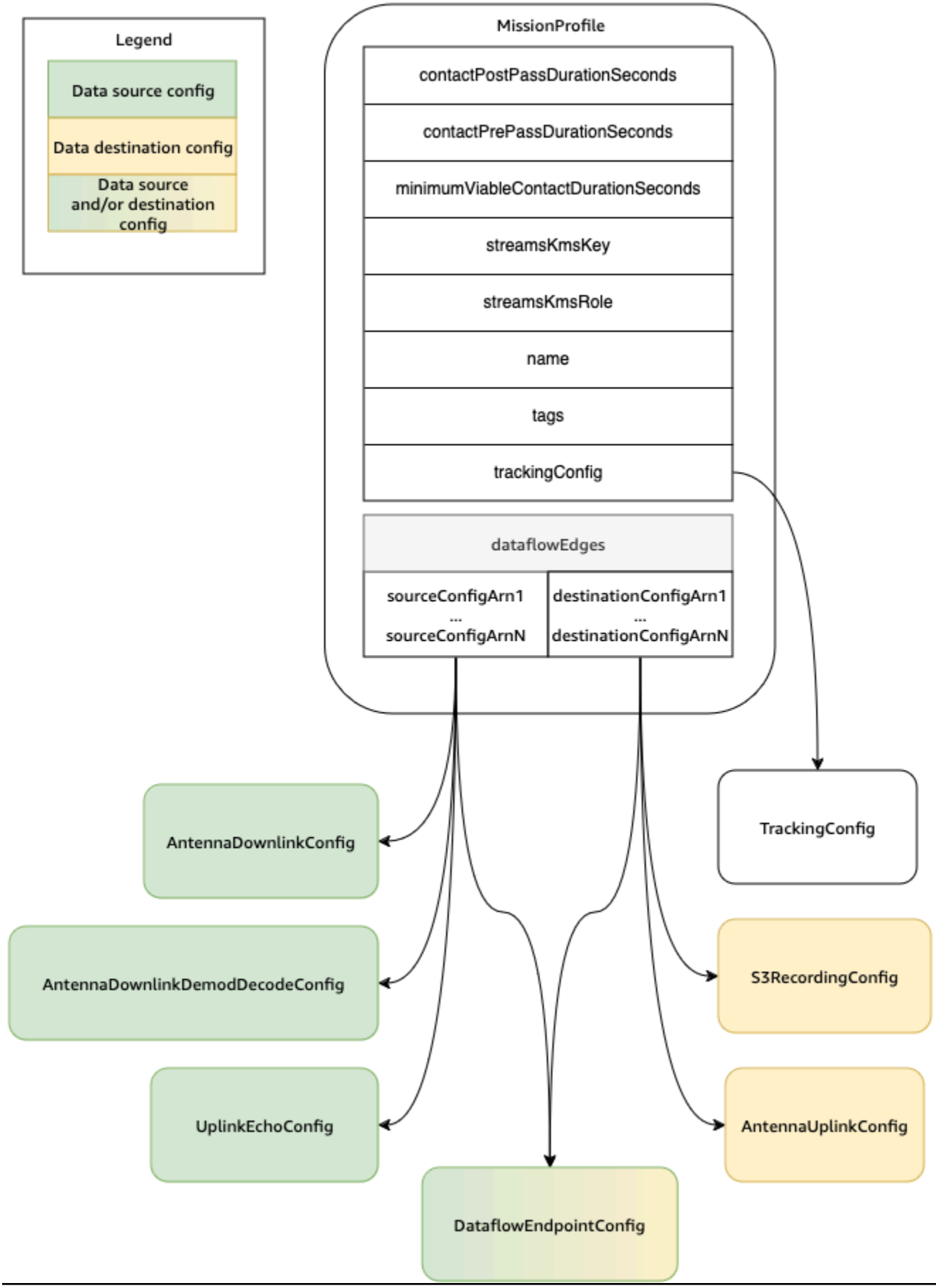
Toutes les autres configurations sont contenues dans le `dataflowEdges` champ du profil de mission. Ces configurations peuvent être considérées comme des nœuds de flux de données qui représentent chacun une ressource AWS Ground Station gérée capable d'envoyer ou de recevoir des données et la configuration associée. Le `dataflowEdges` champ définit les nœuds de flux de données source et de destination (configurations) nécessaires. Un seul bord de flux de données est une liste de deux configurations Amazon Resource Names (ARNs) : la première est la configuration source et la seconde est la configuration de destination. En spécifiant une limite de flux de données entre deux configurations, vous indiquez d'où et AWS Ground Station vers où les données doivent circuler lors d'un contact. Pour plus d'informations, consultez Config.

Les `contactPrePassDurationSeconds` et vous `contactPostPassDurationSeconds` permettent de spécifier les heures relatives au contact où vous recevrez une notification d'

CloudWatch événement. Pour une chronologie des événements liés à votre contact, veuillez lireCycle de vie des contacts.

Le champ `name` du nom du profil de mission permet de distinguer les profils de mission que vous créez.

Les `streamsKmsRole` et `streamsKmsKey` sont utilisés pour définir le cryptage utilisé AWS Ground Station pour la livraison de vos données avec AWS Ground Station l'Agent. Veuillez faire référenceChiffrement des données pendant le transit pour 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

La liste complète des paramètres et des exemples est incluse dans la documentation suivante.

- AWS: : GroundStation : : type de MissionProfile CloudFormation ressource

Config

Les configurations sont des ressources AWS Ground Station utilisées pour définir les paramètres de chaque aspect de votre contact. Ajoutez les configs que vous souhaitez à un profil de mission, puis ce profil de mission sera utilisée lors de l'exécution du contact. Vous pouvez définir plusieurs types différents de configs. Les configurations peuvent être regroupées en deux catégories :

- Configurations de suivi
- Configurations de flux de données

A TrackingConfigest le seul type de configuration de suivi. Il est utilisé pour configurer le réglage automatique de l'antenne lors d'un contact et est requis dans un profil de mission.

Les configurations qui peuvent être utilisées dans un flux de données de profil de mission peuvent être considérées comme des nœuds de flux de données qui représentent chacun une ressource AWS Ground Station gérée capable d'envoyer ou de recevoir des données. Un profil de mission nécessite au moins une paire de ces configurations, l'une représentant une source de données et l'autre une destination. Ces configurations sont résumées dans le tableau suivant.

Nom de la configuration	Source/destination du flux de données
AntennaDownlinkConfig	Source
AntennaDownlinkDemodDecodeConfig	Source
UplinkEchoConfig	Source
S3 RecordingConfig	Destination
AntennaUplinkConfig	Destination
DataflowEndpointConfig	Source et/ou destination

Consultez la documentation suivante pour plus d'informations sur la façon d'effectuer des opérations sur des configurations à l'aide du AWS CloudFormation AWS Command Line Interface, ou du AWS Ground Station API. Des liens vers la documentation pour des types de configuration spécifiques sont également fournis ci-dessous.

- AWSType de CloudFormation ressource GroundStation : : : :Config
- AWS CLI Référence de configuration
- APIRéférence de configuration

Suivi de Config

Vous pouvez utiliser le suivi des configs dans le profil de mission pour déterminer si autotrack doit être activé pendant vos contacts. Cette config possède un seul paramètre : `autotrack`. Le paramètre `autotrack` peut avoir les valeurs suivantes :

- `REQUIRED` - Autotrack est requis pour vos contacts.
- `PREFERRED` - Autotrack est recommandé pour les contacts, mais les contacts peuvent toujours être exécutés sans autotrack.
- `REMOVED` - Aucun autotrack ne doit être utilisé pour vos contacts.

AWS Ground Station utilisera un suivi programmatique qui pointera en fonction de vos éphémérides lorsque le suivi automatique n'est pas utilisé. Veuillez vous référer Données sur les éphémérides satellites pour plus de détails sur la façon dont les éphémérides sont construites.

Autotrack utilisera le suivi du programme jusqu'à ce que le signal attendu soit détecté. Une fois que cela se produit, le suivi se poursuivra en fonction de la force du signal.

Consultez la documentation suivante pour plus d'informations sur la manière d'effectuer des opérations de suivi des configurations à l'aide du AWS CloudFormation AWS Command Line Interface, ou du AWS Ground Station API.

- AWSPropriété : : GroundStation : :Config TrackingConfig CloudFormation
- AWS CLI Référence de configuration (voir la `trackingConfig -> (structure)` section)
- TrackingConfig APIréférence

Config d'antenne de liaison descendante

Vous pouvez utiliser les configurations de liaison descendante de l'antenne pour configurer l'antenne pour la liaison descendante lors de votre contact. Ils consistent en une configuration de spectre qui spécifie la fréquence, la bande passante et la polarisation à utiliser lors de votre contact de liaison descendante.

Cette configuration représente un nœud source dans un flux de données. Il est chargé de numériser les données de radiofréquence. Les données diffusées depuis ce nœud suivront le format Signal Data/IP. Pour des informations plus détaillées sur la façon de créer des flux de données avec cette configuration, voir Flux de données

Si votre cas d'utilisation de la liaison descendante nécessite une démodulation ou un décodage, consultez le. Config de décodage/démodulation des signaux d'antenne de liaison descendante

Consultez la documentation suivante pour plus d'informations sur la façon d'effectuer des opérations sur les configurations de liaison descendante d'antennes à l'aide du AWS CloudFormation AWS Command Line Interface, ou du. AWS Ground Station API

- AWSPropriété : : GroundStation : :Config AntennaDownlinkConfig CloudFormation
- AWS CLI Référence de configuration (voir la `antennaDownlinkConfig -> (structure)` section)
- AntennaDownlinkConfig APIréférence

Config de décodage/démodulation des signaux d'antenne de liaison descendante

Les configurations de décodage par démodulation et/ou décodage d'antenne sont un type de configuration plus complexe et personnalisable que vous pouvez utiliser pour exécuter des contacts de liaison descendante par démodulation et/ou décodage. Si vous souhaitez établir ce type de contact, contactez l' AWS Ground Station équipe en envoyant un e-mail à `<aws-groundstation@amazon.com.>` Nous vous aiderons à définir la bonne config et le bon profil de mission pour votre cas d'utilisation.

Cette configuration représente un nœud source dans un flux de données. Il est chargé de numériser les données de radiofréquence et d'effectuer la démodulation et le décodage conformément aux spécifications. Les données diffusées depuis ce nœud suivront le format de données/IP démodulées/décodées. Pour des informations plus détaillées sur la façon de créer des flux de données avec cette configuration, voir Flux de données

Consultez la documentation suivante pour plus d'informations sur la façon d'effectuer des opérations sur les configurations de décodage par démodage de liaison descendante d'antenne à l'aide du AWS CloudFormation, ou du AWS Command Line Interface. AWS Ground Station API

- AWS::GroundStation::Config AntennaDownlinkDemodDecodeConfig CloudFormation propriété
- AWS CLI Référence de configuration (voir la `antennaDownlinkDemodDecodeConfig -> (structure)` section)
- AntennaDownlinkDemodDecodeConfig APIréférence

Config d'antenne de liaison montante

Vous pouvez utiliser les configurations de liaison montante d'antenne pour configurer l'antenne pour la liaison montante lors de votre contact. Ils consistent en une configuration spectrale avec fréquence, polarisation et puissance isotrope rayonnée effective cible ()EIRP. Pour plus d'informations sur la configuration d'un contact pour le bouclage de la liaison montante, consultez. Config d'écho d'antenne de liaison montante

Cette configuration représente un nœud de destination dans un flux de données. Il convertira le signal de données de radiofréquence numérisé fourni en un signal analogique et l'émettra pour que votre satellite le reçoive. Les données transmises à ce nœud devraient respecter le format Signal Data/IP. Pour des informations plus détaillées sur la façon de créer des flux de données avec cette configuration, voir Flux de données

Consultez la documentation suivante pour plus d'informations sur la façon d'effectuer des opérations sur les configurations de liaison montante d'antenne à l'aide du AWS CloudFormation AWS Command Line Interface, ou du. AWS Ground Station API

- AWSPropriété : : GroundStation : :Config AntennaUplinkConfig CloudFormation
- AWS CLI Référence de configuration (voir la `antennaUplinkConfig -> (structure)` section)
- AntennaUplinkConfig APIréférence

Config d'écho d'antenne de liaison montante

Les configurations d'écho de liaison montante indiquent comment exécuter un écho de liaison montante. Un écho en liaison montante peut être utilisé pour valider les commandes envoyées à votre vaisseau spatial et effectuer d'autres tâches avancées. Ceci est réalisé en enregistrant le signal

réel émis par l' AWS Ground Station antenne (c'est-à-dire la liaison montante). Cela renvoie le signal envoyé par l'antenne à votre point de terminaison de flux de données et doit correspondre au signal transmis. Une configuration d'écho de liaison montante contient celle d'une configuration ARN de liaison montante. L'antenne utilise les paramètres de la configuration de liaison montante pointée par le ARN lors de l'exécution d'un écho de liaison montante.

Cette configuration représente un nœud source dans un flux de données. Les données diffusées depuis ce nœud respecteront le format Signal Data/IP. Pour des informations plus détaillées sur la façon de créer des flux de données avec cette configuration, voir Flux de données

Consultez la documentation suivante pour plus d'informations sur la façon d'effectuer des opérations sur les configurations d'écho de liaison montante à l'aide du AWS CloudFormation AWS Command Line Interface, ou du. AWS Ground Station API

- AWSPropriété : : GroundStation : :Config UplinkEchoConfig CloudFormation
- AWS CLI Référence de configuration (voir la `uplinkEchoConfig -> (structure)` section)
- UplinkEchoConfig APIréférence

Config de point de terminaison de flux de données

> **Note**
>
> Les configurations des points de terminaison Dataflow sont uniquement utilisées pour la livraison de données à Amazon EC2 et ne sont pas utilisées pour la livraison de données à Amazon S3.

Vous pouvez utiliser les configurations de point de terminaison de flux de données pour spécifier quel point de terminaison de flux de données d'un groupe de points de terminaison de flux de données à partir duquel ou vers lequel vous souhaitez que les données circulent lors d'un contact. Les deux paramètres d'une configuration de point de terminaison de flux de données spécifient le nom et la région du point de terminaison de flux de données. Lorsque vous réservez un contact, AWS Ground Station analyse le profil de mission que vous avez spécifié et tente de trouver un groupe de points de terminaison de flux de données dans la AWS région contenant tous les points de terminaison de flux de données spécifiés par les configurations de point de terminaison de flux de données contenues dans votre profil de mission. Si un groupe de points de terminaison de flux de données approprié est trouvé, le statut du contact deviendraSCHEDULED, sinon il deviendra FAILED _TO_. SCHEDULE

Pour plus d'informations sur les statuts possibles d'un contact, consultezAWS Ground Station statuts des contacts.

La `dataflowEndpointName` propriété d'une configuration de point de terminaison de flux de données indique quel point de terminaison de flux de données d'un groupe de points de terminaison de flux de données vers lequel ou depuis lequel les données seront transmises lors d'un contact.

La `dataflowEndpointRegion` propriété indique dans quelle région se trouve le point de terminaison du flux de données. Si une région est spécifiée dans la configuration de votre point de terminaison de flux de données, AWS Ground Station recherche un point de terminaison de flux de données dans la région spécifiée. Si aucune région n'est spécifiée, la région de la station au sol du contact AWS Ground Station sera sélectionnée par défaut. Un contact est considéré comme un contact de livraison de données interrégional si la région du point de terminaison de votre flux de données n'est pas la même que celle de la station au sol du contact. Voir Flux de données pour plus d'informations sur les flux de données entre régions.

Consultez Groupes de points de terminaison de flux de données pour obtenir des conseils sur les avantages que peuvent apporter les différents schémas de dénomination de vos flux de données à votre cas d'utilisation.

Pour des informations plus détaillées sur la façon de créer des flux de données avec cette configuration, voir Flux de données

Consultez la documentation suivante pour plus d'informations sur la manière d'effectuer des opérations sur les configurations des points de terminaison de flux de données à l'aide du AWS CloudFormation AWS Command Line Interface, ou du. AWS Ground Station API

- AWSPropriété : : GroundStation : :Config DataflowEndpointConfig CloudFormation
- AWS CLI Référence de configuration (voir la `dataflowEndpointConfig -> (structure)` section)
- DataflowEndpointConfig APIréférence

Config d'enregistrement Amazon S3

> **Note**
>
> Les configurations d'enregistrement Amazon S3 ne sont utilisées que pour la livraison de données à Amazon S3 et ne sont pas utilisées pour la livraison de données à AmazonEC2.

Cette configuration représente un nœud de destination dans un flux de données. Ce nœud encapsulera les données entrantes provenant du nœud source du flux de données dans des données pcap. Pour des informations plus détaillées sur la façon de créer des flux de données avec cette configuration, voir Flux de données

Vous pouvez utiliser les configurations d'enregistrement S3 pour spécifier un compartiment Amazon S3 auquel vous souhaitez que les données descendantes soient transmises, ainsi que la convention de dénomination utilisée. Ce qui suit décrit les restrictions et les détails relatifs à ces paramètres :

- Le nom du compartiment Amazon S3 doit commencer par`aws-groundstation`.
- Le IAM rôle doit avoir une politique de confiance qui autorise le directeur du `groundstation.amazonaws.com` service à assumer le rôle. Consultez la section Exemple de politique de confiance ci-dessous pour un exemple. Lors de la création de la configuration, l'identifiant de ressource de configuration n'existe pas, la politique de confiance doit utiliser un astérisque (*) à la place de *`your-config-id`* et peut être mis à jour après la création avec l'identifiant de ressource de configuration.

Exemple de politique de confiance

Pour plus d'informations sur la façon de mettre à jour la politique de confiance d'un rôle, consultez la section Gestion IAM des rôles dans le Guide de IAM l'utilisateur.

```
{
  "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"
        }
```

```
      }
    }
  ]
}
```

- Le IAM rôle doit disposer d'une IAM politique lui permettant d'exécuter l'`s3:GetBucketLocation`action sur le compartiment et l'`s3:PutObject`action sur les objets du compartiment. Si le compartiment Amazon S3 possède une politique de compartiment, celle-ci doit également autoriser le IAM rôle à effectuer ces actions. Consultez la section Exemple de politique de rôle ci-dessous pour un exemple.

Exemple de politique de rôle

Pour plus d'informations sur la façon de mettre à jour ou d'associer une politique de rôle, consultez la section Gestion des IAM politiques dans le Guide de IAM l'utilisateur.

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

- Le préfixe sera utilisé pour nommer l'objet de données S3. Vous pouvez spécifier des clés facultatives pour la substitution. Ces valeurs seront remplacées par les informations correspondantes figurant dans vos coordonnées. Par exemple, le préfixe de `{satellite_id}/{year}/{month}/{day}` sera remplacé et donnera une sortie comme `fake_satellite_id/2021/01/10`

  Clés facultatives pour la substitution : `{satellite_id}` `{config-name}` `{config-id}` | | `{year}` | `{month}` | `{day}` |

Consultez la documentation suivante pour plus d'informations sur la façon d'effectuer des opérations sur les configurations d'enregistrement S3 à l'aide du AWS CloudFormation AWS Command Line Interface, ou du AWS Ground Station API.

- AWSPropriété S3 RecordingConfig CloudFormation : GroundStation : : :Config
- AWS CLI Référence de configuration (voir la `s3RecordingConfig -> (structure)` section)
- RecordingConfig APIRéférence S3

Groupes de points de terminaison de flux de données

Les points de terminaison du flux de données définissent l'emplacement vers lequel vous souhaitez que les données soient diffusées de manière synchrone pendant les contacts. Les point de terminaison de flux de données sont toujours créés dans le cadre d'un groupe de points de terminaison de flux de données. Si vous incluez plusieurs points de terminaison de flux de données dans un groupe, cela signifie que les points de terminaison spécifiés peuvent tous être utilisés conjointement au cours d'un seul contact. Par exemple, si un contact a besoin d'envoyer des données vers trois points de terminaison de flux de données distincts, vous devez disposer de trois points de terminaison dans un seul groupe de points de terminaison du flux de données qui correspondent aux configs de point de terminaison de flux de données de votre profil de mission.

> **Tip**
>
> Les points de terminaison du flux de données sont identifiés par le nom que vous avez choisi lors de l'exécution des contacts. Il n'est pas nécessaire que ces noms soient uniques pour l'ensemble du compte. Cela permet d'exécuter plusieurs contacts entre différents satellites et antennes en même temps en utilisant le même profil de mission. Cela peut être

utile si vous avez une constellation de satellites présentant les mêmes caractéristiques de fonctionnement. Vous pouvez augmenter le nombre de groupes de points de terminaison du flux de données pour qu'il corresponde au nombre maximal de contacts simultanés dont votre constellation de satellites a besoin.

Lorsqu'une ou plusieurs ressources d'un groupe de points de terminaison de flux de données sont en cours d'utilisation pour un contact, l'ensemble du groupe est réservé pendant toute la durée du contact. Vous pouvez exécuter plusieurs contacts simultanément, mais ces contacts doivent être exécutés sur différents groupes de points de terminaison de flux de données.

Important

Les groupes de points de terminaison Dataflow doivent être en HEALTHY état de planifier les contacts qui les utilisent. Pour plus d'informations sur la façon de résoudre les problèmes liés aux groupes de points de terminaison de flux de données qui ne sont pas dans un HEALTHY état, consultez. Le dépannage DataflowEndpointGroups n'est pas en HEALTHY état

Consultez la documentation suivante pour plus d'informations sur la manière d'effectuer des opérations sur les groupes de points de terminaison de flux de données à l'aide du AWS CloudFormation AWS Command Line Interface, ou du. AWS Ground Station API

- AWS: : GroundStation : : type de DataflowEndpointGroup CloudFormation ressource
- Référence du groupe Dataflow Endpoint AWS CLI
- Référence du groupe Dataflow Endpoint API

Points de terminaison de flux de données

Les membres d'un groupe de points de terminaison de flux de données sont des points de terminaison de flux de données. Les points de terminaison de flux de données peuvent être définis pour utiliser l' AWS Ground Station agent ou fonctionner avec une application de point de terminaison de flux de données. Pour les deux types d'instances, vous allez créer les structures de support (par exemple, les adresses IP) avant de créer le groupe de points de terminaison du flux de données. Consultez Flux de données les recommandations relatives au type de point de terminaison du flux de données à utiliser et à la manière de configurer les structures de support.

Les sections suivantes décrivent les deux types de points de terminaison pris en charge.

AWS Ground Station Point final de l'agent

Le point de terminaison de l' AWS Ground Station agent utilise l' AWS Ground Station agent en tant que composant logiciel pour mettre fin aux connexions. Utilisez un point de terminaison AWS Ground Station Agent Dataflow lorsque vous souhaitez transférer en liaison descendante plus de 50 MHz % des données de signal numérique. Pour créer un point de terminaison d' AWS Ground Station agent, vous devez uniquement renseigner le `AwsGroundStationAgentEndpoint` champ du EndpointDetails. Pour plus d'informations sur l' AWS Ground Station agent, consultez le guide d'utilisation complet de l'AWS Ground Station agent.

`AwsGroundStationAgentEndpoint` comprend les éléments suivants :

- `Name`- Le nom du point de terminaison du flux de données. Pour que le contact puisse utiliser ce point de terminaison de flux de données, ce nom doit correspondre au nom utilisé dans la configuration de votre point de terminaison de flux de données.
- `EgressAddress`- L'adresse IP et l'adresse du port utilisés pour faire sortir les données de l'agent.
- `IngressAddress`- L'adresse IP et l'adresse du port utilisés pour saisir les données vers l'agent.

Point de terminaison du flux de données

Le point de terminaison Dataflow utilise une application réseau en tant que composant logiciel pour mettre fin aux connexions. Utilisez Dataflow Endpoint lorsque vous souhaitez établir une liaison montante avec des données de signal numérique, une liaison descendante avec moins de 50 % de données de signal numérique ou une liaison descendante avec des données MHz de signal démodulées/décodées. Pour créer un point de terminaison de flux de données, vous devez renseigner les `Security Details` champs `Endpoint` et du. EndpointDetails

`Endpoint` comprend les éléments suivants :

- `Name`- Le nom du point de terminaison du flux de données. Pour que le contact puisse utiliser ce point de terminaison de flux de données, ce nom doit correspondre au nom utilisé dans la configuration de votre point de terminaison de flux de données.
- `Address`- L'adresse IP et l'adresse du port utilisés.

`SecurityDetails` comprend les éléments suivants :

- `roleArn`- Le nom de ressource Amazon (ARN) d'un rôle qui AWS Ground Station sera chargé de créer des interfaces réseau élastiques (ENIs) dans votreVPC. Ils ENIs servent de points d'entrée et de sortie des données diffusées lors d'un contact.
- `securityGroupIds` - Les groupes de sécurité à attacher aux interfaces réseau Elastic.
- `subnetIds`- Une liste de sous-réseaux où sont AWS Ground Station placées des interfaces réseau élastiques pour envoyer des flux à vos instances.

Le IAM rôle transféré `roleArn` doit avoir une politique de confiance qui permet au directeur du `groundstation.amazonaws.com` service d'assumer le rôle. Consultez la section Exemple de politique de confiance ci-dessous pour un exemple. Lors de la création du point de terminaison, l'identifiant de ressource du point de terminaison n'existe pas. La politique de confiance doit donc utiliser un astérisque (*) à la place de *your-endpoint-id*. Il peut être mis à jour après sa création pour utiliser l'identifiant de ressource du point de terminaison afin d'étendre la politique de confiance à ce groupe de points de terminaison de flux de données spécifique.

Le IAM rôle doit disposer d'une IAM politique AWS Ground Station permettant de configurer leENIs. Consultez la section Exemple de politique de rôle ci-dessous pour un exemple.

Exemple de politique de confiance

Pour plus d'informations sur la façon de mettre à jour la politique de confiance d'un rôle, consultez la section Gestion IAM des rôles dans le Guide de IAM l'utilisateur.

```
{
  "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"
```

```
        }
      }
    }
  ]
}
```

Exemple de politique de rôle

Pour plus d'informations sur la façon de mettre à jour ou d'associer une politique de rôle, consultez la section Gestion des IAM politiques dans le Guide de IAM l'utilisateur.

```
{
  "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 Agent

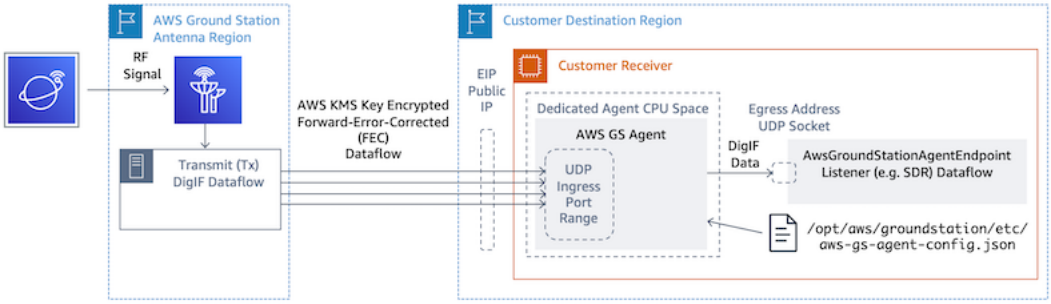
Qu'est-ce que l' AWS Ground Station agent ?

Le AWS Ground Station Agent AWS Ground Station vous permet de recevoir (liaison descendante) des flux de données synchrones à fréquence intermédiaire numérique à large bande (DigIF) lors des contacts avec la Ground Station. AWS Vous pouvez sélectionner deux options pour la livraison des données :

1. Livraison de données à une EC2 instance : livraison de données à une EC2 instance dont vous êtes le propriétaire. Vous gérez l' AWS Ground Station agent. Cette option peut vous convenir le mieux si vous avez besoin d'un traitement des données en temps quasi réel. Consultez la Flux de données section pour plus d'informations sur la livraison EC2 des données.
2. Livraison des données vers un compartiment S3 - La livraison des données vers votre compartiment AWS S3 est entièrement gérée par AWS Ground Station. Consultez le Mise en route guide pour plus d'informations sur la livraison de données S3.

Les deux modes de livraison de données nécessitent la création d'un ensemble de AWS ressources. L'utilisation de CloudFormation pour créer vos AWS ressources est vivement recommandée afin de garantir la fiabilité, la précision et la facilité de prise en charge. Chaque contact peut uniquement transmettre des données à EC2 S3, mais pas aux deux simultanément.

Le schéma suivant montre un flux de données DigIF d'une région d' AWS Ground Station antenne vers votre EC2 instance avec votre radio définie par logiciel () ou un écouteur similaire. SDR



Informations supplémentaires

Pour des informations plus détaillées, consultez le guide de l'utilisateur complet de l'AWS Ground Station agent.

Mise en route

Avant de commencer, vous devez vous familiariser avec les concepts de base de AWS Ground Station. Pour plus d'informations, consultez Comment AWS Ground Station fonctionne.

Vous trouverez ci-dessous les meilleures pratiques pour AWS Identity and Access Management (IAM) et les autorisations dont vous aurez besoin. Après avoir configuré les rôles appropriés, vous pouvez commencer à suivre les étapes restantes.

Inscrivez-vous pour un Compte AWS

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

1. Ouvrez l'https://portal.aws.amazon.com/billing/inscription.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des AWS services et des ressources de ce compte. La meilleure pratique de sécurité consiste à attribuer un accès administratif à un utilisateur, et à utiliser uniquement l'utilisateur racine pour effectuer les tâches nécessitant un accès utilisateur racine.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. Vous pouvez afficher l'activité en cours de votre compte et gérer votre compte à tout moment en accédant à https://aws.amazon.com/ et en choisissant Mon compte.

Création d'un utilisateur doté d'un accès administratif

Une fois que vous vous êtes inscrit à un utilisateur administratif Compte AWS, que vous Utilisateur racine d'un compte AWS l'avez sécurisé AWS IAM Identity Center, que vous l'avez activé et que vous en avez créé un, afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.

   Pour obtenir de l'aide pour vous connecter en utilisant l'utilisateur racine, consultez Connexion en tant qu'utilisateur racine dans le Guide de l'utilisateur Connexion à AWS .
2. Activez l'authentification multifactorielle (MFA) pour votre utilisateur root.

   Pour obtenir des instructions, voir Activer un MFA périphérique virtuel pour votre utilisateur Compte AWS root (console) dans le guide de IAM l'utilisateur.

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez Activation d' AWS IAM Identity Center dans le Guide de l'utilisateur AWS IAM Identity Center .
2. Dans IAM Identity Center, accordez un accès administratif à un utilisateur.

   Pour un didacticiel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, voir Configurer l'accès utilisateur par défaut Répertoire IAM Identity Center dans le Guide de AWS IAM Identity Center l'utilisateur.

Connexion en tant qu'utilisateur doté d'un accès administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l'URLidentifiant envoyé à votre adresse e-mail lorsque vous avez créé l'utilisateur IAM Identity Center.

  Pour obtenir de l'aide pour vous connecter en utilisant un utilisateur d'IAMIdentity Center, consultez la section Connexion au portail AWS d'accès dans le guide de Connexion à AWS l'utilisateur.

Attribution d'un accès à d'autres utilisateurs

1. Dans IAM Identity Center, créez un ensemble d'autorisations conforme à la meilleure pratique consistant à appliquer les autorisations du moindre privilège.

Pour obtenir des instructions, consultez Création d'un ensemble d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .

2. Attribuez des utilisateurs à un groupe, puis attribuez un accès par authentification unique au groupe.

   Pour obtenir des instructions, consultez Ajout de groupes dans le Guide de l'utilisateur AWS IAM Identity Center .

Ajoutez AWS Ground Station des autorisations à votre AWS compte

Pour l'utiliser AWS Ground Station sans avoir besoin d'un utilisateur administratif, vous devez créer une nouvelle politique et l'associer à votre AWS compte.

1. Connectez-vous à la IAMconsole AWS Management Console et ouvrez-la.
2. Créez une stratégie. Procédez comme suit :

   a. Dans le panneau de navigation, choisissez Policies (Politiques), puis Create Policy (Créer une politique).

   b. Dans l'JSONonglet, modifiez le JSON avec l'une des valeurs suivantes. Utilisez celui JSON qui convient le mieux à votre application.

      - Pour les privilèges administratifs de Ground Station, définissez Action sur groundstation : * comme suit :

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

```
}
```

- Pour des autorisations en lecture seule (Read-only), définissez Action sur groundstation:get*, groundstation:list* et groundstation:describe* comme suit :

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

- Pour une sécurité accrue grâce à l'authentification multifactorielle, définissez Action sur groundstation : * et Condition/Bool sur aws ::true comme suit : MultiFactorAuthPresent

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

3. Dans la IAM console, associez la politique que vous avez créée à l'utilisateur souhaité.

Pour plus d'informations sur IAM les utilisateurs et les politiques d'attachement, consultez le guide de IAM l'utilisateur.

Étape 1 : Intégration du satellite

L'intégration d'un satellite AWS Ground Station est un processus en plusieurs étapes impliquant la collecte de données, la validation technique, l'octroi de licences de spectre, ainsi que l'intégration et les tests. Des accords de confidentialité (NDAs) sont également requis.

Vue d'ensemble du processus d'intégration des clients

L'intégration des satellites est un processus manuel qui se trouve dans la section Satellites et ressources de la page de AWS Ground Station console. Ce qui suit décrit le processus global.

1. Consultez la Emplacements section pour déterminer si votre satellite répond aux caractéristiques géographiques et aux caractéristiques de radiofréquence.
2. Pour commencer à intégrer votre satellite à AWS Ground Station, veuillez envoyer un e-mail à `<aws-groundstation@amazon.com>` avec un bref résumé de votre mission et de vos besoins en matière de satellites, y compris le nom de votre organisation, les fréquences requises, la date de lancement des satellites, le type d'orbite du satellite et si vous prévoyez de l'utiliserAWS Ground Station jumeau numérique.
3. Une fois votre demande examinée et approuvée, vous AWS Ground Station demanderez une licence réglementaire aux sites spécifiques que vous prévoyez d'utiliser. La durée de cette étape varie en fonction des lieux et des réglementations en vigueur.
4. Une fois cette approbation obtenue, votre satellite sera visible pour que vous puissiez l'utiliser. AWS Ground Station vous enverra une notification vous informant de la réussite de la mise à jour.

(Facultatif) Dénomination des satellites

Après l'intégration, vous souhaiterez peut-être ajouter un nom à votre enregistrement satellite pour le reconnaître plus facilement. La AWS Ground Station console peut afficher un nom défini par l'utilisateur pour un satellite ainsi que l'identifiant Norad lorsque vous utilisez la page Contacts. L'affichage du nom du satellite facilite grandement la sélection du bon satellite lors de la planification. Pour ce faire, des tags peuvent être utilisés.

Le balisage des satellites AWS Ground Station peut être effectué via la ressource tag-resource API avec le AWS CLI ou l'un des. AWS SDKs Ce guide traitera de l'utilisation du AWS Ground Station CLI pour étiqueter le satellite de diffusion public Aqua (Norad ID 27424) dans. `us-west-2`

AWS Ground Station CLI

Ils AWS CLI peuvent être utilisés pour interagir avec AWS Ground Station. Avant AWS CLI de pouvoir étiqueter vos satellites, les AWS CLI conditions suivantes doivent être remplies :

- Assurez-vous qu'il AWS CLI est installé. Pour plus d'informations sur l'installation AWS CLI, voir Installation de la AWS CLI version 2.
- Assurez-vous qu'il AWS CLI est configuré. Pour plus d'informations sur la configuration AWS CLI, consultez Configuration de la AWS CLI version 2.
- Enregistrez vos paramètres de configuration utilisés fréquemment et vos informations d'identification dans les fichiers qui sont gérés par l' AWS CLI. Vous avez besoin de ces paramètres et informations d'identification pour réserver et gérer vos AWS Ground Station contacts avec AWS CLI. Pour plus d'informations sur l'enregistrement de votre configuration et de vos paramètres d'identification, consultez la section Paramètres des fichiers de configuration et d'identification.

Une fois la configuration AWS CLI terminée et prête à être utilisée, consultez la page AWSGround Station CLI Command Reference pour vous familiariser avec les commandes disponibles. Suivez la structure de AWS CLI commande lorsque vous utilisez ce service et préfixez vos commandes avec `groundstation` pour indiquer le service AWS Ground Station que vous souhaitez utiliser. Pour plus d'informations sur la structure de AWS CLI commande, voir Structure de commande AWS CLI sur la page. Un exemple de structure de commande est fourni ci-dessous.

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

Nommer un satellite

Vous devez d'abord obtenir ARN le ou les satellites que vous souhaitez étiqueter. Cela peut être fait via la liste des satellites API dans le : AWS CLI

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

L'exécution de la CLI commande ci-dessus renverra un résultat similaire à celui-ci :

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

Trouvez le satellite que vous souhaitez étiqueter et notez le`satelliteArn`. Une mise en garde importante concernant le balisage est que la ressource de balisage API nécessite une valeur régionale et que la ressource ARN renvoyée par ARN list-satellites est globale. À l'étape suivante, vous devez ajouter la ARN région dans laquelle vous souhaitez voir le tag (probablement la région dans laquelle vous planifiez). Pour cet exemple, nous utilisons`us-west-2`. Avec ce changement, on ARN passera de :

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

par :

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

Pour afficher le nom du satellite dans la console, le satellite doit avoir une étiquette avec `"Name"` comme clé. De plus, étant donné que nous utilisons le AWS CLI, les guillemets doivent être masqués par une barre oblique inverse. Le tag ressemblera à quelque chose comme suit :

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

Ensuite, vous allez appeler le tag-resource API pour étiqueter le satellite. Cela peut être fait avec des AWS CLI méthodes similaires :

```
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"}'
```

Après cela, vous pourrez voir le nom que vous avez défini pour le satellite dans la AWS Ground Station console.

Changer le nom d'un satellite

Si vous souhaitez modifier le nom d'un satellite, vous pouvez simplement appeler à ARN nouveau tag-resource avec le satellite avec la même "Name" clé, mais avec une valeur différente dans la balise. Cela mettra à jour le tag existant et affichera le nouveau nom dans la console. Voici un exemple d'appel pour cela :

```
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"}'
```

Supprimer le nom d'un satellite

Le nom défini pour un satellite peut être supprimé à l'aide de la ressource untag-resourceAPI. Cela API nécessite le satellite ARN avec la région dans laquelle se trouve le tag et une liste des clés du tag. Pour le nom, la clé du tag est"Name". Voici un exemple d'appel à ceci API en utilisant ce AWS CLI qui suit :

```
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
```

Satellites de diffusion publics

Outre l'embarquement de vos propres satellites, vous pouvez demander à embarquer avec des satellites de diffusion publics compatibles qui fournissent une voie de communication descendante accessible au public. Cela vous permet de les utiliser AWS Ground Station pour transférer les données de ces satellites.

> **Note**
>
> Vous ne pourrez pas établir de liaison ascendante vers ces satellites. Vous ne pourrez utiliser que les voies de communication descendantes accessibles au public.

AWS Ground Station prend en charge l'intégration des satellites suivants pour la liaison descendante des données de diffusion directe :

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

Une fois embarqués, ces satellites sont accessibles pour une utilisation immédiate. AWS Ground Station gère un certain nombre de AWS CloudFormation modèles préconfigurés pour faciliter la prise en main du service. Voir Exemples de configurations de profil de mission des exemples AWS Ground Station d'utilisation.

Pour plus d'informations sur ces satellites et le type de données qu'ils transmettent, voir Aqua, JPSS-1/ NOAA -20 et SNPP Terra.

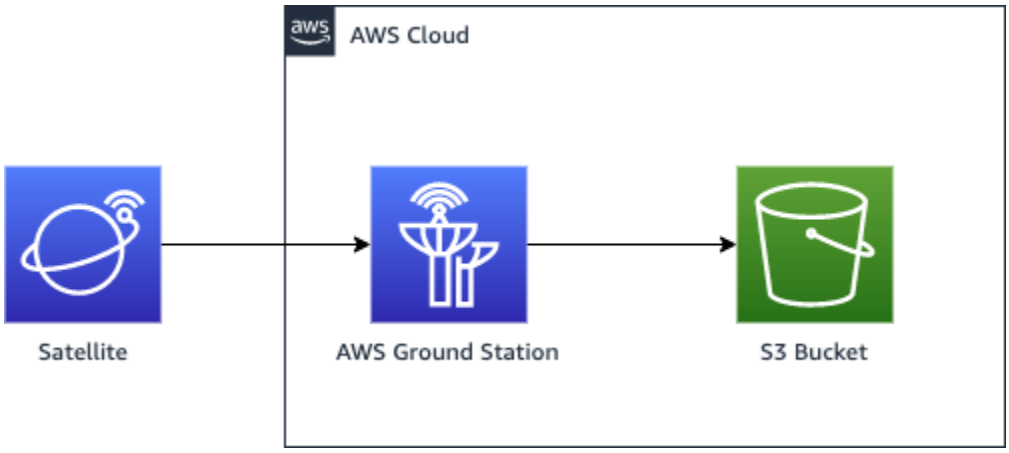
Étape 2 : planifiez les voies de communication de votre flux de données

Vous avez le choix entre une communication synchrone ou asynchrone pour chaque voie de communication de votre satellite. En fonction de votre satellite et de votre cas d'utilisation, vous pouvez avoir besoin de l'un ou des deux types. Les voies de communication synchrones permettent des opérations de liaison montante en temps quasi réel ainsi que des opérations de liaison descendante à bande étroite et à large bande. Les voies de communication asynchrones prennent uniquement en charge les opérations de liaison descendante à bande étroite et à large bande.

Livraison de données asynchrone

Avec la livraison de données vers Amazon S3, vos données de contact sont transmises de manière asynchrone à un compartiment Amazon S3 de votre compte. Vos données de contact sont fournies sous forme de fichiers de capture de paquets (pcap) pour permettre de rejouer les données de

contact dans une radio définie par logiciel (SDR) ou pour extraire les données de charge utile des fichiers pcap à des fins de traitement. Les fichiers pcap sont envoyés à votre compartiment Amazon S3 toutes les 30 secondes à mesure que les données de contact sont reçues par le matériel de l'antenne pour permettre le traitement des données de contact pendant le contact, si vous le souhaitez. Une fois reçues, vous pouvez traiter les données à l'aide de votre propre logiciel de post-traitement ou utiliser d'autres AWS services tels qu'Amazon SageMaker ou Amazon Rekognition. La livraison de données vers Amazon S3 n'est disponible que pour la liaison descendante des données depuis votre satellite ; il n'est pas possible de relier des données vers votre satellite depuis Amazon S3.



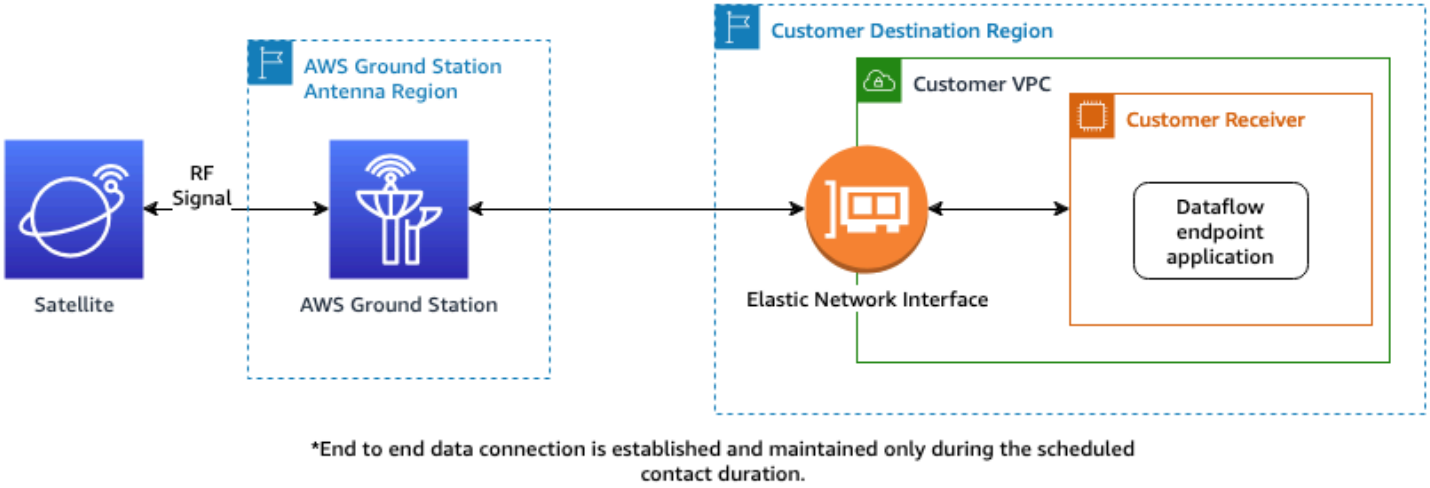
Pour utiliser ce chemin, vous devez créer un compartiment Amazon S3 dans AWS Ground Station lequel envoyer les données. À l'étape suivante, vous devrez également créer une configuration d'enregistrement S3 à l'étape suivante. Consultez le Config d'enregistrement Amazon S3 pour connaître les restrictions relatives à la dénomination des compartiments et pour savoir comment spécifier la convention de dénomination utilisée pour vos fichiers.

Livraison synchrone des données

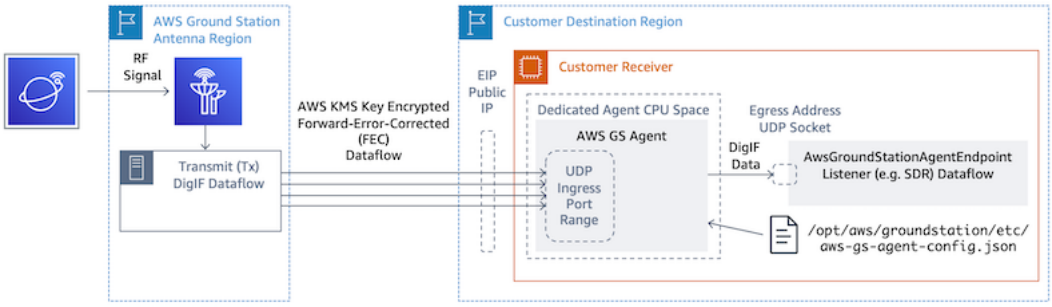
Lors de la livraison de données à AmazonEC2, vos données de contact sont diffusées vers et depuis votre EC2 instance Amazon. Vous pouvez traiter vos données en temps réel sur votre EC2 instance Amazon ou les transférer pour un post-traitement.

Pour utiliser un chemin synchrone, vous devez configurer vos EC2 instances Amazon et créer un ou plusieurs groupes de points de terminaison Dataflow. Pour configurer votre EC2 instance Amazon, référencez leEC2- Installation et configuration. Pour créer votre groupe de points de terminaison Dataflow, veuillez vous référer au. Groupes de points de terminaison de flux de données

Le tableau suivant indique le chemin de communication si vous utilisez la configuration du point de terminaison du flux de données.



Le tableau suivant indique le chemin de communication si vous utilisez la configuration de l' AWS Ground Station agent.



Étape 3 : créer des configurations

À cette étape, vous avez identifié le satellite, les voies de communication et IAM les ressources Amazon EC2 et Amazon S3 selon vos besoins. Au cours de cette étape, vous allez créer AWS Ground Station des configurations qui stockent leurs paramètres respectifs.

Configurations de livraison de données

Les premières configurations à créer concernent l'endroit et la manière dont vous souhaitez que les données soient transmises. À l'aide des informations de l'étape précédente, vous allez créer la plupart des types de configuration suivants.

- Config d'enregistrement Amazon S3- Fournissez des données à votre compartiment Amazon S3.
- Config de point de terminaison de flux de données- Fournissez des données à votre EC2 instance Amazon.

Configurations satellites

Les configurations du satellite indiquent AWS Ground Station comment communiquer avec votre satellite. Vous ferez référence aux informations que vous avez recueilliesÉtape 1 : Intégration du satellite.

- Suivi de Config- Définit les préférences relatives au suivi physique de votre véhicule lors d'un contact. Cela est nécessaire pour la construction du profil de mission.
- Config d'antenne de liaison descendante- Fournissez des données de radiofréquence numérisées.
- Config de décodage/démodulation des signaux d'antenne de liaison descendante - Fournissez des données de radiofréquence démodulées et décodées.
- Config d'antenne de liaison montante- Liez les données vers votre satellite.
- Config d'écho d'antenne de liaison montante- Diffusez un écho des données de votre signal de liaison montante.

Étape 4 : Création d'un profil de mission

À l'aide des configurations créées à l'étape précédente, vous avez identifié comment suivre votre satellite et les moyens possibles de communiquer avec votre satellite. Au cours de cette étape, vous allez créer un ou plusieurs profils de mission. Un profil de mission représente l'agrégation des configurations possibles dans un comportement attendu qui peut ensuite être planifié et exploité.

Pour les derniers paramètres, veuillez vous référer au type de AWS::GroundStation::MissionProfile CloudFormation ressource

1. Donnez un nom à votre profil de mission. Cela vous permet de comprendre rapidement son utilisation au sein de votre système. Par exemple, vous pouvez avoir un satellite-wideband-narrowband-nominal-operations et un satellite-narrowband-emergency-operationssi vous avez un opérateur à bande étroite distinct pour les opérations d'urgence.
2. Définissez votre configuration de suivi.
3. Définissez vos durées de contact minimales viables. Cela vous permet de filtrer les contacts potentiels pour répondre aux besoins de votre mission.
4. Configurez vos streamsKmsKeyet streamsKmsRoleceux qui sont utilisés pour crypter vos données pendant le transport. Ceci est utilisé pour tous les flux de données de AWS Ground Station l'agent.

5. Définissez vos flux de données. Créez vos flux de données pour qu'ils correspondent aux signaux de votre opérateur à l'aide des configurations que vous avez créées à l'étape précédente.
6. [Facultatif] Définissez la durée en secondes de votre contact avant et après le passage. Ceci est utilisé pour émettre des événements par contact avant et après le contact, respectivement. Pour plus d'informations, consultez Automatisation AWS Ground Station grâce aux événements.
7. [Facultatif] Vous pouvez associer des tags à votre profil de mission. Ils peuvent être utilisés pour vous aider à différencier vos profils de mission de manière programmatique.

Vous pouvez faire référence auExemples de configurations de profil de mission, pour ne voir que quelques-unes des configurations potentielles.

Étapes suivantes

Maintenant que vous avez un satellite embarqué et un profil de mission valide, vous êtes prêt à planifier des contacts et à communiquer avec votre satellite avec. AWS Ground Station

Vous pouvez planifier un contact de l'une des manières suivantes :

- La AWS Ground Station console.
- La commande AWS CLI reserve-contact.
- Le AWS SDK. ReserveContactAPI.

Pour plus d'informations sur la façon dont AWS Ground Station suit la trajectoire de votre satellite et sur la manière dont ces informations sont utilisées, veuillez vous référer àDonnées sur les éphémérides satellites.

AWS Ground Station gère un certain nombre de AWS CloudFormation modèles préconfigurés pour faciliter la prise en main du service. Voir Exemples de configurations de profil de mission des exemples de la façon dont il AWS Ground Station peut être utilisé.

Le traitement des données numériques à fréquence intermédiaire ou des données démodulées et décodées qui vous sont fournies AWS Ground Station dépendra de votre cas d'utilisation spécifique. Les articles de blog suivants peuvent vous aider à comprendre certaines des options qui s'offrent à vous :

- Observation de la Terre automatisée à l'aide de la livraison de données AWS Ground Station Amazon S3 (et de son GitHub référentiel associé awslabs/ aws-groundstation-eos-pipeline)
- Virtualisation du segment terrestre du satellite avec AWS
- Observation de la Terre à l'aide de AWS Ground Station : un guide pratique
- Création d'architectures de liaison descendante de données satellites à haut débit avec DigiF et Amphinicy Blink AWS Ground Station WideBand (et son référentiel associé aws-samples/ SDR) GitHub aws-groundstation-wbdigif-snpp

Emplacements

AWS Ground Station fournit un réseau mondial de stations au sol à proximité de notre réseau mondial de régions d'AWSinfrastructure. Vous pouvez configurer votre utilisation de ces emplacements à partir de n'importe quelle AWS région prise en charge. Cela inclut la AWS région dans laquelle les données sont fournies.

Trouver la AWS région pour l'emplacement d'une station au sol

Le réseau AWS Ground Station mondial comprend des stations au sol qui ne sont pas physiquement situées dans la AWSrégion à laquelle elles sont connectées. La liste des stations au sol auxquelles vous avez accès peut être récupérée via la AWS SDK ListGroundStationréponse. La liste complète des emplacements des stations au sol est présentée ci-dessous, et d'autres seront bientôt disponibles. Reportez-vous au guide d'intégration pour ajouter ou modifier les approbations de site pour vos satellites.

Nom de la station au sol	Emplacement de la station Ground	AWSNom de la région	AWSCode de région	Remarques
Alaska 1	Alaska, USA	USA Ouest (Oregon)	us-west-2	Pas physiquement situé dans une AWS région
Bahreïn 1	Bahreïn	Moyen-Orient (Bahreïn)	me-south-1	
Le Cap 1	Le Cap, Afrique du Sud	Afrique (Le Cap)	af-south-1	
Dubbo 1	Dubbo, Australie	Asie-Pacifique (Sydney)	ap-southeast-2	Pas physiquement situé dans une AWS région
Hawaï 1	Hawaï, USA	USA Ouest (Oregon)	us-west-2	Pas physiquement situé dans une AWS région
Irlande 1	Irlande	Europe (Irlande)	eu-west-1	
Ohio 1	Ohio, USA	USA Est (Ohio)	us-east-2	
Oregon 1	État de l'Oregon, USA	USA Ouest (Oregon)	us-west-2	
Punta Arenas 1	Punta Arenas, Chili	Amérique du Sud (São Paulo)	sa-east-1	Pas physiquement situé dans une AWS région
Séoul 1	Séoul, Corée du Sud	Asie-Pacifique (Séoul)	ap-northeast-2	
Singapour 1	Singapour	Asie-Pacifique (Singapour)	ap-southeast-1	

Nom de la station au sol	Emplacement de la station Ground	AWSNom de la région	AWSCode de région	Remarques
Stockholm 1	Stockholm, Suède	Europe (Stockholm)	eu-north-1	

AWS Ground Station AWSrégions prises en charge

Vous pouvez fournir des données et configurer vos contacts via la AWS Ground Station console AWS SDK ou depuis les AWS régions prises en charge. Vous pouvez consulter les régions prises en charge et leurs points de terminaison associés dans les points de AWS Ground Station terminaison et les quotas.

Disponibilité du jumeau numérique

AWS Ground Station jumeau numériqueest disponible dans toutes les AWSrégions où AWS Ground Station il est disponible. Les stations terrestres à double numérique sont des copies exactes des stations au sol de production avec un préfixe modificateur du nom de la station au sol « Digital Twin ». Par exemple, « Digital Twin Ohio 1 » est une station terrestre double numérique qui est une copie exacte de la station au sol de production « Ohio 1 ».

AWS Ground Station masques de site

Des masques de site sont associés à chaque emplacement d' AWS Ground Station antenne. Ces masques empêchent les antennes situées à cet endroit d'émettre ou de recevoir lorsqu'elles pointent dans certaines directions, généralement près de l'horizon. Les masques peuvent prendre en compte :

- Caractéristiques du terrain géographique entourant l'antenne — Par exemple, cela inclut des éléments tels que des montagnes ou des bâtiments, qui bloqueraient un signal de radiofréquence (RF) ou empêcheraient la transmission.
- Interférences de fréquence radio (RFI) — Cela affecte à la fois la capacité de réception (RFIsources externes affectant un signal de liaison descendante dans les antennes de la AWS Ground Station) et de transmission (le signal RF transmis par les antennes de la AWS Ground Station a un impact négatif sur les récepteurs externes).

- Autorisations légales — Les autorisations de site locales pour exploiter une AWS Ground Station dans chaque région peuvent inclure des restrictions spécifiques, telles qu'un angle d'élévation minimum pour la transmission.

Ces masques de site peuvent changer au fil du temps. Par exemple, de nouveaux bâtiments peuvent être construits à proximité d'une antenne, les RFI sources peuvent changer ou l'autorisation légale peut être renouvelée avec différentes restrictions. Les masques du site AWS Ground Station sont mis à votre disposition dans le cadre d'un accord de confidentialité (NDA).

Masques spécifiques au client

En plus des masques de site AWS Ground Station présents sur chaque site, vous pouvez avoir des masques supplémentaires en raison des restrictions relatives à votre propre autorisation légale de communiquer avec vos satellites dans une région donnée. Ces masques peuvent être configurés dans AWS Ground Station de case-by-case manière à garantir la conformité lors de l'utilisation de AWS Ground Station pour communiquer avec ces satellites. Contactez l'équipe de AWS Ground Station pour plus de détails.

Impact des masques de site sur les temps de contact disponibles

Il existe deux types de masques de site : les masques de site de liaison montante (transmission) et les masques de site de liaison descendante (réception).

Lorsque vous listez les heures de contact disponibles à l'aide de l' ListContacts opération, AWS Ground Station affiche les heures de visibilité en fonction du moment où votre satellite s'élèvera au-dessus et se placera en dessous du masque de liaison descendante. Les temps de contact disponibles sont basés sur cette fenêtre de visibilité du masque en lien descendant. Cela garantit que vous ne réservez pas de temps lorsque votre satellite se trouve sous le masque de liaison descendante.

Les masques de site Uplink ne sont pas appliqués aux temps de contact disponibles, même si le profil de mission inclut une configuration de liaison montante d'antenne dans un bord de flux de données. Cela vous permet d'utiliser tout le temps de contact disponible pour la liaison descendante, même si la liaison montante peut ne pas être disponible pendant une partie de cette période en raison du masque du site de liaison montante. Cependant, le signal de liaison montante peut ne pas être transmis pendant une partie ou la totalité du temps réservé à un contact satellite. Vous êtes responsable de la prise en compte du masque de liaison montante fourni lors de la planification des transmissions en liaison montante.

La partie d'un contact qui n'est pas disponible pour la liaison montante varie en fonction de la trajectoire du satellite pendant le contact, par rapport au masque du site de liaison montante à l'emplacement de l'antenne. Dans les régions où les masques de site de liaison montante et de liaison descendante sont similaires, cette durée est généralement courte. Dans d'autres régions, où le masque de liaison montante peut être considérablement plus élevé que le masque de site de liaison descendante, cela peut entraîner l'indisponibilité d'une partie importante, voire de la totalité, de la durée du contact pour la liaison montante. Le temps de contact complet vous est facturé, même si une partie du temps réservé n'est pas disponible pour la liaison montante.

AWS Ground Station Fonctionnalités du site

Pour simplifier votre expérience, AWS Ground Station déterminez un ensemble commun de capacités pour un type d'antenne, puis déployez plusieurs antennes à l'emplacement d'une station au sol. Une partie des étapes d'intégration permet de s'assurer que votre satellite est compatible avec les types d'antennes situés à un endroit précis. Lorsque vous réservez un contact, vous déterminez indirectement le type d'antenne utilisé. Cela garantit que votre expérience à un emplacement donné de station au sol reste la même au fil du temps, quelles que soient les antennes utilisées. Les performances spécifiques de votre contact peuvent varier en raison d'une grande variété de préoccupations environnementales, telles que les conditions météorologiques sur le site.

À l'heure actuelle, tous les sites prennent en charge les fonctionnalités suivantes :

> **Note**
>
> Chaque ligne du tableau suivant indique un chemin de communication indépendant, sauf indication contraire. Des lignes dupliquées existent pour refléter nos capacités multicanaux qui permettent d'utiliser simultanément plusieurs voies de communication.

Type de capacité	Gamme de fréquences	Plage de bande passante	Polarization	Nom commun	Remarques
liaison descendante entre antennes	7750 - 8400 MHz	50 à 400 MHz	RHCP	Liaison descendante à large bande en bande X	La bande passante globale doit être inférieure

Type de capacité	Gamme de fréquences	Plage de bande passante	Polarization	Nom commun	Remarques
liaison descendante entre antennes	7750 - 8400 MHz	50 à 400 MHz	RHCP		à 400 et MHz les plages de fréquences utilisées ne doivent pas se chevaucher. Punta Arenas 1 max est de 167MHz. Nécessite l'agent GS.
liaison descendante entre antennes	7750 - 8400 MHz	50 à 400 MHz	RHCP		
liaison descendante entre antennes	7750 - 8400 MHz	50 à 400 MHz	RHCP		
liaison descendante entre antennes	7750 - 8400 MHz	50 à 400 MHz	RHCP		
liaison descendante entre antennes	7750 - 8400 MHz	50 à 400 MHz	LHCP		
liaison descendante entre antennes	7750 - 8400 MHz	50 à 400 MHz	LHCP		
liaison descendante entre antennes	7750 - 8400 MHz	50 à 400 MHz	LHCP		

Type de capacité	Gamme de fréquences	Plage de bande passante	Polarization	Nom commun	Remarques
liaison descendante entre antennes	7750 - 8400 MHz	50 à 400 MHz	LHCP		
liaison descendante entre antennes	7750 - 8400 MHz	50 à 400 MHz	LHCP		
liaison descendante entre antennes	2200 - 2290 MHz	Jusqu'à 40 MHz	RHCP	Liaison descendante en bande S	Une seule polarisation peut être utilisée à la fois
liaison descendante entre antennes	2200 - 2290 MHz	Jusqu'à 40 MHz	LHCP		
liaison descendante entre antennes	7750 - 8400 MHz	Jusqu'à 40 MHz	RHCP	Liaison descendante à bande étroite en bande X	Une seule polarisation peut être utilisée à la fois
liaison descendante entre antennes	7750 - 8400 MHz	Jusqu'à 40 MHz	LHCP		

Type de capacité	Gamme de fréquences	Plage de bande passante	Polarization	Nom commun	Remarques
antenne-uplink	2025 - 2110 MHz	Jusqu'à 40 MHz	RHCP	Liaison montante en bande S	Une seule polarisation peut être utilisée à la fois EIRP20-53 dBW
antenne-uplink	2025 - 2110 MHz	Jusqu'à 40 MHz	LHCP		
antenna-uplink-echo	2025 - 2110 MHz	2 MHz	RHCP	Écho Uplink	Correspond aux restrictions relatives aux liaisons montantes entre antennes
antenna-uplink-echo	2025 - 2110 MHz	2 MHz	LHCP		
antenna-downlink-demod-decode	7750 - 8400 MHz	Jusqu'à 500 MHz	RHCP	Liaison descendante démodulée et décodée à large bande en bande X	
antenna-downlink-demod-decode	7750 - 8400 MHz	Jusqu'à 500 MHz	LHCP		
suivi	N/A	N/A	N/A	N/A	Support pour le suivi automatique et le suivi des programmes

* RHCP = polarisation circulaire pour les droitiers et LHCP = polarisation circulaire pour les gauchers. Pour plus d'informations sur la polarisation, voir Polarisation circulaire.

Données sur les éphémérides satellites

Une éphéméride, au pluriel, est un fichier ou une structure de données fournissant la trajectoire d'objets astronomiques. Historiquement, ce fichier ne faisait référence qu'à des données tabulaires, mais progressivement, il a été dirigé vers une grande variété de fichiers de données indiquant la trajectoire d'un engin spatial.

AWS Ground Station utilise les données d'éphémérides pour déterminer à quel moment des contacts sont disponibles pour votre satellite et commander correctement les antennes du AWS Ground Station réseau afin qu'elles pointent vers votre satellite. Par défaut, aucune action n'est requise pour fournir AWS Ground Station des éphémérides si un identifiant a été attribué à votre satellite. NORAD

Rubriques

Données d'éphémérides par défaut

Par défaut, AWS Ground Station utilise les données accessibles au public provenant de Space-Track, et aucune action n'est requise pour fournir ces AWS Ground Station éphémérides par défaut. Ces éphémérides sont des ensembles d'éléments sur deux lignes (TLEs) associés à l'identifiant de votre satellite. NORAD Toutes les éphémérides par défaut ont une priorité de 0. Par conséquent, elles seront toujours remplacées par toutes les éphémérides personnalisées non expirées téléchargées via les éphémériAPI, qui doivent toujours avoir une priorité de 1 ou plus.

Les satellites sans NORAD identifiant doivent télécharger des données d'éphémérides personnalisées sur. AWS Ground Station Par exemple, les satellites qui viennent d'être lancés ou qui sont volontairement omis du catalogue Space-Track n'auraient aucun NORAD identifiant et auraient besoin d'éphémérides personnalisées téléchargées. Pour plus d'informations sur la fourniture d'une éphéméride personnalisée, voir : Fournir des données d'éphéméride personnalisées.

Fournir des données d'éphémérides personnalisées

> **Important**
>
> L'éphéméride API est actuellement en état d'aperçu

L'accès aux éphémérides n'APIest fourni qu'en cas de besoin.
`<Si vous souhaitez pouvoir télécharger des données d'éphémérides personnalisées,`

Présentation

L'éphéméride API permet de télécharger des éphémérides personnalisées pour une utilisation avec un satellite AWS Ground Station . Ces éphémérides remplacent les éphémérides par défaut de Space-Track (voir :). Données d'éphémérides par défaut Nous prenons en charge la réception de données d'éphémérides aux formats Orbit Ephemeris Message (OEM) et Elément à deux lignes (). TLE

Le téléchargement d'éphémérides personnalisées peut améliorer la qualité du suivi, gérer les premières opérations lorsqu'aucune éphéméride Space-Track n'est disponible et prendre en compte les manœuvres. AWS Ground Station

> **Note**
>
> Lorsque vous fournissez des éphémérides personnalisées avant qu'un numéro de catalogue satellite ne soit attribué à votre satellite, vous pouvez utiliser 00000 pour le champ du numéro de catalogue satellite duTLE, et 000 pour la partie du numéro de lancement du champ de désignation international des OEM métadonnées TLE or (par exemple 24000A pour un véhicule lancé en 2024).
>
> Pour plus d'informations sur le format deTLEs, consultez la section Ensemble d'éléments sur deux lignes. Pour plus d'informations sur le format deOEMs, consultezOEMformat éphéméride.

OEMformat éphéméride

AWS Ground Station traite les éphémérides fournies par le OEM client conformément à la CCSDSnorme, avec quelques restrictions supplémentaires. OEMles fichiers doivent être au KVN

format. Le tableau suivant décrit les différents champs d'un OEM et en quoi il AWS Ground Station diffère de la CCSDS norme.

Section	Champ	CCSDSrequis	AWS Ground Station requis	Remarques
En-tête	CCSDS_OEM_VERS	Oui	Oui	Valeur requise : 2,0
	COMMENT	Non	Non	
	CLASSIFICATION	Non	Non	
	CREATION_DATE	Oui	Oui	
	ORIGINATOR	Oui	Oui	
	MESSAGE_ID	Non	Non	
Metadonnées	META_START	Oui	Oui	
	COMMENT	Non	Non	
	OBJECT_NAME	Oui	Oui	
	OBJECT_ID	Oui	Oui	
	CENTER_NAME	Oui	Oui	Valeur requise : Terre
	REF_FRAME	Oui	Oui	Valeurs acceptées : EME2 000 ITRF2 000
	REF_FRAME_EPOCH	Non	Non pris en charge*	Pas nécessaire car les REF_ acceptés

Section	Champ	CCSDSrequis	AWS Ground Station requis	Remarques
				FRAMEs ont une époque implicite
	TIME_SYSTEM	Oui	Oui	Valeur requise : UTC
	START_TIME	Oui	Oui	
	USEABLE_START_TIME	Non	Non	
	USEABLE_STOP_TIME	Non	Non	
	STOP_TIME	Oui	Oui	
	INTERPOLATION	Non	Oui	Nécessaire pour AWS Ground Station générer des angles de pointage précis pour les contacts.
	INTERPOLATION_DEGREES	Non	Oui	Nécessaire pour AWS Ground Station générer des angles de pointage précis pour les contacts.
	META_STOP	Oui	Oui	
Données	X	Oui	Oui	Représenté dans `km`

Section	Champ	CCSDSrequis	AWS Ground Station requis	Remarques
	Y	Oui	Oui	Représenté dans `km`
	Z	Oui	Oui	Représenté dans `km`
	X_ DOT	Oui	Oui	Représenté dans `km/s`
	Y_ DOT	Oui	Oui	Représenté dans `km/s`
	Z_ DOT	Oui	Oui	Représenté dans `km/s`
	X_ DDOT	Non	Non	Représenté dans `km/s^2`
	Y_ DDOT	Non	Non	Représenté dans `km/s^2`
	Z_ DDOT	Non	Non	Représenté dans `km/s^2`
Matrice de covariance	COVARIANCE_START	Non	Non	
	EPOCH	Non	Non	
	COV_REF_FRAME	Non	Non	
	COVARIANCE_STOP	Non	Non	

* Si des lignes non prises en charge par AWS Ground Station sont incluses dans le contenu fourniOEM, la validation OEM échouera.

Les écarts importants par rapport à la CCSDS norme AWS Ground Station sont les suivants :

- CCSDSOEM_ _ VERS doit être`2.0`.
- REF_ FRAME doit être l'un `EME2000` ou l'autre`ITRF2000`.
- REF_ FRAME _ n'EPOCHest pas pris en charge par AWS Ground Station.
- CENTER_ NAME doit être`Earth`.
- TIME_ SYSTEM doit être`UTC`.
- INTERPOLATIONet INTERPOLATION _ DEGREES sont tous deux obligatoires pour AWS Ground Station CPE.

Exemple d'OEMéphéméride au format KVN

Voici un exemple tronqué d'OEMéphéméride au KVN format pour le satellite de radiodiffusion public JPSS -1.

```
CCSDS_OEM_VERS = 2.0

COMMENT Orbit data are consistent with planetary ephemeris DE-430

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

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

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

Création d'une éphéméride personnalisée

Une éphéméride personnalisée peut être créée à l'aide de l'CreateEphemerisaction du. AWS Ground Station API Cette action téléchargera une éphéméride en utilisant les données contenues dans le corps de la demande ou provenant d'un compartiment S3 spécifié.

Il est important de noter que le téléchargement d'une éphéméride définit l'éphéméride et lance un flux de travail asynchrone qui validera `VALIDATING` et générera des contacts potentiels à partir de votre éphéméride. Ce n'est qu'une fois qu'une éphéméride aura passé ce flux de travail et `ENABLED` sera devenue qu'elle sera utilisée pour les contacts. Vous devez effectuer un sondage DescribeEphemerispour connaître le statut des éphémérides ou utiliser des CloudWatch événements pour suivre les changements de statut des éphémérides.

Pour résoudre le problème d'une éphéméride non valide, consultez : Résolution des éphémérides non valides

Exemple : créer un élément à deux lignes (TLE) pour définir des éphémérides via API

Le AWS SDKs, et CLI peut être utilisé pour télécharger un élément de deux lignes (TLE) défini sur des éphémérides AWS Ground Station via l'CreateEphemerisappel. Cette éphéméride sera utilisée à la place des données d'éphémérides par défaut pour un satellite (voir Données d'éphémérides par défaut). Cet exemple montre comment procéder à l'aide de AWS SDKfor Python (Boto3).

Un TLE ensemble est un objet JSON formaté qui enchaîne un ou plusieurs TLEs objets pour construire une trajectoire continue. Les TLEs éléments de l'TLEensemble doivent former un ensemble continu que nous pouvons utiliser pour construire une trajectoire (c'est-à-dire qu'il n'y a aucun intervalle de temps entre TLEs les éléments d'un TLE ensemble). Un exemple d'TLEensemble est présenté ci-dessous :

```
# 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**
>
> Les plages temporelles d'un TLE ensemble doivent correspondre exactement pour qu'il s'agisse d'une trajectoire continue valide. TLEs

Un TLE ensemble peut être téléchargé via le client AWS Ground Station boto3 comme suit :

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

Cet appel renverra un ephemerisId qui pourra être utilisé pour référencer les éphémérides à l'avenir. Par exemple, nous pouvons utiliser les informations fournies lors ephemerisId de l'appel ci-dessus pour connaître le statut de l'éphéméride :

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

Un exemple de réponse à l'DescribeEphemerisaction est fourni ci-dessous

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

Il est recommandé d'interroger l'DescribeEphemerisitinéraire ou d'utiliser CloudWatch des événements pour suivre l'état des éphémérides téléchargées, car elles doivent passer par un flux de travail de validation asynchrone avant d'être définies et de devenir utilisables pour la planification ENABLED et l'exécution de contacts.

Notez que l'NORADidentifiant de l'TLEensemble, TLEs 25994 dans les exemples ci-dessus, doit correspondre à l'NORADidentifiant attribué à votre satellite dans la base de données Space-Track.

Exemple : téléchargement de données Ephemeris depuis un compartiment S3

Il est également possible de télécharger un fichier éphéméride directement depuis un compartiment S3 en pointant sur le compartiment et la clé d'objet. AWS Ground Station récupérera l'objet en votre nom. Les informations sur le chiffrement des données au repos AWS Ground Station sont détaillées dans : Data Encryption At Rest For AWS Ground Station

Vous trouverez ci-dessous un exemple de téléchargement d'un fichier OEM éphéméride à partir d'un compartiment S3

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

```
        }
    })
```

Vous trouverez ci-dessous un exemple de données renvoyées par l'DescribeEphemerisaction appelée pour les OEM éphémérides téléchargées dans le bloc d'exemple de code précédent.

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

Exemple : utilisation d'éphémérides fournies par le client avec AWS Ground Station

Pour des instructions plus détaillées sur l'utilisation des éphémérides fournies par le client avec AWS Ground Station, voir Utilisation des éphémérides fournies par le client avec (et son référentiel associé aws-samples/) AWS Ground Station GitHub aws-groundstation-cpe

Quelles éphémérides sont utilisées

Les éphémérides ont une priorité, une date d'expiration et un indicateur activé. Ensemble, ils déterminent quelle éphéméride est utilisée pour un satellite. Une seule éphéméride peut être active pour chaque satellite.

L'éphéméride qui sera utilisée est l'éphéméride activée la plus prioritaire dont la date d'expiration se situe dans le futur. Une valeur de priorité plus élevée indique une priorité plus élevée. Les temps de contact disponibles renvoyés par ListContactssont basés sur cette éphéméride. Si plusieurs

ENABLED éphémérides ont la même priorité, les éphémérides les plus récemment créées ou mises à jour seront utilisées.

> **Note**
>
> AWS Ground Station dispose d'un quota de service sur le nombre d'éphémérides ENABLED fournies par le client par satellite (voir : Quotas de service). Pour télécharger des données d'éphémérides après avoir atteint ce quota, supprimez (en utilisant`DeleteEphemeris`) ou désactivez (en utilisant) les éphémérides les moins `UpdateEphemeris` prioritaires/les plus anciennes créées par le client.

Si aucune éphéméride n'a été créée, ou si aucune éphéméride n'a de ENABLED statut, une éphéméride par défaut AWS Ground Station sera utilisée pour le satellite (depuis Space-Track), si elle est disponible. Cette éphéméride par défaut a la priorité 0.

Effet des nouvelles éphémérides sur les contacts précédemment programmés

Utilisez le DescribeContact APIpour visualiser les effets des nouvelles éphémérides sur les contacts précédemment planifiés en renvoyant les durées de visibilité actives.

Les contacts planifiés avant le téléchargement d'une nouvelle éphéméride conserveront l'heure de contact initialement prévue, tandis que le suivi de l'antenne utilisera les éphémérides actives. Si la position de l'engin spatial, basée sur les éphémérides actives, diffère considérablement de celle des éphémérides précédentes, cela peut entraîner une réduction du temps de contact du satellite avec l'antenne en raison du fonctionnement de l'engin spatial en dehors du masque du site d'émission/réception. Par conséquent, nous vous recommandons d'annuler et de reprogrammer vos futurs contacts après avoir chargé une nouvelle éphéméride très différente de l'éphéméride précédente. Avec le DescribeContact API, vous pouvez déterminer la partie de votre futur contact qui est inutilisable en raison du fonctionnement de l'engin spatial en dehors du masque du site d'émission/réception en comparant votre contact programmé `endTime` avec le `startTime` et renvoyé. `visibilityStartTime` `visibilityEndTime` Si vous choisissez d'annuler et de reprogrammer vos futurs contacts, la plage de temps de contact ne doit pas dépasser la plage de visibilité de plus de 30 secondes. Les contacts annulés peuvent entraîner des frais s'ils sont annulés trop près du moment du contact. Pour plus d'informations sur les contacts annulés, voir : Ground Station FAQs.

Obtenir les éphémérides actuelles d'un satellite

Les éphémérides actuellement utilisées par AWS Ground Station un satellite spécifique peuvent être récupérées en appelant les actions GetSatelliteor ListSatellites. Ces deux méthodes renverront des métadonnées pour les éphémérides actuellement utilisées. Ces métadonnées d'éphémérides sont différentes pour les éphémérides personnalisées téléchargées vers AWS Ground Station et pour les éphémérides par défaut.

Les éphémérides par défaut `source` incluront uniquement les champs et. `epoch` `epoch`C'est l'époque de l'ensemble d'éléments à deux lignes extrait de Space-Track, et il est actuellement utilisé pour calculer la trajectoire du satellite.

Une éphéméride personnalisée aura une `source` valeur de `"CUSTOMER_PROVIDED"` et inclura un identifiant unique dans le `ephemerisId` champ. Cet identifiant unique peut être utilisé pour rechercher les éphémérides via l'DescribeEphemerisaction. Un `name` champ facultatif sera renvoyé si un nom a été attribué à l'éphéméride lors du téléchargement AWS Ground Station via l'CreateEphemerisaction.

Il est important de noter que les éphémérides sont mises à jour dynamiquement, de AWS Ground Station sorte que les données renvoyées ne sont qu'un instantané des éphémérides utilisées au moment de l'appel au. API

Exemple de **`GetSatellite`** retour pour un satellite utilisant une éphéméride par défaut

```
{
    "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
    }
}
```

Exemple **`GetSatellite`** de satellite utilisant une éphéméride personnalisée

```
{
      "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"
      }
  }
```

Revenir aux données d'éphémérides par défaut

Lorsque vous téléchargez des données d'éphémérides personnalisées, elles remplacent les éphémérides AWS Ground Station utilisées par défaut pour ce satellite en particulier. AWS Ground Station n'utilise pas à nouveau les éphémérides par défaut tant qu'aucune éphéméride non expirée fournie par le client n'est actuellement disponible. AWS Ground Station ne répertorie pas non plus les contacts après la date d'expiration des éphémérides actuellement fournies par le client, même si une éphéméride par défaut est disponible après cette date d'expiration.

Pour revenir aux éphémérides Space-Track par défaut, vous devez effectuer l'une des opérations suivantes :

- Supprimez (en utilisant DeleteEphemeris) ou désactivez (en utilisant UpdateEphemeris) toutes les éphémérides activées fournies par le client. Vous pouvez répertorier les éphémérides fournies par le client pour un satellite à l'aide de. ListEphemerides
- Attendez que toutes les éphémérides existantes fournies par le client expirent.

Vous pouvez confirmer que l'éphéméride par défaut est utilisée en appelant GetSatelliteet en vérifiant que l'`source`éphéméride actuelle du satellite est bien celle du satellite. `SPACE_TRACK` Voir Données d'éphémérides par défaut pour plus d'informations sur les éphémérides par défaut.

Flux de données

AWS Ground Station utilise une relation entre le nœud et le bord pour créer des flux de données afin de permettre le traitement en flux de vos données. Chaque nœud est représenté par une configuration qui décrit le traitement attendu. Pour illustrer ce concept, considérez un flux de données allant de `antenna-downlink` à a. `s3-recording` Le `antenna-downlink` nœud représente la transformation analogique-numérique du spectre des fréquences radio selon les paramètres définis dans la configuration. Il `s3-recording` représente un nœud de calcul qui recevra les données entrantes et les stockera dans votre compartiment S3. Le flux de données qui en résulte est une livraison asynchrone de données RF numérisées vers un compartiment S3 en fonction de vos spécifications.

Dans le cadre de votre profil de mission, vous pouvez créer de nombreux flux de données pour répondre à vos besoins. Les sections suivantes décrivent comment configurer vos autres AWS ressources à utiliser AWS Ground Station et proposent des recommandations pour créer des flux de données. Pour obtenir des informations détaillées sur le comportement de chaque nœud, y compris s'il est considéré comme un nœud source ou de destination, consultezConfig.

Rubriques

- AWS Ground Station interfaces de plan de données
- Utilisation de la diffusion de données entre régions
- S3 - Installation et configuration
- VPC- Installation et configuration
- EC2- Installation et configuration

AWS Ground Station interfaces de plan de données

La structure de données qui en résulte pour le flux de données que vous avez choisi dépend de la source du flux de données. Les détails de ces formats vous sont fournis lors de l'embarquement de vos satellites. Les formats utilisés pour chaque type de flux de données sont résumés ci-dessous.

- liaison descendante entre antennes
  - (Bande passante inférieure à 54MHz) les données sont fournies sous forme de paquets de données de VITAsignal/format IP -49.

  - (greater-than-or-equalBande passante jusqu'à 54MHz) les données sont livrées sous forme de paquets AWS Ground Station de classe 2.
- antenna-downlink-demod-decode
  - Les données sont livrées sous forme de paquets de données démodulés/décodés/au format IP.
- antenne-uplink
  - Les données doivent être livrées sous forme de paquets VITAau format -49 Signal Data/IP.
- antenna-uplink-echo
  - Les données sont fournies sous forme de paquets de données de signal/format IP VITA -49.

Utilisation de la diffusion de données entre régions

La fonction de transmission de données AWS Ground Station entre régions vous donne la flexibilité d'envoyer vos données depuis une antenne vers n'importe quelle AWS région AWS Ground Station prise en charge. Cela signifie que vous pouvez maintenir votre infrastructure dans une seule AWS région et planifier des contacts pour toutes celles dans lesquelles AWS Ground Station Emplacements vous êtes intégré.

La livraison de données entre régions est actuellement disponible dans toutes les régions AWS Ground Station prises en charge lorsque vous recevez vos données de contact dans un compartiment Amazon S3. AWS Ground Station gérera pour vous tous les aspects de la livraison.

La livraison de données entre régions à Amazon EC2 avec l' AWS Ground Station agent est disponible dans toutes les antenna-to-destination régions. Aucune configuration ou approbation unique n'est requise pour cette configuration.

La livraison de données entre régions à Amazon EC2 via un point de terminaison de flux de données est disponible par défaut* dans les régions décrites ci-dessous. antenna-to-destination

- Région USA Est (Ohio) (us-east-2) vers région USA Ouest (Oregon) (us-west-2)
- Région USA Ouest (Oregon) (us-west-2) vers région USA Est (Ohio) (us-east-2)

Pour utiliser la livraison de données entre régions vers une EC2 instance Amazon, le point de terminaison du flux de données doit être créé dans votre AWS région actuelle et vous dataflow-endpoint-configdevez spécifier la même région.

Les informations précédentes détaillant les régions prises en charge et les méthodes de livraison pour la livraison de données entre régions sont résumées dans le tableau suivant.

Méthode de réception	Région de l'antenne	Région réceptrice
Livraison de données Amazon S3	Tout est intégré AWS Ground Station Emplacements	Toutes les AWS Ground Station régions
AWS Ground Station Agent sur Amazon EC2	Tout est intégré AWS Ground Station Emplacements	Toutes les AWS Ground Station régions
Point de terminaison de flux de données sur Amazon * EC2	Région USA Est (Ohio) (us-east-2)	Région USA Ouest (Oregon) (us-west-2)
	Région USA Ouest (Oregon) (us-west-2)	Région USA Est (Ohio) (us-east-2)

*Les antenna-to-destination régions supplémentaires non répertoriées nécessitent une configuration spéciale d'Amazon EC2 et du logiciel. Veuillez nous contacter à l'<adresse aws-groundstation@amazon.com> pour obtenir les instructions d'intégration.

S3 - Installation et configuration

Vous pouvez utiliser un compartiment Amazon S3 pour recevoir vos signaux de liaison descendante en utilisant AWS Ground Station. Pour créer le s3-recording-config de destination, vous devez être en mesure de spécifier un compartiment Amazon S3 et un IAM rôle qui autorise AWS Ground Station l'écriture de fichiers dans le compartiment.

Consultez Config d'enregistrement Amazon S3 les restrictions relatives au compartiment, au IAM rôle ou à la création de AWS Ground Station configuration Amazon S3.

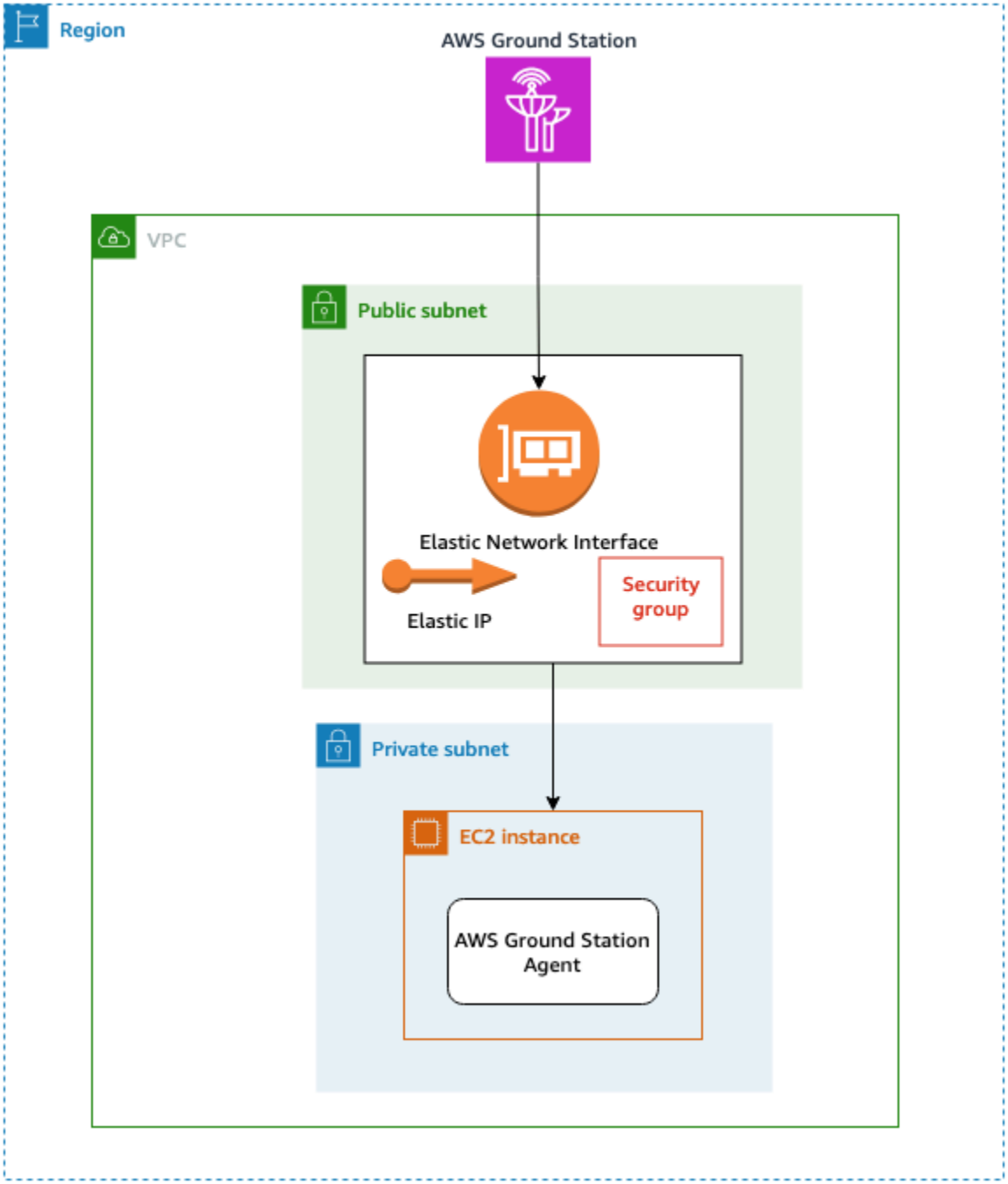
VPC- Installation et configuration

Un guide complet pour configurer un VPC dépasse le cadre de ce guide. Pour une compréhension approfondie, veuillez consulter le guide de AWS VPC l'utilisateur.

Dans cette section, il est décrit comment votre point de terminaison Amazon EC2 et votre point de terminaison Dataflow peuvent exister au sein d'un. VPC AWS Ground Station ne prend pas en

charge plusieurs points de livraison pour un flux de données donné ; il est prévu que chaque flux de données se termine vers un seul récepteur. EC2 Comme nous nous attendons à un seul EC2 récepteur, la configuration n'est pas redondante multi-AZ. Pour des exemples complets qui utiliseront votreVPC, veuillez consulterExemples de configurations de profil de mission.

VPCConfiguration avec l' AWS Ground Station agent



Vos données satellites sont fournies à une instance d' AWS Ground Station agent située à proximité de l'antenne. L' AWS Ground Station agent rayera puis cryptera vos données à l'aide de la AWS KMS clé que vous fournissez. Chaque bande est envoyée à votre adresse IP Amazon EC2 Elastic (EIP) depuis l'antenne source sur le backbone du AWS réseau. Les données arrivent à votre EC2 instance via l'Amazon EC2 Elastic Network Interface (ENI) ci-jointe. Une fois sur votre EC2 instance, l' AWS Ground Station agent installé déchiffre vos données et corrige les erreurs de transfert (FEC) pour récupérer les données perdues, puis les transmet à l'adresse IP et au port que vous avez spécifiés dans votre configuration.

La liste ci-dessous présente les considérations de configuration uniques à prendre en compte lors de la configuration de VPC la livraison de AWS Ground Station l'agent.

Groupe de sécurité - Il est recommandé de configurer un groupe de sécurité dédié uniquement au AWS Ground Station trafic. Ce groupe de sécurité doit autoriser le trafic UDP entrant sur la même plage de ports que vous spécifiez dans votre groupe de points de terminaison Dataflow. AWS Ground Station gère une liste de préfixes AWS gérée pour limiter vos autorisations aux seules AWS Ground Station adresses IP. Consultez les listes de préfixes AWS gérées pour savoir comment remplacer les dans PrefixListIdvos régions de déploiement.

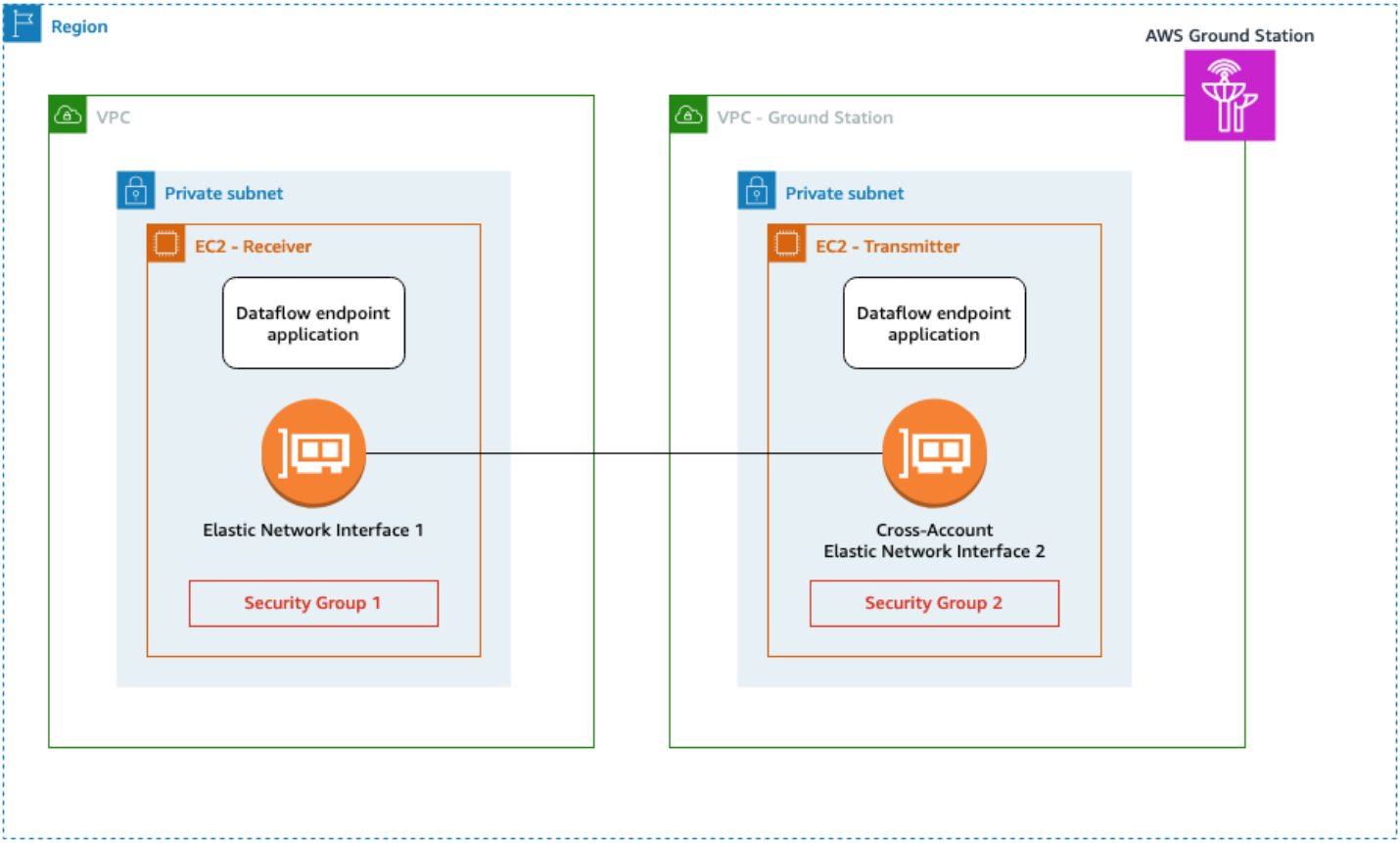
Elastic Network Interface (ENI) : vous devez y associer le groupe de sécurité ci-dessus ENI et le placer dans votre sous-réseau public.

Le CloudFormation modèle suivant montre comment créer l'infrastructure décrite dans cette section.

```
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
```

VPCconfiguration avec un point de terminaison de flux de données



Vos données satellites sont fournies à une instance d'application de point de terminaison de flux de données située à proximité de l'antenne. Les données sont ensuite envoyées via Amazon EC2 Elastic Network Interface (ENI) multi-comptes par AWS Ground Station un VPC propriétaire. Les données arrivent ensuite à votre EC2 instance via le fichier ENI joint à votre EC2 instance Amazon. L'application de point de terminaison de flux de données installée le transmettra ensuite à l'adresse IP et au port que vous avez spécifiés dans votre configuration. L'inverse de ce flux se produit pour les connexions montantes.

La liste ci-dessous présente les considérations de configuration uniques à prendre en compte lors de la configuration de votre point de terminaison VPC pour le flux de données.

IAMRôle : le IAM rôle fait partie du point de terminaison du flux de données et n'apparaît pas dans le diagramme. IAMRôle utilisé pour créer et associer le compte croisé ENI à l'EC2instance AWS Ground Station Amazon.

Groupe de sécurité 1 : ce groupe de sécurité est rattaché au groupe ENI qui sera associé à l'EC2instance Amazon de votre compte. Il doit autoriser le UDP trafic en provenance du groupe de sécurité 2 sur les ports spécifiés dans votre dataflow-endpoint-group.

Elastic Network Interface (ENI) 1 - Vous devez y associer le groupe de sécurité 1 ENI et le placer dans un sous-réseau.

Groupe de sécurité 2 : ce groupe de sécurité est référencé dans le point de terminaison Dataflow. Ce groupe de sécurité sera rattaché au groupe ENI qui AWS Ground Station sera utilisé pour placer des données dans votre compte.

Région - Pour plus d'informations sur les régions prises en charge pour les connexions entre régions, voirUtilisation de la diffusion de données entre régions.

Le CloudFormation modèle suivant montre comment créer l'infrastructure décrite dans cette section.

```
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- Installation et configuration

La configuration correcte de votre EC2 instance est requise pour la livraison synchrone des données signal/IP VITA -49 ou des données d'extension/IP à délivrer via l'agent ou VITA un point de terminaison de flux de données. AWS Ground Station En fonction de vos besoins spécifiques, vous pouvez exécuter le processeur frontal (FE) ou la radio définie par logiciel (SDR) directement sur la même instance, ou vous devrez peut-être utiliser des EC2 instances supplémentaires. La sélection et l'installation de votre FE or ne SDR sont pas abordées dans ce guide de l'utilisateur. Pour plus d'informations sur les formats de données spécifiques, consultezAWS Ground Station interfaces de plan de données.

Pour plus d'informations sur nos conditions de service, veuillez consulter les conditions AWS de service.

Logiciel commun fourni

AWS Ground Station fournit des logiciels courants pour faciliter la configuration de votre EC2 instance.

AWS Ground Station Agent

L' AWS Ground Station agent reçoit les données de liaison descendante à fréquence intermédiaire numérique (DigIF) et sort les données déchiffrées qui permettent ce qui suit :

- Capacité de liaison descendante DigiF de 40 à 400 MHz % MHz de bande passante.
- Livraison de données DigiF à haut débit et à faible instabilité vers n'importe quelle adresse IP publique AWS (IP élastique) du réseau. AWS
- Livraison de données fiable grâce à la correction d'erreur directe (FEC).
- Livraison sécurisée des données à l'aide d'une AWS KMS clé de chiffrement gérée par le client.

Pour plus d'informations, consultez le Guide de AWS Ground Station l'utilisateur de l'agent.

Application de point de terminaison Dataflow

Application réseau utilisée pour envoyer et recevoir des données entre les emplacements des AWS Ground Station antennes et vos EC2 instances Amazon. AWS Ground Station Il peut être utilisé pour la liaison montante et la liaison descendante des données.

Radio définie par logiciel (SDR)

Radio définie par logiciel (SDR) qui peut être utilisée pour moduler/démoduler le signal utilisé pour communiquer avec votre satellite.

AWS Ground Station Images de machines Amazon (AMIs)

Pour réduire les temps de construction et de configuration de ces installations, des offres AMIs préconfigurées sont AWS Ground Station également disponibles. L'application réseau AMIs avec un flux de données et une radio définie par logiciel (SDR) sont mises à la disposition de votre compte une fois votre intégration terminée. Vous pouvez les trouver dans la EC2 console Amazon en recherchant Groundstation dans le fichier privé Amazon Machine Images (AMIs). Les AMIs with AWS Ground Station Agent sont publics et peuvent être trouvés dans la EC2 console Amazon en recherchant Groundstation dans les Amazon Machine Images publiques (AMIs).

Contacts

Vous pouvez saisir des données satellites, identifier l'emplacement des antennes, communiquer et planifier l'heure des antennes pour certains satellites à l'aide de la AWS Ground Station console ou AWS SDK dans la langue de votre choix. AWS CLI Vous pouvez consulter, annuler et replanifier les réservations de contact jusqu'à 15 minutes avant le début du contact*. En outre, vous pouvez consulter les détails de votre plan de tarification des minutes réservées si vous utilisez le modèle de tarification des minutes AWS Ground Station réservées.

AWS Ground Station prend en charge la diffusion de données entre régions. Les configurations de point de terminaison de flux de données qui font partie du profil de mission que vous sélectionnez déterminent dans quelle(s) région(s) les données sont diffusées. Pour plus d'informations sur l'utilisation de la livraison de données entre régions, consultezUtilisation de la diffusion de données entre régions.

Pour planifier des contacts, vos ressources doivent être configurées. Si vous n'avez pas configuré vos ressources, consultezMise en route.

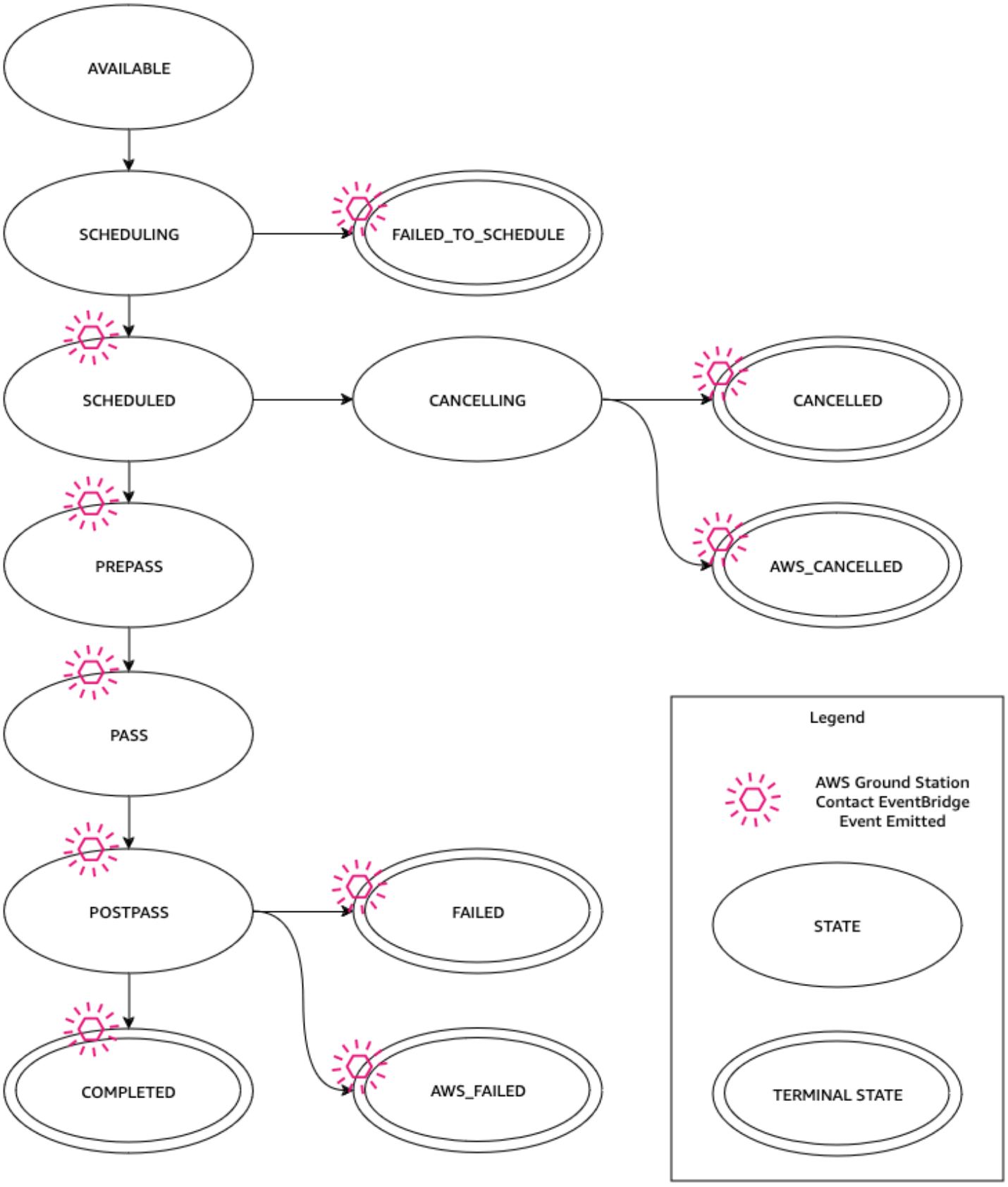
* Les contacts annulés peuvent entraîner des frais s'ils sont annulés trop près du moment du contact. Pour plus d'informations sur les contacts annulés, voir : Ground Station FAQs.

Rubriques

- Cycle de vie des contacts

Cycle de vie des contacts

Comprendre le cycle de vie des contacts peut aider à déterminer comment configurer votre automatisation et lors des efforts de dépannage. Le schéma suivant montre le cycle de vie des AWS Ground Station contacts ainsi que les événements Event Bridge émis au cours du cycle de vie. Il est important de noter que les COMPLETEDFAILED, FAILED _TO_SCHEDULE,CANCELLED, _ et AWS AWS _ CANCELLED FAILED sont des états terminaux. Les contacts ne sortiront pas de l'état terminal. Consultez le AWS Ground Station statuts des contacts pour plus de détails sur ce que chaque statut indique.


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 statuts des contacts

Le statut d'un AWS Ground Station contact donne un aperçu de ce qui arrive à ce contact à un moment donné.

Statuts des contacts

Voici la liste des statuts qu'un contact peut avoir :

- AVAILABLE- Le contact est disponible pour être réservé.
- SCHEDULING- Le contact est en cours de planification.
- SCHEDULED- Le contact a été planifié avec succès.
- FAILED_À_ SCHEDULE - Le contact n'a pas pu être planifié.
- PREPASS- Le contact commence bientôt et les ressources sont en cours de préparation.
- PASS- Le contact est en cours d'exécution et le satellite est en cours de communication.
- POSTPASS- La communication est terminée et les ressources utilisées sont en cours de nettoyage.
- COMPLETED- Le contact s'est terminé sans erreur.
- FAILED- Le contact a échoué en raison d'un problème lié à la configuration de vos ressources.
- AWS_ FAILED - Le contact a échoué en raison d'un problème dans le AWS Ground Station service.
- CANCELLING- Le contact est en cours d'annulation.
- AWS_ CANCELLED - Le contact a été annulé par le AWS Ground Station service. La maintenance de l'antenne ou du site et la dérive des éphémérides sont des exemples de situations où cela peut se produire.
- CANCELLED- Le contact a été annulé par vous.

AWS Ground Station jumeau numérique

La fonction de jumelage numérique pour vous AWS Ground Station fournit un environnement dans lequel vous pouvez tester et intégrer votre logiciel de gestion de mission satellite et de commande et de contrôle. La fonction de jumelage numérique vous permet de tester la planification, la vérification des configurations et la gestion appropriée des erreurs sans utiliser la capacité de l'antenne de production. Le test de votre AWS Ground Station intégration à l'aide de la fonction de jumelage numérique vous permet d'avoir une confiance accrue dans la capacité de votre système à gérer les opérations de vos satellites de manière fluide. Il vous permet également de réaliser des tests AWS Ground Station APIs sans utiliser la capacité de production ni nécessiter de licence de spectre.

Pour commencerÉtape 1 : Intégration du satellite, suivez en demandant à être intégré à la fonction de jumeau numérique. Une fois que votre satellite est intégré à la fonction de jumelage numérique, vous pouvez planifier des contacts avec des stations terrestres à double signal numérique.
La liste des stations au sol auxquelles vous avez accès peut être récupérée via la AWS SDK ListGroundStationsréponse. Les stations terrestres à jumelles numériques sont des copies exactes des stations au sol répertoriées Emplacements avec un préfixe modificateur du nom de la station au sol « Digital Twin ». Cela inclut leurs métadonnées et leurs capacités d'antenne, y compris, mais sans s'y limiter, le masque du site et GPS les coordonnées réelles. À l'heure actuelle, la fonction de jumelage numérique ne prend pas en charge la transmission de données telle que décrite dansFlux de données.

Une fois intégrée, la fonctionnalité Digital Twin émet les mêmes EventBridge événements et API réponses Amazon que le service de production, comme décrit dans. Automatisation AWS Ground Station grâce aux événements Ces événements vous permettront d'affiner vos configurations et vos groupes de points de terminaison de flux de données.

Surveillance

La surveillance est un enjeu important pour assurer la fiabilité, la disponibilité et les performances de AWS Ground Station. AWSfournit les outils de surveillance suivants pour surveiller AWS Ground Station, signaler tout problème et prendre des mesures automatiques le cas échéant.

- AWS EventBridge Les événements fournissent un flux d'événements système en temps quasi réel qui décrivent les modifications apportées aux AWS ressources. EventBridge Les événements permettent une informatique automatisée axée sur les événements, car vous pouvez rédiger des règles qui surveillent certains événements et déclenchent des actions automatisées dans d'autres AWS services lorsque ces événements se produisent. Pour plus d'informations sur les EventBridge événements, consultez le guide de l'utilisateur Amazon EventBridge Events.
- AWS CloudTrailcapture API les appels et les événements connexes effectués par ou pour le compte de votre AWS compte et envoie les fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. Pour plus d'informations AWS CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.
- Amazon CloudWatch Metrics capture les statistiques de vos contacts planifiés lors de l'utilisation AWS Ground Station. CloudWatch Les métriques vous permettent d'analyser les données en fonction de votre canal, de votre polarisation et de l'identifiant du satellite afin d'identifier l'intensité du signal et les erreurs chez vos contacts. Pour plus d'informations, consultez la section Utilisation CloudWatch des métriques Amazon.
- AWS Notifications des utilisateurspeut être utilisé pour configurer des canaux de diffusion afin d'être informé AWS Ground Station des événements. Vous recevez une notification lorsqu'un événement correspond à une règle que vous avez spécifiée. Vous pouvez recevoir des notifications relatives à des événements via plusieurs canaux, notamment des e-mails, des notifications de chat AWS Chatbot ou des notifications push AWS Console Mobile Application. Vous pouvez également consulter les notifications dans le centre de notifications de la AWS console. Notifications des utilisateurs prendre en charge l'agrégation, qui peut réduire le nombre de notifications que vous recevez lors d'événements spécifiques.

Utilisez les rubriques suivantes pour surveiller AWS Ground Station.

Rubriques

- Automatisation AWS Ground Station grâce aux événements

- Enregistrement AWS Ground Station API des appels avec AWS CloudTrail
- Métriques avec Amazon CloudWatch

Automatisation AWS Ground Station grâce aux événements

> **Note**
>
> Le terme « événement » est utilisé partout dans le présent document. CloudWatch Les événements et EventBridge sont le même service sous-jacent etAPI. Les règles permettant de faire correspondre les événements entrants et de les acheminer vers des cibles à des fins de traitement peuvent être établies à l'aide de l'un ou l'autre service.

Les événements vous permettent d'automatiser vos AWS services et de répondre automatiquement aux événements du système tels que les problèmes de disponibilité des applications ou les modifications des ressources. Les événements liés AWS aux services sont diffusés en temps quasi réel. Vous pouvez écrire des règles simples pour indiquer quels événements vous intéressent et les actions automatisées à effectuer quand un événement correspond à une règle. Parmi les actions qui peuvent être déclenchées automatiquement, citons les suivantes :

- Invoquer une fonction AWS Lambda
- Invocation de la commande Amazon EC2 Run
- Relais de l'événement à Amazon Kinesis Data Streams
- Activation d'une machine à AWS Step Functions états
- Notification d'un SNS sujet Amazon ou d'une file d'attente Amazon SQS

Voici quelques exemples d'utilisation d'événements avec AWS Ground Station :

- Invocation d'une fonction Lambda pour automatiser le démarrage et l'arrêt des instances EC2 Amazon en fonction de l'état de l'événement.
- Publier sur un SNS sujet Amazon chaque fois qu'un contact change d'état. Ces rubriques peuvent être configurées pour envoyer des notifications par e-mail au début ou à la fin des contacts.

Pour plus d'informations, consultez le guide de l'utilisateur d'Amazon EventBridge Events.

AWS Ground Station Types d'événements

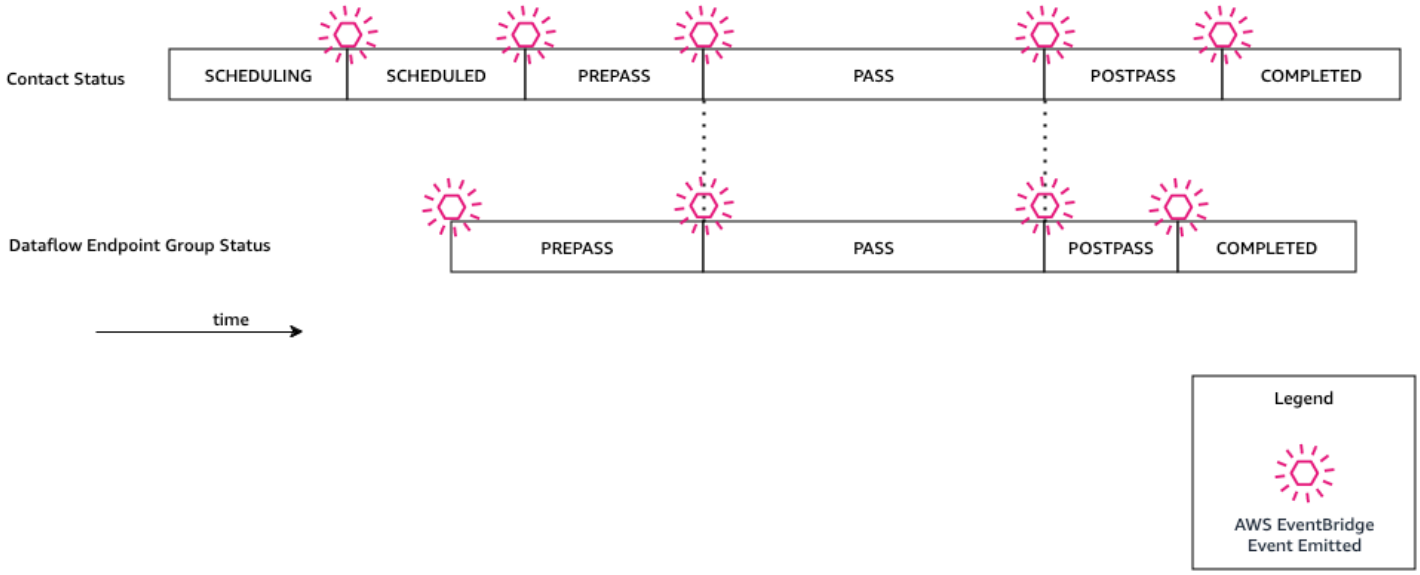
> **Note**
>
> La valeur « source » de tous les événements générés par AWS Ground Station est « aws.groundstation ».

AWS Ground Station émet des événements liés aux changements d'état pour vous permettre de personnaliser votre automatisation. Actuellement, AWS Ground Station prend en charge les événements de changement d'état des contacts, les événements de modification du groupe de points de terminaison du flux de données et les événements de changement d'état des éphémérides. Les sections suivantes fournissent des informations détaillées sur chaque type.

Chronologie des événements de contact

AWS Ground Station émet des événements lorsque votre contact change d'état. Pour plus d'informations sur la nature de ces changements d'État et sur la signification des États eux-mêmes, voirCycle de vie des contacts. Tous les groupes de points de terminaison de flux de données utilisés dans votre contact sont associés à un ensemble indépendant d'événements qui sont également émis. Au cours de cette même période, nous émettons également des événements pour votre groupe de points de terminaison de flux de données. Vous pouvez configurer l'heure précise des événements avant et après le passage lorsque vous configurez votre profil de mission et votre groupe de points de terminaison de flux de données.

Le schéma suivant montre les statuts et les événements émis pour un contact nominal et son groupe de points de terminaison de flux de données associé.



Modification de l'état d'un contact Ground Station

Si vous souhaitez effectuer une action spécifique lorsqu'un prochain contact change d'état, vous pouvez définir une règle pour automatiser cette action. Ceci est utile lorsque vous souhaitez recevoir des notifications sur les changements d'état de votre contact. Si vous souhaitez modifier le moment où vous recevez ces événements, vous pouvez modifier le profil de votre mission contactPrePassDurationSecondset contactPostPassDurationSeconds. Les événements sont envoyés à la région à partir de laquelle le contact a été planifié.

Un exemple d'événement est fourni ci-dessous.

```
{
    "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"
}
```

Les valeurs possibles pour `contactStatus` sont définies dansthe section called "AWS Ground Station statuts des contacts".

Modification de l'état du groupe de points de terminaison du flux de données Ground Station

Si vous souhaitez effectuer une action lorsque votre groupe de points de terminaison de flux de données est utilisé pour recevoir des données, vous pouvez configurer une règle pour automatiser cette action. Cela vous permettra d'effectuer différentes actions en réponse aux états changeants du groupe de points de terminaison de flux de données. Si vous souhaitez modifier le moment où vous recevez ces événements, utilisez un groupe de points de terminaison de flux de données avec un et différent contactPrePassDurationSeconds. contactPostPassDurationSeconds Cet événement sera envoyé à la région du groupe de points de terminaison de flux de données.

Vous trouverez un exemple ci-dessous.

```
{
    "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"
}
```

Les états possibles pour `dataflowEndpointGroupState` sont : `PREPASS`, `PASS`, `POSTPASS` et `COMPLETED`.

Événements Ephemeris

Changement d'état des éphémérides de la station au sol

Si vous souhaitez effectuer une action lorsqu'une éphéméride change d'état, vous pouvez définir une règle pour automatiser cette action. Cela vous permet d'effectuer différentes actions en réponse au changement d'état d'une éphéméride. Par exemple, vous pouvez effectuer une action lorsque la validation d'une éphéméride est terminée, et c'est maintenant le cas. `ENABLED` La notification de cet événement sera envoyée à la région où les éphémérides ont été téléchargées.

Vous trouverez un exemple ci-dessous.

```
    {
    "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"
    }
    }
```

Les états possibles pour les `ephemerisStatus` incluent `ENABLEDVALIDATING`,`INVALID`,`ERROR`,`DISABLED`, `EXPIRED`

Enregistrement AWS Ground Station API des appels avec AWS CloudTrail

AWS Ground Station est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans AWS Ground Station. CloudTrail capture tous les API appels AWS Ground Station sous forme d'événements. Les appels capturés incluent des appels provenant de la AWS Ground Station console et des appels de code vers les AWS Ground Station API opérations. Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris les événements pour AWS Ground Station. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite AWS Ground Station, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des détails supplémentaires.

Pour en savoir plus CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

AWS Ground Station Informations dans CloudTrail

CloudTrail est activé sur votre AWS compte lorsque vous le créez. Lorsqu'une activité se produit dans AWS Ground Station, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votre AWS compte. Pour plus d'informations, consultez la section Affichage des événements avec l'historique des CloudTrail événements.

Pour un enregistrement continu des événements de votre AWS compte, y compris des événements pour AWS Ground Station, créez un parcours. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un parcours dans la console, celui-ci s'applique à toutes les AWS régions. Le journal enregistre les événements de toutes les

régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

- Vue d'ensemble de la création d'un journal d'activité
- CloudTrail Services et intégrations pris en charge
- Configuration des SNS notifications Amazon pour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs régions et réception de fichiers CloudTrail journaux de plusieurs comptes

Toutes les AWS Ground Station actions sont enregistrées CloudTrail et documentées dans la AWS Ground Station APIréférence. Par exemple, les appels au `ReserveContact` `CancelContact` et les `ListConfigs` actions génèrent des entrées dans les fichiers CloudTrail journaux.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été faite avec les informations d'identification de l'utilisateur root ou AWS Identity and Access Management (IAM).
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la demande a été faite par un autre AWS service.

Pour plus d'informations, consultez l'CloudTrail userIdentityélément.

Comprendre les entrées du fichier AWS Ground Station journal

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des API appels publics, ils n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'`ReserveContact`action.

Exemple : 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"
}
```


Métriques avec Amazon CloudWatch

Lors d'un contact, capture et envoie AWS Ground Station automatiquement les données à des CloudWatch fins d'analyse. Vos données peuvent être consultées dans la CloudWatch console Amazon. Pour plus d'informations sur l'accès et CloudWatch les métriques, consultez Using Amazon CloudWatch Metrics.

AWS Ground Station Métriques et dimensions

Quelles métriques sont disponibles ?

Les statistiques suivantes sont disponibles auprès de AWS Ground Station.

> **Note**
>
> Les métriques spécifiques émises dépendent des AWS Ground Station capacités utilisées. Selon votre configuration, seul un sous-ensemble des métriques ci-dessous peut être émis.

Métrique	Dimensions métriques	Description
`AzimuthAngle`	SatelliteId	Angle d'azimut de l'antenne. Le nord réel est à 0 degré et l'est à 90 degrés. Unités : degrés
`BitErrorRate`	Canal, Polarisation, SatelliteId	Le taux d'erreur sur les bits dans un nombre

Métrique	Dimensions métriques	Description
		donné de transmissions binaires. Les erreurs de bits sont causées par le bruit, la distorsion ou les interférences Unités : erreurs de bits par unité de temps
`BlockErrorRate`	Canal, Polarisation, SatelliteId	Taux d'erreur de blocs dans un nombre donné de blocs reçus. Les erreurs de blocs sont causées par des interférences. Unités : blocs erronés/Nombre total de blocs
`CarrierFrequencyRecovery_Cn0`	Catégorie, Config, SatelliteId	Rapport entre le support et la densité du bruit par unité de bande passante. Unités : décibel-Hertz (dB-Hz)

Métrique	Dimensions métriques	Description
`CarrierFrequencyRecovery_Locked`	Catégorie, Config, SatelliteId	Réglé sur 1 lorsque la boucle de récupération de fréquence porteuse du démodulateur est verrouillée et sur 0 lorsqu'elle est déverrouillée. Unités : sans unité
`CarrierFrequencyRecovery_OffsetFrequency_Hz`	Catégorie, Config, SatelliteId	Le décalage entre le centre du signal estimé et la fréquence centrale idéale. Cela est dû au décalage Doppler et au décalage de l'oscillateur local entre le vaisseau spatial et le système d'antenne. Unités : hertz (Hz)

Métrique	Dimensions métriques	Description
`ElevationAngle`	SatelliteId	Angle d'élévation de l'antenne. L'horizon est de 0 degré et le zénith de 90 degrés. Unités : degrés
`Es/N0`	Canal, Polarisation, SatelliteId	Rapport entre l'énergie par symbole et la densité spectrale de puissance du bruit. Unités : décibels (dB)
`ReceivedPower`	Polarisation, SatelliteId	La puissance du signal mesurée dans le démodulateur/décodeur. Unités : décibels par rapport aux milliwatts () dBm

Métrique	Dimensions métriques	Description
`SymbolTimingRecovery_ErrorVectorMagnitude`	Catégorie, Config, SatelliteId	L'amplitude du vecteur d'erreur entre les symboles reçus et les points de constellation idéaux. Unités : pourcentage
`SymbolTimingRecovery_Locked`	Catégorie, Config, SatelliteId	Réglé sur 1 lorsque le symbole du démodulateur (chronomé trage, boucle de restauration) est verrouillé et sur 0 lorsqu'il est déverrouillé. Unités : sans unité

Métrique	Dimensions métriques	Description
`SymbolTimingRecovery_OffsetSymbolRate`	Catégorie, Config, SatelliteId	Le décalage entre le débit de symboles estimé et le taux de symboles de signal idéal. Cela est dû au décalage Doppler et au décalage de l'oscillateur local entre le vaisseau spatial et le système d'antenne. Unités : symboles/seconde

Quelles sont les dimensions utilisées AWS Ground Station ?

Vous pouvez filtrer AWS Ground Station les données à l'aide des dimensions suivantes.

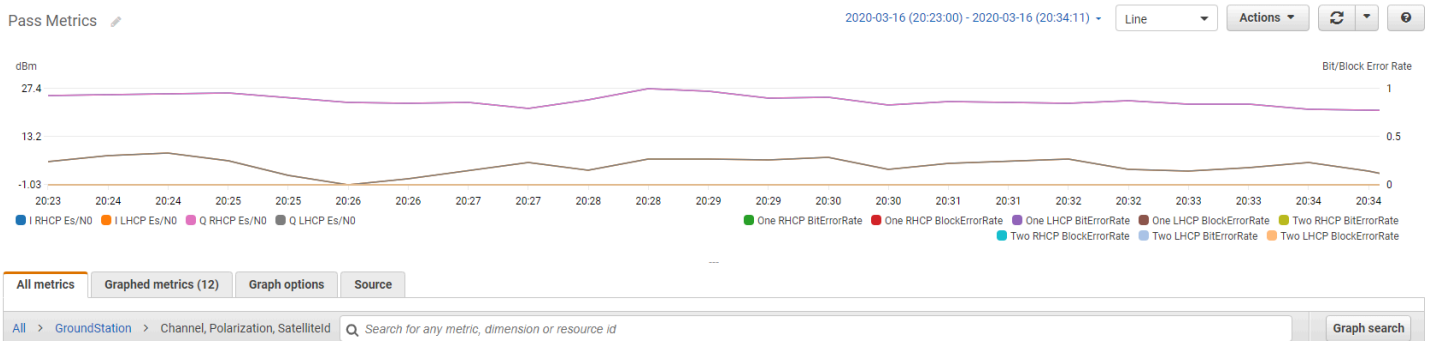
Dimension	Description
`Category`	Démodulation ou décodage.
`Channel`	Les canaux de chaque contact incluent Un, Deux, I (en phase) et Q (quadrature).
`Config`	Une démo d'antenne en liaison descendante décode la configuration arn.

Dimension	Description
`Polarization`	La polarisation de chaque contact inclut LHCP (polarisation circulaire gauche) ou RHCP (polarisa tion circulaire droite).
`SatelliteId`	L'identifiant du satellite contient le numéro ARN du satellite pour vos contacts.

Affichage des métriques

Lors de l'affichage des métriques dans un graphique, il est important de noter que la fenêtre d'agrégation détermine la façon dont vos métriques seront affichées. Chaque métrique d'un contact peut être affichée sous forme de données par seconde pendant 3 heures après la réception des données. Vos données seront agrégées par CloudWatch Metrics sous forme de données par minute une fois cette période de 3 heures écoulée. Si vous devez consulter vos statistiques sur une mesure de données par seconde, il est recommandé de consulter vos données dans les 3 heures suivant leur réception ou de les conserver en dehors des CloudWatch métriques. Pour plus d'informations sur la CloudWatch rétention, consultez Amazon CloudWatch Concepts - Concepts - Conservation métrique.

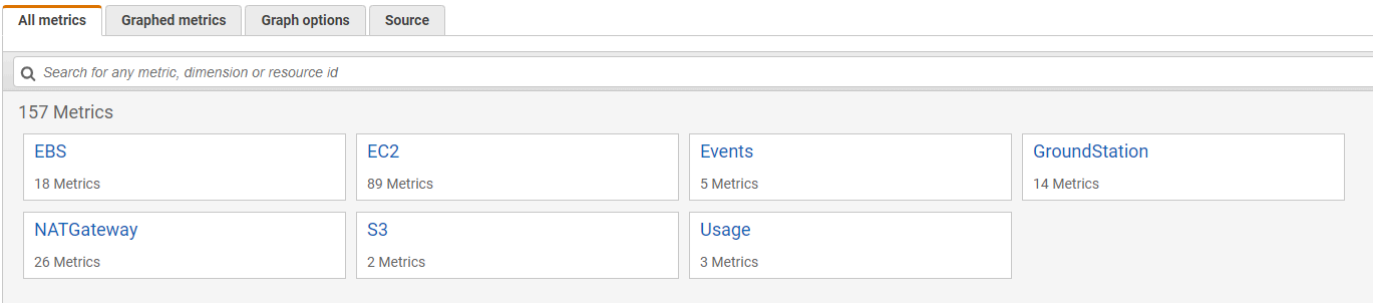
De plus, toutes les données capturées au cours des 60 premières secondes ne contiendront pas suffisamment d'informations pour produire des métriques significatives et ne seront probablement pas affichées. Pour afficher des métriques significatives, il est recommandé d'afficher vos données après 60 secondes.



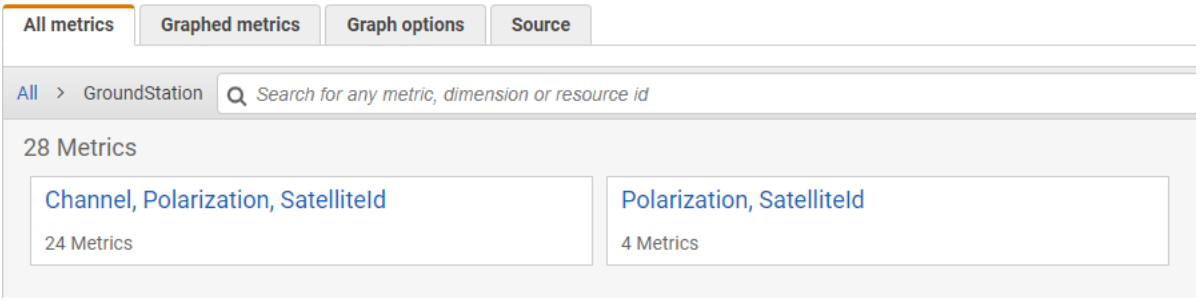
Pour plus d'informations sur la représentation graphique des AWS Ground Station métriques CloudWatch, consultez la section Représentation graphique des métriques.

Pour afficher des métriques à l'aide de la console

1. Ouvrez la CloudWatch console.
2. Dans le panneau de navigation, sélectionnez Métriques.
3. Sélectionnez l'espace de noms GroundStation.



4. Sélectionnez les dimensions métriques souhaitées (par exemple, canal, polarisation, SatelliteId).



5. L'onglet All metrics (Toutes les métriques) affiche toutes les métriques pour cette dimension dans l'espace de noms. Vous pouvez effectuer les actions suivantes :

   a. Pour trier le tableau, utilisez l'en-tête de colonne.

   b. Pour représenter graphiquement une métrique, cochez la case associée à la métrique. Pour sélectionner toutes les mesures, cochez la case dans la ligne d'en-tête du tableau.

   c. Pour filtrer par ressource, sélectionnez l'ID de ressource, puis Add to search.

   d. Pour filtrer par métrique, choisissez le nom de la métrique, puis Add to search (Ajouter à la recherche).

Pour consulter les métriques à l'aide de AWS CLI

1. Assurez-vous qu'il AWS CLI est installé. Pour plus d'informations sur l'installation AWS CLI, voir Installation de la AWS CLI version 2.

2. Utilisez la get-metric-dataméthode du CloudWatch CLI pour générer un fichier qui peut être modifié pour spécifier les métriques qui vous intéressent, puis être utilisé pour rechercher ces métriques.

   Pour ce faire, exécutez ce qui suit :`aws cloudwatch get-metric-data --generate-cli-skeleton`. Cela générera un résultat similaire à :

```
{
   "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. Répertoriez CloudWatch les métriques disponibles en exécutant`aws cloudwatch list-metrics`.

   Si vous l'avez récemment utilisée AWS Ground Station, la méthode doit renvoyer une sortie contenant des entrées telles que :

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

   > **Note**
   >
   > En raison d'une limitation de CloudWatch, si plus de 2 semaines se sont écoulées depuis votre dernière utilisation AWS Ground Station, vous devrez inspecter manuellement le tableau des métriques disponibles pour trouver les noms et les dimensions des métriques dans l'espace de noms des `AWS/GroundStation` métriques. Pour plus d'informations sur la CloudWatch limitation, voir : Afficher les métriques disponibles

4. Modifiez le JSON fichier que vous avez créé à l'étape 2 pour qu'il corresponde aux valeurs requises à l'étape 3, par exemple`SatelliteId`, et `Polarization` à partir de vos indicateurs. Veillez également à mettre à jour les `StartTime` `EndTime` valeurs et pour qu'elles correspondent à celles de votre contact. Par exemple :

```
        {
           "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 publie des métriques toutes les 1 à 60 secondes, selon la métrique. Les métriques ne seront pas renvoyées si le `Period` champ a une valeur inférieure à la période de publication de la métrique.

5. Exécutez `aws cloudwatch get-metric-data` avec le fichier de configuration créé lors des étapes précédentes. Vous trouverez un exemple ci-dessous.

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

Les métriques seront fournies avec des horodatages de votre contact. Un exemple de sortie de AWS Ground Station métriques est fourni ci-dessous.


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

Sécurité dans AWS Ground Station

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficierez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité. AWSfournit des outils et des fonctionnalités spécifiques à la sécurité pour vous aider à atteindre vos objectifs de sécurité. Ces outils et fonctionnalités incluent la sécurité du réseau, la gestion de la configuration, le contrôle d'accès et la sécurité des données.

Lors de l'utilisation AWS Ground Station, nous vous recommandons de suivre les meilleures pratiques du secteur et de mettre en œuvre end-to-end le chiffrement. AWSvous permet APIs d'intégrer le chiffrement et la protection des données. Pour plus d'informations sur AWS la sécurité, consultez le livre blanc Introduction à AWS la sécurité.

Consultez les rubriques suivantes pour apprendre à sécuriser vos ressources .

Rubriques

Identity and Access Management pour AWS Ground Station

AWS Identity and Access Management (IAM) est un outil AWS service qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. IAMles administrateurs contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les AWS Ground Station ressources. IAMest un AWS service outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

- Exemples de politiques basées sur l'identité pour AWS Ground Station
- Résolution des problèmes AWS Ground Station d'identité et d'accès

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez AWS Ground Station.

Utilisateur du service : si vous utilisez le AWS Ground Station service pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de nouvelles AWS Ground Station fonctionnalités pour effectuer votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une fonctionnalité dans AWS Ground Station, consultez Résolution des problèmes AWS Ground Station d'identité et d'accès.

Administrateur du service — Si vous êtes responsable des AWS Ground Station ressources de votre entreprise, vous avez probablement un accès complet à AWS Ground Station. C'est à vous de déterminer les AWS Ground Station fonctionnalités et les ressources auxquelles les utilisateurs de votre service doivent accéder. Vous devez ensuite envoyer des demandes à votre IAM administrateur pour modifier les autorisations des utilisateurs de votre service. Consultez les informations de cette page pour comprendre les concepts de base deIAM. Pour en savoir plus sur la façon dont votre entreprise peut utiliser IAM avec AWS Ground Station, voirComment AWS Ground Station fonctionne avec IAM.

IAMadministrateur — Si vous êtes IAM administrateur, vous souhaiterez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès à AWS Ground Station. Pour consulter des exemples de politiques AWS Ground Station basées sur l'identité que vous pouvez utiliser dansIAM, consultez. Exemples de politiques basées sur l'identité pour AWS Ground Station

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant que Utilisateur racine d'un compte AWS, en tant qu'IAMutilisateur ou en assumant un IAM rôle.

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAMIdentity Center), l'authentification unique de votre entreprise et vos informations d'identification

Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez en tant qu'identité fédérée, votre administrateur a préalablement configuré la fédération d'identité à l'aide de IAM rôles. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez Comment vous connecter à votre compte Compte AWS dans le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer vous-même les demandes, consultez la section Signature des AWS API demandes dans le guide de IAM l'utilisateur.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir plus, consultez Authentification multifactorielle dans le guide de AWS IAM Identity Center l'utilisateur et Utilisation de l'authentification multifactorielle (MFA) AWS dans le guide de l'IAMutilisateur.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes AWS services les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui nécessitent que vous vous connectiez en tant qu'utilisateur root, consultez la section Tâches nécessitant des informations d'identification utilisateur root dans le guide de IAM l'utilisateur.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide AWS services d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies AWS services par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour plus d'informations sur IAM Identity Center, consultez Qu'est-ce qu'IAMIdentity Center ? dans le guide de AWS IAM Identity Center l'utilisateur.

Utilisateurs et groupes IAM

Un IAMutilisateur est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou une seule application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des IAM utilisateurs dotés d'informations d'identification à long terme, telles que des mots de passe et des clés d'accès. Toutefois, si vous avez des cas d'utilisation spécifiques qui nécessitent des informations d'identification à long terme auprès des IAM utilisateurs, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, voir Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification à long terme dans le Guide de IAM l'utilisateur.

Un IAMgroupe est une identité qui définit un ensemble d'IAMutilisateurs. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez nommer un groupe IAMAdminset lui donner les autorisations nécessaires pour administrer IAM des ressources.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, voir Quand créer un IAM utilisateur (au lieu d'un rôle) dans le Guide de IAM l'utilisateur.

IAMrôles

Un IAMrôle est une identité au sein de Compte AWS vous dotée d'autorisations spécifiques. Il est similaire à un IAM utilisateur, mais n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un IAM rôle dans le en AWS Management Console changeant de rôle. Vous pouvez assumer un rôle en appelant une AWS API opération AWS CLI or ou en utilisant une option personnaliséeURL. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez la section Utilisation IAM des rôles dans le Guide de IAM l'utilisateur.

IAMles rôles dotés d'informations d'identification temporaires sont utiles dans les situations suivantes :

- Accès utilisateur fédéré – Pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour plus d'informations sur les rôles pour la fédération, voir Création d'un rôle pour un fournisseur d'identité tiers dans le guide de IAM l'utilisateur. Si vous utilisez IAM Identity Center, vous configurez un ensemble d'autorisations. Pour contrôler les accès auxquels vos identités peuvent accéder après leur authentification, IAM Identity Center met en corrélation l'ensemble d'autorisations avec un rôle dans. IAM Pour plus d'informations sur les jeux d'autorisations, consultez la rubrique Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .
- Autorisations IAM utilisateur temporaires : un IAM utilisateur ou un rôle peut assumer un IAM rôle afin d'obtenir temporairement différentes autorisations pour une tâche spécifique.
- Accès entre comptes : vous pouvez utiliser un IAM rôle pour autoriser une personne (un mandant fiable) d'un autre compte à accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains AWS services cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour connaître la différence entre les rôles et les politiques basées sur les ressources pour l'accès entre comptes, voir Accès aux ressources entre comptes IAM dans le guide de l'IAMutilisateur.
- Accès multiservices — Certains AWS services utilisent des fonctionnalités dans d'autres AWS services. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
  - Sessions d'accès transmises (FAS) — Lorsque vous utilisez un IAM utilisateur ou un rôle pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre

service. FASutilise les autorisations du principal appelant an AWS service, combinées à la demande AWS service pour adresser des demandes aux services en aval. FASles demandes ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes AWS services ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur les politiques relatives FAS aux demandes, consultez la section Transférer les sessions d'accès.

- Rôle de service — Un rôle de service est un IAMrôle qu'un service assume pour effectuer des actions en votre nom. Un IAM administrateur peut créer, modifier et supprimer un rôle de service de l'intérieurIAM. Pour plus d'informations, consultez la section Création d'un rôle auquel déléguer des autorisations AWS service dans le Guide de IAM l'utilisateur.
- Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. AWS service Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés au service apparaissent dans votre Compte AWS fichier et appartiennent au service. Un IAM administrateur peut consulter, mais pas modifier les autorisations pour les rôles liés à un service.

- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un IAM rôle pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une EC2 instance et qui font AWS CLI des AWS API demandes. Cela est préférable au stockage des clés d'accès dans l'EC2instance. Pour attribuer un AWS rôle à une EC2 instance et le rendre disponible pour toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes exécutés sur l'EC2instance d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez la section Utilisation d'un IAM rôle pour accorder des autorisations aux applications exécutées sur des EC2 instances Amazon dans le Guide de IAM l'utilisateur.

Pour savoir s'il faut utiliser IAM des rôles ou des IAM utilisateurs, voir Quand créer un IAM rôle (au lieu d'un utilisateur) dans le guide de IAM l'utilisateur.

Gestion des accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de JSON documents. Pour plus d'informations sur la structure et le contenu

des documents de JSON politique, voir Présentation des JSON politiques dans le guide de IAM l'utilisateur.

Les administrateurs peuvent utiliser AWS JSON des politiques pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour autoriser les utilisateurs à effectuer des actions sur les ressources dont ils ont besoin, un IAM administrateur peut créer des IAM politiques. L'administrateur peut ensuite ajouter les IAM politiques aux rôles, et les utilisateurs peuvent assumer les rôles.

IAMles politiques définissent les autorisations pour une action, quelle que soit la méthode que vous utilisez pour effectuer l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur doté de cette politique peut obtenir des informations sur le rôle auprès du AWS Management Console AWS CLI, ou du AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont JSON des documents de politique d'autorisation que vous pouvez joindre à une identité, telle qu'un IAM utilisateur, un groupe d'utilisateurs ou un rôle. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour savoir comment créer une politique basée sur l'identité, voir Création de IAM politiques dans le Guide de l'IAMutilisateur.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour savoir comment choisir entre une politique gérée ou une politique intégrée, voir Choisir entre des politiques gérées et des politiques intégrées dans le Guide de l'IAMutilisateur.

Politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents JSON de stratégie que vous attachez à une ressource. Les politiques de confiance dans les IAM rôles et les politiques relatives aux compartiments Amazon S3 sont des exemples de politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans

laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. AWS services

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser de politiques AWS gérées depuis une IAM stratégie basée sur les ressources.

Listes de contrôle d'accès (ACLs)

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLssont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format du document JSON de stratégie.

Amazon S3 et Amazon VPC sont des exemples de services compatiblesACLs. AWS WAF Pour en savoir plusACLs, consultez la présentation de la liste de contrôle d'accès (ACL) dans le guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limites d'autorisations — Une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une IAM entité (IAMutilisateur ou rôle). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus d'informations sur les limites d'autorisations, voir Limites d'autorisations pour les IAM entités dans le Guide de IAM l'utilisateur.
- Politiques de contrôle des services (SCPs) : SCPs JSON politiques qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans AWS Organizations. AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer des politiques de contrôle des services (SCPs) à l'un ou à l'ensemble de vos comptes. Les SCP limites d'autorisations pour les entités

présentes dans les comptes des membres, y compris chacune d'entre elles Utilisateur racine d'un compte AWS. Pour plus d'informations sur les Organizations et consultez SCPs les politiques de contrôle des services dans le Guide de AWS Organizations l'utilisateur.

- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez la section Politiques de session dans le guide de IAM l'utilisateur.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de IAM l'utilisateur.

Comment AWS Ground Station fonctionne avec IAM

Avant IAM de gérer l'accès à AWS Ground Station, découvrez quelles IAM fonctionnalités sont disponibles AWS Ground Station.

IAMfonctionnalités que vous pouvez utiliser avec AWS Ground Station

IAMfonctionnalité	AWS Ground Station soutien
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique (spécifiques au service)	Oui

IAMfonctionnalité	AWS Ground Station soutien
ACLs	Non
ABAC(balises dans les politiques)	Oui
Informations d'identification temporaires	Oui
Autorisations de principal	Oui
Fonctions du service	Non
Rôles liés à un service	Oui

Pour obtenir une vue d'ensemble de la façon dont AWS Ground Station les autres AWS services fonctionnent avec la plupart des IAM fonctionnalités, consultez la section AWS Services compatibles IAM dans le Guide de IAM l'utilisateur.

Politiques basées sur l'identité pour AWS Ground Station

Prend en charge les politiques basées sur l'identité : oui

Les politiques basées sur l'identité sont JSON des documents de politique d'autorisation que vous pouvez joindre à une identité, telle qu'un IAM utilisateur, un groupe d'utilisateurs ou un rôle. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour savoir comment créer une politique basée sur l'identité, voir Création de IAM politiques dans le Guide de l'IAMutilisateur.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier les actions et les ressources autorisées ou refusées ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. Pour en savoir plus sur tous les éléments que vous pouvez utiliser dans une JSON politique, consultez la référence aux éléments de IAM JSON politique dans le Guide de IAM l'utilisateur.

Exemples de politiques basées sur l'identité pour AWS Ground Station

Pour consulter des exemples de politiques AWS Ground Station basées sur l'identité, consultez. Exemples de politiques basées sur l'identité pour AWS Ground Station

Politiques basées sur les ressources au sein de AWS Ground Station

Prend en charge les politiques basées sur les ressources : non

Les politiques basées sur les ressources sont des documents JSON de stratégie que vous attachez à une ressource. Les politiques de confiance dans les IAM rôles et les politiques relatives aux compartiments Amazon S3 sont des exemples de politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. AWS services

Pour activer l'accès entre comptes, vous pouvez spécifier un compte entier ou IAM des entités d'un autre compte comme principal dans une politique basée sur les ressources. L'ajout d'un principal entre comptes à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un IAM administrateur du compte de confiance doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, voir Accès aux ressources entre comptes IAM dans le Guide de IAM l'utilisateur.

Actions politiques pour AWS Ground Station

Prend en charge les actions de politique : oui

Les administrateurs peuvent utiliser AWS JSON des politiques pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'`Action`élément d'une JSON politique décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès dans une politique. Les actions de stratégie portent généralement le même nom que l' AWS APIopération associée. Il existe certaines exceptions, telles que les actions avec autorisation uniquement qui n'ont pas d'opération correspondante. API Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une stratégie afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des AWS Ground Station actions, voir Actions définies par AWS Ground Station dans la référence d'autorisation de service.

Les actions de politique en AWS Ground Station cours utilisent le préfixe suivant avant l'action :

```
groundstation
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

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

Pour consulter des exemples de politiques AWS Ground Station basées sur l'identité, consultez. Exemples de politiques basées sur l'identité pour AWS Ground Station

Ressources politiques pour AWS Ground Station

Prend en charge les ressources de politique : oui

Les administrateurs peuvent utiliser AWS JSON des politiques pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Resource` JSON de stratégie indique le ou les objets auxquels s'applique l'action. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de spécifier une ressource en utilisant son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

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

Pour consulter la liste des types de AWS Ground Station ressources et leurs caractéristiquesARNs, consultez la section Ressources définies par AWS Ground Station dans la référence d'autorisation de service. Pour savoir avec quelles actions vous pouvez spécifier pour chaque ressource, consultez la ARN section Actions définies par AWS Ground Station.

Pour consulter des exemples de politiques AWS Ground Station basées sur l'identité, consultez. Exemples de politiques basées sur l'identité pour AWS Ground Station

Clés de conditions de politique pour AWS Ground Station

Prend en charge les clés de condition de politique spécifiques au service : oui

Les administrateurs peuvent utiliser AWS JSON des politiques pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une `OR` opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez autoriser un IAM utilisateur à accéder à une ressource uniquement si celle-ci est étiquetée avec son nom IAM d'utilisateur. Pour plus d'informations, consultez IAMla section Éléments de politique : variables et balises dans le Guide de IAM l'utilisateur.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés contextuelles de condition AWS globales dans le guide de IAM l'utilisateur.

Pour consulter la liste des clés de AWS Ground Station condition, voir Clés de condition pour AWS Ground Station la référence d'autorisation de service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez la section Actions définies par AWS Ground Station.

Pour consulter des exemples de politiques AWS Ground Station basées sur l'identité, consultez. Exemples de politiques basées sur l'identité pour AWS Ground Station

ACLsdans AWS Ground Station

Supports ACLs : Non

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLssont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format du document JSON de stratégie.

ABACavec AWS Ground Station

Supports ABAC (balises dans les politiques) : Oui

Le contrôle d'accès basé sur les attributs (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises à IAM des entités (utilisateurs ou rôles) et à de nombreuses AWS ressources. Le balisage des entités et des ressources est la première étape deABAC. Vous concevez ensuite des ABAC politiques pour autoriser les opérations lorsque le tag du principal correspond à celui de la ressource à laquelle il essaie d'accéder.

ABACest utile dans les environnements qui se développent rapidement et aide dans les situations où la gestion des politiques devient fastidieuse.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informationsABAC, voir Qu'est-ce que c'est ABAC ? dans le guide de IAM l'utilisateur. Pour consulter un didacticiel présentant les étapes de configurationABAC, voir Utiliser le contrôle d'accès basé sur les attributs (ABAC) dans le guide de l'IAMutilisateur.

Utilisation d'informations d'identification temporaires avec AWS Ground Station

Prend en charge les informations d'identification temporaires : oui

Certains AWS services ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui AWS services fonctionnent avec des informations d'identification temporaires, consultez AWS services la section relative à l'utilisation IAM dans le Guide de IAM l'utilisateur.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez la section Passage à un rôle (console) dans le guide de IAM l'utilisateur.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide du AWS CLI ou AWS API. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez la section Informations d'identification de sécurité temporaires dans IAM.

Autorisations principales interservices pour AWS Ground Station

Prend en charge les sessions d'accès transféré (FAS) : Oui

Lorsque vous utilisez un IAM utilisateur ou un rôle pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FASutilise les autorisations du principal appelant an AWS service, combinées à la demande AWS service pour adresser des demandes aux services en aval. FASles demandes ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes AWS services ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur les politiques relatives FAS aux demandes, consultez la section Transférer les sessions d'accès.

Rôles de service pour AWS Ground Station

Supporte les rôles de service : Non

Un rôle de service est un IAMrôle qu'un service assume pour effectuer des actions en votre nom. Un IAM administrateur peut créer, modifier et supprimer un rôle de service de l'intérieurIAM. Pour plus d'informations, consultez la section Création d'un rôle auquel déléguer des autorisations AWS service dans le Guide de IAM l'utilisateur.

> **Warning**
>
> La modification des autorisations associées à un rôle de service peut perturber AWS Ground Station les fonctionnalités. Modifiez les rôles de service uniquement lorsque AWS Ground Station vous recevez des instructions à cet effet.

Rôles liés à un service pour AWS Ground Station

Prend en charge les rôles liés aux services : Oui

Un rôle lié à un service est un type de rôle de service lié à un. AWS service Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés au service apparaissent dans votre Compte AWS fichier et appartiennent au service. Un IAM administrateur peut consulter, mais pas modifier les autorisations pour les rôles liés à un service.

Pour plus de détails sur la création ou la gestion des rôles liés à un service, consultez la section AWS Services compatibles avec. IAM Recherchez un service dans le tableau qui inclut un `Yes` dans la colonne Rôle lié à un service. Choisissez le lien Oui pour consulter la documentation du rôle lié à ce service.

Exemples de politiques basées sur l'identité pour AWS Ground Station

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou modifier les ressources AWS Ground Station . Ils ne peuvent pas non plus effectuer de tâches en utilisant le AWS Management Console, AWS Command Line Interface (AWS CLI) ou AWS API. Pour autoriser les utilisateurs à effectuer des actions sur les ressources dont ils ont besoin, un IAM administrateur peut créer des IAM politiques. L'administrateur peut ensuite ajouter les IAM politiques aux rôles, et les utilisateurs peuvent assumer les rôles.

Pour savoir comment créer une politique IAM basée sur l'identité à l'aide de ces exemples de documents de JSON stratégie, consultez la section Création de IAM politiques dans le guide de l'IAMutilisateur.

Pour plus de détails sur les actions et les types de ressources définis par AWS Ground Station, y compris le format de ARNs pour chacun des types de ressources, voir Actions, ressources et clés de condition AWS Ground Station dans la référence d'autorisation de service.

Rubriques

- Bonnes pratiques en matière de politiques
- Utilisation de la console AWS Ground Station
- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer AWS Ground Station des ressources dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez les politiques AWS gérées ou les politiques AWS gérées pour les fonctions professionnelles dans le Guide de IAM l'utilisateur.
- Appliquer les autorisations du moindre privilège : lorsque vous définissez des autorisations à IAM l'aide de politiques, accordez uniquement les autorisations nécessaires à l'exécution d'une tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation IAM pour appliquer des autorisations, consultez la section Politiques et autorisations du Guide de IAM l'utilisateur. IAM
- Utilisez des conditions dans IAM les politiques pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques pour limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez rédiger une condition de politique pour spécifier que toutes les demandes

doivent être envoyées en utilisantSSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique AWS service, tel que AWS CloudFormation. Pour plus d'informations, voir Éléments IAM JSON de politique : Condition dans le guide de IAM l'utilisateur.

- Utilisez IAM Access Analyzer pour valider vos IAM politiques afin de garantir des autorisations sécurisées et fonctionnelles. IAM Access Analyzer valide les politiques nouvelles et existantes afin qu'elles soient conformes au langage des IAM politiques (JSON) et IAM aux meilleures pratiques. IAMAccess Analyzer fournit plus de 100 vérifications des politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez la section Validation des politiques d'IAMAccess Analyzer dans le guide de IAM l'utilisateur.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des IAM utilisateurs ou un utilisateur root Compte AWS, activez-le MFA pour une sécurité supplémentaire. Pour exiger le MFA moment où les API opérations sont appelées, ajoutez MFA des conditions à vos politiques. Pour plus d'informations, consultez la section Configuration de l'APIaccès MFA protégé dans le Guide de l'IAMutilisateur.

Pour plus d'informations sur les meilleures pratiques en matière de sécuritéIAM, consultez la section Bonnes pratiques en matière de sécurité IAM dans le Guide de IAM l'utilisateur.

Utilisation de la console AWS Ground Station

Pour accéder à la AWS Ground Station console, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher les détails AWS Ground Station des ressources de votre Compte AWS. Si vous créez une stratégie basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette stratégie.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement le AWS CLI ou le AWS API. Au lieu de cela, autorisez uniquement l'accès aux actions correspondant à l'APIopération qu'ils tentent d'effectuer.

Pour garantir que les utilisateurs et les rôles peuvent toujours utiliser la AWS Ground Station console, associez également la politique AWS Ground Station `ConsoleAccess` ou la politique `ReadOnly` AWS gérée aux entités. Pour plus d'informations, consultez la section Ajouter des autorisations à un utilisateur dans le Guide de IAM l'utilisateur.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux IAM utilisateurs de consulter les politiques intégrées et gérées associées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide du AWS CLI ou. 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": "*"
        }
    ]
}
```

Résolution des problèmes AWS Ground Station d'identité et d'accès

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec AWS Ground Station etIAM.

Rubriques

Je ne suis pas autorisé à effectuer une action dans AWS Ground Station

Si vous recevez une erreur qui indique que vous n'êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d'effectuer l'action.

L'exemple d'erreur suivant se produit lorsque l'`mateojackson`IAMutilisateur essaie d'utiliser la console pour afficher les détails d'une *`my-example-widget`* ressource fictive mais ne dispose pas des `groundstation:`*`GetWidget`* autorisations fictives.

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

Dans ce cas, la politique qui s'applique à l'utilisateur `mateojackson` doit être mise à jour pour autoriser l'accès à la ressource *`my-example-widget`* à l'aide de l'action `groundstation:`*`GetWidget`*.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez une erreur selon laquelle vous n'êtes pas autorisé à exécuter `iam:PassRole` l'action, vos stratégies doivent être mises à jour afin de vous permettre de transmettre un rôle à AWS Ground Station.

Certains vous AWS services permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un IAM utilisateur nommé `marymajor` essaie d'utiliser la console pour effectuer une action dans AWS Ground Station. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

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

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite permettre à des personnes extérieures Compte AWS à moi d'accéder à mes AWS Ground Station ressources

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACLs), vous pouvez utiliser ces politiques pour autoriser les utilisateurs à accéder à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si ces fonctionnalités sont prises AWS Ground Station en charge, consultezComment AWS Ground Station fonctionne avec IAM.
- Pour savoir comment donner accès à vos ressources sur un site Comptes AWS qui vous appartient, consultez la section Fournir l'accès à un IAM utilisateur dans un autre site Compte AWS que vous possédez dans le Guide de IAM l'utilisateur.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le Guide de IAM l'utilisateur.
- Pour savoir comment fournir un accès via la fédération d'identité, consultez la section Fournir un accès aux utilisateurs authentifiés de manière externe (fédération d'identité) dans le guide de l'IAMutilisateur.

- Pour connaître la différence entre l'utilisation de rôles et l'utilisation de politiques basées sur les ressources pour l'accès entre comptes, voir Accès aux ressources entre comptes IAM dans le guide de l'IAMutilisateur.

AWS politiques gérées pour AWS Ground Station

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle AWS service est lancée ou que de nouvelles API opérations sont disponibles pour les services existants.

Pour plus d'informations, consultez la section Politiques AWS gérées dans le Guide de IAM l'utilisateur.

AWS politique gérée : AWSGroundStationAgentInstancePolicy

Vous pouvez associer la `AWSGroundStationAgentInstancePolicy` politique à votre IAM identité.

Cette politique accorde à AWS Ground Station l'agent des autorisations d'accès à votre EC2 instance Amazon, ce qui permet à l'instance d'envoyer et de recevoir des données lors des contacts avec Ground Station. Toutes les autorisations de cette politique proviennent du service Ground Station.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `groundstation`— Permet aux instances de point de terminaison de flux de données d'appeler l'agent Ground Station. APIs

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

AWS politique gérée : AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy

Vous ne pouvez pas vous AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy rattacher à vos IAM entités. Cette politique est associée à un rôle lié à un service qui permet d' AWS Ground Station effectuer des actions en votre nom. Pour plus d'informations, consultez la section Utilisation de rôles liés à un service.

Cette politique accorde des EC2 autorisations qui permettent AWS Ground Station de trouver des IPv4 adresses publiques.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `ec2:DescribeAddresses`— Permet AWS Ground Station de répertorier toutes les informations IPs associées EIPs en votre nom.
- `ec2:DescribeNetworkInterfaces`— Permet AWS Ground Station d'obtenir des informations sur les interfaces réseau associées aux EC2 instances en votre nom.

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

AWS Ground Station mises à jour des politiques AWS gérées

Consultez les détails des mises à jour des politiques AWS gérées AWS Ground Station depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au RSS fil sur la page Historique du AWS Ground Station document.

Modification	Description	Date
AWSGroundStationAgentInstancePolicy : nouvelle politique	AWS Ground Station a ajouté une nouvelle politique pour fournir à l'instance de point	12 avril 2023

Modification	Description	Date
	de terminaison du flux de données les autorisations nécessaires pour utiliser l'agent AWS Ground Station.	
AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy : nouvelle politique	AWS Ground Station a ajouté une nouvelle politique qui accorde EC2 des autorisations AWS Ground Station permettant de rechercher les IPv4 adresses publiques associées aux EC2 instances EIPs et les interfaces réseau associées à celles-ci.	2 novembre 2022
AWS Ground Station a commencé à suivre les modifications	AWS Ground Station a commencé à suivre les modifications apportées aux politiques AWS gérées.	01 mars 2021

Utilisation de rôles liés à un service pour Ground Station

AWS Ground Station utilise AWS Identity and Access Management (IAM) des rôles liés à un service. Un rôle lié à un service est un type unique de IAM rôle directement lié à Ground Station. Les rôles liés aux services sont prédéfinis par Ground Station et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service facilite la configuration de Ground Station, car vous n'avez pas à ajouter manuellement les autorisations nécessaires. Ground Station définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seule Ground Station peut assumer ses rôles. Les autorisations définies incluent la politique de confiance et la politique d'autorisations, et cette politique d'autorisations ne peut être attachée à aucune autre IAM entité.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés à un service, consultez la section AWS Services qui fonctionnent avec IAM et recherchez les services dont la

valeur est Oui dans la colonne Rôles liés à un service. Choisissez un Oui ayant un lien permettant de consulter les détails du rôle pour ce service.

Autorisations de rôle liées au service pour Ground Station

Ground Station utilise le rôle lié au service nommé AWSServiceRoleForGroundStationDataflowEndpointGroup: AWS GroundStation utilise ce rôle lié au service pour l'invoquer EC2 afin de rechercher des adresses publiques. IPv4

Le rôle AWSServiceRoleForGroundStationDataflowEndpointGroup lié à un service fait confiance aux services suivants pour assumer le rôle :

- `groundstation.amazonaws.com`

La politique d'autorisation des rôles nommée AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy permet à Ground Station d'effectuer les actions suivantes sur les ressources spécifiées :

- Action : `ec2:DescribeAddresses` sur `all AWS resources (*)`

  Cette action permet à Ground Station de répertorier tous les IPs éléments associés àEIPs.

- Action : `ec2:DescribeNetworkInterfaces` sur `all AWS resources (*)`

  Cette action permet à Ground Station d'obtenir des informations sur les interfaces réseau associées aux EC2 instances

Vous devez configurer les autorisations pour autoriser une IAM entité (telle qu'un utilisateur, un groupe ou un rôle) à créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez la section Autorisations relatives aux rôles liés à un service dans le Guide de l'IAMutilisateur.

Création d'un rôle lié à un service pour Ground Station

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous créez un rôle DataflowEndpointGroup dans le AWS CLI ou le AWS API, Ground Station crée pour vous le rôle lié au service.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous créez un DataflowEndpointGroup, Ground Station crée à nouveau le rôle lié au service pour vous.

Vous pouvez également utiliser la IAM console pour créer un rôle lié à un service avec le cas d'EC2utilisation de Data Delivery to Amazon. Dans le AWS CLI ou le AWS API, créez un rôle lié au service avec le nom du `groundstation.amazonaws.com` service. Pour plus d'informations, consultez la section Création d'un rôle lié à un service dans le Guide de l'IAMutilisateur. Si vous supprimez ce rôle lié à un service, vous pouvez utiliser ce même processus pour créer le rôle à nouveau.

Modification d'un rôle lié à un service pour Ground Station

Ground Station ne vous permet pas de modifier le rôle AWSServiceRoleForGroundStationDataflowEndpointGroup lié au service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Vous pouvez toutefois modifier la description du rôle à l'aide deIAM. Pour plus d'informations, consultez la section Modification d'un rôle lié à un service dans le Guide de l'IAMutilisateur.

Supprimer un rôle lié à un service pour Ground Station

Si vous n'avez plus besoin d'utiliser une fonctionnalité ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement.

Vous ne pouvez supprimer un rôle lié à un service qu'après l'avoir d'abord supprimé DataflowEndpointGroups en utilisant le rôle lié à un service. Cela vous empêche de révoquer par inadvertance les autorisations accordées à votre. DataflowEndpointGroups Si un rôle lié à un service est utilisé avec plusieurs rôles DataflowEndpointGroups, vous devez supprimer tous ceux DataflowEndpointGroups qui utilisent le rôle lié à un service avant de pouvoir le supprimer.

> **Note**
>
> Si le service Ground Station utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer les ressources de Ground Station utilisées par AWSServiceRoleForGroundStationDataflowEndpointGroup

- Supprimer DataflowEndpointGroups via le AWS CLI ou le AWSAPI.

Pour supprimer manuellement le rôle lié à un service à l'aide de IAM

Utilisez la IAM console AWS CLI, le ou le AWS API pour supprimer le rôle AWSServiceRoleForGroundStationDataflowEndpointGroup lié au service. Pour plus d'informations, consultez la section Suppression d'un rôle lié à un service dans le Guide de l'IAMutilisateur.

Régions prises en charge pour les rôles liés au service Ground Station

Ground Station prend en charge l'utilisation de rôles liés au service dans toutes les régions où le service est disponible. Pour plus d'informations, consultez le tableau des régions.

Résolution des problèmes

`NOT_AUTHORIZED_TO_CREATE_SLR`- Cela indique que le rôle de votre compte utilisé pour appeler CreateDataflowEndpointGroup API n'est pas `iam:CreateServiceLinkedRole` autorisé. Un administrateur `iam:CreateServiceLinkedRole` autorisé doit créer manuellement le rôle lié au service pour votre compte.

Chiffrement des données au repos pour AWS Ground Station

AWS Ground Station fournit un chiffrement par défaut pour protéger vos données sensibles au repos à l'aide de clés de chiffrement AWS détenues par vos soins.

- AWSclés détenues : AWS Ground Station utilise ces clés par défaut pour chiffrer automatiquement les données personnelles et les éphémérides directement identifiables. Vous ne pouvez pas consulter, gérer ou utiliser les clés AWS détenues, ni auditer leur utilisation. Cependant, il n'est pas nécessaire de prendre des mesures ou de modifier les programmes pour protéger les clés qui chiffrent les données. Pour plus d'informations, consultez la section AWS-owned keys dans le guide du développeur du service de gestion des AWS clés.

Le chiffrement des données au repos par défaut permet de réduire les frais opérationnels et la complexité liés à la protection des données sensibles. Dans le même temps, il permet de créer des

applications sécurisées qui répondent à une stricte conformité en matière de chiffrement, ainsi qu'aux exigences réglementaires.

AWS Ground Station applique le chiffrement à toutes les données sensibles au repos. Toutefois, pour certaines AWS Ground Station ressources, telles que les éphémérides, vous pouvez choisir d'utiliser une clé gérée par le client à la place des clés gérées par défaut. AWS

- Clés gérées par le client : AWS Ground Station prend en charge l'utilisation d'une clé symétrique gérée par le client que vous créez, détenez et gérez pour ajouter une deuxième couche de chiffrement par rapport au chiffrement que vous AWS possédez déjà. Étant donné que vous avez le contrôle total de cette couche de chiffrement, vous pouvez effectuer les tâches suivantes :
  - Établissement et gestion des stratégies de clé
  - Établir et maintenir IAM des politiques et des subventions
  - Activation et désactivation des stratégies de clé
  - Rotation des matériaux de chiffrement de clé
  - Ajout de balises
  - Création d'alias de clé
  - Planification des clés pour la suppression

  Pour plus d'informations, consultez la section clé gérée par le client dans le guide du développeur du service de gestion des AWS clés.

Le tableau suivant récapitule les ressources pour lesquelles l'utilisation de clés gérées par le client est prise AWS Ground Station en charge.

Type de données	AWSchiffrement par clé détenue	Chiffrement par clé gérée par le client (facultatif)
Données éphémérides utilisées pour calculer la trajectoire d'un satellite	Activées	Activées

> **Note**
>
> AWS Ground Station active automatiquement le chiffrement au repos à l'aide de clés AWS détenues pour protéger gratuitement les données personnelles identifiables. Toutefois, AWS KMS des frais s'appliquent pour l'utilisation d'une clé gérée par le client. Pour plus d'informations sur la tarification, consultez la tarification du service de gestion des AWS clés. Pour plus d'informations AWS KMS, consultez le guide du AWS KMS développeur.

Comment AWS Ground Station utilise les subventions dans AWS KMS

AWS Ground Station nécessite une autorisation de clé pour utiliser votre clé gérée par le client.

Lorsque vous téléchargez une éphéméride cryptée à l'aide d'une clé gérée par le client, vous AWS Ground Station créez une attribution de clé en votre nom en envoyant une CreateGrant demande à. AWS KMS Les subventions AWS KMS sont utilisées pour donner AWS Ground Station accès à une KMS clé de votre compte.

AWS Ground Station nécessite l'autorisation d'utiliser votre clé gérée par le client pour les opérations internes suivantes :

- Envoyez GenerateDataKeydes demandes AWS KMS à pour générer des clés de données chiffrées par votre clé gérée par le client.
- Envoyez des demandes de déchiffrement AWS KMS à pour déchiffrer les clés de données chiffrées afin qu'elles puissent être utilisées pour chiffrer vos données.
- Envoyez des demandes de chiffrement à AWS KMS pour chiffrer les données fournies.

Vous pouvez révoquer l'accès à l'octroi ou supprimer l'accès du service à la clé gérée par le client à tout moment. Si vous le faites, vous AWS Ground Station ne pourrez accéder à aucune des données chiffrées par la clé gérée par le client, ce qui affectera les opérations qui dépendent de ces données. Par exemple, si vous supprimez une attribution de clé pour une éphéméride actuellement utilisée pour un contact, vous ne AWS Ground Station pourrez pas utiliser les données d'éphéméride fournies pour pointer l'antenne pendant le contact. Cela entraînera la fin du contact dans un FAILED état.

Création d'une clé gérée par le client

Vous pouvez créer une clé symétrique gérée par le client à l'aide de la console AWS de gestion ou du AWS KMSAPIs.

Pour créer une clé symétrique gérée par le client

Suivez les étapes de création d'une clé symétrique gérée par le client dans le guide du développeur du service de gestion des AWS clés.

Stratégie de clé

Les politiques de clés contrôlent l'accès à votre clé gérée par le client. Chaque clé gérée par le client doit avoir exactement une stratégie de clé, qui contient des instructions qui déterminent les personnes pouvant utiliser la clé et comment elles peuvent l'utiliser. Lorsque vous créez votre clé gérée par le client, vous pouvez spécifier une stratégie de clé. Pour plus d'informations, consultez la section Gestion de l'accès aux clés gérées par le client dans le Guide du développeur du service de gestion des AWS clés.

Pour utiliser votre clé gérée par le client avec vos AWS Ground Station ressources, les API opérations suivantes doivent être autorisées dans la politique des clés :

`kms:CreateGrant`- Ajoute une autorisation à une clé gérée par le client. Accorde un accès de contrôle à une KMS clé spécifiée, ce qui permet d'accéder aux opérations d'octroi AWS Ground Station requises. Pour plus d'informations sur l'utilisation des subventions, consultez le guide du développeur du service de gestion des AWS clés.

Cela permet AWS à Amazon d'effectuer les opérations suivantes :

- Appelez GenerateDataKeypour générer une clé de données cryptée et la stocker, car la clé de données n'est pas immédiatement utilisée pour chiffrer.
- Appelez Decrypt pour utiliser la clé de données cryptée stockée afin d'accéder aux données cryptées.
- Appelez Encrypt pour utiliser la clé de données pour chiffrer les données.
- Configurez un directeur partant à la retraite pour permettre au service de`RetireGrant`.

`kms:DescribeKey`- Fournit les informations clés gérées par le client AWS Ground Station pour lui permettre de valider la clé avant de tenter de créer une autorisation sur la clé fournie.

Voici des exemples IAM de déclarations de politique que vous pouvez ajouter 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" : "*"
  }
]
```

Pour plus d'informations sur la spécification des autorisations dans une politique, consultez le Guide du développeur du service de gestion des AWS clés.

Pour plus d'informations sur la résolution des problèmes d'accès par clé, consultez le Guide du développeur du service de gestion des AWS clés.

Spécification d'une clé gérée par le client pour AWS Ground Station

Vous pouvez spécifier une clé gérée par le client pour chiffrer les ressources suivantes :

- Éphémérides

Lorsque vous créez une ressource, vous pouvez spécifier la clé de données en fournissant un kmsKeyArn

- kmsKeyArn- Un identifiant de clé pour une clé gérée par AWS KMS le client

AWS Ground Station contexte de chiffrement

Un contexte de chiffrement est un ensemble facultatif de paires clé-valeur qui contient des informations contextuelles supplémentaires sur les données. AWS KMSutilise le contexte de chiffrement comme données authentifiées supplémentaires pour prendre en charge le chiffrement authentifié. Lorsque vous incluez un contexte de chiffrement dans une demande de chiffrement de données, AWS KMS lie le contexte de chiffrement aux données chiffrées. Pour déchiffrer les données, vous devez inclure le même contexte de chiffrement dans la demande.

AWS Ground Station contexte de chiffrement

AWS Ground Station utilise le contexte de chiffrement différent en fonction de la ressource cryptée et spécifie un contexte de chiffrement spécifique pour chaque attribution de clé créée.

Contexte de chiffrement des éphémérides :

Octroi de clés pour le chiffrement des éphémérides, les ressources sont liées à un satellite spécifique ARN

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

> **Note**
>
> Les subventions clés sont réutilisées pour la même paire clé-satellite.

Utilisation du contexte de chiffrement pour la surveillance

Lorsque vous utilisez une clé symétrique gérée par le client pour chiffrer vos éphémérides, vous pouvez également utiliser le contexte de chiffrement dans les enregistrements d'audit et les journaux pour identifier la manière dont la clé gérée par le client est utilisée. Le contexte de chiffrement apparaît également dans les journaux générés par AWS CloudTrail ou Amazon CloudWatch Logs.

Utilisation du contexte de chiffrement pour contrôler l'accès à votre clé gérée par le client

Vous pouvez utiliser le contexte de chiffrement dans les politiques clés et les IAM politiques `conditions` afin de contrôler l'accès à votre clé symétrique gérée par le client. Vous pouvez également utiliser des contraintes de contexte de chiffrement dans un octroi.

AWS Ground Station utilise une contrainte de contexte de chiffrement dans les autorisations afin de contrôler l'accès à la clé gérée par le client dans votre compte ou votre région. La contrainte d'octroi exige que les opérations autorisées par l'octroi utilisent le contexte de chiffrement spécifié.

Vous trouverez ci-dessous des exemples de déclarations de stratégie de clé permettant d'accorder l'accès à une clé gérée par le client dans un contexte de chiffrement spécifique. La condition énoncée dans cette déclaration de stratégie exige que les octrois comportent une contrainte de contexte de chiffrement qui spécifie le contexte de chiffrement.

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

Surveillance de vos clés de chiffrement pour AWS Ground Station

Lorsque vous utilisez une clé gérée par le AWS KMS client avec vos AWS Ground Station ressources, vous pouvez utiliser AWS CloudTrail CloudWatch les journaux Amazon pour suivre les demandes AWS Ground Station envoyées à AWS KMS. Les exemples suivants sont AWS CloudTrail des événements pour`CreateGrant`, `GenerateDataKeyDecrypt`, `Encrypt` et `DescribeKey` pour surveiller les KMS opérations appelées par AWS Ground Station pour accéder aux données chiffrées par votre clé gérée par le client.

`CreateGrant`(Trajectoire nuageuse)

Lorsque vous utilisez une clé gérée par le AWS KMS client pour chiffrer vos ressources éphémérides, envoyez une AWS Ground Station `CreateGrant` demande en votre nom pour accéder à la KMS clé de votre compte. AWS L'autorisation AWS Ground Station créée est spécifique à la ressource associée à la clé gérée par le AWS KMS client. En outre, AWS Ground Station utilise `RetireGrant` cette opération pour supprimer une subvention lorsque vous supprimez une ressource.

L'exemple d'événement suivant enregistre l'opération `CreateGrant` :

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AAAAAAAAAAAAAAAAAAAAA:SampleUser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/SampleUser01",
        "accountId": "111122223333",
        "accessKeyId": "ASIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AAAAAAAAAAAAAAAAAAAAA",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
```

```
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-02-22T22:22:22Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2022-02-22T22:22:22Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "111.11.11.11",
    "userAgent": "ExampleDesktop/1.0 (V1; OS)",
    "requestParameters": {
        "operations": [
            "GenerateDataKeyWithoutPlaintext",
            "Decrypt",
            "Encrypt"
        ],
        "constraints": {
            "encryptionContextSubset": {
                "aws:groundstation:arn":
 "arn:aws:groundstation::111122223333:satellite/00a770b0-082d-45a4-80ed-SAMPLE"
            }
        },
        "granteePrincipal": "groundstation.us-west-2.amazonaws.com",
        "retiringPrincipal": "groundstation.us-west-2.amazonaws.com",
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "responseElements": {
        "grantId":
 "0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE"
    },
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
```

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

`DescribeKey`(Trajectoire nuageuse)

Lorsque vous utilisez une clé gérée par le AWS KMS client pour chiffrer vos ressources éphémérides, vous AWS Ground Station envoyez une `DescribeKey` demande en votre nom pour valider que la clé demandée existe dans votre compte.

L'exemple d'événement suivant enregistre l'opération `DescribeKey` :

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

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

`GenerateDataKey`(Trajectoire nuageuse)

Lorsque vous utilisez une clé gérée par le AWS KMS client pour chiffrer vos ressources éphémérides, AWS Ground Station envoyez une `GenerateDataKey` demande KMS à afin de générer une clé de données avec laquelle chiffrer vos données.

L'exemple d'événement suivant enregistre l'opération `GenerateDataKey` :

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2022-02-22T22:22:22Z",
    "eventSource": "kms.amazonaws.com",
```

```
    "eventName": "GenerateDataKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keySpec": "AES_256",
        "encryptionContext": {
            "aws:groundstation:arn":
 "arn:aws:groundstation::111122223333:satellite/00a770b0-082d-45a4-80ed-SAMPLE",
            "aws:s3:arn":
 "arn:aws:s3:::customerephemerisbucket/0034abcd-12ab-34cd-56ef-123456SAMPLE"
        },
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "sharedEventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventCategory": "Management"
}
```


`Decrypt`(Trajectoire nuageuse)

Lorsque vous utilisez une clé gérée par le AWS KMS client pour chiffrer vos ressources d'éphémérides, AWS Ground Station utilise l'`Decrypt`opération pour déchiffrer les éphémérides fournies si elles sont déjà chiffrées avec la même clé gérée par le client. Par exemple, si une éphéméride est téléchargée depuis un compartiment S3 et qu'elle est chiffrée dans ce compartiment avec une clé donnée.

L'exemple d'événement suivant enregistre l'opération `Decrypt` :

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

Chiffrement des données pendant le transit pour AWS Ground Station

AWS Ground Station fournit un chiffrement par défaut pour protéger vos données sensibles pendant le transport. Les données peuvent être diffusées entre les emplacements des AWS Ground Station antennes et vos EC2 instances Amazon de deux manières, en fonction de la configuration du profil de mission.

- AWS Ground Station Agent
- Point de terminaison du flux de données

Chaque méthode de diffusion de données gère différemment le chiffrement des données en transit. Les sections suivantes décrivent chaque méthode.

AWS Ground Station Streams d'agents

AWS Ground Station L'agent chiffre ses flux à l'aide de AWS KMS clés gérées par le client. L' AWS Ground Station agent exécuté sur votre EC2 instance Amazon déchiffrera automatiquement le flux pour fournir des données déchiffrées.

La AWS KMS clé utilisée pour chiffrer un flux est spécifiée lors de la création d'un `MissionProfile` dans le streamsKmsKeyparamètre. Toutes les autorisations accordant l' AWS Ground Station accès aux clés sont gérées par le biais de la politique relative aux AWS KMS clés attachée à`streamsKmsKey`.

Flux de points de terminaison de flux de données

Les flux de points de terminaison de flux de données sont chiffrés à l'aide de Datagram Transport Layer Security (). DTLS Cela se fait à l'aide de certificats auto-signés et ne nécessite aucune configuration supplémentaire.

Exemples de configurations de profil de mission

Les exemples fournis montrent comment utiliser un satellite de diffusion public et créer un profil de mission qui le soutient. Les modèles qui en résultent sont fournis pour vous aider à prendre contact avec un satellite de diffusion publique et pour vous aider à prendre des décisions concernant vos satellites.

Rubriques

JPSS-1 - Satellite de diffusion public (PBS) - Évaluation

Cette section d'exemple correspond auVue d'ensemble du processus d'intégration des clients. Il fournit une brève analyse de compatibilité avec AWS Ground Station les exemples spécifiques suivants et prépare le terrain pour les exemples spécifiques qui suivent.

Comme indiqué dans la Satellites de diffusion publics section, vous pouvez utiliser certains satellites, ou les voies de communication d'un satellite, accessibles au public. Dans cette section, nous décrivons JPSS-1 dans les AWS Ground Station termes. À titre de référence, nous utilisons le document de contrôle de l'interface de radiofréquences (HRD) du système conjoint de satellites polaires 1 (JPSS-1) pour les stations de diffusion directe (ICD) pour compléter l'exemple. DBS Il convient également de noter que JPSS -1 est associé à l'NORADID 43013.

Le satellite JPSS -1 propose une voie de communication en liaison montante et trois voies de communication en liaison descendante directe, comme le montre la figure 1-1 du. ICD Parmi ces quatre voies de communication, seule la voie de communication descendante High Rate Data (HRD) est disponible pour la consommation publique. Sur cette base, vous verrez que ce chemin sera également associé à des données beaucoup plus spécifiques. Les quatre voies sont les suivantes :

- Chemin de commande (liaison montante) à une fréquence MHz centrale de 2067,27 avec un débit de données de 2 à 128 kbit/s. Ce chemin n'est pas accessible au public.

- Chemin de télémétrie (liaison descendante) à une fréquence MHz centrale de 2247,5 avec un débit de données de 1 à 524 kbps. Ce chemin n'est pas accessible au public.
- SMDchemin (liaison descendante) à une fréquence GHz centrale de 26,7034 avec un débit de 150 à 300 Mbps. Ce chemin n'est pas accessible au public.
- La RF pour le HRD trajet (liaison descendante) à une fréquence MHz centrale de 7812 avec un débit de données de 15 Mbps. Il a une MHz bande passante de 30, et c'est le cas right-hand-circular-polarized. Lorsque vous JPSS embarquez avec -1 AWS Ground Station, c'est le chemin de communication auquel vous avez accès. Ce chemin de communication contient des données scientifiques sur les instruments, des données d'ingénierie des instruments, des données de télémétrie des instruments et des données d'entretien en temps réel des engins spatiaux.

Lorsque nous comparons les chemins de données potentiels, nous constatons que les chemins de commande (liaison montante), de télémétrie (liaison descendante) et HRD (liaison descendante) répondent aux capacités de fréquence, de bande passante et d'utilisation simultanée multicanaux de. AWS Ground Station Le SMD trajet n'est pas compatible car la fréquence centrale est hors de portée des récepteurs existants. Pour plus d'informations sur les fonctionnalités prises en charge, consultezAWS Ground Station Fonctionnalités du site.

> **Note**
>
> Comme le SMD chemin n'est pas compatible avec AWS Ground Station celui-ci, il ne sera pas représenté dans les exemples de configurations.

> **Note**
>
> Comme les chemins de commande (liaison montante) et de télémétrie (liaison descendante) ne sont pas définis dans le et ne sont pas disponibles pour un usage publicICD, les valeurs fournies lors de leur utilisation sont fictives.

Satellite de diffusion publique utilisant la livraison de données Amazon S3

Cet exemple s'appuie sur l'analyse effectuée dans la JPSS-1 - Satellite de diffusion public (PBS) - Évaluation section du guide de l'utilisateur.

Pour cet exemple, vous devez supposer un scénario : vous souhaitez capturer le chemin de HRD communication sous forme de fréquence intermédiaire numérique et le stocker pour un futur traitement par lots. Cela permet d'économiser les échantillons bruts en quadrature de phase (I/Q) de radiofréquence (RF) une fois qu'ils ont été numérisés. Une fois que les données se trouvent dans votre compartiment Amazon S3, vous pouvez les démoduler et les décoder à l'aide du logiciel de votre choix. Consultez le MathWorks didacticiel pour un exemple détaillé de traitement. Après avoir utilisé cet exemple, vous pouvez envisager d'ajouter des composants de tarification au EC2 comptant d'Amazon pour traiter les données et réduire vos coûts de traitement globaux.

Voies de communication

Cette section représente Étape 2 : planifiez les voies de communication de votre flux de données la mise en route.

Tous les extraits de modèle suivants appartiennent à la section Ressources du AWS CloudFormation modèle.

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

> **Note**
>
> Pour plus d'informations sur le contenu d'un AWS CloudFormation modèle, consultez les sections relatives aux modèles.

Compte tenu de notre scénario consistant à fournir un chemin de communication unique à Amazon S3, vous savez que vous n'aurez qu'un seul chemin de livraison asynchrone. Selon la Livraison de données asynchrone section, vous devez définir un compartiment Amazon S3.

```
  # The S3 bucket where AWS Ground Station will deliver the downlinked data.
  GroundStationS3DataDeliveryBucket:
    Type: AWS::S3::Bucket
    DeletionPolicy: Retain
    UpdateReplacePolicy: Retain
```

```
    Properties:
      # Results in a bucket name formatted like: aws-groundstation-data-{account id}-
{region}-{random 8 character string}
      BucketName: !Join ["-", ["aws-groundstation-data", !Ref AWS::AccountId, !Ref
 AWS::Region, !Select [0, !Split ["-", !Select [2, !Split ["/", !Ref AWS::StackId]]]]]]
```

En outre, vous devrez créer les rôles et les politiques appropriés afin d' AWS Ground Station autoriser l'utilisation du bucket.

```
  # The IAM role that AWS Ground Station will assume to have permission find and write
  # data to your S3 bucket.
  GroundStationS3DataDeliveryRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Statement:
          - Action:
              - 'sts:AssumeRole'
            Effect: Allow
            Principal:
              Service:
                - groundstation.amazonaws.com
            Condition:
              StringEquals:
                "aws:SourceAccount": !Ref AWS::AccountId
              ArnLike:
                "aws:SourceArn": !Sub "arn:aws:groundstation:${AWS::Region}:
${AWS::AccountId}:config/s3-recording/*"

  # The S3 bucket policy that defines what actions AWS Ground Station can perform on
 your S3 bucket.
  GroundStationS3DataDeliveryBucketPolicy:
    Type: AWS::IAM::Policy
    Properties:
      PolicyDocument:
        Statement:
          - Action:
              - 's3:GetBucketLocation'
            Effect: Allow
            Resource:
              - !GetAtt GroundStationS3DataDeliveryBucket.Arn
```

```
          - Action:
              - 's3:PutObject'
            Effect: Allow
            Resource:
              - !Join [ "/", [ !GetAtt GroundStationS3DataDeliveryBucket.Arn, "*" ] ]
      PolicyName: GroundStationS3DataDeliveryPolicy
      Roles:
        - !Ref GroundStationS3DataDeliveryRole
```

AWS Ground Station configurations

Cette section représente Étape 3 : créer des configurations la mise en route.

Vous aurez besoin d'une configuration de suivi pour définir vos préférences en matière d'utilisation du suivi automatique. La sélection en PREFERREDtant que piste automatique peut améliorer la qualité du signal, mais elle n'est pas nécessaire pour atteindre la qualité du signal en raison de la qualité d'éphéméride JPSS -1 suffisante.

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

En fonction du chemin de communication, vous devrez définir une configuration antenne-liaison descendante pour représenter la partie satellite, ainsi qu'un enregistrement S3 pour faire référence au compartiment Amazon S3 que vous venez de créer.

```
  # 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 profil de mission

Cette section représente Étape 4 : Création d'un profil de mission la mise en route.

Maintenant que vous disposez des configurations associées, vous pouvez les utiliser pour créer le flux de données. Vous utiliserez les valeurs par défaut pour les autres paramètres.

```
  # 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
```

Assemblage

Grâce aux ressources ci-dessus, vous avez désormais la possibilité de planifier JPSS 1 contact pour la livraison asynchrone de données depuis n'importe lequel de vos contacts intégrés. AWS Ground Station Emplacements

Ce qui suit est un AWS CloudFormation modèle complet qui inclut toutes les ressources décrites dans cette section combinées dans un modèle unique qui peut être directement utilisé dans AWS CloudFormation.

Le AWS CloudFormation modèle nommé `AquaSnppJpss-1TerraDigIfS3DataDelivery.yml` contient un compartiment Amazon S3 et les AWS Ground Station ressources nécessaires pour planifier les contacts et recevoir des données de diffusion directe signal/IP VITA -49.

Si AquaSNPP, JPSS -1/ NOAA -20 et Terra ne sont pas intégrés à votre compte, consultez. Étape 1 : Intégration du satellite

> **Note**
>
> Vous pouvez accéder au modèle en accédant au compartiment Amazon S3 qui intègre le client. Les liens ci-dessous utilisent un compartiment Amazon S3 régional. Modifiez le code de `us-west-2` région pour représenter la région correspondante dans laquelle vous souhaitez créer la AWS CloudFormation pile.
> De plus, les instructions suivantes utilisentYAML. Cependant, les modèles sont disponibles à la fois dans un JSON format YAML et dans un autre. Pour l'utiliserJSON, remplacez l'extension de `.yml` fichier par `.json` lors du téléchargement du modèle.

Pour télécharger le modèle à l'aide de AWS CLI, utilisez la commande suivante :

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

Vous pouvez consulter et télécharger le modèle dans la console en accédant à ce qui suit URL dans votre navigateur :

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

Vous pouvez spécifier le modèle directement en AWS CloudFormation utilisant le lien suivant :

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

Satellite de diffusion public utilisant un point de terminaison de flux de données (bande étroite)

Cet exemple s'appuie sur l'analyse effectuée dans la JPSS-1 - Satellite de diffusion public (PBS) - Évaluation section du guide de l'utilisateur.

Pour compléter cet exemple, vous devez supposer un scénario : vous souhaitez capturer le chemin de HRD communication sous forme de fréquence intermédiaire numérique (DigIF) et le traiter tel qu'il est reçu par une application de point de terminaison de flux de données sur une instance Amazon EC2 à l'aide d'un. SDR

Voies de communication

Cette section représente Étape 2 : planifiez les voies de communication de votre flux de données la mise en route. Dans cet exemple, vous allez créer deux sections dans votre AWS CloudFormation modèle : les sections Paramètres et Ressources.

> **Note**
>
> Pour plus d'informations sur le contenu d'un AWS CloudFormation modèle, consultez les sections relatives aux modèles.

Pour la section Paramètres, vous allez ajouter les paramètres suivants. Vous spécifierez leurs valeurs lors de la création de la pile via la AWS CloudFormation console.

```
Parameters:
  EC2Key:
    Description: The SSH key used to access the EC2 receiver instance. Choose any
 SSH key if you are not creating an EC2 receiver instance. For instructions on how to
```

```
 create an SSH key see https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/create-
key-pairs.html
    Type: AWS::EC2::KeyPair::KeyName
    ConstraintDescription: must be the name of an existing EC2 KeyPair.

  ReceiverAMI:
    Description: The Ground Station DDX AMI ID you want to use. Please note
 that AMIs are region specific. For instructions on how to retrieve an AMI
 see https://docs.aws.amazon.com/ground-station/latest/ug/dataflows.ec2-
configuration.html#dataflows.ec2-configuration.amis
    Type: AWS::EC2::Image::Id
```

> **Note**
>
> Vous devez créer une paire de clés et fournir le nom du EC2 `EC2Key` paramètre Amazon. Consultez la section Créer une paire de clés pour votre EC2 instance Amazon.
> De plus, vous devrez fournir le bon AMI identifiant spécifique à la région lors de la création de la AWS CloudFormation pile. veuillez consulter AWS Ground Station Images de machines Amazon (AMIs).

Les autres extraits de modèle se trouvent dans la section Ressources du AWS CloudFormation modèle.

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

Dans notre scénario consistant à fournir un chemin de communication unique à une EC2 instance, vous disposerez d'un seul chemin de diffusion synchrone. Selon Livraison synchrone des données cette section, vous devez configurer une EC2 instance Amazon avec une application de point de terminaison de flux de données, et créer un ou plusieurs groupes de points de terminaison de flux de données.

```
  # 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
```

En outre, vous devrez également créer les politiques et les rôles appropriés pour AWS Ground Station permettre la création d'une elastic network interface (ENI) dans votre compte.

```
  # 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 configurations

Cette section représente Étape 3 : créer des configurations la mise en route.

Vous aurez besoin d'une configuration de suivi pour définir vos préférences en matière d'utilisation du suivi automatique. La sélection en PREFERREDtant que piste automatique peut améliorer la qualité du signal, mais elle n'est pas nécessaire pour atteindre la qualité du signal en raison de la qualité d'éphéméride JPSS -1 suffisante.

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

Sur la base du chemin de communication, vous devez définir une configuration antenne-liaison descendante pour représenter la partie satellite, ainsi qu'une configuration de point de terminaison de flux de données pour faire référence au groupe de points de terminaison de flux de données qui définit les détails du point de terminaison.

```
  # 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 profil de mission

Cette section représente Étape 4 : Création d'un profil de mission la mise en route.

Maintenant que vous disposez des configurations associées, vous pouvez les utiliser pour créer le flux de données. Vous utiliserez les valeurs par défaut pour les autres paramètres.

```
  # 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
```

Assemblage

Grâce aux ressources ci-dessus, vous avez désormais la possibilité de planifier JPSS 1 à 1 contact pour la livraison synchrone des données depuis n'importe lequel de vos contacts intégrés. AWS Ground Station Emplacements

Ce qui suit est un AWS CloudFormation modèle complet qui inclut toutes les ressources décrites dans cette section combinées dans un modèle unique qui peut être directement utilisé dans AWS CloudFormation.

Le AWS CloudFormation modèle nommé `AquaSnppJpssTerraDigIF.yml` est conçu pour vous permettre de commencer rapidement à recevoir des données de fréquence intermédiaire numérisées (DigIF) pour les satellites Aqua SNPPJPSS, NOAA -1/ -20 et Terra. Il contient une EC2 instance Amazon et les AWS CloudFormation ressources nécessaires pour recevoir les données brutes de diffusion directe de DigiF.

Si AquaSNPP, JPSS -1/ NOAA -20 et Terra ne sont pas intégrés à votre compte, consultez. Étape 1 : Intégration du satellite

> **Note**
>
> Vous pouvez accéder au modèle en accédant au compartiment Amazon S3 qui intègre le client. Les liens ci-dessous utilisent un compartiment Amazon S3 régional. Modifiez le code de `us-west-2` région pour représenter la région correspondante dans laquelle vous souhaitez créer la AWS CloudFormation pile.
> De plus, les instructions suivantes utilisentYAML. Cependant, les modèles sont disponibles à la fois dans un JSON format YAML et dans un autre. Pour l'utiliserJSON, remplacez l'extension de `.yml` fichier par `.json` lors du téléchargement du modèle.

Pour télécharger le modèle à l'aide de AWS CLI, utilisez la commande suivante :

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

Vous pouvez consulter et télécharger le modèle dans la console en accédant à ce qui suit URL dans votre navigateur :

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

Vous pouvez spécifier le modèle directement en AWS CloudFormation utilisant le lien suivant :

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

Quelles ressources supplémentaires le modèle définit-il ?

Le `AquaSnppJpssTerraDigIF` modèle inclut les ressources supplémentaires suivantes :

- (Facultatif) Déclencheurs d'CloudWatch événements : AWS Lambda fonction déclenchée à l'aide d' CloudWatch événements envoyés AWS Ground Station avant et après un contact. La AWS Lambda fonction démarrera et arrêtera éventuellement votre instance de réception.
- (Facultatif) EC2Vérification pour les contacts : possibilité d'utiliser Lambda pour configurer un système de vérification de vos EC2 instances Amazon pour les contacts avec SNS notification. Il est important de noter que cela peut entraîner des frais en fonction de votre utilisation actuelle.
- Ground Station Amazon Machine Image Retrieval Lambda - La possibilité de sélectionner le logiciel installé sur votre instance et celui AMI de votre choix. Les options du logiciel incluent `DDX 2.6.2 Only` et`DDX 2.6.2 with qRadio 3.6.0`. Ces options continueront de s'étendre à mesure que des mises à jour logicielles et des fonctionnalités supplémentaires seront publiées.
- Profils de mission supplémentaires - Profils de mission pour d'autres satellites de diffusion publique (AquaSNPP, et Terra).
- Configurations supplémentaires de liaison descendante d'antenne - Configurations de liaison descendante d'antenne pour des satellites de diffusion publics supplémentaires (Aqua, et Terra). SNPP

Les valeurs et paramètres pour les satellites dans ce modèle sont déjà renseignés. Ces paramètres vous permettent d'utiliser facilement et AWS Ground Station immédiatement ces satellites. Vous n'avez pas besoin de configurer vos propres valeurs pour pouvoir les utiliser AWS Ground Station lors de l'utilisation de ce modèle. Toutefois, vous pouvez personnaliser les valeurs pour que le modèle fonctionne selon votre cas d'utilisation.

Où puis-je recevoir mes données ?

Le groupe de points de terminaison de flux de données est configuré pour utiliser l'interface réseau d'instance de récepteur créée dans le cadre du modèle. L'instance de réception utilise une application de point de terminaison de flux de données pour recevoir le flux de données depuis le port défini par AWS Ground Station le point de terminaison du flux de données. Une fois reçues, les données peuvent être consommées via le UDP port 50000 de l'adaptateur de boucle de l'instance de réception. Pour plus d'informations sur la configuration d'un groupe de points de terminaison de flux de données, consultez AWS::GroundStation::DataflowEndpoint la section Groupe.

Satellite de diffusion public utilisant un point de terminaison de flux de données (démodulé et décodé)

Cet exemple s'appuie sur l'analyse effectuée dans la JPSS-1 - Satellite de diffusion public (PBS) - Évaluation section du guide de l'utilisateur.

Pour compléter cet exemple, vous devez supposer un scénario : vous souhaitez capturer le chemin de HRD communication sous forme de données de diffusion directe démodulées et décodées à l'aide d'un point de terminaison de flux de données. Cet exemple constitue un bon point de départ si vous envisagez de traiter les données à l'aide du logiciel NASA Direct Readout Labs (RT- STPS etIPOPP).

Voies de communication

Cette section représente Étape 2 : planifiez les voies de communication de votre flux de données la mise en route. Dans cet exemple, vous allez créer deux sections dans votre AWS CloudFormation modèle : les sections Paramètres et Ressources.

> **Note**
>
> Pour plus d'informations sur le contenu d'un AWS CloudFormation modèle, consultez les sections relatives aux modèles.

Pour la section Paramètres, vous allez ajouter les paramètres suivants. Vous spécifierez leurs valeurs lors de la création de la pile via la AWS CloudFormation console.

```
Parameters:
```

```
  EC2Key:
    Description: The SSH key used to access the EC2 receiver instance. Choose any
 SSH key if you are not creating an EC2 receiver instance. For instructions on how to
 create an SSH key see https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/create-
key-pairs.html
    Type: AWS::EC2::KeyPair::KeyName
    ConstraintDescription: must be the name of an existing EC2 KeyPair.

  ReceiverAMI:
    Description: The Ground Station DDX AMI ID you want to use. Please note
 that AMIs are region specific. For instructions on how to retrieve an AMI
 see https://docs.aws.amazon.com/ground-station/latest/ug/dataflows.ec2-
configuration.html#dataflows.ec2-configuration.amis
    Type: AWS::EC2::Image::Id
```

> **Note**
>
> Vous devez créer une paire de clés et fournir le nom du EC2 `EC2Key` paramètre Amazon. Consultez la section Créer une paire de clés pour votre EC2 instance Amazon.
> De plus, vous devrez fournir le bon AMI identifiant spécifique à la région lors de la création de la AWS CloudFormation pile. veuillez consulter AWS Ground Station Images de machines Amazon (AMIs).

Les autres extraits de modèle se trouvent dans la section Ressources du AWS CloudFormation modèle.

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

Dans notre scénario consistant à fournir un chemin de communication unique à une EC2 instance, vous disposerez d'un seul chemin de diffusion synchrone. Selon Livraison synchrone des données cette section, vous devez configurer une EC2 instance Amazon avec une application de point de terminaison de flux de données, et créer un ou plusieurs groupes de points de terminaison de flux de données.

```
 # 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
```

Vous aurez également besoin des politiques, des rôles et des profils appropriés pour AWS Ground Station créer une elastic network interface (ENI) dans votre compte.

```
 # 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 configurations

Cette section représente le guide Étape 3 : créer des configurations de l'utilisateur.

Vous aurez besoin d'une configuration de suivi pour définir vos préférences en matière d'utilisation du suivi automatique. La sélection en PREFERREDtant que piste automatique peut améliorer la qualité du signal, mais elle n'est pas nécessaire pour atteindre la qualité du signal en raison de la qualité d'éphéméride JPSS -1 suffisante.

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

En fonction du chemin de communication, vous devez définir une antenna-downlink-demod-decodeconfiguration pour représenter la partie satellite, ainsi qu'une configuration de point de terminaison de flux de données pour faire référence au groupe de points de terminaison de flux de données qui définit les détails du point de terminaison.

> **Note**
>
> Pour plus de détails sur la façon de définir les valeurs pour`DemodulationConfig`, et`DecodeConfig`, veuillez consulter[Config de décodage/démodulation des signaux d'antenne de liaison descendante] .

```
 # 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 profil de mission

Cette section représente le guide Étape 4 : Création d'un profil de mission de l'utilisateur.

Maintenant que vous disposez des configurations associées, vous pouvez les utiliser pour créer le flux de données. Vous utiliserez les valeurs par défaut pour les autres paramètres.

```
 # 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
```

Assemblage

Grâce aux ressources ci-dessus, vous avez désormais la possibilité de planifier JPSS 1 à 1 contact pour la livraison synchrone des données depuis n'importe lequel de vos contacts intégrés. AWS Ground Station Emplacements

Ce qui suit est un AWS CloudFormation modèle complet qui inclut toutes les ressources décrites dans cette section combinées dans un modèle unique qui peut être directement utilisé dans AWS CloudFormation.

Le AWS CloudFormation modèle nommé `AquaSnppJpss.yml` est conçu pour vous permettre d'accéder rapidement pour commencer à recevoir des données pour les satellites AquaSNPP, et JPSS -1/ NOAA -20. Il contient une EC2 instance Amazon et les AWS Ground Station ressources nécessaires pour planifier les contacts et recevoir des données de diffusion directe démodulées et décodées.

Si AquaSNPP, JPSS -1/ NOAA -20 et Terra ne sont pas intégrés à votre compte, consultez. Étape 1 : Intégration du satellite

> **Note**
>
> Vous pouvez accéder au modèle en accédant au compartiment Amazon S3 qui intègre le client. Les liens ci-dessous utilisent un compartiment Amazon S3 régional. Modifiez le code de `us-west-2` région pour représenter la région correspondante dans laquelle vous souhaitez créer la AWS CloudFormation pile.
> De plus, les instructions suivantes utilisentYAML. Cependant, les modèles sont disponibles dans YAML les deux JSON formats. Pour l'utiliserJSON, remplacez l'extension de `.yml` fichier par `.json` lors du téléchargement du modèle.

Pour télécharger le modèle à l'aide de AWS CLI, utilisez la commande suivante :

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

Vous pouvez consulter et télécharger le modèle dans la console en accédant à ce qui suit URL dans votre navigateur :

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

Vous pouvez spécifier le modèle directement en AWS CloudFormation utilisant le lien suivant :

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

Quelles ressources supplémentaires le modèle définit-il ?

Le `AquaSnppJpss` modèle inclut les ressources supplémentaires suivantes :

- (Facultatif) Déclencheurs d'CloudWatch événements : AWS Lambda fonction déclenchée à l'aide d' CloudWatch événements envoyés AWS Ground Station avant et après un contact. La AWS Lambda fonction démarrera et arrêtera éventuellement votre instance de réception.
- (Facultatif) EC2Vérification pour les contacts : possibilité d'utiliser Lambda pour configurer un système de vérification de vos EC2 instances Amazon pour les contacts avec SNS notification. Il est important de noter que cela peut entraîner des frais en fonction de votre utilisation actuelle.
- Ground Station Amazon Machine Image Retrieval Lambda - La possibilité de sélectionner le logiciel installé sur votre instance et celui AMI de votre choix. Les options logicielles incluent `DDX 2.6.2`

`Only` etDDX `2.6.2 with qRadio 3.6.0`. Si vous souhaitez utiliser Wideband DigiF Data Delivery et l' AWS Ground Station agent, consultez. Satellite de diffusion publique utilisant AWS Ground Station l'agent (large bande) Ces options continueront de s'étendre à mesure que des mises à jour logicielles et des fonctionnalités supplémentaires seront publiées.

- Profils de mission supplémentaires - Profils de mission pour d'autres satellites de diffusion publique (AquaSNPP, et Terra).
- Configurations supplémentaires de liaison descendante d'antenne - Configurations de liaison descendante d'antenne pour des satellites de diffusion publique supplémentaires (Aqua, et Terra). SNPP

Les valeurs et paramètres pour les satellites dans ce modèle sont déjà renseignés. Ces paramètres vous permettent d'utiliser facilement et AWS Ground Station immédiatement ces satellites. Vous n'avez pas besoin de configurer vos propres valeurs pour pouvoir les utiliser AWS Ground Station lors de l'utilisation de ce modèle. Toutefois, vous pouvez personnaliser les valeurs pour que le modèle fonctionne selon votre cas d'utilisation.

Où puis-je recevoir mes données ?

Le groupe de points de terminaison de flux de données est configuré pour utiliser l'interface réseau d'instance de récepteur créée dans le cadre du modèle. L'instance de réception utilise une application de point de terminaison de flux de données pour recevoir le flux de données depuis le port défini par AWS Ground Station le point de terminaison du flux de données. Une fois reçues, les données peuvent être consommées via le UDP port 50000 de l'adaptateur de boucle de l'instance de réception. Pour plus d'informations sur la configuration d'un groupe de points de terminaison de flux de données, consultez AWS::GroundStation::DataflowEndpoint la section Groupe.

Satellite de diffusion publique utilisant AWS Ground Station l'agent (large bande)

Cet exemple s'appuie sur l'analyse effectuée dans la JPSS-1 - Satellite de diffusion public (PBS) - Évaluation section du guide de l'utilisateur.

Pour compléter cet exemple, vous devez supposer un scénario : vous souhaitez capturer le chemin de HRD communication sous forme de fréquence intermédiaire numérique à large bande (DigIF) et le traiter tel qu'il est reçu par l'agent AWS Ground Station sur une instance Amazon EC2 à l'aide d'un. SDR

> **Note**
>
> Le signal du chemin de JPSS HRD communication réel a une bande passante de 30MHz, mais vous allez configurer la configuration antenne-liaison descendante pour le traiter comme un signal avec une MHz bande passante de 100 afin qu'il puisse circuler sur le chemin correct pour être reçu par l' AWS Ground Station agent dans cet exemple.

Voies de communication

Cette section représente Étape 2 : planifiez les voies de communication de votre flux de données la mise en route. Pour cet exemple, vous aurez besoin d'une section supplémentaire dans votre AWS CloudFormation modèle qui n'a pas été utilisée dans les autres exemples, la section Mappages.

> **Note**
>
> Pour plus d'informations sur le contenu d'un AWS CloudFormation modèle, consultez les sections relatives aux modèles.

Vous allez commencer par configurer une section Mappings dans votre AWS CloudFormation modèle pour les listes de AWS Ground Station préfixes par région. Cela permet aux listes de préfixes d'être facilement référencées par le groupe de sécurité des EC2 instances Amazon. Pour plus d'informations sur l'utilisation d'une liste de préfixes, consultezVPCConfiguration avec l' AWS Ground Station agent.

```
Mappings:
  PrefixListId:
    us-east-2:
      groundstation: pl-087f83ba4f34e3bea
    us-west-2:
      groundstation: pl-0cc36273da754ebdc
    us-east-1:
      groundstation: pl-0e5696d987d033653
    eu-central-1:
      groundstation: pl-03743f81267c0a85e
    sa-east-1:
      groundstation: pl-098248765e9effc20
```

```
    ap-northeast-2:
      groundstation: pl-059b3e0b02af70e4d
    ap-southeast-1:
      groundstation: pl-0d9b804fe014a6a99
    ap-southeast-2:
      groundstation: pl-08d24302b8c4d2b73
    me-south-1:
      groundstation: pl-02781422c4c792145
    eu-west-1:
      groundstation: pl-03fa6b266557b0d4f
    eu-north-1:
      groundstation: pl-033e44023025215c0
    af-south-1:
      groundstation: pl-0382d923a9d555425
```

Pour la section Paramètres, vous allez ajouter les paramètres suivants. Vous spécifierez leurs valeurs lors de la création de la pile via la AWS CloudFormation console.

```
Parameters:
  EC2Key:
    Description: The SSH key used to access the EC2 receiver instance. Choose any
 SSH key if you are not creating an EC2 receiver instance. For instructions on how to
 create an SSH key see https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/create-
key-pairs.html
    Type: AWS::EC2::KeyPair::KeyName
    ConstraintDescription: must be the name of an existing EC2 KeyPair.

  AZ:
    Description: "The AvailabilityZone that the resources of this stack will be created
 in. (e.g. us-east-2a)"
    Type: AWS::EC2::AvailabilityZone::Name

  ReceiverAMI:
    Description: The Ground Station Agent AMI ID you want to use. Please note
 that AMIs are region specific. For instructions on how to retrieve an AMI
 see https://docs.aws.amazon.com/ground-station/latest/ug/dataflows.ec2-
configuration.html#dataflows.ec2-configuration.amis
    Type: AWS::EC2::Image::Id
```

> **Note**
>
> Vous devez créer une paire de clés et fournir le nom du EC2 `EC2Key` paramètre Amazon. Consultez la section Créer une paire de clés pour votre EC2 instance Amazon.
> De plus, vous devrez fournir le bon AMI identifiant spécifique à la région lors de la création de la AWS CloudFormation pile. veuillez consulter AWS Ground Station Images de machines Amazon (AMIs).

Les autres extraits de modèle se trouvent dans la section Ressources du AWS CloudFormation modèle.

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

Compte tenu de notre scénario consistant à fournir un chemin de communication unique à une EC2 instance Amazon, vous savez que vous n'aurez qu'un seul chemin de livraison synchrone. Selon la Livraison synchrone des données section, vous devez installer et configurer une EC2 instance Amazon avec l' AWS Ground Station Agent, et créer un ou plusieurs groupes de points de terminaison de flux de données. Vous allez commencer par configurer Amazon VPC pour l' AWS Ground Station agent.

```
  ReceiverVPC:
    Type: AWS::EC2::VPC
    Properties:
      EnableDnsSupport: 'true'
      EnableDnsHostnames: 'true'
      CidrBlock: 10.0.0.0/16
      Tags:
      - Key: "Name"
        Value: "AWS Ground Station Example - PBS to AWS Ground Station Agent VPC"
      - Key: "Description"
        Value: "VPC for EC2 instance receiving AWS Ground Station data"

  PublicSubnet:
    Type: AWS::EC2::Subnet
    Properties:
```

```
      VpcId: !Ref ReceiverVPC
      MapPublicIpOnLaunch: 'true'
      AvailabilityZone: !Ref AZ
      CidrBlock: 10.0.0.0/20
      Tags:
      - Key: "Name"
        Value: "AWS Ground Station Example - PBS to AWS Ground Station Agent Public
 Subnet"
      - Key: "Description"
        Value: "Subnet for EC2 instance receiving AWS Ground Station data"

  RouteTable:
    Type: AWS::EC2::RouteTable
    Properties:
      VpcId: !Ref ReceiverVPC
      Tags:
        - Key: Name
          Value: AWS Ground Station Example - RouteTable

  RouteTableAssociation:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref RouteTable
      SubnetId: !Ref PublicSubnet

  Route:
    Type: AWS::EC2::Route
    DependsOn: InternetGateway
    Properties:
      RouteTableId: !Ref RouteTable
      DestinationCidrBlock: '0.0.0.0/0'
      GatewayId: !Ref InternetGateway

  InternetGateway:
    Type: AWS::EC2::InternetGateway
    Properties:
      Tags:
        - Key: Name
          Value: AWS Ground Station Example - Internet Gateway

  GatewayAttachment:
    Type: AWS::EC2::VPCGatewayAttachment
    Properties:
      VpcId: !Ref ReceiverVPC
```

```
      InternetGatewayId: !Ref InternetGateway
```

> **Note**
>
> Pour plus d'informations sur les VPC configurations prises en charge par l' AWS Ground Station agent, consultez la section Exigences relatives àAWS Ground Station l'agent : VPC diagrammes.

Vous allez ensuite configurer l'EC2instance Amazon de Receiver.

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

 # This is required for the EIP if the receiver EC2 instance is in a private subnet.
 # This ENI must exist in a public subnet, be attached to the receiver and be
associated with the EIP.
 ReceiverInstanceNetworkInterface:
   Type: AWS::EC2::NetworkInterface
   Properties:
     Description: Floating network interface
     GroupSet:
       - !Ref InstanceSecurityGroup
     SubnetId: !Ref PublicSubnet

 # An EIP providing a fixed IP address for AWS Ground Station to connect to. Attach it
to the receiver instance created in the stack.
 ReceiverInstanceElasticIp:
   Type: AWS::EC2::EIP
   Properties:
     Tags:
       - Key: Name
         Value: !Join [ "-" , [ "EIP" , !Ref "AWS::StackName" ] ]

 # Attach the ENI to the EC2 instance if using a separate public subnet.
 # Requires the receiver instance to be in a public subnet (SubnetId should be the id
of a public subnet)
 ReceiverNetworkInterfaceAttachment:
```

```
    Type: AWS::EC2::NetworkInterfaceAttachment
    Properties:
      DeleteOnTermination: false
      DeviceIndex: 1
      InstanceId: !Ref ReceiverInstance
      NetworkInterfaceId: !Ref ReceiverInstanceNetworkInterface

  # Associate EIP with the ENI if using a separate public subnet for the ENI.
  ReceiverNetworkInterfaceElasticIpAssociation:
    Type: AWS::EC2::EIPAssociation
    Properties:
      AllocationId: !GetAtt [ReceiverInstanceElasticIp, AllocationId]
      NetworkInterfaceId: !Ref ReceiverInstanceNetworkInterface

  # The EC2 instance that will send/receive data to/from your satellite using AWS
 Ground Station.
  ReceiverInstance:
    Type: AWS::EC2::Instance
    DependsOn: PublicSubnet
    Properties:
      DisableApiTermination: false
      IamInstanceProfile: !Ref GeneralInstanceProfile
      ImageId: !Ref ReceiverAMI
      AvailabilityZone: !Ref AZ
      InstanceType: c5.24xlarge
      KeyName: !Ref EC2Key
      Monitoring: true
      PlacementGroupName: !Ref ClusterPlacementGroup
      SecurityGroupIds:
        - Ref: InstanceSecurityGroup
      SubnetId: !Ref PublicSubnet
      Tags:
        - Key: Name
          Value: !Join [ "-" , [ "Receiver" , !Ref "AWS::StackName" ] ]
      # agentCpuCores list in the AGENT_CONFIG below defines the cores that the AWS
 Ground Station Agent is allowed to run on. This list can be changed to suit your use-
case, however if the agent isn't supplied with enough cores data loss may occur.
      UserData:
        Fn::Base64:
          Fn::Sub:
            - |
              #!/bin/bash
              yum -y update
```

```
              AGENT_CONFIG_PATH="/opt/aws/groundstation/etc/aws-gs-agent-config.json"
              cat << AGENT_CONFIG > "$AGENT_CONFIG_PATH"
              {
                "capabilities": [
                  "arn:aws:groundstation:${AWS::Region}:${AWS::AccountId}:dataflow-
endpoint-group/${DataflowEndpointGroupId}"
                ],
                "device": {
                  "privateIps": [
                    "127.0.0.1"
                  ],
                  "publicIps": [
                    "${EIP}"
                  ],
                  "agentCpuCores": [

 24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,72,73,74,75,76,77,78,79,80,81,8
                  ]
                }
              }
              AGENT_CONFIG

              systemctl start aws-groundstation-agent
              systemctl enable aws-groundstation-agent

              # <Tuning Section Start>
              # Visit the AWS Ground Station Agent Documentation in the User Guide for
 more details and guidance updates

              # Set IRQ affinity with list of CPU cores and Receive Side Scaling mask
              # Core list should be the first two cores (and hyperthreads) on each
 socket
              # Mask set to everything currently
              # https://github.com/torvalds/linux/blob/v4.11/Documentation/networking/
scaling.txt#L80-L96
              echo "@reboot sudo /opt/aws/groundstation/bin/set_irq_affinity.sh '0 1 48
 49' 'ffffffff,ffffffff,ffffffff' >>/var/log/user-data.log 2>&1" >>/var/spool/cron/root

              # Reserving the port range defined in the GS agent ingress address in
 the Dataflow Endpoint Group so the kernel doesn't steal any of them from the GS agent.
 These ports are the ports that the GS agent will ingress data
              # across, so if the kernel steals one it could cause problems ingressing
 data onto the instance.
              echo net.ipv4.ip_local_reserved_ports="42000-50000" >> /etc/sysctl.conf
```

```
              # </Tuning Section End>

              # We have to reboot for linux kernel settings to apply
              shutdown -r now

            - DataflowEndpointGroupId: !Ref DataflowEndpointGroup
              EIP: !Ref ReceiverInstanceElasticIp
```

```
 # The AWS Ground Station Dataflow Endpoint Group that defines the endpoints that AWS
Ground
 # Station will use to send/receive data to/from your satellite.
 DataflowEndpointGroup:
   Type: AWS::GroundStation::DataflowEndpointGroup
   Properties:
     ContactPostPassDurationSeconds: 180
     ContactPrePassDurationSeconds: 120
     EndpointDetails:
       - AwsGroundStationAgentEndpoint:
           Name: !Join [ "-" , [ !Ref "AWS::StackName" , "Downlink" ] ] # needs to
match DataflowEndpointConfig name
           EgressAddress:
             SocketAddress:
               Name: 127.0.0.1
               Port: 55000
           IngressAddress:
             SocketAddress:
               Name: !Ref ReceiverInstanceElasticIp
               PortRange:
                 Minimum: 42000
                 Maximum: 55000
```

Vous aurez également besoin des politiques, des rôles et des profils appropriés pour AWS Ground Station créer l'elastic network interface (ENI) dans votre compte.

```
 # 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 configurations

Cette section représente Étape 3 : créer des configurations la mise en route.

Vous aurez besoin d'une configuration de suivi pour définir vos préférences en matière d'utilisation du suivi automatique. La sélection en PREFERREDtant que piste automatique peut améliorer la qualité du signal, mais elle n'est pas nécessaire pour atteindre la qualité du signal en raison de la qualité d'éphéméride JPSS -1 suffisante.

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

Sur la base du chemin de communication, vous devez définir une configuration antenne-liaison descendante pour représenter la partie satellite, ainsi qu'une configuration de point de terminaison

de flux de données pour faire référence au groupe de points de terminaison de flux de données qui définit les détails du point de terminaison.

```
 # 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 profil de mission

Cette section représente Étape 4 : Création d'un profil de mission la mise en route.

Maintenant que vous disposez des configurations associées, vous pouvez les utiliser pour créer le flux de données. Vous utiliserez les valeurs par défaut pour les autres paramètres.

```
  # 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
```

Assemblage

Grâce aux ressources ci-dessus, vous avez désormais la possibilité de planifier JPSS 1 à 1 contact pour la livraison synchrone des données depuis n'importe lequel de vos contacts intégrés. AWS Ground Station Emplacements

Ce qui suit est un AWS CloudFormation modèle complet qui inclut toutes les ressources décrites dans cette section combinées dans un modèle unique qui peut être directement utilisé dans AWS CloudFormation.

Le AWS CloudFormation modèle nommé `DirectBroadcastSatelliteWbDigIfEc2DataDelivery.yml` est conçu pour vous permettre de commencer rapidement à recevoir des données de fréquence intermédiaire numérisées (DigIF) pour les satellites Aqua SNPPJPSS, NOAA -1/ -20 et Terra. Il contient une EC2 instance Amazon et les AWS CloudFormation ressources nécessaires pour recevoir les données brutes de diffusion directe de DigiF à l'aide AWS Ground Station de l'agent.

Si AquaSNPP, JPSS -1/ NOAA -20 et Terra ne sont pas intégrés à votre compte, consultez. Étape 1 : Intégration du satellite

> **Note**
>
> Vous pouvez accéder au modèle en accédant au compartiment Amazon S3 qui intègre le client. Les liens ci-dessous utilisent un compartiment Amazon S3 régional. Modifiez le code de `us-west-2` région pour représenter la région correspondante dans laquelle vous souhaitez créer la AWS CloudFormation pile.
> De plus, les instructions suivantes utilisentYAML. Cependant, les modèles sont disponibles à la fois dans un JSON format YAML et dans un autre. Pour l'utiliserJSON, remplacez l'extension de `.yml` fichier par `.json` lors du téléchargement du modèle.

Pour télécharger le modèle à l'aide de AWS CLI, utilisez la commande suivante :

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

Vous pouvez consulter et télécharger le modèle dans la console en accédant à ce qui suit URL dans votre navigateur :

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

Vous pouvez définir le modèle directement en AWS CloudFormation utilisant le lien suivant :

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

Quelles ressources supplémentaires le modèle définit-il ?

Le `DirectBroadcastSatelliteWbDigIfEc2DataDelivery` modèle inclut les ressources supplémentaires suivantes :

- Interface réseau élastique de l'instance de réception - (Conditionnel) Une interface réseau élastique est créée dans le sous-réseau spécifié par PublicSubnetIds'il est fourni. Cela est nécessaire si l'instance du récepteur se trouve dans un sous-réseau privé. L'interface Elastic network sera associée à l'instance de réception EIP et attachée à celle-ci.
- IP élastique de l'instance de réception : adresse IP élastique à laquelle se AWS Ground Station connectera. Cela s'attache à l'instance du récepteur ou à l'interface Elastic Network.

- L'une des associations d'adresses IP élastiques suivantes :
  - Association entre l'instance de récepteur et l'adresse IP élastique : association de l'adresse IP élastique à votre instance de récepteur, si elle n'PublicSubnetIdest pas spécifiée. Cela nécessite de SubnetIdréférencer un sous-réseau public.
  - Association entre l'interface réseau élastique de l'instance de récepteur et l'interface IP élastique : association de l'adresse IP élastique à l'interface réseau élastique de l'instance de réception, si elle PublicSubnetIdest spécifiée.
- (Facultatif) Déclencheurs d'CloudWatch événements : AWS Lambda fonction déclenchée à l'aide d' CloudWatch événements envoyés AWS Ground Station avant et après un contact. La AWS Lambda fonction démarrera et arrêtera éventuellement votre instance de réception.
- (Facultatif) Amazon EC2 Verification pour les contacts : possibilité d'utiliser Lambda pour configurer un système de vérification de vos EC2 instances Amazon pour les contacts avec SNS notification. Il est important de noter que cela peut entraîner des frais en fonction de votre utilisation actuelle.
- Profils de mission supplémentaires - Profils de mission pour d'autres satellites de diffusion publique (AquaSNPP, et Terra).
- Configurations supplémentaires de liaison descendante d'antenne - Configurations de liaison descendante d'antenne pour des satellites de diffusion publics supplémentaires (Aqua, et Terra). SNPP

Les valeurs et paramètres pour les satellites dans ce modèle sont déjà renseignés. Ces paramètres vous permettent d'utiliser facilement et AWS Ground Station immédiatement ces satellites. Vous n'avez pas besoin de configurer vos propres valeurs pour pouvoir les utiliser AWS Ground Station lors de l'utilisation de ce modèle. Toutefois, vous pouvez personnaliser les valeurs pour que le modèle fonctionne selon votre cas d'utilisation.

Où puis-je recevoir mes données ?

Le groupe de points de terminaison de flux de données est configuré pour utiliser l'interface réseau d'instance de récepteur créée dans le cadre du modèle. L'instance de réception utilise l' AWS Ground Station agent pour recevoir le flux de données depuis le port défini par AWS Ground Station le point de terminaison du flux de données. Pour plus d'informations sur la configuration d'un groupe de points de terminaison de flux de données, consultez AWS::GroundStation::DataflowEndpoint la section Groupe. Pour plus d'informations sur l' AWS Ground Station agent, voir Qu'est-ce que l' AWS Ground Station agent ?

Résolution des problèmes

La documentation suivante peut vous aider à résoudre les problèmes susceptibles de survenir lors de l'utilisation AWS Ground Station.

Rubriques

Résolution des problèmes liés aux contacts qui fournissent des données à Amazon EC2

Si vous ne parvenez pas à terminer un AWS Ground Station contact, vous devez vérifier que votre EC2 instance Amazon est en cours d'exécution, vérifier que votre application de point de terminaison de flux de données est en cours d'exécution et vérifier que le flux de votre application de point de terminaison de flux de données est correctement configuré.

> **Note**
>
> DataDefender (DDX) est un exemple d'application de point de terminaison de flux de données actuellement prise en charge par AWS Ground Station

Prérequis

Les procédures suivantes supposent qu'une EC2 instance Amazon est déjà configurée. Pour configurer une EC2 instance Amazon dans AWS Ground Station, consultez Getting Started.

Étape 1 : vérifier que votre EC2 instance est en cours d'exécution

1. Localisez l'EC2instance Amazon qui a été utilisée pour le contact que vous êtes en train de dépanner. Procédez comme suit :

a. Dans votre AWS CloudFormationtableau de bord, sélectionnez la pile qui contient votre EC2 instance Amazon.

b. Choisissez l'onglet Ressources et localisez votre EC2 instance Amazon dans la colonne Logical ID. Vérifiez que l'instance est créée dans la colonne Statut.

c. Dans la colonne Physical ID, choisissez le lien de votre EC2 instance Amazon. Vous serez redirigé vers la console EC2 de gestion Amazon.

2. Dans la console EC2 de gestion Amazon, assurez-vous que l'état de votre EC2 instance Amazon est en cours d'exécution.

3. Si votre instance est en cours d'exécution, passez à l'étape suivante. Si votre instance n'est pas en cours d'exécution, démarrez-la en procédant comme suit :

   - Une fois votre EC2 instance Amazon sélectionnée, choisissez Actions > État de l'instance > Démarrer.

Étape 2 : Déterminer le type d'application de flux de données utilisé

Si vous utilisez l'AWS Ground Station agent pour la livraison de données, veuillez vous rediriger vers la section AWS Ground Station Agent de résolution des problèmes. Sinon, si vous utilisez l'application DataDefender (DDX), continuez surthe section called "Étape 3 : vérifier que l'application de flux de données est en cours d'exécution".

Étape 3 : vérifier que l'application de flux de données est en cours d'exécution

Pour vérifier le statut de DataDefender , vous devez vous connecter à votre instance sur AmazonEC2. Pour plus de détails sur la connexion à votre instance, consultez la section Se connecter à votre instance Linux.

La procédure suivante décrit les étapes de résolution des problèmes à l'aide de commandes dans un SSH client.

1. Ouvrez un terminal ou une invite de commande et connectez-vous à votre EC2 instance Amazon en utilisantSSH. Transférez le port 80 de l'hôte distant afin d'afficher l'interface utilisateur DataDefender Web. Les commandes suivantes montrent comment se connecter SSH à une EC2 instance Amazon via un bastion avec la redirection de port activée.

> **Note**
>
> Vous devez remplacer < SSH KEY >, < BASTION HOST > et < HOST > par votre clé SSH, le nom d'hôte Bastion et le nom d'hôte de l'EC2instance Amazon spécifiques.

Pour Windows

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

Pour Mac

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

2. Vérifiez que DataDefender (également appeléDDX) est en cours d'exécution en greppant (vérifiant) un processus en cours nommé ddx dans la sortie. La commande de vérification de l'existence d'un processus en cours d'exécution est fournie ci-dessous, avec un exemple de sortie réussie.

```
[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
```

Si elle DataDefender est en cours d'exécution, passez à la section the section called “Étape 4 : Vérifiez que le flux d'applications de votre flux de données est configuré” Sinon, passez à l'étape suivante.

3. Commencez DataDefender à utiliser la commande ci-dessous.

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

S'il DataDefender est en cours d'exécution après avoir utilisé la commande, passez à la section the section called "Étape 4 : Vérifiez que le flux d'applications de votre flux de données est configuré" Sinon, passez à l'étape suivante.

4. Inspectez les fichiers suivants à l'aide des commandes ci-dessous pour voir s'il y a eu des erreurs lors de l'installation et de la configuration DataDefender.

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

> **Note**
>
> Un problème courant découvert lors de l'inspection de ces fichiers est que l'Amazon sur VPC lequel votre EC2 instance Amazon est exécutée n'a pas accès à Amazon S3 pour télécharger les fichiers d'installation. Si vous découvrez dans vos journaux que c'est le problème, vérifiez les paramètres Amazon VPC et du groupe de sécurité de votre EC2 instance pour vous assurer qu'ils ne bloquent pas l'accès à Amazon S3.

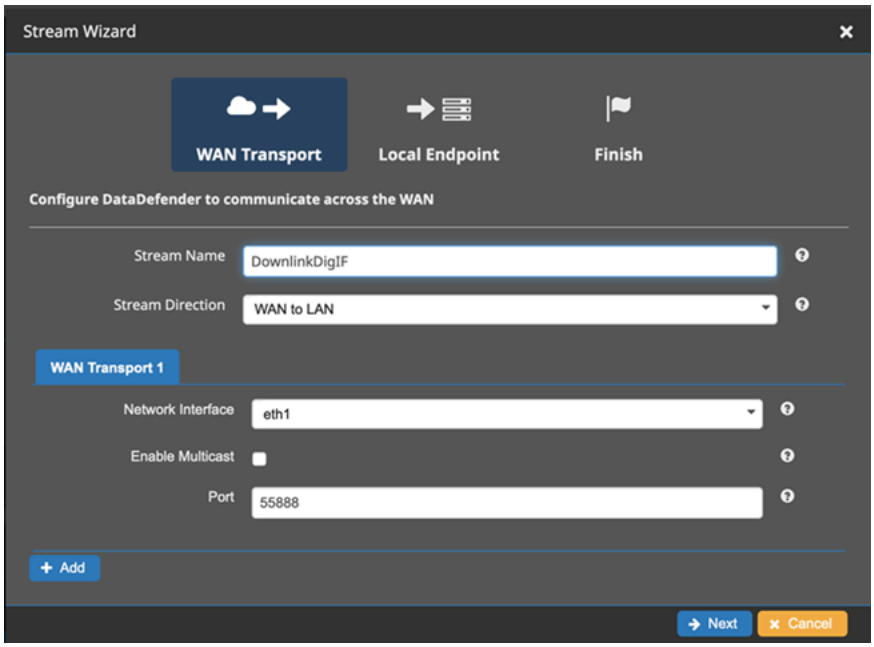
S'il DataDefender est en cours d'exécution après avoir vérifié vos VPC paramètres Amazon, passez àthe section called "Étape 4 : Vérifiez que le flux d'applications de votre flux de données est configuré". Si le problème persiste, contactez le AWS Support et envoyez vos fichiers journaux avec une description de votre problème.

Étape 4 : Vérifiez que le flux d'applications de votre flux de données est configuré

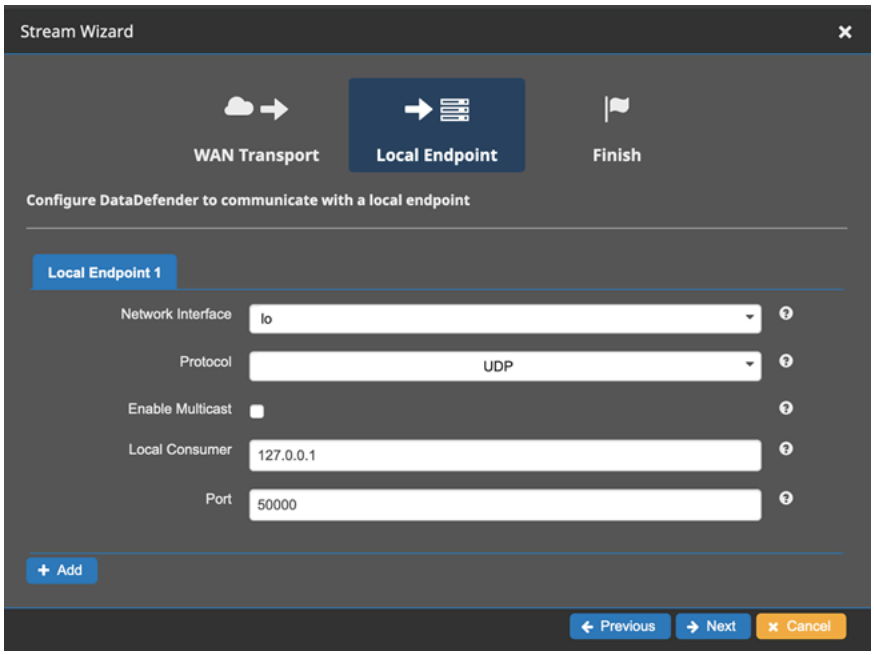
1. Dans un navigateur Web, accédez à votre interface utilisateur DataDefender Web en saisissant l'adresse suivante dans la barre d'adresse : localhost:8080. Ensuite, appuyez sur Entrée.
2. Sur le DataDefendertableau de bord, choisissez Accéder aux détails.
3. Sélectionnez votre flux dans la liste des flux, puis choisissez Edit Stream (Modifier le flux).
4. Dans la boîte de dialogue Stream Wizard (Assistant de flux), procédez comme suit :

   a. Dans le volet WANTransport, assurez-vous que WANl'option « Direction du flux » LAN est sélectionnée.

b. Dans le champ Port, assurez-vous que le WAN port que vous avez choisi pour votre groupe de points de terminaison de flux de données est présent. Par défaut, ce port est 55888. Ensuite, choisissez Suivant.



c. Dans le panneau Local Endpoint (Point de terminaison local), vérifiez qu'un port valide est présent dans la zone Port. Par défaut, ce port est 50000. Il s'agit du port sur lequel vous recevrez vos données après DataDefender les avoir reçues du AWS Ground Station service. Ensuite, choisissez Suivant.



d. Choisissez Finish (Terminer) dans le menu restant si vous avez modifié des valeurs. Sinon, vous pouvez procéder à l'annulation à partir du menu Stream Wizard (Assistant de flux).

Vous avez maintenant vérifié que votre EC2 instance Amazon fonctionne et DataDefender est configurée correctement pour recevoir des données de AWS Ground Station. Si vous continuez à rencontrer des problèmes, contactez AWS le Support.

FAILEDContacts de dépannage

Un contact aura le statut de contact terminal correspondant à la FAILEDdétection AWS Ground Station d'un problème avec la configuration de vos ressources. Les cas d'utilisation courants susceptibles de provoquer des FAILEDcontacts sont fournis ci-dessous, ainsi que les étapes à suivre pour résoudre les problèmes.

> **Note**
>
> Ce guide est spécifiquement destiné à l'état du FAILEDcontact et n'est pas destiné aux autres états de défaillance, tels que AWS_ FAILEDCANCELLED, AWS_ ou FAILEDSCHEDULE_TO_. Pour plus d'informations sur les statuts des contacts, voir the section called "AWS Ground Station statuts des contacts"

Cas d'utilisation des terminaux FAILED Dataflow

Voici la liste des cas d'utilisation courants qui peuvent entraîner un statut de FAILEDcontact pour les flux de données basés sur des points de terminaison de flux de données :

- Le point de terminaison de flux de données ne se connecte jamais - La connexion entre l' AWS Ground Station antenne et votre groupe de points de terminaison de flux de données pour un ou plusieurs flux de données n'a jamais été établie.
- Connexion tardive du point de terminaison du flux de données : la connexion entre l' AWS Ground Station antenne et votre groupe de points de terminaison de flux de données pour un ou plusieurs flux de données a été établie après l'heure de début du contact.

Pour tout cas de défaillance d'un point de terminaison de flux de données, il est recommandé d'examiner les points suivants :

- Vérifiez que l'EC2instance Amazon du destinataire a bien été démarrée avant l'heure de début du contact.
- Vérifiez que le logiciel de point de terminaison du flux de données était opérationnel pendant le contact.

Consultez la section sur les étapes Résolution des problèmes liés aux contacts qui fournissent des données à Amazon EC2 de résolution des problèmes plus spécifiques.

AWS Ground Station Cas FAILED d'utilisation des agents

Voici la liste des cas d'utilisation courants qui peuvent entraîner un statut de FAILEDcontact pour les flux de données basés sur des agents :

- AWS Ground Station État jamais signalé à l'agent : l'agent chargé d'orchestrer la livraison des données sur votre groupe de points de terminaison de flux de données pour un ou plusieurs flux de données n'a jamais correctement signalé l'état à. AWS Ground Station Cette mise à jour du statut devrait avoir lieu quelques secondes après la fin du contact.
- AWS Ground Station Agent démarré en retard : l'agent chargé d'orchestrer la livraison des données sur votre groupe de points de terminaison de flux de données pour un ou plusieurs flux de données a démarré en retard, après l'heure de début du contact.

Pour tout cas de défaillance du flux de données de l' AWS Ground Station agent, il est recommandé de prendre en compte les points suivants :

- Vérifiez que l'EC2instance Amazon du destinataire a bien été démarrée avant l'heure de début du contact.
- Vérifiez que l'application Agent était opérationnelle au début et pendant le contact.
- Vérifiez que l'application Agent et l'EC2instance Amazon n'ont pas été arrêtées dans les 15 secondes suivant la fin du contact. Cela donne à l'agent suffisamment de temps pour signaler l'état à AWS Ground Station.

Consultez la section sur les étapes Résolution des problèmes liés aux contacts qui fournissent des données à Amazon EC2 de résolution des problèmes plus spécifiques.

Résolution des problèmes liés aux FAILED contacts _TO_ SCHEDULE

Un contact se terminera dans un SCHEDULE état FAILED_À_ lorsqu'il AWS Ground Station détecte un problème lié à la configuration de vos ressources ou au sein du système interne. Un contact qui se termine par un SCHEDULE état FAILED_TO_ fournira éventuellement un contexte `errorMessage` supplémentaire. Pour plus d'informations sur la description des contacts, consultez le DescribeContactAPI.

Les cas d'utilisation courants pouvant entraîner des SCHEDULE contacts FAILED_TO_ sont fournis ci-dessous, ainsi que des étapes pour aider à résoudre les problèmes.

> **Note**
>
> Ce guide est spécifiquement destiné à l'état du SCHEDULE contact FAILED_TO_ et n'est pas destiné aux autres états de défaillance, tels que AWS_FAILED, AWS_ CANCELLED ou. FAILED Pour plus d'informations sur les statuts des contacts, voir the section called "AWS Ground Station statuts des contacts"

Les paramètres spécifiés dans votre Antenna Downlink Demod Decode Config ne sont pas pris en charge

Le profil de mission utilisé pour planifier ce contact avait une antenna-downlink-demod-decode configuration qui n'était pas valide.

AntennaDownlinkDemodDecode Configuration existante

- Si vos antenna-downlink-demod-decode configurations ont récemment été modifiées, revenez à une version qui fonctionnait auparavant avant de tenter de planifier.
- S'il s'agit d'une modification intentionnelle d'une configuration existante ou d'une configuration existante qui n'est plus correctement planifiée, suivez l'étape suivante pour intégrer une nouvelle AntennaDownlinkDemodDecode configuration.

AntennaDownlinkDemodDecode Configuration nouvellement créée

Contactez-nous AWS Ground Station directement pour intégrer votre nouvelle configuration. Créez un dossier avec AWSSupport, y compris celui `contactId` qui s'est terminé par l'état FAILED_TO_ SCHEDULE

Étapes générales de résolution des problèmes

Si les étapes de résolution des problèmes précédentes n'ont pas permis de résoudre votre problème :

- Réessayez de planifier le contact ou planifiez un autre contact en utilisant le même profil de mission. Pour plus d'informations sur la façon de réserver un contact, consultez ReserveContact.
- Si vous continuez à recevoir le SCHEDULE statut FAILED_TO_ pour ce profil de mission, contactez le Support AWS

Le dépannage DataflowEndpointGroups n'est pas en HEALTHY état

Vous trouverez ci-dessous les raisons pour lesquelles vos groupes de points de terminaison de flux de données ne sont peut-être pas en bon `HEALTHY` état, ainsi que les mesures correctives appropriées à prendre.

- `NO_REGISTERED_AGENT`- Démarrez votre EC2 instance, qui enregistrera l'agent. Notez que vous devez disposer d'un fichier de configuration de contrôleur valide pour que cet appel réussisse. Reportez-vous au AWS Ground Station Agent pour plus de détails sur la configuration de ce fichier.
- `INVALID_IP_OWNERSHIP`- Utilisez le DeleteDataflowEndpointGroup API pour supprimer le groupe de points de terminaison de flux de données, puis utilisez le CreateDataflowEndpointGroup API pour recréer le groupe de points de terminaison de flux de données à l'aide des adresses IP et des ports associés à l'instance. EC2
- `UNVERIFIED_IP_OWNERSHIP`- L'adresse IP n'a pas encore été validée. La validation a lieu périodiquement, ce problème devrait donc se résoudre de lui-même.
- `NOT_AUTHORIZED_TO_CREATE_SLR`- Le compte n'est pas autorisé à créer le rôle lié au service nécessaire. Consultez les étapes de résolution des problèmes dans Utilisation de rôles liés à un service pour Ground Station

Résolution des éphémérides non valides

Lorsqu'une éphéméride personnalisée est téléchargée, AWS Ground Station elle passe par un flux de travail de validation asynchrone avant de devenir. `ENABLED` Ce flux de travail garantit la validité des identifiants, des métadonnées et de la trajectoire des satellites.

Lorsqu'une éphéméride échoue à la validation, `DescribeEphemeris` renvoie un EphemerisInvalidReason, qui indique pourquoi la validation de l'éphéméride a échoué. Les valeurs potentielles du EphemerisInvalidReasonsont les suivantes :

Valeur	Description	Action de résolution des problèmes
METADATA_INVALID	Les identifiants d'engin spatial fournis, tels que l'identifiant du satellite, ne sont pas valides	Vérifiez l'NORADidentifiant ou les autres identifiants fournis dans les données sur les éphémérides
TIME_RANGE_INVALID	Les heures de début, de fin ou d'expiration ne sont pas valides pour les éphémérides fournies	Assurez-vous que l'heure de début est antérieure à « maintenant » (il est recommandé de définir l'heure de début quelques minutes auparavant), que l'heure de fin est postérieure à l'heure de début et que l'heure de fin est postérieure à l'heure d'expirat ion
TRAJECTORY_INVALID	L'éphéméride fournie définit une trajectoire d'engin spatial non valide	Vérifiez que la trajectoire fournie est continue et qu'elle correspond au bon satellite.
VALIDATION_ERROR	Une erreur de service interne s'est produite lors du traitemen t des éphémérides à des fins de validation	Réessayez de télécharger

Un exemple de `DescribeEphemeris` réponse pour une `INVALID` éphéméride est fourni ci-dessous :

```
{
  "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**
>
> Si le statut d'une éphéméride est le cas`ERROR`, l'éphéméride n'est pas `ENABLED` due à un problème lié au service. AWS Ground Station Vous devriez essayer de fournir à nouveau les éphémérides via. `CreateEphemeris` La nouvelle éphéméride peut apparaître `ENABLED` si le problème était transitoire.

Résolution des problèmes liés aux contacts n'ayant reçu aucune donnée

Il est possible qu'un contact semble avoir réussi, mais qu'il n'ait toujours pas reçu de données. Cela peut signifier que vous recevez des PCAP fichiers vides, voire aucun PCAP fichier du tout si vous utilisez la livraison de données S3. Cela peut se produire pour plusieurs raisons. Ce qui suit décrit certaines de ces causes et explique comment y remédier.

Configuration de liaison descendante incorrecte

Chaque contact recevant des données d'un satellite sera associé à un Config d'antenne de liaison descendante ouConfig de décodage/démodulation des signaux d'antenne de liaison descendante . Si la configuration spécifiée ne correspond pas au signal transmis par un satellite, il ne AWS Ground Station sera pas en mesure de recevoir le signal transmis. Il en résultera qu'aucune donnée ne sera reçue par AWS Ground Station.

Pour résoudre ce problème, veuillez vérifier que les configurations que vous utilisez correspondent au signal transmis par votre satellite. Par exemple, vérifiez que vous avez défini les bons paramètres de fréquence centrale, de bande passante, de polarisation et, si nécessaire, de démodulation et de décodage.

Manœuvre du satellite

Il arrive qu'un satellite effectue une manœuvre qui désactive temporairement certains de ses systèmes de communication. La manœuvre peut également modifier de manière significative la position du satellite dans le ciel. AWS Ground Station ne sera pas en mesure de recevoir un signal d'un satellite qui n'émet aucun signal, ou si l'éphéméride utilisée fait pointer l' AWS Ground Station antenne vers un endroit du ciel où le satellite n'est pas présent.

Si vous essayez de communiquer avec un satellite de diffusion public exploité parNOAA, vous trouverez peut-être un message décrivant une panne ou une manœuvre sur la page des messages d'alerte NOAA par satellite. Le message peut inclure une chronologie indiquant à quel moment la transmission de données devrait reprendre, ou cette chronologie peut être publiée dans un message suivant.

Si vous communiquez avec vos propres satellites, il est de votre responsabilité de comprendre le fonctionnement de vos satellites et l'impact que cela peut avoir sur la communication avec eux AWS Ground Station. Si vous effectuez une manœuvre qui aura un impact sur la trajectoire du satellite, cela peut inclure la fourniture de données d'éphémérides personnalisées mises à jour. Pour plus d'informations sur la fourniture de données d'éphémérides personnalisées, consultez. Fournir des données d'éphémérides personnalisées

AWS Ground Station panne

En AWS Ground Station cas d'échec ou d'annulation d'un contact, le statut du contact AWS Ground Station sera défini sur AWS_ FAILED ou AWS_ CANCELLED. Pour plus d'informations sur le cycle de vie des contacts, consultezCycle de vie des contacts. Dans certains cas, il AWS Ground Station

peut y avoir une défaillance qui empêche la transmission des données vers votre compte, mais n'entraîne pas le CANCELLED statut AWS_ FAILED ou AWS_ du contact. Dans ce cas, vous AWS Ground Station devez publier un événement spécifique au compte sur votre tableau de bord AWS Health. Pour plus d'informations sur le tableau AWS de bord Health, consultez le AWS Health User Guide.

Quotas et limites

Vous pouvez consulter les régions prises en charge, leurs points de terminaison associés, ainsi que les quotas sur les points de AWS Ground Station terminaison et les quotas.

Vous pouvez utiliser la console Service Quotas, AWS APIet le AWS CLIpour demander des augmentations de quotas, le cas échéant.

Modalités du service

Pour les conditions AWS Ground Station de service, veuillez vous référer aux conditions AWS de service.

Historique du document pour le guide de AWS Ground Station l'utilisateur

Le tableau suivant décrit les modifications importantes apportées à chaque version du guide de l' AWS Ground Station utilisateur.

Modification	Description	Date
Nouvelle fonctionnalité	Le guide de l'utilisateur a été mis à jour pour inclure le jumeau AWS Ground Station numérique.	6 août 2024
Mise à jour de documentation	De nombreuses sections du guide de l'utilisateur ont été mises à jour, notamment de nouveaux diagrammes, des exemples, etc.	18 juillet 2024
Mise à jour de documentation	RSSFil d'actualité ajouté au guide de l'utilisateur.	18 juillet 2024
Mise à jour de documentation	Divisez le guide de l'utilisa teur de l' AWS Ground Station agent en un guide de l'utilisa teur distinct.	18 juillet 2024
Nouvelle fonctionnalité	Les contacts peuvent désormais être programmé s jusqu'à 30 secondes en dehors des plages horaires de visibilité. Les temps de visibilit é sont inclus dans DescribeC ontact les réponses.	26 mars 2024
Mise à jour de documentation	Organisation améliorée et ajout de la section « Sélection	6 mars 2024

	et CPU planification des EC2 instances ».	
Mise à jour de documentation	Ajout de nouvelles bonnes pratiques au guide de l'utilisateur de l' AWS Ground Station agent pour exécuter des services et des processus parallèlement à l' AWS Ground Station agent.	23 février 2024
Mise à jour de documentation	Ajout de la page des notes de version de l'agent.	21 février 2024
Mise à jour du modèle	Ajout de la prise en charge d'un sous-réseau public distinct dans le DataDelivery modèle DirectBroadcastSatelliteWbDigIfEc 2.	14 février 2024
Mise à jour de documentation	Ajout d'une référence AWS Notifications des utilisateurs dans la documentation de surveillance.	6 août 2023
Mise à jour de documentation	Ajout d'instructions pour étiqueter les satellites avec un nom à afficher dans la AWS Ground Station console.	26 juillet 2023
Nouvelle fonctionnalité	Ajout du guide de l'utilisateur de l' AWS Ground Station agent pour la sortie de Wideband DigiF Data Delivery	12 avril 2023

Nouvelle politique AWS gérée	AWS Ground Station a ajouté une nouvelle politique nommée AWSGround StationAgentInstancePolicy.	12 avril 2023
Nouvelle fonctionnalité	Mise à jour du guide de l'utilisateur pour la sortie de CPE Preview.	9 novembre 2022
Nouvelle politique AWS gérée	AWS Ground Station a ajouté le AWSServiceRoleForGroundStationDataflowEndpointGroup service-linked-role (SLR) qui inclut une nouvelle politique nommée AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy.	2 novembre 2022
Nouvelle fonctionnalité	Mise à jour du guide de l'utilisateur pour inclure l'intégration avec AWS CLI.	17 avril 2020
Nouvelle fonctionnalité	Le guide de l'utilisateur a été mis à jour pour inclure l'intégration avec CloudWatch Metrics.	24 février 2020
Nouveau modèle	Satellites de diffusion publics (AquaSnppJpss modèle) ajouté au guide de AWS Ground Station l'utilisateur.	19 février 2020
Nouvelle fonctionnalité	Mise à jour du guide de l'utilisateur pour inclure la transmission des données entre régions.	5 février 2020

Mise à jour de documentation	Exemples et descriptions mis à jour pour la surveillance AWS Ground Station avec CloudWatch Events.	4 février 2020
Mise à jour de documentation	Les emplacements des modèles ont été mis à jour et les sections Démarrez et Dépannage ont été révisées.	19 décembre 2019
Nouvelle section de résolution des problèmes	Section de résolution des problèmes ajoutée au guide de AWS Ground Station l'utilisateur.	7 novembre 2019
Nouveau sujet de mise en route	Mise à jour de la rubrique Getting Started, qui inclut les AWS CloudFormation modèles les plus récents.	1 juillet 2019
Version Kindle	Version Kindle publiée du guide de l'AWS Ground Station utilisateur.	20 juin 2019
Nouveau guide et service	Il s'agit de la version initiale AWS Ground Station et du guide de AWS Ground Station l'utilisateur.	23 mai 2019

Glossaire AWS

Pour connaître la terminologie la plus récente d'AWS, consultez le Glossaire AWS dans la Référence Glossaire AWS.

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.