使用者指南

AWS 資料傳輸終端機

AWS 資料傳輸終端機: 使用者指南

Table of Contents

什麼是資料傳輸終端機？

AWS 資料傳輸終端機是一個網路就緒的實體位置，您可以將資料儲存裝置帶到 AWS 雲端 服務之間快速傳輸資料。上傳遠端擷取的資料，讓您更輕鬆地存取遠端擷取的資料。

從 安排在其中一個實體資料傳輸終端機設施的保留 AWS Management Console，抵達排定的時間，然後使用您自己的裝置將您的資料上傳至 AWS 雲端 服務。在您完成排定的保留並離開後，會重新保護設施，並準備好進行下一個排定的保留。

> **Note**
>
> AWS 資料傳輸終端機目前僅適用於 AWS 企業客戶。

若要存取資料傳輸終端機：

- AWS 資料傳輸終端機主控台：https：//https://console.aws.amazon.com/datatransferterminal
- 資料傳輸終端機設施：資料傳輸終端機設施的位置會在主控台中進行保留後提供。如需詳細資訊，請參閱進行資料傳輸。

功能

使用 AWS 資料傳輸終端機可讓您更輕鬆地從遠端位置將資料傳送至 AWS 雲端 服務。以下是資料傳輸終端機的一些優勢，可滿足您的遠端資料上傳需求：

安全、私有和獨家

每個資料傳輸終端機設施都是安全的私有位置，可讓您 AWS 透過快速網路連線，在資料儲存裝置和服務之間進行大型資料傳輸。

專用預留主控台

將核准的人員新增至您的傳輸團隊，並使用資料傳輸終端機主控台來排程 AWS 資料傳輸終端機保留。

光纖網路連線

每個資料傳輸終端機設施都包含兩個 100 Gigabit (Gbps) 光纖 (LR4) 連線，用於快速資料上傳和備援。

控制資料儲存裝置

不需要運送 Snowball 裝置，並等待您的資料上傳至您的 AWS 雲端 服務。在整個資料傳輸過程中，您可以控制實體資料儲存裝置，將資料送達需要更快的地方。

重要概念

使用 AWS 資料傳輸終端機需要程序擁有者為資料傳輸專家排程保留，以存取資料傳輸終端機設施。請參閱下列各節，進一步了解資料傳輸終端機術語。

主題

- 轉接團隊
- 人員
- 設施

轉接團隊

傳輸團隊是由 AWS 帳戶 擁有者決定的人員群組，這些人員可能獲選代表您的組織執行資料傳輸。設定 Transfer 團隊包括為 Transfer 團隊命名並指定團隊的人員。我們建議單一保留有四名或更少的資料傳輸專家。

如需詳細資訊，請參閱排程資料傳輸終端機保留。

人員

人員是指可以進行和管理保留，或可以前往 並使用資料傳輸終端機設施的人員。人員可以是流程擁有者或資料傳輸專家，或兩者都是。

程序擁有者

程序擁有者是可以新增、編輯和移除其 AWS 資料傳輸終端機帳戶中人員的 AWS 帳戶 擁有者。

資料傳輸專家

資料傳輸專家是可以前往資料傳輸終端設施進行資料上傳交易的個人。這些人員必須經過程序擁有者的授權，並新增至您的 AWS 資料傳輸終端機帳戶。存取資料傳輸終端機設施時，將需要政府核發的 ID。

設施

資料傳輸終端設施是資料中樞，由一或多個服務供應商共同擁有和管理。每個設施都需要資料傳輸終端機資料傳輸專家提供政府核發的身分證明，該身分證明必須符合其保留記錄，才能存取資料傳輸終端機套件。

排程考量事項

您可以在 Data Transfer Terminal 主控台中預訂一到六個小時，一週中的任何一天，全年皆可預訂。個別保留可以連續排程，保留之間至少間隔一小時。所有預約都必須至少提前 24 小時完成。

進行資料傳輸所需的時間量會因上傳效能速度而有所不同。在您規劃和排程資料傳輸終端機保留時，請考慮影響上傳效能的下列因素。

設備

有些設備可能包含可能影響上傳效能的設定。如需建議的上傳效能速度，請參閱您的設備規格。

網路條件

流量過重的網路時間會影響資料上傳速度，而且在選擇資料傳輸工作階段的時間時應考慮到。規劃資料傳輸工作階段的離峰時數或在網路活動較少的時間，可能會改善您的上傳速度。

資料傳輸大小

資料傳輸終端機網路連線專為大型資料傳輸而設計。不過，傳輸的資料大小會影響工作階段需要多長時間。

使用案例

雖然任何 AWS 企業客戶都可以存取資料傳輸終端機系統，但特定使用案例可能會從中獲益更多。

自動駕駛和進階駕駛輔助系統 (AD/ADAS)：汽車原始設備製造商 (OEM) 和供應商會從其在北美洲、歐洲和 ASEAN 的許多集群中操作和收集資料的自動駕駛機群產生大型資料集。透過資料傳輸終端機，這些機群車輛收集的資料可以上傳到 AWS 雲端 服務，並用於訓練 AD/ADAS 模型。

媒體和娛樂：Studio 和其他內容創作者通常會在遠端位置產生數位影片和音訊 (AV) 檔案。這些 AV 檔案必須及時上傳至雲端，以便分散地理的生產和編輯團隊可以並行且即時地開始工作流程。透過使用資料傳輸終端機遠端上傳資料，可以縮短生產時間表，並轉換為降低的生產成本。

映射、光圖法和 3D 影像：使用映射或影像應用程式的組織會在遠端位置收集資料，且需要將這些視覺化檔案上傳至 AWS 雲端 進行分析或訓練。Data Transfer Terminal 可將收集和分析這些大型資料集之間的時間降至最低，這有助於 up-to-date 讓驅動程式、農夫和其他使用者取得最新的地理資料。

相關服務

以下 AWS 服務 提供使用資料傳輸終端機時的最佳體驗。

AWS 服務	描述
AWS Snowball Edge	AWS Data Transfer Terminal 透過提供位置以更快地上傳至 AWS 雲端來補充 Snowball 產品，將存取資料的等待時間降至最低。
Amazon Simple Storage Service (Amazon S3)	將您自己的裝置帶到資料傳輸終端機，以快速安全地將資料上傳至 Amazon S3 服務。

使用資料傳輸終端機的技術需求

在資料傳輸終端機排定保留之前，您需要確保擁有連線至網路所需的設備和組態。如需最佳的網路連線和體驗，請參閱下列準則。

設備

您必須攜帶可攜式裝置進行連線，包括監視器、鍵盤、滑鼠和電腦或筆記型電腦，以用於排定的保留。

您的硬體必須能夠使用光纖 (L4) 連線

> **Note**
>
> 作為資料安全最佳實務，請確定您的資料在您帶至資料傳輸終端機的儲存裝置上經過加密和保護，並在使用資料傳輸終端機設施時套用資料加密政策。如需詳細資訊，請參閱 AWS 資料傳輸終端機的安全性

網路需求

確保您的上傳裝置、伺服器或設備（筆記型電腦）已準備好連線至網路，且支援 DHCP。為了獲得最佳資料上傳體驗，您應該有下列項目：

- 100G QSFP28 LR4 (100GBASE-LR4) 光學 QSFP 收發器，與資料傳輸終端設施中提供的光纖纜線連接的 NIC 和 LC 連接器相容。
- IP 地址自動組態 DHCP 已啟用。DNS 伺服器由 DHCP 自動指派。
- Up-to-date軟體和 NIC 驅動程式。

效能最佳化

若要在使用 AWS 資料傳輸終端機時最大化輸送量，請考慮下列建議。

- 建議的硬體：
  - 100 Gbps 網路介面卡
  - 16 核心 CPU
  - 128 GB RAM

  - RAID 陣列中的多個 NVME SSD 磁碟機
- 使用 AWS Common Runtime (AWS CRT) 程式庫來使用 AWS Command Line Interface 或 AWS SDK 上傳。

  透過設定以下參數來最佳化 Amazon S3 傳輸設定。在 AWS 組態檔案中的頂層`s3`索引鍵下設定這些值，預設位置 `~/.aws/config`。

```
[default]
s3 =
    preferred_transfer_client = crt
    target_bandwidth = 100Gb/s
    max_concurrent_requests = 20
    multipart_chunksize = 16MB
```

  請注意，所有 Amazon S3 組態值都會縮排並在最上層`s3`金鑰下巢狀化。

  - 選用：您可以使用 `aws configure set`命令以程式設計方式設定上述值。例如，若要設定預設設定檔的上述值，您可以改為執行下列命令：

```
aws configure set default.s3.preferred_transfer_client crt
aws configure set default.s3.target_bandwidth 100Gb/s
aws configure set default.s3.max_concurrent_requests 20
aws configure set default.s3.multipart_chunksize 16MB
```

- 若要以程式設計方式為預設以外的設定檔設定這些值，請提供 `--profile`旗標。例如，若要設定名為 之設定檔的組態`test-profile`，請執行如下範例的 命令。

```
aws configure set s3.max_concurrent_requests 20 --profile test-profile
```

- 在裝置上啟用 BBR (Linux) 以提高輸送量。

```
sysctl -w net.core.default_qdisc=fq
sysctl -w net.ipv4.tcp_congestion_control=bbr
```

其他資訊

如需 AWS 命令列 Amazon S3 組態以最佳化網路連線和效能的詳細資訊，請參閱下列資源。

- AWS CLI 命令參考中的 AWS CLI Amazon S3 組態

- 在適用於 Java 的 Amazon S3Amazon AppStream 開發套件中使用高效能的 Amazon S3 用戶端：AWS CRT 型用戶端 S3Amazon AppStream
- 如何在 AWS 知識中心使用 AWS CLI 將大型檔案上傳至 Amazon S3 時最佳化效能？

開始使用

透過在其中一個資料傳輸終端機設施進行保留，開始使用遠端資料傳輸到您的 AWS 雲端 服務。首先，您將需要資料傳輸終端機設施和 AWS 企業帳戶支援的設備。

在排程資料傳輸終端機保留之前，請先檢閱本指南的 使用資料傳輸終端機的技術需求區段，以確保您的設備具有資料傳輸的最佳組態。並非所有資料儲存裝置和網路連線設備都與套件中提供的光纖網路連線相容。

當您註冊 時 AWS，您的 AWS 帳戶 會自動註冊 中的所有服務 AWS，包括資料傳輸終端機。您只需支付實際使用服務的費用。

若要設定資料傳輸終端機，請使用下列各節中的步驟。

當您註冊 AWS 並設定資料傳輸終端機時，您可以選擇變更 中的顯示語言 AWS Management Console。如需詳細資訊，請參閱《AWS Management Console 入門指南》中的變更 AWS Management Console的語言。

擁有 後 AWS 帳戶 ，您就可以存取資料傳輸終端機。如需設定和使用 AWS 資料傳輸終端機的詳細資訊，請參閱 排程資料傳輸終端機保留。

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，以及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 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權 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。

排程資料傳輸終端機保留

若要開始使用 AWS 資料傳輸終端機，您需要擁有 AWS 帳戶 並登入 https：//https://console.aws.amazon.com/datatransferterminal 的資料傳輸終端機主控台。登入 Data Transfer Terminal 主控台後，您可以查看現有的保留或進行新的保留。若要排程保留，您需要執行下列動作：

1. 建立轉接團隊。您將需要建立指定的使用者群組來建立保留，並存取資料傳輸終端機設施以進行資料傳輸。若要進一步了解此主題，請參閱 建立轉接團隊。
2. 您的團隊設定完成後，您需要將人員新增至其中。若要進一步了解如何將人員新增至您的轉接團隊，請參閱新增人員。
3. 程序擁有者可以與帳戶中的團隊排程資料傳輸。如需如何排程保留的詳細資訊，請參閱 指定保留詳細資訊。
4. 在提交您的請求之前，請確定保留的詳細資訊正確無誤。提交後，至少 24 小時內無法修改保留請求。如需詳細資訊，請參閱檢閱和確認您的保留。

處理並確認保留後，您的傳輸團隊將能夠在排定的時間存取資料傳輸終端機設施。如需詳細資訊，請參閱在資料傳輸終端機設施進行資料傳輸。

建立轉接團隊

若要存取資料傳輸終端機設施，您需要在 中排程保留 AWS Management Console。登入您的 AWS 帳戶 以存取資料傳輸終端機主控台，並完成下列步驟來排程您的保留。

1. 從資料傳輸終端機首頁中，選取開始使用按鈕。
2. 如果您尚未在帳戶中設定轉接團隊，則會停用建立保留按鈕。您需要建立並命名 Transfer 團隊才能開始。

   a. 選取建立轉接團隊按鈕。

   b. 為團隊命名。

      - 名稱長度必須介於 2 到 64 個字元之間，以字母或數字開頭。
      - 僅使用字母、數字、句點和破折號。無法辨識特殊字元。
      - 請勿包含任何敏感的識別資訊。

   c. 建立轉接團隊描述。

      - 提供有助於識別團隊的描述，例如描述團隊在特定時段、行銷活動或專案的目的。

d. 選取建立轉接團隊按鈕。

您將會返回轉接團隊頁面，而新建立的團隊會顯示在轉接團隊區段下。

更新資料傳輸終端機帳戶的傳輸團隊

若要設定新的轉接團隊，請參閱本指南的 排程資料傳輸終端機保留一節。

若要修改或移除轉接團隊，請執行下列動作：

1. 在轉接團隊頁面上，選取您要修改的轉接團隊。
2. 若要修改轉接團隊名稱和描述，請選取編輯按鈕。
3. 若要新增或移除人員，請選取人員索引標籤，並完成本常見問答集中如何修改、新增或移除我的帳戶？一節所述的步驟。
4. 若要新增或取消所選轉接團隊的保留，請參閱此常見問答集的 更新資料傳輸終端機帳戶上的人員一節。

新增人員

將程序擁有者和資料傳輸專家新增至您的傳輸團隊，以設定資料傳輸並存取資料傳輸終端機設施。若要將人員新增至您的轉接團隊，請執行下列動作：

1. 在轉接團隊頁面上，從轉接團隊區段中列出的轉接團隊卡中選取所需的轉接團隊卡。轉移團隊的摘要頁面隨即顯示。
2. 選擇人員索引標籤，然後註冊人員按鈕，將人員新增至轉接團隊。
3. 在註冊人員頁面上，使用您要新增至轉接團隊之人員的必要資訊完成欄位。

   a. 人員別名：建立唯一的別名以識別人員。

      - 別名用於識別人員，同時保護其身分。
      - 長度上限為 64 個字元，並包含字母、數字和破折號。
      - 不允許特殊字元。

   b. 名字：提供該人員在其政府核發的身分證件上顯示的名字。

   c. 姓氏：提供該人員的姓氏或姓氏，其顯示在其政府核發的身分證明上。

   d. 電子郵件地址：包含良好的電子郵件地址，供接收保留資訊和存取資料傳輸終端機設施的指示的人員使用。

4. 選取註冊人員按鈕，以完成將人員新增至轉接團隊。

更新資料傳輸終端機帳戶上的人員

目前不支援在資料傳輸終端機主控台中修改您帳戶中的現有人員。 AWS 資料傳輸終端機程序擁有者目前只能新增或刪除人員。

若要從您的資料傳輸終端機帳戶移除人員，請執行下列動作：

1. 在轉接團隊頁面上，選取與您要移除的人員相關聯的轉接團隊。
2. 在選取的轉接團隊的摘要頁面上，選取人員索引標籤。
3. 按一下您要移除的別名旁的選項按鈕。請注意，只有在刪除其設定檔時，您才能看到該人員的別名。
4. 選取刪除按鈕。此時會顯示警告，以確認所選人員的預期動作。按一下刪除按鈕以繼續。主控台頂端會出現橫幅，確認已成功刪除人員。

指定保留詳細資訊

下列指示會逐步解說如何在 中排程您的資料傳輸終端機保留 AWS Management Console。如需使用資料傳輸終端機設施的詳細資訊，請參閱 進行資料傳輸。

1. 在即將進行的保留索引標籤中選取保留按鈕。
2. 完成指定保留詳細資訊頁面上的欄位。

    a. 轉接團隊選擇：選取為預設值的轉接團隊會先出現。如果您想要選擇不同的團隊，請按一下下拉箭頭，從可用的轉接團隊清單中選擇。

    b. 程序擁有者：選取您要負責管理保留的人員別名。

    - 保留只允許一個程序擁有者，而且他們必須是 上的授權人員 AWS 帳戶。

      程序擁有者也可以納入為資料傳輸專家之一，以執行資料傳輸活動。

    c. 資料傳輸專家：選取要存取資料傳輸終端機設施的人員，以完成資料傳輸活動。您可以視需要選取多個人員。

    - 最佳實務是將傳輸團隊限制為不超過四 (4) 名資料傳輸專家。

    d. 資料傳輸終端機資訊：指定資料傳輸終端機設施、所需的日期和資料傳輸工作階段的特定時間。

i. 資料傳輸終端機設施：按一下下拉式箭頭以選取資料傳輸終端機設施。

> **Note**
>
> 保留時只會提供設施描述。其他位置資訊將在保留確認電子郵件中提供。

ii. 資料傳輸終端日期和時間：按一下搜尋保留的日期和時間欄位，以檢視行事曆並排程保留。

- 必須至少提前 24 小時預訂，且不可超過六 (6) 個月，且最長不得超過六 (6) 小時。如有必要，單一保留可能會跨越超過一天，以考慮夜間案例。
- 時間使用 24 小時制表示，並且只能以整小時增量保留。
- 若要進行連續保留，您必須在每個資料傳輸工作階段之間建立至少一個小時的個別保留。
- 如需詳細資訊，請參閱排程考量事項。

3. 確認保留詳細資訊正確無誤，然後選取建立按鈕以繼續。這將帶您前往確認頁面，其中提供保留的摘要。

檢閱和確認您的保留

指定保留的詳細資訊後，請選取下一步按鈕以繼續查看概觀頁面。在檢閱和建立頁面上檢閱資料傳輸終端機保留請求的詳細資訊。

- 如果您對請求感到滿意，請選取建立按鈕。
- 如果您需要變更保留，請選取上一個按鈕。

提交保留請求後，程序擁有者將收到一封電子郵件，確認請求已收到並正在處理中。一旦請求獲得核准，另一封電子郵件將確認保留，並提供尋找和存取資料傳輸終端設施的說明。如需有關存取資料傳輸終端機設施的資訊，請參閱 進行資料傳輸。

變更您的保留

在對資料傳輸終端機保留請求進行任何變更之前，有 24 小時的處理期間。

在處理期間之後，若要檢視、編輯或刪除您的保留，請導覽至 主控台中的轉接團隊頁面。

1. 在團隊的卡片上找到並選取所需的保留。

2. 按一下動作功能表，然後選取所需的動作。
   - 檢視：選取檢視選項可讓您檢視保留的詳細資訊，包括日期、時間、位置和指派的人員。
   - 編輯：您可以修改保留的詳細資訊，包括日期、時間、位置和指派的人員。請注意，變更必須在所需的保留日期前 24 小時進行，而且不會立即接受和套用修訂。您的程序擁有者將收到更新請求的確認。
   - Delete：刪除選項可讓您取消保留。取消請求必須在排定的保留日期前至少 24 小時提出。程序擁有者將在請求核准時收到取消保留的確認。

在資料傳輸終端機設施進行資料傳輸

資料傳輸終端機是安全的共同擁有位置，可提供對 AWS 網路的安全存取。若要存取資料傳輸終端機設施，請確定您有一個確認電子郵件，其中包含位置描述和存取指示。如需存取和使用資料傳輸終端機設施的詳細資訊，請參閱下列主題。

主題

要帶什麼

資料傳輸專家應提供執行資料傳輸所需的項目，例如筆記型電腦、隨身碟、固態硬碟 (SSDs) 和 AWS Snowball Edge。確保您的設備已最佳化，以使用資料傳輸終端機設施的光纖網路纜線。如需最佳設備和組態的詳細資訊，請參閱使用資料傳輸終端機的技術需求。

您負責安裝、使用和移除您和隨附的資料傳輸專家帶入資料傳輸終端設施的設備和項目。離開時，必須移除任何帶入套件的物件。 AWS 資料傳輸終端機不負責忘記或遺失的項目。

資料傳輸終端機設施實體地址

不會提供資料傳輸終端機設施的實體地址。相反地，保留中指定的流程擁有者和資料傳輸專家將收到一封電子郵件，其中包含可搜尋的資料傳輸終端機設施公有名稱。 AWS 資料傳輸終端機使用與 相同的位置識別系統 AWS Direct Connect ，因此您可以在網際網路上搜尋公有名稱以尋找資料傳輸終端機設施。如果您沒有包含此資訊的電子郵件，請與您的 AWS 資料傳輸終端機帳戶管理員確認您已包含在傳輸團隊中，而且您的電子郵件資訊正確無誤。

存取 建置

若要存取資料傳輸終端機設施，每位資料傳輸專家都必須提供身分證明或政府核發的 ID。進入建築物後，安全人員會護送您前往資料傳輸終端機套件。

資料傳輸終端機套件中的預期設備。

每個資料傳輸終端機設施應只具有兩 (2) 條光纖纜線、桌或桌和椅子。如果房間中有任何其他設備或項目，支援請立即向 報告。

疑難排解網路連線問題

如果您在使用 AWS 資料傳輸終端機時遇到連線至網路的問題，例如無法連線網際網路或連線速度緩慢，請考慮下列疑難排解秘訣。

主題

設備連線問題

如果您在資料傳輸終端機套件中建立實體連線時遇到困難，請考慮下列事項：

- 每個資料傳輸終端機設施都會有兩 (2) 條單模 LC 光纖纜線。如果其中一條或兩條纜線遺失，請立即聯絡 AWS Support。
- 如果一條光纖纜線無法運作，請嘗試先滾動纜線。如果您仍然無法與第一條纜線連接，請嘗試使用另一條纜線。

如果您仍然無法使用纜線進行連線，請立即聯絡 AWS Support。

連線疑難排解

如果您能夠連接設備，但無法連線到網路，請嘗試下列疑難排解建議。

- 確認您的設備組態符合指定的網路需求。如需詳細資訊，請參閱使用資料傳輸終端機的技術需求
- 切換到其他光纖纜線進行連線。
- 重新啟動您的裝置，同時保持光纖纜線的連接。
- 在裝置上執行基本網路診斷，以確保下列事項：
  - DHCP 已啟用
  - IP 地址會指派給連線的網路界面
  - DNS 伺服器已設定
  - 系統時鐘與 NTP 同步

如果您仍然無法連線，請聯絡 AWS Support，並根據裝置上執行的作業系統 (OS) 提供以下輸出。

Linux/UNIX

- 在終端機或命令列界面 (CLI) 中取得 IP 地址和路由資訊。確認 IP 地址已指派給網路介面，且具有預設閘道地址的預設路由會新增至路由表中。

```
ip address show
ip route show
```

  - 或者，如果 iproute2 未安裝在裝置上，且ip命令無法使用，請使用下列命令：

```
ifconfig
netstat -rn
```

- 收集 DNS 伺服器資訊。這應該會顯示兩個以nameserver關鍵字開頭的 IP 地址。

```
cat /etc/resolv.conf
```

- 收集基本連線測試的輸出。default_gateway_address 以指派的預設閘道 IP 地址取代 。

```
ping -c 5 <default_gateway_address>
ping -c 5 s3.amazonaws.com
traceroute s3.amazonaws.com
```

- 收集 HTTPS 連線測試的輸出。下列命令應會顯示來自 Amazon S3 的HTTP 200 OK回應。

```
curl -i https://s3.amazonaws.com/ping
```

Windows

- 在命令提示中取得 IP 地址、路由和 DNS 伺服器資訊。確認 IP 地址已指派給網路介面、兩個已指派的 DNS 伺服器，以及具有預設閘道地址的預設路由已新增至路由表中。

```
ipconfig /all
route print
```

- 在命令提示字元中收集基本連線測試的輸出。將 取代default_gateway_address為指派的預設閘道的 IP 地址。

```
ping <default_gateway_address>
ping s3.amazonaws.com
tracert s3.amazonaws.com
```

- 在 PowerShell 中收集 HTTPS 連線測試的輸出。下列命令應會顯示HTTP 200 OK回應。

```
Invoke-WebRequest -Uri "https://s3.amazonaws.com/ping"
```

網路輸送量

測量網路中實際資料傳輸率的網路輸送量可能會受到各種因素的影響。下列內容可能會影響您的資料傳輸速度：

- 硬體：上傳資料時，裝置的硬體元件可能會導致連線速度降低。裝置中使用的 CPU 和磁碟可能會達到其效能限制。請考慮在 RAID 陣列中使用 NVME SSDs。請務必使用 AWS CRT 程式庫以獲得更好的效能並降低 CPU 用量。
- 加密負荷：安全傳輸，例如 HTTPS，因為加密負荷而增加處理時間。
- 延遲：延遲是指資料封包從來源傳輸到目的地所需的時間。上傳到不同地理區域的 Amazon S3 儲存貯體時，可以觀察到高延遲，這可能會導致資料傳輸延遲和輸送量降低。最佳實務是盡可能在相同區域內進行資料傳輸。
- 封包遺失：遺失的封包需要重新傳輸，從而減慢資料傳輸速度。

AWS 資料傳輸終端機的安全性

AWS 資料傳輸終端機提供安全的環境，讓您往返 進行資料傳輸 AWS 雲端。如同任何其他實體網路光纖連線，資料傳輸終端機連線不提供預設加密。因此，您將負責強制執行資料加密最佳實務，以確保您的資料傳輸是安全的。

的雲端安全 AWS 是最高優先順序。身為 AWS 客戶，您可以受益於資料中心和網路架構，這些架構專為符合最安全敏感組織的需求而建置。

安全性是 AWS 與您之間的共同責任。共同責任模型將其描述為雲端的安全性和雲端中的安全性：

- 雲端的安全性 – AWS 負責保護在 中執行 AWS 服務的基礎設施 AWS 雲端。 AWS 也為您提供可安全使用的服務。在AWS 合規計畫中，第三方稽核人員會定期測試和驗證我們安全的有效性。若要了解適用於 AWS 資料傳輸終端機的合規計劃，請參閱AWS 合規計劃的 服務範圍。
- 雲端的安全性 – 您的責任取決於您使用 AWS 的服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件可協助您了解如何在使用資料傳輸終端機時套用共同責任模型。下列主題說明如何在使用資料傳輸終端機服務時保護您的資料。您也會了解如何使用其他 AWS 服務來協助您監控和保護資料傳輸終端機資源。

主題

- AWS 資料傳輸終端機中的資料保護
- 資料傳輸終端機的身分和存取管理
- AWS 資料傳輸終端機的合規驗證
- AWS 資料傳輸終端機的彈性
- 在資料傳輸終端機中記錄和監控
- AWS 資料傳輸終端機中的基礎設施安全性

AWS 資料傳輸終端機中的資料保護

AWS 共同責任模型適用於資料傳輸 AWS 終端機中的資料保護。如此模型所述， AWS 負責保護執行所有 的 全球基礎設施 AWS 雲端。您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務 的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱資料隱私權常見問

答集。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全性部落格上的 AWS 共同的責任模型和 GDPR 部落格文章。

基於資料保護目的，我們建議您保護 AWS 帳戶 登入資料，並使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用 設定 API 和使用者活動記錄 AWS CloudTrail。如需有關使用 CloudTrail 追蹤擷取 AWS 活動的資訊，請參閱AWS CloudTrail 《 使用者指南》中的使用 CloudTrail 追蹤。
- 使用 AWS 加密解決方案，以及其中的所有預設安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在 AWS 透過命令列界面或 API 存取 時需要 FIPS 140-3 驗證的密碼編譯模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-3。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用資料傳輸終端機或使用主控台、API AWS CLI、 AWS SDKs的其他 AWS 服務 時。您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供外部伺服器的 URL，我們強烈建議請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

資料加密

AWS 資料傳輸終端機可讓您存取高速網路連線，以便在自我管理儲存系統和 AWS 儲存服務之間安全地傳輸資料。傳輸中儲存資料的加密方式，部分取決於在裝置上啟用的政策，以及傳輸資料的 服務。使用資料傳輸終端機的個人負責管理資料及其傳輸中加密。

靜態加密

AWS 資料傳輸終端機會加密所有靜態資料。

資料傳輸終端機只會擷取保留所需的資料，包括指定參加和排程保留之個人的名字和姓氏和電子郵件地址。此資料收集的目的是確認保留詳細資訊，並確保存取房間以執行資料傳輸。此交易資訊會備份不超過 35 天，不過， AWS 帳戶資訊會保留 10 年。

傳輸中加密

AWS 資料傳輸終端機不會加密傳輸中的資料。當您與資料傳輸終端 API 端點互動以在主控台中設定傳輸團隊、新增人員和排程保留時，資料會在encrypted-in-transit。作為 AWS 共同責任模型的一部分，您可以選擇如何 AWS 服務 透過資料傳輸終端機連線至 。我們強烈建議您選擇 AWS 服務 使用強式encryption-in-transit來連線至 ，例如 TLS 1.2 和 1.3。

例如，使用 Amazon S3 儲存貯體政策中的 `aws:SecureTransport`條件，透過 HTTPS (TLS) 僅使用加密連線，如以下儲存貯體政策所示。

```
{
 "Version": "2012-10-17",
    "Statement": [{
        "Sid": "RestrictToTLSRequestsOnly",
        "Action": "s3:",
        "Effect": "Deny",
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket",
            "arn:aws:s3:::amzn-s3-demo-bucket/"
        ],
        "Condition": {
            "Bool": {
                "aws:SecureTransport": "false"
            }
        },
        "Principal": "*"
    }]
}
```

若要進一步了解使用 Amazon S3 AWS 服務等其他 傳輸中的資料加密，請參閱《Amazon S3 使用者指南》中的使用伺服器端加密保護資料。

金鑰管理

AWS 資料傳輸終端機不會直接支援客戶受管金鑰。針對您在資料傳輸終端機保留期間連線 AWS 的服務，使用可用的客戶受管金鑰支援。請參閱 AWS Key Management Service 開發人員指南中的 AWS KMS 金鑰一節，進一步了解客戶受管金鑰以及如何加密靜態資料。

網際網路流量隱私權

透過發佈的服務 APIs存取資料傳輸終端機主控台。資料傳輸終端機資源獨立於虛擬私有雲端 (VPC)。

資料傳輸終端機的身分和存取管理

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身分驗證 （ 登入 ） 和授權 （ 具有許可 ），以使用資料傳輸終端資源。IAM 是 AWS 服務 您可以免費使用的 。

主題

目標對象

使用方式 AWS Identity and Access Management (IAM) 會有所不同，具體取決於您在資料傳輸終端機中執行的工作。

服務使用者 – 如果您使用資料傳輸終端機服務來執行任務，您的管理員會為您提供所需的登入資料和許可。當您使用更多資料傳輸終端機功能來執行工作時，您可能需要額外的許可。了解存取許可的管理方式可協助您向管理員請求正確的許可。如果您無法存取資料傳輸終端機中的功能，請參閱 對 AWS 資料傳輸終端機身分和存取進行故障診斷。

服務管理員 – 如果您在公司負責資料傳輸終端機資源，您可能擁有資料傳輸終端機的完整存取權。您的任務是判斷服務使用者應存取的資料傳輸終端機功能和資源。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資料傳輸終端機使用 IAM，請參閱 資料傳輸終端機如何與 IAM 搭配使用。

IAM 管理員 – 如果您是 IAM 管理員，建議您了解如何撰寫政策以管理資料傳輸終端機存取權的詳細資訊。若要檢視您可以在 IAM 中使用的資料傳輸終端機身分型政策範例，請參閱 AWS 資料傳輸終端機的身分型政策範例。

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。

根據您的使用者類型，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

當您建立 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

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

聯合身分是您企業使用者目錄、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登入資料 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，也可以連接並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。只有在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 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，當與身分或資源相關聯時， 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 API AWS 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。委託人可以包含帳戶、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 中組織或組織單位 (OU) 的最大許可 AWS Organizations。 AWS Organizations 是一種服務，用於分組和集中管理您企業擁有 AWS 帳戶 的多個 。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，包括支援 RCPs AWS 服務 的 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 在涉及多個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。

資料傳輸終端機如何與 IAM 搭配使用

在您使用 IAM 管理資料傳輸終端機的存取權之前，請先了解哪些 IAM 功能可與資料傳輸終端機搭配使用。

IAM 功能	資料傳輸終端機支援
身分型政策	是
資源型政策	否
政策動作	是
政策資源	是

IAM 功能	資料傳輸終端機支援
政策條件索引鍵	是
ACL	否
ABAC(政策中的標籤)	否
臨時憑證	是
主體許可	否
服務角色	否
服務連結角色	否

若要全面了解資料傳輸終端機和其他 AWS 服務如何與大多數 IAM 功能搭配使用，請參閱《AWS IAM 使用者指南》中的與 IAM 搭配使用的 服務。

資料傳輸終端機的身分型政策

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。

資料傳輸終端機的身分型政策範例

若要檢視資料傳輸終端機身分型政策的範例，請參閱 AWS 資料傳輸終端機的身分型政策範例。

資料傳輸終端機內的資源型政策

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。委託人可以包含帳戶、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。當主體和資源位於不同位置時 AWS 帳戶，信任帳戶中的 IAM 管理員也必須授予主體實體（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。

資料傳輸終端機的政策動作

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，哪個主體在什麼条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。

若要查看資料傳輸終端機動作的清單，請參閱服務授權參考中的AWS 資料傳輸終端機定義的動作。

Data Transfer Terminal 中的政策動作在動作之前使用下列字首：

```
datatransferterminal
```

若要在單一陳述式中指定多個動作，請用逗號分隔。

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

若要檢視資料傳輸終端機身分型政策的範例，請參閱 AWS 資料傳輸終端機的身分型政策範例。

資料傳輸終端機的政策資源

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": "*"
```

若要查看資料傳輸終端機資源類型及其 ARNs的清單，請參閱服務授權參考中的AWS 資料傳輸終端機定義的資源。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 資料傳輸終端機定義的動作。

若要檢視資料傳輸終端機身分型政策的範例，請參閱 AWS 資料傳輸終端機的身分型政策範例。

資料傳輸終端機的政策條件索引鍵

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。

您也可以在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的條件金鑰。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。

若要查看資料傳輸終端機條件索引鍵的清單，請參閱《服務授權參考》中的AWS 資料傳輸終端機的條件索引鍵。若要了解您可以使用條件索引鍵的動作和資源，請參閱AWS 資料傳輸終端機定義的動作。

若要檢視資料傳輸終端機身分型政策的範例，請參閱 AWS 資料傳輸終端機的身分型政策範例。

資料傳輸終端機中的 ACLs

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 與資料傳輸終端機

支援 ABAC （政策中的標籤）：否

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)。

搭配資料傳輸終端機使用臨時憑證

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 ，則會使用暫時登入資料。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。

資料傳輸終端機的跨服務主體許可

支援轉寄存取工作階段 (FAS)：否

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 請求時的政策詳細資訊，請參閱轉發存取工作階段。

資料傳輸終端機的服務角色

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資料傳輸終端機功能。只有在資料傳輸終端機提供指引時，才能編輯服務角色。

資料傳輸終端機的服務連結角色

支援服務連結角色：否

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 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。

如需建立或管理服務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。

AWS 資料傳輸終端機的身分型政策範例

根據預設，使用者和角色沒有建立或修改資料傳輸終端機資源的許可。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，包括每種資源類型的 ARNs 格式，請參閱服務授權參考中的AWS 資料傳輸終端機的動作、資源和條件金鑰。

主題

- 政策最佳實務
- 使用資料傳輸終端機主控台
- 允許使用者檢視他們自己的許可

政策最佳實務

身分型政策會判斷您帳戶中的某人是否可以建立、存取或刪除資料傳輸終端機資源。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 等使用服務動作 AWS 服務，您也可以使用條件來授予其存取權 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。

使用資料傳輸終端機主控台

若要存取 AWS 資料傳輸終端機主控台，您必須擁有一組最低許可。這些許可必須允許您列出和檢視中資料傳輸終端機資源的詳細資訊 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資料傳輸終端機主控台，也請將資料傳輸終端機*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 主控台或使用 或 AWS CLI 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:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
```

```
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

對 AWS 資料傳輸終端機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資料傳輸終端機和 IAM 時可能遇到的常見問題。

主題

- 我無權在資料傳輸終端機中執行動作
- 我想要允許 以外的人員 AWS 帳戶 存取我的資料傳輸終端機資源

我無權在資料傳輸終端機中執行動作

如果您無法在 AWS 資料傳輸終端機主控台中檢視或排程保留，您可能沒有必要的許可。請聯絡您的帳戶管理員，以設定授予您存取權和適當許可的 IAM 身分政策。

我想要允許 以外的人員 AWS 帳戶 存取我的資料傳輸終端機資源

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：

- 若要了解資料傳輸終端機是否支援這些功能，請參閱資料傳輸終端機如何與 IAM 搭配使用。
- 若要了解如何在您擁有 AWS 帳戶 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 中為 IAM 使用者提供存取權。
- 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。
- 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。

資料傳輸終端機 API 參考：動作和資源

建立 AWS Identity and Access Management (IAM) 政策時，此頁面可協助您了解 AWS 資料傳輸終端機 API 操作之間的關係、您可以授予執行許可的對應動作，以及您可以授予許可 AWS 的資源。

一般而言，以下是將資料傳輸終端機許可新增至政策的方式：

- 在 `Action`元素中指定動作。值包含`datatransferterminal:`字首和 API 操作名稱。例如 `datatransferterminal:CreateTask`。
- 在 `Resource`元素中指定與 動作相關的 AWS 資源。

您也可以在資料傳輸終端機政策中使用 AWS 條件金鑰。如需金鑰的完整清單 AWS ，請參閱《IAM 使用者指南》中的可用金鑰。

資料傳輸終端機 API 操作和對應的動作

CreateTransferTeam

動作：`datatransferterminal:CreateTransferTeam`

資源：None

GetTransferTeam

動作：`datatransferterminal:GetTransferTeam`

資源：`arn:aws::$`*`Partition`*`:datatransferterminal:$`*`Region`*`:$`*`Account`*`:transfer-team/$`*`TransferTeamId`*

UpdateTransferTeam

動作：datatransferterminal:UpdateTransferTeam

資源：arn:aws::$*Partition*:datatransferterminal:$*Region*:$*Account*:transfer-team/$*TransferTeamId*

DeleteTransferTeam

動作：datatransferterminal:DeleteTransferTeam

資源：arn:aws::$*Partition*:datatransferterminal:$*Region*:$*Account*:transfer-team/$*TransferTeamId*

ListTransferTeams

動作：datatransferterminal:ListTransferTeams

資源：None

RegisterPerson

動作：datatransferterminal:RegisterPerson

資源：arn:aws::$*Partition*:datatransferterminal:$*Region*:$*Account*:transfer-team/$*TransferTeamId*

GetPerson

動作：datatransferterminal:GetPerson

資源：arn:aws::$*Partition*:datatransferterminal:$*Region*:$*Account*:transfer-team/$*TransferTeamId*/person/$*PersonId*

相依動作：datatransferterminal:GetTransferTeam

相依資源：arn:aws::$*Partition*:datatransferterminal:$*Region*:$*Account*:transfer-team/$*TransferTeamId*

DeregisterPerson

動作：datatransferterminal:DeregisterPerson

資源：arn:aws::$*Partition*:datatransferterminal:$*Region*:$*Account*:transfer-team/$*TransferTeamId*/person/$*PersonId*

相依動作：datatransferterminal:GetTransferTeam

相依資源：arn:aws::$*Partition*:datatransferterminal:$*Region*:$*Account*:transfer-team/$*TransferTeamId*

ListPersons

動作：datatransferterminal:ListPersons

資源：arn:aws::$*Partition*:datatransferterminal:$*Region*:$*Account*:transfer-team/$*TransferTeamId*

CreateReservation

動作：datatransferterminal:CreateReservation

資源：arn:aws::$*Partition*:datatransferterminal:$*Region*:$*Account*:transfer-team/$*TransferTeamId*

相依動作：datatransferterminal:GetTransferTeam

相依資源：arn:aws::$*Partition*:datatransferterminal:$*Region*:$*Account*:transfer-team/$*TransferTeamId*

相依動作：datatransferterminal:GetPerson

相依資源：arn:aws::$*Partition*:datatransferterminal:$*Region*:$*Account*:transfer-team/$*TransferTeamId*/person/$*PersonId*

相依動作：datatransferterminal:GetFacility

相依資源：arn:aws::$*Partition*:datatransferterminal:::facility/$*FacilityId*

GetReservation

動作：datatransferterminal:GetReservation

資源：arn:aws::$*Partition*:datatransferterminal:$*Region*:$*Account*:transfer-team/$*TransferTeamId*/reservation/$*ReservationId*

相依動作：datatransferterminal:GetTransferTeam

相依資源：arn:aws::$*Partition*:datatransferterminal:$*Region*:$*Account*:transfer-team/$*TransferTeamId*

UpdateReservation

動作：datatransferterminal:UpdateReservation

資源：arn:aws::$*Partition*:datatransferterminal:$*Region*:$*Account*:transfer-team/$*TransferTeamId*/reservation/$*ReservationId*

相依動作：datatransferterminal:GetTransferTeam

相依資源：arn:aws::$*Partition*:datatransferterminal:$*Region*:$*Account*:transfer-team/$*TransferTeamId*

相依動作：datatransferterminal:GetPerson

相依資源：arn:aws::$*Partition*:datatransferterminal:$*Region*:$*Account*:transfer-team/$*TransferTeamId*/person/$*PersonId*

DeleteReservation

動作：datatransferterminal:DeleteReservation

資源：arn:aws::$*Partition*:datatransferterminal:$*Region*:$*Account*:transfer-team/$*TransferTeamId*/person/$*PersonId*

相依動作：datatransferterminal:GetTransferTeam

相依資源：arn:aws::$*Partition*:datatransferterminal:$*Region*:$*Account*:transfer-team/$*TransferTeamId*

ListReservations

動作：datatransferterminal:ListReservations

資源：arn:aws::$*Partition*:datatransferterminal:$*Region*:$*Account*:transfer-team/$*TransferTeamId*

ListFacilities

動作：datatransferterminal:ListFacilities

資源：None

GetFacility

動作：datatransferterminal:GetFacility

資源：arn:aws::$*Partition*:datatransferterminal:::facility/$*FacilityId*

GetFacilityAvailability

動作：datatransferterminal:GetFacilityAvailability

資源：arn:aws::$*Partition*:datatransferterminal:::facility/$*FacilityId*/availability

相依動作：datatransferterminal:GetFacility

相依資源：arn:aws::$*Partition*:datatransferterminal:::facility/$*FacilityId*/availability

AWS 資料傳輸終端機的合規驗證

若要了解 是否 AWS 服務 在特定合規計劃的範圍內，請參閱AWS 服務 合規計劃範圍內然後選擇您感興趣的合規計劃。如需一般資訊，請參閱 AWS Compliance Programs。

您可以使用 下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱在 中下載報告 AWS Artifact。

您使用 時的合規責任 AWS 服務 取決於資料的機密性、您公司的合規目標，以及適用的法律和法規。AWS 提供下列資源來協助合規：

- 安全合規與治理 - 這些解決方案實作指南內容討論了架構考量，並提供部署安全與合規功能的步驟。
- HIPAA 合格服務參考 – 列出 HIPAA 合格服務。並非所有 AWS 服務 都符合 HIPAA 資格。
- AWS 合規資源 – 此工作手冊和指南集合可能適用於您的產業和據點。
- AWS 客戶合規指南 – 透過合規的角度了解共同責任模型。本指南摘要說明跨多個架構 （包括國家標準技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準化組織 (ISO)) 保護 AWS 服務和映射指南至安全控制的最佳實務。
- 《AWS Config 開發人員指南》中的使用規則評估資源 – AWS Config 服務會評估資源組態符合內部實務、產業準則和法規的程度。
- AWS Security Hub – 這 AWS 服務 可讓您全面檢視其中的安全狀態 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱「Security Hub 控制參考」。
- Amazon GuardDuty – 這會監控您的環境是否有可疑和惡意活動，以 AWS 服務 偵測對您 AWS 帳戶、工作負載、容器和資料的潛在威脅。GuardDuty 可滿足特定合規架構所規定的入侵偵測需求，以協助您因應 PCI DSS 等各種不同的合規需求。

- AWS Audit Manager – 這 AWS 服務 可協助您持續稽核 AWS 用量，以簡化您管理風險的方式，以及符合法規和業界標準的方式。

AWS 資料傳輸終端機的彈性

AWS 全球基礎設施是以 AWS 區域 和 可用區域為基礎建置。 AWS 區域 提供多個實體隔離和隔離的可用區域，這些可用區域與低延遲、高輸送量和高備援聯網連接。透過可用區域，您可以設計與操作的應用程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域 和可用區域的詳細資訊，請參閱 AWS 全球基礎設施。

AWS 資料傳輸終端機可在全球各地使用。您可以連線到可從網際網路存取的任何 AWS 區域 。

在資料傳輸終端機中記錄和監控

AWS Data Transfer Terminal 已與 整合 AWS CloudTrail，此服務可提供使用者、角色或 AWS 服務在 Data Transfer Terminal 中採取之動作的記錄。CloudTrail 會將資料傳輸終端機的所有 API 呼叫擷取為事件。擷取的呼叫包括來自資料傳輸終端機主控台的呼叫，以及對資料傳輸終端機 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，包括資料傳輸終端機的事件。即使您未設定追蹤，依然可以透過 CloudTrail 主控台中的事件歷史記錄檢視最新事件。您可以使用 CloudTrail 所收集的資訊，判斷向資料傳輸終端機提出的請求、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」。

CloudTrail 中的資料傳輸終端機資訊

建立帳戶 AWS 帳戶 時，您的 上會啟用 CloudTrail。當活動在資料傳輸終端機中發生時，該活動會與事件歷史記錄中的其他服務 AWS 事件一起記錄在 CloudTrail 事件中。您可以在 中檢視、搜尋和下載最近的事件 AWS 帳戶。如需詳細資訊，請參閱「使用 CloudTrail 事件歷史記錄檢視事件」。

若要持續記錄 中的事件 AWS 帳戶，包括資料傳輸終端機的事件，請建立追蹤。線索能讓 CloudTrail 將日誌檔案交付至 Amazon S3 儲存貯體。依預設，當您在主控台中建立追蹤時，該追蹤會套用至所有的 AWS 區域。線索會記錄 AWS 分割區中所有區域的事件，並將日誌檔案傳送到您指定的 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
- 接收多個區域的 CloudTrail 日誌檔案和接收多個帳戶的 CloudTrail 日誌檔案

CloudTrail 會記錄所有資料傳輸終端機動作，並記錄在本指南的 資料傳輸終端機 API 參考：動作和資源區段中。

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：

- 是否使用根或 AWS Identity and Access Management (IAM) 使用者登入資料提出請求。
- 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。

了解資料傳輸終端機日誌檔案項目

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。

AWS 資料傳輸終端機中的基礎設施安全性

資料傳輸 AWS 終端機是受管服務，受到 Amazon Web Services：安全程序概觀白皮書中所述的 AWS 全球網路安全程序所保護。

您可以使用 AWS 發佈的 API 呼叫，透過網路存取資料傳輸終端機。用戶端必須支援 Transport Layer Security (TLS) 1.0 或更新版本。建議使用 TLS 1.2 或更新版本。用戶端也必須支援具備完美轉送私密 (PFS) 的密碼套件，例如臨時 Diffie-Hellman (DHE) 或橢圓曲線臨時 Diffie-Hellman (ECDHE)。現代系統(如 Java 7 和更新版本)大多會支援這些模式。

此外，請求必須使用存取金鑰 ID 和與 IAM 主體相關聯的私密存取金鑰來簽署。或者，您可以使用 AWS Security Token Service (AWS STS) 以產生暫時安全憑證以簽署請求。

Data Transfer Terminal 使用者指南的文件歷史記錄

下表說明 AWS 資料傳輸終端機使用者指南每個版本的重要變更。如需有關此文件更新的通知，您可以訂閱 RSS 摘要。

變更	描述	日期
初次出版	原始文件啟動日期。	2024 年 12 月
更新配置	文件配置和次要措辭和內容編輯的更新。	2025 年 1 月

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。