



使用者指南

AWS Ground Station



AWS Ground Station: 使用者指南

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能附屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

Table of Contents

什麼是 AWS Ground Station ?	1
常用案例	1
後續步驟	2
AWS Ground Station 運作方式	3
衛星加入	3
任務設定檔合成	3
聯絡排程	5
聯絡執行	6
數位分身	8
了解 AWS Ground Station 核心元件	8
任務設定檔	10
組態	12
Dataflow 端點群組	18
AWS Ground Station 代理程式	22
開始使用	24
註冊 AWS 帳戶	24
建立具有管理存取權的使用者	24
將 AWS Ground Station 許可新增至 AWS 您的帳戶	25
加入衛星	27
客戶加入程序概觀	27
(選用) 命名衛星	28
公有廣播衛星	30
規劃您的資料流程通訊路徑	31
非同步資料交付	31
同步資料交付	32
建立組態	32
資料交付組態	33
衛星組態	33
建立任務設定檔	33
了解後續步驟	34
AWS Ground Station 位置	35
尋找地面站點位置的 AWS 區域	35
AWS Ground Station 支援的 AWS 區域	36
數位分身可用性	37

AWS Ground Station 網站遮罩	37
客戶特定的遮罩	37
網站遮罩對可用聯絡時間的影響	37
AWS Ground Station 站點功能	38
了解 AWS Ground Station 如何使用衛星暫時性資料	41
預設暫時性資料	41
提供自訂暫時性資料	41
概觀	42
OEM ephemeris 格式	42
KVN 格式的範例 OEM ephemeris	45
建立自訂 ephemeris	46
範例：透過 API 建立雙行元素 (TLE) 集合 ephemeris	47
範例：從 S3 儲存貯體上傳 Ephemeris 資料	49
範例：搭配 使用客戶提供的 ephemeride AWS Ground Station	50
了解使用哪些 ephemeris	50
新暫時性事件對先前排程聯絡人的影響	50
取得衛星的目前暫時性資料	51
使用預設 ephemeris GetSatellite傳回衛星的範例	51
使用自訂 ephemeris 的GetSatellite衛星範例	52
還原至預設暫時性資料	52
使用資料流程	53
AWS Ground Station 資料平面界面	53
使用跨區域資料交付	54
設定 Amazon S3	55
設定 Amazon VPC	55
使用 AWS Ground Station 代理程式的 VPC 組態	56
具有資料流程端點的 VPC 組態	58
設定 Amazon EC2	60
提供的常見軟體	60
AWS Ground Station Amazon Machine Image AMIs)	61
使用聯絡人	62
了解聯絡生命週期	62
AWS Ground Station 聯絡狀態	64
AWS Ground Station 數位分身	65
監控	66
使用 事件自動化	66

AWS Ground Station 事件類型	67
聯絡事件時間表	67
Ephemeris 事件	70
使用 CloudTrail 記錄 API 呼叫	71
AWS Ground Station CloudTrail 中的資訊	71
了解 AWS Ground Station 日誌檔案項目	72
使用 Amazon CloudWatch 檢視指標	73
AWS Ground Station 指標和維度	73
檢視 指標	77
安全	82
身分和存取權管理	82
目標對象	83
使用身分驗證	83
使用政策管理存取權	86
AWS Ground Station 如何使用 IAM	88
身分型政策範例	93
故障診斷	96
AWS 受管政策	97
AWSGroundStationAgentInstancePolicy	98
AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy	99
政策更新	99
使用服務連結角色	100
Ground Station 的服務連結角色許可	100
為 Ground Station 建立服務連結角色	101
編輯 Ground Station 的服務連結角色	101
刪除 Ground Station 的服務連結角色	101
Ground Station 服務連結角色支援的區域	102
故障診斷	102
的靜態資料加密 AWS Ground Station	102
如何在 AWS KMS 中使用 AWS Ground Station 授予	103
建立客戶受管金鑰	104
指定的客戶受管金鑰 AWS Ground Station	106
AWS Ground Station 加密內容	106
監控 的加密金鑰 AWS Ground Station	108
傳輸期間的資料加密 AWS Ground Station	113
AWS Ground Station 代理程式串流	114

Dataflow 端點串流	114
範例任務設定檔組態	115
JPSS-1 - 公有廣播衛星 (PBS) - 評估	115
使用 Amazon S3 資料交付的公有廣播衛星	116
通訊路徑	116
AWS Ground Station 組態	118
AWS Ground Station 任務描述檔	119
將它放在一起	120
使用資料流程端點的公有廣播衛星 (窄頻帶)	121
通訊路徑	121
AWS Ground Station 組態	128
AWS Ground Station 任務描述檔	129
將它放在一起	129
使用資料流程端點的公有廣播衛星 (解調和解碼)	131
通訊路徑	131
AWS Ground Station 組態	138
AWS Ground Station 任務描述檔	141
將它放在一起	142
使用 AWS Ground Station 代理程式的公有廣播衛星 (寬頻)	144
通訊路徑	144
AWS Ground Station 組態	155
AWS Ground Station 任務描述檔	156
將它放在一起	157
疑難排解	160
對將資料交付至 Amazon EC2 的聯絡人進行故障診斷	160
步驟 1：確認您的 EC2 執行個體正在執行	160
步驟 2：判斷使用的資料流程應用程式類型	161
步驟 3：確認資料流程應用程式正在執行	161
步驟 4：確認您的資料流程應用程式串流已設定	163
步驟 5：確定您的接收者執行個體 (多個) 子網路中有足夠的可用 IP 地址	164
故障診斷失敗的聯絡案例	165
Dataflow 端點 FAILED 使用案例	165
AWS Ground Station 代理程式失敗的使用案例	166
故障診斷 FAILED_TO_SCHEDULE 聯絡人	166
不支援在天線下行解碼組態中指定的設定	167
一般故障診斷步驟	167

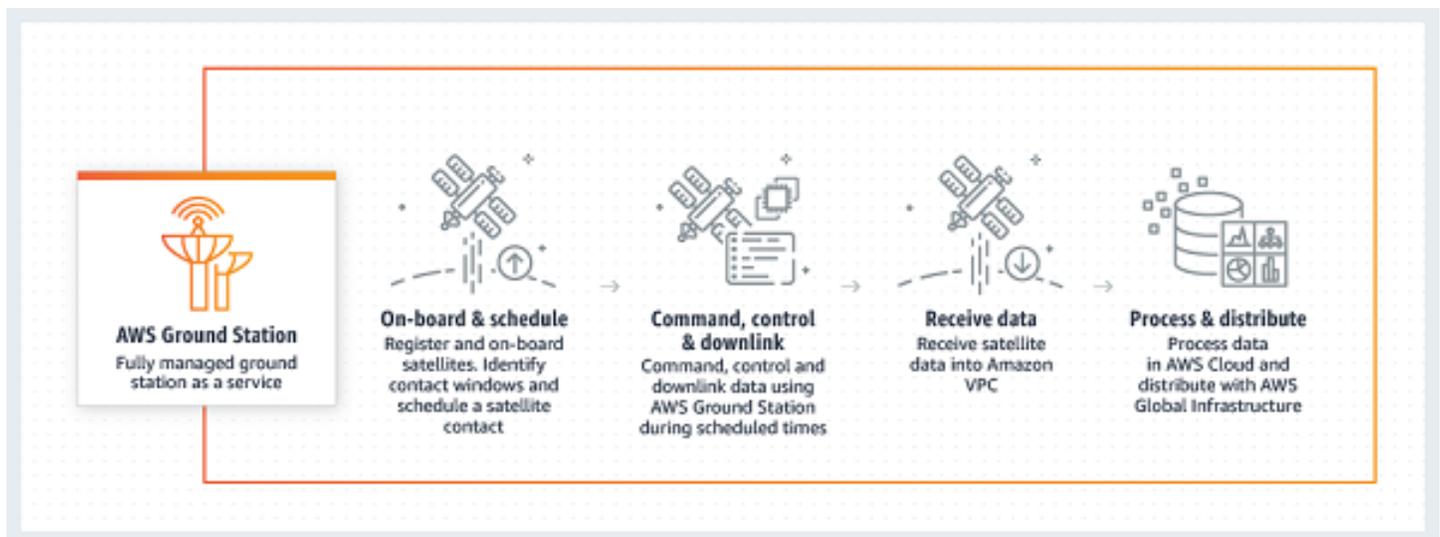
針對未處於 HEALTHY 狀態的 DataflowEndpointGroups 進行故障診斷	167
故障診斷無效的短暫性事件	168
對沒有收到資料的聯絡人進行故障診斷	169
下行組態不正確	169
衛星操控	170
AWS Ground Station 中斷	170
配額和限制	171
服務條款	172
文件歷史記錄	173
AWS 詞彙表	176
.....	clxxvii

什麼是 AWS Ground Station ？

AWS Ground Station 是一種全受管服務，可在全球基礎設施中提供安全、快速且可預測的衛星通訊。使用 AWS Ground Station，您不再需要建置、管理或擴展自己的地面站基礎設施。AWS Ground Station 可讓您專注於創新和快速實驗擷取衛星資料的新應用程式，而不是花費資源來建置、操作和擴展自己的地面站。

使用 AWS 的低延遲、高頻寬全球光纖網路，您可以在天線系統接收數秒內開始處理您的衛星資料。這可讓您在幾秒鐘內將原始資料轉換為已處理的資訊或已分析的知識。

常用案例



AWS Ground Station 可讓您雙向與衛星通訊，並支援下列使用案例：

- 下行資料 – 從衛星接收資料、傳輸 X 頻帶和 S 頻帶頻率、即時交付至 Amazon EC2 執行個體 (VITA-49 格式)，或直接交付至您帳戶中的 Amazon S3 儲存貯體 ([PCAP 格式](#))。此外，對於使用支援的調變和編碼方案的衛星，您可以選擇接收解調和解碼的資料，或原始數位中繼頻率 (DigIF) 範例 (VITA-49 格式)。
- 上行資料 – 透過傳送要傳輸的 DigIF 資料 (VITA-49 格式)，將資料和命令傳送至接收 S 頻帶頻率的衛星 AWS Ground Station。
- 上行回應 - 透過在實體共置天線上接收傳輸的訊號，驗證傳送至太空船的命令，並執行其他進階任務。
- 軟體定義的無線電 (SDR)/前端處理器 (FEP) – 使用可在 Amazon EC2 執行個體上執行的現有 SDR 和/或 FEP，即時處理資料以傳送/接收現有波形，並產生資料產品。

- 遙測、追蹤和命令 (TT&C) – 使用先前列出的使用案例組合來執行 TT&C，以管理您的衛星機群。
- 跨區域資料交付 – 使用來自單一 AWS 區域的 AWS Ground Station 全域天線網路同時操作多個聯絡人。
- 數位分身 – 測試排程、驗證組態，以及以較低成本適當處理錯誤，無需使用生產天線容量。

後續步驟

建議您一開始先閱讀下列各節：

- 若要了解基本 AWS Ground Station 概念，請參閱 [AWS Ground Station 運作方式](#)。
- 若要了解如何設定要使用的帳戶和資源 AWS Ground Station，請參閱 [開始使用](#)。
- 若要以程式設計方式使用 AWS Ground Station，請參閱 [AWS Ground Station API 參考](#)。API 參考 AWS Ground Station 會詳細說明 的所有 API 操作。它還提供支援 Web 服務通訊協定的範例請求、回應和錯誤。您可以使用您選擇的語言的 [AWS CLI](#) 或 [AWS SDK](#) 來撰寫與 互動的程式碼 AWS Ground Station。

AWS Ground Station 運作方式

AWS Ground Station 會操作地面型天線，以促進與衛星的通訊。天線可以執行的操作的實體特性是抽象的，稱為功能。您可以在 [AWS Ground Station 位置](#) 區段中參考天線的實體位置及其目前功能。如果您的使用案例需要額外的功能、其他位置產品或更精確的天線位置，請透過 <aws-groundstation@amazon.com> 聯絡我們。

若要使用其中一個 AWS Ground Station 天線，您必須在特定位置預留時間。此保留稱為聯絡人。若要成功排程聯絡人，AWS Ground Station 需要其他資料以確保成功。

- 您的衛星必須加入一或多個位置 – 這可確保您在請求的位置獲得操作各種功能的核准。
- 您的衛星必須具有有效的暫時性 – 這可確保天線具有視線，並且可以在聯絡期間準確指向您的衛星。
- 您必須擁有有效的任務描述檔 – 這可讓您自訂此聯絡人的行為，包括接收和傳送資料到衛星的方式。您可以針對同一部車輛使用多個任務設定檔來建立不同的聯絡人，以適應您遇到的不同操作狀態或案例。

衛星加入

將衛星加入 AWS Ground Station 是一個多步驟程序，涉及資料收集、技術驗證、頻譜授權，以及整合和測試。本指南的 [衛星加入](#) 區段將引導您完成此程序。

任務設定檔合成

衛星頻率資訊、[資料平面](#) 資訊和其他詳細資訊會封裝在任務設定檔中。任務描述檔是組態元件的集合。這可讓您重複使用不同任務描述檔之間的組態元件，因為符合您的使用案例。由於任務描述檔不會直接參考個別衛星，而是僅包含其技術功能的相關資訊，因此具有相同組態的多個衛星也可以重複使用任務描述檔。

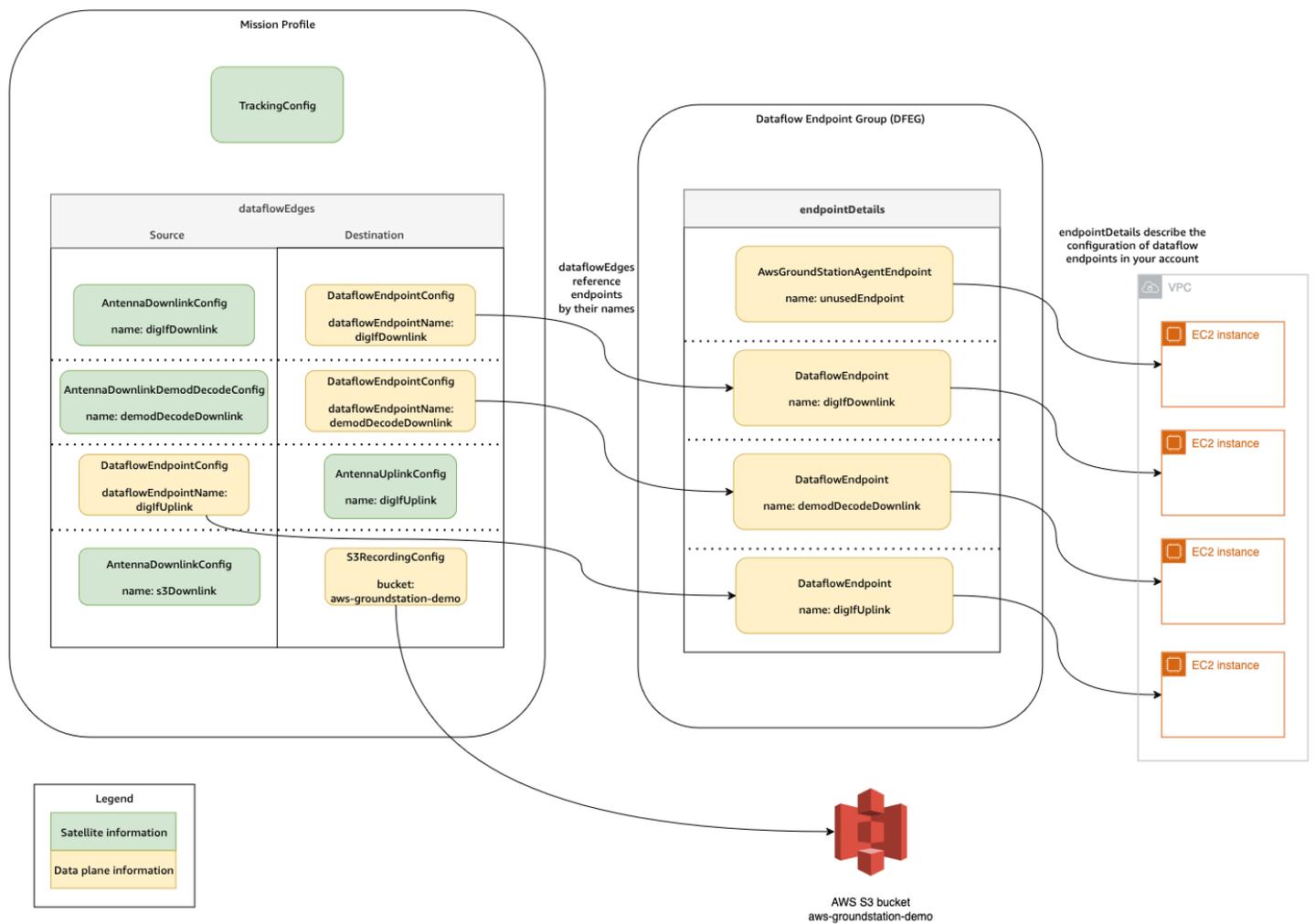
有效的任務描述檔將具有追蹤組態和一或多個資料流程。追蹤組態會指定您在聯絡期間追蹤的偏好設定。資料流程中的每個組態對都會建立來源和目的地。根據您的衛星及其操作模式，任務設定檔中的資料流程確切數量將有所不同，以代表您的上行和下行通訊路徑以及任何資料處理層面。

- 如需設定將在聯絡期間使用的 Amazon VPC、Amazon S3 和 Amazon EC2 資源的詳細資訊，請參閱 [使用資料流程](#)。
- 如需每個組態行為的詳細資訊，請參閱 [使用 AWS Ground Station 組態](#)。

- 如需所有預期參數的特定詳細資訊，請參閱 [使用 AWS Ground Station 任務設定檔](#)。
- 如需如何建立各種任務描述檔以支援使用案例的範例，請參閱 [範例任務設定檔組態](#)。

下圖顯示範例任務描述檔和其他所需的資源。請注意，此範例顯示此任務描述檔不需要的資料流程端點，名為 unusedEndpoint，以示範彈性。此範例支援下列資料流程：

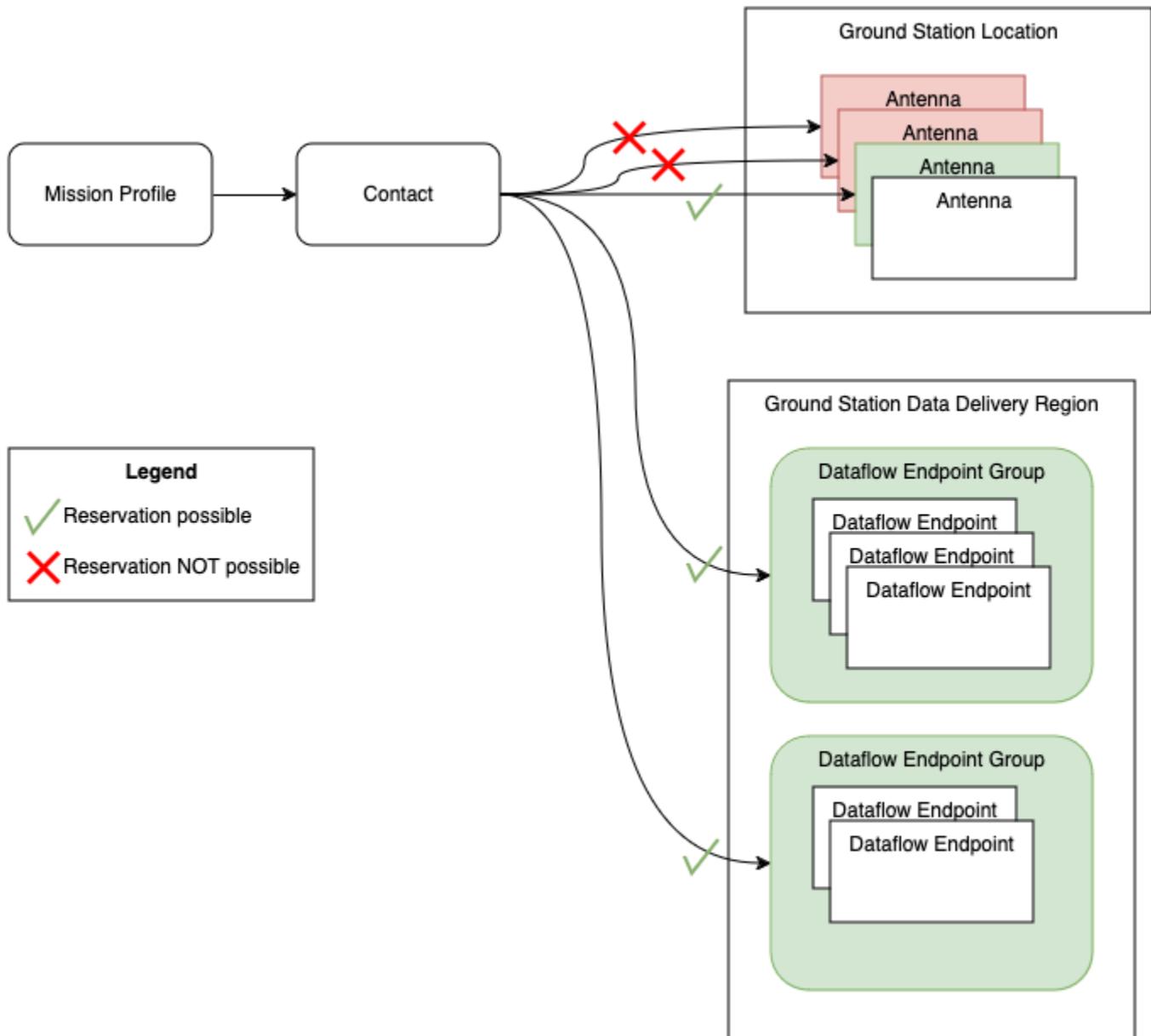
- 將數位中繼頻率資料同步下行至您管理的 Amazon EC2 執行個體。以 digIfDownlink 名稱表示。
- 數位中繼頻率資料的非同步下行至 Amazon S3 儲存貯體。以儲存貯體名稱 aws-groundstation-demo 表示。
- 將解調和解碼資料同步下行至您管理的 Amazon EC2 執行個體。以名稱 demodDecodeDownlink 表示。
- 資料從您管理的 Amazon EC2 執行個體同步上行至 AWS Ground Station 受管天線。以 digIfUplink 名稱表示。



聯絡排程

使用有效的任務設定檔，您可以請求與加入衛星的聯絡。聯絡人保留請求是非同步的，可讓全域天線服務有時間在所有涉及的 AWS 區域中達成一致的排程。在此過程中，會評估所請求地面站位置上的各種天線，以判斷它們是否可用且能夠處理聯絡。在此過程中，也會評估您設定的資料流程端點，以判斷其可用性。進行此評估時，聯絡狀態將處於 SCHEDULING。

此非同步排程程序將在請求的五分鐘內完成，但通常會在一分鐘內完成。請檢閱排程時間的事件 [AWS Ground Station 使用事件自動化型監控](#)。



可以執行且具有可用性的聯絡人會導致排程聯絡人。使用排程聯絡人時，執行聯絡人所需的資源已預留給任務設定檔所定義的所需 AWS 區域。無法執行或沒有可用部分的聯絡人將導致 FAILED_TO_SCHEDULE 聯絡人。如需偵錯詳細資訊[故障診斷 FAILED_TO_SCHEDULE 聯絡人](#)，請參閱。

聯絡執行

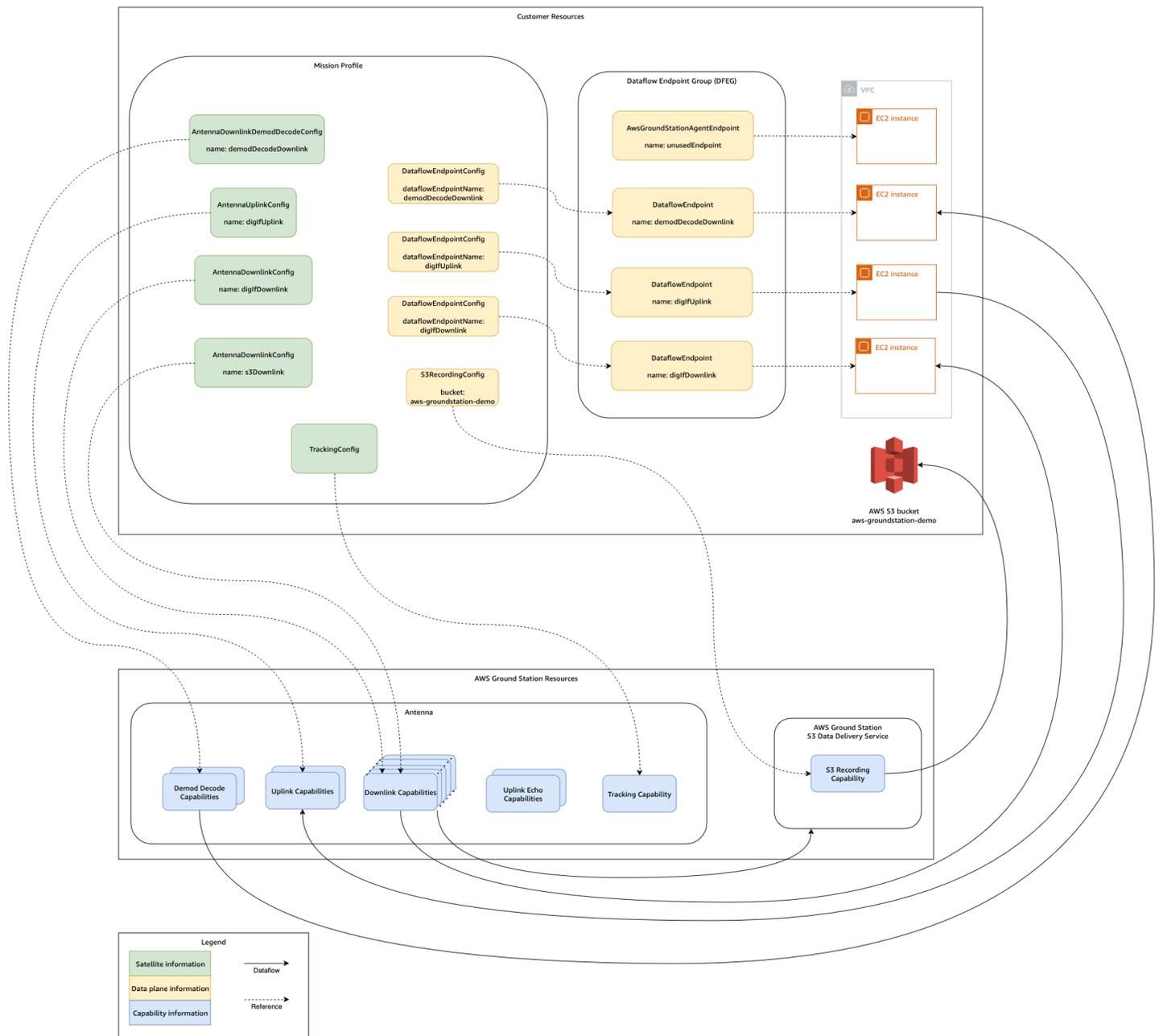
AWS Ground Station 會在您的聯絡保留期間自動協調您的 AWS 受管資源。如果適用，您需負責協調任務描述檔定義為資料流程端點的 EC2 資源。AWS Ground Station 提供 [AWS EventBridge Events](#) 以自動化資源的協調，以降低成本。如需詳細資訊，請參閱[AWS Ground Station 使用 事件自動化](#)。

在聯絡期間，有關聯絡效能的遙測會傳送到 AWS CloudWatch。如需有關如何在執行期間監控聯絡人的資訊，請參閱 [了解使用 監控 AWS Ground Station](#)。

下圖透過顯示在聯絡期間協調的相同資源，繼續先前的範例。

Note

此範例中並未使用所有天線功能。例如，每個支援多個頻率和極化的天線都有十幾種天線下行功能。如需 AWS Ground Station 天線提供的每個功能類型數量及其支援的頻率和極化的詳細資訊，請參閱 [AWS Ground Station 站點功能](#)。



在聯絡結束時，AWS Ground Station 將評估您的聯絡績效，並確定最終聯絡狀態。未偵測到錯誤的聯絡將導致完成聯絡狀態。服務錯誤在聯絡期間造成資料交付問題的聯絡將導致 AWS_FAILED 狀態。用戶端或使用者錯誤在聯絡期間造成資料交付問題的聯絡將導致失敗狀態。超過聯絡時間的錯誤，在傳遞前或傳遞後期間，在判定期間不會納入考量。

如需更多資訊，請參閱[了解聯絡生命週期](#)。

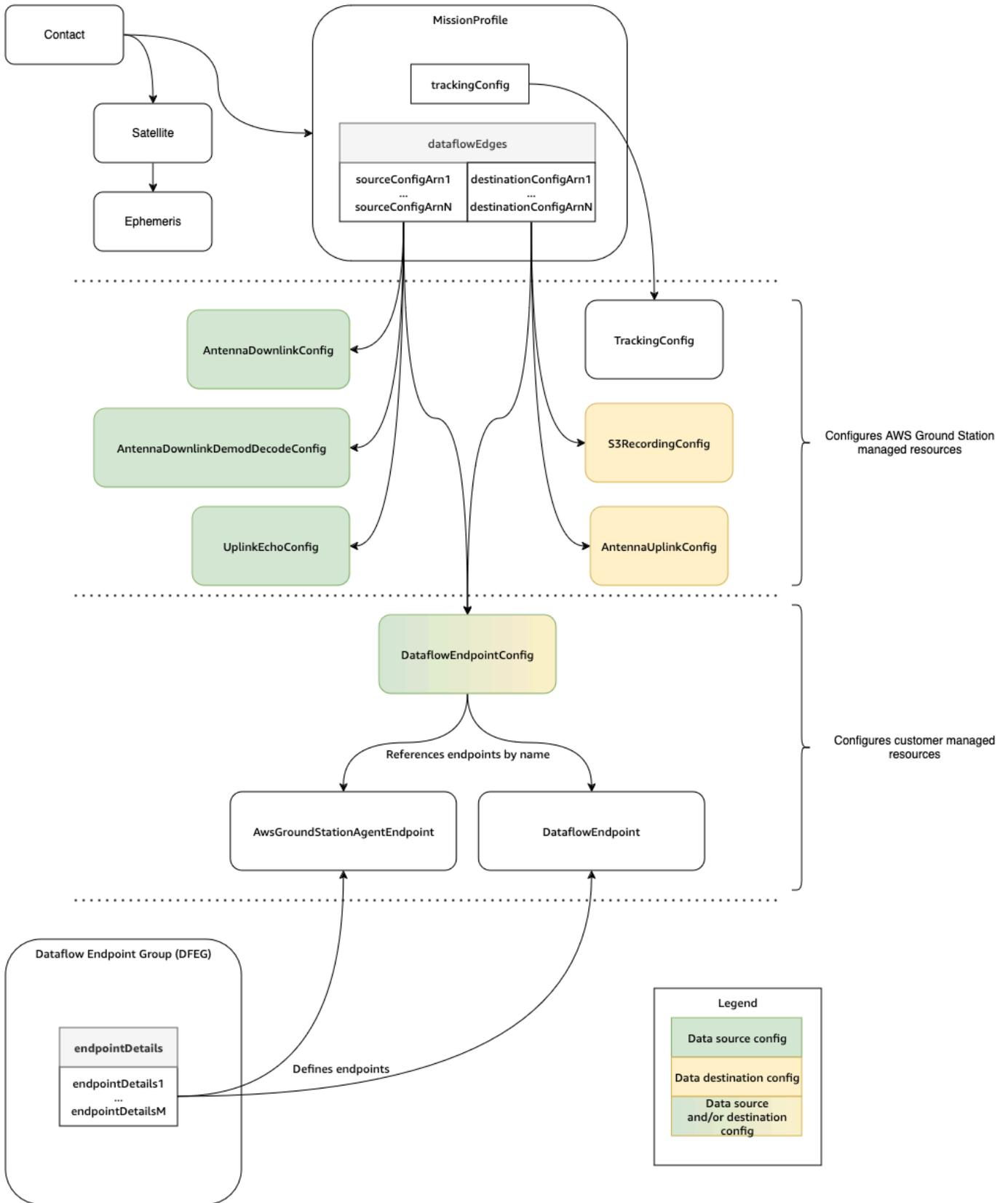
數位分身

的數位分身功能 AWS Ground Station 可讓您針對虛擬地面站位置排程聯絡人。這些虛擬地面站是生產地面站的確切複本，包括天線功能、站點遮罩和實際 GPS 座標。相較於生產地面站點，數位分身功能可讓您測試聯絡協調工作流程的成本一小部分。如需詳細資訊，請參閱「[使用 AWS Ground Station 數位分身功能](#)」。

了解 AWS Ground Station 核心元件

本節提供 AWS Ground Station 核心元件的詳細定義。

下圖顯示的核心元件 AWS Ground Station，以及它們彼此之間的關係。箭頭指出元件之間的相依性方向，其中每個元件指向其相依性。



下列主題詳細說明 AWS Ground Station 核心元件。

主題

- [使用 AWS Ground Station 任務設定檔](#)
- [使用 AWS Ground Station 組態](#)
- [使用 AWS Ground Station Dataflow 端點群組](#)
- [使用 AWS Ground Station 代理程式](#)

使用 AWS Ground Station 任務設定檔

任務設定檔包含如何執行接收的組態和參數。當您預留接收或搜尋可用的接收時，您提供打算使用的任務設定檔。任務設定檔會將所有組態集合在一起，並定義天線的設定方式，以及聯絡期間資料將前往何處。

任務設定檔可以跨共用相同無線電特性的衛星共用。您可以建立其他資料流程端點群組，以限制您要為星座執行的同時聯絡案例上限。

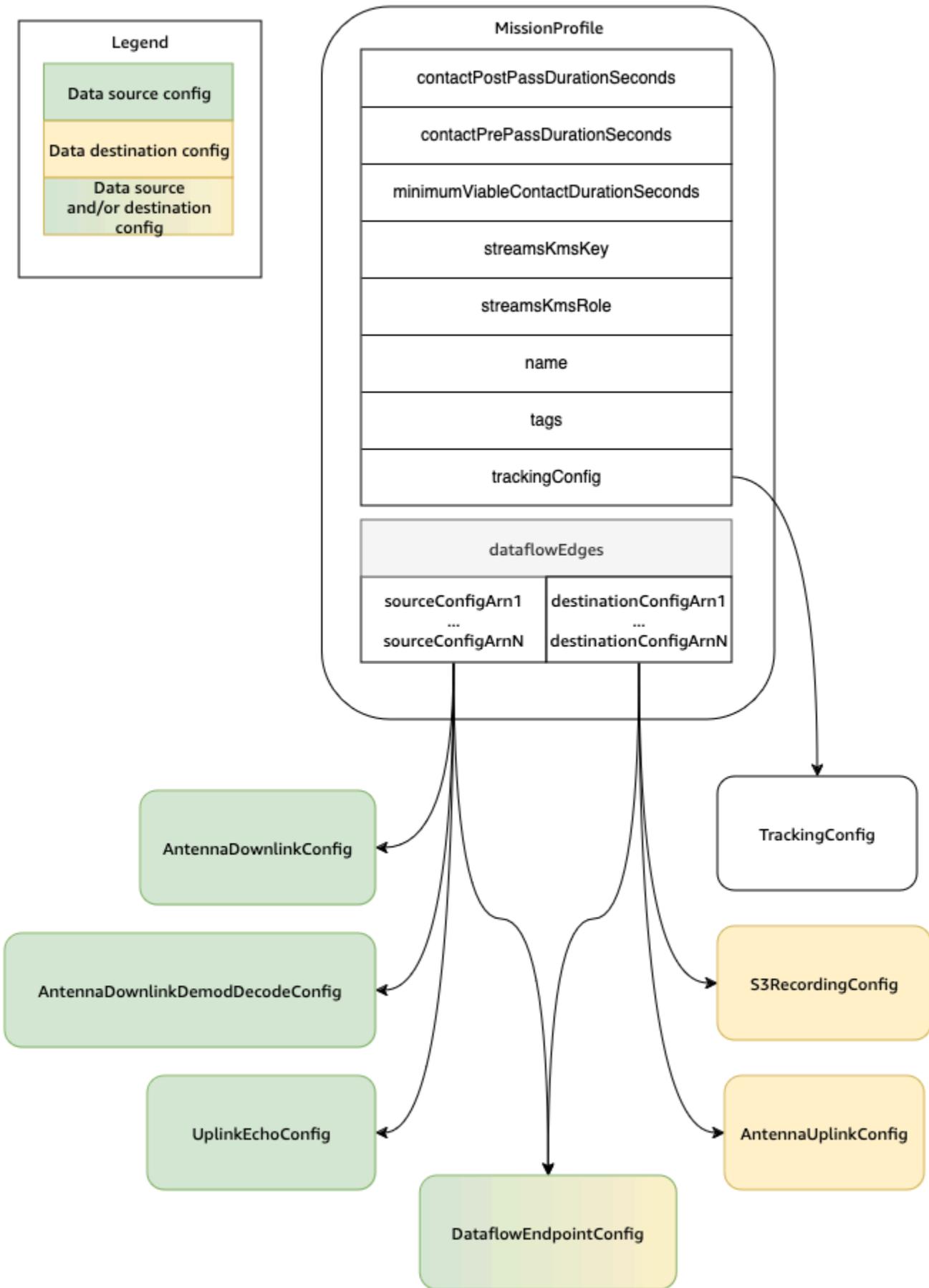
追蹤組態在任務設定檔中指定為唯一欄位。追蹤組態用於指定您在聯絡期間使用程式追蹤和自動追蹤的偏好。如需詳細資訊，請參閱[追蹤組態](#)。

所有其他組態都包含在任務描述檔的 `dataflowEdges` 欄位中。這些組態可視為資料流程節點，每個節點代表可傳送或接收資料的 AWS Ground Station 受管資源及其相關聯的組態。`dataflowEdges` 欄位定義需要哪些來源和目的地資料流程節點（組態）。單一資料流程邊緣是兩個組態 [Amazon Resource Name \(ARNs\)](#) 的清單，第一個是來源組態，第二個是目的地組態。透過在兩個組態之間指定資料流程邊緣，您可以告知在聯絡期間，資料應 AWS Ground Station 從何處和流向何處。如需詳細資訊，請參閱[使用 AWS Ground Station 組態](#)。

`contactPrePassDurationSeconds` 和 `contactPostPassDurationSeconds` 可讓您指定與聯絡人相關的時間，您將會在此接收 CloudWatch Event 通知。如需與您的聯絡相關的事件時間表，請閱讀[了解聯絡生命週期](#)。

任務設定檔的 `name` 欄位有助於區別您建立的任務設定檔。

`streamsKmsRole` 和 `streamsKmsKey` 用於定義用於透過 AWS Ground Station 代理程式交付資料 AWS Ground Station 所用的加密。請參閱[傳輸期間的資料加密 AWS Ground Station](#)。



下列文件包含參數和範例的完整清單。

- [AWS::GroundStation::MissionProfile CloudFormation 資源類型](#)

使用 AWS Ground Station 組態

組態是資源，AWS Ground Station 用來定義聯絡人每個層面的參數。將您想要的組態新增至任務設定檔，然後執行接收時，即會使用該任務設定檔。您可以定義多種不同類型的組態。組態可分為兩個類別：

- 追蹤組態
- 資料流程組態

TrackingConfig 是唯一的追蹤組態類型。它用於在聯絡期間設定天線的自動追蹤設定，在任務設定檔中是必要的。

可在任務設定檔資料流程中使用的組態可視為資料流程節點，每個節點代表可傳送或接收資料的 AWS Ground Station 受管資源。任務描述檔需要至少一對這些組態，一個代表資料來源，另一個代表目的地。這些組態摘要如下表所示。

組態名稱	資料流程來源/目的地
AntennaDownlinkConfig	來源
AntennaDownlinkDemodDecodeConfig	來源
UplinkEchoConfig	來源
S3RecordingConfig	目的地
AntennaUplinkConfig	目的地
DataflowEndpointConfig	來源和/或目的地

如需如何使用 AWS CloudFormation、或 AWS Ground Station API 在組態上執行操作的詳細資訊 AWS Command Line Interface，請參閱下列文件。特定組態類型的文件連結也提供如下。

- [AWS::GroundStation::Config CloudFormation 資源類型](#)

- [Config AWS CLI 參考](#)
- [Config API 參考](#)

追蹤組態

您可以在任務設定檔中使用追蹤組態，以判斷應否在接收期間啟用自動追蹤。此組態有單一參數：`autotrack`。`autotrack` 參數可有下列值：

- `REQUIRED` - 接收需要自動追蹤。
- `PREFERRED` - 接收偏好自動追蹤，但沒有自動追蹤仍可執行接收。
- `REMOVED` - 無任何自動追蹤應用於接收。

AWS Ground Station 將利用程式設計追蹤，當未使用自動追蹤時，該追蹤會根據您的暫時性變化來指向。如需 `ephemeris` 建構方式的詳細資訊，[了解 AWS Ground Station 如何使用衛星暫時性資料](#)，請參閱。

`Autotrack` 將使用程式追蹤，直到找到預期的訊號為止。一旦發生這種情況，它將繼續根據訊號的強度進行追蹤。

如需如何使用 AWS CloudFormation、或 AWS Ground Station API 追蹤組態執行操作的詳細資訊 AWS Command Line Interface，請參閱下列文件。

- [AWS::GroundStation::Config TrackingConfig CloudFormation 屬性](#)
- [組態 AWS CLI 參考](#) (請參閱 `trackingConfig -> (structure)` 一節)
- [TrackingConfig API 參考](#)

天線下行組態

您可以使用天線下行組態，在聯絡期間設定下行的天線。它們由頻譜組態組成，指定下行聯絡期間應使用的頻率、頻寬和極化。

此組態代表資料流程中的來源節點。它負責將無線電頻率資料數位化。從此節點串流的資料將遵循訊號資料/IP 格式。如需如何使用此組態建構資料流程的詳細資訊，請參閱 [使用資料流程](#)

如果您的下行使用案例需要解調或解碼，請參閱 [天線下行解調解碼組態](#)。

如需如何使用 AWS CloudFormation AWS Command Line Interface、或 AWS Ground Station API 在天線下行組態上執行操作的詳細資訊，請參閱下列文件。

- [AWS::GroundStation::Config AntennaDownlinkConfig CloudFormation 屬性](#)
- [組態 AWS CLI 參考](#) (請參閱antennaDownlinkConfig -> (structure)一節)
- [AntennaDownlinkConfig API 參考](#)

天線下行解調解碼組態

天線下行解調解碼組態是一種更複雜且可自訂的組態類型，可用來執行下行聯絡人與解調和/或解碼。如果您有興趣執行這些類型的聯絡，請傳送電子郵件至 < aws-groundstation@amazon.com > 聯絡 AWS Ground Station 團隊。我們會協助您為使用案例定義正確的組態和任務設定檔。

此組態代表資料流程中的來源節點。它負責將無線電頻率資料數位化，並依照指定執行解調和解碼。從此節點串流的資料將遵循解調/解碼的資料/IP 格式。如需如何使用此組態建構資料流程的詳細資訊，請參閱 [使用資料流程](#)

如需如何使用 AWS Command Line Interface、或 AWS Ground Station API 在天線下行解調解碼組態上執行操作的詳細資訊 AWS CloudFormation，請參閱下列文件。

- [AWS::GroundStation::Config AntennaDownlinkDemodDecodeConfig CloudFormation 屬性](#)
- [組態 AWS CLI 參考](#) (請參閱antennaDownlinkDemodDecodeConfig -> (structure)一節)
- [AntennaDownlinkDemodDecodeConfig API 參考](#)

天線上行組態

您可以使用天線上行組態，在聯絡期間設定上行的天線。它們由具有頻率、極化和目標有效等向輻射功率 (EIRP) 的頻譜組態組成。如需如何設定上行回傳聯絡人的詳細資訊，請參閱 [天線上行回應組態](#)。

此組態代表資料流程中的目的地節點。它會將提供的數位無線電頻率資料訊號轉換為類比訊號，並發出它以供衛星接收。串流到此節點的資料預期符合訊號資料/IP 格式。如需如何使用此組態建構資料流程的詳細資訊，請參閱 [使用資料流程](#)

如需如何使用 AWS Command Line Interface、或 AWS Ground Station API 在天線上行組態上執行操作的詳細資訊 AWS CloudFormation，請參閱下列文件。

- [AWS::GroundStation::Config AntennaUplinkConfig CloudFormation 屬性](#)
- [組態 AWS CLI 參考](#) (請參閱antennaUplinkConfig -> (structure)一節)
- [AntennaUplinkConfig API 參考](#)

天線上行回應組態

上行回應組態會通知天線如何執行上行回應。上行回應可用來驗證傳送到您太空船的命令，並執行其他進階任務。這是透過記錄由 AWS Ground Station 天線傳輸的實際訊號（即上行連結）來實現的。這會回應天線傳送回資料流程端點的訊號，且應符合傳輸的訊號。上行回應組態包含上行組態的 ARN。天線在執行上行回應時，使用來自 ARN 指向之上行組態的參數。

此組態代表資料流程中的來源節點。從此節點串流的資料將符合訊號資料/IP 格式。如需如何使用此組態建構資料流程的詳細資訊，請參閱 [使用資料流程](#)

如需如何使用 AWS Command Line Interface、或 AWS Ground Station API 在上行回應組態上執行操作的詳細資訊 AWS CloudFormation，請參閱下列文件。

- [AWS::GroundStation::Config UplinkEchoConfig CloudFormation 屬性](#)
- [Config AWS CLI 參考](#)（請參閱uplinkEchoConfig -> (structure)一節）
- [UplinkEchoConfig API 參考](#)

資料流程端點組態

Note

Dataflow 端點組態僅用於將資料交付至 Amazon EC2，而不會用於將資料交付至 Amazon S3。

您可以使用資料流程端點組態，指定要在聯絡期間從中傳輸資料或資料流端點群組中的[哪些資料流程端點](#)。資料流程端點組態的兩個參數會指定資料流程端點的名稱和區域。保留聯絡人時，AWS Ground Station 會分析您指定的[任務設定檔](#)，並嘗試在 AWS 區域內尋找資料流程端點群組，其中包含任務設定檔中包含的資料流程端點組態所指定的所有資料流程端點。如果找到合適的資料流程端點群組，聯絡狀態將變為 SCHEDULED，否則將變為 FAILED_TO_SCHEDULE。如需聯絡可能狀態的詳細資訊，請參閱 [AWS Ground Station 聯絡狀態](#)。

資料流程端點組態的 dataflowEndpointName 屬性會指定資料流程端點群組中的哪些資料流程端點，在聯絡期間要從中傳輸資料。

dataflowEndpointRegion 屬性指定資料流程端點所在的區域。如果您的資料流程端點組態中指定了區域，會 AWS Ground Station 尋找指定區域中的資料流程端點。如果未指定區域，AWS Ground Station 將預設為聯絡人的地面工作站區域。如果您的資料流程端點的區域與聯絡人的地面工作站區域

不同，則聯絡人會被視為跨區域資料交付聯絡人。[使用資料流程](#) 如需跨區域資料流程的詳細資訊，請參閱。

如需資料流程不同命名方案如何讓您的使用案例受益的秘訣[使用 AWS Ground Station Dataflow 端點群組](#)，請參閱。

如需如何使用此組態建構資料流程的詳細資訊，請參閱 [使用資料流程](#)

如需如何使用 AWS Command Line Interface、或 AWS Ground Station API 在資料流程端點組態上執行操作的詳細資訊 AWS CloudFormation，請參閱下列文件。

- [AWS::GroundStation::Config DataflowEndpointConfig CloudFormation 屬性](#)
- [組態 AWS CLI 參考](#) (請參閱 `dataflowEndpointConfig -> (structure)` 一節)
- [DataflowEndpointConfig API 參考](#)

Amazon S3 錄製組態

Note

Amazon S3 記錄組態僅用於將資料交付至 Amazon S3，而不會用於將資料交付至 Amazon EC2。

此組態代表資料流程中的目的地節點。此節點會將來自資料流程來源節點的傳入資料封裝為 pcap 資料。如需如何使用此組態建構資料流程的詳細資訊，請參閱 [使用資料流程](#)

您可以使用 S3 錄製組態來指定要與使用的命名慣例一起交付下行資料的目標 Amazon S3 儲存貯體。以下指定這些參數的限制和詳細資訊：

- Amazon S3 儲存貯體的名稱必須以 `aws-groundstation` 開頭。
- IAM 角色必須具有信任政策，允許 `groundstation.amazonaws.com` 服務主體擔任該角色。如需範例，請參閱 [以下範例信任政策](#) 一節。在組態建立期間，組態資源 ID 不存在，信任政策必須使用星號 (*) 取代 `your-config-id`，並且可以在建立之後使用組態資源 ID 更新。

範例信任政策

如需如何更新角色信任政策的詳細資訊，請參閱 [《IAM 使用者指南》中的管理 IAM 角色](#)。

```

{
  "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"
        }
      }
    }
  ]
}

```

- IAM 角色必須具有 IAM 政策，允許角色對儲存貯體執行 s3:GetBucketLocation 動作，並對儲存貯體的物件執行 s3:PutObject 動作。如果 Amazon S3 儲存貯體具有儲存貯體政策，則儲存貯體政策也必須允許 IAM 角色執行這些動作。如需範例，[請參閱以下的範例角色政策](#)一節。

範例角色政策

如需如何更新或連接角色政策的詳細資訊，請參閱 [《IAM 使用者指南》中的管理 IAM 政策](#)。

```

{
  "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/*"
    ]
  }
]
}

```

- 命名 S3 資料物件時，將使用字首。您可以指定選用金鑰來取代，這些值將取代為來自您聯絡詳細資訊的對應資訊。例如，字首 {satellite_id}/{year}/{month}/{day} 將被取代，並使用類似的輸出 fake_satellite_id/2021/01/10

替代的選用索引鍵： {satellite_id} | {config-name} | {config-id} | {year} {month} | | {day} |

如需如何使用 AWS CloudFormation AWS Command Line Interface、或 AWS Ground Station API 在 S3 錄製組態上執行操作的詳細資訊，請參閱下列文件。

- [AWS::GroundStation::Config S3RecordingConfig CloudFormation 屬性](#)
- [組態 AWS CLI 參考](#) (請參閱 s3RecordingConfig -> (structure) 一節)
- [S3RecordingConfig API 參考](#)

使用 AWS Ground Station Dataflow 端點群組

Dataflow 端點定義您希望在聯絡期間同步串流資料的位置。資料流程端點一律建立為資料流程端點群組的一部分。透過將多個資料流程端點包含在一個群組中，您宣告可在單一接收中一起使用全部的指定端點。例如，如果接收需要將資料分別傳送到三個資料流程端點，您必須在符合任務設定檔資料流程端點組態的單一資料流程端點群組中有三個端點。

i Tip

執行聯絡人時，資料流程端點會由您選擇的名稱識別。這些名稱在帳戶中不需要是唯一的名稱。這允許使用相同的任務設定檔同時執行不同衛星和天線的多個聯絡人。如果您有具有相同操作特性的衛星星座，這很有用。您可以擴展資料流程端點群組的數量，以符合衛星星座所需的同時聯絡數目上限。

當資料流程端點群組中的一或多項資源正為某項接收使用時，整個群組在接收期間會為該接收保留。您可以同時執行多個聯絡人，但這些聯絡人必須在不同的資料流程端點群組上執行。

A Important

Dataflow 端點群組必須處於 HEALTHY 狀態，才能使用它們排程聯絡人。如需如何對未處於 HEALTHY 狀態的資料流程端點群組進行故障診斷的資訊，請參閱 [針對未處於 HEALTHY 狀態的 DataflowEndpointGroups 進行故障診斷](#)。

如需如何使用 AWS CloudFormation AWS Command Line Interface、或 AWS Ground Station API 在資料流程端點群組上執行操作的詳細資訊，請參閱下列文件。

- [AWS::GroundStation::DataflowEndpointGroup CloudFormation 資源類型](#)
- [Dataflow 端點群組 AWS CLI 參考](#)
- [Dataflow 端點群組 API 參考](#)

資料流程端點

資料流程端點群組的成員是資料流程端點。資料流程端點有兩種類型：[AWS Ground Station 客服人員端點](#)和[資料流程端點](#)。對於這兩種類型的端點，您將在建立資料流程端點群組之前建立支援的建構（例如 IP 地址）。請參閱 [使用資料流程](#) 以取得有關要使用的資料流程端點類型以及如何設定支援建構的建議。

下列各節說明兩種支援的端點類型。

⚠ Important

單一資料流程端點群組內的所有資料流程端點必須屬於相同類型。您無法將 [AWS Ground Station 客服人員端點](#) 與相同群組中的 [Dataflow 端點](#) 混合。如果您的使用案例需要這兩種類型的端點，您必須為每個類型建立單獨的資料流程端點群組。

AWS Ground Station 代理程式端點

Agent AWS Ground Station Endpoint 利用 AWS Ground Station Agent 做為軟體元件來終止連線。當您想要將大於 50MHz 的數位訊號資料下行時，請使用 AWS Ground Station 代理程式資料流程端點。若要建構 AWS Ground Station 代理程式端點，您只會填入 EndpointDetails AwsGroundStationAgentEndpoint 的欄位。如需 AWS Ground Station 代理程式的詳細資訊，請參閱完整的 [AWS Ground Station 代理程式使用者指南](#)。

AwsGroundStationAgentEndpoint 包含下列項目：

- Name - 資料流程端點名稱。若要讓聯絡人使用此資料流程端點，此名稱必須符合資料流程端點組態中使用的名稱。
- EgressAddress - 用於從代理程式輸出資料的 IP 和連接埠地址。
- IngressAddress - 用來將資料輸入至代理程式的 IP 和連接埠地址。

Dataflow 端點

Dataflow 端點利用聯網應用程式做為軟體元件來終止連線。當您想要上行數位訊號資料、下行小於 50MHz 的數位訊號資料，或下行已解調/解碼的訊號資料時，請使用 Dataflow 端點。若要建構 Dataflow 端點，您將填入 EndpointDetails 的 Endpoint 和 Security Details 欄位。

Endpoint 包含下列項目：

- Name - 資料流程端點名稱。若要讓聯絡人使用此資料流程端點，此名稱必須符合資料流程端點組態中使用的名稱。
- Address - 使用的 IP 和連接埠地址。

SecurityDetails 包含下列項目：

- roleArn - 角色的 Amazon Resource Name (ARN)，該角色 AWS Ground Station 將擔任在您的 VPC 中建立彈性網路界面 (ENIs)。這些 ENI 可做為聯絡期間串流之資料的傳入和傳出點。

- `securityGroupIds` - 要連接到彈性網路界面的安全群組。
- `subnetIds` - 子網路清單，其中 AWS Ground Station 可能會放置彈性網路介面，以將串流傳送至您的執行個體。如果指定多個子網路，它們必須可以彼此路由。如果子網路位於不同的可用區域 (AZs)，您可能會產生跨可用區域資料傳輸費用。

傳遞至的 IAM 角色 `roleArn` 必須具有信任政策，允許 `groundstation.amazonaws.com` 服務主體擔任該角色。如需範例，[請參閱以下範例信任政策](#) 一節。在端點建立期間，端點資源 ID 不存在，因此信任政策必須使用星號 (*) 取代 `your-endpoint-id`。這可以在建立後更新為使用端點資源 ID，以便將信任政策範圍限定於該特定資料流程端點群組。

IAM 角色必須具有允許 AWS Ground Station 設定 ENIs 的 IAM 政策。如需範例，[請參閱以下角色政策範例](#) 一節。

範例信任政策

如需如何更新角色信任政策的詳細資訊，請參閱 [《IAM 使用者指南》中的管理 IAM 角色](#)。

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

範例角色政策

如需如何更新或連接角色政策的詳細資訊，請參閱 [《IAM 使用者指南》中的管理 IAM 政策](#)。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2>DeleteNetworkInterfacePermission",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups"
      ]
    }
  ]
}
```

使用 AWS Ground Station 代理程式

AWS Ground Station 客服人員可讓您在 AWS Ground Station 聯絡期間接收（下行）同步寬頻數位中繼頻率 (DigIF) 資料流程。

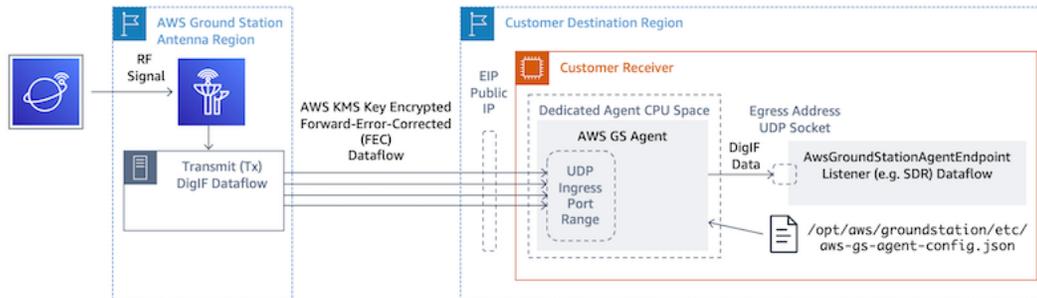
運作方式

您可以選擇兩個資料交付選項：

1. 資料交付至 EC2 執行個體 - 資料交付至您擁有的 EC2 執行個體。您可以管理 AWS Ground Station 代理程式。如果您需要近乎即時的資料處理，此選項可能最適合您。如需 EC2 資料交付的相關資訊，請參閱[使用資料流程](#)一節。
2. 資料交付至 S3 儲存貯體 - 資料交付至您的 AWS S3 儲存貯體完全由管理 AWS Ground Station。如需 S3 資料交付的相關資訊，請參閱[開始使用指南](#)。

這兩種資料交付模式都需要您建立一組 AWS 資源。強烈建議您使用 CloudFormation 來建立 AWS 資源，以確保可靠性、準確性和支援能力。每個聯絡人只能將資料交付至 EC2 或 S3，但不能同時交付至兩者。

下圖顯示使用軟體定義的無線電 (SDR) 或類似接聽程式，從 AWS Ground Station 天線區域到 EC2 執行個體的 DigIF 資料流程。



其他資訊

如需詳細資訊，請參閱完整的[AWS Ground Station 客服人員使用者指南](#)。

開始使用

開始之前，您應該先熟悉其中的基本概念 AWS Ground Station。如需詳細資訊，請參閱[AWS Ground Station 運作方式](#)。

以下是 AWS Identity and Access Management (IAM) 的最佳實務以及您需要的許可。設定適當的角色之後，您可以開始遵循其餘的步驟。

註冊 AWS 帳戶

如果您沒有 AWS 帳戶，請完成下列步驟來建立一個。

註冊 AWS 帳戶

1. 開啟 <https://portal.aws.amazon.com/billing/signup>。
2. 請遵循線上指示進行。

註冊程序的一部分包括接聽電話或文字訊息，並在電話鍵盤上輸入驗證碼。

當您註冊時 AWS 帳戶，AWS 帳戶根使用者會建立。根使用者有權存取該帳戶中的所有 AWS 服務和資源。作為安全最佳實務，請將管理存取權指派給使用者，並且僅使用根使用者來執行[需要根使用者存取權的任務](#)。

AWS 會在註冊程序完成後傳送確認電子郵件給您。您可以隨時登錄 <https://aws.amazon.com/> 並選擇我的帳戶，以檢視您目前的帳戶活動並管理帳戶。

建立具有管理存取權的使用者

註冊之後 AWS 帳戶，請保護 AWS 帳戶根使用者、啟用 AWS IAM Identity Center 和建立管理使用者，以免將根使用者用於日常任務。

保護您的 AWS 帳戶根使用者

1. 選擇根使用者並輸入 AWS 帳戶您的電子郵件地址，以帳戶擁有者[AWS Management Console](#)身分登入。在下一頁中，輸入您的密碼。

如需使用根使用者登入的說明，請參閱 AWS 登入 使用者指南中的[以根使用者身分登入](#)。

2. 若要在您的根使用者帳戶上啟用多重要素驗證 (MFA)。

如需說明，請參閱《IAM 使用者指南》中的[為您的 AWS 帳戶 根使用者（主控台）啟用虛擬 MFA 裝置](#)。

建立具有管理存取權的使用者

1. 啟用 IAM Identity Center。

如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的[啟用 AWS IAM Identity Center](#)。

2. 在 IAM Identity Center 中，將管理存取權授予使用者。

如需使用 IAM Identity Center 目錄 做為身分來源的教學課程，請參閱AWS IAM Identity Center 《使用者指南》中的[使用預設值設定使用者存取 IAM Identity Center 目錄](#)。

以具有管理存取權的使用者身分登入

- 若要使用您的 IAM Identity Center 使用者簽署，請使用建立 IAM Identity Center 使用者時傳送至您電子郵件地址的簽署 URL。

如需使用 IAM Identity Center 使用者登入的說明，請參閱AWS 登入 《使用者指南》中的[登入 AWS 存取入口網站](#)。

指派存取權給其他使用者

1. 在 IAM Identity Center 中，建立一個許可集來遵循套用最低權限的最佳實務。

如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的[建立許可集](#)。

2. 將使用者指派至群組，然後對該群組指派單一登入存取權。

如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的[新增群組](#)。

將 AWS Ground Station 許可新增至 AWS 您的帳戶

若要在不要求管理使用者 AWS Ground Station 的情況下使用，您需要建立新的政策並將其連接到 AWS 您的帳戶。

1. 登入 AWS Management Console 並開啟 [IAM 主控台](#)。
2. 建立新政策。使用下列步驟：

- a. 在導覽窗格中，選擇 Policies (政策)，然後選擇 Create Policy (建立政策)。
- b. 在 JSON 標籤中，使用下列值之一編輯 JSON。使用最適合您的應用程式的 JSON。
 - 對於 Ground Station 管理權限，將動作設定為 `Groundstation : *`，如下所示：

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

- 對於唯讀權限，請將 Action (動作) 設定為 `groundstation:get*`、`groundstation:list*` 和 `groundstation:describe*`，如下所示：

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

- 如需透過多重驗證來增加安全性，將 Action (動作) 設定為 `groundstation:*` 和將 Condition/Bool (條件/布林) 設定為 `aws:MultiFactorAuthPresent:true`，如下所示：

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

3. 在 IAM 主控台中，將您建立的政策連接到所需的使用者。

如需 IAM 使用者和連接政策的詳細資訊，請參閱 [IAM 使用者指南](#)。

加入衛星

將衛星加入 AWS Ground Station 是一個多步驟程序，涉及資料收集、技術驗證、頻譜授權，以及整合和測試。也需要保密協議 (NDAs)。

客戶加入程序概觀

衛星加入是手動程序，可在 AWS Ground Station 主控台頁面的 [衛星和資源](#) 區段中找到。以下說明整體程序。

1. 檢閱 [AWS Ground Station 位置](#) 區段，判斷您的衛星是否符合地理和無線電頻率特性。
2. 若要開始將您的衛星加入 AWS Ground Station，請傳送電子郵件至 `<aws-groundstation@amazon.com>`，其中包含您任務和衛星需求的簡短摘要，包括您的組織名稱、所需的頻率、衛星的啟動時間、衛星的軌道類型，以及您是否計劃使用 [使用 AWS Ground Station 數位分身功能](#)。
3. 審核並核准您的請求後，AWS Ground Station 將在您計劃使用的特定位置申請法規授權。此步驟的持續時間會根據位置和任何現有法規而有所不同。
4. 取得此核准後，您的衛星就會顯示供您使用。AWS Ground Station 會傳送成功更新的通知給您。

(選用) 命名衛星

加入後，您可能想要將名稱新增至衛星記錄，以便更輕鬆地辨識它。AWS Ground Station 使用聯絡人頁面時，主控台能夠顯示使用者定義的衛星名稱以及 Norad ID。顯示衛星名稱可讓您在排程時更輕鬆地選取正確的衛星。若要這樣做，可以使用[標籤](#)。

您可以使用 AWS CLI 或其中一個 AWS 開發套件，透過 tag-resource API 來標記 AWS Ground Station SDKs。 <https://docs.aws.amazon.com/cli/latest/reference/groundstation/tag-resource.html> 本指南將介紹如何使用 AWS Ground Station CLI 在中標記公有廣播衛星 Aqua (Norad ID 27424)us-west-2。

AWS Ground Station CLI

AWS CLI 可用來與 互動 AWS Ground Station。使用 AWS CLI 標記您的衛星之前，必須滿足下列 AWS CLI 先決條件：

- 確定 AWS CLI 已安裝。如需安裝的資訊 AWS CLI，請參閱[安裝 AWS CLI 第 2 版](#)。
- 確定 AWS CLI 已設定。如需設定的相關資訊 AWS CLI，請參閱[設定 AWS CLI 第 2 版](#)。
- 將常用的組態設定和登入資料儲存在 AWS CLI 維護的檔案中。您需要這些設定和登入資料來預留和管理 AWS Ground Station 聯絡人 AWS CLI。如需儲存組態和登入資料設定的詳細資訊，請參閱[組態和登入資料檔案設定](#)。

AWS CLI 設定好並準備好使用後，請檢閱 [AWS Ground Station CLI 命令參考](#) 頁面，以熟悉可用的命令。使用此服務時，請遵循 AWS CLI 命令結構，並使用 為命令加上字首 groundstation，以指定 AWS Ground Station 做為您要使用的服務。如需 AWS CLI 命令結構的詳細資訊，請參閱 [AWS CLI 頁面中的命令結構](#)。以下提供命令結構範例。

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

命名衛星

首先，您需要取得要標記之衛星的 ARN (ASN)。這可以透過 AWS CLI 中的 [list-satellites](#) API 完成：

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

執行上述 CLI 命令將傳回類似以下的輸出：

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

尋找您要標記的衛星，並記下 `satelliteArn`。標記的一個重要注意事項是，[Tag-resource](#) API 需要區域 ARN，而 [list-satellites](#) 傳回的 ARN 是全域的。對於下一個步驟，您應該將 ARN 擴大為您想要查看標籤的區域（可能是您排程的區域）。在此範例中，我們使用 `us-west-2`。透過此變更，ARN 將來自：

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

至：

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

若要在主控台中顯示衛星名稱，衛星必須具有 “Name” 標籤做為金鑰。此外，因為我們使用的是 AWS CLI，引號必須以反斜線逸出。標籤看起來會類似：

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

接著，您將呼叫 [tag-resource](#) API 來標記衛星。這可以使用 AWS CLI 類似 來完成：

```
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"}'
```

執行此操作後，您將能夠在 主控台中 AWS Ground Station 看到您為衛星設定的名稱。

變更衛星的名稱

如果您想要變更衛星的名稱，您可以使用相同的“Name”索引鍵再次使用衛星 ARN 呼叫 [tag-resource](#)，但在標籤中具有不同的值。這將更新現有的標籤，並在主控台中顯示新名稱。對此的範例呼叫如下所示：

```
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"}
```

移除衛星的名稱

可以使用 [untag-resource](#) API 移除衛星的名稱集。此 API 需要具有標籤所在區域的衛星 ARN，以及標籤索引鍵清單。對於名稱，標籤索引鍵為“Name”。使用 AWS CLI 呼叫此 API 的範例如下所示：

```
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
```

公有廣播衛星

除了加入您自己的衛星之外，您還可以請求加入支援公開廣播衛星，以提供可公開存取的下行通訊路徑。這可讓您使用 從這些衛星 AWS Ground Station 下行資料。

Note

您將無法向上連結至這些衛星。您只能使用可公開存取的下行通訊路徑。

AWS Ground Station 支援加入下列衛星，以下行直接廣播資料：

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

加入後，即可存取這些衛星以供立即使用。AWS Ground Station 會維護許多預先設定的 AWS CloudFormation 範本，讓您更輕鬆地開始使用服務。如需 AWS Ground Station 如何使用的範例 [範例任務設定檔組態](#)，請參閱。

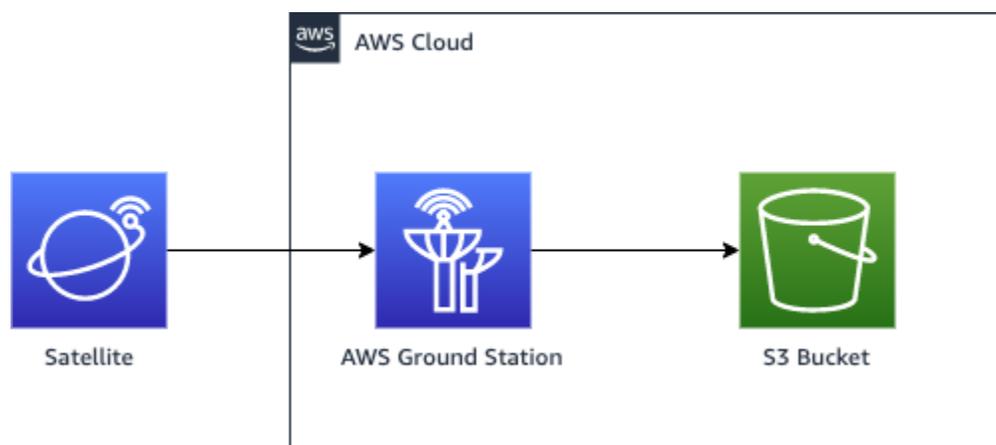
如需有關這些衛星，以及這些衛星傳輸的資料種類詳細資訊，請參閱 [Aqua](#)、[JPSS-1/NOAA-20 and SNPP](#) 和 [Terra](#)。

規劃您的資料流程通訊路徑

您可以選擇衛星上每個通訊路徑的同步和非同步通訊。根據您的衛星和使用案例，您可能需要一種或兩種類型。同步通訊路徑允許近乎即時的上行鏈路，以及窄頻和寬頻下行操作。非同步通訊路徑僅支援窄頻和寬頻下行操作。

非同步資料交付

透過資料交付至 Amazon S3，您的聯絡資料會以非同步方式交付至您帳戶中的 Amazon S3 儲存貯體。您的聯絡人資料會以封包擷取 (pcap) 檔案的形式交付，以允許將聯絡人資料重播至軟體定義的無線電 (SDR)，或從 pcap 檔案擷取承載資料以進行處理。當天線硬體收到聯絡資料時，pcap 檔案每 30 秒會交付到您的 Amazon S3 儲存貯體，以便在需要時在聯絡期間處理聯絡資料。收到後，您可以使用自己的後製處理軟體或使用 Amazon SageMaker AI 或 Amazon Rekognition 等其他 AWS 服務來處理資料。資料交付至 Amazon S3 僅適用於從您的衛星下行資料；無法從 Amazon S3 將資料上行至您的衛星。



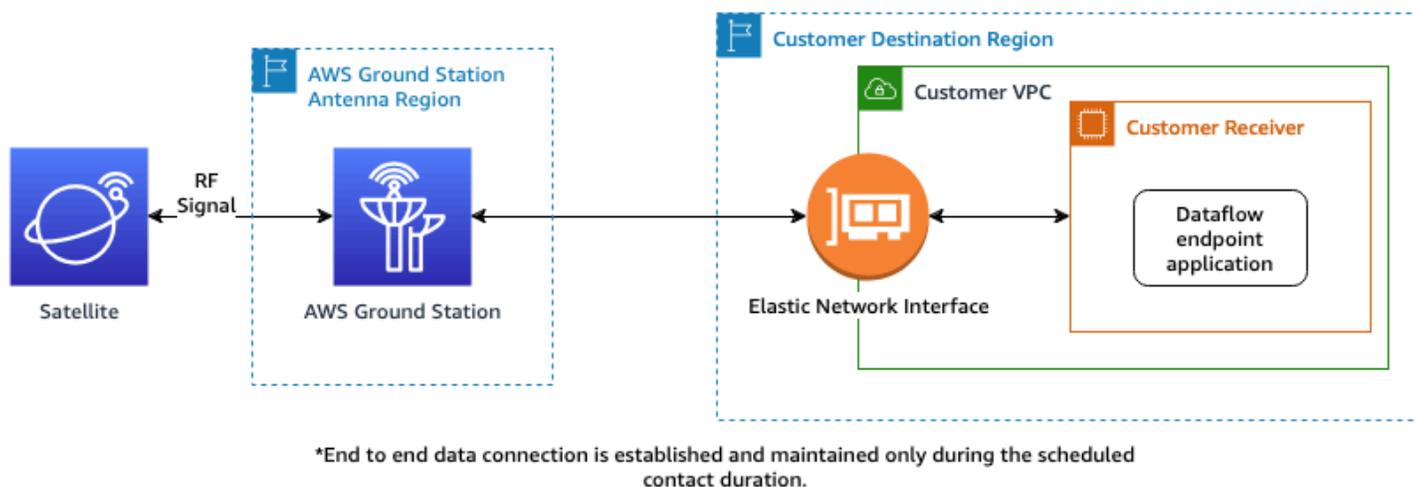
若要使用此路徑，您需要為 建立 Amazon S3 儲存貯體 AWS Ground Station，以將資料交付至其中。在下一個步驟中，您也需要在下一個步驟中建立 S3 錄製組態。如需儲存貯 [Amazon S3 錄製組態](#) 體命名的限制，以及如何指定檔案所使用的命名慣例，請參閱。

同步資料交付

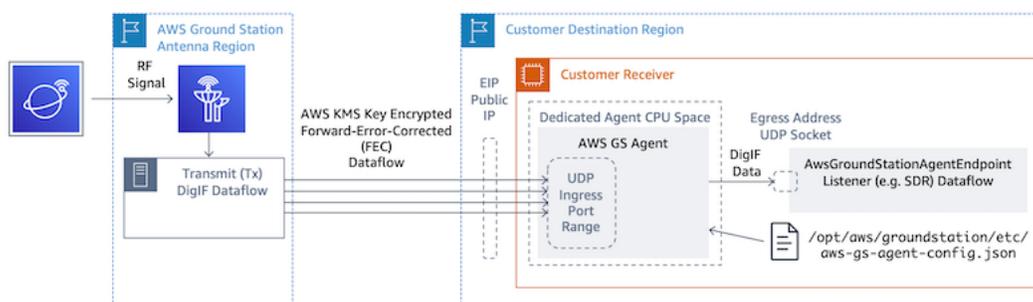
將資料交付至 Amazon EC2 時，您的聯絡資料會串流至 Amazon EC2 執行個體或從中串流。您可以在 Amazon EC2 執行個體上即時處理資料，或轉送資料以進行後續處理。

若要使用同步路徑，您需要使用 [來設定 Amazon EC2 執行個體](#)，並建立一或多個 Dataflow 端點群組。若要設定 Amazon EC2 執行個體，請參閱 [設定 Amazon EC2](#)。若要建立 Dataflow 端點群組，請參閱 [使用 AWS Ground Station Dataflow 端點群組](#)。

如果您使用的是資料流程端點組態，則會顯示通訊路徑。



如果您使用 AWS Ground Station 代理程式組態，則會顯示通訊路徑。



建立組態

在此步驟中，您已視需要識別衛星、通訊路徑和 IAM、Amazon EC2 和 Amazon S3 資源。在此步驟中，您將建立 AWS Ground Station 儲存其個別參數的組態。

資料交付組態

要建立的第一個組態與您希望資料交付的位置和方式相關。使用上一個步驟的資訊，您將建構下列許多組態類型。

- [Amazon S3 錄製組態](#) - 將資料交付至 Amazon S3 儲存貯體。
- [資料流程端點組態](#) - 將資料交付至 Amazon EC2 執行個體。

衛星組態

衛星組態會關聯 AWS Ground Station 如何與您的衛星通訊。您將參考在 [中](#) 收集的資訊 [加入衛星](#)。

- [追蹤組態](#) - 設定偏好在聯絡期間如何實際追蹤您的車輛。這是任務設定檔建構的必要項目。
- [天線下行組態](#) - 交付數位化的無線電頻率資料。
- [天線下行解調解碼組態](#) - 交付解調和解碼的無線電頻率資料。
- [天線上行組態](#) - 將資料上行到您的衛星。
- [天線上行回應組態](#) - 交付上行訊號資料的回應。

建立任務設定檔

使用上一個步驟中建構的組態，您已識別如何追蹤衛星以及與衛星通訊的可能方式。在此步驟中，您將建構一或多個任務設定檔。任務描述檔代表可能組態的彙總成可接著排程和操作的預期行為。

如需最新參數，請參閱 [AWS::GroundStation::MissionProfile CloudFormation 資源類型](#)

1. 為您的任務描述檔命名。這可讓您快速了解其在系統中的使用。例如，如果您有個別satellite-wideband-narrowband-nominal-operationsatellite-narrowband-emergency-operations操作。
2. 設定您的追蹤組態。
3. 設定您的最短可行聯絡持續時間。這可讓您篩選潛在的聯絡人，以符合您的任務需求。
4. 設定用於在傳輸期間加密資料的 streamsKmsKey 和 streamsKmsRole。這用於所有 AWS Ground Station 客服人員資料流程。
5. 設定您的資料流程。使用您在上一個步驟中建立的組態，建立您的資料流程以符合電信業者訊號。
6. **【選用】** 設定您的傳遞前和傳遞後聯絡持續時間秒數。這分別用於在聯絡前後發出每個聯絡事件。如需更多資訊，請參閱 [AWS Ground Station 使用 事件自動化](#)。

7. **【選用】** 您可以將標籤與任務設定檔建立關聯。這些可用於協助以程式設計方式區分您的任務描述檔。

您可以參考 [範例任務設定檔組態](#)，只查看一些潛在的組態。

了解後續步驟

現在您已有加入的衛星和有效的任務描述檔，您已準備好排定聯絡人並與衛星通訊 AWS Ground Station。

您可以透過下列其中一種方式排程聯絡人：

- [AWS Ground Station 主控台](#)。
- CLI [reserve-contact](#) AWS 命令。
- AWS 開發套件。 [ReserveContact](#) API。

如需有關 如何 AWS Ground Station 追蹤衛星軌跡以及如何使用該資訊的資訊，請參閱 [了解 AWS Ground Station 如何使用衛星暫時性資料](#)。

AWS Ground Station 會維護許多預先設定的 AWS CloudFormation 範本，讓您更輕鬆地開始使用服務。如需 AWS Ground Station 如何使用的範例 [範例任務設定檔組態](#)，請參閱。

處理數位中繼頻率資料，或從 提供給您的解調和解碼資料 AWS Ground Station，將取決於您的特定使用案例。下列部落格文章可協助您了解一些可用的選項：

- [使用 AWS Ground Station Amazon S3 資料交付的自動化地球觀察](#)（及其相關聯的 GitHub 儲存庫 [awslabs/aws-groundstation-eos-pipeline](#)）
- [使用 虛擬化衛星地面區段 AWS](#)
- [地球觀察使用 AWS Ground Station：如何引導](#)
- [使用 AWS Ground Station WideBand DigIF 和 Amphinicy Blink SDR](#)（及其相關聯的 GitHub 儲存庫 [aws-samples/aws-groundstation-wbdigif-snpp](#)） [建置高輸送量衛星資料下行架構](#) GitHub [aws-samples/aws-groundstation-wbdigif-snpp](#)

AWS Ground Station 位置

AWS Ground Station 提供與 AWS 基礎設施區域全球網路近在咫尺的全球地面站網路。您可以從任何支援的 AWS 區域設定使用這些位置。這包括交付資料的 AWS 區域。



尋找地面站點位置 AWS 的區域

AWS Ground Station 全球網路包含地面工作站位置，這些位置並非實際位於其連線的 [AWS 區域中](#)。您可以透過 AWS SDK [ListGroundStation](#) 回應擷取您有權存取的地面工作站清單。地面站點位置的完整清單如下所示，即將推出更多。請參閱入門指南，以新增或修改衛星的網站核准。

Ground Station 名稱	Ground Station 位置	AWS 區域名稱	AWS 區域代碼	備註
阿拉斯加 1	美國阿拉斯加	美國西部 (奧勒岡)	us-west-2	不實際位於 AWS 區域
巴林 1	巴林	中東 (巴林)	me-south-1	

Ground Station 名稱	Ground Station 位置	AWS 區域名稱	AWS 區域代碼	備註
開普敦 1	南非開普敦	非洲 (開普敦)	af-south-1	
Dubbo 1	達博, 澳洲	亞太區域 (悉尼)	ap-southeast-2	不實際位於 AWS 區域
夏威夷 1	美國, 夏威夷	美國西部 (奧勒岡)	us-west-2	不實際位於 AWS 區域
愛爾蘭 1	愛爾蘭	歐洲 (愛爾蘭)	eu-west-1	
俄亥俄州 1	美國俄亥俄州	美國東部 (俄亥俄)	us-east-2	
奧勒岡州 1	美國奧勒岡	美國西部 (奧勒岡)	us-west-2	
Punta Arenas 1	Punta Arenas, 智利	南美洲 (聖保羅)	sa-east-1	不實際位於 AWS 區域
首爾 1	首爾、南韓	亞太區域 (首爾)	ap-northeast-2	
新加坡 1	新加坡	亞太區域 (新加坡)	ap-southeast-1	
斯德哥爾摩 1	瑞典斯德哥爾摩	歐洲 (斯德哥爾摩)	eu-north-1	

AWS Ground Station 支援的 AWS 區域

您可以透過 AWS 開發套件或從支援的 AWS 區域 AWS Ground Station 提供資料和設定您的聯絡人。您可以在端點和 [AWS Ground Station 配額中檢視支援的區域及其相關聯的端點](#)。

數位分身可用性

使用 [AWS Ground Station 數位分身功能](#) 可在所有 AWS Ground Station 可使用 [的 AWS 區域中](#) 使用。數位分身地面站是生產地面站的確切副本，字首為「數位分身」的 Ground Station Name。例如，「數位分身俄亥俄 1」是數位分身地面站，其為「俄亥俄 1」生產地面站的確切副本。

AWS Ground Station 網站遮罩

每個 AWS Ground Station [天線位置](#) 都有相關聯的網站遮罩。這些遮罩會在指向某些方向時封鎖該位置的天線傳輸或接收，通常接近地平線。遮罩可能會考慮：

- 圍繞天線的地理地形功能 – 例如，這包括像是山巒或建築物等會封鎖無線電頻率 (RF) 訊號或防止傳輸的物體。
- 無線電頻率干擾 (RFI) – 這會影響接收（外部 RFI 來源影響 AWS Ground Station 天線的下行訊號）和傳輸（AWS Ground Station 天線傳輸的 RF 訊號對外部接收器造成負面影響）的能力。
- 法律授權 – 在每個區域中操作 AWS Ground Station 的本機網站授權可能包括特定限制，例如用於傳輸的最小高度角度。

這些網站遮罩可能會隨著時間而變更。例如，新建建築物可以在天線位置附近建構、RFI 來源可能會變更，或者法律授權可能會以不同的限制續約。您可以根據保密協議 (NDA) 使用 AWS Ground Station 網站遮罩。

客戶特定的遮罩

除了每個站點的 AWS Ground Station 網站遮罩之外，由於您自己的法律授權限制，在給定區域中與衛星通訊，您可能還有其他遮罩。這類遮罩可以在 AWS Ground Station 中逐 case-by-case 設定，以確保在使用 AWS Ground Station 與這些衛星通訊時符合規範。如需詳細資訊，請聯絡 AWS Ground Station 團隊。

網站遮罩對可用聯絡時間的影響

網站遮罩有兩種：上行（傳輸）網站遮罩和下行（接收）網站遮罩。

使用 ListContacts 操作列出可用的聯絡時間時，AWS Ground Station 會根據衛星何時會高於，並設定在下行遮罩下方，傳回可見性時間。可用的聯絡時間是以這個下行遮罩可見性時段為基礎。這可確保當您的衛星低於下行遮罩時，不會預留時間。

上行網站遮罩不會套用至可用的聯絡時間，即使任務設定檔在資料流程邊緣中包含[天線上行組態](#)。這可讓您使用下行的所有可用聯絡時間，即使上行時間因上行網站遮罩而無法使用。不過，上行訊號在部分或全部保留給衛星聯絡人的時間內可能無法傳輸。排程上行傳輸時，您需負責考慮提供的上行遮罩。

無法用於上行的聯絡部分會因聯絡期間的衛星軌跡，相對於天線位置的上行網站遮罩而有所不同。在上行和下行網站遮罩類似的區域中，此持續時間通常很短。在其他區域中，上行遮罩可能遠高於下行網站遮罩，這可能會導致大量的聯絡持續時間無法使用上行。即使部分保留時間無法用於上行，仍會向您收取完整的聯絡時間費用。

AWS Ground Station 站點功能

為了簡化您的體驗，AWS Ground Station 決定一組常見的天線類型功能，然後將多個天線部署到地面站位置。加入步驟的一部分可確保您的衛星與特定位置的天線類型相容。預留聯絡人時，您可以間接判斷使用的天線類型。這可確保您在特定地面站點的體驗隨著時間保持不變，無論使用哪些天線。由於各種環境問題，例如現場的天氣，聯絡人的特定效能會有所不同。

目前，所有網站都支援下列功能：

Note

除非另有說明，否則下表中的每一列都會指出獨立的通訊路徑。存在重複的資料列，以反映我們的多通道功能，允許同時使用多個通訊路徑。

功能類型	頻率範圍	頻寬範圍	Polarization	Common Name (通用名稱)	備註
antenna-downlink	7750 - 8500 MHz	50 - 400 MHz	RHCP	X 頻帶寬頻下行	此功能需要使用 AWS Ground Station 代理程式 。
antenna-downlink	7750 - 8500 MHz	50 - 400 MHz	RHCP		Alaska 1 或 Punta Arenas 1 不支援此功能。
antenna-downlink	7750 - 8500 MHz	50 - 400 MHz	RHCP		

功能類型	頻率範圍	頻寬範圍	Polarization	Common Name (通用名稱)	備註
antenna-downlink	7750 - 8500 MHz	50 - 400 MHz	RHCP		每個位置每個極化的彙總頻寬不得超過400MHz。 所有使用的頻率範圍都必須不重疊。
antenna-downlink	7750 - 8500 MHz	50 - 400 MHz	RHCP		
antenna-downlink	7750 - 8500 MHz	50 - 400 MHz	LHCP		
antenna-downlink	7750 - 8500 MHz	50 - 400 MHz	LHCP		
antenna-downlink	7750 - 8500 MHz	50 - 400 MHz	LHCP		
antenna-downlink	7750 - 8500 MHz	50 - 400 MHz	LHCP		
antenna-downlink	2200 - 2290 MHz	高達 40 MHz	RHCP	S 頻帶下行	一次只能使用一個極化
antenna-downlink	2200 - 2290 MHz	高達 40 MHz	LHCP		
antenna-downlink	7750 - 8500 MHz	高達 40 MHz	RHCP	X 頻帶窄頻帶下行	一次只能使用一個極化
antenna-downlink	7750 - 8500 MHz	高達 40 MHz	LHCP		

功能類型	頻率範圍	頻寬範圍	Polarization	Common Name (通用名稱)	備註
antenna-uplink	2025 - 2110 MHz	高達 40 MHz	RHCP	S 頻帶上行連結	一次只能使用一個極化
antenna-uplink	2025 - 2110 MHz	高達 40 MHz	LHCP		EIRP 20-50 dBW
antenna-uplink-echo	2025 - 2110 MHz	2 MHz	RHCP	上行回應	符合天線上行限制
antenna-uplink-echo	2025 - 2110 MHz	2 MHz	LHCP		
antenna-downlink-demod-decode	7750 - 8500 MHz	高達 500 MHz	RHCP	X 頻帶解調和解碼下行	
antenna-downlink-demod-decode	7750 - 8500 MHz	高達 500 MHz	LHCP		
追蹤	N/A	N/A	N/A	N/A	支援自動追蹤和程式追蹤

* RHCP = 右手圓形極化，LHCP = 左手圓形極化。如需極化的詳細資訊，請參閱[環形極化](#)。

了解 AWS Ground Station 如何使用衛星暫時性資料

[暫時性](#)、複數暫時性，是提供天文物件軌跡的檔案或資料結構。從歷史上來看，此檔案僅指表格式資料，但逐漸會導向至表示太空船軌跡的多種資料檔案。

AWS Ground Station 使用暫時性資料來判斷聯絡人何時可供您的衛星使用，並正確命令 AWS Ground Station 網路中的天線指向您的衛星。根據預設，如果您的衛星有指派的 [NORAD ID](#)，則不需要採取任何動作來 AWS Ground Station 提供暫時性資料。

主題

- [預設暫時性資料](#)
- [提供自訂暫時性資料](#)
- [了解使用哪些 ephemeris](#)
- [取得衛星的目前暫時性資料](#)
- [還原至預設暫時性資料](#)

預設暫時性資料

根據預設，AWS Ground Station 會使用來自 [Space-Track](#) 的公開可用資料，而且不需要採取任何動作來提供 AWS Ground Station 這些預設的短暫性。這些暫時性元素是與衛星 [NORAD ID](#) 相關聯的 [雙行元素集 \(TLEs\)](#)。所有預設的短暫性事件的優先順序為 0。因此，透過 ephemeris API 上傳的任何未過期的自訂暫時性資料一律會被覆寫，其優先順序必須一律為 1 或更高。

沒有 NORAD ID 的衛星必須上傳自訂 ephemeris 資料至其中 AWS Ground Station。例如，剛啟動或刻意從 [Space-Track](#) 目錄省略的衛星，將不會有 NORAD ID，而且需要上傳自訂暫時性資料。如需提供自訂暫時性的詳細資訊，請參閱：[提供自訂暫時性資料](#)。

提供自訂暫時性資料

Important

ephemeris API 目前處於預覽狀態

僅在需要時提供對 Ephemeris API 的存取。如果您需要上傳自訂暫時性資料的能力，您應該聯絡 <aws-groundstation@amazon.com>。AWS Ground Station 會將暫時性資料視為[個人化用量資料](#)。如果您使用此選用功能，AWS 將使用 ephemeris 資料來提供故障診斷支援。

概觀

Ephemeris API 允許將自訂暫時性樣板上傳到 AWS Ground Station，以便與衛星搭配使用。這些暫時性物質會覆寫來自 [Space-Track](#) 的預設暫時性物質（請參閱：[預設暫時性資料](#)）。我們支援以 Orbit Ephemeris Message (OEM) 和雙行元素 (TLE) 格式接收暫時性資料。

上傳自訂暫時化可以改善追蹤品質、處理沒有可用 [Space-Track](#) 暫時化的早期操作 AWS Ground Station，以及考慮操作。

Note

在為衛星指派衛星目錄號碼之前提供自訂 ephemeris 時，您可以將 00000 用於 TLE 的衛星目錄號碼欄位，並將 000 用於 TLE 或 OEM 中繼資料之國際指標欄位的啟動號碼部分（例如，2024 年啟動的車輛為 24000A）。

如需 TLEs 格式的詳細資訊，請參閱[雙行元素集](#)。如需 OEMs 格式的詳細資訊，請參閱[OEM ephemeris 格式](#)。

OEM ephemeris 格式

AWS Ground Station 根據 [CCSDS 標準](#) 處理 OEM 客戶提供的 Ephemerides，但有一些額外的限制。OEM 檔案應為 KVN 格式。下表概述 OEM 中的不同欄位，以及與 CCSDS 標準 AWS Ground Station 的差異。

章節	欄位	需要 CCSDS	AWS Ground Station 必要	備註
標頭	CCSDS_OEM_VERS	是	是	必要值：2.0
	COMMENT	否	否	
	分類	否	否	

章節	欄位	需要 CCSDS	AWS Ground Station 必要	備註
	CREATION_DATE	是	是	
	原始伺服器	是	是	
	MESSAGE_ID	否	否	
中繼資料	META_START	是	是	
	COMMENT	否	否	
	OBJECT_NAME	是	是	
	OBJECT_ID	是	是	
	CENTER_NAME	是	是	必要值：地球
	REF_FRAME	是	是	接受的值： EME2000, ITRF2000
	REF_FRAME_EPOCH	否	不支援*	不需要，因為接受的 REF_FRAMEs 具有隱含 epoch
	TIME_SYSTEM	是	是	必要值：UTC
	START_TIME	是	是	
	USEABLE_START_TIME	否	否	
USEABLE_STOP_TIME	否	否		
STOP_TIME	是	是		

章節	欄位	需要 CCSDS	AWS Ground Station 必要	備註
	INTERPOLATION	否	是	必要，因此 AWS Ground Station 可以為聯絡人產生準確的指向角度。
	INTERPOLATION_DEGREE	否	是	必要，因此 AWS Ground Station 可以為聯絡人產生準確的指向角度。
	META_STOP	是	是	
資料	X	是	是	在中代表 km
	Y	是	是	在中代表 km
	Z	是	是	在中代表 km
	X_DOT	是	是	在中代表 km/s
	Y_DOT	是	是	在中代表 km/s
	Z_DOT	是	是	在中代表 km/s
	X_DDOT	否	否	在中代表 km/s ²
	Y_DDOT	否	否	在中代表 km/s ²
	Z_DDOT	否	否	在中代表 km/s ²
共變數矩陣	轉移_開始	否	否	

章節	欄位	需要 CCSDS	AWS Ground Station 必要	備註
	EPOCH	否	否	
	DISC_REF_FRAME	否	否	
	樞紐分析_停止	否	否	

* 如果提供 OEM 中 AWS Ground Station 包含 不支援的任何資料列，OEM 將驗證失敗。

與的 CCSDS 標準的重要偏差 AWS Ground Station 為：

- CCSDS_OEM_VERS 必須是 2.0。
- REF_FRAME 必須是 EME2000或 ITRF2000。
- 不支援 REF_FRAME_EPOCH AWS Ground Station。
- CENTER_NAME 必須是 Earth。
- TIME_SYSTEM 必須是 UTC。
- CPE AWS Ground Station 需要 INTERPOLATION 和 INTERPOLATION_DEGREE。

KVN 格式的範例 OEM ephemeris

以下是 JPSS-1 公有廣播者衛星的 KVN 格式 OEM ephemeris 截斷範例。

```
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

```

建立自訂 ephemeris

您可以使用 API 中的 AWS Ground Station [CreateEphemeris](#) 動作來建立自訂暫時性資料。此動作將使用請求內文中的資料或從指定的 S3 儲存貯體上傳暫時性資料。

請務必注意，上傳 ephemeris 會將 ephemeris 設定為 `VALIDATING` 並啟動非同步工作流程，以驗證和產生來自 ephemeris 的潛在聯絡人。只有在 ephemeris 通過此工作流程後，`ENABLED` 才會將其用於聯絡人。您應該輪詢 [DescribeEphemeris](#) 以取得暫時性狀態，或使用 CloudWatch 事件來追蹤暫時性狀態變更。

若要對無效的暫時性事件進行故障診斷，請參閱：[故障診斷無效的短暫性事件](#)

範例：透過 API 建立雙行元素 (TLE) 集合 ephemeris

AWS SDKs 和 CLI 可用來 AWS Ground Station 透過 [CreateEphemeris](#) 呼叫，將雙行元素 (TLE) 集合暫時性資料上傳至。此暫時性資料將用於取代衛星的預設暫時性資料 (請參閱[預設暫時性資料](#))。此範例示範如何使用[AWS 適用於 Python 的 SDK \(Boto3\)](#) 執行此操作。

TLE 集是 JSON 格式的物件，可將一或多個 TLEs 串連在一起，以建構連續軌跡。TLEs 集合中的 TLE 必須形成連續集合，我們可以用來建構軌跡 (即 TLE 集合中 TLEs 之間的時間差距)。範例 TLE 集如下所示：

```
# 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

TLEs 集合中 TLE 的時間範圍必須完全相符，才能成為有效的連續軌跡。

您可以透過 boto3 AWS Ground Station 用戶端上傳 TLE 集，如下所示：

```

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)
                    }
                }
            ]
        }
    })

```

此呼叫將傳回 `ephemerisId`，可用於在未來參考 `ephemeris`。例如，我們可以使用上述呼叫中提供的 `ephemerisId` 來輪詢 `ephemeris` 狀態：

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

以下提供 [DescribeEphemeris](#) 動作的範例回應

```

{
  "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}}]"
    }
  }
}

```

```
}
```

建議您輪詢 [DescribeEphemeris](#) 路由或使用 CloudWatch 事件來追蹤上傳的暫時性事件的狀態，因為它必須先經過非同步驗證工作流程，才能將其設定為 ENABLED，並可用於排程和執行聯絡人。

請注意，在上述25994範例中，TLE 集中所有 TLEs中的 NORAD ID 必須符合您的衛星在 [Space-Track](#) 資料庫中指派的 NORAD ID。

範例：從 S3 儲存貯體上傳 Ephemeris 資料

您也可以透過指向儲存貯體和物件金鑰，直接從 S3 儲存貯體上傳 ephemeris 檔案。AWS Ground Station 將代表您擷取物件。有關 中靜態資料加密的詳細資訊 AWS Ground Station ，請參閱：[適用於 AWS Ground Station 的靜態資料加密](#)

以下是從 S3 儲存貯體上傳 OEM ephemeris 檔案的範例

```
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",
            }
        }
    })
```

以下是從 [DescribeEphemeris](#) 動作傳回的資料範例，該動作為上一個範例程式碼區塊中上傳的 OEM ephemeris 呼叫。

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

範例：搭配使用客戶提供的 ephemeride AWS Ground Station

如需搭配使用客戶提供的暫時性資料的詳細指示 AWS Ground Station，請參閱[搭配使用客戶提供的暫時性資料 AWS Ground Station](#)（以及相關聯的 GitHub 儲存庫 [aws-samples/aws-groundstation-cpe](#)）

了解使用哪些 ephemeris

Ephemerides 具有優先順序、過期時間和啟用的旗標。這些會一起決定要用於衛星的暫時性。每個衛星只能有一個暫時作用。

將使用的暫時性資料是啟用最高優先順序的暫時性資料，其過期時間是未來的時間。優先順序值越大表示優先順序越高。ListContacts 傳回的可用聯絡時間是以此暫時性為基礎。如果多個ENABLED暫時性事件具有相同的優先順序，則會使用最近建立或更新的暫時性事件。

Note

AWS Ground Station 對每個衛星ENABLED客戶提供的暫時性資料數量具有服務配額（請參閱：[Service Quotas](#)）。若要在達到此配額後上傳 ephemeris 資料，請刪除（使用 DeleteEphemeris）或停用（使用 UpdateEphemeris）最低優先順序/最早建立的客戶提供的 ephemeride。

如果尚未建立暫時性，或者如果沒有暫時性化具有ENABLED狀態，則 AWS Ground Station 將在可用時使用衛星（來自 [Space-Track](#)）的預設暫時性。此預設 ephemeris 的優先順序為 0。

新暫時性事件對先前排程聯絡人的影響

使用 [DescribeContact API](#) 透過傳回作用中的可見性時間，來檢視新短暫性對先前排程聯絡人的影響。

上傳新 ephemeris 之前排程的聯絡人將保留最初排程的聯絡時間，而天線追蹤將使用作用中的 ephemeris。如果太空船的位置根據作用中的暫時性差異很大，則由於太空船在傳輸/接收站點遮罩之外

操作，這可能會導致與天線的衛星接觸時間縮短。因此，我們建議您在上傳與先前 ephemeris 有很大差異的新 ephemeris 之後，取消和重新排程未來的聯絡。使用 [DescribeContact API](#)，您可以比較您的排程聯絡人和傳回的 `visibilityStartTime` `startTime` `endTime` 和 `visibilityEndTime`，以判斷未來因傳輸/接收網站遮罩外操作的太空船而無法使用的聯絡人部分 `visibilityEndTime`。如果您選擇取消和重新排程未來的聯絡（們），聯絡時間範圍不能超過 30 秒。取消太接近聯絡時間時，取消的聯絡可能會產生費用。如需取消聯絡的詳細資訊，請參閱：[Ground Station FAQs](#)。

取得衛星的目前暫時性資料

AWS Ground Station 特定衛星使用的目前暫時性暫時性，可透過呼叫 [GetSatellite](#) 或 [ListSatellites](#) 動作來擷取。這兩種方法都會傳回目前使用中 ephemeris 的中繼資料。此暫時性中繼資料對於上傳至的自訂暫時性中繼資料 AWS Ground Station 和預設暫時性中繼資料不同。

預設冪等化只會包含 `source` 和 `epoch` 欄位。`epoch` 是從 [Space-Track](#) 提取的 [雙行元素集](#) 的 `epoch`，目前正在用於運算衛星的軌跡。

自訂 ephemeris `source` 的值為 `"CUSTOMER_PROVIDED"` 並在 `ephemerisId` 欄位中包含唯一識別符。此唯一識別符可用於透過 [DescribeEphemeris](#) 動作查詢暫時性資料。如果在 AWS Ground Station 透過 [CreateEphemeris](#) 動作上傳至 期間指派 ephemeris 名稱，則會傳回選用 `name` 欄位。

請務必注意，動態更新暫時性資料，AWS Ground Station 因此傳回的資料只是呼叫 API 時正在使用暫時性資料的快照。

使用預設 ephemeris `GetSatellite` 傳回衛星的範例

```
{
  "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
  }
}
```

使用自訂 ephemeris 的 `GetSatellite` 衛星範例

```
{
  "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"
  }
}
```

還原至預設暫時性資料

當您上傳自訂暫時性資料時，它會覆寫該特定衛星 AWS Ground Station 使用的預設暫時性資料。AWS Ground Station 不會再次使用預設暫時性資料，直到目前沒有啟用、未過期的客戶提供暫時性資料可供使用為止。AWS Ground Station 也不會列出目前客戶提供暫時性資料過期時間之後的聯絡人，即使該過期時間之後仍有預設暫時性資料可用。

若要還原為預設的 [Space-Track](#) 暫時性資料，您需要執行下列其中一項操作：

- 刪除（使用 [DeleteEphemeris](#)）或停用（使用 [UpdateEphemeris](#)）所有啟用的客戶提供的暫時性資料。您可以使用 [ListEphemerides](#) 列出客戶提供的衛星短暫性。
- 等待所有現有客戶提供的暫時性資料過期。

您可以呼叫 [GetSatellite](#) 並確認目前衛星的 ephemeris 為 `SPACE_TRACK`，以確認 source 正在使用預設 ephemeris `SPACE_TRACK`。如需預設短暫性的詳細資訊 [預設暫時性資料](#)，請參閱。

使用資料流程

AWS Ground Station 使用節點和邊緣關係來建構資料流程，以啟用資料的串流處理。每個節點都由描述其預期處理的組態表示。若要說明此概念，請考慮將的資料流程antenna-downlink傳送至 s3-recording。antenna-downlink 節點代表根據組態上定義的參數，無線電頻譜的類比到數位轉型。s3-recording 代表將接收傳入資料的運算節點，並將其存放在 S3 儲存貯體中。產生的資料流程是根據您的規格，將數位化 RF 資料非同步交付至 S3 儲存貯體的資料。

在任務描述檔中，您可以建立許多資料流程來滿足您的需求。下列各節說明如何設定要與 搭配使用的其他 AWS 資源 AWS Ground Station ，並提供建構資料流程的建議。如需每個節點行為的詳細資訊，包括是否被視為來源或目的地節點，請參閱 [使用 AWS Ground Station 組態](#)。

主題

- [AWS Ground Station 資料平面界面](#)
- [使用跨區域資料交付](#)
- [設定 Amazon S3](#)
- [設定 Amazon VPC](#)
- [設定 Amazon EC2](#)

AWS Ground Station 資料平面界面

所選資料流程產生的資料結構取決於資料流程的來源。這些格式的詳細資訊會在衛星加入期間提供給您。以下摘要說明用於每種資料流程的格式。

- antenna-downlink
 - (頻寬小於 54MHz) 資料會以 [VITA-49 訊號資料/IP](#) 格式封包的形式交付。
 - (頻寬greater-than-or-equal-to 54MHz) 資料會以第 2 AWS Ground Station 級封包形式交付。
- antenna-downlink-demod-decode
 - 資料會以解調/解碼資料/IP 格式封包的形式交付。
- 天線上行
 - 資料必須以 [VITA-49 訊號資料/IP](#) 格式封包的形式交付。
- antenna-uplink-echo
 - 資料會以 [VITA-49 訊號資料/IP](#) 格式封包的形式交付。

使用跨區域資料交付

AWS Ground Station 跨區域資料交付功能可讓您靈活地將資料從天線傳送至任何 AWS Ground Station 支援的 AWS 區域。這表示您可以將基礎設施維護在單一 AWS 區域中，並在 [AWS Ground Station 位置](#) 您加入的任何 AWS Ground Station 上排程聯絡人。

在 Amazon S3 儲存貯體中接收您的聯絡資料時，目前所有 AWS Ground Station 支援的區域都可使用跨區域資料交付。AWS Ground Station 會為您管理所有交付層面。

所有 antenna-to-destination 區域皆可使用 AWS Ground Station 代理程式將跨區域資料交付至 Amazon EC2。此設定不需要唯一的組態或核准。

使用資料流程端點的跨區域資料交付至 Amazon EC2 預設為可在下列 antenna-to-destination 區域中使用*。

- 美國東部 (俄亥俄) 區域 (us-east-2) 至美國西部 (奧勒岡) 區域 (us-west-2)
- 美國西部 (奧勒岡) 區域 (us-west-2) 至美國東部 (俄亥俄) 區域 (us-east-2)

若要使用跨區域資料交付至 Amazon EC2 執行個體，必須在您目前的 AWS 區域中建立資料流程端點，且 dataflow-endpoint-config 必須指定相同的區域。

下表摘要說明跨區域資料交付的支援區域和交付方法。

Method of Receiving	Antenna Region	Receiving Region
Amazon S3 資料交付	所有已加入 AWS Ground Station AWS Ground Station 位置	所有 AWS Ground Station 區域
AWS Ground Station Amazon EC2 上的代理程式	所有已加入 AWS Ground Station AWS Ground Station 位置	所有 AWS Ground Station 區域
Amazon EC2 上的資料流程端點*	美國東部 (俄亥俄) 區域 (us-east-2)	美國西部 (奧勒岡) 區域 (us-west-2)
	美國西部 (奧勒岡) 區域 (us-west-2)	美國東部 (俄亥俄) 區域 (us-east-2)

*未列出的其他antenna-to-destination區域需要特殊的 Amazon EC2 和軟體設定。如需加入說明，請傳送電子郵件至 <aws-groundstation@amazon.com> 聯絡我們。

設定 Amazon S3

您可以使用 Amazon S3 儲存貯體來接收使用的下行訊號 AWS Ground Station。若要建立目的地 s3-recording-config，您必須能夠指定 Amazon S3 儲存貯體和 IAM 角色，該角色授權 AWS Ground Station 將檔案寫入儲存貯體。

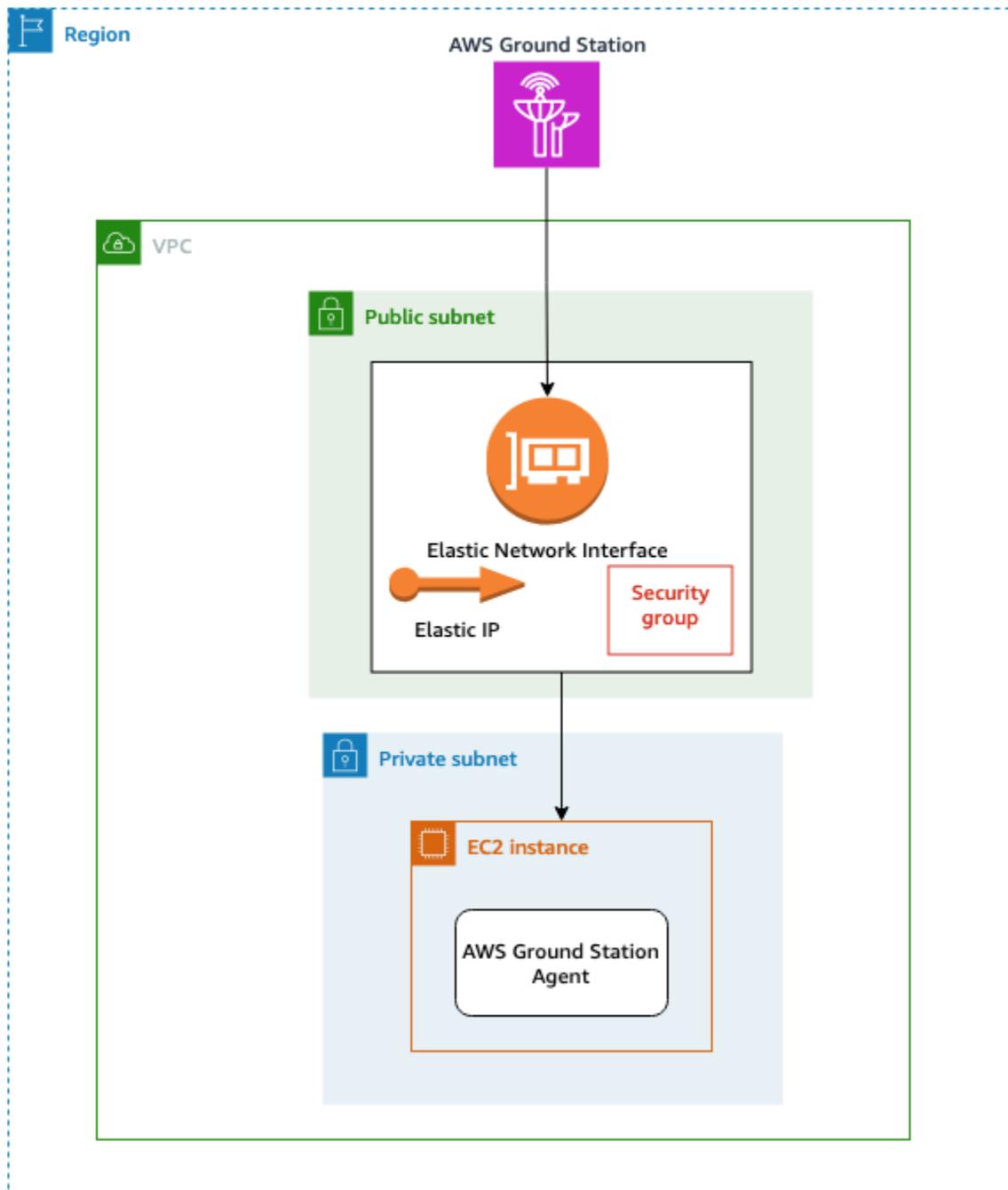
[Amazon S3 錄製組態](#) 如需 Amazon S3 儲存貯體、IAM 角色或 AWS Ground Station 組態建立的限制，請參閱。

設定 Amazon VPC

設定 VPC 的完整指南超出本指南的範圍。如需深入了解，請參閱 [Amazon VPC 使用者指南](#)。

在本節中，會說明您的 Amazon EC2 和資料流程端點如何在 VPC 內存在。AWS Ground Station 不支援特定資料流程的多個交付點 - 預期每個資料流程都會終止為單一 EC2 接收器。由於我們預期單一 EC2 接收器，因此組態不是多可用區域備援。如需將使用您的 VPC 的完整範例，請參閱 [範例任務設定檔組態](#)。

使用 AWS Ground Station 代理程式的 VPC 組態



您的衛星資料會提供給靠近天線的 AWS Ground Station 代理程式執行個體。AWS Ground Station 代理程式會分割資料，然後使用您提供的 AWS KMS 金鑰加密資料。每個條紋都會從 AWS 網路骨幹的來源天線傳送到您的 [Amazon EC2 彈性 IP \(EIP\)](#)。資料會透過連接的 Amazon EC2 彈性網路界面 (ENI) 送達您的 EC2 執行個體。 [Amazon EC2](#) 在您的 EC2 執行個體上，已安裝的 AWS Ground

Station 代理程式會解密您的資料並執行轉送錯誤修正 (FEC) 以復原任何捨棄的資料，然後將其轉送至您在設定中指定的 IP 和連接埠。

以下清單會在設定 VPC 以進行 AWS Ground Station 客服人員交付時，指出唯一的設定考量。

安全群組 - 建議您設定僅限 AWS Ground Station 流量的安全群組。此安全群組應允許 UDP 輸入流量位於您在 Dataflow 端點群組中指定的相同連接埠範圍。AWS Ground Station 會維護 AWS 受管字首清單，將您的許可限制為僅限 AWS Ground Station IP 地址。如需如何取代部署區域的 PrefixListId 的詳細資訊，請參閱 [AWS 受管字首清單](#)。

彈性網路界面 (ENI) - 您需要將上述安全群組與此 ENI 建立關聯，並將其放置在公有子網路中。

下列 CloudFormation 範本示範如何建立本節所述的基礎設施。

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:

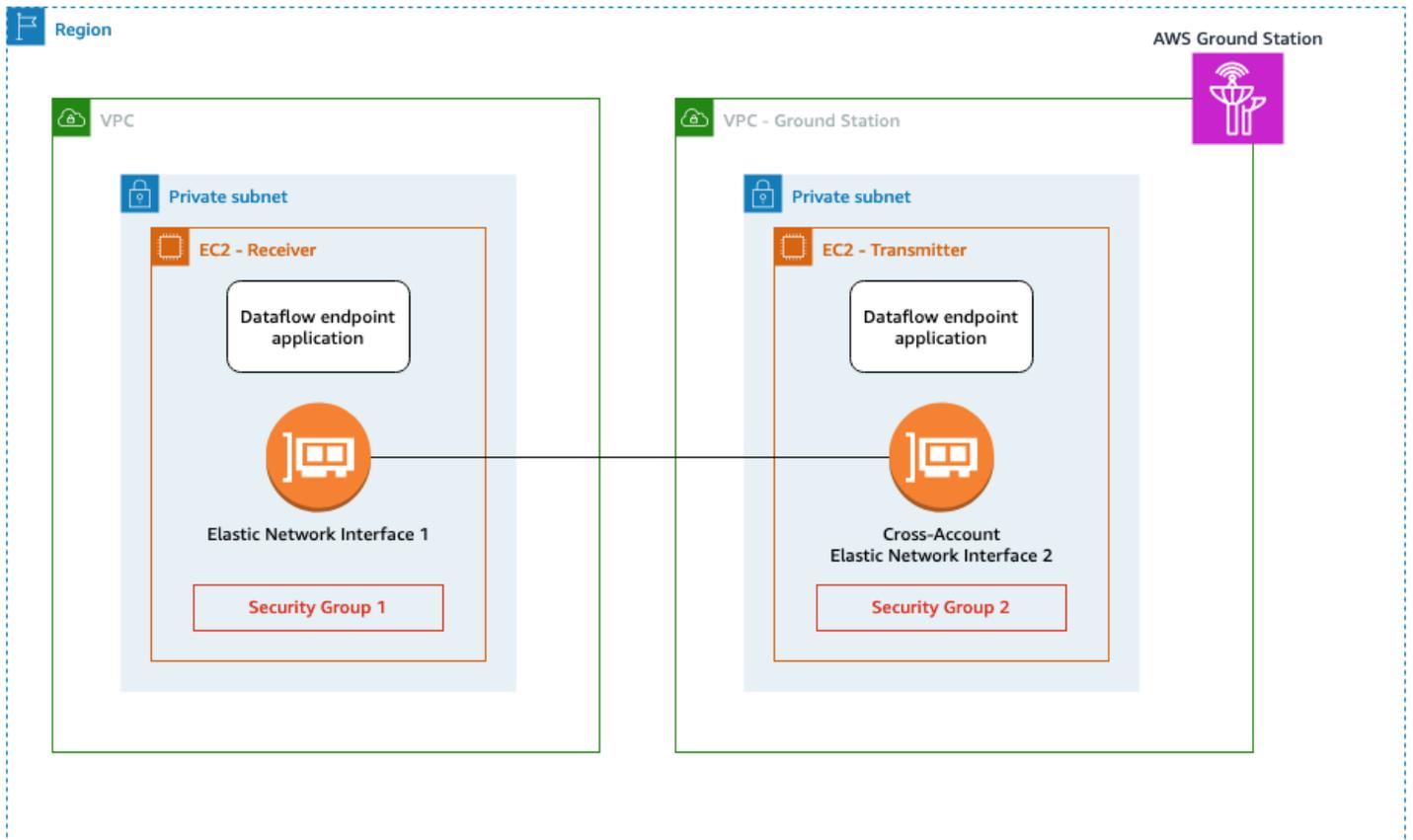
AllocationId:

Fn::GetAtt: [*ReceiveInstanceEIP*, AllocationId]

NetworkInterfaceId:

Ref: *InstanceNetworkInterface*

具有資料流程端點的 VPC 組態



您的衛星資料會提供給靠近天線的資料流程端點應用程式執行個體。然後，資料會透過跨帳戶 [Amazon EC2 彈性網路界面 \(ENI\)](#) 從擁有的 VPC 傳送 AWS Ground Station。然後，資料會透過連接到 Amazon EC2 執行個體的 ENI 到達您的 EC2 執行個體。Amazon EC2 然後，安裝的資料流程端點應用程式會將其轉送到您在設定中指定的 IP 和連接埠。上行連線會發生此流程的反向。

以下清單會在設定 VPC 進行資料流程端點交付時，指出唯一的設定考量。

IAM 角色 - IAM 角色是 Dataflow 端點的一部分，不會顯示在圖表中。用來建立跨帳戶 ENI 並將其連接至 AWS Ground Station Amazon EC2 執行個體的 IAM 角色。

安全群組 1 - 此安全群組會連接到 ENI，該 ENI 將與您帳戶中的 Amazon EC2 執行個體相關聯。它需要在 dataflow-endpoint-group 群組中指定的連接埠上允許來自安全群組 2 的 UDP 流量。

彈性網路界面 (ENI) 1 - 您需要將安全群組 1 與此 ENI 建立關聯，並將其放置在子網路中。

子網路 - 您需要確保帳戶中 Amazon EC2 執行個體的每個資料流程至少有一個可用的 IP 地址。如需子網路大小的詳細資訊，請參閱 [子網路 CIDR 區塊](#)

安全群組 2 - 在 Dataflow 端點中參考此安全群組。此安全群組將連接到 ENI，該 ENI AWS Ground Station 將用來將資料放入您的帳戶。

區域 - 如需跨區域連線支援區域的詳細資訊，請參閱 [使用跨區域資料交付](#)。

下列 CloudFormation 範本示範如何建立本節所述的基礎設施。

DataflowEndpointSecurityGroup:

Type: AWS::EC2::SecurityGroup

Properties:

GroupDescription: Security Group for AWS Ground Station registration of Dataflow Endpoint Groups

VpcId: *YourVpcId*

AWSGroundStationSecurityGroupEgress:

Type: AWS::EC2::SecurityGroupEgress

Properties:

GroupId: !Ref: *DataflowEndpointSecurityGroup*

IpProtocol: udp

FromPort: *55555*

ToPort: *55555*

CidrIp: *10.0.0.0/8*

Description: "Allow AWS Ground Station to send UDP traffic on port 55555 to the 10/8 range."

InstanceSecurityGroup:

Type: AWS::EC2::SecurityGroup

Properties:

GroupDescription: *AWS Ground Station receiver instance security group.*

VpcId: *YourVpcId*

SecurityGroupIngress:

- IpProtocol: udp

FromPort: *55555*

ToPort: *55555*

SourceSecurityGroupId: !Ref *DataflowEndpointSecurityGroup*

```
Description: "Allow AWS Ground Station Ingress from
DataflowEndpointSecurityGroup"
```

ReceiverSubnet:

```
Type: AWS::EC2::Subnet
```

```
Properties:
```

```
# Ensure your CidrBlock will always have at least one available IP address per
dataflow endpoint.
```

```
# See https://docs.aws.amazon.com/vpc/latest/userguide/subnet-sizing.html for
subent sizing guidelines.
```

```
CidrBlock: "10.0.0.0/24"
```

```
Tags:
```

```
- Key: "Name"
```

```
Value: "AWS Ground Station - Dataflow endpoint Example Subnet"
```

```
- Key: "Description"
```

```
Value: "Subnet for EC2 instance receiving AWS Ground Station data"
```

```
VpcId: !Ref ReceiverVPC
```

設定 Amazon EC2

同步交付 VITA-49 Signal/IP 資料或 VITA-49 Extension data/IP 需要正確設定 Amazon EC2 執行個體，才能透過 AWS Ground Station 代理程式或資料流程端點交付。根據您的特定需求，您可以直接在同一個執行個體上執行前端 (FE) 處理器或軟體定義無線電 (SDR)，或者您可能需要使用其他 EC2 執行個體。選擇和安裝您的 FE 或 SDR 超出本使用者指南的範圍。如需特定資料格式的詳細資訊，請參閱 [AWS Ground Station 資料平面界面](#)。

如需服務條款的相關資訊，請參閱 [AWS 服務條款](#)。

提供的常見軟體

AWS Ground Station 提供常見的軟體，以簡化 Amazon EC2 執行個體的設定。

AWS Ground Station 代理程式

AWS Ground Station 代理程式會接收數位中繼頻率 (DigIF) 下行資料，並輸出解密的資料以啟用下列項目：

- 從 40 MHz 到 400 MHz 頻寬的 DigIF 下行功能。 MHz MHz
- 將高速率、低抖動的 DigIF 資料交付至 AWS 網路上的任何公有 IP (AWS 彈性 IP)。
- 使用轉送錯誤校正 (FEC) 提供可靠的資料。

- 使用客戶受管 AWS KMS 金鑰進行加密，以保護資料交付。

如需詳細資訊，請參閱[AWS Ground Station 客服人員使用者指南](#)。

Dataflow 端點應用程式

用於 AWS Ground Station 在 AWS Ground Station 天線位置與 Amazon EC2 執行個體之間傳送和接收資料的聯網應用程式。它可用於資料的上行和下行。

軟體定義的無線電 (SDR)

軟體定義的無線電 (SDR)，可用於調節/取消調節用於與衛星通訊的訊號。

AWS Ground Station Amazon Machine Image AMIs)

為了減少這些安裝的建置和組態時間，AWS Ground Station 也提供預先設定的 AMIs。加入完成後，您的帳戶即可使用具有資料流程端點聯網應用程式的 AMIs 和軟體定義的無線電 (SDR)。您可以在 Amazon EC2 主控台中搜尋私有 [Amazon Machine Image \(AMIs\)](#) 中的地面站，以找到它們。具有 AWS Ground Station 代理 AMIs 是公有的，可以透過在公有 Amazon Machine Image (AMI) 中搜尋地面站，在 Amazon EC2 主控台中找到。 [AMIs](#)

使用聯絡人

您可以使用 AWS Ground Station 主控台或您選擇的語言 AWS SDK，輸入衛星資料、識別天線位置 AWS CLI、通訊和排程所選衛星的天線時間。您可以在聯絡開始前最多 15 分鐘檢閱、取消和重新排程聯絡預留*。此外，如果您使用的是預留分鐘定價模式，您可以檢視 AWS Ground Station 預留分鐘定價計劃的詳細資訊。

AWS Ground Station 支援跨區域資料交付。資料流程端點組態為您選取任務設定檔的一部分，會決定資料傳送到哪個區域。如需使用跨區域資料交付的詳細資訊，請參閱 [使用跨區域資料交付](#)。

若要排程接收，必須設定您的資源。如果您尚未設定資源，請參閱 [開始使用](#)。呼叫 [ReserveContact](#) 時，會 AWS Ground Station 拍攝任務設定檔的快照，並設定資源以在聯絡傳遞期間使用。使用 [UpdateMissionProfile](#) 和 [UpdateConfig](#) APIs 對這些資源的變更不會反映在更新之前預留的聯絡人中。如果您需要將資源變更套用至已排定的聯絡人，您必須先使用 [CancelContact](#) 取消聯絡人，然後使用 [ReserveContact](#) 重新排程聯絡人。

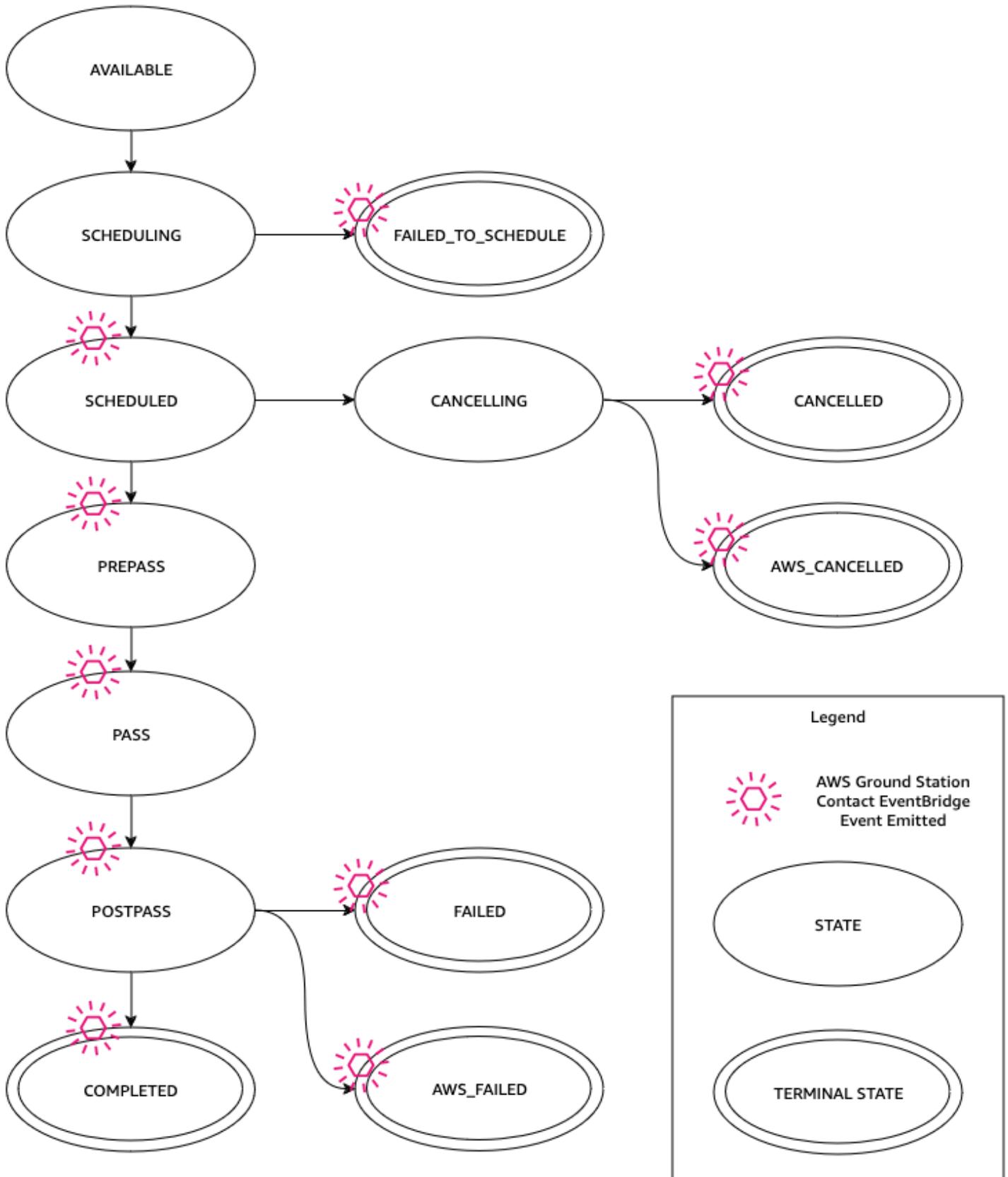
* 取消太接近聯絡時間時，取消聯絡可能會產生費用。如需取消聯絡人的詳細資訊，請參閱：[Ground Station FAQs](#)。

主題

- [了解聯絡生命週期](#)

了解聯絡生命週期

了解聯絡生命週期有助於判斷如何設定自動化，以及在疑難排解期間。下圖顯示 AWS Ground Station 聯絡生命週期以及生命週期期間發出的事件橋接事件。請務必注意，COMPLETED、FAILED、FAILED_TO_SCHEDULE、CANCELLED、AWS_CANCELLED 和 AWS_FAILED 是終端狀態。聯絡人不會從終端機狀態轉換。如需每個狀態所表示內容的詳細資訊 [AWS Ground Station 聯絡狀態](#)，請參閱。



AWS Ground Station 聯絡狀態

AWS Ground Station 聯絡人狀態可讓您深入了解該聯絡人在特定時間發生的情況。

聯絡狀態

以下是聯絡人可以擁有的狀態清單：

- 可用 - 聯絡人可供保留。
- SCHEDULING - 聯絡人正在進行排程。
- 已排程 - 已成功排程聯絡人。
- FAILED_TO_SCHEDULE - 聯絡人無法排程。
- PREPASS - 聯絡人即將開始，並且正在準備資源。
- PASS - 聯絡人目前正在執行，並且正在與衛星通訊。
- POSTPASS - 通訊已完成，正在使用的資源正在清除。
- 已完成 - 聯絡人已完成，沒有錯誤。
- 失敗 - 聯絡人因資源組態問題而失敗。
- AWS_FAILED - 聯絡失敗，因為 AWS Ground Station 服務發生問題。
- 取消 - 聯絡人正在取消。
- AWS_CANCELLED - AWS Ground Station 服務已取消聯絡人。天線或網站維護，以及暫時性漂移是可能發生這種情況的範例。
- 已取消 - 聯絡人已由您取消。

使用 AWS Ground Station 數位分身功能

的數位分身功能 AWS Ground Station 為您提供環境，您可以在其中測試和整合衛星任務管理和命令和控制軟體。數位分身功能可讓您測試排程、驗證組態和適當的錯誤處理，而無需使用生產天線容量。測試與數位分身功能的 AWS Ground Station 整合可讓您對系統能夠順暢地管理衛星操作更具信心。它還可讓您測試 AWS Ground Station APIs 而無需使用生產容量或需要頻譜授權。

若要開始使用，請遵循 [加入衛星](#)，請求加入數位分身功能。一旦您的衛星加入數位分身功能，您就可以針對數位分身地面站點排程聯絡。您可以透過 AWS SDK [ListGroundStations](#) 回應擷取您有權存取的地面工作站清單。數位分身地面站是 中列出的地面站的確切副本 [AWS Ground Station 位置](#)，字首為「數位分身」的地面站名稱。這包括其天線功能和中繼資料，包括但不限於網站遮罩和實際 GPS 座標。目前，數位分身功能不支援 中所述的資料交付 [使用資料流程](#)。

加入後，數位分身功能會發出與生產服務相同的 Amazon EventBridge 事件和 API 回應，如 中所述 [AWS Ground Station 使用 事件自動化](#)。這些事件可讓您微調組態和資料流程端點群組。

了解使用 監控 AWS Ground Station

監控是維護 AWS Ground Station 可靠性、可用性和效能的重要環節。AWS 提供下列監控工具來監看 AWS Ground Station、回報錯誤，並適時採取自動動作。

- Amazon EventBridge Events 提供近乎即時的系統事件串流，描述 AWS 資源的變更。EventBridge Events 可啟用自動事件驅動運算，因為您可以撰寫規則來監控特定事件，並在發生這些事件時觸發 AWS 其他服務中的自動動作。如需 EventBridge Events 的詳細資訊，請參閱 [《Amazon EventBridge Events 使用者指南》](#)。
- AWS CloudTrail 會擷取由您的帳戶發出或代表 AWS 您的帳戶發出的 API 呼叫和相關事件，並將日誌檔案交付至您指定的 Amazon S3 儲存貯體。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 地址，以及呼叫的時間。如需的詳細資訊 AWS CloudTrail，請參閱 [AWS CloudTrail 《使用者指南》](#)。
- Amazon CloudWatch Metrics 會在使用時擷取排程聯絡人的指標 AWS Ground Station。CloudWatch 指標可讓您根據頻道、極化和衛星 ID 來分析資料，以識別聯絡人中的訊號強度和錯誤。如需詳細資訊，請參閱 [使用 Amazon CloudWatch 指標](#)。
- [AWS 使用者通知](#) 可用來設定交付管道，以取得 AWS Ground Station 事件的通知。當事件符合您指定的規則時，便會收到通知。您可以透過多個管道接收事件的通知，包括電子郵件、[聊天應用程式中的 Amazon Q Developer](#) 聊天通知或 [AWS Console Mobile Application](#) 推送通知。您也可以可以在 AWS 主控台 [通知中心](#) 查看通知。使用者通知 支援彙總，這可以減少您在特定事件期間收到的通知數量。

使用下列主題來監控 AWS Ground Station。

主題

- [AWS Ground Station 使用 事件自動化](#)
- [使用 記錄 AWS Ground Station API 呼叫 AWS CloudTrail](#)
- [使用 Amazon CloudWatch 檢視指標](#)

AWS Ground Station 使用 事件自動化

Note

本文件全文使用「事件」一詞。CloudWatch Events 和 EventBridge 是相同的基礎服務和 API。您可以使用任一服務來建置符合傳入事件並將其路由至目標以進行處理的規則。

事件可讓您自動化 AWS 服務，並自動回應系統事件，例如應用程式可用性問題或資源變更。來自 AWS 服務的事件會以近乎即時的方式交付。您可編寫簡單的規則，來指示您在意的事件，以及當事件符合規則時所要自動執行的動作。可自動觸發的一些動作包括下列項目：

- 叫用 AWS Lambda 函數
- 調用 Amazon EC2 執行命令
- 將事件轉傳至 Amazon Kinesis Data Streams
- 啟用 AWS Step Functions 狀態機器
- 通知 Amazon SNS 主題或 Amazon SQS 佇列

搭配使用事件的一些範例 AWS Ground Station 包括：

- 叫用 Lambda 函數，根據事件狀態自動啟動和停止 Amazon EC2 執行個體。
- 每當聯絡人變更狀態時，發佈至 Amazon SNS 主題。這些主題可設定為在聯絡開始或結束時寄出電子郵件通知。

如需詳細資訊，請參閱 [《Amazon EventBridge Events 使用者指南》](#)。

AWS Ground Station 事件類型

Note

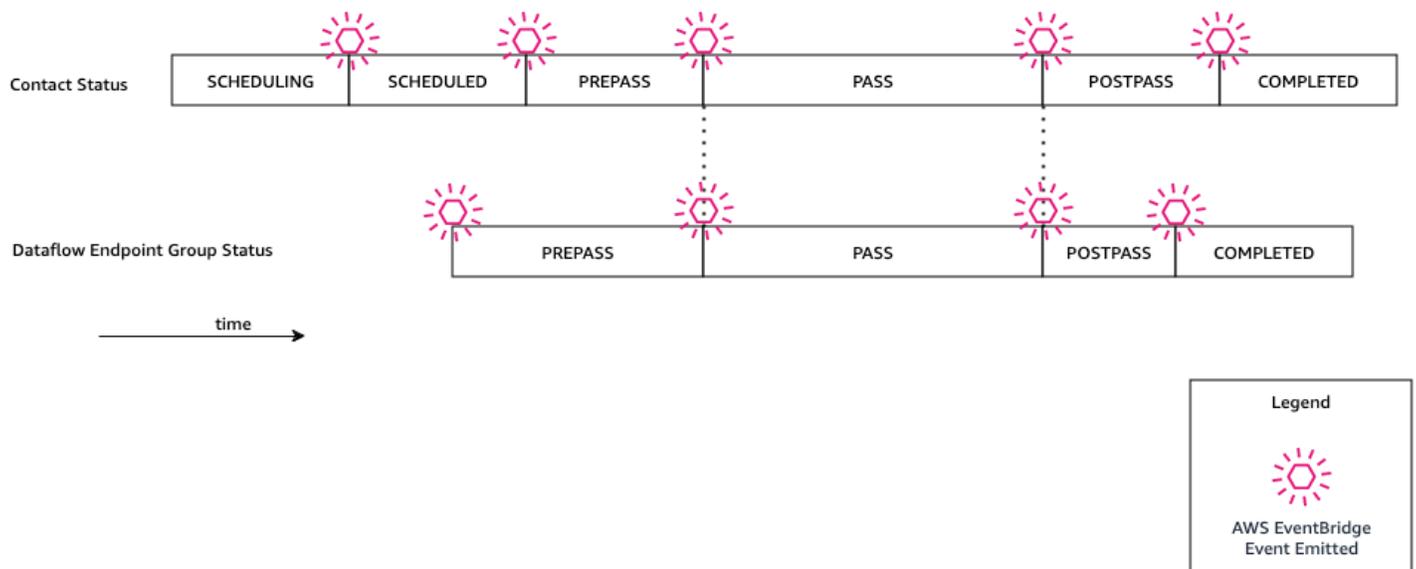
AWS Ground Station 產生的所有事件都有 "aws.groundstation" 做為 "source" 的值。

AWS Ground Station 會發出與狀態變更相關的事件，以支援您自訂自動化的能力。目前，AWS Ground Station 支援聯絡狀態變更事件、資料流程端點群組變更事件和暫時性狀態變更事件。下列各節提供每種類型的詳細資訊。

聯絡事件時間表

AWS Ground Station 當您的聯絡人變更狀態時，會發出事件。如需這些狀態變更以及狀態本身意義的詳細資訊，請參閱 [了解聯絡生命週期](#)。聯絡人中使用的任何資料流程端點群組都有一組獨立的事件，也會發出。在相同的時間範圍內，我們也會為您的資料流程端點群組發出事件。當您設定任務描述檔和資料流程端點群組時，您可以設定傳遞前和傳遞後事件的精確時間。

下圖顯示針對名目聯絡人及其相關聯資料流程端點群組發出的狀態和事件。



Ground Station 聯絡狀態變更

如果您想要在即將到來的聯絡變更狀態時執行特定動作，您可以設定規則來自動化此動作。如果您要接收聯絡狀態變更的相關通知，這種方式就非常有助。如果您想要在收到這些事件時變更，您可以修改任務設定檔的 [contactPrePassDurationSeconds](#) 和 [contactPostPassDurationSeconds](#)。事件會重送至聯絡排程起始的區域。

下面提供範例事件。

```
{
  "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"
  }
}

```

中contactStatus定義了 的可能值[the section called “AWS Ground Station 聯絡狀態”](#)。

Ground Station 資料流程端點群組狀態變更

如果您要在使用資料流程端點群組來接收資料時執行某的動作，您可以設定 規則以自動執行此動作。這樣您就可以在回應資料流程端點群組狀態變更時執行不同的動作。如果您想要在收到這些事件時變更，請使用具有不同 [contactPrePassDurationSeconds](#) 和 [contactPostPassDurationSeconds](#) 的資料流程端點群組。此事件將傳送至資料流程端點群組的區域。

以下提供範例。

```

{
  "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"
  }
}

```

```

    }
  }
}

```

`dataflowEndpointGroupState` 可能的狀態包括 PREPASS、PASS、POSTPASS 和 COMPLETED。

Ephemeris 事件

Ground Station Ephemeris 狀態變更

如果您想要在暫時性變更狀態時執行動作，您可以設定規則來自動化此動作。這可讓您執行不同的動作，以回應暫時性變化狀態。例如，您可以在 `ephemeris` 已完成驗證且現在為 `時執行 動作ENABLED`。此事件的通知會在上傳暫時性事件時傳送至 區域。

以下提供範例。

```

{
  "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"
  }
}

```

的可能狀態 `ephemerisStatus` 包括 ENABLED、VALIDATING、INVALID、ERROR、DISABLED、EXPIRED

使用記錄 AWS Ground Station API 呼叫 AWS CloudTrail

AWS Ground Station 已與服務整合 AWS CloudTrail，此服務提供由使用者、角色或 AWS 服務在其中採取的動作記錄 AWS Ground Station。CloudTrail 會將 AWS Ground Station 的所有 API 呼叫擷取為事件。擷取的呼叫包括從 AWS Ground Station 主控台的呼叫，以及對 AWS Ground Station API 操作的程式碼呼叫。如果您建立線索，則可以將 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括的事件 AWS Ground Station。即使您未設定追蹤，依然可以透過 CloudTrail 主控台的事件歷史記錄檢視最新事件。使用 CloudTrail 收集的資訊，您可以判斷提出的請求 AWS Ground Station、提出請求的 IP 地址、提出請求的人員、提出請求的時間，以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱 [AWS CloudTrail 《使用者指南》](#)。

AWS Ground Station CloudTrail 中的資訊

當您建立 AWS 帳戶時，會在您的帳戶上啟用 CloudTrail。當活動在中發生時 AWS Ground Station，該活動會記錄在 CloudTrail 事件中，以及事件歷史記錄中的其他服務 AWS 事件。您可以在 AWS 帳戶中檢視、搜尋和下載最近的事件。如需詳細資訊，請參閱《使用 CloudTrail 事件歷史記錄檢視事件》<https://docs.aws.amazon.com/awsccloudtrail/latest/userguide/view-cloudtrail-events.html>。

若要持續記錄您 AWS 帳戶中的事件，包括的事件 AWS Ground Station，請建立追蹤。線索能讓 CloudTrail 將日誌檔案交付至 Amazon S3 儲存貯體。根據預設，當您在主控台建立追蹤記錄時，追蹤記錄會套用到所有 AWS 區域。線索會記錄 AWS 分割區中所有區域的事件，並將日誌檔案交付至您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析和處理 CloudTrail 日誌中所收集的事件資料。如需詳細資訊，請參閱下列內容：

- [建立追蹤的概觀](#)
- [CloudTrail 支援的服務和整合](#)
- [設定 CloudTrail 的 Amazon SNS 通知](#)
- [從多個區域接收 CloudTrail 日誌檔案](#)，以及 [從多個帳戶接收 CloudTrail 日誌檔案](#)

CloudTrail 會記錄所有 AWS Ground Station 動作，並記錄在 [AWS Ground Station API 參考](#)中。例如，對 ReserveContact、CancelContact 和 ListConfigs 動作發出的呼叫會在 CloudTrail 記錄檔案中產生專案。

每一筆事件或日誌專案都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 請求是使用根還是 AWS Identity and Access Management (IAM) 使用者登入資料提出。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。

- 請求是否由其他 AWS 服務提出。

如需詳細資訊，請參閱 [CloudTrail userIdentity 元素](#)。

了解 AWS Ground Station 日誌檔案項目

追蹤是一種組態，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一或多個日誌專案。一個事件為任何來源提出的單一請求，並包含請求動作、請求的日期和時間、請求參數等資訊。CloudTrail 日誌檔並非依公有 API 呼叫的堆疊追蹤排序，因此不會以任何特定順序出現。

以下範例顯示的是展示 ReserveContact 動作的 CloudTrail 日誌項目。

範例：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"
}
```

使用 Amazon CloudWatch 檢視指標

在聯絡期間，AWS Ground Station 會自動擷取資料並將其傳送至 CloudWatch 進行分析。您可以在 Amazon CloudWatch 主控台中檢視您的資料。如需存取和 CloudWatch 指標的詳細資訊，請參閱[使用 Amazon CloudWatch 指標](#)。

AWS Ground Station 指標和維度

目前提供哪些指標？

下列指標可從取得 AWS Ground Station。

Note

發出的特定指標取決於正在使用 AWS Ground Station 的功能。根據您的組態，僅可能會發出以下指標的子集。

指標	指標維度	描述
AzimuthAngle	SatelliteId	天線的方位角。 真北是 0 度，而東是 90 度。 單位：度
BitErrorRate	頻道、偏振、SatelliteId	指定位元傳輸次數中位元的錯誤率。位元錯誤是由雜訊、失真或干擾所導致 單位：每單位時間的位元錯誤
BlockErrorRate	頻道、偏振、SatelliteId	指定已接收區塊數中的區塊錯誤率。區塊錯誤是由干擾所導致。 單位：錯誤區塊 / 區塊總數
CarrierFrequencyRecovery_Cn0	類別、Config、SatelliteId	每個單位頻寬的載波雜訊密度比率。 單位：decibel-Hertz (dB-Hz)
CarrierFrequencyRecovery_Locked	類別、Config、SatelliteId	當解調器電信業者頻率復原迴圈鎖定時，將設定為 1，並在解除鎖定時設定為 0。

指標	指標維度	描述
		單位：無單位
CarrierFrequencyRecovery_OffsetFrequency_Hz	類別、Config、Satelliteld	估計訊號中心與理想中心頻率之間的位移。這是因為都卜勒偏移和本機振盪器在太空船和天線系統之間偏移所致。 單位：hertz (Hz)
ElevationAngle	Satelliteld	天線的高度角度。地平線為 0 度，而小數為 90 度。 單位：度
Es/N0	頻道、偏振、Satelliteld	每個符號的能量與雜訊功率光譜密度的比率。 單位：分貝 (dB)
ReceivedPower	極化、Satelliteld	解調器/解碼器中測量得到的訊號強度。 單位：相對於毫瓦 (dBm) 的分貝
SymbolTimingRecovery_ErrorVectorMagnitude	類別、Config、Satelliteld	收到的符號和理想星座點之間的錯誤向量大小。 單位：百分比

指標	指標維度	描述
SymbolTimingRecovery_Locked	類別、Config、SatelliteId	當解調器符號計時復原迴圈鎖定時，設定為 1，解除鎖定時設定為 0 單位：無單位
SymbolTimingRecovery_OffsetSymbolRate	類別、Config、SatelliteId	估計符號率與理想訊號符號率之間的位移。這是因為都卜勒偏移和本機振盪器在太空船和天線系統之間偏移所致。 單位：符號/秒

使用哪些維度 AWS Ground Station ？

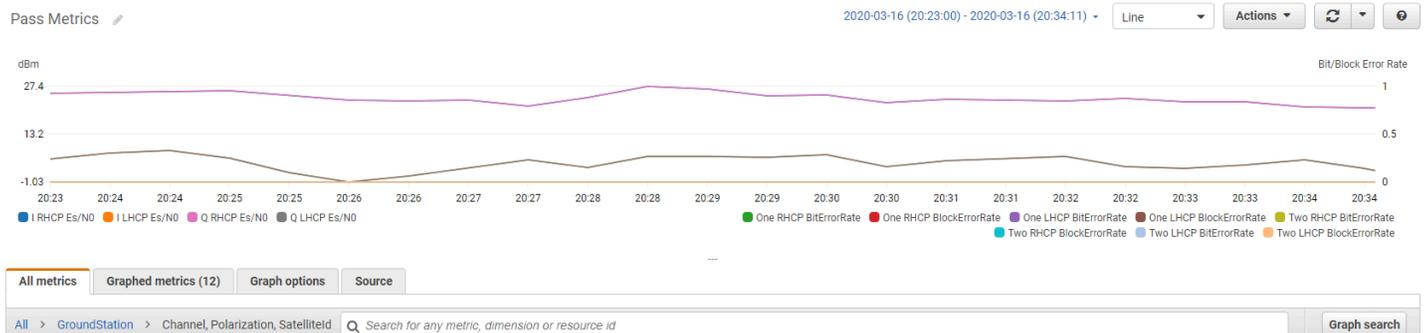
您可以使用下列維度來篩選 AWS Ground Station 資料。

維度	描述
Category	解調或解碼。
Channel	每個聯絡的頻道包含一、二、I (同相) 和 Q (正交)。
Config	天線下行解調解碼組態 arn。
Polarization	每個聯絡的極化包含 LHCP (左側圓極化) 或 RHCP (右側圓極化)。
SatelliteId	衛星 ID 包含聯絡衛星的 ARN。

檢視指標

檢視圖形化指標時，請務必注意彙總視窗會決定如何顯示您的指標。在收到資料之後，聯絡中的每個指標都會持續在 3 小時期間內顯示為每秒資料。您的資料將由 CloudWatch 指標彙總為經過 3 小時期間之後每分鐘的資料。如果您需要檢視每秒資料量值的指標，建議您在收到資料後 3 小時內檢視資料，或將其保留在 CloudWatch 指標之外。如需 CloudWatch 保留的詳細資訊，請參閱 [Amazon CloudWatch 概念 - 指標保留](#)。

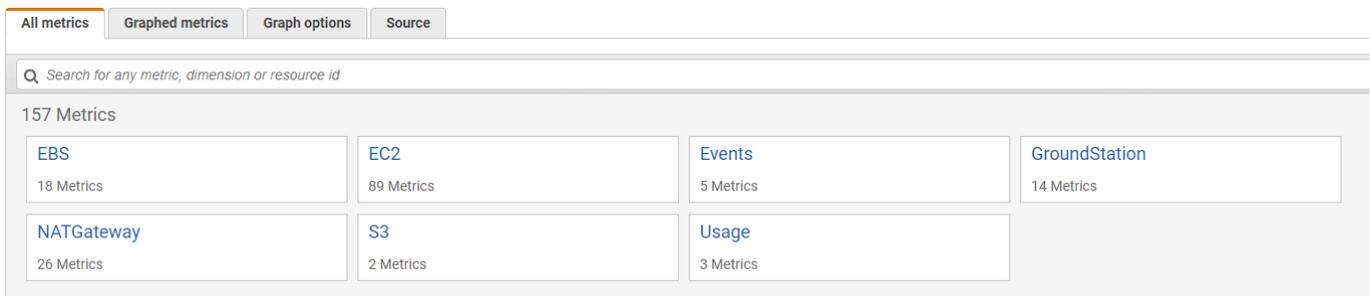
此外，前 60 秒內所擷取的任何資料都不會包含足以產生有意義指標的資訊，而且可能不會顯示。為了檢視有意義的資料，建議您在 60 秒過後再檢視資料。



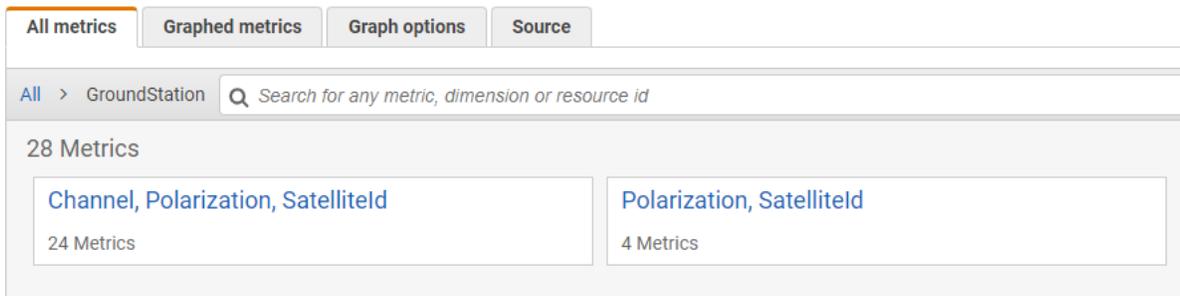
如需在 CloudWatch 中繪製 AWS Ground Station 指標圖形的詳細資訊，請參閱 [繪製指標圖形](#)。

使用主控台檢視指標

1. 開啟 [CloudWatch 主控台](#)。
2. 在導覽窗格中，選擇 Metrics (指標)。
3. 選取 GroundStation 命名空間。



4. 選取所需的指標維度 (例如，頻道、極化、SatelliteId)。



5. All metrics (所有指標) 索引標籤會顯示命名空間中該維度的所有指標。您可以執行下列作業：
 - a. 若要將資料表排序，請使用直欄標題。
 - b. 若要繪製指標圖形，請選取與指標相關聯的核取方塊。若要選取所有指標，請選取資料表標題列中的核取方塊。
 - c. 若要依資源篩選，請選擇資源 ID，然後選擇 Add to search (新增至搜尋)。
 - d. 若要依指標篩選，請選擇指標名稱，然後選擇 Add to search (新增至搜尋)。

使用 檢視指標 AWS CLI

1. 確保 AWS CLI 已安裝。如需安裝的相關資訊 AWS CLI，請參閱[安裝 AWS CLI 第 2 版](#)。
2. 使用 CloudWatch CLI 的 [get-metric-data](#) 方法來產生可修改的檔案，以指定您感興趣的指標，然後用來查詢這些指標。

若要執行此操作，請執行下列動作：`aws cloudwatch get-metric-data --generate-cli-skeleton`。這將產生類似如下的輸出：

```
{
  "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. 透過執行 列出可用的 CloudWatch 指標 `aws cloudwatch list-metrics`。

如果您最近使用過 AWS Ground Station，方法應該會傳回包含下列項目的輸出：

```

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

```

...

Note

由於 CloudWatch 的限制，如果您自上次使用以來已超過 2 週 AWS Ground Station，則您需要手動檢查 [可用指標的資料表](#)，以在指標命名空間中尋找 AWS/GroundStation 指標名稱和維度。如需 CloudWatch 限制的詳細資訊，請參閱：[檢視可用的指標](#)

4. 修改您在步驟 2 中建立的 JSON 檔案，以符合步驟 3 的必要值，例如 SatelliteId 和 Polarization 指標。此外，請務必更新 StartTime、和 EndTime 值，以符合您的聯絡人。例如：

```
{
  "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 根據指標，每 1 到 60 秒發佈一次指標。如果 Period 欄位的值小於指標的發佈期間，則不會傳回指標。

5. `aws cloudwatch get-metric-data` 使用先前步驟中建立的組態檔案執行。以下提供範例。

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

指標會與您聯絡中的時間戳記一起提供。以下提供 AWS Ground Station 指標輸出範例。

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

中的安全性 AWS Ground Station

的雲端安全 AWS 是最高優先順序。身為 AWS 客戶，您將受益於資料中心和網路架構，該架構旨在滿足最安全敏感組織的需求。AWS 提供安全特定的工具和功能，協助您達成安全目標。這些工具和功能包含網路安全性、組態管理、存取控制和資料安全性。

使用時 AWS Ground Station，建議您遵循業界最佳實務並實作 end-to-end 加密。AWS 提供 API，可讓您整合加密和資料保護。如需 AWS 安全性的詳細資訊，請參閱 [AWS 安全簡介白皮書](#)。

請使用下列主題來了解如何保護您的資源。

主題

- [的 Identity and Access Management AWS Ground Station](#)
- [AWS 的 受管政策 AWS Ground Station](#)
- [使用 Ground Station 的服務連結角色](#)
- [的靜態資料加密 AWS Ground Station](#)
- [傳輸期間的資料加密 AWS Ground Station](#)

的 Identity and Access Management AWS Ground Station

AWS Identity and Access Management (IAM) 是 AWS 服務，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員可控制誰可以進行驗證（登入）和授權（具有許可）來使用 AWS Ground Station 資源。IAM 是您可以免費使用 AWS 服務的。

主題

- [目標對象](#)
- [使用身分驗證](#)
- [使用政策管理存取權](#)
- [AWS Ground Station 如何使用 IAM](#)
- [的身分型政策範例 AWS Ground Station](#)
- [對 AWS Ground Station 身分和存取進行故障診斷](#)

目標對象

您使用 AWS Identity and Access Management (IAM) 的方式會有所不同，取決於您執行的工作 AWS Ground Station。

服務使用者 – 如果您使用 AWS Ground Station 服務來執行任務，您的管理員會為您提供所需的登入資料和許可。當您使用更多 AWS Ground Station 功能來執行工作時，您可能需要額外的許可。了解存取的管理方式可協助您向管理員請求正確的許可。若您無法存取 AWS Ground Station 中的某項功能，請參閱 [對 AWS Ground Station 身分和存取進行故障診斷](#)。

服務管理員 – 如果您負責公司 AWS Ground Station 的資源，您可能擁有的完整存取權 AWS Ground Station。您的任務是判斷服務使用者應存取哪些 AWS Ground Station 功能和資源。接著，您必須將請求提交給您的 IAM 管理員，來變更您服務使用者的許可。檢閱此頁面上的資訊，了解 IAM 的基本概念。若要進一步了解貴公司如何搭配使用 IAM AWS Ground Station，請參閱 [AWS Ground Station 如何使用 IAM](#)。

IAM 管理員：如果您是 IAM 管理員，建議您掌握如何撰寫政策以管理 AWS Ground Station 存取權的詳細資訊。若要檢視您可以在 IAM 中使用的以 AWS Ground Station 身分為基礎的政策範例，請參閱 [的身分型政策範例 AWS Ground Station](#)。

使用身分驗證

身分驗證是您 AWS 使用身分憑證登入的方式。您必須以 AWS 帳戶根使用者身分、IAM 使用者身分或擔任 IAM 角色來驗證（登入 AWS）。

您可以使用透過身分來源提供的憑證，以聯合身分 AWS 身分身分身分身分登入。AWS IAM Identity Center (IAM Identity Center) 使用者、您公司的單一登入身分驗證，以及您的 Google 或 Facebook 登入資料，都是聯合身分的範例。您以聯合身分登入時，您的管理員先前已設定使用 IAM 角色的聯合身分。當您使用聯合 AWS 身分存取時，您會間接擔任角色。

視您的使用者類型而定，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需登入的詳細資訊 AWS，請參閱 AWS 登入《使用者指南》中的 [如何登入您的 AWS 帳戶](#)。

如果您以 AWS 程式設計方式存取，AWS 會提供軟體開發套件 (SDK) 和命令列界面 (CLI)，以使用您的憑證以密碼編譯方式簽署您的請求。如果您不使用 AWS 工具，則必須自行簽署請求。如需使用建議的方法自行簽署請求的詳細資訊，請參閱《IAM 使用者指南》中的 [適用於 API 請求的 AWS Signature 第 4 版](#)。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如，AWS 建議您使用多重要素驗證 (MFA) 來提高帳戶的安全性。如需更多資訊，請參閱《AWS IAM Identity Center 使用者指南》中的[多重要素驗證](#)和《IAM 使用者指南》中的[IAM 中的AWS 多重要素驗證](#)。

AWS 帳戶 根使用者

建立時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取帳戶中的所有 AWS 服務和資源。此身分稱為 AWS 帳戶 Theroot 使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需這些任務的完整清單，了解需以根使用者登入的任務，請參閱 IAM 使用者指南中的[需要根使用者憑證的任務](#)。

聯合身分

根據最佳實務，要求人類使用者，包括需要管理員存取權的使用者，使用身分提供者的聯合 AWS 服務身分來使用臨時憑證來存取。

聯合身分是來自您企業使用者目錄、Web 身分提供者、AWS Directory Service、Identity Center 目錄或任何使用透過身分來源提供的憑證 AWS 服務存取的使用者。當聯合身分存取時 AWS 帳戶，它們會擔任角色，而角色會提供臨時登入資料。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，也可以連接和同步到您自己的身分來源中的一組使用者 AWS 帳戶和群組，以便在所有和應用程式中使用。如需 IAM Identity Center 的詳細資訊，請參閱 AWS IAM Identity Center 使用者指南中的[什麼是 IAM Identity Center ?](#)。

IAM 使用者和群組

[IAM 使用者](#)是中的身分 AWS 帳戶，具有單一人員或應用程式的特定許可。建議您盡可能依賴臨時憑證，而不是擁有建立長期憑證 (例如密碼和存取金鑰) 的 IAM 使用者。但是如果特定使用案例需要擁有長期憑證的 IAM 使用者，建議您輪換存取金鑰。如需更多資訊，請參閱 [IAM 使用者指南](#)中的為需要長期憑證的使用案例定期輪換存取金鑰。

[IAM 群組](#)是一種指定 IAM 使用者集合的身分。您無法以群組身分簽署。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有一個名為 IAMAdmins 的群組，並給予該群組管理 IAM 資源的許可。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供臨時憑證。如需更多資訊，請參閱《IAM 使用者指南》中的[IAM 使用者的使用案例](#)。

IAM 角色

IAM 角色是中具有特定許可 AWS 帳戶 的身分。它類似 IAM 使用者，但不與特定的人員相關聯。若要暫時在中擔任 IAM 角色 AWS Management Console，您可以從[使用者切換至 IAM 角色（主控台）](#)。您可以透過呼叫 AWS CLI 或 AWS API 操作或使用自訂 URL 來擔任角色。如需使用角色的方法詳細資訊，請參閱《IAM 使用者指南》中的[擔任角色的方法](#)。

使用臨時憑證的 IAM 角色在下列情況中非常有用：

- **聯合身分使用者存取** — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需有關聯合角色的相關資訊，請參閱《[IAM 使用者指南](#)》中的為第三方身分提供者 (聯合) 建立角色。如果您使用 IAM Identity Center，則需要設定許可集。為控制身分驗證後可以存取的內容，IAM Identity Center 將許可集與 IAM 中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的[許可集](#)。
- **暫時 IAM 使用者許可** – IAM 使用者或角色可以擔任 IAM 角色來暫時針對特定任務採用不同的許可。
- **跨帳戶存取權**：您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的主體) 存取您帳戶的資源。角色是授予跨帳戶存取權的主要方式。不過，對於某些 AWS 服務，您可以將政策直接連接到資源 (而不是使用角色做為代理)。如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的[IAM 中的跨帳戶資源存取](#)。
- **跨服務存取** – 有些 AWS 服務 使用其他 中的功能 AWS 服務。例如，當您在服務中進行呼叫時，該服務通常會在 Amazon EC2 中執行應用程式或將物件儲存在 Amazon Simple Storage Service (Amazon S3) 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
- **轉送存取工作階段 (FAS)** – 當您使用 IAM 使用者或角色在其中執行動作時 AWS，您被視為委託人。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 使用呼叫的委託人許可 AWS 服務，結合 AWS 服務 請求向下游服務提出請求。只有當服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會提出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱《[轉發存取工作階段](#)》。
- **服務角色** – 服務角色是服務擔任的 [IAM 角色](#)，可代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱《IAM 使用者指南》中的[建立角色以委派許可權給 AWS 服務](#)。
- **服務連結角色** – 服務連結角色是一種連結至 的服務角色類型 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 中 AWS 帳戶，並由服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

- 在 Amazon EC2 上執行的應用程式 – 您可以使用 IAM 角色來管理在 EC2 執行個體上執行之應用程式的臨時登入資料，以及提出 AWS CLI 或 AWS API 請求。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體，並將其提供給其所有應用程式，您可以建立連接至執行個體的執行個體描述檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得臨時憑證。如需詳細資訊，請參閱《IAM 使用者指南》中的[使用 IAM 角色來授予許可權給 Amazon EC2 執行個體上執行的應用程式](#)。

使用政策管理存取權

您可以透過建立政策並將其連接到身分或資源 AWS 來控制 AWS 中的存取。政策是中的物件，當與身分或資源建立關聯時，AWS 會定義其許可。當委託人（使用者、根使用者或角色工作階段）發出請求時，會 AWS 評估這些政策。政策中的許可決定是否允許或拒絕請求。大多數政策會以 JSON 文件 AWS 的形式存放在中。如需 JSON 政策文件結構和內容的詳細資訊，請參閱 IAM 使用者指南中的[JSON 政策概觀](#)。

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

預設情況下，使用者和角色沒有許可。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

IAM 政策定義該動作的許可，無論您使用何種方法來執行操作。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該政策的使用者可以從 AWS Management Console AWS CLI、或 AWS API 取得角色資訊。

身分型政策

身分型政策是可以附加到身分（例如 IAM 使用者、使用者群組或角色）的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的[透過客戶管理政策定義自訂 IAM 許可](#)。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管政策是獨立的政策，您可以連接到中的多個使用者、群組和角色 AWS 帳戶。受管政策包括 AWS 受管政策和客戶受管政策。如需了解如何在受管政策及內嵌政策之間選擇，請參閱《IAM 使用者指南》中的[在受管政策和內嵌政策間選擇](#)。

資源型政策

資源型政策是連接到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源

的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中[指定主體](#)。委託人可以包括帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

資源型政策是位於該服務中的內嵌政策。您無法在資源型政策中使用來自 IAM 的 AWS 受管政策。

存取控制清單 (ACL)

存取控制清單 (ACL) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

Amazon S3 AWS WAF 和 Amazon VPC 是支援 ACLs 的服務範例。如需進一步了解 ACL，請參閱 Amazon Simple Storage Service 開發人員指南中的[存取控制清單 \(ACL\) 概觀](#)。

其他政策類型

AWS 支援其他較不常見的政策類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- 許可界限 – 許可範圍是一種進階功能，可供您設定身分型政策能授予 IAM 實體 (IAM 使用者或角色) 的最大許可。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 Principal 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需許可界限的詳細資訊，請參閱 IAM 使用者指南中的[IAM 實體許可界限](#)。
- 服務控制政策 (SCPs) – SCPs 是 JSON 政策，可指定 in. 中組織或組織單位 (OU) 的最大許可 AWS Organizations。AWS Organizations 是一種用於分組和集中管理您企業擁有 AWS 帳戶之多個的服務。若您啟用組織中的所有功能，您可以將服務控制政策 (SCP) 套用到任何或所有帳戶。SCP 會限制成員帳戶中實體的許可，包括每個實體 AWS 帳戶根使用者。如需 Organizations 和 SCP 的詳細資訊，請參閱《AWS Organizations 使用者指南》中的[服務控制政策](#)。
- 資源控制政策 (RCP) - RCP 是 JSON 政策，可用來設定您帳戶中資源的可用許可上限，採取這種方式就不需要更新附加至您所擁有的每個資源的 IAM 政策。RCP 會限制成員帳戶中資源的許可，並可能影響身分的有效許可，包括 AWS 帳戶根使用者，無論它們是否屬於您的組織。如需 Organizations 和 RCPs 的詳細資訊，包括 AWS 服務支援 RCPs 清單，請參閱 AWS Organizations 《使用者指南》中的[資源控制政策 \(RCPs\)](#)。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過撰寫程式的方式建立角色或聯合使用者的暫時工作階段時，做為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需詳細資訊，請參閱 IAM 使用者指南中的[工作階段政策](#)。

多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。若要了解如何 AWS 在涉及多種政策類型時決定是否允許請求，請參閱《IAM 使用者指南》中的[政策評估邏輯](#)。

AWS Ground Station 如何使用 IAM

在您使用 IAM 管理對 的存取之前 AWS Ground Station，請先了解哪些 IAM 功能可與 搭配使用 AWS Ground Station。

您可以搭配 使用的 IAM 功能 AWS Ground Station

IAM 功能	AWS Ground Station 支援
身分型政策	是
資源型政策	否
政策動作	是
政策資源	是
政策條件索引鍵 (服務特定)	是
ACL	否
ABAC (政策中的標籤)	是
暫時性憑證	是
主體許可	是
服務角色	否
服務連結角色	是

若要全面了解 AWS Ground Station 和其他 AWS 服務如何與大多數 IAM 功能搭配使用，請參閱《IAM 使用者指南》中的與 IAM [AWS 搭配使用的 服務](#)。

的身分型政策 AWS Ground Station

支援身分型政策：是

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的[透過客戶管理政策定義自訂 IAM 許可](#)。

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。如要了解您在 JSON 政策中使用的所有元素，請參閱《IAM 使用者指南》中的[IAM JSON 政策元素參考](#)。

的身分型政策範例 AWS Ground Station

若要檢視 AWS Ground Station 身分型政策的範例，請參閱[的身分型政策範例 AWS Ground Station](#)。

內的資源型政策 AWS Ground Station

支援資源型政策：否

資源型政策是附加到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中[指定主體](#)。委託人可以包括帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

如需啟用跨帳戶存取權，您可以指定在其他帳戶內的所有帳戶或 IAM 實體，做為資源型政策的主體。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當委託人和資源位於不同位置時 AWS 帳戶，信任帳戶中的 IAM 管理員也必須授予委託人實體 (使用者或角色) 存取資源的許可。其透過將身分型政策連接到實體來授與許可。不過，如果資源型政策會為相同帳戶中的主體授予存取，這時就不需要額外的身分型政策。如需詳細資訊，請參閱《IAM 使用者指南》中的[IAM 中的快帳戶資源存取](#)。

的政策動作 AWS Ground Station

支援政策動作：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON 政策的 Action 元素描述您可以用來允許或拒絕政策中存取的動作。政策動作通常具有與相關聯 AWS API 操作相同的名稱。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

若要查看 AWS Ground Station 動作清單，請參閱《服務授權參考》中的 [定義的動作 AWS Ground Station](#)。

中的政策動作在動作之前 AWS Ground Station 使用以下字首：

```
groundstation
```

若要在單一陳述式中指定多個動作，請用逗號分隔。

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

若要檢視 AWS Ground Station 身分型政策的範例，請參閱 [的身分型政策範例 AWS Ground Station](#)。

的政策資源 AWS Ground Station

支援政策資源：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Resource JSON 政策元素可指定要套用動作的物件。陳述式必須包含 Resource 或 NotResource 元素。最佳實務是使用其 [Amazon Resource Name \(ARN\)](#) 來指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出操作)，請使用萬用字元 (*) 來表示陳述式適用於所有資源。

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

若要查看 AWS Ground Station 資源類型及其 ARNs，請參閱《服務授權參考》中的 [定義的資源 AWS Ground Station](#)。若要了解您可以使用哪些動作指定每個資源的 ARN，請參閱 [AWS Ground Station 定義的動作](#)。

若要檢視 AWS Ground Station 身分型政策的範例，請參閱 [的身分型政策範例 AWS Ground Station](#)。

的政策條件索引鍵 AWS Ground Station

支援服務特定政策條件金鑰：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。您可以建立使用 [條件運算子](#) 的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。

若您在陳述式中指定多個 Condition 元素，或是在單一 Condition 元素中指定多個索引鍵，AWS 會使用邏輯 AND 操作評估他們。如果您為單一條件索引鍵指定多個值，會使用邏輯 OR 操作 AWS 評估條件。必須符合所有條件，才會授與陳述式的許可。

您也可以指定條件時使用預留位置變數。例如，您可以只在使用者使用其 IAM 使用者名稱標記時，將存取資源的許可授予該 IAM 使用者。如需更多資訊，請參閱 IAM 使用者指南中的 [IAM 政策元素：變數和標籤](#)。

AWS 支援全域條件金鑰和服務特定條件金鑰。若要查看所有 AWS 全域條件索引鍵，請參閱《IAM 使用者指南》中的 [AWS 全域條件內容索引鍵](#)。

若要查看 AWS Ground Station 條件索引鍵的清單，請參閱《服務授權參考》中的 [的條件索引鍵 AWS Ground Station](#)。若要了解您可以使用條件索引鍵的動作和資源，請參閱 [定義的動作 AWS Ground Station](#)。

若要檢視 AWS Ground Station 身分型政策的範例，請參閱 [的身分型政策範例 AWS Ground Station](#)。

中的 ACLs AWS Ground Station

支援 ACL：否

存取控制清單 (ACL) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

ABAC 搭配 AWS Ground Station

支援 ABAC (政策中的標籤)：是

屬性型存取控制 (ABAC) 是一種授權策略，可根據屬性來定義許可。在中 AWS，這些屬性稱為標籤。您可以將標籤連接至 IAM 實體（使用者或角色）和許多 AWS 資源。為實體和資源加上標籤是 ABAC 的第一步。您接著要設計 ABAC 政策，允許在主體的標籤與其嘗試存取的資源標籤相符時操作。

ABAC 在成長快速的環境中相當有幫助，並能在政策管理變得繁瑣時提供協助。

如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，在政策的 [條件元素](#) 中，提供標籤資訊。

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。

如需 ABAC 的詳細資訊，請參閱《IAM 使用者指南》中的 [使用 ABAC 授權定義許可](#)。如要查看含有設定 ABAC 步驟的教學課程，請參閱 IAM 使用者指南中的 [使用屬性型存取控制 \(ABAC\)](#)。

搭配 使用臨時登入資料 AWS Ground Station

支援臨時憑證：是

當您使用臨時登入資料登入時，有些 AWS 服務 無法運作。如需詳細資訊，包括哪些 AWS 服務 使用臨時登入資料，請參閱 [《AWS 服務 IAM 使用者指南》中的 使用 IAM](#)。

如果您 AWS Management Console 使用使用者名稱和密碼以外的任何方法登入，則表示您使用的是臨時登入資料。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取時，該程序會自動建立臨時登入資料。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需切換角色的詳細資訊，請參閱《IAM 使用者指南》中的 [從使用者切換至 IAM 角色 \(主控台\)](#)。

您可以使用 AWS CLI 或 AWS API 手動建立臨時登入資料。然後，您可以使用這些臨時登入資料來存取 AWS。AWS 建議您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱 [IAM 中的暫時性安全憑證](#)。

的跨服務主體許可 AWS Ground Station

支援轉寄存取工作階段 (FAS)：是

當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為委託人。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 使用呼叫的委託人許可 AWS 服務，結合 AWS 服務 請求向下游服務提出請求。只有當服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會提出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的策略詳細資訊，請參閱 [轉發存取工作階段](#)。

AWS Ground Station的服務角色

支援服務角色：否

服務角色是服務擔任的 [IAM 角色](#)，可代您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱《IAM 使用者指南》中的[建立角色以委派許可權給 AWS 服務](#)。

Warning

變更服務角色的許可可能會中斷 AWS Ground Station 功能。只有在 AWS Ground Station 提供指引時，才能編輯服務角色。

的服務連結角色 AWS Ground Station

支援服務連結角色：是

服務連結角色是連結至的一種服務角色 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 AWS 帳戶，並由服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

如需建立或管理服务連結角色的詳細資訊，請參閱[可搭配 IAM 運作的AWS 服務](#)。在表格中尋找服務，其中包含服務連結角色欄中的 Yes。選擇是連結，以檢視該服務的服務連結角色文件。

的身分型政策範例 AWS Ground Station

根據預設，使用者和角色不具備建立或修改 AWS Ground Station 資源的權限。他們也無法使用 AWS Management Console、AWS Command Line Interface (AWS CLI) 或 AWS API 來執行任務。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

如需了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的[建立 IAM 政策 \(主控台\)](#)。

如需定義的動作和資源類型的詳細資訊 AWS Ground Station，包括每種資源類型的 ARNs 格式，請參閱《服務授權參考》中的[的動作、資源和條件索引鍵 AWS Ground Station](#)。

主題

- [政策最佳實務](#)

- [使用 AWS Ground Station 主控台](#)
- [允許使用者檢視他們自己的許可](#)

政策最佳實務

以身分為基礎的政策會判斷您帳戶中的某個人員是否可以建立、存取或刪除 AWS Ground Station 資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用將許可授予許多常見使用案例的 AWS 受管政策。它們可在您的 中使用 AWS 帳戶。我們建議您定義特定於使用案例 AWS 的客戶受管政策，以進一步減少許可。如需更多資訊，請參閱 IAM 使用者指南中的 [AWS 受管政策](#) 或 [任務職能的 AWS 受管政策](#)。
- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱 IAM 使用者指南中的 [IAM 中的政策和許可](#)。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。如果透過特定 使用服務動作 AWS 服務，您也可以使用條件來授予存取，例如 AWS CloudFormation。如需詳細資訊，請參閱 IAM 使用者指南中的 [IAM JSON 政策元素：條件](#)。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您撰寫安全且實用的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的 [使用 IAM Access Analyzer 驗證政策](#)。
- 需要多重要素驗證 (MFA) – 如果您的案例需要 IAM 使用者或 中的根使用者 AWS 帳戶，請開啟 MFA 以提高安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需詳細資訊，請參閱《IAM 使用者指南》 https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_configure-api-require.html 中的透過 MFA 的安全 API 存取。

如需 IAM 中最佳實務的相關資訊，請參閱 IAM 使用者指南中的 [IAM 安全最佳實務](#)。

使用 AWS Ground Station 主控台

若要存取 AWS Ground Station 主控台，您必須擁有一組最低的許可。這些許可必須允許您列出和檢視 中 AWS Ground Station 資源的詳細資訊 AWS 帳戶。如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (使用者或角色) 而言，主控台就無法如預期運作。

對於僅呼叫 AWS CLI 或 AWS API 的使用者，您不需要允許最低主控台許可。反之，只需允許存取符合他們嘗試執行之 API 操作的動作就可以了。

為了確保使用者和角色仍然可以使用 AWS Ground Station 主控台，也請將 AWS Ground Station *ConsoleAccess* 或 *ReadOnly* AWS 受管政策連接到實體。如需詳細資訊，請參閱《IAM 使用者指南》中的[新增許可到使用者](#)。

允許使用者檢視他們自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視附加到他們使用者身分的內嵌及受管政策。此政策包含在主控台上完成此動作的許可，或使用 AWS CLI 或 AWS API 以程式設計方式完成此動作的許可。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "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": "*"
    }
  ]
}
```

```
]
}
```

對 AWS Ground Station 身分和存取進行故障診斷

使用以下資訊來協助您診斷和修正使用 AWS Ground Station 和 IAM 時可能遇到的常見問題。

主題

- [我未獲授權在 中執行動作 AWS Ground Station](#)
- [我未獲得執行 iam:PassRole 的授權](#)
- [我想要允許 以外的人員 AWS 帳戶 存取我的 AWS Ground Station 資源](#)

我未獲授權在 中執行動作 AWS Ground Station

如果您收到錯誤，告知您未獲授權執行動作，您的政策必須更新，允許您執行動作。

下列範例錯誤會在mateojackson IAM 使用者嘗試使用主控台檢視一個虛構 *my-example-widget* 資源的詳細資訊，但卻無虛構 `groundstation:GetWidget` 許可時發生。

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

在此情況下，必須更新 mateojackson 使用者的政策，允許使用 `groundstation:GetWidget` 動作存取 *my-example-widget* 資源。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我未獲得執行 iam:PassRole 的授權

如果您收到錯誤，告知您未獲授權執行 `iam:PassRole` 動作，您的政策必須更新，允許您將角色傳遞給 AWS Ground Station。

有些 AWS 服務可讓您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

名為 marymajor 的 IAM 使用者嘗試使用主控台在 AWS Ground Station 中執行動作時，發生下列範例錯誤。但是，動作要求服務具備服務角色授予的許可。Mary 沒有將角色傳遞至該服務的許可。

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

在這種情況下，Mary 的政策必須更新，允許她執行 iam:PassRole 動作。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我想要允許以外的人員 AWS 帳戶 存取我的 AWS Ground Station 資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

如需進一步了解，請參閱以下內容：

- 若要了解 是否 AWS Ground Station 支援這些功能，請參閱 [AWS Ground Station 如何使用 IAM](#)。
- 若要了解如何 AWS 帳戶 在您擁有的 資源之間提供存取權，請參閱 [《IAM 使用者指南》中的在您擁有 AWS 帳戶 的另一個 中提供存取權給 IAM 使用者](#)。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱 [《IAM 使用者指南》中的將存取權提供給第三方 AWS 帳戶 擁有的](#)。
- 如需了解如何透過聯合身分提供存取權，請參閱 IAM 使用者指南中的 [將存取權提供給在外部進行身分驗證的使用者 \(聯合身分\)](#)。
- 如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱 [《IAM 使用者指南》中的 IAM 中的跨帳戶資源存取](#)。

AWS 的 受管政策 AWS Ground Station

AWS 受管政策是由 AWS AWS 受管政策建立和管理的獨立政策旨在為許多常用案例提供許可，以便您可以開始將許可指派給使用者、群組和角色。

請記住，AWS 受管政策可能不會授予特定使用案例的最低權限許可，因為這些許可可供所有 AWS 客戶使用。我們建議您定義使用案例專屬的 [客戶管理政策](#)，以便進一步減少許可。

您無法變更 AWS 受管政策中定義的許可。如果 AWS 更新受 AWS 管政策中定義的許可，則更新會影響政策連接的所有委託人身分（使用者、群組和角色）。AWS 服務 當新的 啟動或新的 API 操作可用於現有服務時，AWS 最有可能更新 AWS 受管政策。

如需詳細資訊，請參閱《IAM 使用者指南》中的 [AWS 受管政策](#)。

AWS 受管政策：AWSGroundStationAgentInstancePolicy

您可將 AWSGroundStationAgentInstancePolicy 政策連接到 IAM 身分。

此政策會將 AWS Ground Station 代理程式許可授予您的 Amazon EC2 執行個體，允許執行個體在 Ground Station 聯絡期間傳送和接收資料。此政策中的所有許可都來自 Ground Station 服務。

許可詳細資訊

此政策包含以下許可。

- `groundstation` – 允許資料流程端點執行個體呼叫 Ground Station Agent APIs。

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

AWS 受管政策：

AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy

您無法將 AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy 連接至 IAM 實體。此政策會連接到服務連結角色，AWS Ground Station 允許代表您執行動作。如需詳細資訊，請參閱[使用服務連結角色](#)。

此政策會授予允許尋找公 AWS Ground Station 有 IPv4 地址的 EC2 許可。

許可詳細資訊

此政策包含以下許可。

- `ec2:DescribeAddresses` – 允許代表您 AWS Ground Station 列出與 EIPs 相關聯的所有 IPs。
- `ec2:DescribeNetworkInterfaces` – 允許代表您 AWS Ground Station 取得與 EC2 執行個體相關聯之網路介面的相關資訊。

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

AWS Ground Station AWS 受管政策的更新

檢視自此服務開始追蹤這些變更 AWS Ground Station 以來 AWS 受管政策更新的詳細資訊。如需此頁面變更的自動提醒，請訂閱 AWS Ground Station 文件歷史記錄頁面上的 RSS 摘要。

變更	描述	日期
AWSGroundStationAgentInstancePolicy – 新政策	AWS Ground Station 新增了新的政策，以提供資料流程端點執行個體使用 AWS Ground Station Agent 的許可。	2023 年 4 月 12 日
AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy – 新政策	AWS Ground Station 新增了一項新政策，授予 EC2 許可，以允許尋找與 EIPs 相關聯的公有 AWS Ground Station 有 IPv4 地址，以及與 EC2 執行個體相關聯的網路介面。	2022 年 11 月 2 日
AWS Ground Station 開始追蹤變更	AWS Ground Station 已開始追蹤 AWS 受管政策的變更。	2021 年 3 月 1 日

使用 Ground Station 的服務連結角色

AWS Ground Station 使用 AWS Identity and Access Management (IAM) [服務連結角色](#)。服務連結角色是直接連結至 Ground Station 的唯一 IAM 角色類型。服務連結角色由 Ground Station 預先定義，並包含服務代表您呼叫其他 AWS 服務所需的所有許可。

服務連結角色可讓您更輕鬆地設定 Ground Station，因為您不必手動新增必要的許可。Ground Station 定義其服務連結角色的許可，除非另有定義，否則只有 Ground Station 可以擔任其角色。定義的許可包括信任政策和許可政策，且該許可政策無法附加至其他 IAM 實體。

如需支援服務連結角色的其他服務的資訊，請參閱 [AWS 使用 IAM 的服務](#)，並在服務連結角色欄中尋找具有是的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

Ground Station 的服務連結角色許可

Ground Station 使用名為 `AWSServiceRoleForGroundStationDataflowEndpointGroup` 的服務連結角色 – AWS GroundStation 使用此服務連結角色來叫用 EC2 來尋找公有 IPv4 地址。

AWSServiceRoleForGroundStationDataflowEndpointGroup 服務連結角色信任下列服務擔任該角色：

- `groundstation.amazonaws.com`

名為 `AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy` 的角色許可政策可讓 Ground Station 對指定的資源完成下列動作：

- 動作：`all AWS resources (*)` 上的 `ec2:DescribeAddresses`
動作可讓 Ground Station 列出與 EIPs 相關聯的所有 IPs。
- 動作：`all AWS resources (*)` 上的 `ec2:DescribeNetworkInterfaces`
動作可讓 Ground Station 取得與 EC2 執行個體相關聯之網路介面的相關資訊

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的 [服務連結角色許可](#)。

為 Ground Station 建立服務連結角色

您不需要手動建立一個服務連結角色。當您在 AWS CLI 或 AWS API 中建立 `DataflowEndpointGroup` 時，Ground Station 會為您建立服務連結角色。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您建立 `DataflowEndpointGroup` 時，Ground Station 會再次為您建立服務連結角色。

您也可以使用 IAM 主控台，透過資料交付至 Amazon EC2 使用案例來建立服務連結角色。在 AWS CLI 或 AWS API 中，使用服務名稱建立 `groundstation.amazonaws.com` 服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的「[建立服務連結角色](#)」。如果您刪除此服務連結角色，您可以使用此相同的程序以再次建立該角色。

編輯 Ground Station 的服務連結角色

Ground Station 不允許您編輯 `AWSServiceRoleForGroundStationDataflowEndpointGroup` 服務連結角色。因為有各種實體可能會參考服務連結角色，所以您無法在建立角色之後變更角色名稱。然而，您可以使用 IAM 來編輯角色描述。如需詳細資訊，請參閱「[IAM 使用者指南](#)」的編輯服務連結角色。

刪除 Ground Station 的服務連結角色

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您就沒有未主動監控或維護的未使用實體。

您必須先使用服務連結角色刪除 DataflowEndpointGroups，才能刪除服務連結角色。這可避免您不小心撤銷 DataflowEndpointGroups 的許可。如果服務連結角色與多個 DataflowEndpointGroups 搭配使用，您必須先刪除所有使用服務連結角色的 DataflowEndpointGroups，才能將其刪除。

Note

如果 Ground Station 服務在您嘗試刪除資源時使用角色，則刪除可能會失敗。若此情況發生，請等待數分鐘後並再次嘗試操作。

刪除 AWSServiceRoleForGroundStationDataflowEndpointGroup 使用的 Ground Station 資源

- 透過 AWS CLI 或 AWS API 刪除 DataflowEndpointGroups。

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台 AWS CLI、或 AWS API 來刪除

AWSServiceRoleForGroundStationDataflowEndpointGroup 服務連結角色。如需詳細資訊，請參閱「IAM 使用者指南」中的[刪除服務連結角色](#)。

Ground Station 服務連結角色支援的區域

Ground Station 支援在所有提供服務的區域中使用服務連結角色。如需詳細資訊，請參閱[區域表](#)。

故障診斷

NOT_AUTHORIZED_TO_CREATE_SLR - 這表示您帳戶中用來呼叫 CreateDataflowEndpointGroup API 的角色沒有 iam:CreateServiceLinkedRole 許可。具有 iam:CreateServiceLinkedRole 許可的管理員必須為您的帳戶手動建立服務連結角色。

的靜態資料加密 AWS Ground Station

AWS Ground Station 依預設提供加密，以使用 AWS 擁有的加密金鑰來保護您的靜態敏感資料。

- AWS 擁有的金鑰 - 預設 AWS Ground Station 會使用這些金鑰自動加密可直接識別個人身分的資料和暫時性資料。您無法檢視、管理或使用 AWS 擁有的金鑰，或稽核其使用方式；不過，您不需要採取任何動作或變更程式來保護加密資料的金鑰。如需詳細資訊，請參閱《[AWS Key Management Service 開發人員指南](#)》中的 [AWS 擁有的金鑰 AWS Key Management Service](#)。

根據預設，加密靜態資料有助於降低保護敏感資料所涉及的操作開銷和複雜性。同時，它可以建立符合嚴格加密合規性以及法規要求的安全應用程式。

AWS Ground Station 對所有敏感的靜態資料強制執行加密，不過，對於某些 AWS Ground Station 資源，例如暫時性資料，您可以選擇使用客戶受管金鑰來取代預設的 AWS 受管金鑰。

- 客戶受管金鑰 - AWS Ground Station 支援使用您建立、擁有和管理的對稱客戶受管金鑰，在現有 AWS 擁有的加密上新增第二層加密。您可以完全控制此層加密，因此能執行以下任務：
 - 建立和維護金鑰政策
 - 建立和維護 IAM 政策和授予操作
 - 啟用和停用金鑰政策
 - 輪換金鑰密碼編譯資料
 - 新增標籤
 - 建立金鑰別名
 - 安排金鑰供刪除

如需詳細資訊，請參閱 [《AWS Key Management Service 開發人員指南》](#) 中的 [客戶受管金鑰](#)。

下表摘要說明 AWS Ground Station 支援使用客戶受管金鑰的資源

資料類型	AWS 擁有的金鑰加密	客戶自管金鑰加密 (選用)
Ephemeris 資料用於計算衛星的軌跡	已啟用	已啟用

Note

AWS Ground Station 會使用 AWS 擁有的金鑰自動啟用靜態加密，以免費保護個人身分識別資料。不過，使用客戶受管金鑰需支付 AWS KMS 費用。如需有關定價的詳細資訊，請參閱 [AWS Key Management Service 定價](#)。

如需 AWS KMS 的詳細資訊，請參閱 [AWS KMS 開發人員指南](#)。

如何在 AWS KMS 中使用 AWS Ground Station 授予

AWS Ground Station 需要 [金鑰授權](#) 才能使用您的客戶受管金鑰。

當您上傳使用客戶受管金鑰加密的暫時性資料時，會透過傳送 `CreateGrant` 請求至 AWS KMS 來代表您 AWS Ground Station 建立金鑰授權。AWS KMS 中的授權用於授予 AWS Ground Station 您帳戶中 KMS 金鑰的存取權。

AWS Ground Station 需要授予 `aws:kms:*`，才能將客戶受管金鑰用於下列內部操作：

- 將 [GenerateDataKey](#) 請求傳送至 AWS KMS，以產生由客戶受管金鑰加密的資料金鑰。
- 將 [解密](#) 請求傳送至 AWS KMS 以解密加密的資料金鑰，以使用來加密您的資料。
- 將 [加密](#) 請求傳送至 AWS KMS 以加密提供的資料。

您可以隨時撤銷授予的存取權，或移除服務對客戶受管金鑰的存取權。如果您這麼做，AWS Ground Station 則無法存取客戶受管金鑰加密的任何資料，這會影響相依於該資料的操作。例如，如果您從目前用於聯絡的 `ephemeris` 移除金鑰授權，AWS Ground Station 則將無法在聯絡期間使用提供的 `ephemeris` 資料來指向天線。這會導致聯絡人以 `FAILED` 狀態結束。

建立客戶受管金鑰

您可以使用 AWS 管理主控台或 AWS KMS APIs 來建立對稱客戶受管金鑰。

建立對稱客戶自管金鑰

遵循 [AWS Key Management Service 開發人員指南](#) 中建立對稱客戶受管金鑰的步驟。

金鑰政策

金鑰政策會控制客戶受管金鑰的存取權限。每個客戶受管金鑰都必須只有一個金鑰政策，其中包含決定誰可以使用金鑰及其使用方式的陳述式。在建立客戶受管金鑰時，可以指定金鑰政策。如需詳細資訊，請參閱 AWS Key Management Service 開發人員指南中的 [管理客戶受管金鑰的存取權](#)。

若要將客戶受管金鑰與 AWS Ground Station 資源搭配使用，必須在金鑰政策中允許下列 API 操作：

[kms:CreateGrant](#) - 將授予新增至客戶受管金鑰。授予控制對指定 KMS 金鑰的存取，允許存取 [授予操作](#) AWS Ground Station 所需的。如需 [使用授權](#) 的詳細資訊，請參閱 AWS Key Management Service 開發人員指南。

這可讓 Amazon AWS 執行下列動作：

- 呼叫 [GenerateDataKey](#) 以產生加密的資料金鑰並將其存放，因為不會立即使用資料金鑰進行加密。
- 呼叫 [Decrypt](#) 以使用儲存的加密資料金鑰來存取加密的資料。
- 呼叫 [Encrypt](#) 以使用資料金鑰來加密資料。

- 設定淘汰委託人以允許 服務至 RetireGrant。

[kms:DescribeKey](#) - 提供客戶受管金鑰詳細資訊，以允許 在嘗試在提供的金鑰上建立授予之前 AWS Ground Station 驗證金鑰。

以下是您可以為 新增的 IAM 政策陳述式範例 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" : "*"   
}   
]
```

如需在[政策](#) 中指定許可的詳細資訊，請參閱 AWS Key Management Service 開發人員指南。

如需針對[金鑰存取 進行疑難排解](#)的詳細資訊，請參閱 AWS Key Management Service 開發人員指南。

指定的客戶受管金鑰 AWS Ground Station

您可以指定客戶受管金鑰來加密下列資源：

- 括號

建立資源時，您可以提供 kmsKeyArn 來指定資料金鑰

- kmsKeyArn - AWS KMS 客戶受管[金鑰的金鑰識別符](#)

AWS Ground Station 加密內容

[加密內容](#)是一組選用的金鑰值對，包含資料的其他相關內容資訊。AWS KMS 使用加密內容做為額外的驗證資料，以支援驗證加密。當您在加密資料的請求中包含加密內容時，AWS KMS 會將加密內容繫結至加密的資料。若要解密資料，您必須在請求中包含相同的加密內容。

AWS Ground Station 加密內容

AWS Ground Station 會根據加密的資源使用不同的加密內容，並為每個建立的金鑰授權指定特定的加密內容。

Ephemeris 加密內容：

加密 ephemeris 資源的金鑰授予會繫結至特定的衛星 ARN

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

Note

金鑰授權會針對相同的金鑰衛星對重複使用。

使用加密內容進行監控

當您使用對稱客戶受管金鑰來加密暫時性資料時，您也可以使用稽核記錄和日誌中的加密內容來識別客戶受管金鑰的使用方式。加密內容也會出現在 [AWS CloudTrail 或 Amazon CloudWatch Logs 產生的日誌](#) 中。

使用加密內容控制對客戶受管金鑰的存取

您也可以在金鑰政策和 IAM 政策中，使用加密內容作為 conditions 來控制對於對稱客戶受管金鑰的存取。您也可以在授予中使用加密內容條件。

AWS Ground Station 在授予中使用加密內容限制，以控制對您帳戶或區域中客戶受管金鑰的存取。授予條件會要求授予允許的操作使用指定的加密內容。

以下是授予特定加密內容之客戶受管金鑰存取權的金鑰政策陳述式範例。此政策陳述式中的條件會要求具有指定加密內容的加密內容條件。

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

```
}
```

監控 的加密金鑰 AWS Ground Station

當您將 AWS KMS 客戶受管金鑰與 AWS Ground Station 資源搭配使用時，您可以使用 [AWS CloudTrail](#) 或 [Amazon CloudWatch logs](#) 來追蹤 AWS Ground Station 傳送至 AWS KMS 的請求。下列範例是 CreateGrant、Decrypt、GenerateDataKeyEncrypt 和 DescribeKey 的 AWS CloudTrail 事件，用於監控 AWS Ground Station 呼叫的 KMS 操作，以存取客戶受管金鑰加密的資料。

CreateGrant (Cloudtrail)

當您使用 AWS KMS 客戶受管金鑰來加密您的 ephemeral 資源時，會代表您 AWS Ground Station 傳送存取您 AWS 帳戶中 KMS 金鑰的 CreateGrant 請求。建立的 AWS Ground Station 授予專屬於與 AWS KMS 客戶受管金鑰相關聯的資源。此外，當您刪除資源時，AWS Ground Station 會使用 RetireGrant 操作來移除授予。

下面的範例事件會記錄 CreateGrant 操作：

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

```

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

```

```
}
```

DescribeKey (Cloudtrail)

當您使用 AWS KMS 客戶受管金鑰來加密您的 ephemeral 資源時，會代表您 AWS Ground Station 傳送 DescribeKey 請求，以驗證請求的金鑰存在於您的帳戶中。

下面的範例事件會記錄 DescribeKey 操作：

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

```

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

```

GenerateDataKey (Cloudtrail)

當您使用 AWS KMS 客戶受管金鑰來加密您的 ephemeral 資源時，會 AWS Ground Station 傳送GenerateDataKey請求給 KMS，以產生用來加密資料的資料金鑰。

下面的範例事件會記錄 GenerateDataKey 操作：

```

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

```

```

    "aws:s3:arn":
      "arn:aws:s3:::customerephemerisbucket/0034abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
  },
  "responseElements": null,
  "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
  "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
  "readOnly": true,
  "resources": [
    {
      "accountId": "111122223333",
      "type": "AWS::KMS::Key",
      "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "sharedEventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
  "eventCategory": "Management"
}

```

Decrypt (Cloudtrail)

當您使用 AWS KMS 客戶受管金鑰來加密 ephemeris 資源時，如果 ephemeris 已使用相同的客戶受管金鑰加密，則 AWS Ground Station 會使用 Decrypt 操作來解密提供的 ephemeris。例如，如果 ephemeris 正在從 S3 儲存貯體上傳，並使用指定的金鑰在該儲存貯體中加密。

下面的範例事件會記錄 Decrypt 操作：

```

{
  "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"
}
```

傳輸期間的資料加密 AWS Ground Station

AWS Ground Station 根據預設提供加密，可在傳輸期間保護您的敏感資料。視任務設定檔組態而定，可以透過兩種方式在 AWS Ground Station 天線位置和 Amazon EC2 執行個體之間串流資料。

- AWS Ground Station 代理程式
- Dataflow 端點

每個串流資料的方法都會以不同的方式處理傳輸中的資料加密。以下各節說明每個方法。

AWS Ground Station 代理程式串流

AWS Ground Station 代理程式會使用客戶受管 AWS KMS 金鑰加密其串流。在您的 Amazon EC2 執行個體上執行的 AWS Ground Station 代理程式會自動解密串流，以提供解密的資料。

在 [streamsKmsKey](#) 參數MissionProfile中建立時，會指定用於加密串流的 AWS KMS 金鑰。授予金鑰 AWS Ground Station 存取權的所有許可都是透過連接到的 AWS KMS 金鑰政策來處理streamsKmsKey。

Dataflow 端點串流

資料流程端點串流會使用 [Datagram Transport Layer Security \(DTLS\)](#) 進行加密。這是使用自我簽署憑證完成的，不需要額外的組態。

範例任務設定檔組態

提供的範例示範如何取得公有廣播衛星，並建立支援該衛星的任務設定檔。產生的範本可協助您進行公有廣播衛星聯絡，並協助您做出有關衛星的決策。

主題

- [JPSS-1 - 公有廣播衛星 \(PBS\) - 評估](#)
- [使用 Amazon S3 資料交付的公有廣播衛星](#)
- [使用資料流程端點的公有廣播衛星 \(窄頻帶\)](#)
- [使用資料流程端點的公有廣播衛星 \(解調和解碼\)](#)
- [使用 AWS Ground Station 代理程式的公有廣播衛星 \(寬頻\)](#)

JPSS-1 - 公有廣播衛星 (PBS) - 評估

此範例區段符合 [客戶加入程序概觀](#)。它提供與的簡短相容性分析，AWS Ground Station 並為以下特定範例設定階段。

如 [公有廣播衛星](#) 章節所述，您可以利用可公開取得的特定衛星或衛星的通訊路徑。在本節中，我們會在 AWS Ground Station 術語中描述 [JPSS-1](#)。作為參考，我們使用 [關節極衛星系統 1 \(JPSS-1\) Spacecraft High Rate Data \(HRD\) 到 Direct Broadcast Stations \(DBS\) Radio Frequency \(RF\) Interface Control Document \(ICD\)](#) 來完成範例。此外，值得注意的是，JPSS-1 與 NORAD ID 43013 相關聯。

JPSS-1 衛星提供一個上行和三個直接下行通訊路徑，如 ICD 的圖 1-1 所示。在這四個通訊路徑中，只有單一高速率資料 (HRD) 下行通訊路徑可供公有使用。根據此，您會看到此路徑也會有更具體的資料與其相關聯。四個路徑如下所示：

- 中心頻率為 2067.27 MHz 的命令路徑 (上行)，資料速率為 2-128 kbps。此路徑不可公開存取。
- 中心頻率為 2247.5 MHz 的遙測路徑 (下行)，資料速率為 1-524 kbps。此路徑不可公開存取。
- SMD 路徑 (下行)，中心頻率為 26.7034 GHz，資料速率為 150-300 Mbps。此路徑不可公開存取。
- 資料速率為 15 Mbps 的 7812 MHz 中心頻率的 HRD 路徑 (下行) RF。其頻寬為 30 MHz，且為 right-hand-circular-polarized。當您使用加入 JPSS-1 時 AWS Ground Station，這是您可以存取的通訊路徑。此通訊路徑包含檢測科學資料、檢測工程資料、檢測遙測資料和即時太空船管家資料。

當我們比較潛在的資料路徑時，我們看到命令（上行）、遙測（下行）和 HRD（下行）路徑符合的頻率、頻寬和多頻道並行使用功能 AWS Ground Station。SMD 路徑不相容，因為中心頻率超出現有接收器的範圍。如需支援功能的詳細資訊，請參閱 [AWS Ground Station 站點功能](#)。

Note

由於 SMD 路徑與不相容 AWS Ground Station，因此範例組態中不會呈現此路徑。

Note

由於 ICD 中未定義命令（上行）和遙測（下行）路徑，也無法公開使用，因此使用時提供的值是名目值。

使用 Amazon S3 資料交付的公有廣播衛星

此範例建立在 使用者指南的 [JPSS-1 - 公有廣播衛星 \(PBS\) - 評估](#) 區段中完成的分析。

在此範例中，您需要假設一個案例 -- 您想要將 HRD 通訊路徑擷取為數位中繼頻率，並將它存放以供未來批次處理。這可節省原始無線電頻率 (RF) 的階段中正交 (I/Q) 樣本在數位化之後。資料放入 Amazon S3 儲存貯體後，您可以使用任何您想要的軟體來解調和解碼資料。如需詳細處理範例，請參閱 [MathWorks 教學課程](#)。使用此範例後，您可以考慮新增 Amazon EC2 Spot 定價元件來處理資料並降低整體處理成本。

通訊路徑

本節代表 [規劃您的資料流程通訊路徑](#) 入門。

下列所有範本程式碼片段都屬於範本的資源區段 AWS CloudFormation。

Resources:

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

Note

如需 AWS CloudFormation 範本內容的詳細資訊，請參閱[範本章節](#)。

鑑於我們將單一通訊路徑交付至 Amazon S3 的情況，您知道您將擁有單一非同步交付路徑。根據 [非同步資料交付](#) 區段，您必須定義 Amazon S3 儲存貯體。

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

此外，您將需要建立適當的角色和政策，以允許使用儲存貯 AWS Ground Station 體。

```
# 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 組態

本節代表[建立組態](#)入門。

您需要使用追蹤組態，才能在上使用自動追蹤設定偏好設定。選取 PREFERRED 做為自動追蹤可以改善訊號品質，但由於 JPSS-1 ephemeris 品質足夠，因此不需要符合訊號品質。

```

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

```

根據通訊路徑，您需要定義天線下行組態來代表衛星部分，以及 s3 記錄來參考您剛建立的 Amazon S3 儲存貯體。

```
# 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 任務描述檔

本節代表[建立任務設定檔](#)入門。

現在您已有相關聯的組態，您可以使用它們來建構資料流程。您將使用其餘參數的預設值。

```
# 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
```

將它放在一起

使用上述資源，您現在可以排程 JPSS-1 聯絡人，以便從任何已加入的進行非同步資料交付 AWS Ground Station [AWS Ground Station 位置](#)。

以下是完整的 AWS CloudFormation 範本，其中包含本節所述的所有資源，合併為可以直接用於的單一範本 AWS CloudFormation。

名為的 AWS CloudFormation 範本 `AquaSnppJpss-1TerraDigIfS3DataDelivery.yml` 包含 Amazon S3 儲存貯體，以及排程聯絡人和接收 VITA-49 Signal/IP 直接廣播資料所需的 AWS Ground Station 資源。

如果 Aqua、SNPP、JPSS-1/NOAA-20 和 Terra 未加入您的帳戶，請參閱 [加入衛星](#)。

Note

您可以使用有效的 AWS 登入資料來存取客戶加入 Amazon S3 儲存貯體，以存取範本。

以下連結使用區域 Amazon S3 儲存貯體。變更 `us-west-2` 區域碼，代表您要建立 AWS CloudFormation 堆疊的對應區域。

此外，下列指示使用 YAML。但是，範本同時提供 YAML 和 JSON 格式。若要使用 JSON，請在下載範本 `.json` 時將 `.yaml` 副檔名取代為。

若要使用 下載範本 AWS CLI，請使用下列命令：

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

您可以在瀏覽器中瀏覽至以下 URL，以在主控台中檢視和下載範本：

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

您可以使用 AWS CloudFormation 以下連結直接在 中指定範本：

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

使用資料流程端點的公有廣播衛星（窄頻帶）

此範例建立在使用者指南的 [JPSS-1 - 公有廣播衛星 \(PBS\) - 評估](#) 區段中完成的分析。

若要完成此範例，您需要假設一個案例 -- 您想要將 HRD 通訊路徑擷取為數位中繼頻率 (DigIF)，並使用 SDR 在 Amazon EC2 執行個體上的資料流程端點應用程式收到時加以處理。

通訊路徑

本節代表 [規劃您的資料流程通訊路徑](#) 入門。在此範例中，您將在 AWS CloudFormation 範本中建立兩個區段：參數和資源區段。

Note

如需 AWS CloudFormation 範本內容的詳細資訊，請參閱 [範本章節](#)。

針對參數區段，您將新增下列參數。透過 AWS CloudFormation 主控台建立堆疊時，您將指定這些值。

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

您需要建立金鑰對，並提供 Amazon EC2 EC2Key 參數的名稱。請參閱[為您的 Amazon EC2 執行個體建立金鑰對](#)。

此外，建立 AWS CloudFormation 堆疊時，您需要提供正確的區域特定 AMI ID。請參閱[AWS Ground Station Amazon Machine Image AMIs](#)。

剩餘的範本程式碼片段屬於範本的資源區段 AWS CloudFormation 。

Resources:

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

鑒於我們將單一通訊路徑交付至 EC2 執行個體的情況，您將擁有單一同步交付路徑。根據[同步資料交付](#)區段，您必須使用資料流程端點應用程式設定 Amazon EC2 執行個體，並建立一或多個資料流程端點群組。

```
# The EC2 instance that will send/receive data to/from your satellite using AWS
Ground Station.
ReceiverInstance:
  Type: AWS::EC2::Instance
  Properties:
    DisableApiTermination: false
    IamInstanceProfile: !Ref GeneralInstanceProfile
    ImageId: !Ref ReceiverAMI
    InstanceType: m5.4xlarge
    KeyName: !Ref EC2Key
    Monitoring: true
    PlacementGroupName: !Ref ClusterPlacementGroup
    SecurityGroupIds:
      - Ref: InstanceSecurityGroup
    SubnetId: !Ref ReceiverSubnet
```

```

BlockDeviceMappings:
  - DeviceName: /dev/xvda
    Ebs:
      VolumeType: gp2
      VolumeSize: 40
Tags:
  - Key: Name
    Value: !Join [ "-", [ "Receiver" , !Ref "AWS::StackName" ] ]
UserData:
  Fn::Base64:
    |
    #!/bin/bash
    exec > >(tee /var/log/user-data.log|logger -t user-data -s 2>/dev/console)
2>&1
    echo `date +%F %R:%S` ` "INFO: Logging Setup" >&2

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

    echo "Creating ${STREAM_CONFIG_PATH}"
    cat << STREAM_CONFIG > "${STREAM_CONFIG_PATH}"
    {
      "ddx_streams": [
        {
          "streamName": "Downlink",
          "maximumWanRate": 4000000000,
          "lanConfigDevice": "lo",
          "lanConfigPort": 50000,
          "wanConfigDevice": "eth1",
          "wanConfigPort": 55888,
          "isUplink": false
        }
      ]
    }
    STREAM_CONFIG

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

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

```

```

python "${GROUND_STATION_BIN_DIR}/save_default_config.py"

exit 0

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

# The security group for your EC2 instance.
InstanceSecurityGroup:
  Type: AWS::EC2::SecurityGroup
  Properties:
    GroupDescription: AWS Ground Station receiver instance security group.
    VpcId: !Ref ReceiverVPC
    SecurityGroupIngress:
      # To allow SSH access to the instance, add another rule allowing tcp port 22
from your CidrIp
      - IpProtocol: udp
        FromPort: 55888
        ToPort: 55888
        SourceSecurityGroupId: !Ref DataflowEndpointSecurityGroup
        Description: "AWS Ground Station Downlink Stream"

# The security group that the ENI created by AWS Ground Station belongs to.
DataflowEndpointSecurityGroup:
  Type: AWS::EC2::SecurityGroup

```

Properties:

GroupDescription: Security Group for AWS Ground Station registration of Dataflow Endpoint Groups

VpcId: !Ref ReceiverVPC

SecurityGroupEgress:

- IpProtocol: udp
FromPort: 55888
ToPort: 55888
CidrIp: 10.0.0.0/8
Description: "AWS Ground Station Downlink Stream To 10/8"
- IpProtocol: udp
FromPort: 55888
ToPort: 55888
CidrIp: 172.16.0.0/12
Description: "AWS Ground Station Downlink Stream To 172.16/12"
- IpProtocol: udp
FromPort: 55888
ToPort: 55888
CidrIp: 192.168.0.0/16
Description: "AWS Ground Station Downlink Stream To 192.168/16"

The placement group in which your EC2 instance is placed.

ClusterPlacementGroup:

Type: AWS::EC2::PlacementGroup

Properties:

Strategy: cluster

ReceiverVPC:

Type: AWS::EC2::VPC

Properties:

CidrBlock: "10.0.0.0/16"

Tags:

- Key: "Name"
Value: "AWS Ground Station - PBS to dataflow endpoint Example VPC"
- Key: "Description"
Value: "VPC for EC2 instance receiving AWS Ground Station data"

ReceiverSubnet:

Type: AWS::EC2::Subnet

Properties:

Ensure your CidrBlock will always have at least one available IP address per dataflow endpoint.

See <https://docs.aws.amazon.com/vpc/latest/userguide/subnet-sizing.html> for subnet sizing guidelines.

```

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

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

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

```

此外，您還需要建立適當的政策和角色，以允許在帳戶中 AWS Ground Station 建立彈性網路界面 (ENI)。

```

# 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 組態

本節代表[建立組態](#)入門。

您需要使用追蹤組態，才能在上使用自動追蹤來設定偏好設定。選擇 PREFERRED 作為自動追蹤可以改善訊號品質，但由於足夠的 JPSS-1 暫時性品質，因此不需要滿足訊號品質。

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

根據通訊路徑，您需要定義天線下行組態來代表衛星部分，以及定義端點詳細資訊之資料流程端點群組的資料流程端點組態。

```
# 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 任務描述檔

本節代表[建立任務設定檔](#)入門。

現在您已有相關聯的組態，您可以使用它們來建構資料流程。您將使用其餘參數的預設值。

```
# The AWS Ground Station Mission Profile that groups the above configurations to
define how to
# uplink and downlink data to your satellite.
SnpjpsMissionProfile:
  Type: AWS::GroundStation::MissionProfile
  Properties:
    Name: "37849 SNPP And 43013 JPSS"
    ContactPrePassDurationSeconds: 120
    ContactPostPassDurationSeconds: 60
    MinimumViableContactDurationSeconds: 180
    TrackingConfigArn: !Ref TrackingConfig
    DataflowEdges:
      - Source: !Ref SnpjpsDownlinkDigIfAntennaConfig
        Destination: !Ref DownlinkDigIfEndpointConfig
```

將它放在一起

使用上述資源，您現在可以排程 JPSS-1 聯絡人，以便從任何已加入的 同步資料交付 AWS Ground Station [AWS Ground Station 位置](#)。

以下是完整的 AWS CloudFormation 範本，其中包含本節所述的所有資源，合併為可以直接使用的單一範本 AWS CloudFormation。

名為 `AquaSnppJpssTerraDigIF.yml` 的 AWS CloudFormation 範本旨在讓您快速存取，以開始接收 Aqua、SNPP、JPSS-1/NOAA-20 和 Terra 衛星的數位化中繼頻率 (DigIF) 資料。它包含 Amazon EC2 執行個體和接收原始 DigIF 直接廣播資料所需的 AWS CloudFormation 資源。

如果 Aqua、SNPP、JPSS-1/NOAA-20 和 Terra 未加入您的帳戶，請參閱 [加入衛星](#)。

Note

您可以使用有效的 AWS 登入資料存取客戶加入 Amazon S3 儲存貯體來存取範本。以下連結使用區域 Amazon S3 儲存貯體。變更 `us-west-2` 區域碼以代表您要在其中建立堆疊的 AWS CloudFormation 對應區域。

此外，下列指示使用 YAML。但是，範本同時提供 YAML 和 JSON 格式。若要使用 JSON，請在下載範本 `.json` 時將 `.yml` 副檔名取代為。

若要使用下載範本 AWS CLI，請使用下列命令：

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

您可以在瀏覽器中瀏覽至以下 URL，以在主控台中檢視和下載範本：

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

您可以使用 AWS CloudFormation 以下連結直接在 中指定範本：

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

範本定義了哪些其他資源？

`AquaSnppJpssTerraDigIF` 範本包含下列其他資源：

- (選用) CloudWatch Event Triggers - AWS Lambda 使用聯絡 AWS Ground Station 前後由傳送的 CloudWatch Events 觸發的函數。AWS Lambda 函數將啟動並選擇性地停止您的接收者執行個體。

- (選用) 聯絡的 EC2 驗證 - 使用 Lambda 為具有 SNS 通知的聯絡設定 Amazon EC2 執行個體驗證系統的選項 (SNS)。請務必注意，這可能會根據您目前的使用量產生費用。
- Ground Station Amazon Machine Image Retrieval Lambda - 選擇執行個體中安裝的軟體以及您選擇的 AMI 的選項。軟體選項包括 DDX 2.6.2 Only 和 DDX 2.6.2 with qRadio 3.6.0。隨著其他軟體更新和功能發佈，這些選項將繼續擴展。
- 其他任務描述檔 - 其他公有廣播衛星 (Aqua、SNPP 和 Terra) 的任務描述檔。
- 其他天線下行組態 - 其他公有廣播衛星 (Aqua、SNPP 和 Terra) 的天線下行組態。

在此範本中，衛星的值和參數已經產生。這些參數可讓您輕鬆地 AWS Ground Station 立即與這些衛星搭配使用。您不需要設定自己的值，即可在使用此範本 AWS Ground Station 時使用。但是，您可以自訂這些值，讓範本適用於您的使用案例。

我可以在什麼地方接收我的資料？

資料流程端點群組的設定，是使用以範本的一部分建立的接收器執行個體網路界面。接收者執行個體使用資料流程端點應用程式，在資料流程端點定義的連接埠 AWS Ground Station 上接收來自的資料串流。接收到以後，資料就可以透過 UDP 連接埠 50000 在接收器執行個體的回送介面卡上使用。如需設定資料流程端點群組的詳細資訊，請參閱 [AWS::GroundStation::DataflowEndpointGroup](#)。

使用資料流程端點的公有廣播衛星（解調和解碼）

此範例會建置使用者指南 [JPSS-1 - 公有廣播衛星 \(PBS\) - 評估](#) 區段中完成的分析。

若要完成此範例，您需要假設一個案例 -- 您想要使用資料流程端點，以解調和解碼的直接廣播資料的形式擷取 HRD 通訊路徑。如果您計劃使用 NASA Direct Readout Labs 軟體 (RT-STPS 和 IPOPP) 處理資料，則此範例是一個很好的起點。

通訊路徑

本節代表 [規劃您的資料流程通訊路徑](#) 入門。在此範例中，您將在 AWS CloudFormation 範本中建立兩個區段：參數和資源區段。

Note

如需 AWS CloudFormation 範本內容的詳細資訊，請參閱 [範本章節](#)。

針對參數區段，您將新增下列參數。透過 AWS CloudFormation 主控台建立堆疊時，您將指定這些值。

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

您需要建立金鑰對，並提供 Amazon EC2 EC2Key 參數的名稱。請參閱[為您的 Amazon EC2 執行個體建立金鑰對](#)。

此外，建立 AWS CloudFormation 堆疊時，您需要提供正確的區域特定 AMI ID。請參閱[AWS Ground Station Amazon Machine Image AMIs](#)。

剩餘的範本程式碼片段屬於範本的資源區段 AWS CloudFormation 。

Resources:

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

鑑於我們將單一通訊路徑交付至 EC2 執行個體的情況，您將擁有單一同步交付路徑。根據 [同步資料交付區段](#)，您必須使用資料流程端點應用程式設定 Amazon EC2 執行個體，並建立一或多個資料流程端點群組。

```

# 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: tcp
        FromPort: 22
        ToPort: 22
        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
```

您也需要適當的政策、角色和設定檔，AWS Ground Station 才能允許在帳戶中建立彈性網路界面 (ENI)。

```
# 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 組態

本節代表 使用者指南 [建立組態](#) 的。

您需要使用追蹤組態，才能在上使用自動追蹤設定偏好設定。選取 PREFERRED 做為自動追蹤可以改善訊號品質，但由於 JPSS-1 ephemeris 品質足夠，因此不需要符合訊號品質。

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

根據通訊路徑，您需要定義 antenna-downlink-demod-decode 組態來代表衛星部分，以及資料流程端點組態來參考定義端點詳細資訊的資料流程端點群組。

Note

如需如何設定 DemodulationConfig、和 值的詳細資訊 DecodeConfig，請參閱 [天線下行解調解碼組態](#)。

```
# 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 任務描述檔

本節代表 使用者指南 [建立任務設定檔](#)。

現在您已有相關聯的組態，您可以使用它們來建構資料流程。您將使用其餘參數的預設值。

```
# 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
```

將它放在一起

使用上述資源，您現在可以排程 JPSS-1 聯絡人，以便從任何已加入的 同步資料交付 AWS Ground Station [AWS Ground Station 位置](#)。

以下是完整的 AWS CloudFormation 範本，其中包含本節所述的所有資源，合併為可以直接使用的單一範本 AWS CloudFormation。

名為的 AWS CloudFormation 範本 `AquaSnppJpss.yml` 旨在讓您快速存取，以開始接收 Aqua、SNPP 和 JPSS-1/NOAA-20 衛星的資料。它包含 Amazon EC2 執行個體和必要的 AWS Ground Station 資源，以排程聯絡人並接收解調和解碼的直接廣播資料。

如果 Aqua、SNPP、JPSS-1/NOAA-20 和 Terra 未加入您的帳戶，請參閱 [加入衛星](#)。

Note

您可以使用有效的 AWS 登入資料來存取客戶加入 Amazon S3 儲存貯體，以存取範本。以下連結使用區域 Amazon S3 儲存貯體。變更 `us-west-2` 區域碼，代表您要建立 AWS CloudFormation 堆疊的對應區域。

此外，下列指示使用 YAML。但是，範本同時提供 YAML 和 JSON 格式。若要使用 JSON，請在下載範本 `.json` 時將 `.yml` 副檔名取代為。

若要使用 下載範本 AWS CLI，請使用下列命令：

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

您可以在瀏覽器中瀏覽至以下 URL，以在主控台中檢視和下載範本：

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

您可以使用 AWS CloudFormation 以下連結直接在 中指定範本：

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

範本定義了哪些其他資源？

AquaSnppJpss 範本包含下列其他資源：

- (選用) CloudWatch Event Triggers - AWS Lambda 使用聯絡 AWS Ground Station 前後由 傳送的 CloudWatch Events 觸發的函數。AWS Lambda 函數將啟動並選擇性地停止您的接收者執行個體。
- (選用) 聯絡的 EC2 驗證 - 使用 Lambda 為具有 SNS 通知的聯絡設定 Amazon EC2 執行個體驗證系統的選項 (SNS 通知)。請務必注意，這可能會根據您目前的使用量產生費用。
- Ground Station Amazon Machine Image Retrieval Lambda - 選擇執行個體中安裝的軟體以及您選擇的 AMI 的選項。軟體選項包括 DDX 2.6.2 Only 和 DDX 2.6.2 with qRadio 3.6.0。如果您想要使用寬頻 DigIF 資料交付和 AWS Ground Station 代理程式，請參閱 [使用 AWS Ground Station 代理程式的公有廣播衛星 \(寬頻\)](#)。隨著其他軟體更新和功能發佈，這些選項將繼續擴展。
- 其他任務描述檔 - 其他公有廣播衛星 (Aqua、SNPP 和 Terra) 的任務描述檔。
- 其他天線下行組態 - 其他公有廣播衛星 (Aqua、SNPP 和 Terra) 的天線下行組態。

在此範本中，衛星的值 and 參數已經產生。這些參數可讓您立即與這些衛星 AWS Ground Station 搭配使用。您不需要設定自己的值，即可在使用此範本 AWS Ground Station 時使用。但是，您可以自訂這些值，讓範本適用於您的使用案例。

我可以在什麼地方接收我的資料？

資料流程端點群組的設定，是使用以範本的一部分建立的接收器執行個體網路界面。接收者執行個體使用資料流程端點應用程式，從資料流程端點定義的 AWS Ground Station 連接埠接收資料串流。接收到

以後，資料就可以透過 UDP 連接埠 50000 在接收器執行個體的回送介面卡上使用。如需設定資料流程端點群組的詳細資訊，請參閱 [AWS::GroundStation::DataflowEndpointGroup](#)。

使用 AWS Ground Station 代理程式的公有廣播衛星（寬頻）

此範例建立在 使用者指南的 [JPSS-1 - 公有廣播衛星 \(PBS\) - 評估](#) 區段中完成的分析。

若要完成此範例，您需要假設一個案例 -- 您想要將 HRD 通訊路徑擷取為寬頻數位中繼頻率 (DigIF)，並在 Amazon EC2 執行個體上的 AWS Ground Station 代理程式使用 SDR 接收時加以處理。

Note

實際 JPSS HRD 通訊路徑訊號的頻寬為 30 MHz，但您將設定天線下行組態，將其視為頻寬為 100 MHz 的訊號，以便它可以流經 AWS Ground Station 代理程式在此範例中接收的正確路徑。

通訊路徑

本節代表 [規劃您的資料流程通訊路徑](#) 入門。在此範例中，您需要 AWS CloudFormation 範本中尚未在其他範例映射區段中使用的額外區段。

Note

如需 AWS CloudFormation 範本內容的詳細資訊，請參閱 [範本章節](#)。

首先，在 AWS CloudFormation 範本中為依區域列出的 AWS Ground Station 字首清單設定映射區段。這可讓 Amazon EC2 執行個體安全群組輕鬆參考字首清單。如需使用字首清單的詳細資訊，請參閱 [使用 AWS Ground Station 代理程式的 VPC 組態](#)。

```
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
```

針對參數區段，您將新增下列參數。透過 AWS CloudFormation 主控台建立堆疊時，您將指定這些值。

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

您需要建立金鑰對，並提供 Amazon EC2 EC2Key 參數的名稱。請參閱[為您的 Amazon EC2 執行個體建立金鑰對](#)。

此外，建立 AWS CloudFormation 堆疊時，您需要提供正確的區域特定 AMI ID。請參閱[AWS Ground Station Amazon Machine Image AMIs](#)。

剩餘的範本程式碼片段屬於範本的資源區段 AWS CloudFormation 。

Resources:

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

鑑於我們將單一通訊路徑交付至 Amazon EC2 執行個體的案例，您知道您將擁有單一同步交付路徑。根據[同步資料交付](#)區段，您必須使用 AWS Ground Station Agent 設定 Amazon EC2 執行個體，並建立一或多個資料流程端點群組。首先，您將先為 AWS Ground Station 代理程式設定 Amazon VPC。

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

如需 AWS Ground Station 代理程式支援之 VPC 組態的詳細資訊，請參閱 [AWS Ground Station 代理程式需求 - VPC 圖表](#)。

接著，您將設定接收者 Amazon EC2 執行個體。

```
# 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
```

您也需要適當的政策、角色和設定檔，AWS Ground Station 才能允許在帳戶中建立彈性網路界面 (ENI)。

```
# 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 組態

本節代表 [建立組態](#) 入門。

您需要使用追蹤組態，才能在上使用自動追蹤設定偏好設定。選取 PREFERRED 做為自動追蹤可以改善訊號品質，但由於 JPSS-1 ephemeris 品質足夠，因此不需要符合訊號品質。

```

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

```

根據通訊路徑，您需要定義天線下行組態來代表衛星部分，以及定義端點詳細資訊的資料流程端點群組的資料流程端點組態。

```

# The AWS Ground Station Antenna Downlink Config that defines the frequency spectrum
used to
# downlink data from your satellite.
SnpjpsDownlinkDigIfAntennaConfig:
  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 任務描述檔

本節代表[建立任務設定檔](#)入門。

現在您已擁有相關聯的組態，您可以使用它們來建構資料流程。您將使用其餘參數的預設值。

```
# 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 SnpjPssDownlinkDigIfAntennaConfig
    Destination: !Ref DownlinkDigIfEndpointConfig
StreamsKmsKey:
  KmsKeyArn: !GetAtt GroundStationDataDeliveryKmsKey.Arn
StreamsKmsRole: !GetAtt GroundStationKmsKeyRole.Arn
```

將它放在一起

透過上述資源，您現在可以排程 JPSS-1 聯絡人，以便從任何已加入的 同步資料交付 AWS Ground Station [AWS Ground Station 位置](#)。

以下是完整的 AWS CloudFormation 範本，其中包含本節所述的所有資源，合併為可以直接使用的單一範本 AWS CloudFormation。

名為的 AWS CloudFormation 範

本DirectBroadcastSatelliteWbDigIfEc2DataDelivery.yml旨在讓您快速存取，以開始接收 Aqua、SNPP、JPSS-1/NOAA-20 和 Terra 衛星的數位化中繼頻率 (DigIF) 資料。它包含 Amazon EC2 執行個體，以及使用 AWS Ground Station Agent 接收原始 DigIF 直接廣播資料所需的 AWS CloudFormation 資源。

如果 Aqua、SNPP、JPSS-1/NOAA-20 和 Terra 未加入您的帳戶，請參閱 [加入衛星](#)。

Note

您可以使用有效的 AWS 登入資料來存取客戶加入 Amazon S3 儲存貯體，以存取範本。

以下連結使用區域 Amazon S3 儲存貯體。變更us-west-2區域碼，代表您要建立 AWS CloudFormation 堆疊的對應區域。

此外，下列指示使用 YAML。但是，範本同時提供 YAML 和 JSON 格式。若要使用 JSON，請在下載範本.json時將.yml副檔名取代為。

若要使用 下載範本 AWS CLI，請使用下列命令：

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

您可以在瀏覽器中瀏覽至以下 URL，以在主控台中檢視和下載範本：

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

您可以使用 AWS CloudFormation 以下連結直接在 中指定範本：

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

範本定義了哪些其他資源？

DirectBroadcastSatelliteWbDigIfEc2DataDelivery 範本包含下列其他資源：

- 接收者執行個體彈性網路界面 - (條件式) 如果提供彈性網路界面，則會在 PublicSubnetId 指定的子網路中建立彈性網路界面。如果接收者執行個體位於私有子網路中，則此為必要項目。彈性網路界面將與 EIP 建立關聯，並連接到接收者執行個體。
- 接收者執行個體彈性 IP - AWS Ground Station 將連線的彈性 IP。這會連接至接收器執行個體或彈性網路界面。
- 下列其中一個彈性 IP 關聯：
 - 接收者執行個體與彈性 IP 關聯 - 如果未指定 PublicSubnetId，則彈性 IP 與接收者執行個體的關聯。這需要 SubnetId 參考公有子網路。
 - 接收者執行個體彈性網路界面與彈性 IP 關聯 - 如果指定 PublicSubnetId，則彈性 IP 與接收者執行個體彈性網路界面的關聯。
- (選用) CloudWatch Event Triggers - AWS Lambda 使用聯絡 AWS Ground Station 前後由 傳送的 CloudWatch Events 觸發的函數。AWS Lambda 函數將啟動並選擇性地停止您的接收者執行個體。
- (選用) Amazon EC2 聯絡驗證 - 使用 Lambda 為具有 SNS 通知的聯絡設定 Amazon EC2 執行個體驗證系統的選項 (SNS 通知)。請務必注意，這可能會根據您目前的使用量產生費用。
- 其他任務描述檔 - 其他公有廣播衛星 (Aqua、SNPP 和 Terra) 的任務描述檔。
- 其他天線下行組態 - 其他公有廣播衛星 (Aqua、SNPP 和 Terra) 的天線下行組態。

在此範本中，衛星的值和參數已經產生。這些參數可讓您輕鬆地 AWS Ground Station 立即與這些衛星搭配使用。您不需要設定自己的值，即可在使用此範本 AWS Ground Station 時使用。但是，您可以自訂這些值，讓範本適用於您的使用案例。

我可以在什麼地方接收我的資料？

資料流程端點群組的設定，是使用以範本的一部分建立的接收器執行個體網路界面。接收者執行個體使用 AWS Ground Station 代理程式，在資料流程端點定義的連接埠 AWS

Ground Station 上接收來自 的資料串流。如需設定資料流程端點群組的詳細資訊，請參閱 [AWS::GroundStation::DataflowEndpointGroup](#)。如需 代理程式的詳細資訊 AWS Ground Station ，請參閱 [什麼是 AWS Ground Station 代理程式？](#)

疑難排解

下列文件可協助您針對使用時可能發生的問題進行疑難排解 AWS Ground Station。

主題

- [對將資料交付至 Amazon EC2 的聯絡人進行故障診斷](#)
- [故障診斷失敗的聯絡案例](#)
- [故障診斷 FAILED_TO_SCHEDULE 聯絡人](#)
- [針對未處於 HEALTHY 狀態的 DataflowEndpointGroups 進行故障診斷](#)
- [故障診斷無效的短暫性事件](#)
- [對沒有收到資料的聯絡人進行故障診斷](#)

對將資料交付至 Amazon EC2 的聯絡人進行故障診斷

如果您無法成功完成 AWS Ground Station 聯絡，則需要驗證 Amazon EC2 執行個體是否正在執行、確認資料流程端點應用程式正在執行，並確認資料流程端點應用程式的串流已正確設定。

Note

DataDefender (DDX) 是目前支援的資料流程端點應用程式範例 AWS Ground Station

必要條件

下列程序假設 Amazon EC2 執行個體已設定。若要在中設定 Amazon EC2 執行個體 AWS Ground Station，請參閱[入門](#)。

步驟 1：確認您的 EC2 執行個體正在執行

下列程序說明如何在主控台中尋找您的 Amazon EC2 執行個體，並在未執行時啟動執行個體。

1. 找到用於您要疑難排解之聯絡人的 Amazon EC2 執行個體。使用下列步驟：
 - a. 在 AWS CloudFormation 儀表板中，選取包含 Amazon EC2 執行個體的堆疊。
 - b. 選擇資源索引標籤，並在邏輯 ID 欄中尋找您的 Amazon EC2 執行個體。驗證執行個體是在 Status (狀態) 欄中建立。

- c. 在實體 ID 欄中，選擇 Amazon EC2 執行個體的連結。這將帶您前往 Amazon EC2 管理主控台。
2. 在 Amazon EC2 管理主控台中，確保您的 Amazon EC2 執行個體狀態正在執行。
 3. 如果您的執行個體正在執行，請繼續下一個步驟。如果您的執行個體未執行，請依照以下步驟啟動執行個體：
 - 選取 Amazon EC2 執行個體後，選擇動作 > 執行個體狀態 > 開始。

步驟 2：判斷使用的資料流程應用程式類型

如果您使用 AWS Ground Station 代理程式進行資料交付，請重新導向至[疑難排解 AWS Ground Station 代理程式](#)一節。否則，如果您使用 DataDefender (DDX) 應用程式，請繼續 [the section called “步驟 3：確認資料流程應用程式正在執行”](#)。

步驟 3：確認資料流程應用程式正在執行

驗證 DataDefender 狀態需要您連線到 Amazon EC2 中的執行個體。如需連接至執行個體的詳細資訊，請參閱[連接至 Linux 執行個體](#)。

下列程序提供在 SSH 用戶端中使用命令的故障診斷步驟。

1. 開啟終端機或命令提示，並使用 SSH 連線至您的 Amazon EC2 執行個體。轉送遠端主機的連接埠 80，以檢視 DataDefender Web UI。下列命令示範如何使用 SSH 透過啟用連接埠轉送的堡壘連線至 Amazon EC2 執行個體。

Note

您必須以特定 SSH 金鑰、堡壘主機名稱和 Amazon EC2 執行個體主機名稱取代 <SSH KEY>、<BASTION HOST> 和 <HOST>。

適用於 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>
```

適用於 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. 驗證 DataDefender (也稱為 DDX) 是否正在輸出中針對名為 ddx 的執行程序進行 grepping (檢查)。以下提供一個執行中處理程序和一個成功範例輸出的 Grepping 檢查命令。

```
[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
```

如果 DataDefender 正在執行，請跳至 [the section called “步驟 4：確認您的資料流程應用程式串流已設定”](#) 否則，請繼續下一個步驟。

3. 使用以下命令啟動 DataDefender。

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

如果 DataDefender 在使用命令後正在執行，請跳至 [the section called “步驟 4：確認您的資料流程應用程式串流已設定”](#) 否則，請繼續下一個步驟。

4. 使用以下命令檢查下列檔案，以查看安裝和設定 DataDefender 時是否有任何錯誤。

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

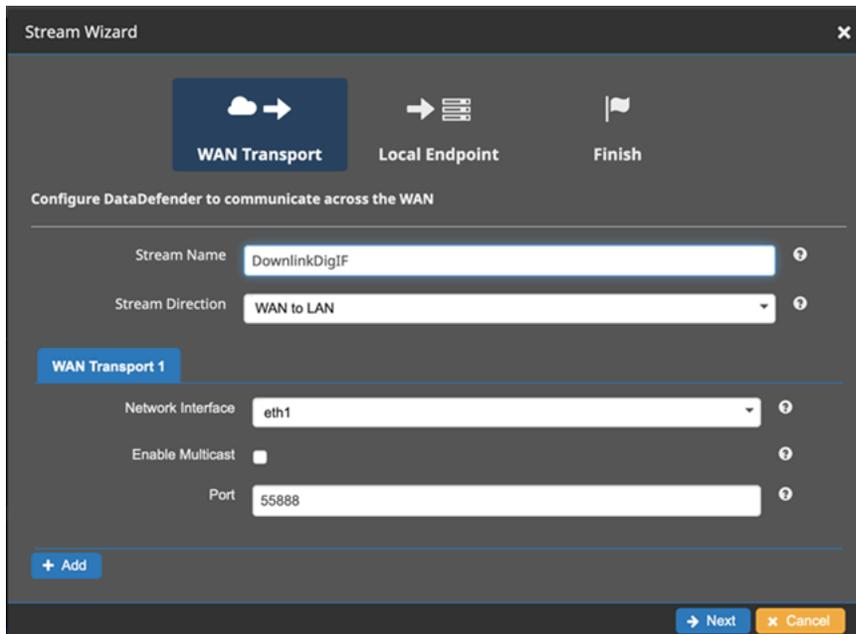
Note

檢查這些檔案時發現的常見問題是 Amazon EC2 執行個體在其中執行的 Amazon VPC 無法存取 Amazon S3 下載安裝檔案。如果您在日誌中發現此問題，請檢查 EC2 執行個體的 Amazon VPC 和安全群組設定，以確保它們不會封鎖對 Amazon S3 的存取。

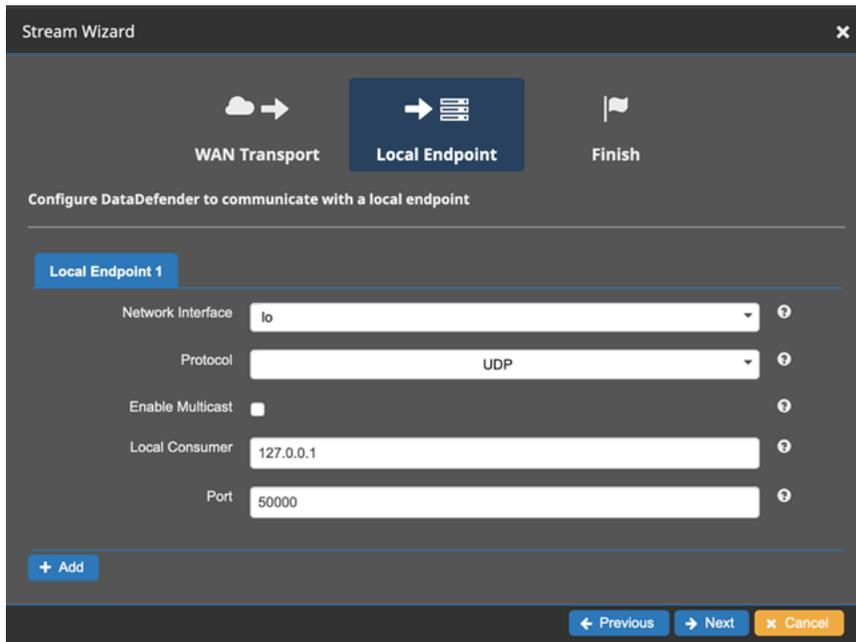
如果 DataDefender 在檢查您的 Amazon VPC 設定後正在執行，請繼續 [the section called “步驟 4：確認您的資料流程應用程式串流已設定”](#)。如果問題持續發生，請[聯絡 AWS Support](#) 並傳送日誌檔案與問題描述。

步驟 4：確認您的資料流程應用程式串流已設定

1. 在 Web 瀏覽器中，透過在地址列中輸入下列地址來存取 DataDefender Web 使用者介面：localhost : 8080。然後按 Enter 鍵。
2. 在 DataDefender 儀表板中，選擇 Go to Details (移至詳細資訊)。
3. 從串流清單中選取串流，然後選擇 Edit Stream (編輯串流)。
4. 在 Stream Wizard (串流精靈) 對話方塊中，執行下列動作：
 - a. 在 WAN 傳輸窗格中，確定已選取串流方向的 WAN 至 LAN。
 - b. 在 Port (連接埠) 方塊中，確保您已為資料流程端點群組選擇的 WAN 連接埠存在。此連接埠預設為 55888。然後選擇下一步。



- c. 在 Local Endpoint (本機端點) 窗格中，確保有效的連接埠存在於 Port (連接埠) 方塊。此連接埠預設為 50000。這是 DataDefender 從 AWS Ground Station 服務接收資料後，您會在其中接收資料的連接埠。然後選擇下一步。



- d. 如果您已變更任何值，請透過其餘功能表選擇 Finish (完成)。否則您可以從 Stream Wizard (串流精靈) 功能表取消。

您現在已確保 Amazon EC2 執行個體和 DataDefender 都已正確執行和設定，以接收來自的資料 AWS Ground Station。繼續進行[the section called “步驟 5：確定您的接收者執行個體（多個）子網路中有足夠的可用 IP 地址”](#)。

步驟 5：確定您的接收者執行個體（多個）子網路中有足夠的可用 IP 地址

下列程序說明如何在主控台的 Amazon EC2 接收器執行個體中尋找可用的 IP 地址數量。

1. 針對用於您要疑難排解之聯絡案例的每個 Amazon EC2 接收者執行個體。使用下列步驟：
 - a. 在 AWS CloudFormation 儀表中，選取包含 Amazon EC2 執行個體的堆疊。
 - b. 選擇資源索引標籤，並在邏輯 ID 欄中尋找您的 Amazon EC2 執行個體。驗證執行個體是在 Status (狀態) 欄中建立。
 - c. 在實體 ID 欄中，選擇 Amazon EC2 執行個體的連結。這將帶您前往 Amazon EC2 管理主控台。
2. 在 Amazon EC2 管理主控台中，尋找並按一下 Amazon EC2 接收者執行個體的執行個體摘要中的子網路 ID 連結。這將帶您前往對應的 Amazon VPC 管理主控台。

3. 在 Amazon VPC 管理主控台中選取相符的子網路，並檢查子網路的詳細資訊以取得可用的 IPv4 地址。如果此數字不等於使用此 Amazon EC2 接收器執行個體的資料流程端點，請執行下列動作：
 - a. 更新 AWS CloudFormation 範本對應的子網路 CidrBlock 以正確調整大小。如需子網路大小的詳細資訊，請參閱[子網路 CIDR 區塊](#)。
 - b. 使用更新後的 AWS CloudFormation 範本重新部署堆疊。

如果您持續遇到問題，[請聯絡 AWS Support](#)。

故障診斷失敗的聯絡案例

當 AWS Ground Station 偵測到資源組態問題時，聯絡人的終端聯絡人狀態將為 FAILED。以下提供可能導致 FAILED 聯絡人的常見使用案例，以及協助故障診斷的步驟。

Note

本指南專門用於 FAILED 聯絡狀態 - 不適用於其他失敗狀態，例如 AWS_FAILED、AWS_CANCELLED 或 FAILED_TO_SCHEDULE。如需聯絡狀態的詳細資訊，請參閱 [the section called “AWS Ground Station 聯絡狀態”](#)

Dataflow 端點 FAILED 使用案例

以下是可能導致資料流程端點型資料流程的 FAILED 聯絡狀態的常見使用案例清單：

- 資料流程端點永遠不會連線 - AWS Ground Station 從未建立一或多個資料流程的天線與資料流程端點群組之間的連線。
- Dataflow 端點會延遲連線 - 在聯絡開始時間之後建立一或多個資料流程的 AWS Ground Station 天線與 Dataflow 端點群組之間的連線。
- Dataflow 端點的子網路沒有可用的 IP 地址 - 由於接收器執行個體子網路中沒有任何可用的 IP 地址，因此 AWS Ground Station 的資料交付解決方案無法在您的私有網路中建立 ENI。

對於任何資料流程端點失敗案例，建議查看下列項目：

- 在聯絡開始時間之前，確認接收者 Amazon EC2 執行個體已成功啟動。
- 確認資料流程端點軟體已在聯絡期間啟動並執行。

- 確保每個接收器執行個體子網路的每個資料流程端點至少有一個可用的 IP 地址。

如需更具體對將資料交付至 [Amazon EC2 的聯絡人進行故障診斷](#) 的故障診斷步驟，請參閱上的一節。

AWS Ground Station 代理程式失敗的使用案例

以下是可能導致客服人員型資料流程聯絡狀態失敗的常見使用案例清單：

- AWS Ground Station 客服人員從未報告狀態 - 負責協調資料流程端點群組上一或多個資料流程之資料交付的客服人員從未成功報告狀態 AWS Ground Station。此狀態更新應在聯絡結束時間的幾秒鐘內進行。
- AWS Ground Station 客服人員延遲開始 - 負責協調 Dataflow 端點群組上一或多個資料流程資料交付的客服人員，在聯絡開始時間後延遲開始。

對於任何 AWS Ground Station 客服人員資料流程失敗案例，建議查看下列項目：

- 在聯絡開始時間之前，確認接收者 Amazon EC2 執行個體已成功啟動。
- 確認客服人員應用程式已在聯絡開始時和期間啟動並執行。
- 確認客服人員應用程式和 Amazon EC2 執行個體未在聯絡結束後 15 秒內關閉。這可讓客服人員有足夠的時間向其報告狀態 AWS Ground Station。

如需更具體對將資料交付至 [Amazon EC2 的聯絡人進行故障診斷](#) 的故障診斷步驟，請參閱上的一節。

故障診斷 FAILED_TO_SCHEDULE 聯絡人

當偵測到資源組態或內部系統的問題時 AWS Ground Station，聯絡人將結束為 FAILED_TO_SCHEDULE 狀態。結束為 FAILED_TO_SCHEDULE 狀態的聯絡人將選擇性地提供 errorMessage 以取得其他內容。如需描述聯絡人的資訊，請參閱 [DescribeContact](#) API。

以下提供可能導致 FAILED_TO_SCHEDULE 聯絡人的常見使用案例，以及協助疑難排解的步驟。

Note

本指南專門針對 FAILED_TO_SCHEDULE 聯絡狀態 - 而不適用於其他失敗狀態，例如 AWS_FAILED、AWS_CANCELLED 或 FAILED。如需聯絡狀態的詳細資訊，請參閱 [the section called “AWS Ground Station 聯絡狀態”](#)

不支援在天線下行解碼組態中指定的設定

用於排程此聯絡人的[任務描述](#)檔具有無效的 [antenna-downlink-demod-decode 組態](#)。

先前現有的 AntennaDownlinkDemodDecode 組態

- 如果您的 antenna-downlink-demod-decode 組態最近已變更 - 在嘗試排程之前，請復原至先前運作的版本。
- 如果這是對現有組態的刻意變更，或先前現有的組態不再成功排程，請依照下一個步驟，了解如何加入新的 AntennaDownlinkDemodDecode 組態。

新建立的 AntennaDownlinkDemodDecode 組態

AWS Ground Station 直接聯絡 以加入您的新組態。使用 [AWS Support](#) 建立案例contactId，包括以 FAILED_TO_SCHEDULE 狀態結尾的

一般故障診斷步驟

如果上述疑難排解步驟無法解決您的問題：

- 使用相同的任務設定檔重新嘗試排程聯絡人或排程另一個聯絡人。如需如何保留聯絡人的資訊，請參閱 [ReserveContact](#)。
- 如果您繼續收到此任務設定檔的 FAILED_TO_SCHEDULE 狀態，[請聯絡 AWS Support](#)

針對未處於 HEALTHY 狀態的 DataflowEndpointGroups 進行故障診斷

下列是資料流程端點群組可能未處於 HEALTHY 狀態的原因，以及要採取的適當修正動作。

- NO_REGISTERED_AGENT - 啟動 EC2 執行個體，這會註冊代理程式。請注意，您必須擁有有效的控制器組態檔案，才能讓此呼叫成功。如需設定該檔案的詳細資訊[使用 AWS Ground Station 代理程式](#)，請參閱。
- INVALID_IP_OWNERSHIP - 使用 DeleteDataflowEndpointGroup API 刪除資料流程端點群組，然後使用 CreateDataflowEndpointGroup API，使用與 EC2 執行個體相關聯的 IP 地址和連接埠重新建立資料流程端點群組。
- UNVERIFIED_IP_OWNERSHIP - IP 地址尚未驗證。驗證會定期進行，因此應該自行解決。

- NOT_AUTHORIZED_TO_CREATE_SLR - 帳戶未獲授權建立必要的服務連結角色。檢查 [中的疑難排解步驟](#) [使用 Ground Station 的服務連結角色](#)

故障診斷無效的短暫性事件

當自訂暫時性資料上傳到時 AWS Ground Station，它會先經過非同步驗證工作流程，再變成 ENABLED。此工作流程可確保衛星識別符、中繼資料和軌跡有效。

當 ephemeris 驗證失敗時，DescribeEphemeris 會傳回 EphemerisInvalidReason，讓您深入了解 ephemeris 驗證失敗的原因。EphemerisInvalidReason 的潛在值如下：

Value	描述	故障診斷動作
METADATA_INVALID	提供的太空船識別符，例如衛星 ID 無效	檢查 ephemeris 資料中提供的 NORAD ID 或其他識別符
TIME_RANGE_INVALID	開始、結束或到期時間（對）提供的暫時性資料無效	確定開始時間早於 `now`（建議設定過去幾分鐘的開始時間）、結束時間晚於開始時間，以及結束時間晚於過期時間
TRAJECTORY_INVALID	提供的 ephemeris 會定義無效的太空船軌跡	確認提供的軌跡是連續的，且適用於正確的衛星。
VALIDATION_ERROR	處理 ephemeris 進行驗證時發生內部服務錯誤	重試上傳

以下是 ephemeris INVALID 的範例 DescribeEphemeris 回應：

```
{
  "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

如果暫時狀態為 ERROR，則暫時不是 ENABLED 由於 AWS Ground Station 服務發生問題。您應該嘗試透過 再次提供 `ephemerisCreateEphemeris`。ENABLED 如果問題是暫時性的，新的暫時性事件可能會變成暫時性的。

Note

AWS Ground Station 將暫時性資料視為 [個人化用量資料](#)。如果您使用此選用功能，AWS 將使用 `ephemeris` 資料來提供故障診斷支援。

對沒有收到資料的聯絡人進行故障診斷

聯絡人可能顯示成功，但仍然沒有收到任何資料。這可能表示您收到空白的 PCAP 檔案，或者如果您使用 S3 資料交付，則完全沒有 PCAP 檔案。這可能有許多原因。以下討論一些原因，以及如何解決這些原因。

下行組態不正確

從衛星接收資料的每個聯絡人都會有關聯的 [天線下行組態](#) 或 [天線下行解調解碼組態](#)。如果指定的組態與衛星傳輸的訊號不一致，AWS Ground Station 將無法接收傳輸的訊號。這將導致未收到任何資料 AWS Ground Station。

若要修正此問題，請確認您使用的組態同意衛星傳輸的訊號。例如，確認您已設定正確的中心頻率、頻寬、極化，並視需要解調和解碼參數。

衛星操控

有時候，衛星可能會執行動作，暫時停用其部分通訊系統。操控也可能大幅變更天空中衛星的位置。AWS Ground Station 將無法接收來自未傳輸訊號之衛星的訊號，或者如果使用的暫時性訊號導致 AWS Ground Station 天線指向天空中不存在衛星的位置。

如果您嘗試與 NOAA 營運的公有廣播衛星通訊，您可以在 NOAA [衛星提醒訊息頁面上找到描述中斷或操作的訊息](#)。訊息可能包含預計資料傳輸會恢復的時間軸，或者可能會張貼在後續訊息中。

如果您與自己的衛星通訊，您有責任了解您的衛星操作，以及這可能會影響與的通訊 AWS Ground Station。如果您執行的動作會影響衛星軌跡，這可能包括提供更新的自訂暫時性資料。如需提供自訂暫時性資料的詳細資訊，請參閱 [提供自訂暫時性資料](#)。

AWS Ground Station 中斷

如果 AWS Ground Station 導致聯絡失敗或取消，AWS Ground Station 會將聯絡狀態設定為 AWS_FAILED 或 AWS_CANCELLED。如需聯絡生命週期的詳細資訊，請參閱 [了解聯絡生命週期](#)。在某些情況下，AWS Ground Station 可能會失敗，導致資料無法交付至您的帳戶，但不會導致聯絡人處於 AWS_FAILED 或 AWS_CANCELLED 狀態。發生這種情況時，AWS Ground Station 應該將帳戶特定事件發佈至您的 AWS 運作狀態儀表板。如需運作狀態 AWS 儀表板的詳細資訊，請參閱 [AWS 運作狀態使用者指南](#)。

配額和限制

您可以在端點和配額中檢視支援的區域、其相關聯的[AWS Ground Station 端點和配額](#)。

您可以使用 [Service Quotas 主控台](#)、[AWS API](#)與[AWS CLI](#)在需要時請求增加配額。

服務條款

如需 AWS Ground Station 服務條款，請參閱 [AWS 服務條款](#)。

AWS Ground Station 使用者指南的文件歷史記錄

下表說明 AWS Ground Station 使用者指南每個版本的重要變更。

變更	描述	日期
文件更新	新增有關已設定資源之聯絡使用率的說明。	2025 年 4 月 4 日
新功能	更新使用者指南以包含 AWS Ground Station 數位分身。	2024 年 8 月 6 日
文件更新	已更新使用者指南的許多章節，包括新圖表、範例等。	2024 年 7 月 18 日
文件更新	已將 RSS 摘要新增至 使用者指南。	2024 年 7 月 18 日
文件更新	將 AWS Ground Station 客服人員使用者指南分割成單獨的使用者指南。	2024 年 7 月 18 日
新功能	聯絡人現在可以在可見性時間範圍之外排程最多 30 秒。可見性時間包含在 DescribeContact 回應中。	2024 年 3 月 26 日
文件更新	已改善組織並新增「EC2 執行個體選擇和 CPU 規劃」區段。	2024 年 3 月 6 日
文件更新	將新的最佳實務新增至 AWS Ground Station 代理程式使用者指南，以搭配 AWS Ground Station 代理程式執行 服務和程序。	2024 年 2 月 23 日
文件更新	新增客服人員版本備註頁面。	2024 年 2 月 21 日

範本更新	新增對 DirectBroadcastSatelliteWbDigIfEc2DataDelivery 範本中個別公有子網路的支援。	2024 年 2 月 14 日
文件更新	在監控文件中新增對 AWS 使用者通知的推薦。	2023 年 8 月 6 日
文件更新	新增了使用要在 AWS Ground Station 主控台中顯示的名稱標記衛星的指示。	2023 年 7 月 26 日
新功能	新增了適用於寬頻 DigIF 資料交付版本的 AWS Ground Station 代理程式使用者指南	2023 年 4 月 12 日
新的 AWS 受管政策	AWS Ground Station 新增名為 AWSGroundStationAgentInstancePolicy 的新政策。	2023 年 4 月 12 日
新功能	更新了 CPE 預覽版發行的使用者指南。	2022 年 11 月 9 日
新的 AWS 受管政策	AWS Ground Station 新增了 AWSServiceRoleForGroundStationDataflowEndpointGroup service-linked-role(SLR)，其中包含名為 AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy 的新政策。	2022 年 11 月 2 日
新功能	更新使用者指南以包含的整合 AWS CLI。	2020 年 4 月 17 日
新功能	更新了使用者指南，以包含與 CloudWatch 指標的整合。	2020 年 2 月 24 日

新範本	公有廣播衛星 (AquaSnppJpss 範本) 已新增至 AWS Ground Station 使用者指南。	2020 年 2 月 19 日
新功能	已更新使用者只能，加入跨區域資料傳送。	2020 年 2 月 5 日
文件更新	更新 AWS Ground Station 使用 CloudWatch Events 進行監控的範例和說明。	2020 年 2 月 4 日
文件更新	範本位置已更新，且已修訂「入門」和「故障診斷」章節。	2019 年 12 月 19 日
新的故障診斷區段	故障診斷章節已新增至 AWS Ground Station 使用者指南。	2019 年 11 月 7 日
新的入門主題	已更新入門主題，其中包含最新的 AWS CloudFormation 範本。	2019 年 7 月 1 日
Kindle 版本	AWS Ground Station 使用者指南的發佈 Kindle 版本。	2019 年 6 月 20 日
新的服務與指南	這是 AWS Ground Station 和 AWS Ground Station 使用者指南的初始版本。	2019 年 5 月 23 日

AWS 詞彙表

如需最新的 AWS 術語，請參閱 AWS 詞彙表 參考中的[AWS 詞彙表](#)。

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。