aws

使用者指南

Amazon Elastic File System

Amazon Elastic File System: 使用者指南

Table of Contents

Amazon Elastic File System 是什麼？

Amazon Elastic File System (Amazon EFS) 提供無伺服器、完全彈性的檔案儲存功能，讓您無需佈建或管理儲存容量和效能，即可分享檔案資料。Amazon EFS 可隨需擴展至 PB 級，而不會中斷應用程式，並可隨著您新增和移除檔案而自動擴展及縮減。因爲 Amazon EFS 採用簡單的 Web 服務介面，您可以快速輕鬆地建立和設定檔案系統。此服務會為您管理所有檔案儲存基礎設施，這表示您可以避免部署、修補和維護複雜檔案系統組態的複雜性。

Amazon EFS 支援網路檔案系統第 4 版 (NFSv4.1 和 NFSv4.0) 協定，因此您目前使用的應用程式和工具都可以與 Amazon EFS 無縫配合使用。Amazon EFS 可在大多數類型的 Amazon Web Services 運算實例中訪問，包括亞馬 Amazon EC2，Amazon ECS，Amazon EKS 和。 AWS Lambda AWS Fargate

此服務設計為具有高可擴展性、高可用性和高耐用性。Amazon EFS 提供下列檔案系統類型，以滿足您的可用性和耐久性需求：

- 地區 (建議) — 區域檔案系統 (建議使用) 以冗餘方式將資料儲存在同一個地理位置分隔的多個可用區域。 AWS 區域跨多個可用區域儲存資料可提供資料的持續可用性，即使一或多個可用區域中的一或多個 AWS 區域 可用區域無法使用。
- 單一區域 — 單一區域檔案系統會將資料儲存在單一可用區域內。將資料儲存在單一可用區域中，為資料提供持續的可用性。不過，在可用區域全部或部分遺失或損壞的情況下，儲存在這些類型檔案系統中的資料可能會遺失。

如需建立檔案系統類型的詳細資訊，請參閱 EFS 檔案系統類型。

Amazon EFS 提供各種工作負載所需的輸送量、IOPS 以及低延遲。EFS 檔案系統可擴展至 PB 級、提高輸送量水準、允許從運算執行個體大量平行存取資料。對於大部分的工作負載，我們建議使用預設模式，即一般用途效能模式和彈性輸送量模式。

- 一般用途 —「一般用途」效能模式非常適合延遲敏感的應用程式，例如 Web 服務環境、內容管理系統、主目錄和一般檔案服務。
- 彈性 — 彈性輸送量模式旨在自動擴展或縮減輸送量效能，以滿足工作負載活動的需求。

如需 EFS 效能和輸送量模式的詳細資訊，請參閱Amazon EFS 效能。

Amazon EFS 提供 file-system-access 語意，例如強大的資料一致性和檔案鎖定。如需詳細資訊，請參閱 在 Amazon EFS 中的資料一致性。Amazon EFS 也可讓您透過「可攜式作業系統介面」(POSIX) 的許可來支援控制檔案系統的存取。如需詳細資訊，請參閱 Amazon EFS 中的安全。

Amazon EFS 支援身分驗證、授權和加密功能，以滿足安全和合規要求。Amazon EFS 支援兩種檔案系統加密形式：傳輸中加密和靜態加密。您可在 Amazon EFS 檔案系統建立時啟用靜態資料加密。如果您這麼做，所有資料和中繼資料都會加密。當您掛載檔案系統時，可以啟用傳輸中加密。NFS 用戶端對 EFS 的存取由 AWS Identity and Access Management (IAM) 政策和網路安全政策 (例如安全群組) 控制。如需詳細資訊，請參閱Amazon EFS 的資料加密、Amazon Elastic File System 的身分與存取管理及控制 NFS 用戶端對 Amazon EFS 檔案系統的網路存取。

> **Note**
>
> 不支援使用 Amazon EFS 搭配以 Microsoft Windows 爲基礎的 Amazon EC2 執行個體。

您第一次使用 Amazon EFS 嗎？

若是第一次使用 Amazon EFS，建議您依序閱讀以下區段：

1. 如需 Amazon EFS 產品和定價概觀，請參閱 Amazon EFS。
2. 如需 Amazon EFS 的技術概觀，請參閱 Amazon EFS 如何運作。
3. 請嘗試入門的練習：
   - 開始使用
   - 演練

如果您想要進一步了解 Amazon EFS，以下主題會更詳細地討論此服務：

- 使用 Amazon EFS 資源
- 管理 Amazon EFS 檔案系統
- EFS S

Amazon EFS 如何運作

在下面內容中，您可以找到 Amazon EFS 運作方式，其實作詳細資訊和安全考量的說明。

主題

概觀

Amazon Elastic File System (EFS) 提供簡單的無伺服器 set-and-forget 彈性檔案系統。您可以使用 Amazon EFS 建立檔案系統，在您的 Amazon EC2 執行個體上掛載檔案系統，接著便可從檔案系統讀取並寫入 Amazon EC2 執行個體的資料。您可以使用網路檔案系統版本 4.0 和 4.1 (NFSv4) 通訊協定，在虛擬私有雲端 (VPC) 中掛載 Amazon EFS 檔案系統。我們建議您使用最新一代的 Linux NFSv4.1 用戶端，例如您可以在與 Amazon EFS 掛載輔助程式一起使用的最新 Amazon Linux、Amazon Linux 2、Red Hat、Ubuntu 和 macOS Big Sur AMIs 中找到這些用戶端。如需說明，請參閱安裝 Amazon EFS 工具。

如需支援此通訊協定的 Amazon EC2 Linux 和 macOS Amazon Machine Image (AMI) 清單，請參閱 NFS 支援。針對部分 AMI，必須先安裝 NFS 用戶端才能在 Amazon EC2 執行個體上掛載檔案系統。如需說明，請參閱安裝 NFS 用戶端。

您可以同時從多個 NFS 用戶端中存取 Amazon EFS 檔案系統，讓擴展範圍超過單一連線的應用程式可以存取檔案系統。在相同 AWS 區域 區域的多個可用區域中執行的 Amazon EC2 和其他 AWS 執行個體可以存取此檔案系統，因此許多使用者可以存取和共用共同的資料來源。

如需可 AWS 區域 在其中建立 Amazon EFS 檔案系統的清單，請參閱Amazon Web Services 一般參考。

若要在 VPC 中存取 Amazon EFS 檔案系統，您可以在 VPC 中建立一或多個掛載目標。

- 針對區域檔案系統，您可以在 AWS 區域的每個可用區域中建立掛載目標。
- 針對單區域檔案系統，您只能在與檔案系統相同的可用區域中建立單一掛載目標。

如需詳細資訊，請參閱 EFS 儲存類別。

掛載目標會提供 NFSv4 端點的 IP 地址，您可以在該端點上掛載 Amazon EFS 檔案系統。您將使用其 Domain Name Service (DNS) 名稱掛載您的檔案系統，該名稱會解析為與 EC2 執行個體所在相同可用區域中的 EFS 掛載目標 IP 地址。您可在 AWS 區域的每個可用區域中建立一個掛載目標。如果在您 VPC 中可用區域內有多個子網路，則您可在其中一個子網路中建立一個掛載目標。則在該可用區域的所有 EC2 執行個體都可以共用單一掛載目標。

> **Note**
>
> Amazon EFS 檔案系統可以掛載目標，但是這些掛載目標一次只能出現在一個 VPC 中。

掛載目標本身的設計具有高可用性。當您在設計高可用性且將容錯移轉到其他可用區域的應用程式時，請注意每個可用區域中的掛載目標 IP 地址和 DNS 都是靜態的，他們是多個資源的備份備援元件。

透過使用 DNS 名稱掛載檔案系統後，您可以像任何其他 POSIX 相容的檔案系統一樣使用它。如需有關 NFS 層級之許可和相關考量的資訊，請參閱 在網路檔案系統 (NFS) 層級處理使用者、群組和權限。

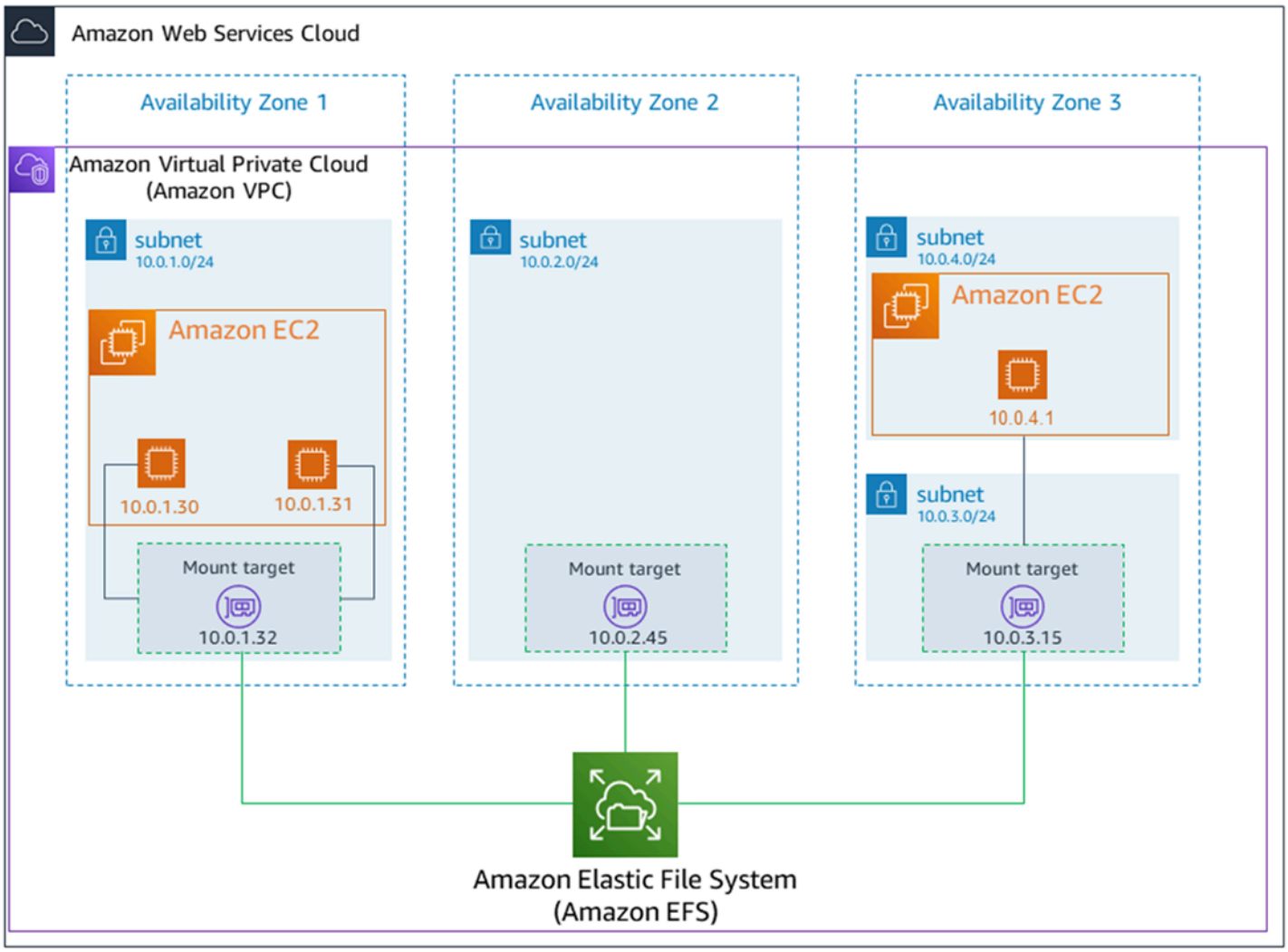
使用連接到 Amazon VPC 時，您可以將 Amazon EFS 檔案系統掛接到現場部署資料中心伺服器上，AWS Direct Connect 或者 AWS VPN 您可以在現場部署伺服器上掛載 EFS 檔案系統以將資料集遷移到 EFS、啟用雲端爆量案例，或將現場部署資料備份到 Amazon EFS。

如何使用 Amazon EFS 搭配 Amazon EC2

本區段說明 Amazon EFS 區域和單區域檔案系統如何掛載到 Amazon VPC 中的 EC2 執行個體上。

Amazon EFS 區域檔案系統

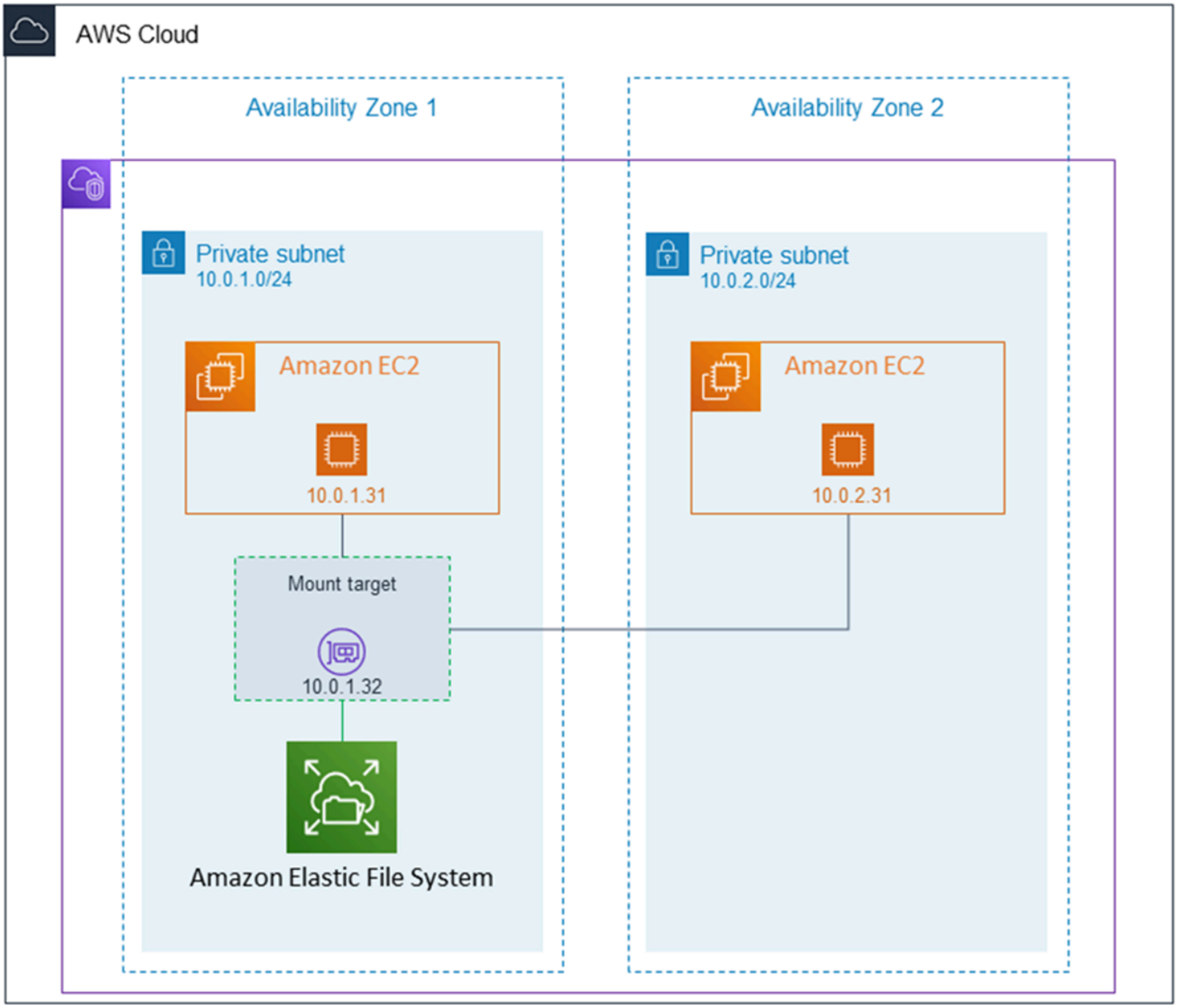
Amazon EFS 檔案系統設定在 AWS 區域的多個可用區域中，下圖顯示了存取該檔案系統的多個 EC2 執行個體。



在此圖例中，虛擬私有雲端 (VPC) 有三個可用區域。因爲檔案系統是「區域性」的，因此在每個可用區域都會建立一個掛載目標。出於效能和成本考量，我們建議您從同一可用區域內的掛載目標中存取檔案系統。其中一個可用區域有兩個子網路。不過，只在其中一個子網路中建立掛載目標。如需詳細資訊，請參閱 使用 EFS 掛載協助程式掛載 EFS 檔案系統。

Amazon EFS 單區域檔案系統

下圖顯示存取單區域檔案系統 (位於單一 AWS 區域的不同可用區域中) 的多個 EC2 執行個體。



在此圖例中，VPC 有兩個可用區域，每個區域都有一個子網路。由於檔案系統類型是單區域，因此只有一個掛載目標。出於更高效能和成本考量，我們建議您通過與掛載檔案系統的 EC2 執行個體位於相同可用區域的掛載目標來掛載檔案系統。

在此範例中，因爲在不同可用區域中存取掛載目標，所以位於 us-west-2c 可用區域中的 EC2 執行個體將爲此支付 EC2 資料存取費用。如需詳細資訊，請參閱 掛載單區域檔案系統。

Amazon EFS 如何搭配使用 AWS Direct Connect 和 AWS 受管 VPN

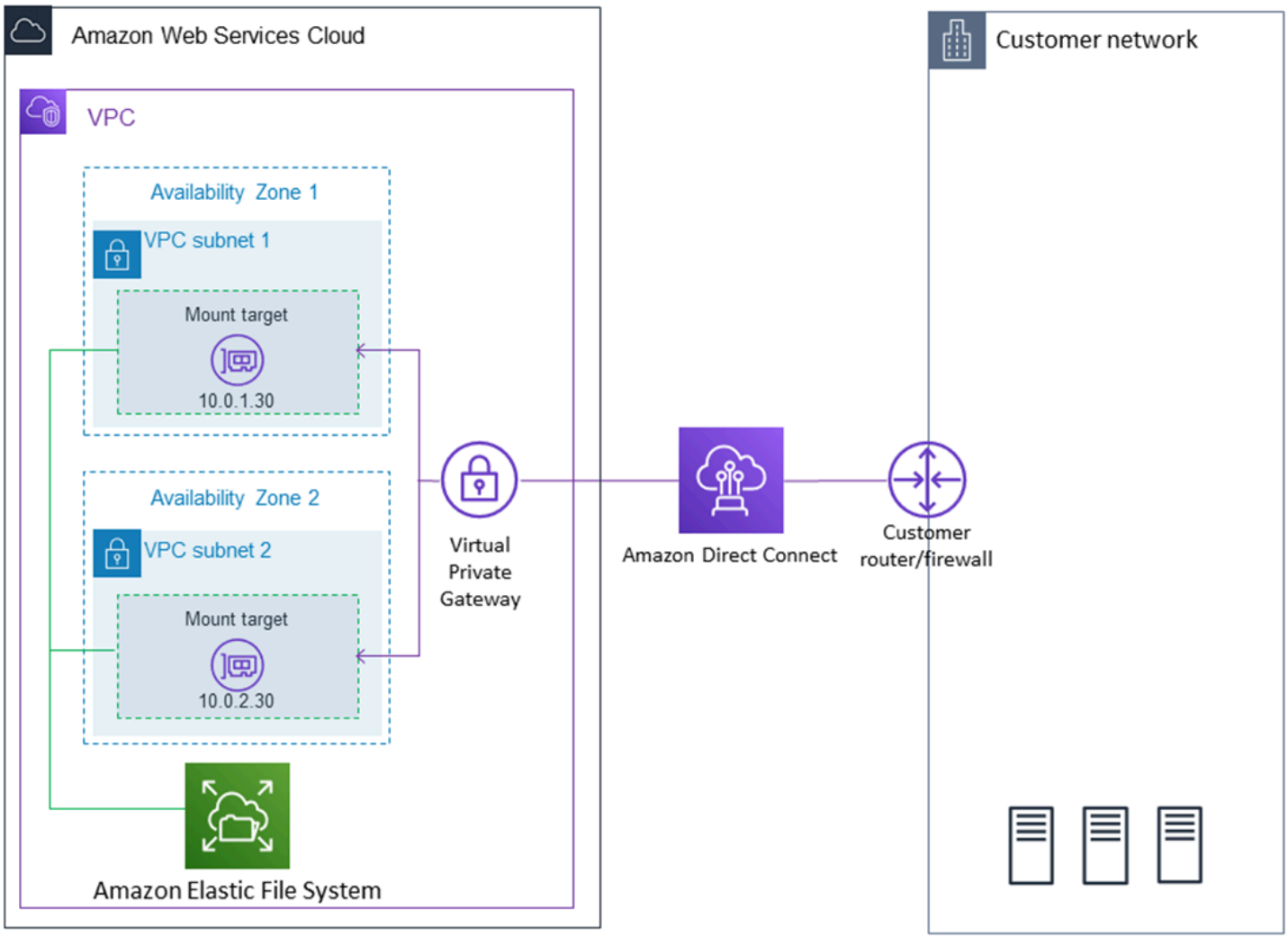
透過使用掛載在現場部署伺服器上的 Amazon EFS 檔案系統，您可以將現場部署資料遷移到 Amazon EFS 檔案系統中 AWS 雲端 託管的資料。您也可以利用爆量。換言之，您可以將資料從內部部署伺服器移入 Amazon EFS，並在 Amazon VPC 中的 Amazon EC2 執行個體機群上，分析該資料。然後，您便可以將結果永久儲存在您的檔案系統，或將該結果移回您的現場部署伺服器。

使用 Amazon EFS 搭配內部部署伺服器運作時，請謹記以下幾點考量：

- 您的現場部署伺服器必須是以 Linux 為基礎的作業系統。我們建議 Linux 核心版本 4.0 或更新版本。
- 為簡化說明，我們建議使用掛載目標 IP 地址 (而不是 DNS 名稱) 來在內部部署伺服器上掛載 Amazon EFS 檔案系統。

內部部署存取不會對 Amazon EFS 檔案系統產生額外成本。您需要支付 AWS Direct Connect 連線到 Amazon VPC 的費用。如需詳細資訊，請參閱 AWS Direct Connect 定價。

下圖示範如何從內部部署 (已掛載檔案的系統內部部署伺服器) 存取 Amazon EFS 檔案系統的範例。



如果您可以使用內部部署伺服器與 VPC 之間的 AWS Direct Connect 連線到達該裝載目標的子網路，則可以在 VPC 中使用任何裝載目標。若要從內部部署伺服器存取 Amazon EFS，請將規則新增至掛載目標的安全群組，以允許從內部部署伺服器到 NFS 連接埠 (2049) 的傳入流量。如需包括詳細程序的詳細資訊，請參閱 逐步解說：使用 AWS Direct Connect 和 VPN 建立和掛載內部部署的檔案系統。

Amazon EFS 如何使用 AWS Backup

若要為您的檔案系統提供全面的備份實作，您可以搭配使用 Amazon EFS AWS Backup。 AWS Backup 是一項全受管備份服務，可讓您輕鬆地跨雲端和內部部署 AWS 服務集中及自動化資料備份。您可以使用集中設定備份原則 AWS Backup，並監視 AWS 資源的備份活動。Amazon EFS 始終優先考慮檔案系統操作而不是備份操作。若要進一步瞭解如何使用備份 EFS 檔案系統 AWS Backup，請參閱備份 Amazon EFS 檔案系統。

實作摘要

在 Amazon EFS 中，檔案系統是一項主要資源。每個檔案系統都有屬性 (如 ID、建立字符、建立時間、檔案系統大小 (以位元組為單位)、為檔案系統而建立的掛載目標數，以及檔案系統生命週期狀態)。如需詳細資訊，請參閱 CreateFileSystem。

Amazon EFS 還支援其他資源來設定主要資源。其中包括掛載目標和存取點：

- 掛載目標：若要存取檔案系統，您必須在 VPC 中建立掛載目標。每個掛載目標都有下列屬性：掛載目標 ID、在其中建立掛載目標的子網路 ID、為其建立掛載目標的檔案系統 ID、可掛載檔案系統的 IP 地址、VPC 安全群組以及掛載目標狀態。您可以在 `mount` 命令中使用此 IP 地址或 DNS 名稱。

  每個檔案系統都有以下表單的 DNS 名稱。

  ```
  file-system-id.efs.aws-region.amazonaws.com
  ```

  使用 `mount` 命令，您可以指定此 DNS 名稱來掛載 Amazon EFS 檔案系統。假設您在 EC2 執行個體上主目錄以外或現場部署伺服器上建立 `efs-mount-point` 子目錄。那麼，您可以使用掛載命令來掛載檔案系統。例如，在 Amazon Linux AMI 上，您可以使用以下 `mount` 命令。

  ```
  $ sudo mount -t nfs -o
   nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport file-system-DNS-name:/ ~/efs-mount-point
  ```

  如需詳細資訊，請參閱 管理掛載目標。
- 存取點：存取點會使用存取點，將操作系統使用者、群組和檔案系統路徑套用至要求提出的任何檔案系統。存取點的作業系統使用者和群組會覆寫 NFS 用戶端提供的任何身分資訊。檔案系統路徑會公開給用戶端作為存取點的根目錄。這可確保每個應用程式在存取共用檔案型資料集時，一律使用正確的作業系統身分和正確的目錄。使用存取點的應用程式只能在其專屬目錄及子目錄中存取資料。如需詳細資訊，請參閱 使用 Amazon EFS 存取點。

掛載目標和標籤是與檔案系統相關聯的 子資源。您只能在現有檔案系統的內容進行建立。

Amazon EFS 提供 API 操作讓您可建立和管理這些資源。除了為每個資源建立和刪除操作，Amazon EFS 也支援描述操作，此操作可讓您能夠擷取資源資訊。您有下列選項，可用來建立和管理這些資源：

- 例如，使用 Amazon EFS 主控台，請參閱 開始使用。

- 使用 Amazon EFS 命令列介面 (CLI)：例如，請參閱 逐步解說：建立 Amazon EFS 檔案系統，並使用 AWS CLI。
- 您也可以透過程式設計方式來管理這些資源，如下所示：
  - 使用 AWS 開發套件 — 開發 AWS 套件透過包裝基礎 Amazon EFS API 來簡化您的程式設計任務。SDK用戶端也使用您提供的存取金鑰來驗證請求。如需詳細資訊，請參閱範本程式碼與程式庫。
  - 從您的應用程式直接呼叫 Amazon EFS API：如果您因為某些原因，而無法使用 SDK，您可以直接從應用程式進行 Amazon EFS API 呼叫。不過，如果您使用此選項，您需要編寫必要的程式碼來驗證請求。如需關於 Amazon EFS API 的詳細資訊，請參閱 EFS S。

身分驗證與存取控制

您必須擁有有效的登入資料才能進行 Amazon EFS API 請求 (例如建立檔案系統)。此外，您還必須有許可才能建立或存取資源。

您在 AWS Identity and Access Management (IAM) 中建立的使用者和角色必須獲得建立或存取資源的權限。如需許可的詳細資訊，請參閱「Amazon Elastic File System 的身分與存取管理」。

NFS 用戶端的 IAM 授權是 Amazon EFS 的額外安全性選項，其使用 IAM 大規模簡化網路檔案系統 (NFS) 用戶端的存取權管理。透過 NFS 用戶端的 IAM 授權，您可以透過本質上可擴展的方式，使用 IAM 管理對 EFS 檔案系統的存取。NFS 用戶端的 IAM 授權也優化了雲端環境。如需對 NFS 用戶端使用 IAM 授權的詳細資訊，請參閱 使用 IAM 控制檔案系統資料存取。

在 Amazon EFS 中的資料一致性

Amazon EFS 提供應用程式期望從 NFS 獲得的 close-to-open 一致性語意。

在 Amazon EFS 中，出現如遇下列情況時，「區域性」檔案系統的寫入操作會永久儲存在所有跨可用區域中：

- 應用程式執行同步寫入操作 (例如，使用 `open` Linux 命令與 `O_DIRECT` 旗標或 `fsync` Linux 命令)。
- 應用程式會關閉檔案。

根據存取模式，Amazon EFS 可以提供比 close-to-open 語義更強的一致性保證。執行同步資料存取和執行非附加寫入的應用程式對資料存取具有 read-after-write 一致性。

檔案鎖定

NFS 用戶端應用程式可以在 Amazon EFS 檔案上使用 NFS 第 4 版檔案鎖定 (包括位元組範圍鎖定) 進行讀取和寫入操作。

請記住下列關於 Amazon EFS 如何鎖定檔案的事項：

- Amazon EFS 僅支援諮詢鎖定和讀取/寫入操作，在執行這些操作之前不會檢查衝突鎖定。例如，若要避免原子作業的檔案同步處理問題，您的應用程式必須注意 NFS 語意 (例如 close-to-open 一致性)。
- 對於所有已連線執行個體與檔案存取使用者，任何一個特定檔案可讓檔案系統擁有最多 512 個鎖定。

EFS 儲存類別

Amazon EFS 針對不同的資料儲存需求提供不同的儲存類別。標準是寫入資料的第一個儲存類別，也是經常存取資料的儲存類別。對於較少存取的檔案，Amazon EFS 提供 EFS Infrequent Access (IA) 和 EFS 封存儲存類別。IA 儲存類別針對每季存取數次的資料進行成本最佳化，而「封存」儲存類別針對每年僅存取幾次或更少的資料進行成本最佳化。如需關於 Amazon EFS 儲存類別的詳細資訊，請參閱 EFS 儲存類別。

生命週期管理

若要管理您的檔案系統，以便在整個生命週期中以符合成本效益的方式儲存檔案系統，請使用 生命週期管理會根據為檔案系統定義的生命週期設定，在儲存類別之間自動轉移資料。生命週期組態是一組生命週期政策，用於定義將檔案系統資料轉移到其他儲存類別的時間。如需詳細資訊，請參閱 管理檔案系統儲存。

複寫

您可以根據自己的喜好使用複寫建立 Amazon EFS 檔案系統 AWS 區域 的複本。複寫會自動且透明地將 EFS 檔案系統上的資料和中繼資料複製到在您選擇的中建立的新目的地 EFS 檔案系統。 AWS 區域 EFS 會自動保持來源和目標檔案系統的同步。複寫會持續進行，旨在提供幾分鐘內達到復原點目標 (RPO) 和復原時間點目標 (RTO)。這些特徵可協助您達成合規性和業務持續性目標。如需更多詳細資訊，請參閱 複寫檔案系統。

開始使用 Amazon Elastic File System

拉恩如何快速開始使用 Amazon Elastic File System（Amazon EFS）。在這個入門練習中，您將建立 EFS 檔案系統並啟動 EC2 執行個體。您也可以使 AWS DataSync 用然後清理資源，將檔案傳輸到 EFS 檔案系統。

此入門練習中包含以下步驟。

1. 檢閱執行此入門練習的先決條件
2. 建立您的 EFS 檔案系統並啟動 EC2 執行個體
3. 使用以下方法將檔案傳輸到 Amazon EFS 檔案系統 AWS DataSync
4. 清理資源並保護您的 AWS 帳戶

開始使用的先決條件

開始入門練習之前，請確保您具有以下要求：

- 您已使用 Amazon EC2 進行設定，並且熟悉啟動 EC2 執行個體。您需要具有管理存取權限的使用者、key pair 和安全性群組。 AWS 帳戶如需詳細資訊，請參閱設定為使用 Amazon EC2。
- Amazon VPC、Amazon EC2 和 Amazon EFS 都在同一 AWS 區域中。本練習使用美國西部 (奧勒岡) 區域 (us-west-2)。
- 您在此入門練習中 AWS 區域 使用的預設 VPC。如果您沒有預設 VPC，或者想要透過新的或現有的安全性群組從新的 VPC 掛載檔案系統，請參閱。針對 Amazon EC2 執行個體和掛載目標使用 VPC 安全群組
- 您未曾變更預設安全群組的預設傳入存取規則。

您也可以使用 AWS Command Line Interface (AWS CLI) 命令執行類似的入門練習，以進行 Amazon EFS API 呼叫。如需詳細資訊，請參閱 逐步解說：建立 Amazon EFS 檔案系統，並使用 AWS CLI。

建立您的 EFS 檔案系統並啟動 EC2 執行個體

確定您符合此入門練習的先決條件後，您可以建立 EFS 檔案系統並啟動 Amazon EC2 執行個體。完成所有必要步驟以開始使用第一個 EFS 檔案系統的最快方法是在執行個體啟動期間使用 EC2 新啟動精靈。

> **Note**
>
> 您無法搭配使用 Amazon EFS 與以 Microsoft Windows 為基礎的 Amazon EC2 執行個體。

使用 EC2 啟動精靈建立您的 EFS 檔案系統並啟動 Amazon EC2 執行個體

如需在建立 EC2 執行個體啟動時建立和掛接 EFS 檔案系統的指示，請參閱搭配 Amazon EC2 使用 Amazon EFS。

以下是在執行個體啟動期間建立 EFS 檔案系統時要執行的步驟。

1. 使用您選擇的 key pair 和網路設定，建立在 Linux 作業系統上執行的 EC2 執行個體。
2. 建立具有建議設定並自動掛接至 EC2 執行個體的共用 EFS 檔案系統。
3. 啟動 EC2 執行個體，以便 EFS 檔案系統隨時可用於檔案傳輸。

或者，在 Amazon EFS 主控台中，您可以使用建議的設定或自訂設定建立檔案系統。您也可以使用 AWS CLI 和 API 建立檔案系統。如需建立檔案系統所有選項的詳細資訊，請參閱建立 Amazon EFS 檔案系統。

使用以下方法將檔案傳輸到 Amazon EFS 檔案系統 AWS DataSync

建立 EFS 檔案系統之後，您可以使用將檔案從現有檔案系統傳輸至該檔案系統 AWS DataSync。DataSync 是一種資料傳輸服務，可簡化、自動化並加速內部部署儲存系統與儲存服務透過網際網路或儲存服務之間的資料移動和 AWS 複寫。 AWS Direct Connect DataSync 可以傳輸檔案資料，以及檔案系統中繼資料，例如擁有權、時間戳記和存取權限。

如需有關 DataSync 的詳細資訊，請參閱 AWS DataSync。

將檔案傳輸到 Amazon EFS 的先決條件 AWS DataSync

在將檔案傳輸到 EFS 檔案系統之前，請確定您具備下列各項：

- 可以從其中傳輸檔案的來源 NFS 檔案系統。您必須透過 NFS 第 3 版、第 4 版或第 4.1 版存取此來源系統。範例中的檔案系統，包括位於內部部署資料中心、自我受管雲端檔案系統和 Amazon EFS 檔案系統中的檔案系統。
- 您已設定使用 DataSync。若要深入瞭解，請參閱《AWS DataSync 使用者指南》 AWS DataSync中的〈設定〉。

若要將檔案傳輸到 EFS 檔案系統，請使用 AWS DataSync

如需使用將檔案傳輸 DataSync 至 EFS 檔案系統的指示，請參閱使用指南 AWS DataSync中的使用 AWS DataSync 傳輸資料。

以下是使用將檔案傳輸到 EFS 檔案系統時將執行的步驟 DataSync。

1. 連線到您的 Amazon EC2 執行個體。
2. 在您的環境中下載、部署及啟用代理程式。
3. 建立和設定來源與目的地位置。
4. 建立並設定任務。
5. 執行任務以將檔案從來源傳輸至目的地。

清理資源並保護您的 AWS 帳戶

透過本指南所提供的逐步解說，您可以進一步探索 Amazon EFS。在執行此清理步驟之前，您可以在這些逐步解說中使用您在此入門練習中建立並連接到的資源。如需詳細資訊，請參閱 演練。在完成逐步解說後，或者，如果您不想探索各項逐步解說，則應遵循下述步驟以清除資源並保護 AWS 帳戶。

清除資源和保護帳戶

1. 連線到您的 Amazon EC2 執行個體。
2. 使用下列命令卸載 EFS 檔案系統。

```
$ sudo umount efs
```

3. 前往 https://console.aws.amazon.com/efs/ 開啟 Amazon Elastic File System 主控台。
4. 刪除您在入門練習的第一個步驟中建立的 EFS 檔案系統。
   a. 選擇您要從檔案系統清單刪除的 EFS 檔案系統。
   b. 針對 Actions (動作)，選擇 Delete file system (刪除檔案系統)。
   c. 在永久刪除檔案系統對話方塊中，輸入要刪除 EFS 檔案系統的檔案系統 ID，然後選擇刪除檔案系統。
5. 終止您為此入門練習啟動的 Amazon EC2 執行個體。如需相關指示，請參閱AWS IAM Identity Center 使用者指南中的終止 Amazon EC2 執行個體。
6. 刪除您為此入門練習建立的安全性群組。如需指示，請參閱《AWS IAM Identity Center 使用指南》中的「刪除安全性群組」。

> **Warning**
>
> 無法刪除 VPC 的預設安全群組。

了解 Amazon EFS 檔案系統類型和儲存類別

本區段說明 Amazon Elastic File System (Amazon EFS) 檔案系統的檔案系統和儲存類別選項。

EFS 檔案系統類型

Amazon EFS 提供區域和單區域檔案系統類型。

- 地區 — 區域檔案系統 (建議使用) 以冗餘方式將資料儲存在同一個地理位置分隔的多個可用區域。AWS 區域跨多個可用區域儲存資料可提供資料的持續可用性，即使一或多個可用區域中的一或多個 AWS 區域 可用區域無法使用。
- 單一區域 — 單一區域檔案系統會將資料儲存在單一可用區域內。將資料儲存在單一可用區域中，為資料提供持續可用性。不過，在可用區域全部或部分遺失或損壞的情況下，儲存在這些類型檔案系統中的資料可能會遺失。

  在可 AWS 用區域全部或部分遺失或損壞的情況下，單一區域儲存類別中的資料可能會遺失。例如，火災和水災等事件可能會導致資料遺失。除了這些類型的事件之外，我們的單區域儲存類別使用與區域性儲存類別類似的工程設計，以保護物件免受獨立磁碟、主機和機架層級故障影響，而且每処設計都能為資料提供高達 99.999999999% 的耐久性。

  為了增加資料保護，Amazon EFS 會自動使用備份單區檔案系統 AWS Backup。您可以將檔案系統備份還原到中的任何操作可用區域 AWS 區域，或將其還原到不同的可用區域 AWS 區域。使用建立和管理的 EFS 檔案系統備份 AWS Backup 會複寫到三個可用區域，並且專為耐久性而設計。如需詳細資訊，請參閱 AWS Backup.

  > **Note**
  >
  > 一個區域檔案系統僅適用於特定可用區域。如需列出可在其中使用單一區域檔案系統之可用區域的表格，請參閱單一區域檔案系統支援的可用區域。

下列資料表比較了各種檔案系統類型，包括可用性、耐久性和其他因素。

檔案系統類型。	設計用途	耐用性 (設計目的)	可用性	可用區域	其他考量
區域性	需要最高耐久性和可用性的資料。	99.999999999% (11 9s)	99.99%	>=3	無
單區域	不需要最高耐久性和可用性的資料。	99.999999999% (11 9s)	99.99%	1	不適應可用區域的損失

單一區域檔案系統支援的可用區域

一個區域檔案系統僅適用於特定可用區域。下表列出您可以在其中使用「一個區域」檔案系統的每個可用區域的 AZ ID。 AWS 區域 若要查看您帳戶中 AZ ID 與可用區域的對應，請參閱 AWS Resource Access Manager 使用指南中的資源可用區域 ID。 AWS

支援單一區域檔案系統的可用區域

AWS 區域 名稱	AWS 區域 代碼	支援的 AZ ID
美國東部 (俄亥俄)	us-east-2	use2-az1、use2-az2、use2-az3
美國東部 (維吉尼亞北部)	us-east-1	use1-az1、use1-az2、use1-az4、use1-az5、use1-az6
美國西部 (加利佛尼亞北部)	us-west-1	usw1-az1、usw1-az3
美國西部 (奧勒岡)	us-west-2	usw2-az1、usw2-az2、usw2-az3、usw2-az4
非洲 (開普敦)	af-south-1	AFS1, AFS1, AFS1-阿茲 2, AFS1
亞太區域 (香港)	ap-east-1	阿比 1, 阿比 1, 阿比 1, 阿比 1-偶氮
亞太區域 (孟買)	ap-south-1	aps1-az1、aps1-az2、aps1-az3

AWS 區域 名稱	AWS 區域 代碼	支援的 AZ ID
亞太區域 (大阪)	ap-northeast-3	窒息 3-az1, 窒息 3-az2, 窒息 3-az3
亞太區域 (首爾)	ap-northeast-2	apne2-az1、apne2-az 2、apne2-az3
亞太區域 (新加坡)	ap-southeast-1	阿西 1, 應用 1-偶氮
亞太區域 (悉尼)	ap-southeast-2	apse2-az1、apse2-az 2、apse2-az3
亞太區域 (東京)	ap-northeast-1	窒息 1-偶氮, 窒息 1-偶氮
加拿大 (中部)	ca-central-1	cac1-az1、cac1-az2
中國 (北京)	cn-north-1	cnn1-az1、cnn1-az2
中國 (寧夏)	cn-northwest-1	cnnw1-az1、cnnw1-az 2、cnnw1-az3
歐洲 (法蘭克福)	eu-central-1	euc1-az1、euc1-az2、euc1-az3
歐洲 (愛爾蘭)	eu-west-1	euw1-az1、euw1-az2、euw1-az3
歐洲 (倫敦)	eu-west-2	欧盟 2-AZ1, 欧维 2-偶氮
歐洲 (米蘭)	eu-south-1	歐斯 1-AZ1, 歐洲 1-偶氮, 歐洲 1-AZ3
歐洲 (巴黎)	eu-west-3	euw3-az1、euw3-az3
歐洲 (斯德哥爾摩)	eu-north-1	eun1-az1、eun1-az2、eun1-az3
中東 (巴林)	me-south-1	mes1-az1、mes1-az2、mes1-az3

AWS 區域 名稱	AWS 區域 代碼	支援的 AZ ID
南美洲 (聖保羅)	sa-east-1	sae1-az1、sae1-az2、sae1-az3
AWS GovCloud (美國東部)	us-gov-east-1	使用 1-az1, 使用 1-AZ2, 使用 1-AZ3
AWS GovCloud (美國西部)	us-gov-west-1	usgw1-az1、usgw1-az2、usgw1-az3

EFS 儲存類別

Amazon EFS 提供不同儲存類別，專爲最有效的儲存而設計，具體取決於使用案例。

- EFS 標準：EFS 標準儲存體類別使用固態硬碟 (SSD) 儲存，為經常存取的檔案提供最低延遲等級。新的檔案系統資料會先寫入 EFS 標準儲存類別，然後使用生命週期管理，將其分層到 EFS 不常存取和 EFS 封存儲存類別。
- EFS 不常存取 (IA) — 一種成本最佳化的資料儲存類別，每季僅存取幾次。
- EFS 封存：一種成本優化的資料儲存類別，每年存取幾次或更少。

  具有彈性輸送量的 EFS 檔案系統支援 EFS 封存儲存類別。一旦封存儲存類別中有檔案系統的資料，您就無法將檔案系統的輸送量更新為爆增或已佈建輸送量。

將儲存體成本最佳化

IA 和封存儲存類別針對不需要標準存儲延遲性能的文件進行了成本優化。從任一不常用儲存類別讀取時的第一位組元延遲高於標準儲存類別的第一位組員延遲。

使用生命週期管理，您可以根據工作負載的存取模式，在儲存類別之間自動分層資料，將儲存成本最佳化。您可以在檔案系統上設定轉換成標準生命週期原則，將檔案從 IA 或封存儲存類別移至標準儲存類別。此設定會在存取時將檔案從 IA 或封存轉換回標準。如果您希望檔案保留在經常存取的標準儲存類別中，請關閉檔案系統上的生命週期管理。如需詳細資訊，請參閱 管理檔案系統儲存。

比較儲存體方案

下表比較儲存體方案。如需關於每個儲存類別效能的詳細資訊，請參閱 Amazon EFS 效能。

儲存方案	設計用途	第一位元組讀取延遲	耐久性 (專為) [1]	可用性 SLA	可用區域	每個檔案的最低帳單費用 [2]	最低儲存時間
EFS 標準	需要低於一毫秒延遲效能的作用中資料	次毫秒	99.999999999% (十一九年代)	99.99% (區域性) 99.9% (一個區域)	=>3 (區域性) 1 個 (一個區域)	不適用	不適用
EFS Infrequent Access	每季僅存取幾次的非作用中資料。	幾十毫秒				128 KiB	不適用
EFS 封存	每年存取幾次或更少的非作用中資料	幾十毫秒		99.9% (區域性)	=>3 (區域性)	128 KiB	90 天

> **Note**
>
> [1] 由於「一個區域」檔案系統會將資料儲存在單一可 AWS 用區域中，因此在發生災難或其他錯誤影響可用區域內所有資料複本或可用區域銷毀時，儲存在這些類型檔案系統中的資料可能會遺失。
>
> [2] 生命週期政策在太平洋時間下午 12 點或之後更新，將小於 128 KiB 的檔案分層至 IA 類別。如需 Amazon EFS 如何計量個別檔案和中繼資料帳單的詳細資訊，請參閱計量：Amazon EFS 如何報告檔案系統和物件大小。

儲存類別定價

我們將依據每個儲存類別中的資料量向您收費。讀取 IA 或 Archive 儲存體中的檔案時，或使用生命週期管理在儲存類別之間轉換的資料，也會向您收取資料存取費用。 AWS 帳單會分別顯示每個儲存類別的容量，以及根據檔案系統儲存類別的計量存取。如需進一步了解，請參閱 Amazon EFS 定價。

此外，不常存取 (IA) 和封存儲存類別的每個檔案的最低帳單費用為 128 KiB。小於 128 KiB 的檔案 Support 僅適用於在太平洋時間 2023 年 11 月 26 日中午 12:00 或之後更新的生命週期政策。如需

Amazon EFS 如何計量個別檔案和中繼資料帳單的詳細資訊，請參閱計量：Amazon EFS 如何報告檔案系統和物件大小。

使用佈建或爆量輸送量的檔案系統要額外定價。

- 用於使用佈建輸送量的檔案系統時，您要為提供上述佈建輸送量支付的費用，將根據標準儲存類別中的資料量計算。
- 用於使用爆量輸送量的檔案系統時，允許的輸送量僅會根據 EFS 標準儲存類別中的資料存放量計算。

如需 EFS 輸送量模式的詳細資訊，請參閱輸送量模式。

> **Note**
>
> 使用備份已啟用 AWS Backup 生命週期管理的 EFS 檔案系統時，不會產生資料存取費用。若要進一步瞭解 AWS Backup 和生命週期管理，請參閱EFS 儲存類別。

檢視儲存類別大小

您可以使用 Amazon EFS 主控台、或 EFS API，檢視檔案系統每個儲存類別中存放的資料量。 AWS CLI

在 Amazon EFS 主控台中檢視儲存資料大小

檔案系統詳細資訊頁面上的計量大小索引標籤會以位元組的二進位倍數 (KiB、MiB、GiB 和 TiB) 顯示檔案系統目前的計量大小。此指標每 15 分鐘會發出一次，並讓您檢視檔案系統在一段時間內的計量大小。計量大小會顯示下列檔案系統儲存大小的資訊：

- 總大小是儲存在檔案系統中的資料大小 (以二進位位元組為單位)，包括所有儲存類別。
- 標準大小是 EFS 標準儲存類別中儲存的資料大小 (以二進位位元組為單位)。
- IA 大小是 EFS Infrequent Access 儲存類別中儲存的資料大小 (以二進位位元組為單位)。小於 128KiB 的檔案會四捨五入至 128 千兆位元。
- 封存大小是 EFS 封存儲存類別中儲存的資料大小 (以二進位位元組為單位)。小於 128KiB 的檔案會四捨五入至 128 千兆位元。

在 Amazon EFS 主控台的檔案系統詳細資訊頁面上，您也可以檢視在監控索引標籤上的 `Storage bytes` 指標。如需詳細資訊，請參閱 存取 CloudWatch 量度。

使用檢視儲存區資料大小 AWS CLI

您可以使用 AWS CLI 或 EFS API 檢視檔案系統每個儲存類別中儲存的資料量。通過呼叫 `describe-file-systems` CLI 命令 (對應的 API 操作為 DescribeFileSystems) 來檢視資料儲存詳細資訊。

```
$  aws efs describe-file-systems \
--region us-west-2 \
--profile adminuser
```

在回應中，`ValueInIA` 顯示檔案系統的 Infrequent Access 儲存類別中最近一次計量大小 (以位元組為單位)。`ValueInStandard` 顯示標準儲存類別中最近一次計量大小 (以位元組為單位)。`ValueInArchive` 顯示「封存」儲存類別中最近一次計量大小 (以位元組為單位)。這三個值的總和等於整個檔案系統的大小，顯示在中`Value`。

```
{
   "FileSystems":[
      {
         "OwnerId":"251839141158",
         "CreationToken":"MyFileSystem1",
         "FileSystemId":"fs-47a2c22e",
         "PerformanceMode" : "generalPurpose",
         "CreationTime": 1403301078,
         "LifeCycleState":"created",
         "NumberOfMountTargets":1,
         "SizeInBytes":{
            "Value": 29313746702,
            "ValueInIA": 675432,
            "ValueInStandard": 29312741784,
            "ValueInArchive":329486
        },
        "ThroughputMode": "elastic"
      }
   ]
}
```

如需其他可檢視和計量磁碟使用量的詳細資訊的方式，請參閱計量 Amazon EFS 檔案系統物件。

使用 Amazon EFS 資源

Amazon EFS 可提供與 POSIX 相容的彈性、共用檔案儲存。您建立的檔案系統支援從多個 Amazon EC2 執行個體同時讀取和寫入存取。您也可以從建立檔案系統的所有可用區域 AWS 區域 存取檔案系統。

您可以根據 Amazon VPC，使用網路檔案系統版本 4.0 和 4.1 通訊協定 (NFSv4)，在虛擬私有雲端 (VPC) 的 EC2 執行個體上掛載 Amazon EFS 檔案系統。如需詳細資訊，請參閱 Amazon EFS 如何運作。

例如，假設您有一或多個在 VPC 中啟動的 EC2 執行個體。現在，您想要在這些執行個體上建立和使用檔案系統。以下為您需要在 VPC 中使用 Amazon EFS 檔案系統時執行的一般步驟：

- 建立 Amazon EFS 檔案系統：建立檔案系統時，建議使用名稱標籤。名稱標籤值會顯示在主控台中，讓您更容易識別檔案系統。您也可以對檔案系統新增其他可選標籤。
- 建立檔案系統的掛載目標：若要在 VPC 中存取檔案系統，並將檔案系統掛載到 Amazon EC2 執行個體，您必須在 VPC 子網路建立掛載目標。
- 建立安全群組：Amazon EC2 執行個體及掛載目標都需要關聯的安全群組。做為虛擬防火牆的這些安全群組會控制其中的流量。您可以使用與掛載目標相關聯的安全群組來控制檔案系統的輸入流量。若要這麼做，請將輸入規則新增至掛載目標安全群組，以允許從特定 EC2 執行個體存取。然後，您可以將檔案系統只掛載在該 EC2 執行個體。

主題

資源 ID

Amazon EFS 會在建立所有 EFS 資源時指派唯一的資源識別碼 (ID)。所有 EFS 資源 ID 都包含一個資源識別碼，以及數字 0-9 和小寫字母 a—f 的組合。

在 2021 年 10 月之前，指派給新建立之檔案系統和掛載目標資源的 ID 是採用連字號後 8 個字元 (例如 `fs-12345678`) 的格式。從 2021 年 5 月到 2021 年 10 月，我們已將這些資源類型的 ID 變更為連字號後 17 個字元 (例如 `fs-1234567890abcdef0`)。根據您建立帳戶的時間點，您可能會有以下具有短 ID 之資源類型的資源，雖然任何這些類型的新資源都會獲得較長的 ID：資源 ID 永遠不會變更。

創建令牌和等冪性

等冪性可確保 API 請求只完成一次。若使用等冪性請求，如果原始請求成功完成，則後續請求不會有其他影響。這對於防止在您與 Amazon EFS API 互動時建立重複的任務非常有用。

Amazon EFS API 支援具有用戶端請求權杖的等冪性。客戶端請求字符是您在發出建立任務請求時指定的唯一字串。

客戶端請求令牌可以是包含多達 64 個 ASCII 字符的任何字符串。如果您在成功請求後的一分鐘內重複使用用戶端要求權杖，API 會傳回原始要求的工作詳細資訊。

如果您使用的是主控台，它會產生字符。如果您在控制台中使用「自定義創建」流程，則為您生成的創建令牌具有以下格式：

```
"CreationToken": "console-d215fa78-1f83-4651-b026-facafd8a7da7"
```

如果您使用「快速建立」建立具有服務建議設定的檔案系統，則建立權杖的格式如下：

```
"CreationToken": "quickCreated-d7f56c5f-e433-41ca-8307-9d9c0f8a77a2"
```

建立 Amazon EFS 檔案系統

接下來，您可以了解如何使用 AWS Management Console 和建立 Amazon EFS 檔案系統 AWS CLI。

主題

- 建立檔案系統所需的權限

- 檔案系統的組態選項

建立檔案系統所需的權限

若要建立 EFS 資源，例如檔案系統和存取點，您必須擁有對應 API 作業和資源的 AWS Identity and Access Management (IAM) 許可。

建立 IAM 使用者，並透過使用者政策授予他們 Amazon EFS 動作的許可。您也可以使用角色來授予跨帳戶許可。Amazon Elastic File System 也使用 IAM 服務連結角色，其中包含代表您呼叫其他人所需 AWS 服務 的許可。如需管理 API 作業權限的詳細資訊，請參閱Amazon Elastic File System 的身分與存取管理。

檔案系統的組態選項

您可以使用 Amazon EFS 主控台或使用 AWS Command Line Interface (AWS CLI) 來建立檔案系統。您也可以直接使用 AWS 開發套件或 Amazon EFS API，以程式設計方式建立檔案系統。如果您使用的是 Amazon EFS API 或 AWS 開發套件，則可以使用 `CreateFileSystem` EFS API 動作來建立檔案系統政策。

使用主控台或 AWS CLI中的自訂建立流程建立 Amazon EFS 檔案系統時，您可以選擇下列檔案系統功能和組態選項的設定。

檔案系統類型。

檔案系統類型決定 Amazon EFS 檔案系統在中儲存資料的可用性和耐久性 AWS 區域。您的檔案系統類型有下列選擇：

- 選擇區域以建立檔案系統，實現以備援方式將檔案系統資料和中繼資料存放於 AWS 區域中的所有可用區域中。您可在 AWS 區域的每個可用區域中建立一個掛載目標。區域提供最高等級的可用性和耐用性。
- 選擇單區域建立一個檔案系統，以備援方式將資料和中繼資料存儲於一個單獨的可用區域內。使用儲存類別的檔案系統只能有一個掛載目標。此掛載目標必須位於建立檔案系統的可用區域中。

自動備份

當您使用主控台建立檔案系統時，依預設會一律啟用自動備份。當您使用 CLI 或 API 建立檔案系統時，只有在建立使用單區域檔案系統的檔案系統時，才會預設啟用自動備份。如需詳細資訊，請參閱自動備份。

生命週期政策

生命週期管理使用生命週期原則，根據存取模式，自動將檔案移入和移出成本較低的不常存取 (IA) 儲存類別。當您使用建立檔案系統時 AWS Management Console，會使用下列預設設定來設定檔案系統的生命週期原則：

- 轉移至 IA 設定為自上次存取後 30 天。
- TransitionTo封存設定為自上次存取後 90 天。
- 轉移至標準設定為無。

使用 Amazon EFS API 或 AWS 開發套件建立檔案系統時，您無法同時設定生命週期政策。 AWS CLI 您必須等到檔案系統建立完畢，然後使用 PutLifecycleConfiguration API 作業來更新生命週期原則。如需詳細資訊，請參閱 管理檔案系統儲存。

加密

您可在檔案系統建立時啟用靜態加密。如果您為檔案系統啟用靜態加密，儲存在其上的所有資料和中繼資料都會加密。當您掛載檔案系統時，可以稍後啟用傳輸中加密。如需 Amazon EFS 加密的詳細資訊，請參閱 Amazon EFS 的資料加密。

若要在 VPC 中建立檔案系統掛載目標，您必須指定 VPC 子網路。主控台會使用在所選 AWS 區域中的帳戶來預先填入 VPC 的清單。首先，您選擇您的 VPC，然後在 VPC 主控台列出的可用區域。對於每個可用區域，您可以從清單中選取子網路，或使用預設子網路 (如果存在)。在您選擇子網路後，您可以指定子網路中的可用 IP 地址或讓 Amazon EFS 選擇一個地址。

輸送量模式

有三種輸送量模式可供選擇：

- 彈性 (建議)：提供即時自動縱向擴展和縮小的輸送量，以符合工作負載的效能需求。

> **Note**
>
> 彈性輸送量僅適用於具有一般用途效能模式的檔案系統。

- 已佈建：提供您指定的輸送量層級，與檔案系統的大小無關。
- 大量批量：提供可隨標準儲存體中資料量擴展的輸送量。

如需詳細資訊，請參閱 輸送量模式。

> **Note**
>
> 與使用彈性和佈建輸送量相關的額外費用。如需詳細資訊，請參閱 Amazon EFS 定價。

效能模式

建立檔案系統時，您還可以選擇效能模式。效能模式有兩種選擇一般用途和最高 I/O。

- 一般用途模式的每個作業延遲最低，建議所有檔案系統使用。
- Max I/O 是前一代的效能類型，專為高度平行化的工作負載而設計，可以容忍比一般用途模式更高的延遲。單區域檔案系統或使用彈性輸送量的檔案系統不支援最大 I/O 模式。

> **Important**
>
> 由於最大 I/O 的每個操作延遲較高，我們建議所有檔案系統使用「一般用途」效能模式。

如需詳細資訊，請參閱 效能模式。

快速建立具有建議設定的檔案系統 (主控台)

在此步驟中，使用 Amazon EFS 主控台建立具有建議設定的 Amazon EFS 檔案系統。如果您要建立帶自訂組態的檔案系統，請參閱 使用自訂設定建立檔案系統 (主控台)。

快速建立具有建議設定的 Amazon EFS 檔案系統

1. 登入 AWS Management Console 並開啟 Amazon EFS 主控台，網址為 https://console.aws.amazon.com/efs/。
2. 選擇建立檔案系統以開啟建立檔案系統對話方塊。
3. (選用) 輸入您的檔案系統名稱。
4. 對於虛擬私有雲端 (VPC)，請選擇您的 VPC，或將其設定為預設 VPC。
5. 選擇建立以建立使用下列服務建議設定的檔案系統：
   - 啟用自動備份。如需詳細資訊，請參閱 備份 Amazon EFS 檔案系統。
   - 掛載使用下列設定配置的目標：
     - 在建立檔案系統的每個可用區域 AWS 區域 中建立。

    - 位於所選 VPC 的預設子網路中。
    - 使用 VPC 的預設安全群組：您可以在建立檔案系統之後管理安全群組。

    如需詳細資訊，請參閱 管理檔案系統網路存取權限。
- 區域檔案系統類型：如需詳細資訊，請參閱 EFS 檔案系統類型。
- 一般用途效能模式：如需詳細資訊，請參閱 效能模式。
- 彈性輸送量：如需詳細資訊，請參閱 輸送量模式。
- 使用 Amazon EFS 的預設金鑰啟用靜態資料加密 (aws/elasticfilesystem) — 如需詳細資訊，請參閱加密靜態資料。
- 生命週期管理 — Amazon EFS 建立具有下列生命週期政策的檔案系統：
    - 轉移至 IA 設定為自上次存取後 30 天。
    - TransitionTo封存設定為自上次存取後 90 天。
    - 轉移至標準設定為無。

    如需詳細資訊，請參閱 管理檔案系統儲存。

建立檔案系統後，除了可用性和持久性、加密和效能模式，您可以自訂檔案系統的其他設定。

檔案系統頁面上方會出現一個橫幅，顯示您建立的檔案系統狀態。當檔案系統可供使用時，橫幅中會出現存取檔案系統詳細資訊頁面的連結。

如需關於建立檔案系統狀態的詳細資訊，請參閱 檔案系統狀態。

使用自訂設定建立檔案系統 (主控台)

本節說明使用 Amazon EFS 主控台建立具有自訂設定的 EFS 檔案系統，而非使用服務建議設定的程序。如需使用服務建議的設定建立檔案系統的詳細資訊，請參閱快速建立具有建議設定的檔案系統 (主控台)。

使用主控台建立具有自訂設定的 Amazon EFS 檔案系統需要四個步驟：

- 步驟 1：設定一般檔案系統設定，包括儲存類別和輸送量模式。
- 步驟 2：設定檔案系統網路設定，包括虛擬私有雲端 (VPC) 和掛載目標。針對每個掛載目標，設定可用區域、子網路、IP 地址和安全群組。
- 步驟 3：(選用) 建立檔案系統原則以控制 NFS 用戶端對檔案系統的存取。
- 步驟 4：檢閱檔案系統設定，進行任何變更，然後建立檔案系統。

步驟 1：設定檔案系統設定

1. 登入 AWS Management Console 並開啟 Amazon EFS 主控台，網址為 https://console.aws.amazon.com/efs/。
2. 選擇建立檔案系統以開啟建立檔案系統對話方塊。
3. 選擇自訂以建立自訂的檔案系統，而不是使用服務建議的設定來建立檔案系統。檔案系統設定 頁面隨即開啟。
4. 針對一般設定，執行下列操作：

   a. (選用) 輸入檔案系統的名稱。

   b. 針對檔案系統類型，選擇可用性選項：

      - 選擇區域以建立檔案系統，實現以備援方式將資料和中繼資料存放於 AWS 區域中的所有可用區域中。區域提供最高等級的可用性和耐用性。
      - 選擇單區域建立一個檔案系統，以備援方式將資料和中繼資料存儲於一個單獨的可用區域內。如果您選擇「一個區域」，請選擇您要在其中建立檔案系統的可用區域，或保留預設值。如需詳細資訊，請參閱 EFS 儲存類別。

   c. 自動備份預設為開啟。您可以清除核取方塊來關閉自動備份。如需詳細資訊，請參閱 備份 Amazon EFS 檔案系統。

   d. 對於生命週期管理，如有必要，請變更生命週期原則。

      - 轉換為 IA：根據上次在標準儲存中存取檔案之後的時間，選取將檔案轉換為 Infrequent Access (IA) 儲存類別的時間。
      - 轉換至封存：根據上次在標準儲存體中存取檔案之後的時間，選取將檔案轉換為封存儲存類別的時間。
      - 轉換為標準：選取是否要將檔案系統轉換為儲存類別。

      如需生命週期政策的詳細資訊，請參閱 管理檔案系統儲存。

   e. 對於加密，靜態資料加密預設為啟用。依預設，Amazon EFS 會使用您的 AWS Key Management Service (AWS KMS) EFS 服務金鑰 (`aws/elasticfilesystem`)。若要選擇要用於加密的其他 KMS 金鑰，請展開自訂加密設定，然後從清單中選擇金鑰。或者，針對您要使用的 KMS 金鑰輸入 KMS 金鑰識別碼或 Amazon 資源名稱 (ARN)。

      如果您需要建立新的金鑰，請選擇 [建立] AWS KMS key以啟動 AWS KMS 主控台並建立新金鑰。

      您可以清除核取方塊來關閉靜態資料的加密。

5. 針對效能設定，執行下列操作：

   a. 對於輸送量模式，預設會選取彈性模式。

      - 若要使用佈建的輸送量，請選擇已佈建，然後在佈建輸送量 (MiB/s) 中，輸入要為檔案系統要求佈建的輸送量。「最大讀取輸送量」的顯示量是您輸入輸送量的三倍。
      - 若要使用成組分解輸送量，請選擇大量批次設定

      Amazon EFS 檔案系統以其他請求的三分之一的速率計量讀取請求。進入輸送量模式之後，會顯示檔案系統每月成本的估計值。您可以在檔案系統可用之後變更輸送量模式。

      如需為效能需求選擇正確輸送量模式的更多資訊，請參閱 輸送量模式。

   b. 針對效能模式，預設為一般用途。若要變更效能模式，請展開其他設定，然後選擇最大 I/O。

      檔案系統變為可用之後，您無法變更效能模式。如需詳細資訊，請參閱 效能模式。

      > **Important**
      >
      > 由於最大 I/O 的每個操作延遲較高，我們建議所有檔案系統使用「一般用途」效能模式。

6. (選用) 將標籤鍵值組新增至檔案系統。
7. 選擇「下一步」以設定檔案系統的網路存取。

步驟 2：設定網路

在步驟 2 中，您可以設定檔案系統的網路設定，包括 VPC 和掛載目標。

1. 選擇您希望 EC2 執行個體連線至檔案系統的虛擬私有雲端 (VPC)。如需詳細資訊，請參閱 管理檔案系統網路存取權限。
2. 對於裝載目標，您可以為檔案系統建立一或多個掛載目標。為每個掛載目標設定下列屬性：

   - 可用區域 — 依預設，裝載目標會在 AWS 區域. 如果您不想在特定可用區域中建立掛載目標，請選擇移除以刪除該區域的掛載目標。在您打算存取檔案系統的每個可用區域中建立掛載目標，不需要花費任何費用。
   - 子網路 ID：從可用區域中的可用子網路中選擇。預設子網路已預先選取。

- IP 地址：依預設，Amazon EFS 會從子網路中的可用位址自動選擇 IP 地址。或者，您可以輸入子網路中的特定 IP 地址。雖然掛載目標具有單一 IP 地址，但它們是備援且高可用性的網路資源。
- 安全群組：您可以為掛載目標指定一或多個安全群組。如需詳細資訊，請參閱 針對 Amazon EC2 執行個體和掛載目標使用 VPC 安全群組。

  若要新增其他安全群組，或變更安全群組，請選擇選擇安全群組，然後從清單中新增其他安全群組。如果您不想使用預設的安全群組，您可以將其刪除。如需詳細資訊，請參閱 建立安全群組。

3. 選擇新增掛載目標，為沒有可用區域建立掛載目標。如果為每個可用區域設定掛載目標，則無法使用此選項。
4. 選擇下一步以設定檔案系統政策。

步驟 3：建立檔案系統政策 (選用)

或者，您可以為您的檔案系統建立檔案系統政策。EFS 檔案系統政策是用來控制 NFS 用戶端對檔案系統的存取權限的 IAM 資源政策。如需詳細資訊，請參閱 使用 IAM 控制檔案系統資料存取。

1. 在政策選項中，您可以選擇任何可用預先設定策略的組合：
   - 根據預設阻止根訪問
   - 預設強制執行唯讀存取權
   - 為所有用戶端強制執行傳輸中加密
2. 使用原則編輯器來自訂預先設定的原則或建立您自己的原則。當您選擇其中一個預先設定的原則時，JSON 原則定義會顯示在原則編輯器中。您可以編輯 JSON 以建立您選擇的政策。若要復原變更，請選擇清除。

   預先設定的原則會再次在政策選項中使用。
3. 選擇下一步以檢閱並建立檔案系統。

步驟 4：檢閱和建立

1. 檢閱每個檔案系統組態群組。您可以選擇編輯，此時對每個群組進行變更。
2. 選擇建立以建立您的檔案系統，並傳回檔案系統頁面。

頂端的橫幅表示正在建立新的檔案系統。當檔案系統可供使用時，橫幅中會出現存取新檔案系統詳細資訊頁面的連結。

建立檔案系統 (AWS CLI)

當您使用時 AWS CLI，請依序建立這些資源。首先，您會建立檔案系統。然後，您可以使用對應的 AWS CLI 指令，為檔案系統建立掛載目標和任何其他可選標籤。

下列範例用`adminuser`於`--profile`參數值。您需要使用適當的使用者描述檔，以提供您的憑證。如需詳細資訊，請參閱《使用指南》 AWS CLI中的使AWS Command Line Interface 用的先決條件。

- 若要建立使用 EFS 存檔儲存類別並啟用自動備份的加密檔案系統，請使用 Amazon EFS `create-file-system` CLI 命令 (相應的作業為 CreateFileSystem)，如下所示。

```
aws efs create-file-system \
--creation-token creation-token \
--encrypted \
--backup \
--performance-mode generalPurpose \
--throughput-mode bursting \
--region aws-region \
--tags Key=key,Value=value Key=key1,Value=value1 \
--profile adminuser
```

例如，以下 `create-file-system` 命令會在 `us-west-2` AWS 區域中建立檔案系統。此命令指定 `MyFirstFS` 做為建立字符。如需可在 AWS 區域 其中建立 Amazon EFS 檔案系統的清單，請參閱中的 Amazon EFS 端點和配額Amazon Web Services 一般參考。

```
aws efs create-file-system \
--creation-token MyFirstFS \
--backup \
--encrypted \
--performance-mode generalPurpose \
--throughput-mode bursting \
--region us-west-2 \
--tags Key=Name,Value="Test File System" Key=developer,Value=rhoward \
--profile adminuser
```

順利建立檔案系統後，Amazon EFS 會以 JSON 的形式傳回檔案系統描述，如下範例所示。

```
{
    "OwnerId": "123456789abcd",
    "CreationToken": "MyFirstFS",
    "Encrypted": true,
    "FileSystemId": "fs-c7a0456e",
    "CreationTime": 1422823614.0,
    "LifeCycleState": "creating",
    "Name": "Test File System",
    "NumberOfMountTargets": 0,
    "SizeInBytes": {
        "Value": 6144,
        "ValueInIA": 0,
        "ValueInStandard": 6144
        "ValueInArchive": 0
    },
    "PerformanceMode": "generalPurpose",
    "ThroughputMode": "bursting",
    "Tags": [
      {
         "Key": "Name",
         "Value": "Test File System"
      }
   ]
}
```

- 下列範例會使用 availability-zone-name 屬性，建立在 us-west-2a 可用區域中使用標準儲存類別的檔案系統。

```
aws efs create-file-system \
--creation-token MyFirstFS \
--availability-zone-name us-west-2a \
--backup \
--encrypted \
--performance-mode generalPurpose \
--throughput-mode bursting \
--region us-west-2 \
--tags Key=Name,Value="Test File System" Key=developer,Value=rhoward \
--profile adminuser
```

順利建立檔案系統後，Amazon EFS 會以 JSON 的形式傳回檔案系統描述，如下範例所示。

```
{
    "AvailabilityZoneId": "usw-az1",
    "AvailabilityZoneName": "us-west-2a",
    "OwnerId": "123456789abcd",
    "CreationToken": "MyFirstFS",
    "Encrypted": true,
    "FileSystemId": "fs-c7a0456e",
    "CreationTime": 1422823614.0,
    "LifeCycleState": "creating",
    "Name": "Test File System",
    "NumberOfMountTargets": 0,
    "SizeInBytes": {
        "Value": 6144,
        "ValueInIA": 0,
        "ValueInStandard": 6144
        "ValueInArchive": 0
    },
    "PerformanceMode": "generalPurpose",
    "ThroughputMode": "bursting",
    "Tags": [
      {
         "Key": "Name",
         "Value": "Test File System"
      }
   ]
}
```

Amazon EFS 還提供 `describe-file-systems` CLI 命令 (對應的 API 操作為 DescribeFileSystems)，您可以使用該命令來在您的帳戶中擷取檔案系統的清單，如下所示：

```
aws efs describe-file-systems \
--region aws-region \
--profile adminuser
```

Amazon EFS 會傳回您在指定區域中 AWS 帳戶 建立的檔案系統清單。

刪除 Amazon EFS 檔案系統

檔案系統的刪除是無法復原的破壞性動作。您將遺失存放在其中的檔案系統和所有資料。您從檔案系統刪除的任何資料都將遺失且無法恢復。當使用者刪除檔案系統中的資料時，該資料即會變得無法使用。EFS 會在最後強制覆寫資料。

> **Note**
>
> 您無法刪除屬於複製組態一部分的檔案系統。您必須先刪除複製組態。如需詳細資訊，請參閱刪除複寫組態。

> **Important**
>
> 在刪除檔案系統前，應一律先將其卸載。

刪除檔案系統 (主控台)

刪除檔案系統

1. 前往 https://console.aws.amazon.com/efs/ 開啟 Amazon Elastic File System 主控台。
2. 選取您要在檔案系統頁面刪除的檔案系統。
3. 選擇刪除。
4. 在「刪除檔案系統」對話方塊中，輸入顯示的檔案系統 ID，然後選擇「確認」以確認刪除。

   主控台可為您簡化檔案系統的刪除作業。首先它會刪除關聯的掛載目標，然後才刪除檔案系統。

刪除檔案系統 (CLI)

您必須先刪除為檔案系統建立的所有掛載目標和存取點，才能使用 AWS CLI 指令刪除檔案系統。

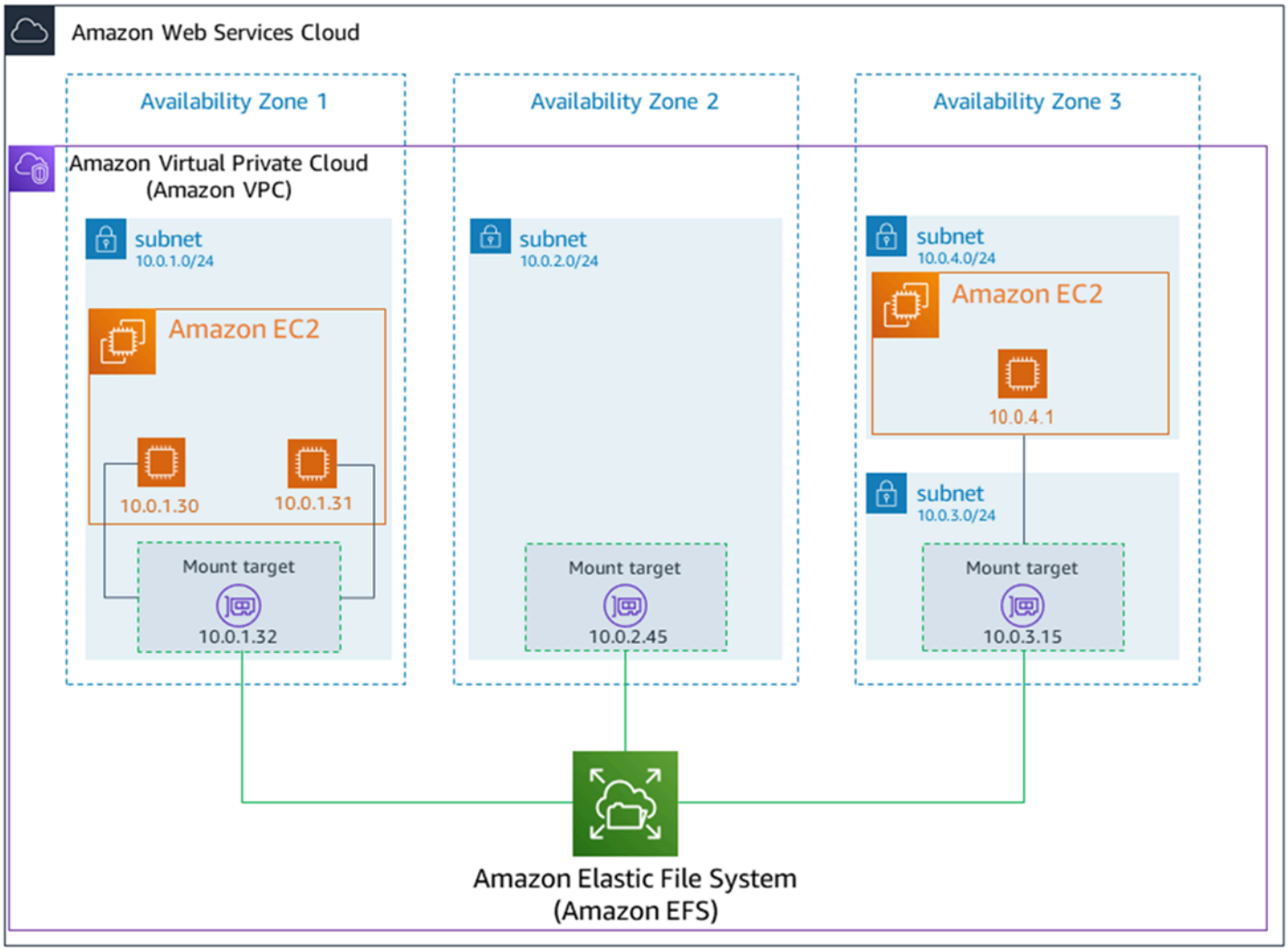
如需 AWS CLI 指令範例，請參閱步驟 4：清理。

管理掛載目標

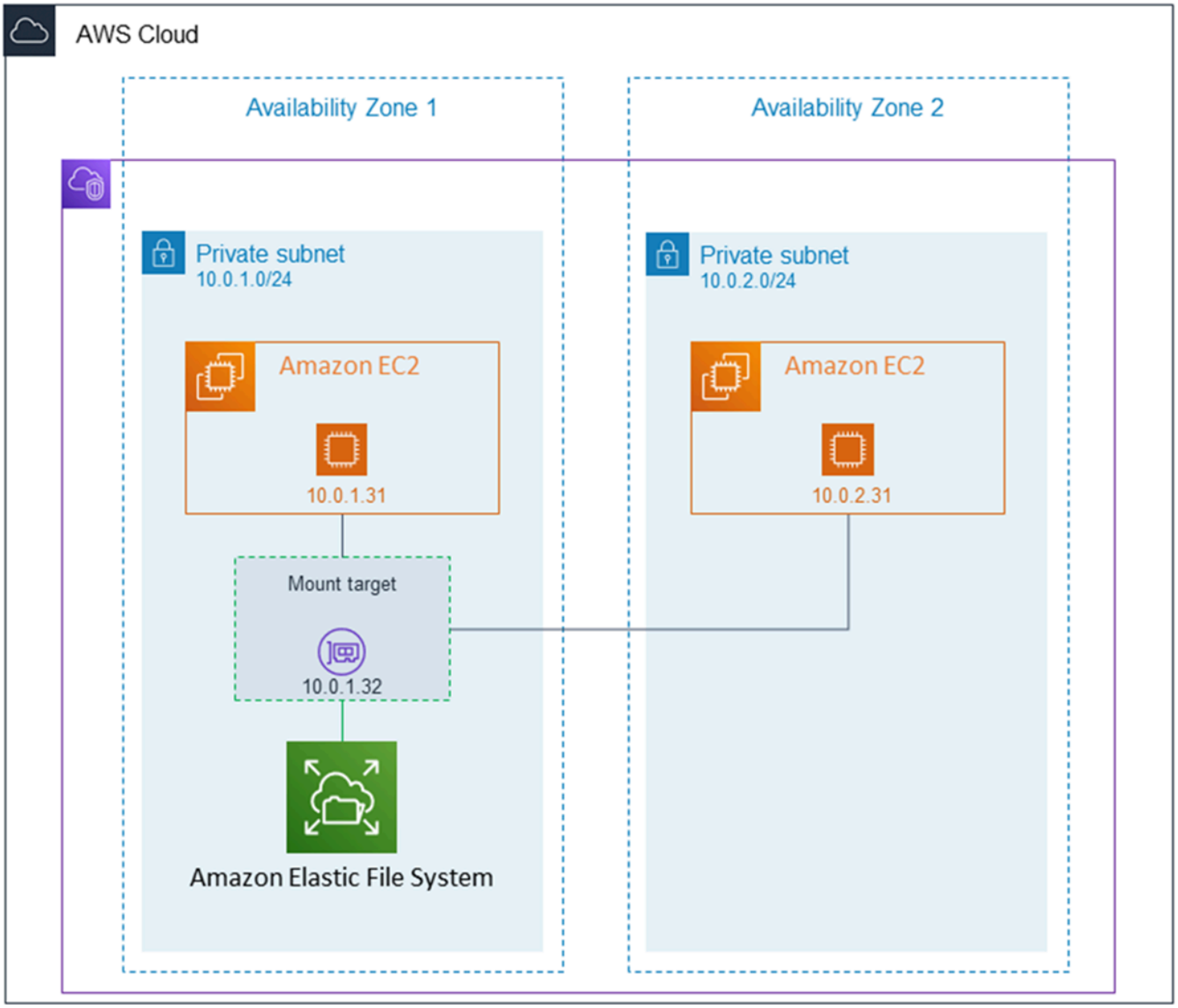
建立 Amazon EFS 檔案系統之後，您可以建立掛載目標。對於使用區域儲存類別的 Amazon EFS 檔案系統，您可以在 AWS 區域. 若為單一 Zone 檔案系統，您只能在與檔案系統相同的可用區域中建立單

一掛載目標。然後，您可以在包括 Amazon EC2、Amazon ECS 和虛擬私有雲 (VPC) AWS Lambda 在內的運算執行個體上掛載檔案系統。

下圖顯示具有在 VPC 中所有可用區域中建立掛載目標的區域檔案系統。



下圖顯示在與檔案系統相同的可用區域中建立的單一掛載目標的單區域檔案系統。使用 `us-west2c` 可用區域中的 EC2 執行個體存取檔案系統會產生資料存取費用，因為該執行個體位於與掛載目標不同的可用區域。



掛載目標安全群組就像是會控制流量的虛擬防火牆。例如，其會決定哪一個用戶端可以存取此檔案系統。本節說明下列各項：

- 掛載目標安全群組，以及如何啟用流量。
- 將檔案系統掛載到您的用戶端上。
- NFS 層級許可考量。

  一開始，只有 Amazon EC2 執行個體上的根使用者具有檔案系統的 read-write-execute 許可。此主題討論的是 NFS 層級的許可，並提供範例，示範如何常見案例中的授予許可。如需詳細資訊，請參閱 在網路檔案系統 (NFS) 層級處理使用者、群組和權限。

您可以使用、或以程式設計方式使用 AWS SDK AWS Management Console AWS CLI，為檔案系統建立掛載目標。使用主控台時，您可以在先建立檔案系統時或在檔案系統建立後，建立掛載目標。

如需在建立檔案系統時使用 Amazon EFS 主控台建立掛接目標的指示，請參閱步驟 2：設定網路。

管理掛載目標 (主控台)

請使用下列程序新增或修改現有 Amazon EFS 檔案系統的掛載目標。

在 Amazon EFS 檔案系統上管理掛載目標

1. 登入 AWS Management Console 並開啟 Amazon EFS 主控台，網址為 https://console.aws.amazon.com/efs/。
2. 在左側導覽窗格中選擇檔案系統。檔案系統頁面會顯示您帳戶中的 EFS 檔案系統。
3. 選擇要管理掛載目標的檔案系統，方法是選擇檔案系統的名稱或檔案系統 ID 來顯示檔案系統詳細資訊頁面。
4. 選擇「網路」以顯示現有掛載目標的清單。
5. 選擇管理以顯示可用區域頁面並進行修改。

   在此頁面上，對於現有的掛載目標，您可以新增和移除安全群組，或刪除掛載目標。您也可以建立新的掛載目標。

   > **Note**
   >
   > 對於單區域檔案系統，您只能建立與檔案系統位於相同可用區域中的單一掛載目標。

   - 若要從裝載目標移除安全群組，請選擇安全群組 ID 旁邊的 X。
   - 若要將安全群組新增至裝載目標，請選擇選取安全群組以顯示可用安全群組的清單。或者，在清單頂端的搜尋欄位中輸入安全群組 ID。
   - 若要將掛載目標排入佇列以進行刪除，請選擇移除。

     > **Note**
     >
     > 刪除掛載目標前，請先卸載檔案系統。

   - 若要新增裝載目標，請選擇新增裝載目標。此選項僅適用於使用 EFS 區域儲存區類別的檔案系統，且裝載目標不存在於的每個可用區域中 AWS 區域。

6. 選擇儲存以儲存任何變更。

若要變更 Amazon EFS 檔案系統 (主控台) 的 VPC 擬私人雲端

若要變更檔案系統網路組態的 VPC，您必須刪除檔案系統的所有現有掛載目標。

1. 前往 https://console.aws.amazon.com/efs/ 開啟 Amazon Elastic File System 主控台。
2. 在左側導覽窗格中選擇檔案系統。檔案系統頁面會顯示您帳戶中的 EFS 檔案系統。
3. 針對您要變更 VPC 的檔案系統，選擇名稱或檔案系統 ID。此時會顯示檔案系統詳細資訊頁面。
4. 選擇網路以顯示現有掛載目標的清單。
5. 選擇管理。便會顯示可用區域頁面。
6. 移除頁面顯示的所有掛載目標。
7. 選擇儲存以儲存變更並刪除裝載目標。網路標籤會將裝載目標狀態顯示為刪除。
8. 當所有裝載目標狀態顯示為已刪除時，請選擇管理。便會顯示可用區域頁面。
9. 從虛擬私有雲端 (VPC) 清單中選擇新 VPC。
10. 選擇新增裝載目標以新增裝載目標。針對您新增的每個裝載目標，輸入下列內容：
    - 可用區域
    - 子網路 ID
    - IP 地址，或將其設定保持為 自動
    - 一或多個安全群組
11. 選擇儲存以實作 VPC 並裝載目標變更。

管理掛載目標 (CLI)

> **Note**
> 對於單區域檔案系統，您只能建立與檔案系統位於相同可用區域中的單一掛載目標。

若要建立掛載目標 (CLI)

- 若要建立掛載目標，請使用 `create-mount-target` CLI 命令 (對應操作為 CreateMountTarget)，如下所示：

```
$ aws efs create-mount-target \
--file-system-id file-system-id \
--subnet-id  subnet-id \
--security-group ID-of-the-security-group-created-for-mount-target \
--region aws-region \
--profile adminuser
```

下列範例顯示具有範例資料的命令。

```
$ aws efs create-mount-target \
--file-system-id fs-0123467 \
--subnet-id  subnet-b3983dc4 \
--security-group sg-01234567 \
--region us-east-2 \
--profile adminuser
```

順利建立掛載目標後，Amazon EFS 會以 JSON 的形式傳回掛載目標描述，如下範例所示。

```
{
    "MountTargetId": "fsmt-f9a14450",
    "NetworkInterfaceId": "eni-3851ec4e",
    "FileSystemId": "fs-b6a0451f",
    "LifeCycleState": "available",
    "SubnetId": "subnet-b3983dc4",
    "OwnerId": "23124example",
    "IpAddress": "10.0.1.24"
}
```

擷取檔案系統 (CLI) 的掛載目標清單

- 您可以透過使用 describe-mount-targets CLI 命令 (對應操作為 DescribeMountTargets) 來擷取為檔案系統建立之掛載目標清單，如下所示。

```
$ aws efs describe-mount-targets --file-system-id fs-a576a6dc
```

```
{
    "MountTargets": [
        {
            "OwnerId": "111122223333",
```

```
            "MountTargetId": "fsmt-48518531",
            "FileSystemId": "fs-a576a6dc",
            "SubnetId": "subnet-88556633",
            "LifeCycleState": "available",
            "IpAddress": "172.31.25.203",
            "NetworkInterfaceId": "eni-0123456789abcdef1",
            "AvailabilityZoneId": "use2-az2",
            "AvailabilityZoneName": "us-east-2b"
        },
        {
            "OwnerId": "111122223333",
            "MountTargetId": "fsmt-5651852f",
            "FileSystemId": "fs-a576a6dc",
            "SubnetId": "subnet-44223377",
            "LifeCycleState": "available",
            "IpAddress": "172.31.46.181",
            "NetworkInterfaceId": "eni-0123456789abcdefa",
            "AvailabilityZoneId": "use2-az3",
            "AvailabilityZoneName": "us-east-2c"
        },
        {
            "OwnerId": "111122223333",
            "MountTargetId": "fsmt-5751852e",
            "FileSystemId": "fs-a576a6dc",
            "SubnetId": "subnet-a3520bcb",
            "LifeCycleState": "available",
            "IpAddress": "172.31.12.219",
            "NetworkInterfaceId": "eni-0123456789abcdef0",
            "AvailabilityZoneId": "use2-az1",
            "AvailabilityZoneName": "us-east-2a"
        }
    ]
}
```

若要刪除現有的掛載目標 (CLI)

- 若要刪除現有的裝載目標，請使用`delete-mount-target` AWS CLI 指令 (對應的作業為DeleteMountTarget)，如下所示。

> **Note**
>
> 刪除掛載目標前，請先卸載檔案系統。

```
$ aws efs delete-mount-target \
--mount-target-id mount-target-ID-to-delete \
--region aws-region-where-mount-target-exists
```

以下是含有範例資料的範例。

```
$ aws efs delete-mount-target \
--mount-target-id fsmt-5751852e \
--region us-east-2 \
```

修改現有掛載目標的安全群組

- 若要修改對裝載目標有效的安全性群組，請使用`modify-mount-target-security-group` AWS CLI 指令 (對應的作業為ModifyMountTargetSecurityGroups) 來取代任何現有的安全性群組，如下所示。

```
$ aws efs modify-mount-target-security-groups \
--mount-target-id mount-target-ID-whose-configuration-to-update \
--security-groups  security-group-ids-separated-by-space \
--region aws-region-where-mount-target-exists \
--profile adminuser
```

以下是含有範例資料的範例。

```
$ aws efs modify-mount-target-security-groups \
--mount-target-id fsmt-5751852e \
--security-groups  sg-1004395a sg-1114433a \
--region us-east-2
```

如需詳細資訊，請參閱 逐步解說：建立 Amazon EFS 檔案系統，並使用 AWS CLI。

建立安全群組

Amazon EC2 執行個體和掛載目標同時擁有關聯的安全群組。做為虛擬防火牆的這些安全群組會控制其中的流量。如果您在建立掛載目標未提供安全群組，Amazon EFS 會將 VPC 的預設安全群組與其相關聯。

無論如何，若要啟用 EC2 執行個體和掛載目標 (和檔案系統) 之間的流量，您必須在這些安全群組中設定以下的規則：

- 您要將掛載目標與其關聯的安全群組，必須允許從所有您要在其上掛載檔案系統的 EC2 執行個體，對在 NFS 連接埠上之 TCP 通訊協定的傳入存取。
- 每個掛載檔案系統 EC2 執行個體都必須有安全群組，該安全群組會允許對 NFS 連接埠之掛載目標的傳出存取。

若要變更與 EFS 檔案系統掛載目標相關聯的安全群組，請參閱 管理掛載目標。

如需有關安全群組的詳細資訊，請參閱 Amazon EC2 使用者指南中的適用於 Linux 執行個體的 Amazon EC2 安全群組。

> **Note**
>
> 下節是專門針對 Amazon EC2，討論如何建立安全群組，以便您可以使用 Secure Shell (SSH) 連接到任何已掛載 Amazon EFS 檔案系統的執行個體。如果您不是使用 SSH 連接到 Amazon EC2 執行個體，您可以略過此節。

使用主控台建立安全群組

您可以使 AWS Management Console 用在 VPC 中建立安全群組。若要將 Amazon EFS 檔案系統連接到 Amazon EC2 執行個體，您將需要建立兩個安全群組：一個用於 Amazon EC2 執行個體，另一個用於您的 Amazon EFS 掛載目標。

1. 在 VPC 中建立兩個安全群組。如需指示，請參閱 Amazon VPC 使用者指南中的建立安全群組。
2. 在 VPC 主控台中，確認這些安全群組的預設規則。兩個安全群組應該只有讓流量離開的傳出規則。
3. 您需要如下對安全群組授予其他存取權：

a. 將規則新增到 EC2 安全群組，以允許 SSH 存取連接埠 22 上的執行個體，如下所示。如果您打算使用像 PuTTY 這樣的 SSH 用戶端透過終端機介面連接和管理 EC2 執行個體，這會很有用。或者，您可以限制 Source (來源) 地址。

   如需指示，請參閱 Amazon VPC 使用者指南中的將規則新增至安全群組。

b. 將規則新增至裝載目標安全性群組，以允許從 TCP 連接埠 2049 上的 EC2Security 群組進行輸入存取。指派為來源的安全群組是與 EC2 執行個體關聯的安全群組。

   若要檢視與檔案系統掛載目標相關聯的安全群組，請在 EFS 主控台中選擇「檔案系統詳細資訊」頁面中的「網路」標籤。如需詳細資訊，請參閱 管理掛載目標。

> **Note**
>
> 您不需要新增傳出規則，因為預設的傳出規則可讓所有流量離開。(如果您沒有此預設傳出規則，新增一個傳出規則，以開啟 NFS 連接埠上的 TCP 連接，以便將掛載目標安全群組識別做為目的地。)

4. 驗證現在兩個安全群組皆獲授權傳入和傳出存取，如此區段所述。

使用 CLI 建立安全性群組

如需示範如何使用建立安全性群組的範例 AWS CLI，請參閱步驟 1：建立 Amazon EC2 資源。

建立檔案系統原則

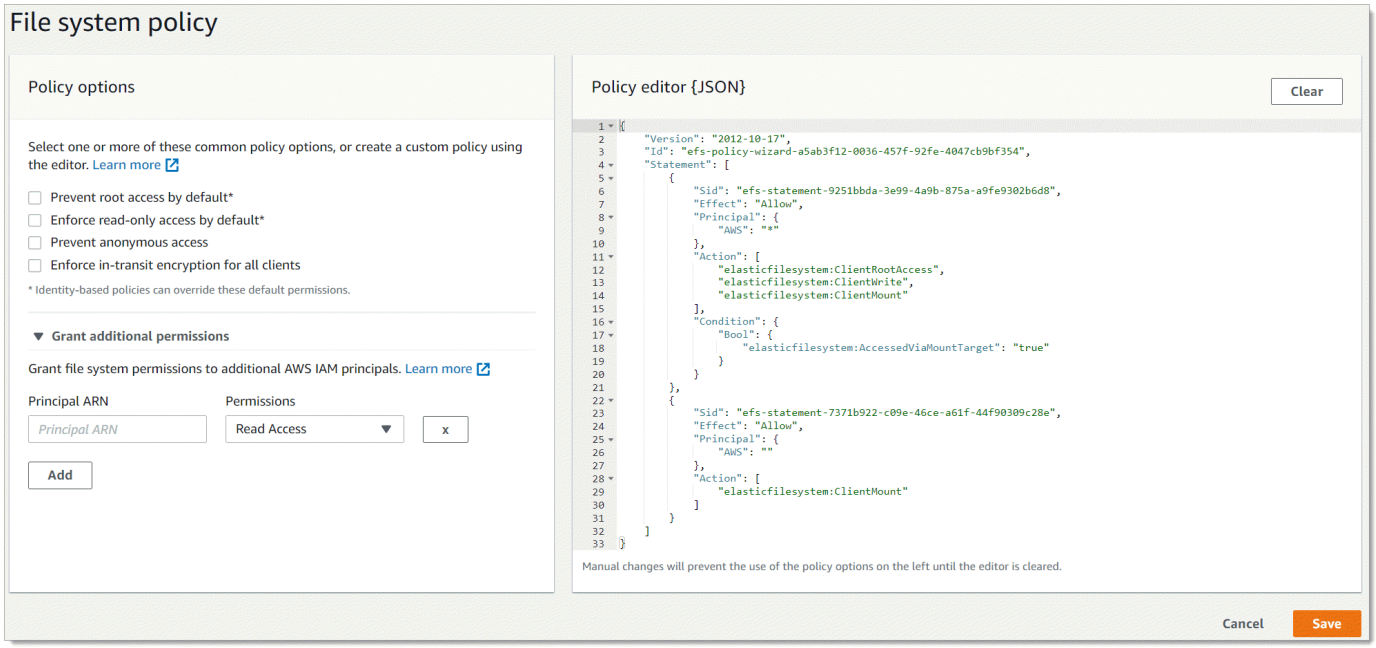
您可以使用 Amazon EFS 主控台或使用 AWS CLI來建立檔案系統政策。您也可以直接使用 AWS 開發套件或 Amazon EFS API，以程式設計方式建立檔案系統政策。EFS 檔案系統政策字元限制為 20,000 以內。如需使用 EFS 檔案系統原則和範例的詳細資訊，請參閱 使用 IAM 控制檔案系統資料存取。

> **Note**
>
> Amazon EFS 檔案系統政策變更可能需要數分鐘才能生效。

建立檔案系統原則 (主控台)

1. 前往 https://console.aws.amazon.com/efs/ 開啟 Amazon Elastic File System 主控台。

2. 選擇 File Systems (檔案系統)。
3. 在 File systems (檔案系統) 頁面上，選擇您要編輯或針對其建立檔案系統政策的檔案系統。即會顯示該檔案系統的詳細資訊頁面。
4. 選擇檔案系統政策，然後選擇編輯。File system policy (檔案系統政策) 頁面隨即顯示。



5. 在政策選項中，您可以選擇任何預先設定的檔案系統原則組合：

   - 預設情況下防止根存取：此選項會 `ClientRootAccess` 從一組允許的 EFS 動作中移除。
   - 預設情況下強制執行唯讀存取：此選項會 `ClientWriteAccess` 從一組允許的 EFS 動作中移除。
   - 防止匿名存取：此選項會 `ClientMount` 從允許的 EFS 動作集中移除。
   - 對所有用戶端強制執行傳輸中加密：此選項會拒絕存取未加密的用戶端。

   當您選擇預先設定的原則時，原則 JSON 物件會顯示在原則編輯器窗格中。

6. 使用「授與其他權限」將檔案系統權限授與其他 IAM 主體，包括另一個 AWS 帳戶主體。選擇新增，然後輸入要授與權限之實體的主體 ARN。選擇您要授予的許可。其他權限會顯示在原則編輯器中。
7. 您可以使用原則編輯器來自訂預先設定的原則，或建立您自己的檔案系統原則。當您使用編輯器時，預先設定的原則選項將無法使用。若要清除目前的檔案系統原則並開始建立新原則，請選擇清除。

   當您清除編輯器時，預先設定的策略會再次變為可用。

8. 完成編輯策略後，請選擇儲存。

建立檔案系統原則 (CLI)

在下列範例中，put-file-system-policyCLI 命令會建立檔案系統原則，以允許指定的 EFS 檔案系統 AWS 帳戶 唯讀存取權。等效 API 命令為 PutFileSystemPolicy。

```
aws efs put-file-system-policy --file-system-id fs-01234567 --policy '{
    "Id": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "elasticfilesystem:ClientMount"
            ],
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            }
        }

    ]
}'
```

```
{
    "FileSystemId": "fs-01234567",
    "Policy": "{
    "Version" : "2012-10-17",
    "Id" : "1",
    "Statement" : [
        {
           "Sid" : "efs-statement-7c8d8687-1c94-4fdc-98b7-555555555555",
           "Effect" : "Allow",
           "Principal" : {
              "AWS" : "arn:aws:iam::111122223333:root"
           },
           "Action" : [
              "elasticfilesystem:ClientMount"
           ],
           "Resource" : "arn:aws:elasticfilesystem:us-east-2:555555555555:file-system/
fs-01234567"
           }
        ]
```

```
    }
}
```

建立存取點

您可以使用 AWS Management Console 或建立 Amazon EFS 存取點 AWS CLI。您也可以直接使用 AWS 開發套件或 Amazon EFS API 以程式設計方式建立存取點。存取點建立後，您就無法修改該存取點。檔案系統最多可以有 1,000 個存取點。如需 EFS 存取點的詳細資訊，請參閱使用 Amazon EFS 存取點。

建立存取點 (主控台)

您可以使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 和 Amazon EFS API 和開發套件來建立和刪除 Amazon EFS 存取點。存取點建立後，您就無法修改該存取點。檔案系統最多可以有 1,000 個存取點。

> **Note**
>
> 如果快速連續傳送多個在相同檔案系統上建立存取點的要求，而且檔案系統已接近 1,000 個存取點的限制，您可能會遇到這些要求的限流回應。這是為了確保檔案系統不會超過指定的存取點配額。

1. 前往 https://console.aws.amazon.com/efs/ 開啟 Amazon Elastic File System 主控台。
2. 選擇「存取點」以開啟「存取點」視窗。
3. 選擇建立存取點以顯示建立存取點頁面。

   您也可以選擇檔案系統來開啟建立存取點頁面。選擇檔案系統名稱或檔案系統 ID，然後選擇存取點和建立存取點，為該檔案系統建立存取點。

   a. 在詳細資訊面板上，輸入以下資訊：

      - 檔案系統：輸入檔案系統名稱或 ID，然後選擇相符的檔案系統。您也可以從選擇輸入欄位時顯示的清單中選擇檔案系統。
      - (選用) 名稱，輸入存取點的名稱。
      - (選用) 根目錄路徑：您可以指定存取點的根目錄；預設存取點根為/。若要輸入根目錄路徑，請使用格式/foo/bar。如需詳細資訊，請參閱 使用存取點強制採用根目錄。

b. (選用) 在 POSIX 使用者面板中，您可以指定完整的 POSIX 身分，以便針對使用該存取點的 NFS 用戶端執行所有檔案作業，以強制執行使用者和群組資訊。如需詳細資訊，請參閱 使用存取點強制執行使用者身分。

- 使用者 ID：輸入使用者的數字 POSIX 使用者 ID。
- 群組 ID：輸入使用者的數字 POSIX 群組 ID。
- 次要群組 ID：輸入選用逗號分隔的次要群組 ID 清單。

c. (選用) 對於根目錄建立許可，您可以指定 Amazon EFS 建立根目錄路徑時要使用的許可 (如果已指定且根目錄不存在)。如需詳細資訊，請參閱 使用存取點強制採用根目錄。

> **Note**
>
> 如果您未指定任何根目錄擁有權和權限，且根目錄尚未存在，EFS 將不會建立根目錄。嘗試使用存取點掛載檔案系統將會失敗。

- 擁有者使用者 ID：輸入用作為根目錄擁有者的數字 POSIX 使用者 ID。
- 擁有者群組 ID：輸入用作根目錄擁有者群組的數字 POSIX 群組 ID。
- 許可：輸入目錄的 Unix 模式。常見的組態是 755。確定已為存取點使用者設定執行位元，以便他們能夠掛載。

4. 選擇建立存取點以使用此組態建立存取點。

建立存取點 (CLI)

在下列範例中，`create-access-point`CLI 命令會為 EFS 檔案系統建立存取點。等效 API 命令為 CreateAccessPoint。

```
aws efs create-access-point --file-system-id fs-abcdef0123456789a --client-token
 010102020-3 \
--root-directory “Path=/efs/mobileapp/
east,CreationInfo={OwnerUid=0,OwnerGid=11,Permissions=775}” \
--posix-user “Uid=22,Gid=4” \
--tags Key=Name,Value=east-users
```

如果要求成功，CLI 會以存取點描述回應。

```
{
```

```
    "ClientToken": "010102020-3",
    "Name": "east-users",
    "AccessPointId": "fsap-abcd1234ef5678901",
    "AccessPointArn": "arn:aws:elasticfilesystem:us-east-2:111122223333:access-point/
fsap-abcd1234ef5678901",
    "FileSystemId": "fs-01234567",
    "LifeCycleState": "creating",
    "OwnerId": "111122223333",
    "PosixUser": {
      "Gid": 4,
      "Uid": 22
    },
    "RootDirectory": {
    "CreationInfo": {
         "OwnerGid": 0,
         "OwnerUid": 11,
         "Permissions": "775"
      },
        "Path": "/efs/mobileapp/east",
    },
    "Tags": []
}
```

> **Note**
>
> 如果快速連續傳送多個在相同檔案系統上建立存取點的要求，而且檔案系統已接近 1,000 個存取點的限制，您可能會遇到這些要求的限流回應。這是為了確保檔案系統不會超過指定的存取點配額。

刪除存取點

刪除存取點時，任何使用該存取點的用戶端都無法存取其所設定之 Amazon EFS 檔案系統。

刪除存取點 (主控台)

1. 前往 https://console.aws.amazon.com/efs/ 開啟 Amazon Elastic File System 主控台。
2. 在左側導覽窗格中，選擇存取點以開啟存取點頁面。
3. 選取要刪除的存取點。
4. 選擇刪除。

5. 選擇確認以確認動作並刪除存取點。

刪除存取點 (CLI)

在下列範例中，delete-access-point CLI 命令會刪除指定的存取點。等效 API 命令為 DeleteAccessPoint。如果命令成功，服務會傳回含有空白 HTTP 主體的 HTTP 204 回應。

```
aws efs delete-access-point --access-point-id fsap-092e9f80b3fb5e6f3 --client-token
 010102020-3
```

標記 Amazon EFS 資源

為協助您管理 Amazon EFS 資源，您可以用標籤形式將您自己的中繼資料指派給每個資源。使用標籤，您可以使用不同的方式對 AWS 資源進行分類，例如按用途、擁有者或環境。當您有許多相同類型的資源時，此分類非常有用 — 您可以根據指定給該資源的標籤快速識別特定資源。本主題說明標籤並示範如何建立它們。

標籤基本概念

標籤是指派給 AWS 資源的標籤。每個標籤皆包含由您定義的一個金鑰與一個選用值。

標籤可讓您以不同的方式對 AWS 資源進行分類，例如，依目的、擁有者或環境。例如，您可以為您帳戶的 Amazon EFS 檔案系統定義一組標籤，協助您追蹤各個檔案系統的擁有者。

我們建議您為每種資源類型建立符合您需求的標籤金鑰。使用一致的標籤金鑰組可讓您更輕鬆管理您的資源。您可以根據您新增的標籤搜尋和篩選資源。

籤對 Amazon EFS 來說不具有任何語意上的意義，並會嚴格解譯為字元字串。此外，標籤不會自動指派給您的資源。您可以編輯標籤金鑰和值，並且可以隨時從資源移除標籤。您可以將標籤的值設為空白字串，但您無法將標籤的值設為 Null。若您將與現有標籤具有相同鍵的標籤新增到該資源，則新值會覆寫舊值。如果您刪除資源，也會刪除任何該資源的標籤。

標籤限制

以下基本限制適用於標籤：

- 每一資源最多標籤數 – 50
- 對於每一個資源，每個標籤金鑰必須是唯一的，且每個標籤金鑰只能有一個值。

- 索引鍵長度上限 - 128 個 UTF-8 Unicode 字元
- 值的長度上限 - 256 個 UTF-8 Unicode 字元
- 雖然 Amazon EFS 允許標籤中的任何字元，但其他服務可能更具限制性。服務間允許的字元包括：可用 UTF-8 表示的英文字母、數字和空格，還有以下字元：+ - = . _ : / @。
- 標籤金鑰與值皆區分大小寫。
- 前aws:綴保留供 AWS 使用。如果標籤具有此字首的標籤金鑰，則您無法編輯或刪除標籤的金鑰或值。具 aws: 字首的標籤，不算在受資源限制的標籤計數內。

您無法僅根據資源的標籤更新或刪除資源；您必須指定資源識別碼。例如，若要刪除您標記有標籤金鑰 (稱為 DeleteMe) 的檔案系統，您必須將 DeleteFileSystem 動作與檔案系統的資源識別碼 (例如 fs-1234567890abcdef0) 結合使用。

當您標記公有或共享資源時，您指派的標籤僅適用於您的 AWS 帳戶. 沒有其他 AWS 帳戶 人可以訪問這些標籤。對於以標籤為基礎的共用資源存取控制，每個標籤都 AWS 帳戶 必須指派自己的一組標籤，以控制對資源的存取。

您可以標記 Amazon EFS 檔案系統和存取點資源。

使用存取控制的標籤

您可以使用標籤來控制對 Amazon EFS 資源的存取，以及實作屬性型存取控制 (ABAC)。

> **Note**
>
> 複寫不支援將標籤用於屬性型存取控制 (ABAC)。

標記您的 資源

您可以為您帳戶中現有的 Amazon EFS 檔案系統和存取點資源新增標籤。

標記檔案系統或存取點資源 (主控台)

- 您可以使用資源詳細資料畫面上的標籤索引標籤，使用 Amazon EFS 主控台將標籤套用至現有資源。在 Amazon EFS 主控台中，您可以在建立資源時指定資源的標籤。例如，您可以使用 Name 做為鍵以及您指定的值來新增標籤。在大多數的案例中，主控台會立即在建立資源後套用標籤 (而非在資源建立過程時)。主控台可能會根據 Name 標籤整理資源，但此標籤對 Amazon EFS 服務來說不具有任何語意上的意義。

標記檔案系統或存取點資源 (CLI)

- 如果您使用的是 Amazon EFS API AWS CLI、或 AWS 開發套件，則可以使用 `TagResource` EFS API 動作將標籤套用至現有資源。此外，有些資源建立動作可讓您在建立資源時指定資源的標籤。

  下表列出了用於管理標籤的 AWS CLI 命令以及對等的 Amazon EFS API 動作。

CLI 命令	描述	等效的 API 操作
tag-resource	新增標籤或更新現有的標籤	TagResource
list-tags-for-resource	擷取現有的標籤	ListTagsForResource
untag-resource	刪除現有的標籤	UntagResource

安裝 Amazon EFS 工具

此 amazon-efs-utils 套件是 Amazon EFS 工具的開放原始碼集合，該集合也稱為 Amazon EFS 用戶端。在以下內容中，您可以找到 Amazon EFS 用戶端的說明。Amazon EFS 掛載協助程式包含在 Amazon EFS 用戶端中，可讓您更輕鬆地掛載 EFS 檔案系統。使用 EFS 用戶端可以使用 Amazon CloudWatch 監控 EFS 檔案系統的掛載狀態。掛載 EFS 檔案系統之前，您需要在 Amazon EC2 執行個體上安裝 Amazon EFS 用戶端。

主題

關於 Amazon EFS 用戶端

Amazon EFS 用戶端 (amazon-efs-utils) 是 Amazon EFS 工具的開放原始碼集合。使用 Amazon EFS 客戶端無需額外費用，您可以從以下 GitHub 位置下載：https://github.com/aws/efs-utils。

該amazon-efs-utils軟件包預先安裝在 Amazon Linux 2023（AL2023），Amazon Linux 2（AL2）和 Amazon Linux（AL1）Amazon 機器映像（AMI）上。 套件可在 Amazon Linux 套件儲存庫中取得，您可以在其他 Linux 發行版本建置和安裝套件。您也可以使 AWS Systems Manager 用自動安裝或更新套件。如需詳細資訊，請參閱 用 AWS Systems Manager 於自動安裝或更新 Amazon EFS 用戶端。

> **Note**
>
> Amazon Linux（AL1）AMI 於 2023 年 12 月 31 end-of-life 日到達，並且不支持 2024 年 4 月及更高版本（2.0 及更高版本）發布的amazon-efs-utils軟件包。我們建議您將應用程式升級到 Amazon Linux 2023 (AL2023)，其中包括直到 2028 年的長期支援。

Amazon EFS 用戶端包含掛載協助程式和工具，以便更輕鬆地為 Amazon EFS 檔案系統執行傳輸中的資料加密。掛載協助程式是您在掛載特定類型的檔案系統時所使用的一種程式。我們建議您使用 Amazon EFS 用戶端中包含的掛載協助程式，來掛載 Amazon EFS 檔案系統。使用 Amazon EFS 用

戶端可簡化 EFS 檔案系統的掛載操作，並改善檔案系統效能。如需使用 EFS 客戶端和掛載協助程式的詳細資訊，請參閱 掛載 EFS 檔案系統。

當您安裝 amazon-efs-utils 套件時，系統會自動安裝 amazon-efs-utils 中的依存項目。

- NFS 用戶端
  - nfs-utils 適用於 RHEL、CentOS、Amazon Linux 和 Fedora 發行版
  - nfs-common 適用於 Debian 和 Ubuntu 發行版
- 網路轉送 (stunnel 套件、版本 4.56 或更新版本)
- Python (版本 3.4 或更新版本)
- OpenSSL 1.0.2 或更新版本

> **Note**
>
> 預設下，使用 Amazon EFS 掛載協助程式搭配 Transport Layer Security (TLS) 時，掛載協助程式會強制執行憑證主機名稱檢查。Amazon EFS 掛載協助程式使用其 TLS 功能的 stunnel 程式。某些版本的 Linux 操作系統，預設下不包含 stunnel 支援 TLS 功能的版本。使用其中一個 Linux 版本時，使用 TLS 掛載 Amazon EFS 檔案系統。
> 安裝 amazon-efs-utils 套件后，如需升級系統的 stunnel 版本，請參閱 升級 stunnel。
> 您可以用 AWS Systems Manager 來管理 Amazon EFS 用戶端，並自動執行在 EC2 執行個體上安裝或更新 amazon-efs-utils 套件所需的任務。如需詳細資訊，請參閱 用 AWS Systems Manager 於自動安裝或更新 Amazon EFS 用戶端。
> 對於加密的問題，請參閱 故障診斷加密。

支援的發行版

Amazon EFS 用戶端已驗證了下列 Linux 和 Mac 發行版：

發佈	套件類型	**init** 系統
Amazon Linux 2023 (AL2023)	rpm	systemd
Amazon Linux 2 (AL2)	rpm	systemd
CentOS 7, 8	rpm	systemd

發佈	套件類型	**init** 系統
Amazon 亞馬遜 **Note** Amazon Linux（AL1）AMI 於 2023 年 12 月 31 end-of-life 日到達，並且不支持 2024 年 4 月或更高版本（2.0 及更高版本）發行的`amazon-efs-utils` 軟件包。	rpm	`upstart`
Debian 9、Debian 10 操作系統	deb	`systemd`
Fedora 28 - Fedora 32 操作系統	RPM	`systemd`
macOS Big Sur		`launchd`
macOS Monterey		`launchd`
macOS Ventura		`launchd`
OpenSUSE Leap, Tumbleweed	RPM	`systemd`
Oracle8	rpm	`systemd`
紅帽企業版 (RHEL) 7, 8, 9	rpm	`systemd`
SUSE Linux Enterprise Server (SLES) 12, 15	RPM	`systemd`
Ubuntu 16.04 LTS, 18.04 LTS, 20.04 LTS	deb	`systemd`

如需套件已經過驗證的受支援發行版的完整清單，請參閱 Github 上 `amazon-efs-utils` 的 README。

用 AWS Systems Manager 於自動安裝或更新 Amazon EFS 用戶端

您可以使用 AWS Systems Manager 來簡化 Amazon EFS 用戶端 (amazon-efs-utils) 的管理作業。 AWS Systems Manager 是可用來檢視和控制基礎結構的 AWS 服務 AWS。 AWS Systems Manager 您可以使用自動化 EC2 執行個體上安裝或更新amazon-efs-utils套件所需的工作。Systems Manager 功能 (例如 Distributor 和 Systems Manager) 可讓您自動進行下列程序：

- 維護 Amazon EFS 用戶端的版本控制。
- 集中存放 Amazon EFS 用戶端，並有系統地將其分配到 Amazon EC2 執行個體中。
- 自動化程序使您的 Amazon EC2 執行個體維持在定義的狀態。

如需詳細資訊，請參閱 AWS Systems Manager 使用者指南。

Amazon EFS 客戶端在安裝過程中的作用

您可以使用 Amazon EFS 用戶端自動監控 Amazon CloudWatch 日誌的檔案系統掛載狀態，並升級stunnel到所選 Linux 發行版的最新版本。使用 Systems Manager 在 Amazon EC2 執行個體上安裝 Amazon EFS 用戶端時，會執行下列動作：

- 使用 安裝和升級 botocore 中所述的相同步驟安裝 botocore 套件。Amazon EFS 用戶端用 botocore 來監控 EFS 檔案系統掛載狀態。
- 透過更新，啟用對 CloudWatch 記錄檔中 EFS 檔案系統掛載狀態的監控efs-utils.conf。如需詳細資訊，請參閱 監視掛載嘗試成功或失敗狀態。
- 對於執行 RHEL7 或 CentOS7 的 EC2 執行個體，Amazon EFS 用戶端會按照 升級 stunnel 中所述自動升級 stunnel。需要升級 stunnel 才能使用 TLS 成功掛載 EFS 檔案系統，而且隨附 RHEL7 和 CentOS7 的 stunnel 版本不支援 Amazon EFS 用戶端 (amazon-efs-utils)。

Systems Manager Distributor 支援的操作系統

您的 EC2 執行個體必須執行下列其中一個操作系統，才能與 AWS Systems Manager 共同作用，實現自動更新或安裝 Amazon EFS 用戶端。

平台	平台版本	架構
Amazon Linux 2023 (AL2023)	AL2023	x86_64 (重力同 2 或更新版本的處理器)

平台	平台版本	架構
Amazon Linux 2 (AL2)	2.0	x86_64, arm64 (Amazon Linux 2、A1 執行個體類型)
Amazon 亞馬遜	2017.09, 2018.03	x86_64
CentOS	7、8	x86_64
Red Hat Enterprise Linux (RHEL)	7、8	x86_64、arm64 (RHEL 7.6 及更新版本、A1 執行個體類型)
SUSE Linux Enterprise Server (SLES)	12, 15	x86_64
Ubuntu Server	16.04、18.04、20.04	x86_64, arm64 (Ubuntu Server 16 和更新版本、A1 執行個體類型)

如何使用 AWS Systems Manager 自動安裝或更新 amazon-efs-utils

若要設定 Systems Manager 自動安裝或更新 amazon-efs-utils 套件，需要兩種一次性設定。

1. 設定具有所需權限的 AWS Identity and Access Management (IAM) 執行個體設定檔。
2. 設定用於安裝或更新 State Manager Association (包括排程) 的過程

步驟 1：使用所需許可設定 IAM 執行個體設定檔。

依預設， AWS Systems Manager 沒有管理 Amazon EFS 用戶端以及安裝或更新 amazon-efs-utils 套件的權限。您必須使用 AWS Identity and Access Management (IAM) 執行個體設定檔授予對 Systems Manager 的存取權限。執行個體設定檔是在啟動時將 IAM 角色資訊傳遞到 EC2 執行個體的容器。

使用受`AmazonElasticFileSystemsUtils` AWS 管理的權限原則將適當的權限指派給角色。您可以為執行個體設定檔建立新角色或將 `AmazonElasticFileSystemsUtils` 許可政策新增至現有角色。然後，您必須使用此執行個體設定檔來啟動 Amazon EC2 執行個體。如需詳細資訊，請參閱步驟 4：建立 Systems Manager 的 IAM 執行個體設定檔。

步驟 2：設定 State Manager Association，用於安裝或更新 Amazon EFS 用戶端

amazon-efs-utils 套件隨附於 Distributor 中，並準備好讓您部署至受管 EC2 執行個體。若要檢視可供安裝amazon-efs-utils的最新版本，您可以使用 AWS Systems Manager 主控台或偏好的 AWS 命令列工具。若要存取 Distributor，請開啟 https://console.aws.amazon.com/systems-manager/，並在左側導覽窗格中選擇 Distributor。在 Amazon 所有區段找到 AmazonEFSUtils。選擇 AmazonEFSUtils，查看套件詳細資訊。如需詳細資訊，請參閱檢視套件。

使用 State Manager，您可以立即或按計劃在受管 EC2 執行個體上安裝或更新 amazon-efs-utils 套件。此外，您可以確保 amazon-efs-utils 自動安裝在新 EC2 執行個體上。如需有關使用 Distributor 和 State Manager 安裝或更新套件的詳細資訊，請參閱使用 Distributor。

若要使用 Systems Manager 主控台在執行個體上自動安裝或更新 amazon-efs-utils 套件，請參閱排程套件安裝或更新 (主控台)。系統會提示您建立關聯 State Manager，該關聯會定義您要套用至一組執行個體的狀態。建立關聯時，請使用下列輸入：

- 針對參數，選擇動作 > 安裝和安裝類型 > 原地更新。
- 對於目標，建議設定為選擇所有執行個體，以將所有新的和現有的 EC2 執行個體註冊為自動安裝或更新 AmazonEFSUtils。或者，您也可以指定執行個體標記、手動選擇執行個體，或選擇資源群組，以便將該關聯套用至執行個體子集中。如果指定執行個體標籤，則必須使用標籤啟動 EC2 執行個體，以允許 AWS Systems Manager 自動安裝或更新 Amazon EFS 用戶端。
- 對於指定排程，建議將 AmazonEFSUtils 設定為每 30 天一次。使用控制項來為關聯建立 Cron 或速率排程。

若 AWS Systems Manager 要使用將多個 Amazon EFS 檔案系統掛接到多個 EC2 執行個體，請參閱使用將 EFS 掛接到多個 EC2 執行個體 AWS Systems Manager。

手動安裝 Amazon EFS 用戶端

您可以在 Amazon EC2 Linux 執行個體上手動安裝 Amazon EFS 用戶端 2023 (AL2023)、Amazon Linux 2 (AL2)、Amazon Linux (AL1)、其他支援的 Linux 發行套件，以及在執行 macOS 大蘇爾、macOS 蒙特雷和 macOS 文圖拉的 EC2 Mac 執行個體上。

這些操作系統的 安裝程序如下區段所述。如需有關安裝和更新 Amazon EFS 用戶端的指示，請參閱 Github 上的amazon-efs-utils讀我檔案中的安裝。

主題

- 在 Amazon EC2 Linux 執行個體上安裝亞馬遜 EFS 用戶端
- 在其他 Linux 發行版上安裝 Amazon EFS 用戶端
- 執行 macOS Big Sur、macOS Monterey 或 macOS Ventura 時，將 Amazon EFS 安裝在 EC2 Mac 執行個體上。

在 Amazon EC2 Linux 執行個體上安裝亞馬遜 EFS 用戶端

從下列位置安裝在 Amazon EC2 Linux 執行個體上的`amazon-efs-utils`套件：

- 適用於 Amazon Linux 的 Amazon 機器映像（AMI）軟件包存儲庫。下列說明是從 AMI `amazon-efs-utils` 套件儲存庫安裝套件的說明。
- AWS EFS-實用程序 GitHub 存儲庫。如需有關從中安裝`amazon-efs-utils`套件的詳細資訊 GitHub，請參閱在其他 Linux 發行版上安裝 Amazon EFS 用戶端。

> **Note**
>
> - 如果您使用的是 AWS Direct Connect，您可以在中找到安裝說明逐步解說：使用 AWS Direct Connect 和 VPN 建立和掛載內部部署的檔案系統。
> - Amazon Linux（AL1）AMI 於 2023 年 12 月 31 end-of-life 日到達，並且不支持 2024 年 4 月及更高版本（2.0 及更高版本）發布的`amazon-efs-utils`軟件包。我們建議您將應用程式升級至亞馬遜 Linux 2023 (AL2023)，其中包括直到 2028 年的長期支援。

若要從 Amazon EC2 Linux 執行個體上的 AMI 套件儲存庫安裝套件 **`amazon-efs-utils`**

1. 請確定您已建立 AL2023、Amazon 2 (AL2) 或 Amazon 伺服器 (AL1) EC2 執行個體。有關如何執行此操作的詳細資訊，請參閱步驟 1：啟動執行個體。
2. 透過安全殼層 (SSH) 存取執行個體的終端機，並使用適當的使用者名稱登入。有關如何執行此操作的詳細資訊，請參閱使用安全殼層從 Linux 或 macOS Connect 到您的 Linux 執行個體。
3. 若要安裝此 `amazon-efs-utils` 套件，請執行下列命令：

```
sudo yum install -y amazon-efs-utils
```

在其他 Linux 發行版上安裝 Amazon EFS 用戶端

如果您不想從 Amazon Linux AMI `amazon-efs-utils` 套件儲存庫取得套件，也可以在上取得該套件 GitHub。

複製套件後，根據 Linux 發行版本支援的套件類型，您可以使用以下一種方法建置和安裝 `amazon-efs-utils`：

- RPM — 此套件類型受 Amazon Linux 2023 (AL2023)、Amazon Linux 2 (AL2)、Amazon Linux (AL1)、紅帽 Linux、CentOS 及類似產品的支援。
- DEB – 此套件類型受 Ubuntu、Debian 和類似發行版本的支援。

有關為其他 Linux 發行版安裝`amazon-efs-utils`軟件包的說明，請參閱 Github 上的`amazon-efs-utils`自述文件中的其他 Linux 發行版本。

執行 macOS Big Sur、macOS Monterey 或 macOS Ventura 時，將 Amazon EFS 安裝在 EC2 Mac 執行個體上。

執行 macOS Big Sur、macOS Monterey 或 macOS Ventura 時，可將 `amazon-efs-utils` 套件安裝在 EC2 Mac 執行個體上。

如需在 Mac 執行個體上安裝`amazon-efs-utils`套件的說明，請參閱在 macOS 大蘇爾、MacOS 蒙特雷、macOS 索諾瑪和 macOS 文圖拉散佈在 Github 上的`amazon-efs-utils`讀我檔案中。

後續步驟

在 EC2 執行個體上安裝 `amazon-efs-utils` 之後，請繼續執行掛載檔案系統的後續步驟：

- 安裝以`botocore`便您可以使用 Amazon CloudWatch 監控檔案系統的掛載狀態。
- 升級至 `stunnel` 最新版本以啟用傳輸中的資料加密功能。
- 使用 EFS 掛載協助程式掛載檔案系統。

安裝和升級 `botocore`

Amazon EFS 用戶端用`botocore`來與其他 AWS 服務互動。如果您想要在 CloudWatch 日誌中監控 Amazon EFS 檔案系統的掛載嘗試成功或失敗，則必須執行此動作。如需詳細資訊，請參閱 監視掛載嘗試成功或失敗狀態。

有關安裝和升級的說明botocore，請參閱 Github 上的amazon-efs-utils自述文件botocore中的安裝。

升級 stunnel

使用 Amazon EFS 掛載協助程式對傳輸中的資料進行加密時，需要 OpenSSL 版本 1.0.2 或更新版本，同時需要支援線上憑證狀態通訊協定 (OCSP) 和憑證主機名稱檢查的 stunnel 版本。Amazon EFS 掛載協助程式使用其 TLS 功能的 stunnel 程式。注意某些版本的 Linux 操作系統，預設下不包含 stunnel 支援 TLS 功能的版本。使用其中一個 Linux 發行版本時，藉助 TLS 來掛載 Amazon EFS 檔案系統會失敗。

在安裝 Amazon EFS 掛載協助程式後，您可以透過下列指示來升級系統版本 stunnel。

在 Amazon Linux、Amazon Linux 2 和其他支援的 Linux 發行版本 (除了 SLES 12) 上升級 **stunnel**

1. 在網頁瀏覽器中，前往 stunnel 下載頁面 https://stunnel.org/downloads.html。
2. 尋找以 tar.gz 格式提供的 stunnel 最新版本。請記下檔案名稱，您會需要在後續步驟中用到。
3. 開啟 Linux 用戶端的終端機，依顯示順序執行下列命令。

   a. 對於 RPM：

   ```
   sudo yum install -y gcc openssl-devel tcp_wrappers-devel
   ```

   對於 DEB：

   ```
   sudo apt-get install build-essential libwrap0-dev libssl-dev
   ```

   b. 將 *latest-stunnel-version* 取代為您在稍早步驟 2 中記下的檔案名稱。

   ```
   sudo curl -o latest-stunnel-version.tar.gz https://www.stunnel.org/
   downloads/latest-stunnel-version.tar.gz
   ```

   c.
   ```
   sudo tar xvfz latest-stunnel-version.tar.gz
   ```

   d.
   ```
   cd latest-stunnel-version/
   ```

   e.
   ```
   sudo ./configure
   ```

f.
```
sudo make
```

g. 目前的 stunnel 套件已安裝在 bin/stunnel 中。因此，您可以安裝新版本，請使用下列命令移除該目錄。

```
sudo rm /bin/stunnel
```

h. 若要安裝最新版本：

```
sudo make install
```

i. 創建 symlink：

```
sudo ln -s /usr/local/bin/stunnel /bin/stunnel
```

若要在 macOS 上升級 stunnel

- 在 EC2 Mac 執行個體上開啟終端機，然後執行下列命令以升級至最新版本的 stunnel。

```
brew upgrade stunnel
```

在 SLES 12 上升級 stunnel

- 執行下列指令，並依照 zypper 套件管理員指示，在執行 SLES12 的運算執行個體上升級 stunnel。

```
sudo zypper addrepo https://download.opensuse.org/repositories/security:Stunnel/
SLE_12_SP5/security:Stunnel.repo
sudo zypper refresh
sudo zypper install -y stunnel
```

使用所需的功能安裝的某個版本 stunnel 後，您可以使用 TLS 掛載檔案系統與 Amazon EFS 建議的設定。

停用憑證主機名稱檢查

如果您無法安裝所需的相依性，您可以在 Amazon EFS 掛載協助程式組態中選擇性地停用憑證主機名稱檢查。我們不建議您在生產環境中停用此功能。若要停用憑證主機名稱檢查，請執行下列動作：

1. 使用您選擇的文字編輯器，開啟 `/etc/amazon/efs/efs-utils.conf` 檔案。
2. 將 `stunnel_check_cert_hostname` 值設為 false。
3. 將變更儲存到檔案並將其關閉。

如需使用傳輸中資料加密的詳細資訊，請參閱 掛載 EFS 檔案系統。

啟用線上憑證狀態通訊協定

為了在無法從 VPC 存取 CA 時，讓檔案系統可用性最大化，當您選擇加密傳輸中的資料時，線上憑證狀態通訊協定 (OCSP) 預設不會啟用。Amazon EFS 會使用 Amazon 憑證授權(CA) 來發行和簽署其 TLS 憑證，而 CA 則會指示用戶端使用 OCSP 檢查已撤銷的憑證。OCSP 端點必須可以透過網際網路，從您的 Virtual Private Cloud 存取，以便檢查憑證的狀態。在服務內，EFS 會持續監控憑證狀態並核發新的憑證，以取代任何它所偵測到的已撤銷憑證。

為了盡可能提供最強的安全，您可以啟用 OCSP，讓您的 Linux 用戶端可以檢查已撤銷憑證。OCSP 可保護不受惡意使用已撤銷憑證的危害，雖然這種情況在您的 VPC 中極為罕見。如果 EFS TLS 憑證已撤銷，Amazon 會發佈資訊安全公告，並且發行新版本的 EFS 掛載協助程式，該協助程式會拒絕已撤銷的憑證。

在您的 Linux 用戶端上針對所有未來與 EFS 的 TLS 連線啟用 OCSP

1. 在您的 Linux 用戶端上開啟終端機。
2. 使用您選擇的文字編輯器，開啟 `/etc/amazon/efs/efs-utils.conf` 檔案。
3. 將 `stunnel_check_cert_validity` 值設為 true。
4. 將變更儲存到檔案並將其關閉。

在 **`mount`** 命令中啟用 OCSP

- 在掛載檔案系統時，使用以下掛載命令啟用 OCSP。

```
$ sudo mount -t efs -o tls,ocsp fs-12345678:/ /mnt/efs
```

掛載 EFS 檔案系統

在下列區段中，您可以了解如何使用 Amazon EFS 掛載協助程式掛載 Amazon EFS 檔案系統。此外，了解如何使用 `fstab` 檔案，讓檔案系統在任何系統重新啟動後自動重新掛載。使用 EFS 掛載協助程式，您可以選擇下列掛載 Amazon EFS 檔案系統的選項：

- 在支援的 EC2 執行個體上掛載
- 使用 IAM 授權掛載
- 使用 Amazon EFS 存取點掛載
- 使用內部部署的 Linux 用戶端掛載
- EC2 執行個體重新啟動時自動掛載 EFS 檔案系統
- 建立新 EC2 執行個體時掛載檔案系統

> **Note**
>
> Amazon EFS 不支援從 Amazon EC2 Windows 執行個體中掛載。

EFS 掛載協助程式是 `amazon-efs-utils` 套件的一部分。`amazon-efs-utils` 套件是 Amazon EFS 工具的開放原始碼集合。如需詳細資訊，請參閱 手動安裝 Amazon EFS 用戶端。

在 Amazon EFS 掛載協助程式可供使用前，我們建議使用標準 Linux NFS 用戶端來掛載 Amazon EFS 檔案系統。如需詳細資訊，請參閱 使用網路檔案系統掛載 EFS 檔案系統。

主題

使用 EFS 掛載協助程式掛載 EFS 檔案系統

EFS 掛載協助程式可協助您將 EFS 檔案系統掛載到 EC2 Linux 和 Mac 執行個體上，執行列在 關於 Amazon EFS 用戶端 中支援的發行版。

Amazon EFS 掛載協助程式會將掛載檔案系統簡化。根據預設，其中包含 Amazon EFS 建議掛載選項。此外，基於疑難排解考量，掛載協助程式具有內建的記錄功能。如果您的 Amazon EFS 檔案系統發生問題，可以與 Sup AWS port 部門共用這些日誌。如需關於掛載檔案系統的詳細資訊，請參閱 掛載 EFS 檔案系統。

> **Note**
>
> Amazon EFS 不支援從 Amazon EC2 Windows 執行個體中掛載。

主題

運作方式

掛載協助程式定義一個稱為 `efs` 的全新網路檔案系統類型，此類型與在 Linux 中標準 `mount` 命令完全相容。掛載協助程式也支援使用EC2 Linux 執行個體 `/etc/fstab` 組態檔案中的項目，在執行個體啟動時自動掛載 Amazon EFS 檔案系統。

> **Warning**
>
> 使用 _netdev 選項，此選項用於在自動掛載檔案系統時識別網路檔案系統。若 _netdev 已遺失，EC2 執行個體可能會停止回應。此結果是因為網路檔案系統在運算執行個體開始聯網後需要初始化。如需詳細資訊，請參閱 自動掛載失敗且執行個體沒有回應。

您可以指定下列一個屬性來掛載檔案系統：

- 檔案系統 DNS 名稱：如果您使用檔案系統 DNS 名稱，且掛載協助程式無法解析該名稱，例如當您在不同的 VPC 中掛載檔案系統時，該名稱將回復為使用掛載目標 IP 地址。如需詳細資訊，請參閱 從另一個 AWS 帳戶 或 VPC 掛載 EFS 檔案系統。
- 檔案系統 ID：如果您使用檔案系統 ID，則掛載協助程式會將其解析為掛載目標彈性網絡介面 (ENI) 的本機 IP 地址，而不呼叫外部資源。
- 掛載目標 IP 地址：您可以使用一個檔案系統掛載目標的 IP 地址。

您可以在 Amazon EFS 主控台中找到所有這些屬性的值。您可以在連接熒幕中找到檔案系統 DNS 名稱。

將傳輸中的資料加密宣告為 Amazon EFS 檔案系統的掛載選項時，掛載協助程式會初始化用戶端 `stunnel` 程序與稱為 `amazon-efs-mount-watchdog` 的監管程序。此 `amazon-efs-mount-watchdog` 程序會監控 TLS 掛載的運作狀態，並在第一次透過 TLS 掛載 EFS 檔案系統時自動啟動。如果您的用戶端是在 Linux 上執行，則此程序會根據 Linux 分佈由 `upstart` 或 `systemd` 來管理。對於在支援 macOS 上執行的用戶端，由 `launchd` 管理。

`Stunnel` 是一種開放原始碼多功能網路轉送。用戶端 `stunnel` 程序會在本機連接埠上接聽傳入流量，以及掛載協助程式會將 NFS 用戶端流量重新導向到此本機連接埠。

掛載協助程式使用 TLS 版本 1.2 來與檔案系統通訊。使用 TLS 需要憑證，而且這些憑證是由信任的 Amazon 憑證授權單位所簽署。如需加密運作方式的詳細資訊，請參閱 Amazon EFS 的資料加密。

Amazon EFS 客戶端使用的掛載選項

Amazon EFS 掛載協助程式用戶端使用下列 Amazon EFS 優化的掛載選項：

- `nfsvers=4.1`：在 EC2 執行個體上掛載時使用

  `nfsvers=4.0`：在執行 macOS Big Sur、Monterey 和 Ventura 的支援 EC2 Mac 執行個體上掛載使用。

- `rsize=1048576`：設定 NFS 用戶端為每個網路 READ 請求接收的資料位元組上限為 1048576 (最大可用值)，以避免效能降低。
- `wsize=1048576`：設定 NFS 用戶端為每個網路 WRITE 請求發送的資料位元組上限為 1048576 (最大可用值)，以避免效能降低。
- `hard`：設定 NFS 用戶端在 NFS 請求逾時的復原行為，因此 NFS 請求會重試直到伺服器回覆為止，以確保資料完整。
- `timeo=600`：將 NFS 用戶端等待重試 NFS 請求回應的逾時值設為 600 十分之一秒 (60 秒)，以避免效能降低。
- `retrans=2`：將 NFS 用戶端在請求嘗試進一步復原動作前的重試次數設為 2。
- `noresvport`：告知 NFS 用戶端在網路連線重新建立時，使用新的傳輸控制通訊協定 (TCP) 來源連接埠。使用 `noresvport` 選項，以確保您的 EFS 檔案系統在重新連線或網路復原事件發生後持續可用。
- `mountport=2049`：僅在執行 macOS Big Sur、Monterey 和 Ventura 的 EC2 Mac 執行個體上掛載時使用。

取得支援日誌

掛載協助程式具有 Amazon EFS 檔案系統的內建記錄。您可以與 Sup AWS port 人員共用這些記錄，以進行疑難排解。您可以使用 EFS 掛載協助程式找到儲存在 `/var/log/amazon/efs` 用戶端上的日誌。這些日誌適用於 EFS 掛載協助程式，stunnel 程序 (預設禁用) 和監控 stunnel 程序的 `amazon-efs-mount-watchdog` 程序。

> **Note**
>
> `amazon-efs-mount-watchdog` 程式可確保每個掛載的 stunnel 程序為執行中，並在 Amazon EFS 檔案系統卸載時停止 stunnel 程式。如果因為某些原因而導致 stunnel 程序意外終止，監視程式程序會將其重新啟動。

您可以在 `/etc/amazon/efs/efs-utils.conf` 中變更日誌的組態。若要讓任何記錄變更生效，您必須使用 EFS 掛載協助程式卸載和重新掛載檔案系統。掛載協助程式與監視程式日誌的日誌容量限制為 20 MiB。stunnel 程序的日誌依預設是停用的。

> **Important**
>
> 您可以啟用 stunnel 程序日誌的記錄。然而，啟用 stunnel 日誌可能會在您的檔案系統佔用極大的空間。

使用 EFS 掛載協助程式的先決條件

您可以使用 Amazon EFS 掛載協助程式在 Amazon EC2 執行個體上掛載 Amazon EFS 檔案系統。若要使用掛載協助程式，您需要下列資訊：

- 掛載的檔案系統 ID：EFS 掛載協助程式將檔案系統 ID 解析為掛載目標彈性網絡介面 (ENI) 的本機 IP 地址，而不呼叫外部資源。
- Amazon EFS 掛載目標：您在虛擬私有雲端 (VPC) 中建立掛載目標。如果您使用服務建議的設定值在主控台中建立檔案系統，則會在檔案系統所在的每個可用區域中建立掛載目標。 AWS 區域 如需關於建立掛載目標的說明，請參閱 管理掛載目標。

  > **Note**
  >
  > 建議您在新建立的掛載目標的生命週期狀態可用之後等待 60 秒，然後再通過 DNS 掛載檔案系統。此等待可讓 DNS 記錄在檔案系統所在的 AWS 區域 位置完全傳播。

  如果您在與您 EC2 執行個體不同的可用區域中使用掛載目標，您需要為跨可用區域傳送的資料支付標準 EC2 費用。您的檔案系統操作也可能受到延遲。
- 從其他可用區域掛載單區域檔案系統：
  - 檔案系統可用區域名稱：如果您正在掛載 EFS 單區域檔案系統，且該檔案系統位於與 EC2 執行個體不同可用區域。
  - 掛載目標 DNS 名稱：或者，您可以指定掛載目標的 DNS 名稱來替代可用區域名稱。
- 執行支援 Linux 或 macOS 分佈的 Amazon EC2 執行個體：使用掛載協助程式掛載檔案系統的支援發行版如下：
  - Amazon Linux 2
  - Amazon Linux 2023
  - Amazon Linux 2017.09 和更新版本
  - macOS Big Sur

- Red Hat Enterprise Linux (和例如 CentOS 之類的導數) 版本 7 和更新版本
- Ubuntu 16.04 LTS 和更新版本

> **Note**
>
> 執行 macOS Big Sur 的 EC2 Mac 執行個體支援 NFS 4.0。

- Amazon EFS 掛載協助程式已安裝在 EC2 執行個體上：掛載協助程式是一款公用程式 `amazon-efs-utils` 套件中的工具。如需關於安裝 `amazon-efs-utils` 的資訊，請參閱 EFS 用戶端的自動化安裝 和手動安裝 `amazon-efs-utils`。
- 在 VPC 中的 EC2 執行個體：正在連接的 EC2 執行個體，必須位於以 Amazon VPC 服務為基礎的虛擬私有雲端 (VPC) 中。還必須將其配置為使用由提供的 DNS 服務器 AWS。如需 Amazon DNS 伺服器的資訊，請參閱《Amazon VPC 使用者指南》中的 DHCP 選項集。
- VPC 已啓用 DNS 主機名稱：連接的 EC2 執行個體的 VPC 必須已啟用 DNS 主機名稱。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的檢視 EC2 執行個體的 DNS 主機名稱。
- 對於不同的 EC2 執行個體和檔案系統 AWS 區域 — 如果要掛載的 EC2 執行個體和檔案系統位於不同的位置 AWS 區域，則需要編輯`efs-utils.conf`檔案中的`region`屬性。如需詳細資訊，請參閱從其他裝載 Amazon EFS 檔案系統 AWS 區域。

使用 EFS 掛載協助程式在 Amazon EC2 Linux 執行個體上掛載

此程序需要下列項目：

- 您已經在 EC2 執行個體上安裝了 `amazon-efs-utils` 套件。如需詳細資訊，請參閱 手動安裝 Amazon EFS 用戶端。
- 您已經為檔案系統建立了掛載目標。如需詳細資訊，請參閱 管理掛載目標。

在 EC2 Linux 執行個體上使用 Amazon EFS 掛載協助程式掛載 Amazon EFS 檔案系統。

1. 透過 Secure Shell (SSH) 打開 EC2 執行個體的終端機，並使用適當的使用者名稱登入。如需詳細資訊，請參閱使用安全殼層從 Linux 或 macOS Connect 至您的 Linux 執行個體。
2. 使用下列指令建立要用作檔案系統掛載點的目錄 `efs`：

   ```
   sudo mkdir efs
   ```

3. 執行下列一項命令來掛載檔案系統。

> **Note**
>
> 如果 EC2 執行個體和您要掛載的檔案系統位於不同的 AWS 區域區域，請參閱 從其他裝載 Amazon EFS 檔案系統 AWS 區域 以編輯 `efs-utils.conf` 檔案中的 `region` 屬性。

- 使用檔案系統 ID 掛載：

```
sudo mount -t efs file-system-id efs-mount-point/
```

請在 *file-system-id* 和 `efs` 中使用您正在掛載的檔案系統 ID 來取代 *efs-mount-point*。

```
sudo mount -t efs fs-abcd123456789ef0 efs/
```

或者，如果您想要使用傳輸中資料的加密，可以使用下列命令來掛載檔案系統。

```
sudo mount -t efs -o tls fs-abcd123456789ef0:/ efs/
```

- 使用檔案系統 DNS 名稱掛載：

```
sudo mount -t efs -o tls file-system-dns-name efs-mount-point/
```

```
sudo mount -t efs -o tls fs-abcd123456789ef0.efs.us-east-2.amazonaws.com efs/
```

- 使用下列掛載目標 IP 地址掛載：

```
sudo mount -t efs -o tls,mounttargetip=mount-target-ip file-system-id efs-mount-point/
```

```
sudo mount -t efs -o tls,mounttargetip=192.0.2.0 fs-abcd123456789ef0 efs/
```

您可以在連接對話方塊中檢視和複製要掛載檔案系統的確切指令。

a. 在 Amazon EFS 主控台中，請選擇您要掛載的檔案系統，顯示其詳細資訊頁面。

b. 若要顯示用於此檔案系統的掛載指令，請選擇右上角的「連接」。

連接熒幕會顯示用於掛載檔案系統的確切指令，如下列方法：

- (通過 DNS 掛載) 使用搭載 EFS 掛載協助程式或 NFS 用戶端的檔案系統 DNS 名稱。
- (通過 IP 掛載) 在 NFS 用戶端已選「可用區」中，使用掛載目標 IP 地址來掛載。

使用 EFS 掛載協助程式在 Amazon EC2 Mac 執行個體上掛載

此程序需要下列項目：

- 您已經在 EC2 執行個體上安裝了 `amazon-efs-utils` 套件。如需詳細資訊，請參閱 執行 macOS Big Sur、macOS Monterey 或 macOS Ventura 時，將 Amazon EFS 安裝在 EC2 Mac 執行個體上。。
- 您已經為檔案系統建立了掛載目標。您可以在建立檔案系統時建立掛載目標，並將其新增至現有檔案系統中。如需詳細資訊，請參閱 管理掛載目標。
- 您正在執行 macOS Big Sur、Monterey 或 Ventura 的 EC2 Mac 執行個體上掛載檔案系統。(不支援其他 macOS 版本)。

> **Note**
>
> 僅支援執行 macOS Big Sur、Monterey 和 Ventura 的 EC2 Mac 執行個體。其他 macOS 版本不支援搭配 Amazon EFS 使用。

在執行 macOS Big Sur、Monterey 或 Ventura 的 EC2 Mac 執行個體上，使用 EFS 掛載協助程式掛載 Amazon EFS 檔案系統

1. 透過 Secure Shell (SSH) 打開 EC2 執行個體的終端機，並使用適當的使用者名稱登入。如需詳細資訊，請參閱 Amazon EC2 使用者指南中的使用適用於 Mac 執行個體的安全殼層 Connect 線到執行個體。
2. 使用下列指令建立要用作檔案系統掛載點的目錄：

```
sudo mkdir efs
```

3. 執行下列命令來掛載檔案系統。

> **Note**
>
> 依預設，無論您是否使用掛載命令中的 `tls` 選項，EFS 掛載協助程式在 EC2 Mac 執行個體上掛載時都會使用傳輸中加密。

```
sudo mount -t efs file-system-id efs-mount-point/
```

```
sudo mount -t efs fs-abcd123456789ef0 efs/
```

您也可以在掛載時使用 `tls` 選項。

```
sudo mount -t efs -o tls fs-abcd123456789ef0:/ efs
```

若要在不使用傳輸中加密的情況下於 EC2 Mac 執行個體上掛載檔案系統，請使用 `notls` 選項，如下列命令所示。

```
sudo mount -t efs -o notls file-system-id efs-mount-point/
```

您可以在管理主控台的連接對話方塊中檢視和複製要掛載檔案系統的確切指令，如下所述。

a. 在 Amazon EFS 主控台中，請選擇您要掛載的檔案系統，顯示其詳細資訊頁面。

b. 若要顯示用於此檔案系統的掛載指令，請選擇右上角的「連接」。

   連接熒幕會顯示用於掛載檔案系統的確切指令，如下列方法：

   - (通過 DNS 掛載) 使用搭載 EFS 掛載協助程式或 NFS 用戶端的檔案系統 DNS 名稱。
   - (通過 IP 掛載) 在 NFS 用戶端已選「可用區」中，使用掛載目標 IP 地址來掛載。

從其他裝載 Amazon EFS 檔案系統 AWS 區域

如果您從與檔案系統不同 AWS 區域 的 Amazon EC2 執行個體掛接 EFS 檔案系統，則需要編輯`efs-utils.conf`檔案中的`region`屬性值。

若要編輯 **efs-utils.conf** 區域中的區域屬性

1. 透過 Secure Shell (SSH) 存取 EC2 執行個體的終端機，並使用適當的使用者名稱登入。有關如何執行此操作的詳細資訊，請參閱 Amazon EC2 使用者指南中的使用安全殼層連接到 Linux 執行個體。
2. 使用您偏好的文字編輯器開啟 `efs-utils.conf` 檔案。
3. 找出下面的一行：

   ```
   #region = us-east-1
   ```

   a. 取消註解該行。

   b. 如果檔案系統不在 `us-east-1` 區域中，請用以檔案系統所在區域的 ID 取代 `us-east-1`。

   c. 儲存變更。
4. 新增跨區域掛載託管項目。如需如何執行此作業的資訊，請參閱 步驟 3：新增掛載目標的主機項目。
5. 使用 EFS 掛載協助程式為 Linux 或 Mac 執行個體掛載檔案系統。

掛載單區域檔案系統

Amazon EFS 單區域檔案系統僅支援與檔案系統位於相同可用區域的單一掛載目標。您無法新增其他掛載目標。本區段描述了掛載單區域檔案系統時應考量的事項。

您可以使用與檔案系統掛載目標位於相同可用區域的 Amazon EC2 運算執行個體存取 EFS 檔案系統，以避免在可用區域間收取資料傳輸費用，並獲得更好的效能。

本節包含下列程序：

- 您已經在 EC2 執行個體上安裝了 `amazon-efs-utils package`。如需詳細資訊，請參閱 手動安裝 Amazon EFS 用戶端。
- 您已經為檔案系統建立了掛載目標。如需詳細資訊，請參閱 管理掛載目標。

在其他可用區域的 EC2 上掛載單區域檔案系統

如果您正在位於不同可用區域的 EC2 執行個體上掛載單區域檔案系統，則必須在掛載協助程式掛載命令中指定檔案系統可用區域名稱或檔案系統掛載目標的 DNS 名稱。

使用下列指令建立要用作檔案系統掛載點的目錄 `efs`：

```
sudo mkdir efs
```

使用下列命令來通過 EFS 掛載協助程式掛載檔案系統。此命令指定檔案系統的可用區域名稱。

```
sudo mount -t efs -o az=availability-zone-name,tls file-system-id mount-point/
```

這是具有下列示例值的命令：

```
sudo mount -t efs -o az=us-east-1a,tls fs-abcd1234567890ef efs/
```

下列指令會掛載檔案系統，並指定檔案系統掛載目標的 DNS 名稱。

```
sudo mount -t efs -o tls mount-target-dns-name mount-point/
```

這是具有掛載目標 DNS 名稱範例的命令。

```
sudo mount -t efs -o tls us-east-1a.fs-abcd1234567890ef9.efs.us-east-1.amazonaws.com
 efs/
```

使用 EFS 掛載協助程式，在不同的可用區域中自動掛載單區檔案系統

如果您正在位於不同可用區域的 EC2 執行個體上使用 /etc/fstab 來掛載 EFS單區域檔案系統，則必須在 /etc/fstab 項目中指定檔案系統可用區域名稱或檔案系統掛載目標的 DNS 名稱。

```
availability-zone-name.file-system-id.efs.aws-region.amazonaws.com:/ efs-mount-point
 efs defaults,_netdev,noresvport,tls 0 0
```

```
us-east-1a.fs-abc123def456a7890.efs.us-east-1.amazonaws.com:/ efs-one-zone efs
 defaults,_netdev,noresvport,tls 0 0
```

使用 NFS 自動掛載單區域檔案系統

如果您使用/etc/fstab在位於不同可用區域的 EC2 執行個體上使用單一區域儲存裝載 EFS 檔案系統，則必須在項目中指定檔案系統的可用區域名稱，並在/etc/fstab項目中指定檔案系統的可用區域名稱。

```
availability-zone-name.file-system-id.efs.aws-region.amazonaws.com:/ efs-mount-point
 nfs4
```

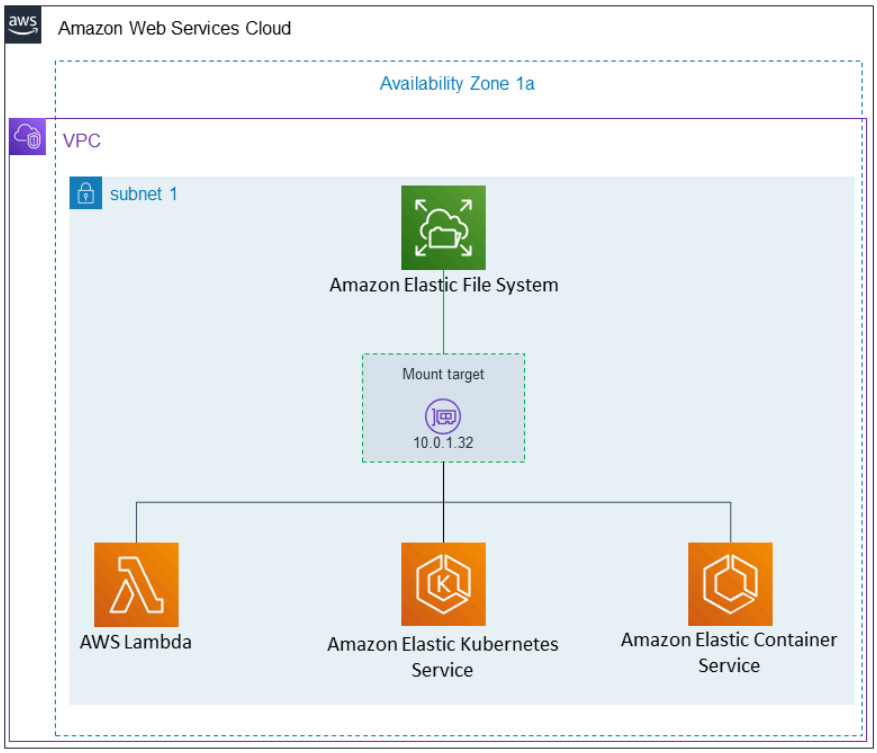
```
 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport,_netdev 0
 0
```

```
us-east-1a.fs-abc123def456a7890.efs.us-east-1.amazonaws.com:/ efs-one-zone nfs4
 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport,_netdev 0
 0
```

如需關於如何編輯 `/etc/fstab` 檔案和用於此命令的值詳細資訊，請參閱 使用 NFS 自動掛載 EFS 檔案系統。

在其他 AWS 運算執行個體上掛載具有單區檔案系統的檔案系統

當您將單區檔案系統與 Amazon 彈性容器服務、Amazon Elastic Kubernetes Service 搭配使用時 AWS Lambda，或者您需要將該服務設定為使用 EFS 檔案系統所在的相同可用區域，如下所示，並在以下各節中說明。



從 Amazon Elastic Container Service 処連接

您可以搭配 Amazon ECS 使用 Amazon EFS 檔案系統，在容器執行個體的機群中共用檔案系統資料，如此您的任務無論出現在哪個執行個體上都可以存取到相同的永續性儲存中。若要搭配 Amazon ECS 使用 Amazon EFS 單區域檔案系統，您應該在啟動任務時，只選擇與檔案系統位於相同可用區域中

的子網路。如需詳細資訊，請參閱《Amazon Elastic Container Service 開發人員指南》中的 Amazon EFS 磁碟區。

從 Amazon Elastic Kubernetes Service 処連接

從 Amazon EKS 掛載單區域檔案系統時，您可以使用支援 Amazon EFS 存取點的 Amazon EFS 容器儲存介面 (CSI) 驅動程式，在 Amazon EKS 或自我管理的 Kubernetes 叢集中的多個 Pod 之間公用檔案系統。Amazon EFS CSI 驅動程式安裝在 Fargate 堆疊中。將 Amazon EFS CSI 驅動程式與 Amazon EFS 單區域檔案系統搭配使用時，您可以在啟動 Pod 時使用 `nodeSelector` 選項，以確保在與檔案系統相同的可用區域內排程。

連線來源 AWS Lambda

您可以 AWS Lambda 將 Amazon EFS to 用於跨函數叫用共用資料、讀取大型參考資料檔案，以及將函數輸出寫入永久和共用存放區。Lambda 將函數執行個體安全地連接到位於相同可用區域和子網路的 Amazon EFS 掛載目標上。當您將 Lambda 與單區域檔案系統搭配使用時，請將函數設定為僅啟動調用至與檔案系統位於相同可用區域的子網路中。

使用 IAM 授權掛載

若要使用 AWS Identity and Access Management (IAM) 授權在 Linux 執行個體上掛接 Amazon EFS 檔案系統，請使用 EFS 掛載協助程式。如需 NFS 用戶端 IAM 授權的詳細資訊，請參閱使用 IAM 控制檔案系統資料存取。

在下列區段中，您將需要建立目錄，將其作爲檔案系統掛載點使用：您可以使用以下命令建立掛載點目錄 `efs`：

```
sudo mkdir efs
```

然後，您可以使用 `efs` 取代 *`efs-mount-point`* 的執行個體。

使用 EC2 執行個體設定檔與 IAM 進行掛載

如果您藉助 IAM 授權掛載到具有執行個體設定檔的 Amazon EC2 執行個體上，請使用 `tls` 和 `iam` 掛載選項，如下所示。

```
$ sudo mount -t efs -o tls,iam file-system-id efs-mount-point/
```

要使用 IAM 授權自動掛載到具有執行個體設定檔的 Amazon EC2 執行個體，請將以下的列新增到 EC2 執行個體上的 `/etc/fstab` 檔案中。

```
file-system-id:/ efs-mount-point efs _netdev,tls,iam 0 0
```

使用命名描述檔與 IAM 進行掛載

您可以使用登入資料檔案中的 IAM 登入資料或 AWS CLI 設定檔~/.aws/credentials，透過 AWS CLI IAM 授權進行掛載~/.aws/config。如果未指定 "awsprofile"，則會使用「預設」設定檔。

若要使用憑證檔案來掛載 IAM 授權至 Linux 執行個體，請使用 tls、awsprofile 和 iam 掛載選項，如下所示。

```
$ sudo mount -t efs -o tls,iam,awsprofile=namedprofile file-system-id efs-mount-point/
```

若要使用憑證檔案以 IAM 授權自動掛載至 Linux 執行個體，請將以下行新增至 EC2 執行個體上的 /etc/fstab 檔案。

```
file-system-id:/ efs-mount-point efs _netdev,tls,iam,awsprofile=namedprofile 0 0
```

使用 EFS 存取點進行掛載

您可以使用 EFS 掛載協助程式來掛載使用存取點的 EFS 檔案系統。

> **Note**
>
> 使用 EFS 存取點掛載檔案系統時，您必須為檔案系統設定一或多個掛載目標。

在使用存取點掛載檔案系統時，除了一般掛載選項以外，掛載命令還需要包含 access-point-id 和 tls 掛載選項。範例顯示如下。

```
$ sudo mount -t efs -o tls,accesspoint=access-point-id file-system-id efs-mount-point
```

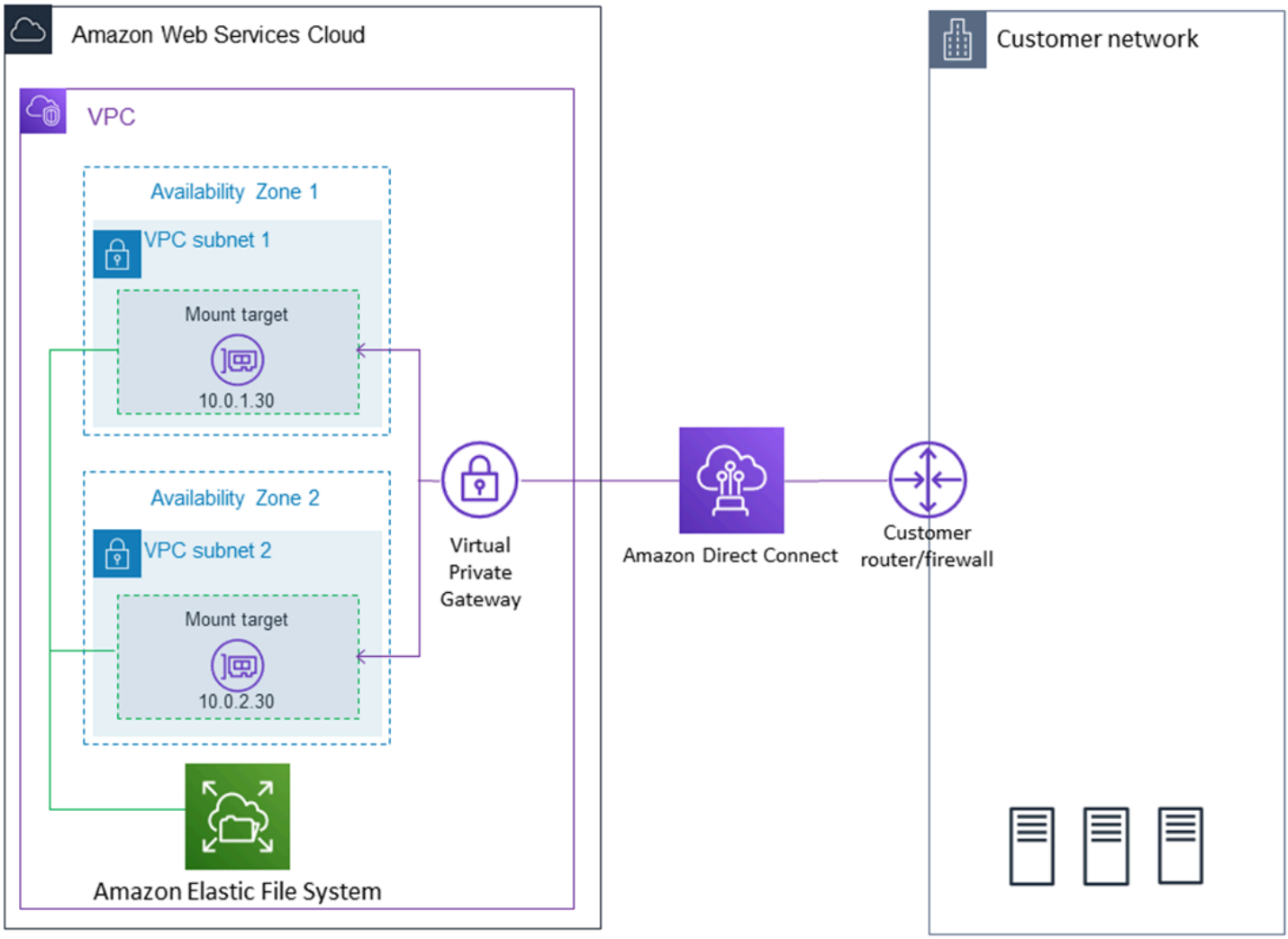
若要使用存取點自動掛載檔案系統，請將下列行新增到 EC2 執行個體上的 /etc/fstab 檔案中。

```
file-system-id efs-mount-point efs _netdev,tls,accesspoint=access-point-id 0 0
```

如需 EFS 存取點的詳細資訊，請參閱使用 Amazon EFS 存取點。

使用 EFS 掛載協助程式 AWS Direct Connect 和 VPN，透過內部部署 Linux 用戶端進行裝載

使用 AWS Direct Connect 或 VPN 連接到 Amazon VPC 時，您可以將 Amazon EFS 檔案系統掛接到現場部署資料中心伺服器上。下圖顯示從現場部署裝載 Amazon EFS 檔案系統時 AWS 服務 所需的高階示意圖。



如需如何使用`amazon-efs-utils` AWS Direct Connect 和 VPN 將 Amazon EFS 檔案系統掛接到現場部署 Linux 用戶端的詳細資訊，請參閱逐步解說：使用 AWS Direct Connect 和 VPN 建立和掛載內部部署的檔案系統。

自動掛載 Amazon EFS 檔案系統

當 EFS 檔案系統使用 EFS 掛載協助程式或 NFS 重新啟動時，您可以將 Amazon EC2 執行個體設定為自動掛載 EFS 檔案系統。

- 使用 EFS 掛載協助程式：
  - 使用 EC2 啟動執行個體精靈建立新 EC2 執行個體時，附加 EFS 檔案系統。
  - 使用 EFS 檔案系統的項目來更新 EC2 `/etc/fstab` 檔案。
- 使用無 EFS 掛載協助程式的 NFS 來更新 EC2 `/etc/fstab` 檔案，以支援 EC2 Linux 和 Mac 執行個體。

> **Note**
>
> Amazon EC2 Mac 執行個體在執行 macOS Big Sur 或 Monterey 時，EFS 掛載協助程式不支援自動掛載在此執行個體上。反之，您可以使用 NFS 在 EC2 Mac 執行個體上設定 /etc/fstab 檔案，以自動掛載 EFS 檔案系統。

主題

使用 EFS 掛載協助程式自動重新掛載 EFS 檔案系統

使用 EFS 掛載協助程式設定 EC2 Linux 執行個體上的 `/etc/fstab`，以便在執行個體重新啟動時自動重新掛載 EFS 檔案系統。

主題

在建立 EC2 執行個體時附加 EFS 檔案系統，以便在重新開機時自動掛載

此方法使用 EFS 掛載協助程式來掛載檔案系統，並更新 EC2 執行個體上的 /etc/fstab 檔案。掛載協助程式是 `amazon-efs-utils` 工具組的一部分。

使用 EC2 啟動執行個體精靈建立新的 Amazon EC2 Linux 執行個體時，您可以將其設為自動掛載 Amazon EFS 檔案系統。如此一來，在執行個體初次啟動和重新啟動時，EC2 執行個體就會自動掛載檔案系統。

> **Note**
>
> Amazon EC2 Mac 執行個體在執行個體啟動時執行 macOS Big Sur 或 Monterey，那麼 Amazon EFS 檔案系統不支援掛載在此執行個體上。

在執行此程序之前，請確認您已經建立 Amazon EFS 檔案系統。如需詳細資訊，請參閱「開始使用 Amazon EFS」練習中的 快速建立具有建議設定的檔案系統 (主控台)。

> **Note**
>
> 您無法搭配使用 Amazon EFS 與以 Microsoft Windows 為基礎的 Amazon EC2 執行個體。

若您尚未擁有金鑰對，則必須建立一組金鑰對，才能啟動並連線至 Amazon EC2 執行個體。依照 Amazon EC2 使用者指南中的設定使用 Amazon EC2 中的步驟建立 key pair。如果您已有金鑰對，您可以將其用於本練習。

設定 EC2 執行個體在啟動時自動掛載 EFS 檔案系統

1. 前往 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 選擇 Launch Instance (啟動執行個體)。
3. 在 Step 1: Choose an Amazon Machine Image (AMI) (步驟 1：選擇 Amazon Machine Image (AMI)) 的清單最上方尋找 Amazon Linux AMI，然後選擇 Select (選取)。
4. 在步驟 2：選擇執行個體類型中，選擇下一步：設定執行個體詳細資訊。
5. 在步驟 3：設定執行個體詳細資訊 中，提供下列資訊：
   - 針對網路選擇與您掛載的 EFS 檔案系統相同的 VPC 項目。
   - 針對 Subnet (子網路) 選擇任何可用區域中的預設子網路。
   - 針對檔案系統選擇您要掛載的 EFS 檔案系統。檔案系統 ID 旁顯示的路徑是 EC2 執行個體將使用的掛載點，您可以加以變更。
   - 在進階詳細資料中，使用者資料會自動產生，而其中會包含將您所指定 EFS 檔案系統掛載至檔案系統時的必要命令。
6. 選擇 Next: Add Storage (下一步：新增儲存體)。
7. 選擇 Next: Add Tags (下一步：新增標籤)。
8. 為執行個體命名，並選擇下一步：設定安全群組。

9. 在步驟 6：設定安全群組中，將指派安全群組)設定為選取現有安全群組。選擇預設安全群組，以確保它可以存取您的 EFS 檔案系統。

   您無法使用此安全群組透過 Secure Shell (SSH) 存取您的 EC2 執行個體。若要透過 SSH 存取，您可以編輯預設安全性並新增規則，以允許 SSH 或允許 SSH 的新安全群組。您可以使用以下設定：

   - Type (類型)：SSH
   - Protocol (通訊協定)：TCP
   - Port Range (連接埠範圍)：22
   - Source (來源)：Anywhere (任何位置) 0.0.0.0/0
10. 選擇 Review and Launch (檢閱和啟動)。
11. 選擇啟動。
12. 選取您建立的金鑰對核取方塊，然後選擇 Launch Instances (啟動執行個體)。

您的 EC2 執行個體現在已設定為在啟動時和重新啟動時掛載 EFS 檔案系統。

使用搭配 EFS 掛載協助程式的 **/etc/fstab** 自動掛載 EFS 檔案系統

/etc/fstab 檔案包含檔案系統的資訊，而在執行個體啟動期間執行的 mount -a 命令則會掛載所有列在 /etc/fstab 檔案中的檔案系統。在此程序中，您將手動更新 EC2 Linux 執行個體上的 /etc/fstab，以便執行個體使用 EFS 掛載協助程式在執行個體重新啟動時自動重新掛載 EFS 檔案系統。

> **Note**
>
> Amazon EC2 Mac 執行個體在執行 macOS Big Sur 或 Monterey 時，Amazon EFS 檔案系統不支援使用搭配 EFS 掛載協助程式的 /etc/fstab 自動掛載在此執行個體上。反之，EC2 Mac 執行個體在執行 macOS Big Sur 或 Monterey 時，您可以使用帶有 /etc/fstab 的 NFS 來將檔案系統自動掛載在此執行個體上。

這種方法都會使用 EFS 掛載協助程式來掛載檔案系統。掛載協助程式是 amazon-efs-utils 工具組的一部分。

amazon-efs-utils 工具可以安裝在 Amazon Linux 和 Amazon Linux 2 Amazon Machine Image (AMI) 上。如需 amazon-efs-utils 的相關資訊，請參閱 安裝 Amazon EFS 工具。如果您使用的是 Red Hat Enterprise Linux (RHEL) 等其他 Linux 發行版本，則需手動建置並安裝 amazon-efs-utils。如需詳細資訊，請參閱 在其他 Linux 發行版上安裝 Amazon EFS 用戶端。

必要條件

您必須先設定下列需求，才能順利實作此程序：

- 您已經建立要自動重新掛載的 Amazon EFS 檔案系統。如需詳細資訊，請參閱 快速建立具有建議設定的檔案系統 (主控台)。
- 您已經建立要設定為自動重新掛載 EFS 檔案系統的 EC2 Linux 執行個體。
- EFS 掛載協助程式已安裝在 EC2 Linux 執行個體上。如需詳細資訊，請參閱 安裝 Amazon EFS 工具。

更新 EC2 執行個體上的 /etc/fstab 檔案

1. 連線到您的 EC2 執行個體：

   - 若要從執行 macOS 或 Linux 的電腦連接至您的執行個體，請指定 SSH 命令的 .pem 檔案。為此，您必須使用 `-i` 選項和私密金鑰路徑。
   - 若要從執行 Windows 的電腦連線至執行個體，您可以使用 MindTerm 或 PuTTY。您需要安裝 PuTTY 並將 .pem 檔案轉換為 .ppk 檔案，才可以使用該程式。

   如需詳細資訊，請參閱 Amazon EC2 使用者指南中的下列主題：

   - 使用 PuTTY 從視窗 Connect 到您的 Linux 執行個體
   - 使用安全殼層從 Linux 或 macOS Connect 至您的 Linux 執行個體
2. 在編輯器中開啟 `/etc/fstab` 檔案。
3. 使用 IAM 授權或 EFS 存取點自動掛載：

   - 要使用 IAM 授權自動掛載到具有執行個體設定檔的 Amazon EC2 執行個體，請將以下的列新增到 `/etc/fstab` 檔案中。

     ```
     file-system-id:/ efs-mount-point efs _netdev,noresvport,tls,iam 0 0
     ```
   - 若要使用憑證檔案以 IAM 授權自動掛載到 Linux 執行個體，請將下行新增至 `/etc/fstab` 檔案。

     ```
     file-system-id:/ efs-mount-point efs
      _netdev,noresvport,tls,iam,awsprofile=namedprofile 0 0
     ```
   - 若要使用 EFS 存取點自動掛載檔案系統，請將下行新增至 `/etc/fstab` 檔案。

```
file-system-id:/ efs-mount-point efs
 _netdev,noresvport,tls,iam,accesspoint=access-point-id 0 0
```

> **Warning**
>
> 使用 _netdev 選項，此選項用於在自動掛載檔案系統時識別網路檔案系統。若 _netdev 已遺失，EC2 執行個體可能會停止回應。此結果是因為網路檔案系統在運算執行個體開始聯網後需要初始化。如需詳細資訊，請參閱 自動掛載失敗且執行個體沒有回應。

如需詳細資訊，請參閱 使用 IAM 授權掛載 及 使用 EFS 存取點進行掛載。

4. 儲存對檔案所做的變更。
5. 將 'fake' 選項以及 'all' 和 'verbose' 選項與 mount 命令搭配使用，以測試 fstab 項目。

```
$ sudo mount -fav
home/ec2-user/efs      : successfully mounted
```

您的 EC2 執行個體已完成設定，可在重新啟動時掛載 EFS 檔案系統。

> **Note**
>
> 在某些情況下，不論掛載的 Amazon EFS 檔案系統處於何種狀態，Amazon EC2 執行個體都需要啟動。遇到這種情況時，請將 nofail 選項新增至 /etc/fstab 檔案中的檔案系統項目。

您新增至 /etc/fstab 檔案的程式碼行會執行下列動作。

欄位	描述
file-system-id :/	您 Amazon EFS 檔案系統的 ID。您可以從控制台或以編程方式從 CLI 或 AWS SDK 獲取此 ID。
efs-mount-point	EFS 檔案系統在 EC2 執行個體上的掛載點。

欄位	描述
`efs`	檔案系統類型。您使用掛載協助程式時，此類型一律為 `efs`。
`mount options`	檔案系統的掛載選項。這是以逗號分隔的下列選項清單： • `_netdev`：此選項告知作業系統檔案系統位於需要網路存取的裝置上。此選項可防止執行個體掛載到檔案系統，直到用戶端啟用網路。 • `noresvport` ：告知 NFS 用戶端在網路連線重新建立時，使用新的傳輸控制通訊協定 (TCP) 來源連接埠。這可讓您確保在網路復原事件後，EFS 檔案系統具有不中斷的可用性。 • `tls`：啟用傳輸中的資料加密。 • `iam`：使用此選項以掛載 IAM 授權至具有執行個體設定檔的 Amazon EC2 上。使用 `iam` 掛載選項也需要使用 `tls` 選項。如需詳細資訊，請參閱 使用 IAM 控制檔案系統資料存取。 • `awsprofile=` *`namedprofile`* ：將此選項與 `iam` 和 `tls` 選項搭配使用，以使用憑證檔案對 Linux 執行個體進行 IAM 授權的掛載。如需 EFS 存取點的詳細資訊，請參閱使用 IAM 控制檔案系統資料存取。 • `accesspoint=` *`access-point-id`* ：將 `tls` 選項與 EFS 選項搭配使用，以使用 EFS 存取點進行掛載。如需 EFS 存取點的詳細資訊，請參閱使用 Amazon EFS 存取點。
`0`	非零值表示檔案系統應該由 dump 進行備份。對於 EFS，這個值應為 `0`。
`0`	`fsck` 在開機時檢查檔案系統的順序。對於 EFS 檔案系統，這個值應為 `0`，以表示 `fsck` 不應在啟動時執行。

使用 NFS 自動掛載 EFS 檔案系統

更新 EC2 執行個體上的 **`/etc/fstab`** 檔案

1. 連線到您的 EC2 執行個體：
   - 若要從執行 macOS 或 Linux 的電腦連接至您的執行個體，請指定 SSH 命令的 .pem 檔案。為此，您必須使用 `-i` 選項和私密金鑰路徑。

- 若要從執行 Windows 的電腦連線至執行個體，您可以使用 MindTerm 或 PuTTY。您需要安裝 PuTTY 並將 .pem 檔案轉換為 .ppk 檔案，才可以使用該程式。

  如需詳細資訊，請參閱 Amazon EC2 使用者指南中的下列主題：

  - 使用 PuTTY 從視窗 Connect 到您的 Linux 執行個體
  - 使用安全殼層從 Linux 或 macOS Connect 至您的 Linux 執行個體

2. 在編輯器中開啟 /etc/fstab 檔案。
3. 若要使用代替 EFS 掛載協助程式的 EFS 存取點自動掛載檔案系統，請將下行新增至 /etc/fstab 檔案。

   - 以您正在掛載的檔案系統 ID 取代 *file_system_id*。
   - 用文件系統中 AWS 區域 的替換 *aws-region*，例如。us-east-1
   - 以檔案系統的掛載點取代 *mount_point*。

   ```
   file_system_id.efs.aws-region.amazonaws.com:/ mount_point nfs4
    nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport,_netdev
    0 0
   ```

您新增至 /etc/fstab 檔案的程式碼行會執行下列動作。

欄位	描述
file-system-id :/	您 Amazon EFS 檔案系統的 ID。您可以從控制台或以編程方式從 CLI 或 AWS SDK 獲取此 ID。
efs-mount-point	EFS 檔案系統在 EC2 執行個體上的掛載點。
nfs4	指定檔案系統類型。
mount options	以逗號分隔的檔案系統掛載選項清單： • nfsvers=4.1 ：指定使用 NFS v4.1。 • rsize=1048576 ：為改善效能，從 EFS 檔案系統上的檔案中讀取資料時，請設定 NFS 用戶端為每個網路 READ 請求接收的最大資料位元組數，1048576 可能是最大數。

欄位	描述
	• wsize=1048576 ：為改善效能，從 EFS 檔案系統上的檔案中讀取資料時，請設定 NFS 用戶端為每個網路 WRITE 請求發送的最大資料位元組數，1048576 可能是最大數。 • hard：設定 NFS 用戶端在 NFS 請求逾時的復原行為，因此 NFS 請求會重試直到伺服器回覆為止。我們建議您使用硬掛載選項 (hard)，以確保資料的完整性。如果您使用 soft 掛載，請將 timeo 參數設定為至少 150 十分之一秒 (15 秒)。這有助於降低軟掛載固有的資料損壞風險。 • timeo=600 ：將 NFS 用戶端等待重試 NFS 請求回應的逾時值設為 600 十分之一秒 (60 秒)。如果您必須變更逾時參數 (timeo)，我們建議您使用至少為 150 的值，相當於 15 秒。這有助於避免效能降低。 • retrans=2 ：將 NFS 用戶端在請求嘗試進一步復原動作前的重試次數設為 2。 • noresvport ：告知 NFS 用戶端在網路連線重新建立時，使用新的傳輸控制通訊協定 (TCP) 來源連接埠。這可讓您確保在網路復原事件後，EFS 檔案系統具有不中斷的可用性。 • _netdev：防止用戶端嘗試掛載到檔案系統，直到網路完成啟用。
0	指定 dump 值；0 告知 dump 公用程式不必備份檔案系統。
0	告知 fsck 公用程式不要在啟動時執行。

使用將 EFS 掛接到多個 EC2 執行個體 AWS Systems Manager

您可以遠端安全地將 EFS 檔案系統掛載到多個 Amazon EC2 執行個體，而不必使用 AWS Systems Manager Run命令登入執行個體。若要取得有關 AWS Systems Manager 執行命令的更多資訊，請參閱《AWS Systems Manager 使用指南》中的 AWS Systems Manager run 命令。使用此方法掛載 EFS 檔案系統之前，必須具備下列先決條件：

1. EC2 執行個體會使用包含 AmazonElasticFileSystemsUtils 許可政策的執行個體設定檔進行啟動。如需詳細資訊，請參閱 步驟 1：使用所需許可設定 IAM 執行個體設定檔。。
2. Amazon EFS 用戶端 (amazon-efs-utils 套件) 的 1.28.1 版或更新版本已安裝在 EC2 執行個體上。您可以使用 AWS Systems Manager 在執行個體上自動安裝套件。如需詳細資訊，請參閱 步驟 2：設定 State Manager Association，用於安裝或更新 Amazon EFS 用戶端。

使用主控台將多個 EFS 檔案系統掛載到多個 EC2 執行個體上

1. 開啟主 AWS Systems Manager 控台，網址為 https://console.aws.amazon.com/systems-manager/。
2. 在導覽窗格中，選擇 執行命令。
3. 選擇 Run a command (執行指令)。
4. 在命令搜尋欄位中輸入 **AWS-RunShellScript**。
5. 選取 AWS-RunShell 指令碼。
6. 在命令參數中，為您想掛載的每個 EFS 檔案系統輸入要使用的掛載命令。例如：

   ```
   sudo mount -t efs -o tls fs-12345678:/ /mnt/efs
   sudo mount -t efs -o tls,accesspoint=fsap-12345678 fs-01233210 /mnt/efs
   ```

   如需關於使用 Amazon EFS 用戶端掛載 EFS 掛載命令的詳細資訊，請參閱 使用 EFS 掛載協助程式在 Amazon EC2 Linux 執行個體上掛載 或 使用 EFS 掛載協助程式在 Amazon EC2 Mac 執行個體上掛載。
7. 選取要在其上執行命令的目標 AWS Systems Manager 受管 EC2 執行個體。
8. 進行任何您想要的其他設定。然後選擇執行以執行命令，並掛載命令中指定的 EFS 檔案系統。

   執行命令之後，您可以在命令歷程中查看其狀態。

從另一個 AWS 帳戶 或 VPC 掛載 EFS 檔案系統

您可以使用 EFS 掛載協助程式透過 NFS 用戶端的 IAM 授權和 EFS 存取點來掛載 Amazon EFS 檔案系統。根據預設，EFS 掛載協助程式會使用網域名稱服務 (DNS) 來解析 EFS 掛載目標的 IP 地址。如果您要從不同帳戶或虛擬私有雲端 (VPC) 掛載檔案系統，則需手動解析 EFS 掛載目標。

您可在下文中找到判斷正確 EFS 掛載目標 IP 地址以供 NFS 用戶端使用的說明。您也可以找到使用該 IP 地址設定用戶端以掛載 EFS 檔案系統的說明。

從其他 VPC 中使用 IAM 或存取點掛載

使用 VPC 對等互連或傳輸閘道來連接 VPC 時，即使 VPC 屬於不同帳戶，Amazon EC2 執行個體仍可在另一個 VPC 存取 EFS 檔案系統。

必要條件

使用下列程序之前，請先執行以下步驟：

- 要在掛載 EFS 檔案系統的運算執行個體上安裝 Amazon EFS 用戶端，這是公用程式 amazon-efs-utils 集的一部分。您可以使用包含在中 amazon-efs-utils 的 EFS 掛載協助程式來掛載檔案系統。如需安裝 amazon-efs-utils 的指示，請參閱安裝 Amazon EFS 工具。
- 針對您附加到執行個體的 IAM 角色，允許 IAM 政策中的 ec2:DescribeAvailabilityZones 動作。我們建議您將受 AWS 管政策附加AmazonElasticFileSystemsUtils到 IAM 實體，以提供實體必要的許可。
- 從另一個裝載時 AWS 帳戶，請更新檔案系統資源策略，以允許其他 AWS 帳戶人的主參與者 ARN elasticfilesystem:DescribeMountTarget 執行動作。例如：

```
{
    "Id": "access-point-example03",
    "Statement": [
        {
            "Sid": "access-point-statement-example03",
            "Effect": "Allow",
            "Principal": {"AWS": "arn:aws:iam::555555555555"},
            "Action": "elasticfilesystem:DescribeMountTargets",
            "Resource": "arn:aws:elasticfilesystem:us-east-2:111122223333:file-
system/fs-12345678"
        }
    ]
}
```

  如需關於 EFS 檔案系統資源政策的詳細資訊，請參閱 Amazon EFS 中的資源型政策。
- 安裝 botocore。當將檔案系統掛載到另一個 VPC 上而檔案系統 DNS 名稱無法解析時，EFS 用戶端會使用 botocore 來擷取掛載目標 IP 地址。如需詳細資訊，請參閱 amazon-efs-utils README 檔案中安裝 botocore。
- 設定 VPC 對等互連或 VPC 傳輸閘道。

  您必須使用 VPC 對等連接或 VPC 傳輸閘道來連接用戶端的 VPC 和 EFS 檔案系統的 VPC。使用 VPC 對等互連或傳輸閘道來連接 VPC 時，即使 VPC 屬於不同帳戶，Amazon EC2 執行個體仍可在另一個 VPC 存取 EFS 檔案系統。

  傳輸閘道是網路傳輸中樞，您可以用於互相連接 VPC 和現場部署網路。如需使用 VPC 傳輸閘道的詳細資訊，請參閱《Amazon VPC 傳輸閘道指南》中的開始使用傳輸閘道。

  VPC 對等連接是在兩個 VPC 之間的網路連線。這種連線類型可讓您使用私有網際網路通訊協定第 4 版 (IPv4) 或網際網路通訊協定第 6 版 (IPv6) 地址，在兩者間路由流量。您可以使用 VPC 對

等連線來連接相同 AWS 區域 或兩者之間的 VPC。 AWS 區域如需 VPC 互連的詳細資訊，請參閱《Amazon VPC 互連指南》中的什麼是 VPC 互連？。

為確保檔案系統具備高可用性，建議您一律使用與 NFS 用戶端所在同一可用區域的 EFS 掛載目標 IP 地址。如果要掛載另一個帳戶中的 EFS 檔案系統，請確保 NFS 用戶端和 EFS 掛載目標位於相同的可用區域 ID。此要求適用的原因是，AZ 名稱在各個帳戶間可能會有不同。

使用 IAM 或存取點掛載另一個 VPC 中的 EFS 檔案系統

1. 連線到您的 EC2 執行個體：

   - 若要從執行 macOS 或 Linux 的電腦連接至您的執行個體，請指定 SSH 命令的 .pem 檔案。為此，您必須使用 `-i` 選項和私密金鑰路徑。
   - 若要從執行 Windows 的電腦連線至執行個體，您可以使用 MindTerm 或 PuTTY。您需要安裝 PuTTY 並將 .pem 檔案轉換為 .ppk 檔案，才可以使用該程式。

   如需詳細資訊，請參閱 Amazon EC2 使用者指南中的下列主題：

   - 使用 PuTTY 從視窗 Connect 到您的 Linux 執行個體
   - 使用安全殼層從 Linux 或 macOS Connect 至您的 Linux 執行個體

2. 您可以使用下列命令來建立掛載檔案系統的目錄。

   ```
   $ sudo mkdir /mnt/efs
   ```

3. 若要透過 IAM 授權掛載檔案系統，請使用下列命令：

   ```
   $ sudo mount -t efs -o tls,iam file-system-dns-name /mnt/efs/
   ```

   如需搭配使用 IAM 授權與 EFS 的詳細資訊，請參閱使用 IAM 控制檔案系統資料存取。

   若要透過 EFS 存取點掛載檔案系統，請使用下列命令：

   ```
   $ sudo mount -t efs -o tls,accesspoint=access-point-id file-system-dns-name /mnt/
   efs/
   ```

   如需 EFS 存取點的詳細資訊，請參閱使用 Amazon EFS 存取點。

從不同 AWS 區域區域掛載 Amazon EFS 檔案系統。

如果您要從與檔案系統不同 AWS 區域 的其他 VPC 掛接 EFS 檔案系統，則需要編輯該`efs-utils.conf`檔案。在 `/dist/efs-utils.conf` 中找出下列各行：

```
#region = us-east-1
```

取消註解行，並取代檔案系統所在區域的 ID 值 (如果檔案系統不在 `us-east-1` 中)。

從相同 VPC AWS 帳戶 中的另一個安裝

您可以使用共用 VPC 掛接由其他 AWS 帳戶執行個體擁有的 Amazon EC2 執 AWS 帳戶 行個體擁有的 Amazon EFS 檔案系統。如需設定共用 VPC 的詳細資訊，請參閱《Amazon VPC 互連指南》中的使用共用 VPC。

在您設定 VPC 共用之後，EC2 執行個體就可以使用網域名稱系統 (DNS) 名稱解析或 EFS 掛載協助程式，掛載 EFS 檔案系統。我們建議您使用 EFS 掛載協助程式掛載 EFS 檔案系統。

使用網路檔案系統掛載 EFS 檔案系統

> **Note**
>
> 在本節中，您可以了解如何在沒有 amazon-efs-utils 套件的情況下掛接 Amazon EFS 檔案系統。若要在您的檔案系統使用傳輸中的資料加密，您必須使用 Transport Layer Security (TLS) 掛載您的檔案系統。為此，我們建議您使用該 amazon-efs-utils 軟件包。如需詳細資訊，請參閱 安裝 Amazon EFS 工具。

接下來，您可以了解如何安裝網路檔案系統 (NFS) 用戶端，以及如何在 Amazon EC2 執行個體上掛載您的 Amazon EFS 檔案系統。您也可以找到 `mount` 命令的解釋，以及在 `mount` 命令中指定您檔案系統的網域名稱系統 (DNS) 時可使用的選項。此外，您可以找到如何使用 `fstab` 檔案，讓檔案系統在任何系統重新啟動後自動重新掛載。

> **Note**
>
> 您必須建立、設定及啟動您的相關 AWS 資源，然後才可以掛載檔案系統。如需詳細說明，請參閱 開始使用 Amazon Elastic File System。

> **Note**
>
> 掛載檔案系統之前，您需要為 Amazon EC2 執行個體創建 VPC 安全群組，並使用所需的傳入和傳出存取挂載目標。如需詳細資訊，請參閱 針對 Amazon EC2 執行個體和掛載目標使用 VPC 安全群組。

主題

NFS 支援

當您在 Amazon EC2 執行個體上掛載檔案系統時，Amazon EFS 支援網路檔案系統版本 4.0 與 4.1 (NFSv4) 通訊協定。雖有支援 NFSv4.0，但建議您使用 NFSv4.1。在 Amazon EC2 執行個體上掛載您的 Amazon EFS 檔案系統還需要 NFS 用戶端，此用戶端必須支援您所選擇的 NFSv4 協定。執行 macOS Big Sur 的 Amazon EC2 MacOS 執行個體僅支援 NFS v4.0。

Amazon EFS 不支援 `nconnect` 掛載選項。

> **Note**
>
> 對於 Linux 核心版本 5.4.*，Linux NFS 用戶端會使用 128 KB 的預設 `read_ahead_kb` 值。我們建議將此值增加到 15 MB。如需詳細資訊，請參閱 優化 NFS read_ahead_kb 大小。

為達到最佳化效能並避免各種已知的 NFS 用戶端錯誤，建議您使用最新的 Linux 核心。如果您使用的是企業 Linux 發行版本，我們建議下列事項：

- Amazon Linux 2
- Amazon Linux 2017.09 或更新版本
- Red Hat Enterprise Linux (和例如 CentOS 之類的導數) 版本 7 和更新版本
- Ubuntu 16.04 LTS 和更新版本

- SLES 12 Sp2 或更新版本

如果您使用的是另一個發行版本或自訂核心，建議使用核心版本 4.3 或更新版本。

> **Note**
>
> 由於同步開啟太多檔案而造成效能不佳，就特定的工作負載而言，RHEL 6.9 可能是次佳選擇。

> **Note**
>
> 不支援執行 Microsoft Windows 時使用 Amazon EC2 執行個體掛載 Amazon EFS 檔案系統。

疑難排解 AMI 與核心版本

若要排解使用 EC2 執行個體的 Amazon EFS 時與特定 AMI 或核心版本相關的疑難問題，請參閱 AMI 與核心問題疑難排解。

安裝 NFS 用戶端

若要在 Amazon EC2 執行個體掛載您的 Amazon EFS 檔案系統，必須先安裝 NFS 用戶端。若要連接到您的 EC2 執行個體並安裝 NFS 用戶端，您需要 EC2 執行個體的公有 DNS 名稱以及用於登入的使用者名稱。您執行個體的使用者名稱通常是 `ec2-user`。

連接 EC2 執行個體並安裝 NFS 用戶端

1. 連線至 EC2 執行個體。請注意以下有關連接執行個體的事項：

   - 若要從執行 macOS 或 Linux 的電腦連接至您的執行個體，請使用 `-i` 選項與私密金鑰的路徑，將 .pem 檔案指定給 Secure Shell (SSH) 用戶端。
   - 若要從執行 Windows 的電腦連線至執行個體，您可以使用 MindTerm 或 PuTTY。如果您計劃使用 PuTTY，則需要安裝它，然後使用下列程序將 .pem 檔案轉換為 .ppk 檔案。

   如需詳細資訊，請參閱 Amazon EC2 使用者指南中的下列主題：

   - 使用 PuTTY 從 Windows 連接至您的 Linux 執行個體

- 使用 SSH 連接至您的 Linux 執行個體

  金鑰檔案無法公開提供 SSH 檢視。您可以使用 chmod 400 ***filename***.pem 命令來設定這些許可。如需詳細資訊，請參閱建立金鑰對。

2. (選用) 取得更新並重新啟動。

```
$ sudo yum -y update
            $  sudo reboot
```

3. 重新開機後，請重新連線至您的 EC2 執行個體。
4. 安裝 NFS 用戶端。

   如果您使用的是 Amazon Linux AMI 或 Red Hat Linux AMI，請使用以下命令來安裝 NFS 用戶端。

```
$ sudo yum -y install nfs-utils
```

   如果您使用的是 Ubuntu Amazon EC2 AMI，請使用下列命令安裝 NFS 用戶端。

```
$ sudo apt-get -y install nfs-common
```

5. 使用下列命令啟動 NFS 服務。針對 RHEL 7：

```
$ sudo service nfs start
```

   針對 RHEL 8：

```
$ sudo service nfs-server start
```

6. 確認 NFS 服務已啟動，如下所示。

```
$ sudo service nfs status
Redirecting to /bin/systemctl status nfs.service
# nfs-server.service - NFS server and services
   Loaded: loaded (/usr/lib/systemd/system/nfs-server.service; disabled; vendor
 preset: disabled)
   Active: active (exited) since Wed 2019-10-30 16:13:44 UTC; 5s ago
  Process: 29446 ExecStart=/usr/sbin/rpc.nfsd $RPCNFSDARGS (code=exited, status=0/
SUCCESS)
```

```
 Process: 29441 ExecStartPre=/bin/sh -c /bin/kill -HUP `cat /run/gssproxy.pid`
(code=exited, status=0/SUCCESS)
 Process: 29439 ExecStartPre=/usr/sbin/exportfs -r (code=exited, status=0/SUCCESS)
Main PID: 29446 (code=exited, status=0/SUCCESS)
  CGroup: /system.slice/nfs-server.service
```

如果您使用自訂核心 (亦即如果您建置自訂的 AMI)，您必須至少包含 NFSv4.1 用戶端核心模組，以及正確的 NFS4 userspace 掛載協助程式。

> **Note**
>
> 如果您在啟動 Amazon EC2 執行個體時，選擇 Amazon Linux AMI 2016.03.0 或 Amazon Linux AMI 2016.09.0，則無需安裝 `nfs-utils`，因為它預設已包含在 AMI 中。

下一步：掛載檔案系統

使用下列程序之一以掛載您的檔案系統。

- 以 DNS 名稱掛載於 Amazon EC2
- 以 IP 地址掛載
- 自動掛載 Amazon EFS 檔案系統

建議的 NFS 掛載選項

我們建議設定下列 Linux 掛載選項值：

- `noresvport`：告知 NFS 用戶端在網路連線重新建立時，使用新的傳輸控制通訊協定 (TCP) 來源連接埠。舊版 Linux 核心 (v5.4 及以下版本) 中包含的 NFS 用戶端軟體包含一種行為，即中斷連線時會引發 NFS 用戶端嘗試在相同的 TCP 來源連接埠上重新連線。此行為不符合 TCP RFC 要求，而且會阻止這些用戶端快速重新建立與 EFS 檔案系統的連線。

  使用 `noresvport` 選項有助於確保 NFS 用戶端以透明方式重新連線至 EFS 檔案系統，並在網路復原事件發生後重新連線時保持持續可用。

> **Important**
>
> 我們強烈建議您使用 `noresvport` 掛載選項，以確保您的 EFS 檔案系統在重新連線或網路復原事件發生後持續可用。
> 考慮使用 EFS 掛載協助程式掛載檔案系統。EFS 掛載協助程式使用適用於 Amazon EFS 檔案系統的最佳 NFS 掛載選項。

- `rsize=1048576`：NFS 用戶端為每個網路 READ 請求接收資料時，設定資料位元組上限。讀取來自 EFS 檔案系統上檔案的資料時，將會套用這個值。我們建議您使用最大的大小 (最多 1048576) 以避免效能降低。
- `wsize=1048576`：NFS 用戶端為每個網路 WRITE 請求傳送資料時，設定資料位元組上限。將資料寫入至 EFS 檔案系統上的檔案時，將會套用這個值。我們建議您使用最大的大小 (最多 1048576) 以避免效能降低。
- `hard`：設定 NFS 用戶端在 NFS 請求逾時的復原行為，因此 NFS 請求會重試直到伺服器回覆為止。我們建議您使用硬掛載選項 (`hard`)，以確保資料的完整性。如果您使用 `soft` 掛載，請將 `timeo` 參數設定為至少 `150` 十分之一秒 (15 秒)。這有助於降低軟掛載固有的資料損壞風險。
- `timeo=600`：將 NFS 用戶端等待重試 NFS 請求回應的逾時值設為 600 十分之一秒 (60 秒)。如果您必須變更逾時參數 (`timeo`)，我們建議您使用至少為 `150` 的值，相當於 15 秒。這有助於避免效能降低。
- `retrans=2`：將 NFS 用戶端在請求嘗試進一步復原動作前的重試次數設為 2。
- `_netdev`：在 `/etc/fstab` 中出現時，防止用戶端嘗試掛載到 EFS 檔案系統，直到網路完成啟用。
- `nofail`：如果不論掛載的 EFS 檔案系統處於何種狀態，EC2 執行個體都需要啟動，請將 `nofail` 選項新增至 `/etc/fstab` 檔案中的檔案系統項目。

如果您不使用上述的預設值，請注意下列資訊：

- 一般而言，避免設定任何與預設值不同的掛載選項，這可能導致效能降低和其他問題。例如，變更讀取或寫入的緩衝大小，或停用屬性快取皆可能造成效能降低。
- Amazon EFS 會忽略來源連接埠。如果您變更 Amazon EFS 來源連接埠，不會有任何影響。
- Amazon EFS 不支援 `nconnect` 掛載選項。
- Amazon EFS 不支援任何 Kerberos 安全變體。例如，下列掛載命令會失敗。

```
$ mount -t nfs4 -o krb5p <DNS_NAME>:/ /efs/
```

- 我們建議您使用檔案系統的 DNS 名稱來掛載該檔案系統。系統會在與您 Amazon EC2 執行個體相同的可用區域中，將此名稱解析為 Amazon EFS 掛載目標的 IP 地址。如果您在與您 Amazon EC2 執行個體不同的可用區域中使用掛載目標，您需要為跨可用區域傳送的資料支付標準 EC2 費用。您的檔案系統操作也可能受到延遲。
- 如需更多掛載選項和預設值的詳細說明，請參閱 Linux 文件中的 `man fstab` 和 `man nfs` 頁面。

以 DNS 名稱掛載於 Amazon EC2

> **Note**
>
> 在掛載檔案系統之前，您需要將規則新增至掛載目標安全群組，以便從 EC2 安全群組傳入 NFS 存取處。如需詳細資訊，請參閱 針對 Amazon EC2 執行個體和掛載目標使用 VPC 安全群組。

- 檔案系統 DNS 名稱：使用檔案系統的 DNS 名稱是最簡單的掛載選項。檔案系統的 DNS 名稱會自動解析為連接 Amazon EC2 執行個體之可用區域中掛載目標的 IP 地址。您可以從主控台取得此 DNS 名稱，或者如果您有檔案系統 ID，即可使用以下慣例來建構 DNS 名稱。

```
file-system-id.efs.aws-region.amazonaws.com
```

> **Note**
>
> 解析檔案系統 DNS 名稱的 DNS 時，需要 Amazon EFS 檔案系統在用戶端執行個體的相同可用區域中具有掛載目標。

  - 使用檔案系統 DNS 名稱，您可以使用以下命令將檔案系統掛載到 Amazon EC2 Linux 執行個體。

```
sudo mount -t nfs -o
 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport file-system-id.efs.aws-region.amazonaws.com:/ /efs-mount-point
```

  - 使用檔案系統 DNS 名稱時，您可以藉助下列命令，並在執行受支援 macOS 版本 (Big Sur、Monterey、Ventura) 的 Amazon EC2 Mac 執行個體上掛載檔案系統。

```
sudo mount -t nfs -o
 nfsvers=4.0,rsize=65536,wsize=65536,hard,timeo=600,retrans=2,noresvport,mountport=2049 fil
system-id.efs.aws-region.amazonaws.com:/ /efs
```

> **Important**
>
> 在執行受支援 macOS 版本的 EC2 Mac 執行個體上掛載時，您必須使用 `mountport=2049` 才能成功連線到 EFS 檔案系統。

- 掛載目標 DNS 名稱：在 2016 年 12 月，我們引進檔案系統 DNS 名稱。我們持續為每個可用區域掛載目標提供 DNS 名稱，以提供回溯相容性。掛載目標 DNS 名稱的一般形式如下。

```
availability-zone.file-system-id.efs.aws-region.amazonaws.com
```

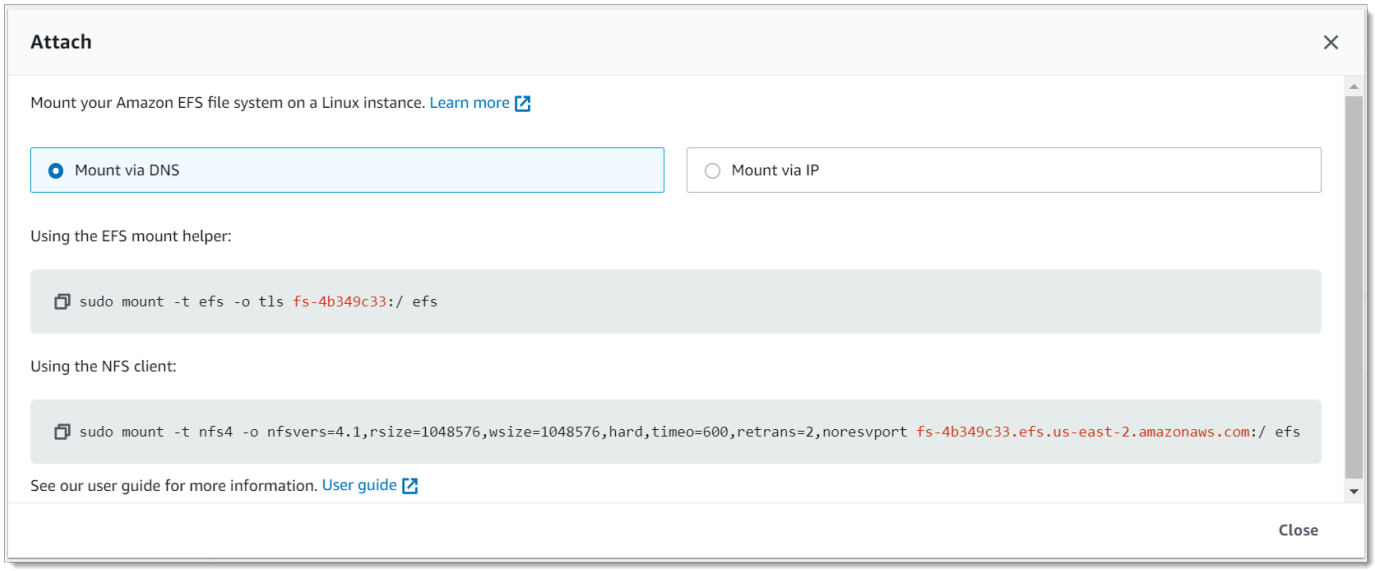
> **Note**
>
> 支援跨可用區域掛載目標 DNS 名稱解決方案。

在某些情況下，您可能會刪除掛載目標，然後在相同的可用區域中建立新的掛載目標。在此情況下，可用區域中新掛載目標的 DNS 名稱與舊掛載目標的 DNS 名稱相同。

您可以在附加對話方塊中檢視和複製要掛載檔案系統的確切指令。

檢視檔案系統的掛載指令

1. 在 Amazon EFS 主控台中，請選擇您要掛載的檔案系統，顯示其詳細資訊頁面。
2. 若要顯示用於此檔案系統的掛載指令，請選擇右上角的「連接」。



連接畫面會顯示用於掛載檔案系統的確切指令。

3. 當使用 EFS 掛載協助程式或 NFS 用戶端掛載時，透過 DNS 掛載預設試圖會使用檔案系統的 DNS 名稱來顯示掛載檔案系統的命令。

如需支援 Amazon E AWS 區域 FS 的清單，請參閱中的 Amazon Elastic File System AWS 一般參考。

若要在 `mount` 命令中使用 DNS 名稱，必須符合下列條件：

- 連接的 EC2 執行個體必須位於 VPC 中，且必須設定為使用 Amazon 提供的 DNS 伺服器。如需關於 Amazon DNS 伺服器的資訊，請參閱《Amazon VPC 使用者指南》中的 DHCP 選項集。
- 在連接 EC2 執行個體的 VPC 上，DNS Resolution (DNS 解析) 和 DNS Hostnames (DNS 主機名稱) 必須全部啟用。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的檢視 EC2 執行個體的 DNS 主機名稱。
- 連接的 EC2 執行個體必須與 EFS 檔案系統位在相同的 VPC 中。如需有關存取及掛載來自其他位置或不同 VPC 之檔案系統的詳細資訊，請參閱逐步解說：使用 AWS Direct Connect 和 VPN 建立和掛載內部部署的檔案系統和逐步解說：掛載來自不同 VPC 的檔案系統 。

> **Note**
>
> 建議您在建立掛載目標之後等待 90 秒，然後再掛載您的檔案系統。此等待可讓 DNS 記錄在檔案系統所在的 AWS 區域 位置完全傳播。

以 IP 地址掛載

除了以 DNS 名稱掛載 Amazon EFS 檔案系統之外，Amazon EC2 執行個體可使用掛載目標的 IP 地址來掛載檔案系統。以 IP 地址掛載的運作方式適用於 DNS 已停用的環境 (例如已停用 DNS 主機名稱的 VPC)。

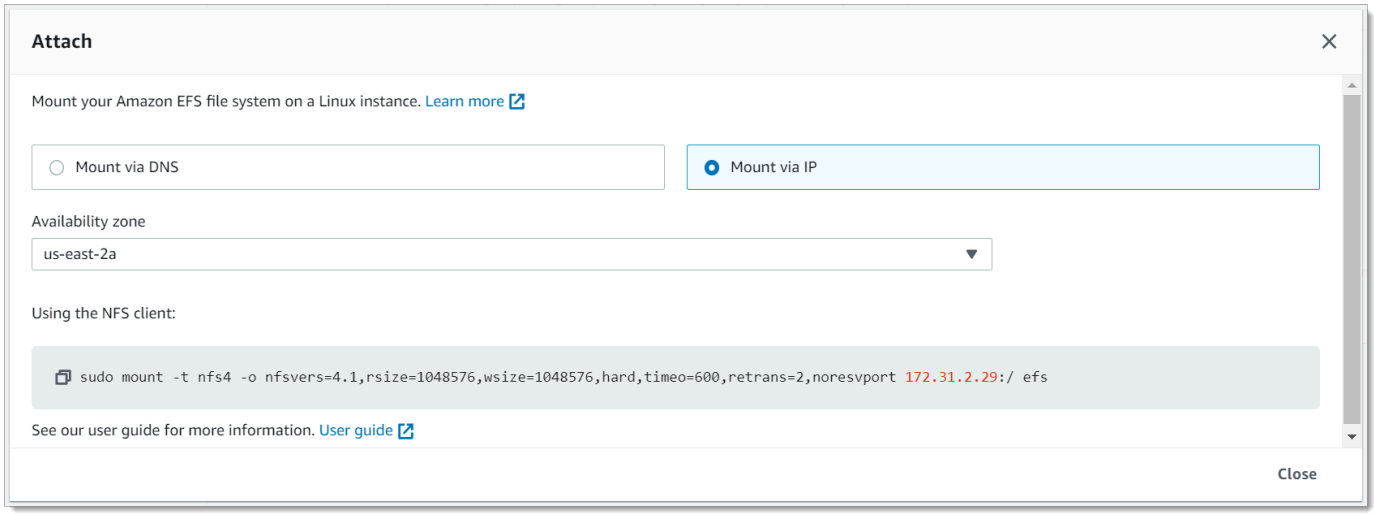
您也可以使用掛載目標 IP 地址設定掛載檔案系統，做為已預設使用其 DNS 名稱掛載檔案系統之應用程式的備用選項。當連接到掛載目標 IP 地址時，EC2 執行個體應使用與連接執行個體相同之可用區域中的掛載目標 IP 地址進行掛載。

您可以在附加對話方塊中檢視和複製要掛載檔案系統的確切指令。

> **Note**
>
> 掛載檔案系統之前，您需要為掛載目標安全群組新增規則，以便自 EC2 安全群組傳入 NFS 存取処。如需詳細資訊，請參閱 針對 Amazon EC2 執行個體和掛載目標使用 VPC 安全群組。

若想使用掛載目標的 IP 地址來檢視並複製掛載 EFS 檔案系統的確切命令

1. 前往 https://console.aws.amazon.com/efs/ 開啟 Amazon Elastic File System 主控台。
2. 在 Amazon EFS 主控台中，請選擇您要掛載的檔案系統，顯示其詳細資訊頁面。
3. 若要顯示用於此檔案系統的掛載指令，請選擇右上角的「連接」。



4. 連接畫面會顯示用於掛載檔案系統的確切指令。

   在 NFS 用戶端的已選可用區域中，選擇透過 IP 掛載，即可顯示使用掛載目標的 IP 地址來掛載檔案系統的命令。

- 使用 mount 命令中的掛載目標 IP 地址時，您可以藉助下列命令在 Amazon EC2 Linux 執行個體上掛載檔案系統。

```
sudo mount -t nfs -o
 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport mount-target-IP:/   /efs
```

- 使用 mount 命令中的挂載目標 IP 地址時，您可以藉助下列命令在 Amazon EC2 Mac 執行個體上掛載檔案系統、執行 macOS Big Sur。

```
sudo mount -t nfs -o
 nfsvers=4.0,rsize=65536,wsize=65536,hard,timeo=600,retrans=2,noresvport,mountport=2049 mount-target-IP:/ /efs
```

> **Important**
>
> 在執行 macOS Big Sur的 EC2 Mac 執行個體上掛載時，您必須使用 mountport=2049 才能成功連線到 EFS 檔案系統。

使用 IP 位址進行掛載 AWS CloudFormation

您也可以使用 AWS CloudFormation 範本中的 IP 位址掛載檔案系統。如需詳細資訊，請參閱適用於社群提供之組態檔案的 awsdocs/彈性豆樣本儲存庫中的儲存空間-EFS-掛載檔案系統-ip- addr.config。GitHub

其他掛載注意事項

我們建議設定下列 Linux 掛載選項值：

- rsize=1048576：NFS 用戶端為每個網路 READ 請求接收資料時，設定資料位元組上限。讀取來自 EFS 檔案系統上檔案的資料時，將會套用這個值。我們建議您使用最大的大小 (最多 1048576) 以避免效能降低。
- wsize=1048576：NFS 用戶端為每個網路 WRITE 請求傳送資料時，設定資料位元組上限。將資料寫入至 EFS 檔案系統上的檔案時，將會套用這個值。我們建議您使用最大的大小 (最多 1048576) 以避免效能降低。

- `hard`：設定 NFS 用戶端在 NFS 請求逾時的復原行為，因此 NFS 請求會重試直到伺服器回覆為止。我們建議您使用硬掛載選項 (`hard`)，以確保資料的完整性。如果您使用 `soft` 掛載，請將 `timeo` 參數設定為至少 `150` 十分之一秒 (15 秒)。這有助於降低軟掛載固有的資料損壞風險。
- `timeo=600`：將 NFS 用戶端等待重試 NFS 請求回應的逾時值設為 600 十分之一秒 (60 秒)。如果您必須變更逾時參數 (`timeo`)，我們建議您使用至少為 `150` 的值，相當於 15 秒。這有助於避免效能降低。
- `retrans=2`：將 NFS 用戶端在請求嘗試進一步復原動作前的重試次數設為 2。
- `noresvport`：告知 NFS 用戶端在網路連線重新建立時，使用新的傳輸控制通訊協定 (TCP) 來源連接埠。這可讓您確保在網路復原事件後，EFS 檔案系統具有不中斷的可用性。
- `_netdev`：在 `/etc/fstab` 中出現時，防止用戶端嘗試掛載到 EFS 檔案系統，直到網路完成啟用。

一般而言，避免設定任何與預設值不同的掛載選項，這可能導致效能降低和其他問題。如果您不使用上述的預設值，請注意下列資訊：

- 變更讀取或寫入的緩衝大小，或停用屬性快取皆可能造成效能降低。
- Amazon EFS 會忽略來源連接埠。如果您變更 Amazon EFS 來源連接埠，不會有任何影響。
- Amazon EFS 不支援任何 Kerberos 安全變體。例如，下列掛載命令會失敗。

```
$ mount -t nfs4 -o krb5p <DNS_NAME>:/ /efs/
```

- 我們建議您使用檔案系統的 DNS 名稱來掛載該檔案系統。Amazon EFS 在會與您 Amazon EC2 執行個體相同的可用區域中，將此名稱解析為 Amazon EFS 掛載目標的 IP 地址，而無需呼叫外部資源。如果您在與您 Amazon EC2 執行個體不同的可用區域中使用掛載目標，您需要為跨可用區域傳送的資料支付標準 EC2 費用。您的檔案系統操作也可能受到延遲。
- 如需更多掛載選項和預設值的詳細說明，請參閱 Linux 文件中的 `man fstab` 和 `man nfs` 頁面。

> **Note**
>
> 如果不論掛載的 EFS 檔案系統處於何種狀態，EC2 執行個體都需要啟動，請將 `nofail` 選項新增至 `/etc/fstab` 檔案中的檔案系統項目。

卸載檔案系統

在刪除檔案系統之前，我們建議您將其從每個連接至的 Amazon EC2 執行個體上卸載。您可以在 Amazon EC2 執行個體上執行 umount 命令來卸載執行個體上的檔案系統。您無法透過 AWS CLI、或透過任何 AWS 開發套件卸載 Amazon EFS 檔案系統。 AWS Management Console若要卸載 Amazon EFS 檔案系統，其連接至執行 Linux 的 Amazon EC2 執行個體，使用 umount 命令，如下所示：

```
umount /mnt/efs
```

我們建議您不要指定任何其他 umount 選項。請避免設定任何其他與預設值不同的 umount 選項。

您可以執行 df 命令，以確認 Amazon EFS 檔案系統已卸載。此命令會顯示目前掛載於 Linux 型 Amazon EC2 執行個體上的檔案系統磁碟用量統計資料。如果您想卸載的 Amazon EFS 檔案系統未列在 df 命令輸出中，這表示該檔案系統已卸載。

Example ：識別 Amazon EFS 檔案系統的掛載狀態並將其卸載

```
$ df -T
Filesystem Type 1K-blocks Used Available Use% Mounted on
/dev/sda1 ext4 8123812 1138920 6884644 15% /
availability-zone.file-system-id.efs.aws-region.amazonaws.com :/ nfs4 9007199254740992
 0 9007199254740992 0% /mnt/efs
```

```
$ umount /mnt/efs
```

```
$ df -T
```

```
Filesystem Type 1K-blocks Used Available Use% Mounted on
/dev/sda1 ext4 8123812 1138920 6884644 15% /
```

掛載問題疑難排解

以下內容提供您如何排解 Amazon EFS 的檔案系統掛載問題。

- 在 Windows 執行個體上掛載檔案系統失敗
- 伺服器已拒絕存取
- 自動掛載失敗且執行個體沒有回應

在 Windows 執行個體上掛載檔案系統失敗

在 Microsoft Windows 上的 Amazon EC2 執行個體掛載檔案系統失敗。

採取動作

不要使用不支援的 Windows EC2 執行個體的 Amazon EFS。

伺服器已拒絕存取

檔案系統掛載失敗，並顯示下列訊息：

```
/efs mount.nfs4: access denied by server while mounting 127.0.0.1:/
```

如果 NFS 用戶端沒有檔案系統的掛載許可，就會發生這個問題。

採取動作

如果您嘗試使用 IAM 掛載檔案系統，請確定您在掛載命令中使用的是 `-o iam` 選項。這會告訴 EFS 掛載協助程式，將您的憑證傳遞到 EFS 掛載目標。如果您仍然不具備存取權，請檢查檔案系統政策和身

分政策，以確定沒有適用於連線的 DENY 子句，而且至少有一個適用於連線的 ALLOW 子句。如需詳細資訊，請參閱 使用 IAM 控制檔案系統資料存取 及 建立檔案系統原則。

自動掛載失敗且執行個體沒有回應

如果檔案系統已自動掛載於執行個體上且沒有宣告 _netdev 選項，則可能發生此問題。若 _netdev 已遺失，EC2 執行個體可能會停止回應。此結果是因為網路檔案系統在運算執行個體開始聯網後需要初始化。

採取動作

如果發生此問題，請聯絡 Sup AWS port 部門。

在 /etc/fstab 中掛載多個 Amazon EFS 檔案系統失敗

對於在 /etc/fstab 擁有兩個或以上 Amazon EFS 項目，並使用 systemd init 系統的執行個體而言，可能有些時候不會掛載這些部分或全部的項目。在這種情況下，dmesg 輸出會顯示一或多個類似以下的行。

```
NFS: nfs4_discover_server_trunking unhandled error -512. Exiting with error EIO
```

採取動作

在這種情況下，我們建議您在 /etc/systemd/system/mount-nfs-sequentially.service 建立新的 systemd 服務檔案。在檔案中需要插入代碼，代碼內容取決于您是通過手動掛載檔案系統還是使用 Amazon EFS 掛載協助程式。

- 如果您要手動掛載檔案系統，則 ExecStart 指令必須指向網路檔案系統 (NFS4)。在檔案中插入下列代碼：

```
[Unit]
Description=Workaround for mounting NFS file systems sequentially at boot time
After=remote-fs.target

[Service]
Type=oneshot
ExecStart=/bin/mount -avt nfs4
RemainAfterExit=yes

[Install]
WantedBy=multi-user.target
```

- 如果您使用的是 Amazon EFS 掛載協助程式，則 `ExecStart` 命令必須指向 EFS 而非 NFS4，才能使用 Transport Layer Security (TLS)。在檔案中插入下列代碼：

```
[Unit]
Description=Workaround for mounting NFS file systems sequentially at boot time
After=remote-fs.target

[Service]
Type=oneshot
ExecStart=/bin/mount -avt efs
RemainAfterExit=yes

[Install]
WantedBy=multi-user.target
```

建立檔案后，請執行以下兩個命令：

1. `sudo systemctl daemon-reload`
2. `sudo systemctl enable mount-nfs-sequentially.service`

然後重新啟動您的 Amazon EC2 執行個體。檔案系統為隨需掛載，通常可在一秒內完成。

出現「錯誤 fs 類型」錯誤訊息的掛載命令失敗

出現以下錯誤訊息的掛載命令失敗。

```
mount: wrong fs type, bad option, bad superblock on 10.1.25.30:/,
missing codepage or helper program, or other error (for several filesystems
(e.g. nfs, cifs) you might need a /sbin/mount.<type> helper program)
In some cases useful info is found in syslog - try dmesg | tail or so.
```

採取動作

如果您收到此訊息，請安裝 `nfs-utils` (或 Ubuntu 的 `nfs-common`) 套件。如需詳細資訊，請參閱安裝 NFS 用戶端。

出現「錯誤的掛載選項」錯誤訊息的掛載命令失敗

出現以下錯誤訊息的掛載命令失敗。

```
mount.nfs: an incorrect mount option was specified
```

採取動作

此錯誤訊息最可能表示您的 Linux 發行版本不支援 4.0 和 4.1 版本的網路檔案系統 (NFSv4)。您可以執行以下命令以確認是否為此情況。

```
$ grep CONFIG_NFS_V4_1 /boot/config*
```

如果上述命令傳回 `# CONFIG_NFS_V4_1 is not set`，則您的 Linux 發行版本不支援 NFSv4.1。如需適用於 Amazon Elastic Compute Cloud (Amazon EC2) 且支援 NFSv4.1 的 Amazon Machine Image (AMI) 詳細資訊，請參閱 NFS 支援。

使用存取點掛載失敗

使用存取點進行掛載時，掛載命令會失敗，並顯示下列錯誤訊息：

```
mount.nfs4: mounting access_point failed, reason given by server: No such file or
 directory
```

採取動作

此錯誤訊息指出指定的 EFS 路徑不存在。請確定您已提供存取點根目錄的擁有權和權限。EFS 不使用這項資訊將不能建立根目錄。如需詳細資訊，請參閱 使用 Amazon EFS 存取點。

如果您未指定任何根目錄擁有權和權限，且根目錄尚未存在，EFS 將不會建立根目錄。如果出現以上情況，那麼嘗試使用存取點掛載檔案系統將會失敗。

在檔案系統建立後立即發生檔案系統掛載失敗

建立網域名稱服務 (DNS) 記錄的掛載目標後，最多可能需要 90 秒才能在 AWS 區域區域中完全傳播。

採取動作

如果您以程式設計方式建立和掛載檔案系統 (例如使用範 AWS CloudFormation 本)，建議您實作等待條件。

檔案系統掛載停止回應，然後因逾時錯誤而失敗

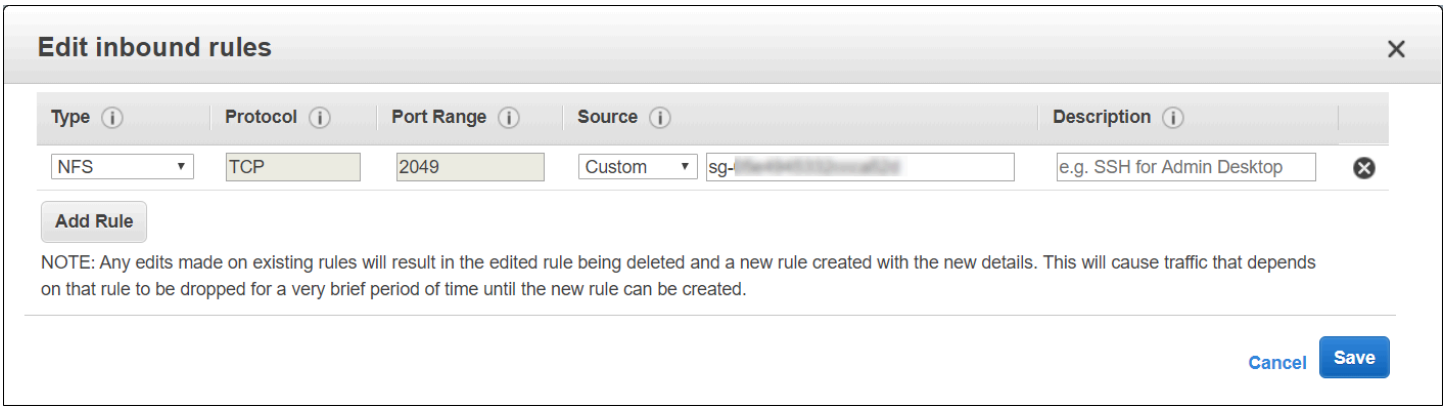
檔案系統掛載命令停止回應一至兩分鐘，然後因逾時錯誤而失敗。下列代碼顯示了範例。

```
$ sudo mount -t nfs -o
 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport mount-
target-ip:/ mnt

[2+ minute wait here]
mount.nfs: Connection timed out
$Â
```

採取動作

當 Amazon EC2 執行個體或掛載目標安全群組未正確設定時，則可能發生此錯誤。請確定掛載目標安全群組具有輸入規則，此規則允許透過 EC2 安全群組進行 NFS 存取。



如需詳細資訊，請參閱 建立安全群組。

確認您指定的掛載目標 IP 地址為有效。如果您指定了錯誤的 IP 地址，且在該 IP 地址沒有其他內容可拒絕掛載，則您可能會遇到這個問題。

使用 DNS 名稱進行 NFS 掛載檔案系統失敗

嘗試使用 NFS 用戶端 (不使用 amazon-efs-utils 用戶端) 掛載檔案系統，而掛載目標通過檔案系統的 DNS 名稱來標識，結果失敗，如下列範例所示：

```
$ sudo mount -t nfs -o
 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport file-
system-id.efs.aws-region.amazonaws.com:/ mnt
mount.nfs: Failed to resolve server file-system-id.efs.aws-region.amazonaws.com:
  Name or service not known.

$
```

採取動作

檢查 VPC 組態。如果您使用的是自訂 VPC，請確保 DNS 設定已啟用。如需詳細資訊，請參閱 Amazon VPC 使用者指南中的 VPC 的 DNS 屬性。此外，檔案系統和掛載目標 DNS 名稱無法從其所在的 VPC 外部進行解析。

在`mount`命令中使用檔案系統的 DNS 名稱來掛載檔案系統之前，您必須執行下列動作：

- 請確認相同可用區域中有做為 Amazon EC2 執行個體的 Amazon EFS 掛載目標。
- 請確認有掛載目標位於 Amazon EC2 執行個體所在的同一 VPC。否則，您無法將 DNS 名稱解析用於在另一個 VPC 中的 EFS 掛載目標。如需詳細資訊，請參閱 從另一個 AWS 帳戶 或 VPC 掛載 EFS 檔案系統。
- 在 Amazon VPC 中連線您的 Amazon EC2 執行個體，並設為使用 Amazon 提供的 DNS 伺服器。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的 Amazon VPC 中的 DHCP 選項集。
- 確認連線 Amazon EC2 執行個體的 Amazon VPC 擁有已啟用的 DNS 主機名稱。如需詳細資訊，請參閱 Amazon VPC 使用者指南中的 VPC 的 DNS 屬性。

出現「nfs 未回應」的檔案系統掛載失敗

出現 "`nfs: server_name still not responding`" 傳輸控制通訊協定 (TCP) 重新連線事件，Amazon EFS 檔案系統掛載失敗。

採取動作

使用 `noresvport` 掛載選項，確定 NFS 用戶端會在網路連線重新建立時使用新的 (TCP) 來源連接埠。這可讓您確保網路復原事件後的不中斷可用性。

掛載目標生命週期狀態已停滯

該掛載目標生命週期狀態停滯在建立或刪除狀態。

採取動作

重試 `CreateMountTarget` 或 `DeleteMountTarget` 呼叫。

掛載目標生命週期狀態顯示錯

掛載目標生命週期狀態顯示錯誤。

採取動作

如果虛擬私有雲端 (VPC) 的託管區域有衝突，Amazon EFS 將無法為新檔案系統掛載目標建立必要的網域名稱系統 (DNS) 記錄。Amazon EFS 無法在客戶擁有的託管區域內建立新記錄。如果您需要維護具有衝突 `efs.<region>.amazonaws.com` DNS 範圍的託管區域，請在單獨的 VPC 中建立託管區域。如需關於在 VPC中考量 DNS 的詳細資訊，請參閱 VPC 中的 DNS 屬性。

若要解決此問題，請從 VPC 刪除有衝突的 `efs.<region>.amazonaws.com` 託管，然後再次建立掛載目標。如需建立掛載目標的詳細資訊，請參閱 管理掛載目標。

掛載未回應

Amazon EFS 掛載沒有回應。例如，`ls` 命令停止回應。

採取動作

如果另一個應用程式正在寫入大量資料到檔案系統，則可能發生此錯誤。對寫入操作尚未完成前的檔案進行存取可能會被拒。一般而言，對正在被寫入的檔案嘗試任何存取的命令或應用程式都可能造成停止回應。例如，當 `ls` 命令遇到被寫入的檔案時，可能會停止回應。這是因為一些 Linux 發行版本設定了 `ls` 命令別名，因此除了列出目錄內容外，它也會擷取檔案屬性。

若要解決這個問題，請確認另一個應用程式正在寫入檔案至 Amazon EFS 掛載，並處於 `Uninterruptible sleep` (D) 狀態，如以下範例所示：

```
$ ps aux | grep large_io.py
root 33253 0.5 0.0 126652 5020 pts/3 D+ 18:22 0:00 python large_io.py /efs/large_file
```

在您已確認是這種情況後，您可以等待其他寫入操作完成，或實施解決方法來處理此問題。在 `ls` 範例中，您可以直接使用 `/bin/ls` 命令，而不要使用別名。如此可讓命令繼續執行，而不會因正在寫入的檔案而停止回應。一般而言，如果應用程式的資料寫入可以強制定期排清資料 (或許使用 `fsync(2)`)，如此一來可協助其他應用程式改善您的檔案系統回應能力。不過，這項改善措施可能會犧牲應用程式寫入資料時的效能。

掛載的客戶端中斷連線

客戶端掛載到 Amazon EFS 檔案系統后，偶爾會因爲各種原因中斷連線。發生中斷時，將 NFS 用戶端設計為自動連線，盡量減少日常中斷對應用程式效能和可用性的影響。在大多數情況下，用戶端會在數秒內透明地重新連線。

然而，舊版 Linux 核心 (v5.4 及以下版本) 中包含的 NFS 用戶端軟體存在一種行為，即中斷連線時會引發 NFS 用戶端嘗試在相同的 TCP 來源連接埠上重新連線。此行為不符合 TCP RFC 要求，而且會阻止這些用戶端無法快速重新建立與 EFS 伺服器 (在此情況下為 EFS 檔案系統) 的連線。

若要解決此問題，強烈建議您使用 Amazon EFS 掛載協助程式掛載 EFS 檔案系統。EFS 掛載協助程式使用適用於 Amazon EFS 檔案系統的最佳掛載設定。如需關於 EFS 客戶端和掛載協助程式的詳細資訊，請參閱 安裝 Amazon EFS 工具。

如果您無法使用 EFS 掛載協助程式，強烈建議您使用 `noresvport` NFS 掛載選項，此選項會指示 NFS 用戶端使用新的 TCP 來源連接埠重新建立連線，以避免無法使用的問題。如需詳細資訊，請參閱 建議的 NFS 掛載選項。

新掛載的檔案系統操作傳回「錯誤的檔案處理」錯誤

新掛載檔案系統執行的操作傳回了 `bad file handle` 錯誤。

如果 Amazon EC2 執行個體已透過特定 IP 地址連接到一個檔案系統和一個掛載目標，而該檔案系統與掛載目標已被刪除，則可能出現此錯誤。如果您使用相同掛載目標 IP 地址建立了新的檔案系統與掛載目標以連接到 Amazon EC2 執行個體，則可能發生此問題。

採取動作

您可以透過卸載檔案系統來解決此錯誤，然後重新掛載該檔案系統至 Amazon EC2 執行個體。如需卸載 Amazon EFS 檔案系統的詳細資訊，請參閱 卸載檔案系統。

卸載檔案系統失敗

如果您的檔案系統正在忙碌中，則無法將其卸載。

採取動作

您可以透過下列方式來解決問題：

- 使用惰性卸載，umount -l它會在執行時將檔案系統從檔案系統階層中分離出來，然後在檔案系統不再忙碌時立即清除所有對檔案系統的參照。
- 等待所有讀取和寫入操作完成，然後再次嘗試 umount 命令。
- 使用 umount -f 指令強制卸載。

> **Warning**
>
> 強制卸載會中斷目前在該檔案系統中進行的任何資料讀取或寫入操作。使用此選項時，請參閱 umount 命令手冊頁，獲取詳細咨詢和指導方針。

將資料傳輸到 Amazon EFS

您可以使用 AWS Transfer Family 和 AWS DataSync 將資料傳輸到 Amazon EFS 檔案系統。 AWS DataSync 是一種線上資料傳輸服務，可在網路檔案系統 (NFS)、伺服器訊息區 (SMB) 檔案伺服器、自行管理物件儲存，以及 AWS 服務之間複製資料。如需 DataSync 搭配 Amazon EFS 使用的詳細資訊，請參閱用 AWS DataSync 於將資料傳輸到 Amazon EFS。

AWS Transfer Family 這是一項全受管 AWS 服務，可透過安全檔案傳輸通訊協定 (SFTP)、檔案傳輸通訊協定 (FTP) 和透過安全通訊端層 (FTPS) 協定將檔案傳入和傳出 Amazon EFS 檔案系統。使用 Transfer Family 后，您可以讓業務合作夥伴存取儲存在 Amazon EFS 檔案系統中的檔案，以支援各種使用案例，例如資料分發、供應鏈、內容管理和 Web 服務應用程式。如需關於在 Amazon EFS 中使用 Transfer Family 的詳細資訊，請參閱 用 AWS Transfer Family 於將資料傳輸到 Amazon EFS。

主題

用 AWS DataSync 於將資料傳輸到 Amazon EFS

AWS DataSync 是一種線上資料傳輸服務，可簡化、自動化並加速在內部部署儲存系統之間以及儲存服務之間的資料移動和複寫速度。 AWS DataSync 可以在網路檔案系統 (NFS)、伺服器訊息區 (SMB) 檔案伺服器、自我管理物件儲存、Amazon S3 儲存貯體 AWS Snowcone、Amazon EFS 檔案系統和 Windows 檔案伺服器檔案系統的 FSx 之間複製資料。

您也可以使用 DataSync 在兩個 EFS 檔案系統之間傳輸檔案，包括不同 AWS 區域 s 中的檔案系統和不同檔案系統所擁有的檔案系統。 AWS 帳戶使 DataSync 用在 EFS 檔案系統之間複製資料，您可以執行一次性資料移轉、針對分散式工作負載定期資料擷取，以及自動化複寫以進行資料保護和復原。

如需詳細資訊，請參閱 開始使用 Amazon Elastic File System 及《AWS DataSync 使用者指南》https://docs.aws.amazon.com/datasync/latest/userguide/。

用 AWS Transfer Family 於將資料傳輸到 Amazon EFS

AWS Transfer Family 這是一項全受管 AWS 服務，可透過下列協定將檔案傳入和傳出 Amazon EFS 檔案系統：

- Secure Shell (SSH) 檔案傳輸通訊協定 (SFTP) (AWS Transfer for SFTP)
- 檔案傳輸通訊協定安全 (FTPS) (AWS Transfer for FTPS)
- 檔案傳輸通訊協定 (FTP) (AWS Transfer for FTP)

使用 Transfer Family，您可以安全地讓第三方 (例如廠商、合作夥伴或客戶) 透過支援的通訊協定在全球範圍內大規模存取您的檔案，而無需管理任何基礎架構。此外，您現在可以使用 SFTP、FTPS 和 FTP 用戶端，從 Windows、macOS 和 Linux 環境中輕鬆存取 EFS 檔案系統。這有助於將 NFS 用戶端和存取點以外的資料存取性擴展到多個環境中的使用者。

使用 Transfer Family 在 Amazon EFS 檔案系統中傳輸資料，其計算方式與其他用戶端使用方式相同。如需詳細資訊，請參閱 輸送量模式 及 Amazon EFS 配額。

若要進一步了解 AWS Transfer Family，請參閱使AWS Transfer Family 用者指南。

> **Note**
>
> 對於擁有具有允許在 2021 年 1 月 6 日之前建立的公共存取政策的 Amazon EFS 檔案系統，Tran AWS 帳戶 sfer Family 與 Amazon EFS 搭配使用預設為停用。要啟用使用 Transfer Family 訪問您的文件系統，請聯繫 AWS Support。

主題

AWS Transfer Family 搭配 Amazon EFS 使用的先決條件

若要使用 Transfer Family 來存取 Amazon EFS 檔案系統的檔案，您的組態必須符合下列條件：

- Transfer Family 伺服器和您的 Amazon EFS 檔案系統位於同一個 AWS 區域中。
- IAM 政策設定為允許存取 Transfer Family 使用的 IAM 角色。如需詳細資訊，請參閱《AWS Transfer Family 使用者指南》中的建立 IAM 角色和政策。
- (選用) 如果 Transfer Family 伺服器屬於其他帳戶，請啟用跨帳户存取權。
  - 請確定您的檔案系統政策不允許公開存取。如需詳細資訊，請參閱 封鎖對 Amazon EFS 檔案系統的公開存取。

- 修改檔案系統政策以啟用跨帳戶存取權。如需詳細資訊，請參閱 設定 Transfer Family 的跨帳戶存取權。

設定您的 Amazon EFS 檔案系統以搭配使用 AWS Transfer Family

設定 Amazon EFS 檔案系統與 Transfer Family 搭配使用時，需要執行下列步驟：

- 步驟 1. 取得分配給 Transfer Family 列使用者的 POSIX ID 清單。
- 步驟 2. 使用分配給 Transfer Family 使用者的 POSIX ID，確保 Transfer Family 使用者可以存取您的檔案系統目錄。
- 步驟 3. IAM 政策設定為允許存取 Transfer Family 使用的 IAM 角色。

設定 Transfer Family 使用者的檔案和目錄許可

請確定 Transfer Family 使用者可存取 EFS 檔案系統上所需的檔案和目錄。使用分配給 Transfer Family 使用者的 POSIX ID 清單，將存取許可指派給目錄。在此範例中，使用者會在 EFS 掛載點下建立名為 `transferFam` 的目錄。根據您的使用情況，可選用建立目錄。如果需要，您可以在 EFS 檔案系統上選擇其名稱和位置。

將檔案和目錄許可指派給 Transfer Family 的 POSIX 使用者

1. 連線到您的 Amazon EC2 執行個體。只有運行以 Linux 為基礎的 EC2 執行個體，才能掛載 Amazon EFS 文件系統。
2. 如果 EFS 檔案系統尚未掛載在 EC2 執行個體上，請掛載 EFS 檔案系統。如需詳細資訊，請參閱 掛載 EFS 檔案系統。
3. 下列範例會在 EFS 檔案系統上建立目錄，並將其群組變更為 Transfer Family 使用者的 POSIX 群組 ID，在此範例中 ID 為 1101。

    a. 使用下列命令，建立 `efs/transferFam` 目錄。實際上，您可以使用已選檔案系統上的名稱和位置。

```
[ec2-user@ip-192-0-2-0 ~]$ ls
efs  efs-mount-point  efs-mount-point2
[ec2-user@ip-192-0-2-0 ~]$ ls efs
[ec2-user@ip-192-0-2-0 ~]$ sudo mkdir efs/transferFam
[ec2-user@ip-192-0-2-0 ~]$ ls -l efs
total 0
```

```
drwxr-xr-x 2 root root 6 Jan  6 15:58 transferFam
```

b. 使用下列命令，將 `efs/transferFam` 的群組變更為指派給 Transfer Family 使用者的 POSIX GID。

```
[ec2-user@ip-192-0-2-0 ~]$ sudo chown :1101 efs/transferFam/
```

c. 確認變更。

```
[ec2-user@ip-192-0-2-0 ~]$ ls -l efs
total 0
drwxr-xr-x 2 root 1101 6 Jan  6 15:58 transferFam
```

允許存取 Transfer Family 使用的 IAM 角色

在 Transfer Family 中，您可以建立以資源為基礎的 IAM 政策和 IAM 角色，以定義使用者對 EFS 檔案系統的存取權。如需詳細資訊，請參閱《AWS Transfer Family 使用者指南》中的建立 IAM 角色和政策。您必須使用 IAM 身分政策或檔案系統政策授予該 Transfer Family IAM 角色對 EFS 檔案系統的存取權。

下列檔案系統政策範例，即授予 `ClientMount` (讀取) 和 `ClientWrite` 對 IAM 角色 `EFS-role-for-transfer` 的存取權。

```
{
    "Version": "2012-10-17",
    "Id": "efs-policy-wizard-8698b356-4212-4d30-901e-ad2030b57762",
    "Statement": [
        {
            "Sid": "Grant-transfer-role-access",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/EFS-role-for-transfer"
            },
            "Action": [
                "elasticfilesystem:ClientWrite",
                "elasticfilesystem:ClientMount"
            ]
        }
    ]
}
```

如需建立檔案系統政策的詳細資訊，請參閱 建立檔案系統原則。如需使用以身分爲基礎的 IAM 政策來管理對 EFS 資源存取權的詳細資訊，請參閱 Amazon EFS 身分型政策。

設定 Transfer Family 的跨帳户存取權

如果用來存取檔案系統的 Transfer Family 伺服器屬於不同的伺服器 AWS 帳戶，您必須授與該帳戶對您檔案系統的存取權。此外，您的檔案系統政策必須是非公開狀態。如需封鎖對檔案系統的公開存取的詳細資訊，請參閱 封鎖對 Amazon EFS 檔案系統的公開存取。

您可以在檔案系統原則中授與不同的檔案系統 AWS 帳戶 存取權。在 Amazon EFS 主控台中，使用檔案系統政策編輯器的授與其他許可區段來指定要授與的檔案系統存取權限 AWS 帳戶 和層級。如需建立或編輯檔案系統政策的詳細資訊，請參閱 建立檔案系統原則。

您可以使用帳戶 ID 或帳戶 Amazon Resource Name (ARN) 來指定帳戶。如需關於 ARN 的詳細資訊，請參閱《IAM 使用者指南》中的 IAM ARN。

下列範例是非公用檔案系統政策，該政策將授予檔案系統跨帳户存取權。該政策有下列兩種陳述式：

1. 第一種陳述式為 NFS-client-read-write-via-fsmt，即使用檔案系統掛載目標將讀取、寫入和根權限授予存取檔案系統的 NFS 用戶端。
2. 第二個陳述式只會授與讀取和寫入權限給 AWS 帳戶 111122223333，這是擁有 Transfer Family 伺服器的帳戶，需要存取您帳戶中此 EFS 檔案系統的帳戶。Grant-cross-account-access

```
{
    "Statement": [
        {
            "Sid": "NFS-client-read-write-via-fsmt",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Action": [
                "elasticfilesystem:ClientRootAccess",
                "elasticfilesystem:ClientWrite",
                "elasticfilesystem:ClientMount"
            ],
            "Condition": {
                "Bool": {
                    "elasticfilesystem:AccessedViaMountTarget": "true"
                }
            }
```

```
        },
        {
            "Sid": "Grant-cross-account-access",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "elasticfilesystem:ClientWrite",
                "elasticfilesystem:ClientMount"
            ]
        }
    ]
}
```

下列檔案系統政策會新增一份陳述式，用來授予 Transfer Family 所使用的 IAM 角色的存取權。

```
{
    "Statement": [
        {
            "Sid": "NFS-client-read-write-via-fsmt",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Action": [
                "elasticfilesystem:ClientRootAccess",
                "elasticfilesystem:ClientWrite",
                "elasticfilesystem:ClientMount"
            ],
            "Condition": {
                "Bool": {
                    "elasticfilesystem:AccessedViaMountTarget": "true"
                }
            }
        },
        {
            "Sid": "Grant-cross-account-access",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
```

```
                "elasticfilesystem:ClientWrite",
                "elasticfilesystem:ClientMount"
            ]
        },
        {
            "Sid": "Grant-transfer-role-access",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/EFS-role-for-transfer"
            },
            "Action": [
                "elasticfilesystem:ClientWrite",
                "elasticfilesystem:ClientMount"
            ]
        }
    ]
}
```

管理 Amazon EFS 檔案系統

檔案系統管理任務是指建立和刪除檔案系統，管理標籤、檔案系統備份、存取，以及管理現有檔案系統掛載目標的網路存取權限。

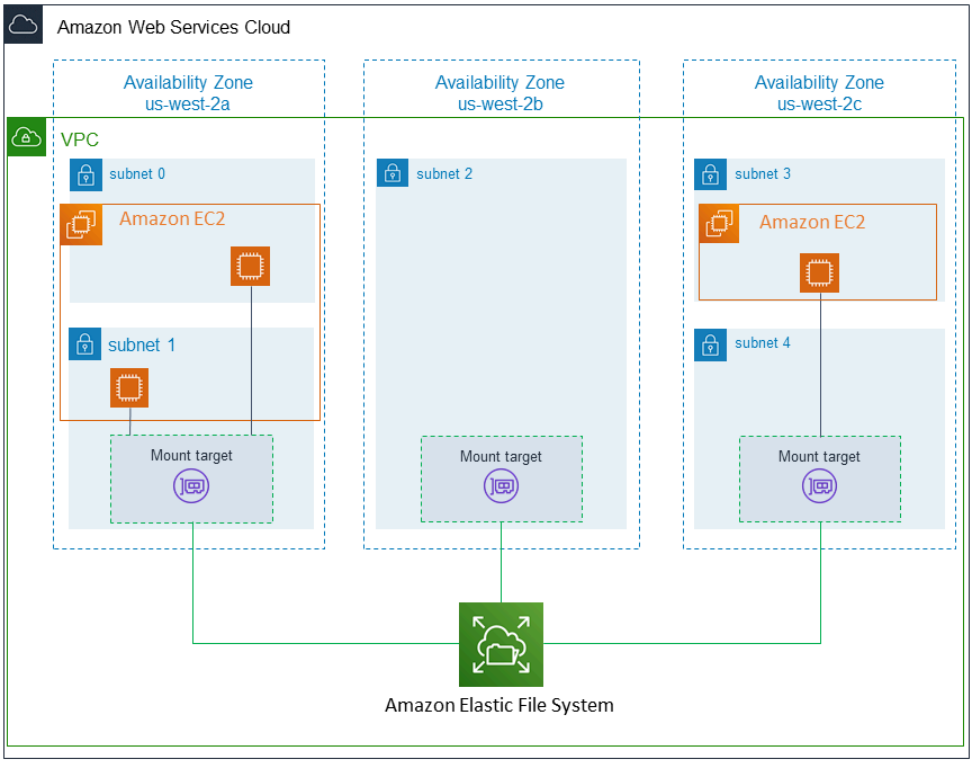
您可以使用或以程式設計方式使用 AWS Management Console AWS Command Line Interface (AWS CLI) 或 API 來執行這些檔案系統管理工作，如以下各節所述。

主題

管理檔案系統網路存取權限

您可以使用為檔案系統建立的掛載目標，將檔案系統掛接到 Amazon EC2 或虛擬私有雲 (VPC) 中的其他 AWS 運算執行個體。管理檔案系統網路存取權限，即指管理檔案系統掛載目標。

下圖說明 VPC 中的 EC2 執行個體如何使用掛載目標存取 Amazon EFS 檔案系統。



下圖說明在三種不同 VPC 子網路中啟動的 EC2 執行個體如何存取 Amazon EFS 檔案系統。該圖也會顯示每個可用區域中的一個掛載目標 (無論每個可用區域中有幾個子網路)。

每個可用區域只能建立一個掛載目標。如果一個可用區域有多個子網路，如圖其中一區域所示，您可以在其中一個子網路中建立掛載目標。只要您在可用區域中有一個掛載目標，在其任一子網路中啟動的 EC2 執行個體都可以共用相同的掛載目標。

管理掛載目標是指這些活動：

- 在 VPC 中建立和刪除掛載目標 – 至少，您應該在要從中存取檔案系統的每個可用區域中建立掛載目標。
- 更新掛載目標組態：當您建立掛載目標時，會將安全群組與掛載目標關聯。安全群組就像是虛擬防火牆，控制進出掛載目標的流量。您可以新增傳入規則以控制掛載目標以及檔案系統的存取。建立掛載目標之後，您可能會希望修改指派給它們的安全群組。

以下區段提供有關管理檔案系統網路存取權限的資訊。

主題

- 在 VPC 中建立或刪除掛載目標

- 為您的掛載目標變更 VPC
- 更新掛載目標組態

在 VPC 中建立或刪除掛載目標

若要在 VPC 中存取 Amazon EFS 檔案系統，您需要掛載目標。關於 Amazon EFS 檔案系統，下列項目為真：

- 您可在每個可用區域中建立一個掛載目標。
- 如果 VPC 在可用區域中有多個子網路，您僅可在其中一個子網路中建立一個掛載目標。在可用區域的所有 EC2 執行個體都可以共用單一掛載目標。

> **Note**
>
> 我們建議您在每個可用區域中建立一個掛載目標。透過在另一個可用區域建立的掛載目標，在一個可用區域中的 EC2 執行個體上掛載檔案系統，有成本上的考量。如需詳細資訊，請參閱 Amazon EFS。此外，始終在執行個體的可用區域処使用掛載目標，您會少一些故障。如果掛載目標的區域發生故障，您便無法透過掛載目標存取您的檔案系統。

如果您刪除了掛載目標，該操作會強制中斷任何掛載的檔案系統掛載，此舉可能會中斷使用該掛載的執行個體或應用程式。為了避免應用程式中斷，請在刪除掛載目標前停止應用程式並卸載檔案系統。如需詳細資訊，請參閱 管理掛載目標。

> **Note**
>
> 刪除掛載目標前，請先卸載檔案系統。如需詳細資訊，請參閱 卸載檔案系統。

您一次僅能在一個 VPC 中使用一個檔案系統。也就是說，您一次只可以在一個 VPC 中為檔案系統建立掛載目標。如果您想要從其他 VPC 存取檔案系統，您必須先從目前的 VPC 刪除掛載目標。然後在另一個 VPC 中建立新的掛載目標。

使用 AWS Management Console、和 API AWS CLI，您可以在檔案系統上建立和管理掛載目標。針對現有掛載目標，您可以新增和移除安全群組，或刪除掛載目標。如需詳細資訊，請參閱 管理掛載目標。

為您的掛載目標變更 VPC

您每次要根據 Amazon EFS 服務才能在 VPC 中使用 Amazon EFS 檔案系統。也就是說，您可以在 VPC 中建立適用於您檔案系統的掛載目標，並使用這些掛載目標提供存取檔案系統的權限。

您可以從下列目標掛載 Amazon EFS 檔案系統：

- 相同 VPC 中的 Amazon EC2 執行個體
- 透過 VPC 對等之 VPC 連線內的 EC2 執行個體
- 使用內部部署伺服器 AWS Direct Connect
- 透過 AWS 虛擬私人網路 (VPN) 使用 Amazon VPC 的現場部署伺服器

VPC 互連連線是指兩個 VPC 之間的聯網連線，透過此機制，您可以在兩者間路由流量。連線可以使用網際網路通訊協定第 4 版 (IPv4) 或網際網路通訊協定第 6 版 (IPv6) 地址。如需關於 Amazon EFS 如何搭配 VPC 對等一起使用的詳細資訊，請參閱 從另一個 AWS 帳戶 或 VPC 掛載 EFS 檔案系統。

若要從另一個 VPC 的 EC2 執行個體中存取檔案系統，您必須執行以下操作：

- 刪除目前掛載目標。
- 變更 VPC。
- 建立新的掛載目標。

如需中執行這些步驟的詳細資訊 AWS Management Console，請參閱若要變更 Amazon EFS 檔案系統 (主控台) 的 VPC 擬私人雲端。

使用 CLI

若要使用另一個 VPC 中的檔案系統，請先刪除您先前在 VPC 中建立的任何掛載目標。然後在另一個 VPC 中建立新的掛載目標。如需 AWS CLI 命令的範例，請參閱管理掛載目標 (CLI)。

更新掛載目標組態

在您為檔案系統建立掛載目標後，可能需要更新生效的安全群組。您不能改變現有掛載目標的 IP 地址。若要變更 IP 地址，請刪除掛載目標並用新的地址建立新的掛載目標。刪除掛載目標會中斷任何現有的檔案系統掛載。

> **Note**
>
> 刪除掛載目標前，請先卸載檔案系統。

每個掛載目標都有一個 IP 地址。當您建立掛載目標時，您可以從子網路選擇您將掛載目標的 IP 地址。如果您省略了值，Amazon EFS 會從該子網路選擇一個未使用的 IP 地址。

沒有任何 Amazon EFS 操作可在建立掛載目標之後變更 IP 地址。因此，您無法以程式設計方式或使用 AWS CLI來變更 IP 地址。但是，主控台可讓您變更的 IP 地址。在幕後，主控台會刪除掛載目標並再次建立掛載目標。

> **Warning**
>
> 如果您變更掛載目標的 IP 地址，將損壞所有現有的檔案系統掛載，而且必須重新掛載該檔案系統。

任何檔案系統網路存取權限的組態變更，都不會影響檔案系統本身。您的檔案系統和資料都將保留為未變更。

修改安全群組

安全群組會定義傳入和傳出存取。當您變更與掛載目標相關聯的安全群組時，請確保您授予必要的傳入和傳出存取權限。這樣做可讓您的 EC2 執行個體與檔案系統通訊。

如需有關安全群組的詳細資訊，請參閱 Amazon EC2 使用者指南中的適用於 Linux 執行個體的 Amazon EC2 安全群組。

若要修改裝載目標的安全性群組，請參閱管理掛載目標。

管理檔案系統輸送量

Elastic 是預設輸送量模式，建議在大多數使用案例中使用。使用彈性輸送量后，效能會縱向擴展或縮小以滿足工作負載活動的需求。但是，如果您知道工作負載 (包括輸送量、延遲和儲存需求) 的特定存取模式，則可以選擇變更輸送量模式。

您可以選擇的其他輸送量模式包括：

- 佈建輸送量：您可以指定檔案系統可以驅動的輸送量層級，而不受檔案系統的大小或爆量額度餘額影響。
- 爆量輸送量：輸送量會隨檔案系統中的儲存容量進行擴展，並支援爆增至更高層級，而且每天爆增時間長達 12 小時。

如需 Amazon EFS 輸送量模式的詳細資訊，請參閱輸送量模式。

> **Note**
>
> 您可以在檔案系統可用之後，變更輸送量模式和佈建輸送量總量。但是，每當您將檔案系統變更為佈建輸送量或增加佈建輸送量總量時，必須等待至少 24 小時，才能再次變更輸送量模式或減少佈建數量。

您可以使用 Amazon EFS 主控台、 AWS Command Line Interface (AWS CLI) 和 Amazon EFS API 來管理檔案系統輸送量模式。

管理檔案系統輸送量 (主控台)

1. 開啟 Amazon Elastic File System 主控台，網址為 https://console.aws.amazon.com/efs/。
2. 在左側導覽窗格中，選擇檔案系統以顯示帳戶中的 EFS 檔案系統清單。
3. 選擇您要變更輸送量模式的檔案系統。
4. 在檔案系統詳細資訊頁面的一般區段中，選擇編輯。屏幕將顯示編輯頁面。
5. 修改輸送量模式設定。

   - 若要使用彈性輸送量或佈建輸送量，請選擇增強，然後選擇彈性或佈建。

     如果您選擇已佈建，則在佈建輸送量 (MIB/s) 中，輸入要佈建檔案系統要求的輸送量量。「最大讀取輸送量」的顯示量是您輸入輸送量的三倍。EFS 檔案系統讀取請求速率是其他請求速率的三分之一。輸入輸送量後，系統會顯示檔案系統每月成本的估計值。

     > **Note**
     >
     > 您可以在檔案系統可用之後，變更輸送量模式和佈建輸送量總量。但是，每當您將檔案系統輸送量變更為已佈建或增加佈建的輸送量時，您必須等待至少 24 小時，才能再次變更輸送量模式或減少佈建的數量。

   - 若要使用爆量輸送量，請選擇爆量。

如需為效能需求選擇正確輸送量模式的更多資訊，請參閱 輸送量模式。

6. 請選擇儲存變更實作變更。

管理檔案系統輸送量 (CLI)

- 使用 update-file-systemCLI 命令或 UpdateFileSystem API 動作來變更檔案系統的輸送量模式。

管理檔案系統儲存

若要管理檔案系統，以便在整個生命週期中以符合成本效益的方式儲存檔案系統，使用生命週期管理會根據為檔案系統定義的生命週期組態，在儲存類別之間自動轉換 生命週期組態是一組生命週期政策，用於定義將檔案系統資料轉移到其他儲存類別的時間。

生命週期政策

生命週期原則會指示生命週期管理何時將檔案轉入和移出 EFS 不常存取 (IA) 和 EFS 封存儲存類別。轉移時間取決於上次在標準儲存類別中存取檔案的時間。生命週期政策適用於整個 EFS 檔案系統。

EFS 生命週期政策包括：

- 轉換為 IA — 指示生命週期管理何時將檔案移入不常存取儲存體，這是針對每季僅存取幾次資料的成本最佳化。依預設，30 天內未存取在標準儲存中的檔案會轉移動至 IA 中。
- 轉換至封存 — 指示生命週期管理何時將檔案移入封存儲存類別，此類別針對每年僅存取幾次或更少的資料進行了成本最佳化。依預設，90 天內未存取在標準儲存中的檔案會轉移動至「封存」中。
- 轉換為標準 — 指示生命週期管理是否要將檔案從 IA 或封存轉換回標準儲存，以便為頻繁存取的資料提供低於一毫秒的讀取延遲。依預設，檔案不會移回標準儲存，而且會保留在 IA 或「封存」儲存類別中。對於需要最快延遲效能 (例如處理大量小型檔案的應用程式) 的效能敏感性使用案例，請選擇將檔案轉移至標準儲存的首次存取中。

若要關於設定檔案系統生命週期政策的詳細資訊，請參閱 管理檔案系統的生命週期政策。

若要判斷上次在標準儲存類別中的存取時間，內部計時器會追蹤上次存取檔案的時間 (而不是通過非可公開檢視的 POSIX 檔案系統屬性來實現)。每當存取「標準」中的檔案時，就會重設生命週期管理計時器。生命週期管理將檔案移至 IA 或封存儲存類別之後，除非設定了「轉換成標準」原則，否則檔案會無限期保留在該原則中，這會指示生命週期管理在存取時將檔案移回「標準」。

中繼資料操作 (例如列出目錄內容) 不計入檔案存取。將檔案內容轉移至 IA 或「封存」儲存類別過程期間，檔案儲存在標準儲存類別中，並依據儲存費率計費。

生命週期管理的檔案系統操作

與 EFS 檔案系統工作負載操作相比，生命週期管理的檔案系統操作的優先級較低。將檔案轉進或轉出 IA 和「封存」儲存類別所需的時間，依據檔案大小和檔案系統工作負載而有所不同。

包括檔案名稱、擁有權資訊和檔案系統目錄結構等檔案中繼資料，一律存放在標準儲存，以確保中繼資料效能一致。在檔案系統的 IA 或「封存」儲存類別中，檔案的所有寫入操作都會先寫入標準儲存類別，然後可在 24 小時後轉移至適用的儲存類別。

管理檔案系統的生命週期政策

使用建立使用服務建議設定的 Amazon EFS 檔案系統時 AWS Management Console，檔案系統的生命週期政策會使用下列預設設定：

- 轉移至 IA 設定為自上次存取后 30 天。
- 轉移至封存設定為自上次存取后 90 天。
- 轉移至標準設定為無。

如需關於使用服務建議設定建立檔案系統的詳細資訊，請參閱 快速建立具有建議設定的檔案系統 (主控台)。

您可以在建立檔案系統之後或使用自訂設定建立檔案系統時，設定生命週期政策。

轉移至 IA 和轉移至封存生命週期政策的可能值包括：

- 無
- 自上次存取後 1 天
- 自上次存取後 7 天
- 自上次存取後 14 天
- 自上次存取後 30 天
- 自上次存取後 60 天
- 自上次存取後 90 天
- 自上次存取後 180 天
- 自上次存取後 270 天

- 自上次存取後 365 天

轉移至標準生命週期政策的可能值包括：

- 無
- 首次存取

您可以使用 AWS Management Console 和來設定生命週期原則 AWS CLI，如下列程序所述。

在現有檔案系統 (主控台) 上管理生命週期政策

您可以使用設 AWS Management Console 定現有檔案系統的生命週期原則。

1. 登入 AWS Management Console 並開啟 Amazon EFS 主控台，網址為 https://console.aws.amazon.com/efs/。
2. 選擇檔案系統以顯示帳戶中的檔案系統清單。
3. 選擇您要修改生命週期政策的檔案系統。
4. 在檔案系統詳細資訊頁面的一般區段中，選擇編輯。屏幕將顯示編輯頁面。
5. 對於生命週期管理，您可以變更下列生命週期政策：
   - 轉移至 IA 設定為其中一種可用的設定。若要停止將檔案移入 IA 儲存，請選擇無。
   - 轉移至封存設定為其中一種可用的設定。若要停止將檔案移入「封存」儲存，請選擇無。
   - 轉移至標準設定為首次存取，以便進行非中繼資料存取時，將 IA 儲存中的檔案移至標準儲存中。

     若要在第一次存取時停止將檔案從 IA 或「封存」儲存移至標準儲存，請設定為無。
6. 選擇儲存變更，以儲存您所做的變更。

在現有檔案系統 (CLI) 上管理生命週期政策

您可以使用設 AWS CLI 定或修改檔案系統的生命週期原則。

- 執行put-lifecycle-configuration AWS CLI 命令或 PutLifecycleConfiguration API 命令，指定您要管理其生命週期管理之檔案系統的檔案系統 ID。

```
$  aws efs put-lifecycle-configuration \
--file-system-id File-System-ID \
```

```
--lifecycle-policies "[{\"TransitionToIA\":\"AFTER_60_DAYS\"},
{\"TransitionToPrimaryStorageClass\":\"AFTER_1_ACCESS\"},{\"TransitionToArchive\":
\"AFTER_90_DAYS\"}]" \
--region us-west-2 \
--profile adminuser
```

您會收到以下回應。

```
{
    "LifecyclePolicies": [
        {
            "TransitionToIA": "AFTER_60_DAYS"
        },
        {
            "TransitionToPrimaryStorageClass": "AFTER_1_ACCESS"
        },
        {
            "TransitionToArchive": "AFTER_90_DAYS"
        }
    ]
}
```

停止現有檔案系統的生命週期管理 (CLI)

- 執行 `put-lifecycle-configuration` 命令，以指定您要停止生命週期管理之檔案系統的系統 ID。保持 `--lifecycle-policies` 屬性空白。

```
$  aws efs put-lifecycle-configuration \
--file-system-id File-System-ID \
--lifecycle-policies \
--region us-west-2 \
--profile adminuser
```

您會收到以下回應。

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

管理加密檔案系統的存取權

透過 Amazon EFS，您可以建立加密檔案系統。Amazon EFS 支援兩種形式的檔案系統加密、傳輸中加密和靜態加密。您需要執行的任何金鑰管理僅與靜態加密有關。Amazon EFS 將自動在傳輸中為您管理加密金鑰。

如果您建立了使用靜態加密的檔案系統，則資料和中繼資料都會使用靜態加密。Amazon EFS 使用 AWS Key Management Service (AWS KMS) 進行金鑰管理。當您使用靜態加密建立檔案系統時，指定 AWS KMS key。KMS 金鑰可以是 `aws/elasticfilesystem` (AWS 受管金鑰 適用於 Amazon EFS)，也可以是您管理的客戶受管金鑰。

檔案資料 (檔案內容) 是使用您在建立檔案系統時指定的 KMS 金鑰進行靜態加密。中繼資料 (檔案名稱、目錄名稱和目錄內容) 是由 Amazon EFS 管理的金鑰進行加密。

檔案系統 AWS 受管金鑰 的 EFS 用作 KMS 金鑰，用來加密檔案系統中的中繼資料，例如檔案名稱、目錄名稱和目錄內容。您擁有用於靜態加密檔案資料 (檔案的內容) 的用戶管理金鑰。

您可以管理存取您的 KMS 金鑰以及加密檔案系統內容的人選。此存取權由 AWS Identity and Access Management (IAM) 政策和 AWS KMS. IAM 政策可控制使用者存取 Amazon EFS API 動作的權限。AWS KMS 金鑰原則會控制使用者存取您在建立檔案系統時指定的 KMS 金鑰。如需詳細資訊，請參閱下列內容：

- 《IAM 使用者指南》中的 IAM 使用者
- 《AWS Key Management Service 開發人員指南》中的在 AWS KMS中使用金鑰政策
- 《AWS Key Management Service 開發人員指南》中的使用授予。

身為金鑰管理員，您可以匯入外部金鑰。您也可以透過啟用、停用或刪除來修改金鑰。您指定的 KMS 金鑰狀態 (當您使用靜態加密建立檔案系統時) 會影響對其內容的存取權。KMS 金鑰必須`enabled`處於狀態，使用者才能存取使用該金鑰加密的 encrypted-at-rest 檔案系統內容。

在 Amazon EFS KMS 金鑰上執行管理動作

之後，您可以尋找如何啟用、停用或刪除與 Amazon EFS 檔案系統相關聯的 KMS 金鑰。您也可以在執行這些動作時從檔案系統了解預期的行為。

管理檔案系統 KMS 金鑰的存取權

您可以停用或刪除用戶自訂受管的 KMS 金鑰，或者您可以撤銷 Amazon EFS 對 KMS 金鑰的存取。停用和撤銷 Amazon EFS 對您金鑰的存取權是可還原的動作。練習刪除 KMS 金鑰時請格外小心。刪除 KMS 金鑰是不可復原的動作。

如果您停用或刪除已掛載檔案系統的 KMS 金鑰，則下列事項屬實：

- 該 KMS 金鑰無法用作新 encrypted-at-rest 檔案系統的金鑰。
- 使用該 KMS 金鑰的現有 encrypted-at-rest 檔案系統會在一段時間後停止運作。

如果您對任何現有掛載的檔案系統撤銷 Amazon EFS 存取，該行為與停用或刪除關聯的 KMS 金鑰無異。換句話說， encrypted-at-rest 檔案系統會繼續運作，但會在一段時間後停止工作。

您可以防止存取具有已停用、刪除或撤銷 Amazon EFS 存取權的 KMS 金鑰的已掛載 encrypted-at-rest 檔案系統。若要這樣做，請卸載該檔案系統並刪除您的 Amazon EFS 掛載目標。

您無法立即刪除 AWS KMS key，但您可以排程在 7-30 天內刪除它。在排定刪除 KMS 金鑰期間，您不能使用該 KMS 金鑰進行加密操作。您也可以取消排定的 KMS 金鑰刪除。

若要了解如何停用和重新啟用客戶受管 KMS 金鑰，請參閱《 AWS Key Management Service 開發人員指南》中的啟用和停用金鑰。若要了解如何排程刪除客戶受管 KMS 金鑰，請參閱《 AWS Key Management Service 開發人員指南中》的刪除 KMS 金鑰。

計量：Amazon EFS 如何報告檔案系統和物件大小

以下各節說明 Amazon EFS 如何報告檔案系統內物件的檔案系統大小和大小。

計量 Amazon EFS 檔案系統物件

在 Amazon EFS 系統中，您可看見的物件包含一般檔案、目錄、符號連結和特殊檔案 (FIFO 和通訊端)。這些物件中的每一個都被計量為 2 kibibyte (KiB) 的中繼資料 (對其自己的 inode) 和一或多個 4 KiB 資料的增量。以下清單說明適用於不同類型檔案系統物件的計量資料大小：

- 一般檔案：一般檔案的計量資料大小是檔案的邏輯大小，四捨五入到下一個 4 KiB 遞增，只是它可能會低於稀疏檔案。

  稀疏檔案是一種在達到其邏輯大小之前，不會將資料寫入檔案所有位置的檔案。對於稀疏檔案，在某些情況下實際使用的儲存量少於四捨五入到下一個 4 KiB 遞增的邏輯大小。在這些情況下，Amazon EFS 會報告實際使用的儲存量做為計量的資料大小。

- 目錄：目錄的計量資料大小是用於目錄項目與存放該目錄項目資料結構的實際儲存量，會四捨五入到下一個 4 KiB 遞增。計量資料大小不包含檔案資料所使用的實際儲存量。
- 符號連結和特殊檔案 – 這些物件的計量資料大小一律為 4 KiB。

當 Amazon EFS 報告物件佔用的空間時，透過 NFSv4.1 space_used 屬性，它將包括該物件目前的計量資料大小，但不包括其中繼資料的大小。您可以使用兩種公用程式來計量檔案的磁碟使用量，即 du 和 stat 公用程式。以下是如何在空文件中使用該du實用程序，其中包括返回以千字節為單位的輸出的-k選項的示例。

```
$ du -k file
4       file
```

下面的例子演示了如何在一個空文件中使用該stat實用程序返回文件的磁盤使用情況。

```
$ /usr/bin/stat --format="%b*%B" file | bc
4096
```

若要計量目錄的大小，請使用 stat 公用程式。找出 Blocks 值，然後將該值乘以區塊大小。下面範例是泛如何在空白目錄上使用 stat 公用程式：

```
$ /usr/bin/stat --format="%b*%B" . | bc
4096
```

Amazon EFS 檔案系統的計量大小

Amazon EFS 檔案系統的計量大小包括所有 EFS 儲存類別中所有目前物件的大小總和。每個物件的大小是根據計量期間 (以小時為單位，例如從上午 8:00 至上午 9:00)，代表該物件大小的代表性抽樣而計算。

空白檔案佔用了其檔案系統計量大小的 6 KiB (2 KiB 中繼資料 + 4 KiB 資料)。檔案系統在建立時都擁有單一的空白根目錄，因此有 6 KiB 的計量大小。

特定檔案系統的計量大小，定義了該小時中的擁有者帳戶因檔案系統計費的使用量。

> **Note**
>
> 在該小時內的任何特定時間中，計算的計量大小並不代表檔案系統一致的快照。相反地，它代表在每小時內的不同時間點，存在於檔案系統的物件大小；或可能代表不同時間前的小時數。

這些大小將會加總，以決定該小時的檔案系統計量大小。因此，當檔案系統沒有進行寫入時，檔案系統大小的計量大小最終將與儲存的物件計量大小一致。

您可以透過下列方式查看 Amazon EFS 檔案系統的計量大小：

- 使用命describe-file-systems AWS CLI 令和 DescribeFileSystemAPI 操作，響應包括以下內容：

```
"SizeInBytes":{
            "Timestamp": 1403301078,
            "Value": 29313744866,
            "ValueInIA": 675432,
            "ValueInStandard": 29312741784
            "ValueInArchive": 327650
        }
```

  其中的ValueInStandard計量大小也可用於判斷使用大量批量輸送量模式之檔案系統的 I/O 輸送量基準和成組分解率。
- 檢視StorageBytes CloudWatch 測量結果，此測量結果會顯示每個儲存體類別中的總計量資料大小。如需關於 StorageBytes 指標的詳細資訊，請參閱Amazon EFS 的 Amazon CloudWatch 指標。
- 在 Linux 中，在 EC2 執行個體終端提示上執行 df 命令。

  請勿將檔案系統根目錄上的du命令用於儲存計量，因為回應不會反映用於計量檔案系統的完整資料。

> **Note**
>
> ValueInStandard 的計量大小也可用來判斷您的 I/O 輸送量基準和爆量率。如需詳細資訊，請參閱 爆量吞吐量。

計量不常存取和封存儲存類別

EFS 不常存取 (IA) 和封存儲存類別以 4 KiB 增量計費，每個檔案的最低帳單費用為 128 KiB。IA 和封存檔案中繼資料 (每個檔案 2 KiB) 一律會儲存並計量在標準儲存類別中。只有在太平洋時間 2023 年 11 月 26 日中午 12:00 或之後更新的生命週期原則，才能 Support 援小於 128 KiB 的檔案。IA 和歸檔儲存的資料存取以 128 KiB 增量計費。

您可以使用指StorageBytes CloudWatch 標來檢視每個儲存體類別中的計量資料大小。此測量結果也會顯示在 IA 和「存檔」儲存體類別中捨入小型檔案所使用的位元組總數。如需檢視 CloudWatch 測量結果的詳細資訊，請參閱存取 CloudWatch 量度。如需關於 StorageBytes 指標的詳細資訊，請參閱Amazon EFS 的 Amazon CloudWatch 指標。

計量輸送量

Amazon EFS 對讀取請求輸送量的計量速率是其他檔案系統 I/O 操作的三分之一。例如，如果您要驅動每秒 30 MB (MiBps) 的讀取和寫入輸送量，則讀取部分會計為有效輸送量 MiBps 的 10，寫入部分計為 30 MiBps，而合併的計量輸送量為 40。 MiBps針對消耗率調整的組合輸送量會反映在MeteredIOBytes CloudWatch 量度中。

計量彈性吞吐量

為檔案系統啟用彈性輸送量模式時，您只需為從檔案系統讀取或寫入的中繼資料和資料量付費。Amazon EFS 檔案系統使用彈性輸送量模式計量器和帳單中繼資料讀取作為讀取操作，中繼資料寫入為寫入操作。中繼資料作業以 4 KiB 的增量計量，而資料作業則以 32 KiB 的增量計量。

計量佈建輸送量

對於使用佈建輸送量模式的檔案系統，您只需支付啟用輸送量的時間量。Amazon EFS 會計量每小時啟用一次佈建輸送量模式的檔案系統。對於佈建輸送量模式設定少於一小時時的計量，Amazon EFS 會使用毫秒精確度計算平均時間。

使用 AWS 預算管理 Amazon EFS 檔案系統成本

您可以使用 AWS 預算來規劃和管理 Amazon EFS 檔案系統成本。

您可以從 AWS Billing and Cost Management 主控台使用 AWS 預算。若要使用 AWS 預算，請為 EFS 檔案系統建立每月成本預算。您可以設定將預算設為當預測成本超過預算金額時通知您，然後視需要進行調整，以維持預算。

有與使用 AWS 預算相關的成本。對於常規 AWS 帳戶，您的前兩個預算是免費的。如需有關 AWS 預算 (包括成本) 的詳細資訊，請參閱《AWS Billing 使用指南》中的「使用預算管理成本」。

您可以使用預算參數，在帳戶、 AWS 區域服務或標籤層級設定 Amazon EFS 成本和用量的自訂預算。在下一節中，您可以找到如何在具有預算的 EFS 檔案系統上設定成本 AWS 預算的詳細說明。您可以使用成本分配標籤來執行此操作。

必要條件

若要執行下列各節中參考的程序，請確定您具備下列項目：

- EFS 檔案系統
- 具有下列許可的 AWS Identity and Access Management (IAM) 政策：
  - 存取主 AWS Billing and Cost Management 控台。
  - 執行 `elasticfilesystem:CreateTags` 和 `elasticfilesystem:DescribeTags` 動作的能力。

建立 EFS 檔案系統的每月成本預算

使用標籤為您的 Amazon EFS 檔案系統建立每月成本預算，需要三個步驟。

使用標籤為 EFS 檔案系統建立每月成本預算

1. 建立標籤以用來識別您要追蹤成本的檔案系統。如要瞭解如何作業，請參閱標記 Amazon EFS 資源。
2. 在「帳單與成本管理」主控台，將標籤激活為成本分配標籤。如需詳細資訊，請參閱《AWS Billing 使用者指南》中的啟用使用者定義的成本分配標籤。
3. 在 [Billing and Cost Management] 主控台的 [預算] 底下，在 [預算] 中建立每月成本 AWS 預算。如需詳細程序，請參閱《AWS Billing 使用者指南》中的建立成本預算。

建立 EFS 每月成本預算之後，您可以在 Budgets (預算) 儀表板中檢視該預算，其顯示以下預算資料：

- 預算期間該預算目前產生的成本與用量。
- 預算期間的預算成本。
- 預算期間的預測成本。
- 顯示相較於預算金額的成本，以百分比顯示。
- 顯示相較於預算金額的預測成本，以百分比顯示。

如需關於檢視 EFS 成本預算的詳細資訊，請參閱《AWS Billing 使用者指南》中的檢視預算。

檔案系統狀態

您可以使用 Amazon EFS 主控台或 AWS CLI來檢視 Amazon EFS 檔案系統狀態。Amazon EFS 檔案系統可以具有下列資料表所述的其中一個狀態值。

檔案系統狀態	描述
AVAILABLE	檔案系統狀態良好，可存取和使用。
CREATING	Amazon EFS 正在建立新檔案系統。
DELETING	Amazon EFS 正在刪除檔案系統以回應使用者啟動的刪除請求。如需詳細資訊，請參閱 刪除 Amazon EFS 檔案系統。
DELETED	Amazon EFS 已刪除檔案系統以回應使用者啟動的刪除請求。如需詳細資訊，請參閱 刪除 Amazon EFS 檔案系統。
UPDATING	檔案系統正在更新，以回應使用者啟動的更新要求。
ERROR	適用於單區域檔案系統，包括複寫組態中的檔案系統。 檔案系統出故障且無法復原。若要存取檔案系統資料，請將此檔案系統的備份還原至新檔案系統中。如需詳細資訊，請參閱： • 還原復原點. • EFS 儲存類別 • 複寫檔案系統

監控 Amazon EFS

監控是維護 Amazon EFS 和 AWS 解決方案的可靠性、可用性和效能的重要組成部分。我們建議您從 AWS 解決方案的所有部分收集監控資料，以便在發生多點故障時更輕鬆地對多點失敗進行偵錯。不過，在您開始監控 Amazon EFS 之前，應先建立監控計畫，為下列問題提供解答：

- 監控目標是什麼？
- 要監控哪些資源？
- 監控這些資源的頻率為何？
- 要使用哪些監控工具？
- 誰將執行監控任務？
- 發生問題時應該通知誰？

下一步是在各個時間點和不同的負載條件下測量效能，以在您的環境中確立 Amazon EFS 正常效能的基準。當您監控 Amazon EFS 時，請考慮存放歷史監控資料。這個儲存的資料會提供基準，讓您可與目前的效能資料比較，以識別出正常的效能模式和效能異常狀況，再規劃方法來處理問題。

例如，使用 Amazon EFS，您可以監控網路輸送量、讀取、寫入及中繼資料操作的 I/O、用戶端連線，以及檔案系統的爆量額度餘額。若效能不符合您所建立的基準，您可能需要變更檔案系統的大小或連接用戶端的數量，以便針對工作負載將檔案系統最佳化。

若要建立基準，您至少必須監控下列項目：

- 您檔案系統的網路傳輸量。
- 檔案系統的用戶端連線數量。
- 每個檔案系統操作的位元組數，包括資料讀取、資料寫入及中繼資料操作。

主題

監控工具

AWS 提供各種可用來監控 Amazon EFS 的工具。您可以設定其中一些工具來進行監控，但有些工具需要手動介入。建議您盡可能自動化監控任務。

自動化監控工具

您可以使用下列自動化監控工具來監看 Amazon EFS，並在發生錯誤時進行回報：

- Amazon A CloudWatch lar ps — 觀看您指定期間內的單一指標，並根據指定臨界值在多個時段內相對於指定閾值的指標值執行一或多個動作。動作是傳送至亞馬遜簡單通知服務 (Amazon SNS) 主題或 Amazon EC2 Auto Scaling 政策的通知。 CloudWatch 警示不會僅因為處於特定狀態而叫用動作；狀態必須已變更並維持指定數目的期間。如需詳細資訊，請參閱 使用 Amazon 監控 Amazon EFS 指 CloudWatch。
- Amazon CloudWatch 日誌 — 監控、存放和存取來自 AWS CloudTrail 或其他來源的日誌檔。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南中的監控日誌檔。
- Amazon E CloudWatch vents — 匹配事件並將其路由到一個或多個目標函數或串流，以進行變更、擷取狀態資訊並採取糾正措施。有關更多信息，請參閱 Amazon 用 CloudWatch 戶指南中的 Amazon CloudWatch 事件是什麼。
- AWS CloudTrail 記錄監控 — 在帳戶之間共用記錄檔、即時監控記 CloudTrail 錄檔案，方法是將記錄檔傳送至 CloudWatch 記錄檔、使用 Java 撰寫記錄處理應用程式，以及驗證您的記錄檔在傳送之後未變更 CloudTrail。若要取得更多資訊，請參閱《使用指南》中的〈AWS CloudTrail 使用 CloudTrail 記錄檔〉。

手動監控工具

監控 Amazon EFS 的另一個重要部分是手動監控 Amazon CloudWatch 警示未涵蓋的項目。Amazon EFS 和其他 AWS Management Console 儀表板可提供您 AWS 環境狀態的 at-a-glance 檢視。CloudWatch建議您也查看檔案系統上的日誌檔。

- 從 Amazon EFS 主控台中，您可以找到檔案系統的下列項目：
  - 目前的計量大小
  - 掛載目標的數量
  - 生命週期狀態
- CloudWatch 主頁顯示：

- 目前警示與狀態
- 警示與資源的圖表
- 服務運作狀態

此外，您可以使用執行 CloudWatch 以下操作：

- 請建立自訂儀表板來監控您使用的服務。
- 用於疑難排解問題以及探索驅勢的圖形指標資料。
- 搜尋並瀏覽所有資 AWS 源指標。
- 建立與編輯要通知發生問題的警示。

使用 Amazon 監控 Amazon EFS 指 CloudWatch

您可以使用 Amazon 監控檔案系統 CloudWatch，Amazon 將來自 Amazon EFS 的原始資料收集並處理為可讀且接近即時的指標。這些統計資料會記錄 15 個月的時間，以便您更清楚 Web 應用程式或服務的執行效能。

預設情況下，Amazon EFS 指標資料會 CloudWatch 在 1 分鐘的時間內自動傳送到，除非某些個別指標有註明。Amazon EFS 主控台會根據來自 Amazon 的原始資料顯示一系列圖形 CloudWatch。視您的需求而定，您可能希望從主控台取得檔案系統的資料， CloudWatch 而不是從主控台取得圖形。

有關 Amazon 的更多信息 CloudWatch，請參閱 Amazon CloudWatch 用戶指南。

Amazon EFS CloudWatch 指標報告為原始位元組。位元組不會捨入到單位的十進位或二進位倍數。

Amazon EFS 的 Amazon CloudWatch 指標

Amazon EFS 指標使用 `EFS` 命名空間，並為單一維度、`FileSystemId` 提供指標。在 Amazon EFS 主控台個找到檔案系統的 ID，其格式為 `fs-abcdef0123456789a`。

`AWS/EFS` 命名空間包含下列指標。

`TimeSinceLastSync`

顯示自上次成功同步至複寫組態中目的地檔案系統之後所經過的時間總量。`TimeSinceLastSync` 值發生之前，對來源檔案系統上的資料所做的任何變更都已經成功複寫。系統可能無法在來源上完全複寫發生與 `TimeSinceLastSync` 之後的任何變更。

單位：秒

有效統計資訊：Minimum、Maximum、Average

PercentIOLimit

顯示檔案系統有多接近一般用途效能模式的 I/O 限制。

單位：百分比

有效統計資訊：Minimum、Maximum、Average

BurstCreditBalance

檔案系統擁有的叢發額度。叢發額度可讓檔案系統將輸送量大幅提升至超過基準水準一段時間。

Minimum 統計資訊是一段期間內任何一分鐘的最小叢發額度餘額。Maximum 統計資訊是一段期間內任何一分鐘的最大叢發額度餘額。Average 統計資訊是一段期間內的平均叢發額度餘額。

單位：位元組

有效統計資訊：Minimum、Maximum、Average

PermittedThroughput

檔案系統可以驅動的最大輸送量。

- 對於使用彈性輸送量的檔案系統，此值會反映檔案系統的最大寫入輸送量。
- 對於使用佈建輸送量的檔案系統，如果 EFS Standard 儲存類別中儲存的資料量允許您的檔案系統驅動比佈建更高的輸送量，則此量度會反映更高的輸送量，而不是佈建的數量。
- 對於處於大量批次輸送量模式的檔案系統，此值是檔案系統大小和BurstCreditBalance的函數。

Minimum 統計資訊是一段期間內任何一分鐘允許的最小輸送量。Maximum 統計資訊是一段期間內任何一分鐘允許的最高輸送量。Average 統計資訊是一段期間內允許的平均輸送量。

> **Note**
>
> 讀取操作的計量速率是其他操作速率的三分之一。

單位：位元組/秒

有效統計資訊：Minimum、Maximum、Average

MeteredIOBytes

計算每個檔案系統操作 (包括資料讀取、資料寫入和中繼資料操作) 的位元組數時，讀取操作的的計量速率是其他操作速率的三分之一。

您可以建立與之比較的CloudWatch 度量數學運算MeteredIOBytes式PermittedThroughput。如果這些值相等，表示您正在消耗配置給檔案系統的整個輸送量總量。在此情況下，您可能會考慮變更檔案系統的輸送量模式，以取得更多輸送量。

Sum 統計資訊是與所有檔案系統操作相關的計量位元組總數。Minimum 統計資訊是一段期間內最小操作的大小。Maximum 統計資訊是一段期間內最大操作的大小。Average 統計資訊是一段期間內操作的平均大小。SampleCount 統計資訊提供所有操作的計數。

單位：

- Minimum、Maximum、Average 及 Sum 統計資訊的位元組數。
- SampleCount 的計數。

有效的統計資訊：Minimum、Maximum、Average、Sum、SampleCount

TotalIOBytes

每個檔案系統操作的實際位元組數，包括資料讀取、資料寫入及中繼資料操作。這是應用程式驅動的實際數量，而非正在計算的檔案系統輸送量。該數量可能高於 PermittedThroughput 中顯示的數字。

Sum 統計資訊是與所有檔案系統操作相關的位元組總數。Minimum 統計資訊是一段期間內最小操作的大小。Maximum 統計資訊是一段期間內最大操作的大小。Average 統計資訊是一段期間內操作的平均大小。SampleCount 統計資訊提供所有操作的計數。

> **Note**
>
> 若要計算一段期間的每秒平均操作，請將 SampleCount 統計資訊除以該期間的秒數。若要計算一段期間的平均輸送量 (每秒位元組數)，請將 Sum 統計資訊除以該期間的秒數。

單位：

- Minimum、Maximum、Average 及 Sum 統計資訊的位元組數。
- SampleCount 的計數。

有效的統計資訊：Minimum、Maximum、Average、Sum、SampleCount

DataReadIOBytes

每個檔案系統讀取作業的實際位元組數。

Sum 統計資訊是與讀取操作相關的位元組總數。Minimum 統計資訊是一段期間內最小讀取操作的大小。Maximum 統計資訊是一段期間內最大讀取操作的大小。Average 統計資訊是一段期間內讀取操作的平均大小。SampleCount 統計資訊提供讀取操作的計數。

單位：

- Minimum、Maximum、Average 及 Sum 的位元組數。
- SampleCount 的計數。

有效的統計資訊：Minimum、Maximum、Average、Sum、SampleCount

DataWriteIOBytes

每個檔案系統寫入作業的實際位元組數。

Sum 統計資訊是與寫入操作相關的位元組總數。Minimum 統計資訊是一段期間內最小寫入操作的大小。Maximum 統計資訊是一段期間內最大寫入操作的大小。Average 統計資訊是一段期間內寫入操作的平均大小。SampleCount 統計資訊提供寫入操作的計數。

單位：

- 位元組是 Minimum、Maximum、Average 及 Sum 統計資訊的單位。
- SampleCount 的計數。

有效的統計資訊：Minimum、Maximum、Average、Sum、SampleCount

MetadataIOBytes

每個中繼資料作業的實際位元組數。

Sum 統計資訊是與中繼資料操作相關的位元組總數。Minimum 統計資訊是一段期間內最小中繼資料操作的大小。Maximum 統計資訊是一段期間內最大中繼資料操作的大小。Average 統計資訊是一段期間內平均中繼資料操作的大小。SampleCount 統計資訊提供中繼資料操作的計數。

單位：

- 位元組是 Minimum、Maximum、Average 及 Sum 統計資訊的單位。
- SampleCount 的計數。

有效的統計資訊：Minimum、Maximum、Average、Sum、SampleCount

MetadataReadIOBytes

每個中繼資料讀取作業的實際位元組數。

Sum統計資料是與中繼資料讀取作業相關聯的位元組總數。Minimum統計資料是期間內最小中繼資料讀取作業的大小。Maximum統計資料是期間內最大的中繼資料讀取作業的大小。Average統計資料是期間內中繼資料讀取作業的平均大小。SampleCount統計資料提供中繼資料讀取作業的計數。

單位：

- 位元組是 Minimum、Maximum、Average 及 Sum 統計資訊的單位。
- SampleCount 的計數。

有效的統計資訊：Minimum、Maximum、Average、Sum、SampleCount

MetadataWriteIOBytes

每個中繼資料寫入作業的實際位元組數。

Sum統計資料是與中繼資料寫入作業相關聯的位元組總數。Minimum統計資料是期間內最小中繼資料寫入作業的大小。Maximum統計資料是期間內最大的中繼資料寫入作業的大小。Average統計資料是期間內中繼資料寫入作業的平均大小。SampleCount統計資料提供中繼資料寫入作業的計數。

單位：

- 位元組是 Minimum、Maximum、Average 及 Sum 統計資訊的單位。
- SampleCount 的計數。

有效的統計資訊：Minimum、Maximum、Average、Sum、SampleCount

ClientConnections

檔案系統的用戶端連線數量。使用標準用戶端時，每個已掛載的 Amazon EC2 執行個體皆有一個連線。

> **Note**
>
> 若要計算一分鐘以上期間的平均 ClientConnections，請將 Sum 統計資訊除以該期間的分鐘數。

單位：用戶端連線計數

有效的統計資訊：Sum

StorageBytes

檔案系統的大小 (以位元組為單位)，包括儲存在 EFS 儲存類別中的資料量。此量度會發射到 CloudWatch 每 15 分鐘一次。

StorageBytes量度具有以下維度：

- Total是所有儲存類別中儲存在檔案系統中資料的計量大小 (以位元組為單位)。對於 EFS 不常存取 (IA) 和 EFS 封存儲存體類別，小於 128KiB 的檔案會四捨五入為 128KiB。
- Standard是儲存在 EFS 標準儲存類別中之資料的計量大小 (位元組)。
- IA是 EFS 不常存取儲存類別中儲存的實際資料大小 (以位元組為單位)。
- IASizeOverhead是將小檔案捨入至 128KiB 之後，EFS 不常存取儲存類別 (在IA維度中指示) 中的實際資料大小與儲存類別的計量大小之間的差異 (以位元組為單位)。
- Archive是儲存在 EFS 封存儲存體類別中的實際資料大小 (以位元組為單位)。
- ArchiveSizeOverhead是將小檔案四捨五入至 128KiB 之後，EFS Archive 儲存類別中的實際資料大小 (以位Archive元組為單位) 與儲存類別的計量大小之間的差異 (以位元組為單位)。

單位：位元組

有效統計資訊：Minimum、Maximum、Average

> **Note**
>
> 透過使用以 1024 為基數的二進制單位 (KiB、MiB、GiB 和 TiB)，StorageBytes 顯示於 Amazon EFS 主控台檔案系統指標頁面上。

如何使用 Amazon EFS 指標？

Amazon EFS 回報的指標可提供資訊，您可透過不同方式加以分析。下列清單顯示一些常見的指標用途。這些是協助您開始的建議，而不是完整清單。

運作方式？	相關指標
如何判斷我的傳輸量？	您可以監控 Sum 指標的每日 TotalIOBytes 統計資料，查看您的傳輸量。

運作方式？	相關指標
如何追蹤連接至檔案系統的 Amazon EC2 執行個體數量？	您可以監控 Sum 指標的 ClientConnections 統計資料。若要計算一分鐘以上期間的平均 ClientConnections ，請將總和除以該期間的分鐘數。
如何查看我的叢發額度餘額？	您可以監控檔案系統的 BurstCreditBalance 指標來查看餘額。如需爆量和叢發額度的詳細資訊，請參閱 爆量吞吐量。

使用 CloudWatch 指標監視輸送量效能

輸送量監控的 CloudWatch 指標 (TotalIOBytesReadIOBytes、WriteIOBytes、和MetadataIOBytes) 代表您在檔案系統上推動的實際輸送量。此指標 MeteredIOBytes 計算了您正在驅動的整體計量輸送量。您可以使用 Amazon EFS 主控台監控區段中的輸送量使用率 (%) 圖表來監控輸送量使用率。如果您使用自訂 CloudWatch 儀表板或其他監視工具，則可以建立與之比較MeteredIOBytes的CloudWatch 度量數學運算式PermittedThroughput。

PermittedThroughput 衡量檔案系統允許的輸送量。此值基於以下列一種方法：

- 對於彈性輸送量中的檔案系統，此值會反映檔案系統的最大寫入輸送量。
- 對於使用佈建輸送量的檔案系統，如果 EFS Standard 儲存類別中儲存的資料量允許您的檔案系統驅動比佈建更高的輸送量，則此量度會反映更高的輸送量，而不是佈建的數量。
- 對於使用成組分解輸送量的檔案系統，此值是檔案系統大小和BurstCreditBalance的函數。監控 BurstCreditBalance 以確保您的檔案系統以爆增速率而非基本速率運作。如果餘額一致為零或接近零，請考慮切換至彈性輸送量或佈建輸送量以取得額外的輸送量。

當 MeteredIOBytes 和 PermittedThroughput 值相等時，您的檔案系統會耗用所有可用的輸送量。對於使用佈建輸送量的檔案系統，您可以佈建額外的輸送量。

使用 Amazon EFS 指標數學

使用度量數學，您可以查詢多個 CloudWatch 量度，並使用數學運算式根據這些量度建立新的時間序列。您可以在 CloudWatch 主控台中視覺化產生的時間序列，並將其新增至儀表板。例如，您可以使用 Amazon EFS 指標，將 DataRead 操作的取樣計數除以 60。結果便是指定 1 分鐘期間檔案系統的每秒讀取平均次數。如需有關度量數學的詳細資訊，請參閱 Amazon 使用 CloudWatch 者指南中的使用指標數學運算。

以下為一些實用的 Amazon EFS 指標數學運算式。

主題

公制數學：輸送量 MiBps

若要計算一段時間週期的平均輸送量 (in MiBps)，請先選擇總和統計值 (`DataReadIOBytes`、`DataWriteIOBytes`、`MetadataIOBytes`、或`TotalIOBytes`)。然後將該值轉換為 MiB，再除以該期間內的秒數。

假設您的範例邏輯如下：(`TotalIOBytes` 的總和 ÷ 1048576 (以轉換為 MiB)) ÷ 期間內的秒數

然後，您的 CloudWatch 指標信息如下。

ID	可用指標	統計數字	期間
m1	• `DataReadIOBytes` • `DataWriteIOBytes` • `MetadataIOBytes` • `TotalIOBytes`	sum	1 分鐘

您的指標數學 ID 和表達式如下。

ID	表達式
e1	(m1/1048576)/PERIOD(m1)

指標數學：輸送量百分比

此指標數學運算式會計算用於不同 I/O 類型的整體輸送量百分比，例如，由讀取請求驅動的總輸送量百分比。若要計算一段期間一種 I/O 類型 (DataReadIOBytes、DataWriteIOBytes 或 MetadataIOBytes) 使用的輸送量百分比，請先將個別總和統計數據乘以 100。然後將該結果除以同一期間的 TotalIOBytes 總和統計數據。

假設您的範例邏輯如下：(DataReadIOBytes 的總和 x 100 (以轉換為百分比)) ÷ TotalIOBytes 的總和

然後，您的 CloudWatch 指標信息如下。

ID	可用指標或多個指標	統計數字	期間
m1	• TotalIOBytes	sum	1 分鐘
m2	• DataReadIOBytes	sum	1 分鐘

您的指標數學 ID 和表達式如下。

ID	表達式
e1	(m2*100)/m1

指標數學：允許輸送使用的百分比率

若要計算一段期間內允許輸送量使用率的百分比 (MeteredIOBytes)，請先將輸送量乘以 100。MiBps然後將結果除以同一時期PermittedThroughput轉換為 MiB 的平均統計值。

假設您的範例邏輯是這樣的：(輸送量 MiBps x 100 (轉換為百分比) 的量度數學運算式) ÷ (PermittedThroughput÷ 1,048,576 的總和 (將位元組轉換為 MiB))

然後，您的 CloudWatch 指標信息如下。

ID	可用指標或多個指標	統計數字	期間
m1	`MeteredIOBytes`	sum	1 分鐘
m2	`Permitted Throughput`	average	1 分鐘

您的指標數學 ID 和表達式如下。

ID	表達式
e1	(m1/1048576)/PERIOD(m1)
e2	m2/1048576
e3	`((e1)*100)/(e2)`

指標數學：輸送量 IOPS

若要計算一段期間的每秒平均操作 (IOPS)，請將取樣計數統計數據 (`DataReadIOBytes`、`DataWriteIOBytes`、`MetadataIOBytes` 或 `TotalIOBytes`) 除以該期間的秒數。

假設您的範例邏輯如下：`DataWriteIOBytes` 的取樣計數 ÷ 期間內的秒數

然後，您的 CloudWatch 指標信息如下。

ID	可用指標	統計數字	期間
m1	• `DataReadIOBytes` • `DataWriteIOBytes` • `MetadataIOBytes`	取樣計數	1 分鐘

ID	可用指標	統計數字	期間
	• TotalIOBytes		

您的指標數學 ID 和表達式如下。

ID	表達式
e1	m1/PERIOD(m1)

指標數學：IOPS 的百分比

若要計算一段期間的不同 I/O 類型 (DataReadIOBytes、DataWriteIOBytes 或 MetadataIOBytes) 每秒 IOPS 百分比，請先將個別取樣計數統計數據乘以 100。然後將該值除以同一期間的 TotalIOBytes 取樣計數統計數據。

假設您的範例邏輯如下：(MetadataIOBytes 的取樣計數 x 100 (以轉換為百分比)) ÷ TotalIOBytes 的取樣計數

然後，您的 CloudWatch 指標信息如下。

ID	可用指標	統計數字	期間
m1	• TotalIOBytes	取樣計數	1 分鐘
m2	• DataReadIOBytes • DataWriteIOBytes • MetadataIOBytes	取樣計數	1 分鐘

您的指標數學 ID 和表達式如下。

ID	表達式
e1	(m2*100)/m1

指標數學：以 KiB 為單位的平均 I/O 大小

若要計算一段期間的平均 I/O 大小 (以 KiB 為單位)，請將 `DataReadIOBytes`、`DataWriteIOBytes` 或 `MetadataIOBytes` 指標的個別總和統計數據除以該指標的相同取樣計數統計數據。

假設您的範例邏輯如下：(`DataReadIOBytes` 的總和 ÷ 1024 (轉換為 KiB))÷ `DataReadIOBytes` 的取樣計數

然後，您的 CloudWatch 指標信息如下。

ID	可用指標	統計數字	期間
m1	• `DataReadIOBytes` • `DataWriteIOBytes` • `MetadataIOBytes`	sum	1 分鐘
m2	• `DataReadIOBytes` • `DataWriteIOBytes` • `MetadataIOBytes`	取樣計數	1 分鐘

您的指標數學 ID 和表達式如下。

ID	表達式
e1	`(m1/1024)/m2`

透過 Amazon EFS 的 AWS CloudFormation 範本使用指標數學

您也可以透過 AWS CloudFormation 範本建立度量數學運算式。您可以從上的 Amazon EFS 教學中下載和自訂一個此類範本以供使用 GitHub。若要取得有關使用 AWS CloudFormation 樣板的更多資訊，請參閱使用指南中的〈使AWS CloudFormation 用 AWS CloudFormation 樣板〉。

監視掛載嘗試成功或失敗狀態

您可以使用 Amazon CloudWatch Logs 遠端監控和報告 EFS 檔案系統掛載嘗試的成功或失敗，而無需登入用戶端。使用下列程序設定 EC2 執行個體，使其使用 CloudWatch Logs 監控其檔案系統掛載嘗試的成功或失敗。

啟用 CloudWatch 記錄檔中的掛載嘗試成功或失敗通知

1. 在 EC2 執行個體上安裝 `amazon-efs-utils` 來掛載檔案系統。如需詳細資訊，請參閱 用 AWS Systems Manager 於自動安裝或更新 Amazon EFS 用戶端 或 手動安裝 Amazon EFS 用戶端 。
2. 在 EC2 執行個體上安裝 `botocore` 用來掛載檔案系統。如需詳細資訊，請參閱 安裝和升級 `botocore`。
3. 在中啟用 CloudWatch 記錄檔功能`amazon-efs-utils`。當您使用 AWS Systems Manager 安裝和設定時`amazon-efs-utils`，系統會自動為您完成 CloudWatch 記錄。手動安裝 `amazon-efs-utils` 套件時，您必須取消第 `cloudwatch-log` 區段第 `# enabled = true` 行註解，然後手動更新 `/etc/amazon/efs/efs-utils.conf` 組態檔案。使用下列其中一個命令來手動啟用 CloudWatch 記錄檔。

   對於 Linux 執行個體：

   ```
   sudo sed -i -e '/\[cloudwatch-log\]/{N;s/# enabled = true/enabled = true/}' /etc/
   amazon/efs/efs-utils.conf
   ```

   對於 MacOS 執行個體：

   ```
   EFS_UTILS_VERSION= efs-utils-version
   sudo sed -i -e '/\[cloudwatch-log\]/{N;s/# enabled = true/enabled = true/;}' /usr/
   local/Cellar/amazon-efs-utils/${EFS_UTILS_VERSION}/libexec/etc/amazon/efs/efs-
   utils.conf
   ```

   對於 Mac2 執行個體：

   ```
   EFS_UTILS_VERSION= efs-utils-version
   ```

```
sudo sed -i -e '/\[cloudwatch-log\]/{N;s/# enabled = true/enabled = true/;}' /opt/
homebrew/Cellar/amazon-efs-utils/${EFS_UTILS_VERSION}/libexec/etc/amazon/efs/efs-
utils.conf
```

4. 您可以選擇性地設定 CloudWatch 記錄群組名稱，並在`efs-utils.conf`檔案中設定記錄保留天數。如果您想要為每個掛載的檔案系統建立不同的記錄群組，請新增`/{fs_id}`至`efs-utils.conf`檔案中`log_group_name`欄位的結尾，如下所示： CloudWatch

```
[cloudwatch-log]
log_group_name = /aws/efs/utils/{fs_id}
```

5. 將受`AmazonElasticFileSystemsUtils` AWS 管政策附加到 EC2 執行個體的 IAM 角色，或連接至執行個體上設定的 AWS 登入資料。您可以使用「系統管理員」來執行此動作，如需詳細資訊，請參閱 步驟 1：使用所需許可設定 IAM 執行個體設定檔。。

以下是掛載嘗試狀態日誌項目的範例：

```
Successfully mounted fs-12345678.efs.us-east-1.amazonaws.com at /home/ec2-user/efs
Mount failed, Failed to resolve "fs-01234567.efs.us-east-1.amazonaws.com"
```

若要在 CloudWatch 記錄檔中檢視裝載狀態

1. 請在以下位置開啟 CloudWatch 主控台。 https://console.aws.amazon.com/cloudwatch/
2. 從左側導覽列中選擇日誌群組。
3. 選擇 /aws/efs/utils 日誌群組。您將看到每個 Amazon EC2 執行個體和 EFS 檔案系統組合的日誌串流。
4. 選擇日誌串流以檢視特定日誌事件，包括裝載嘗試成功或失敗狀態。

存取 CloudWatch 量度

您可以透過多種方式檢視 Amazon EFS 指標： CloudWatch

- 在 Amazon EFS 主控台
- 在 CloudWatch 主控台中
- 使用 CloudWatch CLI
- 應用 CloudWatch 程式介面

以下程序旨在說明如何使用這些多種工具來存取指標。

若要在 Amazon EFS 主控台中檢視 CloudWatch 指標和警示

1. 登入 AWS Management Console 並開啟 Amazon EFS 主控台，網址為 https://console.aws.amazon.com/efs/。
2. 選擇檔案系統。
3. 選擇您要檢視其 CloudWatch 測量結果的檔案系統。
4. 選擇監控以顯示檔案系統指標頁面。

   「檔案系統測量結果」頁面會顯示檔案系統的預設 CloudWatch測量結果集。您已設定的任何 CloudWatch 警示也會以這些量度顯示。對於使用「最大 I/O」效能模式的檔案系統，指標預設設定內容包括取代「百分比 IO」限制的「爆增額度」餘額。您可以使用「度量設定」對話方塊 (開啟設定) 來覆寫預設設定。

   > **Note**
   >
   > 「輸送量使用率 (%)」量度不是量 CloudWatch 度，而是使用 CloudWatch 量度數學計算衍生出來的。

5. 您可以使用檔案系統指標頁面上的控制項，調整指標和警示的顯示方式，如下所示。
   - 在時間序列或單值之間切換顯示模式。
   - 顯示或隱藏為檔案系統設定的任何 CloudWatch 警示。
   - 選擇 [查看更多資訊 CloudWatch於] 以檢視中的量度 CloudWatch。
   - 選擇 [新增至儀表板] 以開啟 CloudWatch 儀表板並新增顯示的指標。
   - 將顯示的指標時間視窗從 1 小時調整為 1 週。

使用 CloudWatch 主控台檢視指標

1. 請在以下位置開啟 CloudWatch 主控台。 https://console.aws.amazon.com/cloudwatch/
2. 在導覽窗格中，選擇 指標。
3. 選取 EFS 命名空間。
4. (選用) 若要檢視指標，請在搜尋欄位中鍵入其名稱。
5. (選擇性) 若要依維度篩選，請選取 FileSystemId。

若要存取量度 AWS CLI

- 使用具有 `--namespace "AWS/EFS"` 命名空間的 `list-metrics` 命令。如需詳細資訊，請參閱《AWS CLI 命令參考》https://docs.aws.amazon.com/cli/latest/reference/。

若要從 CloudWatch API 存取指標

- 呼叫 `GetMetricStatistics`。如需詳細資訊，請參閱 Amazon CloudWatch API 參考資料。

建立 CloudWatch 警示以監控 Amazon EFS

您可以建立 CloudWatch 警示，在警示狀態變更時傳送 Amazon SNS 訊息。警示會在您指定的期間監看單一指標。警示會根據在數段期間內與指定閾值相關的指標值，來執行一個或多個動作。此動作是傳送到 Amazon SNS 主題或 Auto Scaling 政策的通知。

警示只會呼叫持續狀態變更的動作。 CloudWatch 警報不會只因為處於特定狀態而叫用動作；狀態必須已變更並維持指定數目的期間。

Amazon EFS CloudWatch 警示的其中一個重要用途是為檔案系統強制執行靜態加密。您可在 Amazon EFS 檔案系統建立時啟用靜態加密。若要強制執行 Amazon EFS 檔案系統的資料 encryption-at-rest 政策，您可以使用 Amazon CloudWatch 並 AWS CloudTrail 偵測檔案系統的建立，並確認已啟用靜態加密。如需詳細資訊，請參閱 演練：靜態強制執行 Amazon EFS 檔案系統強制執行靜態加密。

> **Note**
>
> 目前，您無法強制執行傳輸中加密。

下列程序概述如何建立 Amazon EFS 的警示。

使用 CloudWatch 主控台設定鬧鐘

1. 請登入 AWS Management Console 並開啟 CloudWatch 主控台，網址為 https://console.aws.amazon.com/cloudwatch/。
2. 選擇建立警示。這會啟動 Create Alarm Wizard (建立警示精靈)。
3. 選擇 EFS 指標並捲動檢視 Amazon EFS 指標，以找到您要設定警示的指標。若要在此對話方塊中僅顯示 Amazon EFS 指標，請在您的檔案系統搜尋檔案系統 ID。選取要建立警示的指標，然後選擇下一步。

4. 填入指標的 Name (名稱)、Description (說明)、Whenever (每當) 值。
5. 如果您想要 CloudWatch 在到達鬧鐘狀態時傳送電子郵件給您，請在「每當此警示：」欄位中選擇「狀態為鬧鐘」。在傳送通知至： 欄位中，選擇現有的 SNS 主題。如果您選取建立主題，即可為新電子郵件訂閱清單設定名稱和電子郵件地址。此清單會儲存並顯示在欄位中供未來警示使用。

   > **Note**
   >
   > 如果您使用建立主題來建立新的 Amazon SNS 主題，電子郵件地址必須先經過驗證才會接收通知。電子郵件只有在警示進入警示狀態時才會傳送。如果此警示狀態在驗證電子郵件地址之前發生變更，就不會收到通知。

6. 此時，Alarm Preview (警示預覽) 區域會提供您機會預覽您將建立的警示。選擇建立警示 。

若要使用設定鬧鐘 AWS CLI

- 呼叫 `put-metric-alarm`。如需詳細資訊，請參閱《AWS CLI 命令參考》https://docs.aws.amazon.com/cli/latest/reference/。

若要使用 CloudWatch API 設定警示

- 呼叫 `PutMetricAlarm`。如需詳細資訊，請參閱 Amazon CloudWatch API 參考資料。

使用記錄 Amazon EFS API 呼叫 AWS CloudTrail

Amazon EFS 與這項服務整合在一起 AWS CloudTrail，該服務可提供 Amazon EFS 中使用者、角色或 AWS 服務所採取的動作記錄。 CloudTrail 以事件形式擷取 Amazon EFS 的所有 API 呼叫，包括來自 Amazon EFS 主控台的呼叫，以及從程式碼呼叫到 Amazon EFS API 操作。

如果您建立追蹤，您可以啟用持續交付 CloudTrail 事件到 Amazon S3 儲存貯體，包括 Amazon EFS 的事件。如果您未設定追蹤，您仍然可以在 [事件歷程記錄] 中檢視 CloudTrail 主控台中最近的事件。使用收集的資訊 CloudTrail，您可以判斷向 Amazon EFS 發出的請求、提出請求的來源 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。

如需詳細資訊，請參閱 AWS CloudTrail 使用者指南。

Amazon EFS 信息 CloudTrail

CloudTrail 在您創建帳戶 AWS 帳戶 時啟用。Amazon EFS 中發生活動時，該活動會與事件歷史記錄中的其他 AWS 服務 CloudTrail 事件一起記錄在事件中。您可以檢視、搜尋和下載 AWS 帳戶的最新事件。如需詳細資訊，請參閱檢視具有事 CloudTrail 件記錄的事件。

如需您 AWS 帳戶的事件的持續記錄 (包括 Amazon EFS 的事件)，請建立追蹤。追蹤可 CloudTrail 將日誌檔交付到 Amazon S3 儲存貯體。根據預設，當您在主控台中建立追蹤時，追蹤會套用至所有 AWS 區域項目。追蹤記錄來自 AWS 分區 AWS 區域 中所有的事件，並將日誌檔傳送到您指定的 Amazon S3 儲存貯體。此外，您還可以設定其他 AWS 服務，以進一步分析 CloudTrail 記錄中收集的事件資料並採取行動。如需詳細資訊，請參閱 AWS CloudTrail 使用者指南中的以下主題：

- 建立追蹤的概觀
- CloudTrail 支援的服務與整合
- 設定 Amazon SNS 通知 CloudTrail
- 從多個區域接收 CloudTrail 記錄檔並從多個帳戶接收 CloudTrail 記錄檔

所有 Amazon EFS API 呼叫都由記錄 CloudTrail。例如，呼叫`CreateMountTarget`和`CreateTags`作業會`CreateFileSystem`在 CloudTrail 記錄檔中產生項目。

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：

- 請求是以根使用者還是 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。

若要取得更多資訊，請參閱《AWS CloudTrail 使用者指南》中的使用者 CloudTrail userIdentity 元素。

了解 Amazon EFS 日誌檔案項目

追蹤是一種組態，可讓事件以日誌檔的形式傳遞到您指定的 Amazon S3 儲存貯體。 CloudTrail 記錄檔包含一或多個記錄項目。事件代表來自任何來源的單一請求，包括有關請求的操作，動作的日期和時間，請求參數等信息。 CloudTrail 日誌文件不是公共 API 調用的有序堆棧跟踪，因此它們不會以任何特定順序顯示。

下列範例會示範從主控台建立檔案系統標籤時的`CreateTags`作業 CloudTrail 記錄項目。

```
{
 "eventVersion": "1.06",
 "userIdentity": {
  "type": "Root",
  "principalId": "111122223333",
  "arn": "arn:aws:iam::111122223333:root",
  "accountId": "111122223333",
  "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "sessionContext": {
   "attributes": {
    "mfaAuthenticated": "false",
    "creationDate": "2017-03-01T18:02:37Z"
   }
  }
 },
 "eventTime": "2017-03-01T19:25:47Z",
 "eventSource": "elasticfilesystem.amazonaws.com",
 "eventName": "CreateTags",
 "awsRegion": "us-west-2",
 "sourceIPAddress": "192.0.2.0",
 "userAgent": "console.amazonaws.com",
 "requestParameters": {
  "fileSystemId": "fs-00112233",
  "tags": [{
    "key": "TagName",
    "value": "AnotherNewTag"
   }
  ]
 },
 "responseElements": null,
 "requestID": "dEXAMPLE-feb4-11e6-85f0-736EXAMPLE75",
 "eventID": "eEXAMPLE-2d32-4619-bd00-657EXAMPLEe4",
 "eventType": "AwsApiCall",
 "apiVersion": "2015-02-01",
 "recipientAccountId": "111122223333"
}
```


下列範例顯示 CloudTrail 記錄項目，示範從主控台刪除檔案系統標籤時所DeleteTags採取的動作。


```
{
 "eventVersion": "1.06",
 "userIdentity": {
```

```
  "type": "Root",
  "principalId": "111122223333",
  "arn": "arn:aws:iam::111122223333:root",
  "accountId": "111122223333",
  "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "sessionContext": {
   "attributes": {
    "mfaAuthenticated": "false",
    "creationDate": "2017-03-01T18:02:37Z"
   }
  }
 },
 "eventTime": "2017-03-01T19:25:47Z",
 "eventSource": "elasticfilesystem.amazonaws.com",
 "eventName": "DeleteTags",
 "awsRegion": "us-west-2",
 "sourceIPAddress": "192.0.2.0",
 "userAgent": "console.amazonaws.com",
 "requestParameters": {
  "fileSystemId": "fs-00112233",
  "tagKeys": []
 },
 "responseElements": null,
 "requestID": "dEXAMPLE-feb4-11e6-85f0-736EXAMPLE75",
 "eventID": "eEXAMPLE-2d32-4619-bd00-657EXAMPLEe4",
 "eventType": "AwsApiCall",
 "apiVersion": "2015-02-01",
 "recipientAccountId": "111122223333"
}
```

EFS 服務連結角色的日誌項目

Amazon EFS 服務連結角色可對 AWS 資源進行 API 呼叫。您會看到 EFS 服務連結角色呼叫的 CloudTrail 記錄項目。`username: AWSServiceRoleForAmazonElasticFileSystem`如需 EFS 和服務連結角色的詳細資訊，請參閱 使用 Amazon EFS 的服務連結角色。

下列範例顯示示範 Amazon EFS 建立 AWSServiceRoleForAmazonElasticFileSystem 服務連結角色時所`CreateServiceLinkedRole`採取的動作的 CloudTrail 記錄項目。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
```

```
        "type": "IAMUser",
        "principalId": "111122223333",
        "arn": "arn:aws:iam::111122223333:user/user1",
        "accountId": "111122223333",
        "accessKeyId": "A111122223333",
        "userName": "user1",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2019-10-23T22:45:41Z"
            }
        },
        "invokedBy": "elasticfilesystem.amazonaws.com”
    },
    "eventTime": "2019-10-23T22:45:41Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "CreateServiceLinkedRole",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "user_agent",
    "requestParameters": {
        "aWSServiceName": "elasticfilesystem.amazonaws.com”
    },
    "responseElements": {
        "role": {
            "assumeRolePolicyDocument":
 "111122223333-10-111122223333Statement111122223333Action111122223333AssumeRole111122223333Effe
%22%3A%20%22Allow%22%2C%20%22Principal%22%3A%20%7B%22Service%22%3A%20%5B%22
 elasticfilesystem.amazonaws.com%22%5D%7D%7D%5D%7D",
            "arn": "arn:aws:iam::111122223333:role/aws-service-role/
elasticfilesystem.amazonaws.com/AWSServiceRoleForAmazonElasticFileSystem",
            "roleId": "111122223333",
            "createDate": "Oct 23, 2019 10:45:41 PM",
            "roleName": "AWSServiceRoleForAmazonElasticFileSystem",
            "path": "/aws-service-role/elasticfilesystem.amazonaws.com/“
        }
    },
    "requestID": "11111111-2222-3333-4444-abcdef123456",
    "eventID": "11111111-2222-3333-4444-abcdef123456",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

下列範例顯示示範由 AWSServiceRoleForAmazonElasticFileSystem服務連結角色所執行之CreateNetworkInterface動作的 CloudTrail 記錄項目，如中所述。sessionContext

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::0123456789ab:assumed-role/
AWSServiceRoleForAmazonElasticFileSystem/0123456789ab",
        "accountId": "0123456789ab",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::0123456789ab:role/aws-service-role/
elasticfilesystem.amazonaws.com/AWSServiceRoleForAmazonElasticFileSystem",
                "accountId": "0123456789ab",
                "userName": "AWSServiceRoleForAmazonElasticFileSystem"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2019-10-23T22:50:05Z"
            }
        },
        "invokedBy": "AWS Internal"
    },
    "eventTime": "20You 19-10-23T22:50:05Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "CreateNetworkInterface",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "elasticfilesystem.amazonaws.com”,
    "userAgent": "elasticfilesystem.amazonaws.com",
    "requestParameters": {
        "subnetId": "subnet-71e2f83a",
        "description": "EFS mount target for fs-1234567 (fsmt-1234567)",
        "groupSet": {},
        "privateIpAddressesSet": {}
    },
    "responseElements": {
        "requestId": "0708e4ad-03f6-4802-b4ce-4ba987d94b8d",
        "networkInterface": {
```

```
            "networkInterfaceId": "eni-0123456789abcdef0",
            "subnetId": "subnet-12345678",
            "vpcId": "vpc-01234567",
            "availabilityZone": "us-east-1b",
            "description": "EFS mount target for fs-1234567 (fsmt-1234567)",
            "ownerId": "666051418590",
            "requesterId": "0123456789ab",
            "requesterManaged": true,
            "status": "pending",
            "macAddress": "00:bb:ee:ff:aa:cc",
            "privateIpAddress": "192.0.2.0",
            "privateDnsName": "ip-192-0-2-0.ec2.internal",
            "sourceDestCheck": true,
            "groupSet": {
                "items": [
                    {
                        "groupId": "sg-c16d65b6",
                        "groupName": "default"
                    }
                ]
            },
            "privateIpAddressesSet": {
                "item": [
                    {
                        "privateIpAddress": "192.0.2.0",
                        "primary": true
                    }
                ]
            },
            "tagSet": {}
        }
    },
    "requestID": "11112222-3333-4444-5555-666666777777",
    "eventID": "aaaabbbb-1111-2222-3333-444444555555",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```


EFS 身分驗證的日誌項目

適用於 NFS 用戶端的 Amazon EFS 授權會發出`NewClientConnection`和`UpdateClientConnection` CloudTrail 事件。在初始連線之後和重新連線之後立即授權連連線時，就會發出 `NewClientConnection` 事件。系統重新授權鏈接且已更改允

許的動作時，將發出 UpdateClientConnection。允許的動作新清單不包含 ClientMount 時，也會發出該事件。如需 EFS 授權的詳細資訊，請參閱 使用 IAM 控制檔案系統資料存取。

下列範例顯示示範NewClientConnection事件的 CloudTrail 記錄項目。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::0123456789ab:assumed-role/abcdef0123456789",
        "accountId": "0123456789ab",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE ",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::0123456789ab:role/us-east-2",
                "accountId": "0123456789ab",
                "userName": "username"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2019-12-23T17:50:16Z"
            },
            "ec2RoleDelivery": "1.0"
        }
    },
    "eventTime": "2019-12-23T18:02:12Z",
    "eventSource": "elasticfilesystem.amazonaws.com",
    "eventName": "NewClientConnection",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "elasticfilesystem",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "27859ac9-053c-4112-aee3-f3429719d460",
    "readOnly": true,
    "resources": [
        {
            "accountId": "0123456789ab",
            "type": "AWS::EFS::FileSystem",
```

```
            "ARN": "arn:aws:elasticfilesystem:us-east-2:0123456789ab:file-system/
fs-01234567"
        },
        {
            "accountId": "0123456789ab",
            "type": "AWS::EFS::AccessPoint",
            "ARN": "arn:aws:elasticfilesystem:us-east-2:0123456789ab:access-point/
fsap-0123456789abcdef0"
        }
    ],
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "0123456789ab",
    "serviceEventDetails": {
        "permissions": {
            "ClientRootAccess": true,
            "ClientMount": true,
            "ClientWrite": true
        },
        "sourceIpAddress": "10.7.3.72"
    }
}
```

適用於檔案系統的 Amazon EFS 日誌 encrypted-at-rest檔項目

Amazon EFS 提供下列檔案系統的選項：使用靜態加密、傳輸中加密或兩者。如需詳細資訊，請參閱 Amazon EFS 的資料加密。

Amazon EFS 會在發出 AWS KMS API 請求以產生資料金鑰和解密 Amazon EFS 資料時傳送加密內容。檔案系統 ID 是靜態加密之所有檔案系統的加密內容。在 CloudTrail 記錄項目`requestParameters`欄位中，加密內容看起來類似下列內容。

```
"EncryptionContextEquals": {}
"aws:elasticfilesystem:filesystem:id" : "fs-4EXAMPLE"
```

Amazon EFS 效能

以下各節概述了 Amazon EFS 效能，並說明檔案系統組態對關鍵效能維度的影響方式。我們也提供一些重要的提示和建議，用來優化檔案系統效能。

主題

效能摘要

檔案系統效能通常使用從延遲、輸送量以及每秒讀寫次數 (IOPS) 這幾個維度來衡量。Amazon EFS 在這些維度上的效能取決於檔案系統的組態。下列組態會影響 Amazon EFS 檔案系統效能：

- 檔案系統類型：區域性或單區域
- 效能模式：一般用途或最大 I/O

> **Important**
>
> 最大 I/O 效能模式的每個操作延遲時間高於「一般用途」效能模式的延遲時間。為獲得更快效能，我們建議您始終使用「一般用途」效能模式。如需詳細資訊，請參閱 效能模式。

- 輸送量模式：彈性、佈建或爆量

下表概述使用「一般用途」效能模式之檔案系統的效能規格，以及檔案系統類型和輸送量模式的可能不同組合。

使用一般用途效能模式之檔案系統的效能規格

儲存和輸送量組態		Latency (延遲)		最大 IOPS		最大輸送量		
檔案系統類型	輸送量模式	讀取操作	寫入操作	讀取操作	寫入操作	每個檔案系統讀取 [1]	每個檔案系統寫入 [1]	每個客戶端讀/寫
區域性	彈性	低至 250 微秒 (µs)	低至 2.7 毫秒 (毫秒)	90,000—250,000 [2]	50,000	每秒 3—20 吉位元組 () GiBps	1-5 GiBps	每秒 1,500 兆字節 () [3] MiBps
區域性	佈建	低至 250 µs	低至 2.7 毫秒	55,000	25,000	3—10 GiBps	1—3.33 GiBps	500 MiBps
區域性	爆量	低至 250 µs	低至 2.7 毫秒	35,000	7,000	3—5 GiBps	1—3 GiBps	500 MiBps
單區域	彈性、佈建、爆裂	低至 250 µs	低至 1.6 毫秒	35,000	7,000	3 GiBps [4]	1 GiBps [4]	500 MiBps

Note

註腳：

1. 最大讀取和寫入輸送量取決於 AWS 區域。超過最大 AWS 區域區域最大輸送量的輸送量需要增加輸送量配額。Amazon EFS 服務團隊會考慮任何額外輸送量的要求。 case-by-case 核准可能取決於您的工作負載類型。若要進一步了解請求提高配額的信息，請參閱 Amazon EFS 配額。
2. 使用彈性輸送量的檔案系統最多可為不常存取的資料驅動 90,000 個讀取 IOPS，針對經常存取的資料驅動 250,000 個讀取 IOPS。適用其他建議以達到最大 IOPS。如需詳細資訊，請參閱 the section called “優化工作負載需要較高的輸送量和 IOPS”。
3. 對於使用彈性輸送量的檔案系統，且使用 Amazon EFS 用戶端 (版本) 或 Amazon EFS CSI 驅動程式 (aws-efs-csi 驅動程式) 的 2.0 版或更新amazon-efs-utils 版本進行裝載的檔案系統，最大的合併讀取和寫入輸送量 MiBps 為 1,500。對於所有其他檔案系統，輸送量限制為 500 MiBps。如需 Amazon EFS 用戶端的詳細資訊，請參閱 安裝 Amazon EFS 工具

4. 使用大量批量輸送量的一個區域檔案系統可以驅動與區域檔案系統相同的 per-file-system 讀取和寫入輸送量 (讀取的最大讀取量 GiBps 為 5，寫入 GiBps 為 3)。

儲存類別

Amazon EFS 儲存類別專為最有效的儲存而設計，具體取決於使用案例。

- EFS 標準儲存體類別使用固態硬碟 (SSD) 儲存為經常存取的檔案提供最低延遲等級。此儲存類別提供讀取時間低至 250 微秒的第一個位元組延遲，而寫入則為 2.7 毫秒。
- EFS 不常存取 (IA) 和 EFS 封存儲存體類別會儲存較少存取的資料，這些資料不需要經常存取資料所需的延遲效能。這些儲存類別提供几十毫秒的第一個位元組延遲。

如需 EFS 儲存類別的詳細資訊，請參閱the section called “EFS 儲存類別”。

效能模式

Amazon EFS 提供以下兩種效能模式：一般用途和最大 I/O。

- 一般用途模式的每個作業延遲最低，而且是檔案系統的預設效能模式。一個區域檔案系統一律使用「一般用途」效能模式。為獲得更快效能，我們建議您始終使用「一般用途」效能模式。
- 最大 I/O 模式是上一代效能類型，專為高度平行化的工作負載而設計，可用於比「一般用途」模式更高的延遲。單區域檔案系統或使用彈性輸送量的檔案系統不支援最大 I/O 模式。

> **Important**
>
> 由於最大 I/O 的每個操作延遲較高，我們建議所有檔案系統使用「一般用途」效能模式。

若要協助確保您的工作負載維持在使用「一般用途」效能模式的檔案系統可用的 IOPS 限制內，您可以監視`PercentIOLimit` CloudWatch 測量結果。如需詳細資訊，請參閱 Amazon EFS 的 Amazon CloudWatch 指標。

應用程式可彈性地擴展 IOPS，達到與效能模式相關的極限。IOPS 不會單獨向您收費；其費用計入檔案系統的輸送量帳戶中。每個網路檔案系統 (NFS) 請求都會按 4 KB 輸送量計費，或按其實際請求和回應中較大的輸送量計費。

輸送量模式

檔案系統的輸送量模式會決定檔案系統可用的輸送量。Amazon EFS 提供以下三種輸送量模式：彈性、佈建和爆量。讀取輸送量有折扣，可讓您獲得比寫入輸送量更高的讀取輸送量。每個輸送量模式可用的最大輸送量取決於所在 AWS 區域區域。如需關於不同區域中檔案系統輸送量上限的詳細資訊，請參閱 Amazon EFS 配額。

您的檔案系統可以實現讀取和寫入輸送量綜合為 100%。例如，如果您的檔案系統使用其讀取輸送量限制的 33%，檔案系統可以同時達到其寫入輸送量限制的 67%。在主控台的檔案系統詳細資訊頁面上，您可以在其輸送量使用率 (%)圖表中監視檔案系統的輸送量使用量。如需詳細資訊，請參閱 使用 CloudWatch 指標監視輸送量效能。

選擇正確的檔案系統輸送量模式。

根據工作負載的效能需求，為檔案系統選擇正確的輸送量模式。

- 彈性輸送量 (建議) — 如果您的工作負載和效能需求極高或無法預測，或應用程式以 5% 或更低的 average-to-peak 比率驅動輸送量，請使用預設的彈性輸送量。如需詳細資訊，請參閱 彈性輸送量。
- 佈建輸送量 — 如果您知道工作負載的效能需求，或應用程式以 5% 或更高的 average-to-peak 比率驅動輸送量，請使用佈建的輸送量。如需詳細資訊，請參閱 佈建輸送量。
- 大量批量輸送量 — 當您想要隨檔案系統儲存量調整的輸送量時，請使用突增輸送量。

  如果在使用大量批量輸送量之後，您發現應用程式受到輸送量限制 (例如，它使用的允許輸送量的 80% 以上，或者您已使用所有的突發積分)，則應使用彈性或佈建輸送量。如需詳細資訊，請參閱 爆量吞吐量。

您可以使用 Amazon CloudWatch 透過 average-to-peak 比較指標與`MeteredIOBytes`指標來確定工作負載的比率。`PermittedThroughput`如需 Amazon EFS 請求指標的詳細資訊，請參閱 Amazon EFS 的 Amazon CloudWatch 指標。

彈性輸送量

對於使用彈性輸送量的檔案系統，Amazon EFS 會自動擴展或縮減輸送量效能，以符合工作負載活動的需求。對於效能需求難以預測的尖峰或無法預測的工作負載，或是將輸送量平均提高 5% 或以下的應用程式 (average-to-peak比率)，彈性輸送量是最佳輸送量模式。

由於具有彈性輸送量的檔案系統的輸送量效能會自動調整，因此您不需要指定或佈建輸送量容量來滿足您的應用程式需求。您只需為讀取或寫入的中繼資料和資料量付費，而且在使用彈性輸送量時，不會累積或消耗突發積分。

> **Note**
>
> 彈性輸送量僅適用於使用一般目的效能模式的檔案系統。

如需各區域彈性輸送量限制的相關資訊，請參閱您可以提高的 Amazon EFS 配額。

佈建輸送量

使用佈建輸送量，您可以指定檔案系統可以驅動的輸送量層級，而不受檔案系統的大小或突發積分餘額影響。如果您知道工作負載的效能需求，或者如果您的應用程式將輸送量提高 5% 或更高的 average-to-peak 比率，請使用佈建輸送量。

對於使用佈建輸送量的檔案系統，您需支付針對檔案系統啟用的輸送量量收費。按月收費的輸送量總量根據超出文件檔案標準儲存基礎線輸送量的輸送量配送，且在 AWS 區域區域上限為現行爆量基礎線輸送量。

如果檔案系統的基準輸送量超過佈建輸送量量，它會自動使用檔案系統允許的大量批量輸送量 (最多達到該中現行的\ 大量基準輸送量限制)。 AWS 區域

如需每RegionProvisioned 輸送量限制的相關資訊，請參閱您可以提高的 Amazon EFS 配額。

爆量吞吐量

對於需要隨檔案系統儲存容量調整的輸送量的工作負載，建議使用大量輸送量。使用大量輸送量時，基本輸送量與標準儲存類別中檔案系統的大小成比例，速率為 KiBps 每個 GiB 儲存體 50。檔案系統消耗低於其基本輸送量率時，會累積爆量額度，並在輸送量超過基本速率時扣除。

當突發積分可用時，檔案系統最多可以將 MiBps每 TiB 儲存的輸送量提高至 100，最高可達 100 個上 AWS 區域 限，最少為 100 MiBps。如果沒有可用的突發點數，檔案系統最多可以為 MiBps 每 TiB 的儲存磁碟機 50 個，最少 1 MiBps 個。

如需每個區域大量批量輸送量的相關資訊，請參閱。General resource quotas that cannot be changed

了解 Amazon EFS 爆量額度

使用大量批量輸送量，每個檔案系統都可以在一段時間內以基準速率 (由 EFS Standard 儲存類別中儲存的檔案系統大小決定) 獲得突發積分。基準速率為 MiBps 每個千兆位元組 [TiB] 儲存空間 50 (相當於

KiBps 每 GiB 的儲存裝置 50)。Amazon EFS 將讀取操作計量高達寫入操作速率的三分之一，允許檔案系統提高每 GiB 讀取輸送量的基準速率最高可達 150 個，或者 KiBps 每 GiB 的寫入輸送量提高 50 KiBps 個。

檔案系統可以持續以其基準計量速率來驅動輸送量。每當檔案系統不活躍或驅動輸送量低於其基準計量速率時，就會纍計爆量額度。累積的爆量額度讓檔案系統能夠將輸送量提高到超過其基準傳輸率。

例如，在標準儲存類別中具有 100 GiB 計量資料的檔案系統，其基準輸送量為 5。 MiBps在 24 小時的閒置期間內，檔案系統可獲得 432,000 MiB 價值的信用額度 (5 MiB × 86,400 秒 = 432,000 MiB)，可用來以 100 的速度爆發 72 分鐘 (432,000 miB ÷ 100 MiBps = 72 分鐘)。 MiBps

大於 1 TiB 的檔案系統，如果在剩下 50% 的時間都處於閒置狀態，就能隨時在最多 50% 的時間中爆量增加。

下表提供爆量動作的範例。

檔案系統大小	爆量輸送量	基準輸送量
標準儲存中 100 GiB 的計量資料	• 突發為 300（MiBps）只讀，每天最多 72 分鐘，或者 • 突發到 100 MiBps 只寫，每天最多 72 分鐘	• 連續驅動最多 15 個 MiBps 只讀 • 連續驅動多達 5 個 MiBps 唯寫
標準儲存中 1 TiB 的計量資料	• 突發為 300 MiBps 只讀，每天 12 小時，或者 • 突發到 100 MiBps 只寫，每天 12 小時	• 磁碟機 150 連續 MiBps 唯讀 • 驅動 50 只 MiBps 寫連續
標準儲存中 10 TiB 的計量資料	• 突發為 3 GiBps 只讀，每天 12 小時，或者 • 每天突發為 1 次 GiBps 只寫 12 小時	• 磁碟機 1.5 連續 GiBps 唯讀 • 驅動 500 只 MiBps 寫連續
通常，較大的文件系統	• 每 TiB 的儲存空間突發為 300 個 MiBps 唯讀狀態，每天 12 小時，或者 • 每 TiB 的儲存空間突增至 100 次 MiBps 唯寫，每天 12 小時	• 每 TiB 的儲存裝置連續磁碟機 150 個 MiBps 唯讀 • 每 TiB 的儲存裝置連續磁碟機 50 個 MiBps 唯寫

> **Note**
>
> Amazon EFS MiBps 為所有檔案系統提供 1 的計量輸送量，即使基準率較低也是如此。
> 在計算基準傳輸率和爆量傳輸率時所使用的檔案系統大小，是透過 DescribeFileSystems 操作所取得的 `ValueInStandard` 計量大小相同。
> 檔案系統可獲得額度，小於 1 TiB 的檔案系統，其額度餘額上限為 2.1 TiB，大於 1 TiB 的檔案系統，上限則為每 TiB 儲存容量 2.1 TiB。這個行爲意味著檔案系統可以累積足夠的額度，來連續爆量增加長達 12 小時。

切換輸送量和變更佈建量的限制

您可以切換現有檔案系統的輸送量模式，並變更輸送量總量。但是，在將輸送量模式切換為佈建輸送量或變更佈建輸送量量之後，下列動作會在 24 小時內限制：

- 從佈建輸送量模式切換至彈性或大量輸送量模式。
- 減少佈建輸送量量。

Amazon EFS 效能秘訣

使用 Amazon EFS 時，請記住下列效能秘訣：

平均 I/O 大小

Amazon EFS 的分散式本質，實現了高度的可用性、持久性與可擴展性。這種分散式架構讓每個檔案作業只會產生些許的延遲負擔。由於每個作業的低延遲，因此整體輸送量通常會隨著平均 I/O 大小的增加而提高，因為延遲負擔會由大量的資料分攤。

優化工作負載需要較高的輸送量和 IOPS

對於需要高輸送量和 IOPS 的工作負載，請使用設定為一般用途效能模式和彈性輸送量的區域檔案系統。

> **Note**
>
> 若要針對經常存取的資料達到最大 250,000 個讀取 IOPS，檔案系統必須使用彈性輸送量。

若要獲得最高效能，您必須依照下列方式設定應用程式或工作負載來充分利用平行處理。

1. 將工作負載平均分配到所有用戶端和目錄，其目錄數目至少與已使用的用戶端數目相同。
2. 將單個執行緒不同資料集或文件對齊，最大限度減少爭用。
3. 將工作負載分配到 10 個或更多 NFS 用戶端，單一掛載目標中每個用戶端至少有 64 個執行緒。

同時連接

您可以同時在多達數千個 Amazon EC2 和其他 AWS 運算執行個體上掛載 Amazon EFS 檔案系統。如果可以跨更多執行個體來平行執行應用程式，您就能跨運算執行個體提高檔案系統上的總輸送量。

請求模型

如果您啟用非同步寫入檔案系統的功能，則待執行的寫入作業會在非同步寫入 Amazon EFS 之前，先暫存於 Amazon EC2 執行個體上的緩衝區。非同步寫入作業的延遲通常較低。執行非同步寫入時，核心會使用額外的記憶體來進行快取。

檔案系統如果啟用了同步寫入功能，或是使用略過快取的選項 (例如 `O_DIRECT`) 來開啟檔案，則該檔案系統會向 Amazon EFS 發出同步請求。每項操作都會在用戶端與 Amazon EFS 之間來回往返執行。

> **Note**
>
> 您所選擇的請求模型，必須在一致性 (如果使用多個 Amazon EC2 執行個體) 和速度之間權衡折衷。使用同步寫入功能可在處理下一個請求之前完成每個寫入要求交易，藉此提高資料一致性。通過緩衝等待的寫入操作來使用非同步寫入可以提高輸送量。

NFS 用戶端掛載設定

確定您正在使用建議的掛載選項 (如 掛載 EFS 檔案系統 和 其他掛載注意事項 中所述)。

當您在 Amazon EC2 執行個體上掛載檔案系統時，Amazon EFS 支援網路檔案系統版本 4.0 與 4.1 (NFSv4) 通訊協定。與 NFSv4.0 (每秒少於 1,000 個檔案) 相比，NFSv4.1 (每秒超過 10,000 個檔案) 可為并行小型檔案讀取操作提供更好的效能。執行 macOS Big Sur 的 Amazon EC2 MacOS 執行個體僅支援 NFSv4.0。

請勿使用下列掛載選項：

- `noac`、`actimeo=0`、`acregmax=0`、`acdirmax=0`：這些選項會停用屬性快取，這會對效能造成非常大的影響。
- `lookupcache=pos`、`lookupcache=none`：這些選項會停用檔案名稱查閱快取，這會對效能造成非常大的影響。
- `fsc`：此選項可啟用本機檔案快取，但不會變更 NFS 快取一致性，也不會減少延遲。

> **Note**
>
> 在掛載檔案系統時，您可以考慮將 NFS 用戶端讀取和寫入緩衝區大小增加到 1 MB。

優化小型檔案效能

您可以盡可能減少檔案重新開啟、增加平行處理，以及盡量綁定參考檔案，以改善小型檔案的效能。

- 減少到伺服器的往返次數。

  如果稍後在工作流程中需要檔案，非必要不關閉檔案。打開文件描述元可以直接訪問快取中的本地副本。檔案開啟、關閉和中繼資料操作通常無法以非同步方式或透過管線進行。

  讀取或寫入小型文件時，額外的兩次往返非常重要。

  每次往返 (文件開啓，文件關閉) 時間與讀取或寫入批量資料的時間相同。更有效的方法是在計算工作開始時，一次性打開輸入或輸出文件，并在整個計算工作期間保持打開狀態。
- 使用平行處理原則來減少往返時間的影響。
- 將參考檔案綁定在一個 `.zip` 檔案中。某些應用程式會使用大量小型參考文件，這些文件大部分為只讀。將這些文件綁定在 `.zip` 檔案中，以便您可以一次打開關閉多個檔案。

  `.zip` 格式允許隨機訪問單個檔案。

優化磁碟效能

在正修改的大型目錄 (超過 10 萬個檔案) 上同時執行清單 (ls) 時，Linux NFS 用戶端可能會當機，而不會傳回回應。已在核心 5.11 中修正此問題，該核心已移植至 Amazon Linux 2 核心 4.14、5.4 和 5.10。

如果可能，建議您將檔案系統上的目錄數目保持在 10,000 以下。盡可能使用嵌套子目錄。

列出目錄時，如果不需要文件屬性則避免獲取，因爲這些文件屬性本來就不存儲在目錄中。

優化 NFS read_ahead_kb 大小

NFS `read_ahead_kb` 屬性定義了 Linux 內核在連續讀取操作期間預先讀取或預取的千位元組數。

對於 5.4.* 之前的 Linux 核心版本，`read_ahead_kb` 值的設定方式為 `NFS_MAX_READAHEAD` 乘以 `rsize` (在掛載選項中設定的用戶端設定讀取緩衝區大小) 的值。使用建議掛載選項時，此公式會將 `read_ahead_kb` 設定為 15 MB。

> **Note**
>
> 從 Linux 核心版本 5.4.* 開始時，Linux NFS 用戶端會使用預設值`read_ahead_kb` 128 KB。我們建議將此值增加到 15 MB。

在 `amazon-efs-utils` 版本 1.33.2 版及更高版本中可用的 Amazon EFS 掛載協助程式會在掛載檔案系統後，自動將 `read_ahead_kb` 值修改為等於 15* `rsize` 或 15 MB。

對於 Linux 核心 5.4 或更高版本，如果您不使用掛載輔助程式來掛載檔案系統，請考慮手動設定 `read_ahead_kb` 為 15 MB 以改善效能。掛載檔案系統之後，您可以使用下列指令來重設 `read_ahead_kb` 值。使用此命令之前，請取代下列值：

- 按所需的大小取代 *`read-ahead-value-kb`* (以 KB 為單位)。
- 用檔案系統的掛載點取代 *`efs-mount-point`*。

```
device_number=$(stat -c '%d' efs-mount-point)
((major = ($device_number & 0xFFF00) >> 8))
((minor = ($device_number & 0xFF) | (($device_number >> 12) & 0xFFF00)))
sudo bash -c "echo read-ahead-value-kb > /sys/class/bdi/$major:$minor/read_ahead_kb"
```

下列範例將 `read_ahead_kb` 大小設定為 15 MB。

```
device_number=$(stat -c '%d' efs)
((major = ($device_number & 0xFFF00) >> 8))
((minor = ($device_number & 0xFF) | (($device_number >> 12) & 0xFFF00)))
sudo bash -c "echo 15000 > /sys/class/bdi/$major:$minor/read_ahead_kb"
```

疑難排解 Amazon EFS：效能問題

一般而言，如果您在解決 Amazon EFS 問題時遇到困難，請確認您使用的是最新的 Linux 核心。如果您使用的是企業 Linux 發行版本，我們建議下列事項：

- 具有核心 4.3 或更新版本的 Amazon Linux 2
- Amazon Linux 2015.09 或更新版本
- RHEL 7.3 或更新版本
- Ubuntu 16.04 的所有版本
- Ubuntu 14.04 含核心 3.13.0-83 或更新版本
- SLES 12 Sp2 或更新版本

如果您使用的是另一個發行版本或自訂核心，建議使用核心版本 4.3 或更新版本。

> **Note**
>
> 由於同步開啟太多檔案而造成效能不佳，就特定的工作負載而言，RHEL 6.9 可能是次佳選擇。

主題

無法建立 EFS 檔案系統

建立 EFS 檔案系統的請求失敗訊息如下所示：

```
User: arn:aws:iam::111122223333:user/username is not authorized to
perform: elasticfilesystem:CreateFileSystem on the specified resource.
```

採取動作

檢查您的 AWS Identity and Access Management (IAM) 政策，確認您已獲授權建立具有指定資源條件的 EFS 檔案系統。如需詳細資訊，請參閱 Amazon Elastic File System 的身分與存取管理。

拒絕在 NFS 檔案系統上存取允許的檔案

當指派給使用者的存取群組 ID (GID) 超過 16 個時，使用者嘗試在 NFS 檔案系統上執行操作，可能被拒絕对檔案系統上允许的文件进行存取。這類問題發生的原因是 NFS 通訊協定對每位使用者最多支援 16 個 GID，并且任何超出的 GID 會從 NFS 用戶端請求処截斷，具體可見 RFC 5531 中的定義。

採取動作

可以重新架構 NFS 使用者和群組對應，以便指定給每位使用者的存取群組 (GID) 數不超過 16 個。

存取 Amazon EFS 主控台時發生錯誤

本區段說明使用者在存取 Amazon EFS 管理主控台時可能遇到的錯誤。

驗證 `ec2:DescribeVPCs` 憑證時發生錯誤

存取 Amazon EFS 主控台時，系統會顯示下列錯誤訊息：

```
AuthFailure: An error occurred authenticating your credentials for ec2:DescribeVPCs.
```

此錯誤表示您的登入憑證未成功通過 Amazon EC2 服務驗證。在您選擇的 VPC 中建立 EFS 檔案系統時，Amazon EFS 主控台會代表您呼叫 Amazon EC2 服務。

採取動作

確保正確設定用戶端存取 Amazon EFS 主控台的時間。

Amazon EC2 執行個體停止回應

若您在刪除檔案系統掛載目標前未先行卸載該檔案系統，Amazon EC2 執行個體可能會因此停止回應。

採取動作

刪除掛載目標前，請先卸載檔案系統。如需卸載 Amazon EFS 檔案系統的詳細資訊，請參閱 卸載檔案系統。

應用程式撰寫大量資料造成的停止回應

撰寫大量資料至 Amazon EFS 的應用程式停止回應並造成該執行個體重新啟動。

採取動作

如果應用程式需要很長的時間才能將所有資料寫入至 Amazon EFS，Linux 可能會重新啟動，因為該程序已無法回應。此行為之定義由 `kernel.hung_task_panic` 與 `kernel.hung_task_timeout_secs` 這兩種核心組態參數負責。

在以下例子中，ps 命令會在執行個體重新啟動前將停止回應程序的狀態回報為 D，代表該程序正在等待 I/O。

```
$ ps aux | grep large_io.py
root 33253 0.5 0.0 126652 5020 pts/3 D+ 18:22 0:00 python large_io.py
/efs/large_file
```

為避免重新啟動，請提高偵測到停止回應任務時的逾時時間或停用核心錯誤。以下命令可在大多數的 Linux 系統上停用停止回應的任務核心錯誤。

```
$ sudo sysctl -w kernel.hung_task_panic=0
```

同步開啟太多檔案而造成效能不佳

同時開啟多個檔案的應用程式無法如預期般提高 I/O 平行效能。

採取動作

這個問題會發生在網路檔案系統第 4 版 (NFSv4) 協定，以及使用 NFSv4.1 的 RHEL 6 用戶端上，因為這些 NFS 用戶端序列化 NFS OPEN 和 CLOSE 操作。使用 NFS 通訊協定第 4.1 版，以及建議使用、無此問題發生的一種 Linux 發行版本。

如果您無法使用 NFSv4.1，請注意 Linux NFSv4.0 用戶端會依使用者 ID 和群組 ID 順序開啟和關閉請求。即使多個程序或多個執行緒同時發出請求，序列化依然會進行。當所有 ID 相符時，用戶端一次只會傳送一個開啟或關閉操作到 NFS 伺服器。若要解決這些問題，您可以執行下列任何動作：

- 您可以在同一個 Amazon EC2 執行個體上以不同的使用者 ID 執行個別程序。
- 您可以將所有開啟請求中的使用者 ID 保持不變，並改為修改一組群組 ID。
- 您可以從單獨的 Amazon EC2 執行個體執行每個程序。

自訂 NFS 設定造成寫入延遲

您擁有自訂的 NFS 用戶端設定，而 Amazon EC2 執行個體最多需要三秒鐘才能查看從另一個 Amazon EC2 執行個體對檔案系統執行的寫入操作。

採取動作

如果您遭遇此問題，您可以使用下列其中一種方法解決：

- 如果 Amazon EC2 執行個體上讀取資料的 NFS 用戶端已啟用屬性快取，請卸載您的檔案系統。然後透過 `noac` 選項將其重新掛載，以停用屬性快取。NFSv4.1 的屬性快取預設為啟用。

  > **Note**
  >
  > 停用用戶端快取可能會降低應用程式效能。

- 您也可以使用相容於 NFS 程序的程式設計語言以隨需清除屬性快取。若要執行此操作，您可以在讀取請求之前立即傳送 `ACCESS` 程序請求。

  例如，使用 Python 程式設計語言，您可以建構下列呼叫。

  ```
  # Does an NFS ACCESS procedure request to clear the attribute cache, given a path to
   the file
  import os
  os.access(path, os.W_OK)
  ```

使用 Oracle Recovery Manager 建立備份比較慢

如果 Oracle Recovery Manager 在開始備份任務之前暫停了 120 秒，則使用 Oracle Recovery Manager 建立備份可能較慢。

採取動作

如果您遭遇此問題，請參閱 Oracle 說明中心 (Oracle Help Center) 中的啟用和停用 NFS 的 Direct NFS 用戶端控制來停用 Oracle Direct NFS。

> **Note**
>
> Amazon EFS 不支援 Oracle Direct NFS。

AMI 與核心問題疑難排解

當使用 Amazon EC2 執行個體的 Amazon EFS 時，您可透過下列資訊來排解與特定 Amazon Machine Image (AMI) 或核心版本相關的問題。

主題

無法進行 chown

您無法使用 Linux chown 命令變更檔案/目錄的擁有權。

具有此錯誤的核心版本

2.6.32

採取動作

您可以執行以下動作以解決錯誤：

- 如果您要為必要的一次性設定步驟執行 chown 以變更 EFS 根目錄的擁有權，您可以從執行較新核心的執行個體執行 chown 命令。例如，使用最新版的 Amazon Linux。
- 如果 chown 是您的生產工作流程的一部分，您必須更新核心版本以使用 chown。

由於用戶端錯誤造成檔案系統重複保持執行操作

由於用戶端錯誤造成的檔案系統停滯於執行重複操作。

採取動作

將用戶端軟體更新到最新版本。

死鎖的用戶端

變為死鎖的用戶端。

具有此錯誤的核心版本

- 使用 Linux 3.10.0-229.20.1.el7.x86_64 核心的 CentOS-7
- 使用 Linux 4.2.0-18-generic 核心版本的 Ubuntu 15.10

採取動作

執行以下任意一項：

- 升級到較新的核心版本。針對 CentOS-7，Linux 3.10.0-327 或更新版本的核心包含了修正。
- 降級到較舊的核心版本。

在大型目錄中列出檔案需要很長的時間

如果您的 NFS 用戶端在逐一查看目錄以完成清單操作時，目錄正在更改，則可能發生這種情況。在此重複期間，不論 NFS 用戶端是否注意到目錄的內容變更，NFS 用戶端都會從頭再次啟動逐一查看。因此，檔案變更頻繁的大型目錄 ls 命令可能需要很長的時間才能完成。

具有此錯誤的核心版本

低於 2.6.32-696.el6 的 CentOS 及 RHEL 核心版本

採取動作

若要解決這個問題，請升級到較新的核心版本。

備份 Amazon EFS 檔案系統

AWS Backup 這是一種簡單且經濟實惠的方式，可透過備份 Amazon EFS 檔案系統來保護您的資料。AWS Backup 是一種統一的備份服務，旨在簡化備份的建立、遷移、還原和刪除作業，同時提供更好的報告和稽核功能。 AWS Backup 可以更輕鬆地制定集中式備份策略，以實現法律、法規和專業合規性。 AWS Backup 同時提供一個集中的位置，讓您可以執行下列作業，讓保護 AWS 儲存磁碟區、資料庫和檔案系統變得更加簡單：

- 設定及稽核您要備份的 AWS 資源
- 自動化備份排程
- 設定保留政策
- 監控所有最近的備份與還原活動

Amazon EFS 與原生整合 AWS Backup。您可以使用 EFS 主控台、API 和 AWS Command Line Interface (AWS CLI) 為檔案系統啟用自動備份。自動備份使用預設備份計畫，其中包含 AWS Backup 建議的自動備份設定。如需詳細資訊，請參閱 自動備份。您也可 AWS Backup 以使用手動設定自己的備份計畫，在其中指定備份頻率、備份時間、保留備份的時間長度，以及備份的生命週期原則。接著，您可以指派 Amazon EFS 檔案系統或其他 AWS 資源至該備份計畫。

增量備份

AWS Backup 執行 EFS 檔案系統的增量備份。在初始備份期間，會製作整個檔案系統的副本。而在該檔案系統的後續備份期間，只會複製已變更、新增或移除的檔案和目錄。對於每個增量備份， AWS Backup 保留必要的參考資料，以便進行完整還原。這個方法無須複製所有資料，可大幅減少完成備份所需的時間，並節省儲存成本。

備份一致性

Amazon EFS 專門設計來提供高可用性。當 Amazon EFS 正在 AWS Backup進行您的備份時，您可以同時存取和修改您的 Amazon EFS 檔案系統。不過，如果您在備份進行中對檔案系統進行修改，可能會發生不一致的情形 (例如重複、有誤差或被排除的資料)。修改行為包括寫入、重新命名、移動或刪除操作。為確保備份一致性，我們建議您在備份進行中暫停會修改檔案系統的應用程式或處理程序。或者，將備份排程在不會修改檔案系統的時段進行。

Backup 效能

通常，您可以期望使用以下備份和還原速率 AWS Backup。對於某些工作負載，例如包含大型檔案或目錄的工作負載，速率可能會較低。

- 每秒 1,000 個檔案或每秒 300 MB 的 Backup 速率，以較慢者為準。
- 每秒 500 個文件或 150 兆比特的恢復速率，以較慢者為準。

備份作業的最長持續時間 AWS Backup 為 30 天。

使用 AWS Backup 不會消耗累積的突發積分，而且不會計入一般用途效能模式檔案作業限制。如需詳細資訊，請參閱 Amazon EFS 檔案系統配額。

備份完成時段

您可以選擇指定備份的完成時段。這個時段定義備份需完成的期間。如果指定完成時段，請務必考慮預期的效能以及檔案系統的大小和組成。這樣做可協助確保您的備份可以在時段內完成。

未在指定時段內完成的備份，會標記為未完成狀態。在下次排定的備份期間，會在離開的時間點 AWS Backup 繼續執行。您可以在AWS Backup 管理主控台中查看所有備份的狀態。

EFS 儲存類別

您可以用 AWS Backup 來備份 EFS 檔案系統中的所有資料，無論資料所在的儲存類別為何。當備份已啟用生命週期管理且在 Infrequent Access (IA) 或「封存」儲存類別中有資料的 EFS 檔案系統時，您不需支付資料存取費用。

當還原復原點時，所有檔案都會還原到標準的儲存類別。如需儲存類別的詳細資訊，請參閱EFS 儲存類別和管理檔案系統儲存。

適用於建立和還原備份的 IAM 許可

您可以使用 `elasticfilesystem:backup` 和 `elasticfilesystem:restore` 動作來支援或拒絕 IAM 實體 (如使用者、群組或角色)，才可建立或還原 EFS 檔案系統備份。您可以在檔案系統政策或基於身分的 IAM 政策中使用這些動作。如需詳細資訊，請參閱 Amazon Elastic File System 的身分與存取管理 及 使用 IAM 控制檔案系統資料存取。

隨需備份

使用AWS Backup 管理主控台 或 CLI，可以視需求將單一資源儲存到備份保存庫。跟排程備份不同的是，您不需要建立備份計畫即可啟動隨需備份。您仍然可以指派生命週期給您的備份，這會自動將復原點移到冷儲存層，並記下何時刪除它。

並行備份

AWS Backup 將備份限制為每個資源一個並行備份。因此，如果備份任務已在進行中，那麼可能無法排程或隨需備份。如需有關 AWS Backup 配額的詳細資訊，請參閱《AWS Backup 開發人員指南》中的 AWS Backup 限制。

自動備份

使用 Amazon EFS 主控台建立檔案系統時，依預設會開啟自動備份。您可以在使用 CLI 或 API 建立檔案系統後開啟自動備份。預設 EFS 備份計劃會使用 AWS Backup 建議的自動備份設定，也就是每日備份，保留期為 35 天。使用預設 EFS 備份計畫建立的備份會儲存在預設 EFS 備份保存庫中，EFS 也會代表您建立該保存庫。無法刪除預設備份計畫和備份保存庫。您可以使用 AWS Backup 主控台編輯預設備份計畫設定。如需詳細資訊，請參閱《AWS Backup 開發人員指南》中的選項 3：建立自動備份。您可以查看所有自動備份，並使用AWS Backup 主控台編輯預設 EFS 備份計劃設定。您可以隨時使用 Amazon EFS 主控台或 CLI 關閉自動備份，如下節所述。

啟用自動備份時，Amazon EFS 會將值為 `enabled` 的 `aws:elasticfilesystem:default-backup` 系統標籤索引鍵應用至 EFS 檔案系統。

> **Note**
>
> 自動備份會從 AWS Backup 服務選擇退出組態中排除。如需詳細資訊，請參閱《AWS Backup 開發人員指南》中的開始使用 AWS Backup。

開啟或關閉現有檔案系統的自動備份

建立檔案系統後，您可以使用主控台、CLI 或 EFS API 來開啟或關閉自動備份。

開啟或關閉現有檔案系統 (主控台) 的自動備份

1. 前往 https://console.aws.amazon.com/efs/ 開啟 Amazon Elastic File System 主控台。

2. 在檔案系統頁面中，選擇您要開啟或關閉自動備份的檔案系統，並顯示檔案系統詳細資訊頁面。
3. 在一般設定面板中選擇編輯。
4. • 若要開啟自動備份，請選取啟用自動備份。
   • 若要關閉自動備份，請清除啟用自動備份。
5. 選擇儲存變更。

開啟或關閉現有檔案系統 (CLI) 的自動備份

- 使用 `put-backup-policy` CLI 命令 (對應的 API 操作為 PutBackupPolicy) 開啟或關閉現有檔案系統的自動備份。
  - 使用以下命令開啟自動備份。

```
$ aws efs put-backup-policy --file-system-id fs-01234567 \
--backup-policy Status="ENABLED"
```

EFS 采用新備份政策。

```
{
   "BackupPolicy": {
      "Status": "ENABLING"
   }
}
```

  - 使用以下命令關閉自動備份。

```
$ aws efs put-backup-policy --file-system-id fs-01234567 \
--backup-policy Status="DISABLED"
```

EFS 采用新備份政策。

```
{
   "BackupPolicy": {
      "Status": "DISABLING"
   }
}
```

用 AWS Backup 來手動設定備份

當您使 AWS Backup 用手動設定檔案系統備份時，您必須先建立備份計畫。備份計畫定義備份排程、備份時段、保留政策、生命週期政策和標籤。您可以使用AWS Backup 管理主控台 AWS CLI、或 AWS Backup API 建立備份計劃。在備份計畫中，您可以定義下列項目：

- 排程：備份的發生時機
- 備份時段：備份必須啟動的時段
- 生命週期：何時將復原點移至冷儲存，以及何時將其刪除
- 備份保存庫：哪一個保存庫可用來組織備份規則建立的復原點。

建立好備份計畫後，使用標籤或 Amazon EFS 檔案系統 ID 將特定的 Amazon EFS 檔案系統指派給備份計畫。指派計畫後， AWS Backup 會根據您定義的備份計畫，開始代表您自動備份 Amazon EFS 檔案系統。您可以使用主 AWS Backup 控台管理備份組態或監視備份活動。如需詳細資訊，請參閱《AWS Backup 開發人員指南》。

> **Note**
>
> 不支援通訊埠和具名管道，會從備份中省略這兩項。

還原復原點

使用 AWS Backup 主控台或 CLI 時，您可以將復原點還原至新的 EFS 檔案系統或現有檔案系統。您可以執行還原整個檔案系統的完整還原。或者，您可以使用部分還原來還原特定檔案和目錄。若要還原特定檔案或目錄，您必須指定與掛載點相關的相對路徑。例如，如果檔案系統是掛載到 `/user/home/myname/efs`，且檔案路徑為 `user/home/myname/efs/file1`，請輸入 `/file1`。路徑區分大小寫，不能包含特殊字元、萬用字元和規則表達式 (regex) 字串。

> **Note**
>
> 若要還原復原點，使用者必須擁有該 `backup:StartRestoreJob` 權限。

當您執行「完整」或「部分」還原時，您的復原點會還原到還原目錄 `aws-backup-restore_`*`timestamp-of-restore`* 中。還原完成後，您可以在檔案系統的根目錄看到還原目錄。如果您嘗試針對相同的路徑進行多次還原，則可能存在數個包含已還原項目的目錄。如果還原無法

完成，您會看到目錄 aws-backup-failed-restore_*timestamp-of-restore*。您必須在使用 restore 和 failed-restore 目錄時手動刪除它們。

> **Note**
>
> 對於部分還原至現有 EFS 檔案系統，請將檔案和目錄 AWS Backup 還原至檔案系統根目錄下的新目錄。指定項目的完整階層會保留在復原目錄中。例如，如果目錄 A 包含子目錄 B、C 和 D，則在復原 A、B、C 和 D 時 AWS Backup 保留階層結構。

還原復原點後，無法還原到適當目錄的資料片段會放置到 aws-backup-lost+found 目錄中。如果備份進行的同時對檔案系統進行了修改，片段便可能移到這個目錄。

刪除備份

預設的 EFS 備份保存庫存取政策設定為拒絕刪除復原點。若要刪除 EFS 檔案系統的現有備份，您必須變更保存庫存取政策。如果嘗試在不修改保存庫存取政策的情況下刪除 EFS 復原點，您會收到下列錯誤訊息：

```
"Access Denied: Insufficient privileges to perform this action. Please consult with the
 account administrator for necessary permissions."
```

若要編輯預設的備份保存庫存取政策，您必須擁有編輯政策的權限。如需詳細資訊，請參閱《IAM 使用者指南》中的允許所有 IAM 動作 (管理員存取)。

若要在中刪除 EFS 復原點 AWS Backup

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在左導覽窗格中，選擇備份文件庫。
3. 在備份保存庫清單中，選擇 aws/efs/automatic-backup-vault。
4. 在保存庫詳細資料頁面上，選擇頁面右上角的管理存取。編輯存取政策頁面隨即出現。
5. 若要允許 EFS 備份保存庫上的所有動作，請在 JSON 編輯器中找到 "Effect": "Deny", 行，然後將該行編輯為讀取 "Effect": "Allow",。
6. 選擇儲存政策以儲存變更。
7. 在保存庫詳細資訊頁面上，向下滾動至備份區段，然後從備份清單中選取要刪除的復原點。選擇動作，然後選擇刪除。

8. 依照說明確認刪除。然後選擇刪除恢復點。

複寫檔案系統

您可以根據自己的偏好建立 EFS 檔案系統 AWS 區域 的複本。在 EFS 檔案系統上啟用複寫時，Amazon Elastic File System (Amazon EFS)會自動、透明地將來源檔案系統上的資料和中繼資料複寫到目的地檔案系統。如果發生災難或在執行遊戲日練習時，您可以容錯移轉至複本檔案系統，然後容錯移轉回至主要檔案系統以繼續操作。為了管理建立目的地檔案系統並使其與來源檔案系統保持同步的程序，Amazon EFS 使用複寫組態。如需關於建立檔案系統複寫組態的詳細資訊，請參閱 複寫組態。

為檔案系統建立複寫組態後，Amazon EFS 會自動同步來源和目的地檔案系統。對來源檔案系統所做的變更不會以一 point-in-time 致的方式傳輸到目的地檔案系統，而是根據複製的上次同步時間傳輸。上次同步時間會指出來源與目的地之間上次成功同步的完成時間。從上次同步時間開始，對來源檔案系統所做的變更會複寫到目的地檔案系統中，而在上次同步時間之後對來源檔案系統所做的變更可能不會複寫到目的地檔案系統中。如需詳細資訊，請參閱 監控複寫狀態。

可在所有 EFS AWS 區域 中使用複寫。若要在預設停用的區域中使用複寫，您必須先選擇加入區域。如需詳細資訊，請參閱《AWS 一般參考指南》中的管理 AWS 區域。如果您稍後選擇退出某個區域，Amazon EFS 會暫停該區域的所有複寫活動。若要繼續該區域的複寫活動，您需要再次選擇加入 AWS 區域。

> **Note**
>
> 複寫不支援將標籤用於屬性型存取控制 (ABAC)。

主題

複寫組態

當您為檔案系統建立複寫組態時，可以選擇在其中建立複寫的 AWS 區域 區域，以及選擇是否要複寫到新的或現有的目的地檔案系統。

> **Note**
>
> 檔案系統只是複寫組態的一部分。您無法在另一個複寫組態中使用目的地檔案系統作為來源檔案系統。

複寫到新檔案系統

Amazon EFS 會自動建立新的檔案系統，並將來源檔案系統上的資料和中繼資料複製到您選擇的新唯讀目標檔案系統。 AWS 區域 建立具備下列屬性的目的地檔案系統：

- 檔案系統類型：檔案系統類型決定了 Amazon EFS 檔案系統存放在 AWS 區域中資料的可用性和耐久性。
  - 選擇區域以建立檔案系統，實現以備援方式將資料和中繼資料存放於 AWS 區域中的所有可用區域中。
  - 選擇單區域建立一個檔案系統，以備援方式將資料和中繼資料存儲於一個單獨的可用區域內。

  如需建立檔案系統類型的詳細資訊，請參閱 EFS 檔案系統類型。
- 加密：所有目的地檔案系統都會在啟用靜態加密的情況下建立。您可以指定用來加密目的檔案系統的 AWS Key Management Service (AWS KMS) 金鑰。如不指定 KMS 金鑰，則會使用 Amazon EFS 的服務管理 KMS 金鑰。

  > **Important**
  >
  > 建立目的地檔案系統之後，您無法變更 KMS 金鑰。

- 自動備份：對於使用單區域儲存的目的地檔案系統，預設會啟用自動備份。建立檔案系統之後，您可以變更自動備份設定。如需更多資訊，請參閱自動備份
- 效能模式 — 目的檔案系統的效能模式與來源檔案系統的模式相符，除非目的檔案系統使用單一區域儲存。在這種情況下，會使用「一般用途效能」模式。無法變更效能模式。
- 輸送量模式 — 目的地檔案系統的輸送量模式與來源檔案系統的輸送量模式相符。建立檔案系統之後，您可以修改模式。

  如果來源檔案系統的輸送量模式為「已佈建」，則目的檔案系統的佈建輸送量會符合來源檔案系統的輸送量，除非來源檔案的佈建量超過目的地檔案系統區域的限制。如果來源檔案系統的佈建量超過目

的地檔案系統的區域限制，則目的地檔案系統的佈建輸送量為區域限制量。如需詳細資訊，請參閱 您可以提高的 Amazon EFS 配額。

- 生命週期管理 — 未在目標檔案系統上啟用生命週期管理。建立目的地檔案系統之後，您可以將其啟用。如需詳細資訊，請參閱 管理檔案系統儲存。

複寫到現有的檔案系統中

EFS 會將來源檔案系統上的資料和中繼資料複寫到您選擇的目的 AWS 區域 檔案系統。複寫期間，EFS 會識別檔案系統之間的資料差異，並將差異套用至目的地檔案系統。

複寫至現有檔案系統時，適用下列需求。

- 必須停用目的地檔案系統的複寫覆寫保護。此複寫覆寫保護可防止檔案系統用作複寫組態中的目的地。如需關於停用保護的詳細資訊，請參閱 檔案系統保護。

  停用複寫覆寫保護需要彈性檔案系統:UpdateFileSystemProtection 動作的權限。如需詳細資訊，請參閱 AWS受管理的策略： AmazonElasticFileSystemFullAccess。

- 如果來源檔案系統已加密，則目的地檔案系統也必須加密。此外，如果來源檔案未加密且目的地檔案系統已加密，則在執行容錯移轉之後，您將無法復原至來源目的地。如需加密的詳細資訊，請參閱 Amazon EFS 的資料加密。

檔案系統保護

建立 Amazon EFS 檔案系統時，預設會啟用其複寫覆寫保護。此複寫覆寫保護可防止檔案系統用作複寫組態中的目的地。您必須先停用保護，才能使用檔案系統做為複寫組態中的目的地。如果您刪除複寫組態，那麼檔案系統的複寫覆寫保護會重新啟動，且檔案系統變為可寫入。

停用複寫覆寫保護需要有 `elasticfilesystem:UpdateFileSystemProtection` 動作的權限。如需詳細資訊，請參閱 AWS受管理的策略： AmazonElasticFileSystemFullAccess。

Amazon EFS 檔案系統的複寫覆寫保護狀態可以具有下列資料表所述的一個狀態值。

檔案系統狀態	描述
ENABLED	檔案系統不能在複寫組態中作爲目的地檔案系統。檔案系統可寫入。複寫覆寫保護預設為 ENABLED。
DISABLED	檔案系統能在複寫組態中作爲目的地檔案系統。
複寫	檔案系統正在複寫組態中用作目的地檔案系統。檔案系統為只讀，只有 Amazon EFS 在複寫期間才能修改。

停用複寫覆寫保護 (主控台)

1. 登入 AWS Management Console 並開啟 Amazon EFS 主控台，網址為 https://console.aws.amazon.com/efs/。
2. 在左側導覽窗格中選擇檔案系統。
3. 在檔案系統清單中，選擇您要在複寫組態中用作目的地檔案系統的 Amazon EFS 檔案系統。
4. 在檔案系統保護區段中，關閉複寫覆寫保護。

必要許可

Amazon EFS 使用名為的 `AWSServiceRoleForAmazonElasticFileSystem` 服務連結角色來同步來源檔案系統和目的地檔案系統之間的複寫狀態。若要使用 EFS 複寫，您必須設定下列許可，以允許 IAM 實體 (如使用者、群組或角色) 建立服務連結角色、複寫組態和檔案系統。

- `elasticfilesystem:CreateReplicationConfiguration`*
- `elasticfilesystem:DeleteReplicationConfiguration`*
- `elasticfilesystem:DescribeFileSystem`
- `elasticfilesystem:DescribeReplicationConfigurations`*
- `elasticfilesystem:CreateFileSystem`*
- `iam:CreateServiceLinkedRole`：請參閱 使用 Amazon EFS 的服務連結角色 中範例。

> **Note**
>
> * 您可以改用受 `AmazonElasticFileSystemFullAccess` 管政策來自動取得所有必要的 EFS 權限。如需詳細資訊，請參閱 AWS受管理的策略：AmazonElasticFileSystemFullAccess。

成本

為了方便複寫，Amazon EFS 會在目的地檔案系統上建立隱藏目錄和中繼資料。這些資料大約相當於 12 MiB 的計量付費資料，您要為這些資料付費。如需關於計量檔案系統的詳細資訊，請參閱 計量：Amazon EFS 如何報告檔案系統和物件大小。

效能

當您在容錯恢復過程中建立新複寫或改變現有複寫方向時，Amazon EFS 會執行初始同步，其中包括一系列一次性設定動作以支援複寫。完成初始同步所需的時間長短取決於很多因素，例如來源檔案系統的大小以及其中的檔案數目。

初始複寫完成後，Amazon EFS 會對大多數檔案系統維持 15 分鐘的復原點目標 (RPO)。但是，如果來源檔案系統的檔案變更頻繁，而且檔案量超過 1 億個或檔案大小超過 100 GB，則複寫時常可能超過 15 分鐘。如需關於監視上次成功完成複寫的時長的相關資訊，請參閱 監控複寫狀態。

您可以使用主控台 AWS Command Line Interface (AWS CLI)、API 和 Amazon 監控上次成功同步的時間 CloudWatch。在中 CloudWatch，使用 TimeSinceLastSyncEFS 量度。如需詳細資訊，請參閱 監控複寫狀態。

掛載目的地檔案系統

Amazon EFS 在建立目的地檔案系統時不會建立任何掛載目標。若要掛載目的地檔案系統，您必須建立一或多個掛載目標。如需更多資訊，請參閱使用 EFS 掛載協助程式掛載 EFS 檔案系統

因為目的地檔案系統為只讀，且其是複寫組態成員，所以任何寫入其中的操作都會失敗。但是，您可以將目的地檔案系統用於只讀使用案例，包括測試和開發。

檔案系統容錯移轉和容錯恢復

如果發生災難或執行遊戲日練習，您可以刪除複本檔案系統的複寫組態，以容錯移轉至複本檔案系統。刪除複寫組態之後，複本會變成可寫入，因此您可以在應用程式工作流程中開始使用該複本。當災難緩

解或遊戲日練習結束時，您可以繼續使用複本作為主要檔案系統，或者您可以執行容錯恢復以繼續原始主要檔案系統上的操作。

在容錯恢復程序期間，您可以選擇捨棄對複本檔案系統所做的變更，或通過將變更複寫回主檔案系統來保留這些變更。

- 若要在容錯移轉期間捨棄對複本所做的變更，請在主要檔案系統上重新建立原始複寫組態，其中複本檔案系統是複寫的目標。在複寫期間，Amazon EFS 會通過更新複本檔案系統資料來同步檔案系統，以便匹配主檔案系統。
- 若要在容錯移轉期間複寫對複本所做的變更，請在複本檔案系統上建立複寫組態，其中主檔案系統是複寫的目標。複寫期間，Amazon EFS 會識別複本檔案系統的差異，並將其傳輸回主檔案系統。複寫完成後，您可以重新建立原始複寫組態或建立新組態來繼續複寫主要檔案系統。

Amazon EFS 完成複寫程序所需的時間會有所不同，並且視檔案系統的大小及其中的檔案數目等因素而定。如需詳細資訊，請參閱 效能。

建立一個複寫組態

您可以使用 Amazon EFS 主控台、API 或複寫 EFS 檔案系統。 AWS CLI 以下各節提供使用上述每種方法的詳細說明。

建立複寫組態 (主控台)

1. 登入 AWS Management Console 並開啟 Amazon EFS 主控台，網址為 https://console.aws.amazon.com/efs/。
2. 開啟下列您要複寫的檔案系統：
   a. 在左側導覽窗格中選擇檔案系統。
   b. 在檔案系統清單中，選擇您要複寫的 Amazon EFS 檔案系統。您選擇的檔案系統不能是現有複寫組態中的來源或目的地檔案系統。
3. 選擇複寫索引標籤，然後在複寫區段中選擇建立複寫。建立複寫頁面隨即開啟。
4. 在複寫設定區段中，定義複寫設定：
   a. 對於複寫組態，請選擇是否要將檔案系統複寫到新的或現有的檔案系統中。
   b. 在「目的地」 AWS 區域 中 AWS 區域，選擇要複製檔案系統的位置。
5. 如果您要複寫到新的目的檔案系統，請在目的地檔案系統設定區段中定義目的地檔案系統設定。

a. 針對檔案系統類型，選擇檔案系統的儲存選項。

- 若要建立一個檔案系統，以冗餘方式將資料儲存在多個地理位置分隔的可用區域 AWS 區域，請選擇 [地區]。
- 若要建立以冗餘方式將資料儲存在單一可用區域中的檔案系統 AWS 區域，請選擇 [一個區域]，然後選取 [可用區域]。

如需詳細資訊，請參閱 EFS 檔案系統類型。

> **Note**
>
> 在 Amazon EFS 可用的 AWS 區域 區域的所有可用區域中，單區域不可用。

b. 對於加密，目的地檔案系統會自動啟用靜態資料加密。依預設，EFS 會為 Amazon EFS (`aws/elasticfilesystem`) 使用 AWS Key Management Service (AWS KMS) 服務金鑰。若要使用不同的 KMS 金鑰，請選擇 KMS 金鑰或為現有金鑰輸入 ARN。

> **Important**
>
> 建立目的地檔案系統之後，您無法變更 KMS 金鑰。

6. 如果正在複寫到現有的目的地檔案系統，請選擇瀏覽 EFS，然後選取檔案系統。目的地檔案系統的路徑出現在目的地方塊中。

   如果在檔案系統上啟用複寫覆寫保護，則屏幕會顯示警告，提示您停用保護。若要停用保護，請選擇停用保護，然後關閉複寫覆寫保護。停用保護之後，點擊重新整理按鈕，清除訊息。

7. 選擇建立複寫。如果您要複寫到新檔案系統中，則屏幕會顯示一則訊息，要求您確認複寫。在輸入方塊中輸入確認，然後點擊建立複寫。

   此時屏幕會顯示複寫區段，並顯示複寫詳細資訊。複寫狀態初始值為啟用，且上次同步為空白。狀態顯示為已啟用后，上次同步會顯示初始同步處理。

8. 若要查看目的地檔案系統的組態資訊，請在目的地檔案系統上方選擇檔案系統 ID。目的地檔案系統的檔案系統詳細資訊頁面會顯示在新瀏覽器索引標籤中 (具體依據您的瀏覽器設定)。

建立複寫組態 (主控台)

使用 `create-replication-configuration` 命令來建立複寫組態。等效 API 命令為 CreateReplicationConfiguration。

Example ：建立區域目的地檔案系統的複寫組態

以下範例是為檔案系統 *fs-0123456789abcdef1* 建立的複寫組態。此範例使用Region參數在中建立目標檔案系統*eu-west-2* AWS 區域。加密目的地檔案系統時，KmsKeyId 參數會指定要使用的 KMS 金鑰 ID。

```
aws efs create-replication-configuration \
--source-file-system-id fs-0123456789abcdef1 \
--destinations "[{\"Region\":\"eu-west-2\", \"KmsKeyId\":\"arn:aws:kms:us-
east-2:111122223333:key\/abcd1234-ef56-ab78-cd90-1111abcd2222\"}]"
```

回 AWS CLI 應如下：

```
{
    "SourceFileSystemArn": "arn:aws:elasticfilesystem:us-east-1:111122223333:file-
system/fs-0123456789abcdef1",
    "SourceFileSystemRegion": "us-east-1",
    "Destinations": [
        {
            "Status": "ENABLING",
            "FileSystemId": "fs-0123456789abcde22",
            "Region": "eu-west-2"
        }
    ],
    "SourceFileSystemId": "fs-0123456789abcdef1",
    "CreationTime": 1641491892.0,
    "OriginalSourceFileSystemArn": "arn:aws:elasticfilesystem:us-
east-1:111122223333:file-system/fs-0123456789abcdef1"
}
```

Example ：建立單區域目的地檔案系統的複寫組態

以下範例是為檔案系統 *fs-0123456789abcdef1* 建立的複寫組態。此範例使用 AvailabilityZoneName 參數在 *us-west-2a* 的可用區域中建立單區域目的地檔案系統。由於未指定 KMS 金鑰，因此會使用帳戶的 Amazon EFS 預設 AWS KMS 服務金鑰加密目的地檔案系統 (aws/elasticfilesystem)。

```
aws efs create-replication-configuration \
--source-file-system-id fs-0123456789abcdef1 \
--destinations AavailabilityZoneName=us-west-2a
```

檢視多個複寫組態

若要查看檔案系統的複寫組態，您可以使用 Amazon EFS 主控台或 AWS CLI。

檢視複寫組態 (主控台)

1. 前往 https://console.aws.amazon.com/efs/ 開啟 Amazon Elastic File System 主控台。
2. 在左側導覽窗格中選擇檔案系統。
3. 從清單中選擇檔案系統。
4. 選擇複寫索引標籤，顯示複寫區段。

   在複寫區段中，您可以看到複寫組態的下列資訊：

   - 複寫狀態可能是啟用、已啓用、刪除、暫停、已暫停或錯誤。

     建立複寫組態之後，因為選擇退出來源或目標區域，系統會出現「暫停」狀態。若要繼續複寫檔案系統，您需要再次選擇加入 AWS 區域。如需詳細資訊，請參閱《AWS 一般參考指南》中的管理 AWS 區域。

     複寫狀態會在複寫建立后顯示出來，同時檔案系統會做為來源或目的地檔案系統。

     當來源檔案系統或目的檔案系統 (或兩者) 處於故障狀態且無法復原時，系統會顯示「錯誤」狀態。如需詳細資訊，請參閱 監控複寫狀態。若要還原，您必須刪除複寫組態，然後將故障檔案系統 (來源或目的地) 的最新備份還原至新檔案系統中。
   - 複寫方向顯示資料正在複寫的方向。列出的第一個檔案系統是資料來源，其資料會複寫到列出的第二個檔案系統中，即目的地檔案系統。
   - 上次同步顯示上次成功同步在目的地檔案系統上的時間。在此之前，對來源檔案系統上的資料所做的任何變更都會成功複寫到目的檔案系統中。在此之後，系統可能無法完全複寫發生的任何變更。
   - 複製檔案系統會依據檔案系統 ID、複製組態 (來源或目的地) 中的角色、所在位置及其權限，列出複製組態 AWS 區域 中的每個檔案系統。來源檔案系統具有可寫入的許可，而目的地檔案系統具有只讀許可。

檢視複寫組態 (主控台)

使用 describe-replication-configurations CLI 命令來檢視複寫組態。您可以檢視特定檔案系統或特 AWS 帳戶 定檔案系統的所有複製組態的複製組態 AWS 區域。等效 API 命令為 DescribeReplicationConfigurations。

若要檢視檔案系統的複寫組態，請使用 file-system-id URI 請參數。您可以指定來源檔案系統或目的地檔案系統的 ID。

```
aws efs describe-replication-configurations --file-system-id fs-0123456789abcdef1
```

```
{
    "Replications": [
        {
            "SourceFileSystemArn": "arn:aws:elasticfilesystem:eu-
west-1:111122223333:file-system/fs-abcdef0123456789a",
            "CreationTime": 1641491892.0,
            "SourceFileSystemRegion": "eu-west-1",
            "OriginalSourceFileSystemArn": "arn:aws:elasticfilesystem:eu-
west-1:111122223333:file-system/fs-abcdef0123456789a",
            "SourceFileSystemId": "fs-abcdef0123456789a",
            "Destinations": [
                {
                    "Status": "ENABLED",
                    "FileSystemId": "fs-0123456789abcdef1",
                    "Region": "us-east-1"
                }
            ]
        }
    ]
}
```

若要檢視中帳戶的所有複寫組態 AWS 區域，請勿指定file-system-id參數。

```
aws efs describe-replication-configurations
```

```
{
    "Replications": [
        {
            "SourceFileSystemArn": "arn:aws:elasticfilesystem:eu-
west-1:555555555555:file-system/fs-0123456789abcdef1",
```

```
            "CreationTime": 1641491892.0,
            "SourceFileSystemRegion": "eu-west-1",
            "OriginalSourceFileSystemArn": "arn:aws:elasticfilesystem:eu-
west-1:555555555555:file-system/fs-0123456789abcdef1",
            "SourceFileSystemId": "fs-0123456789abcdef1",
            "Destinations": [
                {
                    "Status": "ENABLED",
                    "FileSystemId": "fs-abcdef0123456789a",
                    "Region": "us-east-1",
                    "LastReplicatedTimestamp": 1641491802.375
                }
            ]
        },
        {
            "SourceFileSystemArn": "arn:aws:elasticfilesystem:eu-
west-1:555555555555:file-system/fs-021345abcdef6789a",
            "CreationTime": 1641491822.0,
            "SourceFileSystemRegion": "eu-west-1",
            "OriginalSourceFileSystemArn": "arn:aws:elasticfilesystem:eu-
west-1:555555555555:file-system/fs-021345abcdef6789a",
            "SourceFileSystemId": "fs-021345abcdef6789a",
            "Destinations": [
                {
                    "Status": "ENABLED",
                    "FileSystemId": "fs-012abc3456789def1",
                    "Region": "us-east-1",
                    "LastReplicatedTimestamp": 1641491823.575
                }
            ]
        }
    ]
}
```

刪除複寫組態

如果您需要容錯移轉至目的地檔案系統，請刪除該檔案系統所屬的複寫組態。刪除複寫組態之後，目的地檔案系統會變成可寫入，並重新啟用其複寫覆寫保護。如需詳細資訊，請參閱 檔案系統容錯移轉和容錯恢復。

刪除複寫組態並將目的地檔案系統變更為可寫入，可能需要幾分鐘的時間才能完成。刪除組態後，Amazon EFS 可能會使用下列命名慣例，將一些資料寫入目的地檔案系統根目錄中的 `lost+found` 目錄中：

```
efs-replication-lost+found-source-file-system-id-TIMESTAMP
```

> **Note**
>
> 您無法刪除屬於複製組態一部分的檔案系統。您必須先刪除複寫組態，才能刪除檔案系統。

您可以使用主控台、CLI 或 API 從來源或目的地檔案系統中刪除現有複寫組態。

刪除複寫組態 (主控台)

1. 前往 https://console.aws.amazon.com/efs/ 開啟 Amazon Elastic File System 主控台。
2. 在左側導覽窗格中選擇檔案系統。
3. 選擇複寫組態中要刪除的來源或目的地檔案系統。
4. 選擇複寫索引標籤，顯示複寫區段。
5. 選擇刪除複寫以刪除複寫組態。出現提示時，確認您的選擇。

刪除複寫組態 (CLI)

使用 `delete-replication-configuration` CLI 命令來刪除複寫組態。等效 API 命令為 DeleteReplicationConfiguration。

若要指定刪除的複寫組態，請使用 `source-file-system-id` 參數。

```
aws efs --region us-west-2 delete-replication-configuration \
--source-file-system-id fs-0123456789abcdef1
```

監控複寫狀態

您可以在複寫組態中監視上次成功同步處理完成的時間。在此之前，對來源檔案系統上的資料所做的任何變更都已經成功複寫到目的檔案系統中。在此之後，系統可能無法完全複寫發生的任何變更。若要監控上次成功完成複寫的時間，您可以使用主控台、CLI、API 或 Amazon CloudWatch。

- 在主控台中：在檔案系統詳細資訊中的上次同步屬性 > 複寫區段會顯示來源與目的地之間上次成功同步處理完成的時間。
- 在 CLI 或 API 中：`Destination` 物件中的 `LastReplicatedTimestamp` 屬性會顯示上次成功同步處理完成的時間。若要存取此屬性，請使用 `describe-replication-configurations` CLI 指令。DescribeReplicationConfigurations 與 API 操作等效。
- 輸入 CloudWatch — Amazon EFS 的`TimeSinceLastSync` CloudWatch指標會顯示自上次成功同步完成後經過的時間。如需詳細資訊，請參閱 Amazon EFS 的 Amazon CloudWatch 指標。

您也可以使用主控台、CLI 或 API 監視複寫組態的狀態。複寫組態可能會有下表中所述的狀態值。

複寫狀態	描述
ENABLED	複寫組態正常且可供使用。
ENABLING	Amazon EFS 正在建立複寫組態。
DELETING	Amazon EFS 正在刪除複寫組態以回應使用者啟動的刪除請求。
PAUSING	Amazon EFS 正在暫停複寫，因為複寫組態中的一個或兩個檔案系統選擇退出該區域。
PAUSED	暫停複寫，因為複寫組態中的一個或兩個檔案系統選擇退出該區域。若要繼續複寫，您需要再次選擇加入 AWS 區域。如需詳細資訊，請參閱《AWS 一般參考指南》中的管理 AWS 區域。
ERROR	複寫組態中的一個 (或兩個) 檔案系統處於故障狀態且無法復原。若要存取檔案系統資料，請將故障檔案系統的備份還原至新檔案系統中。如需更多詳細資訊，請參閱 還原復原點。

Amazon Elastic File System 演練

本區段提供您可以用於探索 Amazon EFS 和測試端對端設定的演練。

主題

逐步解說：建立 Amazon EFS 檔案系統，並使用 AWS CLI

本逐步解說使用 AWS CLI 來探索 Amazon EFS API。在此逐步解說中，您會建立加密 Amazon EFS 檔案系統，掛載在您 VPC 中的 Amazon EC2 執行個體，然後測試設定。

> **Note**
>
> 此逐步解說與入門練習相似。在 開始使用 練習中，您會使用主控台來建立 EC2 和 Amazon EFS 資源。在本逐步解說中，您可以使 AWS CLI 用執行相同的操作，主要是為了熟悉 Amazon EFS API。

在本逐步解說中，您會在帳戶中建立下列 AWS 資源：

- Amazon EC2 資源：
  - 兩個安全群組 (適用於您的 EC2 執行個體和 Amazon EFS 檔案系統)。

    您對安全群組新增規則以授予適當傳入/傳出存取權。這樣做可以藉由使用標準的 NFSv4.1 TCP 連接埠，透過掛載目標讓您的 EC2 執行個體連接到檔案系統。
  - 您 VPC 中的 Amazon EC2 執行個體。
- Amazon EFS 資源：

- 一個檔案系統。
- 適用您檔案系統的掛載目標。

  若要在 EC2 執行個體上掛載檔案系統，您需要在 VPC 中建立掛載目標。您可在 VPC 中的每個可用區域建立一個掛載目標。如需詳細資訊，請參閱 Amazon EFS 如何運作。

然後，您將在 EC2 執行個體上測試檔案系統。逐步解說最後的清理步驟將為您提供移除這些資源的資訊。

本逐步解說會在美國西部 (奧勒岡) 區域 (`us-west-2`) 中建立所有這些資源。無論 AWS 區域 您使用哪種方式，請務必始終如一地使用它。您的所有資源 VPC、EC2 資源和 Amazon EFS 資源必須在相同的 AWS 區域區域。

開始之前

- 您可以使用您的根憑證登 AWS 帳戶 入主控台，並嘗試入門練習。不過， AWS Identity and Access Management (IAM) 建議您不要使用 AWS 帳戶. 反之，在帳戶中建立一個管理員使用者並使用這些憑證來管理帳戶中的資源。反之，在帳戶中建立一個管理員使用者並使用這些憑證來管理帳戶中的資源。如需詳細資訊，請參閱使用指南中的為 IAM 身分中心使用AWS IAM Identity Center 者指派 AWS 帳戶 存取權限。
- 您可以使用預設 VPC 或在帳戶中建立的自訂 VPC。預設的 VPC 設定適用於此逐步解說。不過，如果您使用的是自訂 VPC，請檢查下列各項：
  - DNS 主機名稱已啟用。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的更新 VPC 的 DNS 支援。
  - 該網際網路閘道已連接至您的 VPC。如需詳細資訊，請參閱Amazon VPC 使用者指南中的網際網路閘道。
  - 該 VPC 子網路已設定為 VPC 子網路啟動的執行個體申請公有 IP 地址。如需詳細資訊，請參閱Amazon VPC 使用者指南中的您 VPC 中的 IP 定址。
  - 該 VPC 路由表包含傳送所有網際網路綁定型流量到網際網路閘道的規則。
- 您需要設置 AWS CLI 並添加管理員用戶配置文件。

正在設定 AWS CLI

請使用下列指示來設定 AWS CLI 和使用者設定檔。

若要設定 AWS CLI

1. 下載和設定 AWS CLI。如需說明，請參閱《AWS Command Line Interface 使用者指南》中的下列主題。

   使用 AWS 指令行介面進行設置

   安裝指 AWS 令行介面

   規劃指 AWS 令行介面

2. 設定設定檔。

   您可以將使用者認證儲存在 AWS CLI `config`檔案中。在此逐步解說中的範例 CLI 命令會指定 adminuser 設定檔。在 `config` 檔案中建立 adminuser 設定檔。您也可以在 `config` 檔案中將管理員使用者描述檔設為預設，如下所示。

   ```
   [profile adminuser]
   aws_access_key_id = admin user access key ID
   aws_secret_access_key = admin user secret access key
   region = us-west-2

   [default]
   aws_access_key_id = admin user access key ID
   aws_secret_access_key = admin user secret access key
   region = us-west-2
   ```

   上述設定檔也會設定預設值 AWS 區域。如果您不在 CLI 命令中指定區域，則將會採用 us-west-2 區域。

3. 在命令提示字元中輸入下列命令，以驗證設定。這些命令均不會明確提供登入資料，因此會使用預設描述檔的登入資料。

   - 嘗試 help 命令。

     您也可以透過新增 `--profile` 參數明確指定使用者描述檔。

     ```
     aws help
     ```

     ```
     aws help \
     --profile adminuser
     ```

下一步驟

步驟 1：建立 Amazon EC2 資源

步驟 1：建立 Amazon EC2 資源

請於本步驟執行以下操作：

- 建立兩個安全群組。
- 對安全群組新增規則以授予其他存取權。
- 啟動 EC2 執行個體。在後續步驟中，您將在此執行個體上建立並掛載一個 Amazon EFS 檔案系統。

主題

步驟 1.1：建立兩個安全群組

在此區段中，您將在 VPC 中為 EC2 執行個體和 Amazon EFS 掛載目標建立安全群組。稍後在逐步解說中，您將指派這些安全群組至 EC2 執行個體與 Amazon EFS 掛載目標。如需安全群組的相關資訊，請參閱適用於 Linux 執行個體的 Amazon EC2 安全群組。

建立安全群組

1. 使用 `create-security-group` CLI 命令建立兩個安全群組：

   a. 為您的 EC2 執行個體建立安全群組 (`efs-walkthrough1-ec2-sg`)，並提供您的 VPC ID。

   ```
   $ aws ec2 create-security-group \
   --region us-west-2 \
   --group-name efs-walkthrough1-ec2-sg \
   --description "Amazon EFS walkthrough 1, SG for EC2 instance" \
   --vpc-id vpc-id-in-us-west-2 \
   --profile adminuser
   ```

   記下該安全群組 ID。以下是回應範例。

```
{
    "GroupId": "sg-aexample"
}
```

您可使用下列命令來找到 VPC ID。

```
$ aws  ec2 describe-vpcs
```

b. 為您的 Amazon EFS 掛載目標建立安全群組 (`efs-walkthrough1-mt-sg`)。您需提供您的 VPC ID。

```
$ aws ec2 create-security-group \
--region us-west-2 \
--group-name efs-walkthrough1-mt-sg \
--description "Amazon EFS walkthrough 1, SG for mount target" \
--vpc-id vpc-id-in-us-west-2 \
--profile adminuser
```

記下該安全群組 ID。以下是回應範例。

```
{
    "GroupId": "sg-aexample"
}
```

2. 確認安全群組。

```
aws ec2 describe-security-groups \
--group-ids list of security group IDs separated by space \
--profile adminuser \
--region us-west-2
```

均應該只有一個讓所有流量離開的傳出規則。

在下一區段中，您將授權啟用下列項目的其他存取權：

- 讓您連接至您的 EC2 執行個體。
- 啟用 EC2 執行個體和 Amazon EFS 掛載目標之間的流量 (您會透過這些設定，在此逐步解說稍候關聯這些安全群組)。

步驟 1.2：對安全群組新增規則以授予傳入/傳出存取權

在此步驟中，您將對安全群組新增規則以授予傳入/傳出存取權。

新增規則

1. 為您的 EC2 執行個體 (efs-walkthrough1-ec2-sg) 授予對安全群組傳入 Secure Shell (SSH) 連接的權限，如此您便可從任何主機使用 SSH 連接到您的 EC2 執行個體。

   ```
   $ aws ec2 authorize-security-group-ingress \
   --group-id id of the security group created for EC2 instance \
   --protocol tcp \
   --port 22 \
   --cidr 0.0.0.0/0 \
   --profile adminuser \
   --region us-west-2
   ```

   驗證該安全群組已有您新增的傳入和傳出規則。

   ```
   aws ec2 describe-security-groups \
   --region us-west-2 \
   --profile adminuser \
   --group-id security-group-id
   ```

2. 對 Amazon EFS 掛載目標 (efs-walkthrough1-mt-sg) 授予安全群組的傳入存取權。

   在命令提示字元中，使用 adminuser 設定檔執行下列 AWS CLI authorize-security-group-ingress命令，以新增輸入規則。

   ```
   $ aws ec2 authorize-security-group-ingress \
   --group-id ID of the security group created for Amazon EFS mount target \
   --protocol tcp \
   --port 2049 \
   --source-group ID of the security group created for EC2 instance \
   --profile adminuser \
   --region us-west-2
   ```

3. 驗證現在兩個安全群組皆授權傳入存取權。

   ```
   aws ec2 describe-security-groups \
   --group-names efs-walkthrough1-ec2-sg   efs-walkthrough1-mt-sg \
   --profile adminuser \
   ```

```
--region us-west-2
```

步驟 1.3：啟動 EC2 執行個體

在此步驟中，您將啟動一個 EC2 執行個體。

啟動 EC2 執行個體

1. 收集以下所需資訊，以在啟動 EC2 執行個體時使用：

   - 金鑰對名稱：
     - 如需簡介資訊，請參閱設定為使用 Amazon EC2。
     - 如需建立 .pem 檔案的指示，請參閱 Amazon EC2 使用者指南中的建立金鑰配對。
   - 您要啟動之 Amazon Machine Image (AMI) 的 ID。

     您用來啟動 EC2 執行個體的 AWS CLI 命令需要您想要部署為參數的 AMI ID。本練習使用 Amazon Linux HVM AMI。

     > **Note**
     >
     > 您可以使用用途最廣泛、以 Linux 為基礎的 AMI。如果您使用其他 Linux AMI，請確保您是使用分發的套件管理員，在執行個體上安裝 NFS 用戶端。此外，您可能要視情況新增套裝軟體。

     對於 Amazon Linux HVM AMI，您可以在 Amazon Linux AMI 找到最新的 ID。您將從 Amazon Linux AMI ID 表格選擇 ID 值，如下所示：

     - 選擇 US West Oregon (美國西部奧勒岡) 區域。此逐步解說假設您正在美國西部 (奧勒岡) (us-west-2) 中建立所有資源。
     - 選擇 EBS-backed HVM 64-bit (EBS 後端 HVM 64 位元) 類型 (因為在 CLI 命令中，您將指定不支援執行個體存放區的 `t2.micro` 執行個體類型)。

   - 為 EC2 執行個體建立的安全群組 ID。
   - AWS 區域。此逐步解說使用了 us-west-2 區域。
   - 您想啟動執行個體的 VPC 子網路 ID。您可以使用 `describe-subnets` 命令取得子網路清單。

```
$ aws ec2 describe-subnets \
--region us-west-2 \
--filters "Name=vpc-id,Values=vpc-id" \
--profile adminuser
```

在您選擇子網路 ID 後，從 describe-subnets 結果中記下以下值：

- 子網路 ID：在建立掛載目標時，您會需要這個值。在本練習中，您會在啟動 EC2 執行個體的相同子網路中建立一個掛載目標。
- 子網路的可用區域：您需要此值來建構掛載目標 DNS 名稱，該名稱用於在 EC2 執行個體上掛載檔案系統。

2. 執行下列 AWS CLI run-instances命令以啟動 EC2 執行個體。

```
$ aws ec2 run-instances \
--image-id AMI ID \
--count 1 \
--instance-type t2.micro \
--associate-public-ip-address \
--key-name key-pair-name \
--security-group-ids ID of the security group created for EC2 instance \
--subnet-id VPC subnet ID \
--region us-west-2 \
--profile adminuser
```

3. 記下由 run-instances 命令傳回的執行個體 ID。
4. 您建立的 EC2 執行個體必須擁有公有 DNS 名稱，該名稱是用以連接並掛載檔案系統至 EC2 執行個體。公有 DNS 名稱為下列形式：

```
ec2-xx-xx-xx-xxx.compute-1.amazonaws.com
```

執行以下 CLI 命令並記下公有 DNS 名稱。

```
aws ec2 describe-instances \
--instance-ids EC2 instance ID \
--region us-west-2 \
--profile adminuser
```

如果您不尋找公有 DNS 名稱，請在您啟動 EC2 執行個體的 VPC 中檢查 VPC 組態。如需詳細資訊，請參閱 開始之前。

5. (選用) 將名稱指派給您建立的 EC2 執行個體。若要這樣做，新增具有金鑰名稱的標籤，並且將值設為您想要指派給執行個體的名稱。您可以執行下列 AWS CLI `create-tags`命令來執行此操作。

```
$  aws ec2 create-tags \
--resources  EC2-instance-ID \
--tags Key=Name,Value=Provide-instance-name  \
--region us-west-2 \
--profile adminuser
```

下一步驟

步驟 2：建立 Amazon EFS 資源

步驟 2：建立 Amazon EFS 資源

請於本步驟執行以下操作：

- 建立加密 Amazon EFS 檔案系統。
- 啟用生命週期管理。
- 在您已啟動 EC2 執行個體的可用區域中建立掛載目標。

主題

- 步驟 2.1：建立 Amazon EFS 檔案系統
- 步驟 2.2：啟用生命週期管理
- 步驟 2.3：建立掛載目標

步驟 2.1：建立 Amazon EFS 檔案系統

在此步驟中，您將建立一個 Amazon EFS 檔案系統。請記下 `FileSystemId`，以在下一步驟供檔案系統建立掛載目標時使用。

建立檔案系統

- 搭配可選的 `Name` 標籤，建立檔案系統。

  a. 在命令提示字元中，執行下列 AWS CLI `create-file-system` 命令。

```
$  aws efs create-file-system \
--encrypted \
--creation-token FileSystemForWalkthrough1 \
--tags Key=Name,Value=SomeExampleNameValue \
--region us-west-2 \
--profile adminuser
```

您會收到以下回應。

```
{
    "OwnerId": "111122223333",
    "CreationToken": "FileSystemForWalkthrough1",
    "FileSystemId": "fs-c657c8bf",
    "CreationTime": 1548950706.0,
    "LifeCycleState": "creating",
    "NumberOfMountTargets": 0,
    "SizeInBytes": {
        "Value": 0,
        "ValueInIA": 0,
        "ValueInStandard": 0
    },
    "PerformanceMode": "generalPurpose",
    "Encrypted": true,
    "KmsKeyId": "arn:aws:kms:us-west-2:111122223333:a5c11222-7a99-43c8-9dcc-
abcdef123456",
    "ThroughputMode": "bursting",
    "Tags": [
        {
            "Key": "Name",
            "Value": "SomeExampleNameValue"
        }
    ]
}
```

b. 請記下 FileSystemId 值。在步驟 2.3：建立掛載目標中，當您建立此檔案系統的掛載目標時，您將需要此值。

步驟 2.2：啟用生命週期管理

在此步驟中，您必須在檔案系統上啟用生命週期管理，才能使用不常存取的儲存類別。如需了解詳細資訊，請參閱 管理檔案系統儲存 和 EFS 儲存類別。

啟用生命週期管理

- 在命令提示字元中，執行下列 AWS CLI `put-lifecycle-configuration`命令。

```
$  aws efs put-lifecycle-configuration \
--file-system-id fs-c657c8bf \
--lifecycle-policies TransitionToIA=AFTER_30_DAYS \
--region us-west-2 \
--profile adminuser
```

您會收到以下回應。

```
{
  "LifecyclePolicies": [
    {
        "TransitionToIA": "AFTER_30_DAYS"
    }
  ]
}
```

步驟 2.3：建立掛載目標

在此步驟中，您將在啟動 EC2 執行個體的可用區域中，為您的檔案系統建立掛載目標。

1. 請務必備妥下列資訊：
   - 您欲建立掛載目標的檔案系統 ID (例如，`fs-example`)。
   - 您在步驟 1 中啟動 EC2 執行個體的 VPC 子網路 ID。

     在此逐步解說中，您將在啟動 EC2 執行個體的相同子網路中建立掛載目標，因此您需要子網路 ID (例如，`subnet-example`)。
   - 您在之前步驟中為掛載目標所建立的安全群組 ID。
2. 在命令提示字元中，執行下列 AWS CLI `create-mount-target`命令。

```
$ aws efs create-mount-target \
--file-system-id file-system-id \
--subnet-id  subnet-id \
--security-group ID-of-the security-group-created-for-mount-target \
```

```
--region us-west-2 \
--profile adminuser
```

您會收到以下回應。

```
{
    "MountTargetId": "fsmt-example",
    "NetworkInterfaceId": "eni-example",
    "FileSystemId": "fs-example",
    "PerformanceMode" : "generalPurpose",
    "LifeCycleState": "available",
    "SubnetId": "fs-subnet-example",
    "OwnerId": "account-id",
    "IpAddress": "xxx.xx.xx.xxx"
}
```

3. 您也可以使用 `describe-mount-targets` 命令來取得您在檔案系統上建立的掛載目標說明。

```
$ aws efs describe-mount-targets \
--file-system-id file-system-id \
--region us-west-2 \
--profile adminuser
```

下一步驟

步驟 3：在 EC2 執行個體上掛載檔案系統並進行測試

步驟 3：在 EC2 執行個體上掛載檔案系統並進行測試

請於本步驟執行以下操作：

主題

- 步驟 3.1：收集資訊
- 步驟 3.2：在您的 EC2 執行個體上安裝 NFS 用戶端
- 步驟 3.3：在您的 EC2 執行個體上掛載檔案系統並進行測試

步驟 3.1：收集資訊

在您遵照本區段中的步驟時，請確定您有下列資訊：

- 您 EC2 執行個體的公有 DNS 名稱格式如下：

```
ec2-xx-xxx-xxx-xx.aws-region.compute.amazonaws.com
```

- 您檔案系統的 DNS 名稱。您可以使用以下一般表單建構此 DNS 名稱：

```
file-system-id.efs.aws-region.amazonaws.com
```

使用該掛載目標來掛載檔案系統的 EC2 執行個體，可以解析檔案系統的 DNS 名稱至掛載目標的 IP 地址。

> **Note**
>
> Amazon EFS 不要求您的 Amazon EC2 執行個體擁有公有 IP 地址或公有 DNS 名稱。先前列出的要求僅適用於此逐步解說範例，以確保您能從 VPC 外部使用 SSH 連接到執行個體。

步驟 3.2：在您的 EC2 執行個體上安裝 NFS 用戶端

您可以從執行 Windows、Linux、macOS X 或任何其他 Unix 變體版本的電腦連接到 EC2 執行個體。

安裝 NFS 用戶端

1. 連線到您的 EC2 執行個體：

   - 若要從執行 macOS 或 Linux 的電腦連接至您的執行個體，可透過 `-i` 選項與私密金鑰路徑來指定 SSH 命令的 .pem 檔案。
   - 若要從執行 Windows 的電腦連線至執行個體，您可以使用 MindTerm 或 PuTTY。如果您計劃使用 PuTTY，則需要安裝它，然後使用下列程序將 .pem 檔案轉換為 .ppk 檔案。

   如需詳細資訊，請參閱 Amazon EC2 使用者指南中的下列主題：

   - 使用 PuTTY 從視窗 Connect 到您的 Linux 執行個體
   - 使用安全殼層從 Linux 或 macOS Connect 至您的 Linux 執行個體

2. 使用 SSH 工作階段在 EC2 執行個體上執行以下命令：

   a. (選用) 取得更新並重新啟動。

```
$  sudo yum -y update
$  sudo reboot
```

重新開機後，請重新連線至您的 EC2 執行個體。

b. 安裝 NFS 用戶端。

```
$ sudo yum -y install nfs-utils
```

> **Note**
>
> 在預設情況下，AMI 中已包含 `nfs-utils`，因此您在啟動 Amazon EC2 執行個體時選擇了 Amazon Linux AMI 2016.03.0 Amazon Linux AMI，便無須再安裝。

步驟 3.3：在您的 EC2 執行個體上掛載檔案系統並進行測試

現在，您將在您的 EC2 執行個體上掛載檔案系統。

1. 建立目錄 (「efs-mount-point」)。

```
$ mkdir ~/efs-mount-point
```

2. 掛載 Amazon EFS 檔案系統。

```
$ sudo mount -t nfs -o
 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport mount-target-DNS:/   ~/efs-mount-point
```

該 EC2 執行個體可解析掛載目標 DNS 名稱至 IP 地址。您可以選擇性的直接指定掛載目標 IP 地址。

```
$ sudo mount -t nfs -o
 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport mount-target-ip:/  ~/efs-mount-point
```

3. 您現在已在 EC2 執行個體上掛載了 Amazon EFS 檔案系統，您可以建立檔案。

   a. 變更該目錄。

```
$ cd ~/efs-mount-point
```

b. 列出該目錄內容。

```
$ ls -al
```

其應該保留為空。

```
drwxr-xr-x 2 root     root     4096 Dec 29 22:33 .
drwx------ 4 ec2-user ec2-user 4096 Dec 29 22:54 ..
```

c. 檔案系統根目錄在建立時是屬於根使用者，且根使用者擁有寫入權限，因此您需要變更權限以新增檔案。

```
$ sudo chmod go+rw .
```

現在，如果您嘗試 `ls -al` 命令，您將看到權限已遭變更。

```
drwxrwxrwx 2 root     root     4096 Dec 29 22:33 .
drwx------ 4 ec2-user ec2-user 4096 Dec 29 22:54 ..
```

d. 建立 文字檔案。

```
$ touch test-file.txt
```

e. 列出目錄內容。

```
$ ls -l
```

您現在已成功在 VPC 中的 EC2 執行個體上建立並掛載了一個 Amazon EFS 檔案系統。

您掛載的檔案系統在重新啟動期間將不會保留。若要自動重新掛載目錄，您可以使用 `fstab` 檔案。如需詳細資訊，請參閱 重新啟動時自動重新掛載。如果您正在使用 Auto Scaling 群組來啟動 EC2 執行個體，您也可以在啟動組態中設定指令碼。如需範例，請參閱逐步解說：設定 Apache Web 伺服器並提供 Amazon EFS 檔案。

下一步驟

步驟 4：清理

步驟 4：清理

如果您不再需要您建立的資源，您應該予以移除。您可利用 CLI 實現此功能。

- 移除 EC2 資源 (EC2 執行個體和兩個安全群組)。當您刪除掛載目標時，Amazon EFS 會刪除網路介面。
- 移除 Amazon EFS 資源 (檔案系統、掛載目標)。

若要刪除本逐步解說中建立的 AWS 資源

1. 終止在此逐步解說中建立的 EC2 執行個體。

   ```
   $ aws ec2 terminate-instances \
   --instance-ids instance-id \
   --profile adminuser
   ```

   您也可以使用主控台刪除 EC2 資源。如需說明，請參閱終止執行個體。

2. 刪除該掛載目標。

   在刪除檔案系統前，您必須刪除為該檔案系統建立的掛載目標。您可以使用 `describe-mount-targets` CLI 命令取得掛載目標清單。

   ```
   $  aws efs describe-mount-targets \
   --file-system-id file-system-ID \
   --profile adminuser \
   --region aws-region
   ```

   然後使用 `delete-mount-target` CLI 命令來刪除掛載目標。

   ```
   $ aws efs delete-mount-target \
   --mount-target-id ID-of-mount-target-to-delete \
   --profile adminuser \
   --region aws-region
   ```

3. (選用) 刪除您建立的兩個安全群組。您不需支付建立安全群組的費用。

   您必須先刪除掛載目標的安全群組，才能刪除 EC2 執行個體的安全群組。掛載目標的安全群組規則是參考自 EC2 安全群組。因此，您無法先刪除 EC2 執行個體的安全群組。

如需指示，請參閱 Amazon EC2 使用者指南中的刪除安全群組。

4. 使用 `delete-file-system` CLI 命令刪除檔案系統。您可以使用 `describe-file-systems` CLI 命令取得檔案系統清單。您可以自回應取得檔案系統 ID。

```
aws efs describe-file-systems \
--profile adminuser \
--region aws-region
```

提供檔案系統 ID 以刪除檔案系統。

```
$ aws efs delete-file-system \
--file-system-id ID-of-file-system-to-delete \
--region aws-region \
--profile adminuser
```

逐步解說：設定 Apache Web 伺服器並提供 Amazon EFS 檔案

您可以讓執行 Apache Web 伺服器的 EC2 執行個體提供存放在 Amazon EFS 檔案系統上的檔案。您能夠透過一個 EC2 執行個體提供檔案，亦可以視應用程式需求，讓多個 EC2 執行個體從 Amazon EFS 檔案系統提供檔案。操作程序如下所述。

- 在 EC2 執行個體上設定 Apache Web 伺服器。
- 建立 Auto Scaling 群組，即可在多個 EC2 執行個體上設定 Apache Web 伺服器。您可以使用 Amazon EC2 Auto Scaling 建立多個 EC2 執行個體，這項 AWS 服務可讓您根據應用程式需求增加或減少群組中的 EC2 執行個體數量。若您擁有多個 Web 伺服器，則需一併具備負載平衡器，藉此將請求的流量分佈至各伺服器。

> **Note**
>
> 執行這兩個操作程序時，您建立的所有資源皆會位於美國西部 (奧勒岡) 區域 (`us-west-2`)。

透過單一 EC2 執行個體提供檔案

請遵循下列步驟，即可在一個 EC2 執行個體上設定 Apache Web 伺服器，以便提供您在 Amazon EFS 檔案系統中建立的檔案。

1. 請依照入門練習中的步驟進行操作，藉此取得可正常運作的組態，而該組態是由下列項目所組成：

   - Amazon EFS 檔案系統
   - EC2 執行個體
   - 掛載在 EC2 執行個體上的檔案系統

   如需說明，請參閱開始使用 Amazon Elastic File System。在遵照步驟執行時，請記住以下內容：

   - EC2 執行個體的公有 DNS 名稱。
   - 掛載目標的公有 DNS 名稱，該掛載目標位於啟動 EC2 執行個體時所使用的可用區域中。
2. (選用) 您可以選擇在入門練習建立的掛載點中卸載檔案系統。

   ```
   $ sudo umount  ~/efs-mount-point
   ```

   在本逐步解說中，您可以為檔案系統建立另一個掛載點。
3. 在 EC2 執行個體上安裝 Apache Web 伺服器並加以設定，如下所示：

   a. 連線至 EC2 執行個體並安裝 Apache Web 伺服器。

      ```
      $ sudo yum -y install httpd
      ```

   b. 啟動 服務。

      ```
      $ sudo service httpd start
      ```

   c. 建立掛載點。

      首先請注意，DocumentRoot 檔案中的 /etc/httpd/conf/httpd.conf 會指向 /var/www/html (DocumentRoot "/var/www/html")。

      Amazon EFS 檔案系統將掛載於文件根目錄底下的子目錄。

      在 /var/www/html 下，建立名爲 efs-mount-point 的子目錄，用於掛載檔案系統端點。

      ```
      $ sudo mkdir /var/www/html/efs-mount-point
      ```

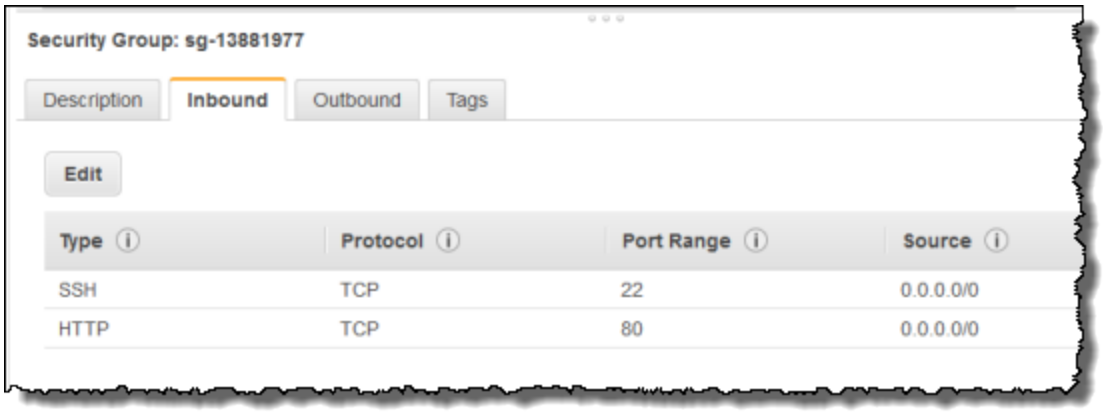
   d. 使用下列指令掛載 Amazon EFS 檔案系統。用檔案系統的 ID 取代 file-system-id。

```
$ sudo mount -t efs file-system-id:/ /var/www/html/efs-mount-point
```

4. 測試設定。

   a. 在入門練習所建立的 EC2 執行個體安全群組中新增規則，以便讓 TCP 連接埠 80 接受來自任何位置的 HTTP 流量。

      新增規則之後，EC2 執行個體安全群組將具備以下傳入規則。



      如需說明，請參閱使用主控台建立安全群組。

   b. 建立範例 html 檔案。

      i. 將目錄變更為掛載點。

```
$ cd /var/www/html/efs-mount-point
```

      ii. 建立名爲 sampledir 的子目錄，並變更所有權。

```
$  sudo mkdir sampledir
$  sudo chown  ec2-user sampledir
$  sudo chmod -R o+r sampledir
```

      變更目錄，才能在 sampledir 子目錄中建立檔案。

```
$  cd sampledir
```

      iii. 建立範例 hello.html 檔案。

```
$ echo "<html><h1>Hello from Amazon EFS</h1></html>" > hello.html
```

c. 開啟瀏覽器視窗並輸入存取檔案的 URL，該 URL 為 EC2 執行個體的公有 DNS 名稱，後面會加上檔案名稱。例如：

```
http://EC2-instance-public-DNS/efs-mount-point/sampledir/hello.html
```

現在，您可以開始提供 Amazon EFS 檔案系統上所存放的網頁內容。

> **Note**
>
> 根據此處的設定，EC2 執行個體不會在開機時自動啟動 Web 伺服器 (httpd)，亦不會在開機時掛載檔案系統。您可以在下一個逐步解說中建立啟動組態，以便進行這項設定。

透過多個 EC2 執行個體提供檔案

請遵循下列步驟，即可由多個 EC2 執行個體提供相同的 Amazon EFS 檔案系統內容，藉此改善可擴展性或可用性。

1. 請依照 快速建立具有建議設定的檔案系統 (主控台) 練習中的步驟進行操作，進而建立並測試 Amazon EFS 檔案系統。

   > **Important**
   >
   > 在本逐步解說中，您不會用到在入門練習中建立的 EC2 執行個體；相反地，您將需要啟動新的 EC2 執行個體。

2. 透過下述步驟，在 VPC 中建立負載平衡器。

   a. 定義負載平衡器

      在 Basic Configuration (基本組態) 區段中選取 VPC，您將在該 VPC 中建立要掛載檔案系統的 EC2 執行個體。

      在選取子網路區段中，選取所有可用的子網路。如需詳細資訊，請參閱下一區段的 `cloud-config` 指令碼。

   b. 指派安全群組

為負載平衡器建立新的安全群組，藉此允許任何位置在連接埠 80 上進行 HTTP 存取，如下所示：

- Type (類型)：HTTP
- Protocol (通訊協定)：TCP
- Port Range (連接埠範圍)：80
- Source (來源)：Anywhere (任何位置) 0.0.0.0/0

> **Note**
>
> 一切就緒後，您還能夠更新 EC2 執行個體安全群組的傳入規則存取權，即可僅允許來自負載平衡器的 HTTP 流量。

c. 設定運作狀態檢查

將 Ping Path (Ping 路徑) 的值設為 `/efs-mount-point/test.html`。`efs-mount-point` 是掛載檔案系統的子目錄。在此程序的後續步驟中，您可以新增 `test.html` 頁面。

> **Note**
>
> 請勿新增任何 EC2 執行個體。稍後，您會建立 Auto Scaling 群組，並在該群組中啟動 EC2 執行個體、指定此負載平衡器。

如需建立負載平衡器的詳細資訊，請參閱《Elastic Load Balancing 使用者指南》中的 Elastic Load Balancing 入門。

建立包含兩個 EC2 執行個體的 Auto Scaling 群組。首先，請建立可以說明執行個體的啟動組態。接著，請指定該啟動組態，以便建立 Auto Scaling 群組。在下列步驟中，您可以看見在 Amazon EC2 主控台中指定用來建立 Auto Scaling 群組的組態資訊。

1. 在左側導覽窗格的 AUTO SCALING (AUTO SCALING) 下方，選擇 Launch Configurations (啟動組態)。
2. 選擇 Create Auto Scaling group (建立 Auto Scaling 群組) 來啟動精靈。
3. 選擇 Create launch configuration (建立啟動組態)。

4. 從快速入門中，選取最新版的 Amazon Linux 2 AMI。該 AMI 與入門練習中 建立您的 EFS 檔案系統並啟動 EC2 執行個體 所使用的 AMI 相同。
5. 在 Advanced (進階) 區段中，執行下列步驟：

   - 針對 IP Address Type (IP 地址類型)，選擇 Assign a public IP address to every instance (將公有 IP 地址指派給每個執行個體)。
   - 將以下指令碼複製/貼上至 User data (使用者資料) 方塊。

     您必須提供 *file-system-id* 與 *aws-region* 的值，進而更新該指令碼 (若有遵照入門練習的步驟進行操作，則表示您已在 us-west-2 區域中建立檔案系統)。

     在指令碼中，請注意下列事項：

     - 該指令碼會安裝 NFS 用戶端與 Apache Web 伺服器。
     - echo 命令會在 /etc/fstab 檔案中寫入以下項目，藉此找出檔案系統的 DNS 名稱，以及掛載該檔案系統的子目錄。透過此項目，即可確保系統在每次重新開機後，一律會掛載檔案。請注意，系統會動態建構檔案系統的 DNS 名稱。如需詳細資訊，請參閱 以 DNS 名稱掛載於 Amazon EC2。

       ```
       file-system-ID.efs.aws-region.amazonaws.com:/ /var/www/html/efs-mount-point
        nfs4    defaults
       ```

     - 建立 efs-mount-point 子目錄並掛載檔案系統。
     - 建立 test.html 頁面，讓 ELB 運作狀態檢查可以找到您在建立負載平衡器時指定為 ping 點的檔案。

     如需使用者資料指令碼的詳細資訊，請參閱執行個體中繼資料和使用者

     ```
     #cloud-config
     package_upgrade: true
     packages:
     - nfs-utils
     - httpd
     runcmd:
     - echo "$(curl -s http://169.254.169.254/latest/meta-data/placement/availability-
     zone).file-system-id.efs.aws-region.amazonaws.com:/    /var/www/html/efs-mount-
     point    nfs4    defaults" >> /etc/fstab
     - mkdir /var/www/html/efs-mount-point
     - mount -a
     - touch /var/www/html/efs-mount-point/test.html
     - service httpd start
     ```

```
- chkconfig httpd on
```

6. 在指派安全群組中，選擇選取現有的安全群組，然後選擇您為 EC2 執行個體建立的安全群組。
7. 現在，設定 Auto Scaling 群組的詳細資訊時，請採用下列資訊：
   a. 在 Group size (群組大小) 中，選擇 **`Start with 2 instances`**。系統即會建立兩個 EC2 執行個體。
   b. 從 Network (網路) 清單中選取 VPC。
   c. 選取子網路，該子網路所在的可用區域與您在先前步驟建立啟動組態時，為了指定 User Data (使用者資料) 指令碼的掛載目標 ID 而使用的可用區域相同。
   d. 在進階詳細資訊區段中
      i. 在 Load Balancing (負載平衡) 中，選擇 Receive traffic from Elastic Load Balancer(s) (從一或多個 Elastic Load Balancer 接收流量)，然後選取您為本練習建立的負載平衡器。
      ii. 在 Health Check Type (運作狀態檢查類型) 中，選擇 ELB (ELB)。
8. 如需建立 Auto Scaling 群組，請依照《Amazon EC2 Auto Scaling 使用者指南》中的設定擴展規模和負載平衡的應用程式所述的指示。您亦可善用上述資料表中的資訊 (若適用)。
9. 一旦成功建立 Auto Scaling 群組，即代表您具備兩個已安裝 `nfs-utils` 與 Apache Web 伺服器的 EC2 執行個體。在每個執行個體上，請確認您的 `/var/www/html/efs-mount-point` 子目錄已掛載 Amazon EFS 檔案系統。如需 Connect 至 EC2 執行個體的指示，請參閱 Amazon EC2 使用者指南中的連線到 Linux 執行個體。

   > **Note**
   >
   > 在預設情況下，AMI 中已包含 `nfs-utils`，因此您在啟動 Amazon EC2 執行個體時選擇了 Amazon Linux AMI 2016.03.0 Amazon Linux AMI，便無須再安裝。

10. 建立範例頁面 (index.html)。
    a. 變更目錄。

    ```
    $ cd /var/www/html/efs-mount-point
    ```

    b. 建立 `sampledir` 的子目錄，並變更所有權。然後，請變更目錄，才能在 `sampledir` 子目錄中建立檔案。如果您有遵照先前的 透過單一 EC2 執行個體提供檔案 進行操作，則表示已建立 `sampledir` 子目錄，所以可以略過此步驟。

    ```
    $  sudo mkdir sampledir
    ```

```
$  sudo chown  ec2-user sampledir
$  sudo chmod -R o+r sampledir
$  cd sampledir
```

c. 建立範例 index.html 檔案。

```
$ echo "<html><h1>Hello from Amazon EFS</h1></html>" > index.html
```

11. 現在，您可以測試設定。請使用負載平衡器的公有 DNS 名稱來存取 index.html 頁面。

```
http://load balancer public DNS Name/efs-mount-point/sampledir/index.html
```

負載平衡器會將請求傳送至其中一個執行 Apache Web 伺服器的 EC2 執行個體。接著，Web 伺服器會提供存放在 Amazon EFS 檔案系統上的檔案。

逐步解說：建立可寫入的每個使用者子目錄與設定重新啟動時自動重新掛載

建立 Amazon EFS 檔案系統並在 EC2 執行個體本機掛接之後，它會公開一個名為#####目錄的空目錄。其中一個常用案例是在此檔案系統根目錄下為您在 EC2 執行個體上建立的每位使用者建立「可寫入」子目錄，並掛載於使用者的主目錄上。然後，使用者在其主目錄中建立的所有檔案和子目錄都會在 Amazon EFS 檔案系統上建立。

在此逐步解說中，您首先要在 EC2 執行個體上建立使用者「mike」。然後，您可以將 Amazon EFS 子目錄掛接到使用者麥克風的主目錄上。此逐步解說也說明如何設定在系統重新啟動時讓子目錄自動重新掛載。

假設您已在 EC2 執行個體的本機目錄上建立並掛載 Amazon EFS 檔案系統。我們稱它為 *EFSroot*。

> **Note**
>
> 您可以按照本開始使用練習在您的 EC2 執行個體上建立和掛載 Amazon EFS 檔案系統。

在下列步驟中，您會建立使用者 (mike)、為使用者建立子目錄 (*EFSRoot*/mike)、讓使用者 mike 成為子目錄的擁有者、授與他完整權限，最後將 Amazon EFS 子目錄掛載到使用者的主目錄 (/home/mike)。

1. 建立使用者 mike：

   - 登入 EC2 執行個體。使用根權限 (在此情況下，使用 sudo 命令)，建立使用者 mike 並指派密碼。

     ```
     $ sudo useradd -c "Mike Smith" mike
     $ sudo passwd mike
     ```

     這也會為使用者建立主目錄 /home/mike。

2. 在 *EFSroot* 下為使用者 mike 建立子目錄：

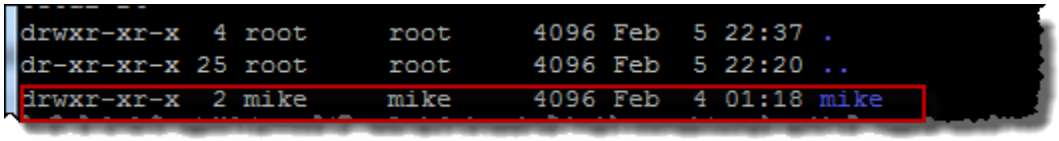
   a. 在 mikeEFSroot ###### 。

      ```
      $  sudo mkdir /EFSroot/mike
      ```

      您需要以您的本機目錄名稱取代 *EFSroot*。

   b. 根使用者和根群組是 /mike 子目錄的擁有者 (您可以使用 ls -l 命令來確認)。若要為使用者 mike 啟用此子目錄的完整許可，授予 mike 此目錄的所有權。

      ```
      $ sudo chown mike:mike /EFSroot/mike
      ```

3. 使用 mount 命令，將 *EFSroot*/mike 子目錄掛載到 mike 的主目錄上。

   ```
   $  sudo mount -t nfs -o
    nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport mount-target-DNS:/mike  /home/mike
   ```

   #### *DNS* 位址可識別遠端 Amazon EFS 檔案系統根目錄。

現在，使用者 mike 的主目錄是 Amazon EFS 檔案系統中可由 mike 寫入的子目錄。若您卸載此掛載目標，使用者若無重新掛載便無法存取自己的 EFS 目錄，而重新掛載需要根許可。

重新啟動時自動重新掛載

您可以使用 `fstab` 檔案，讓檔案系統在任何系統重新啟動後自動重新掛載。如需詳細資訊，請參閱 自動掛載 Amazon EFS 檔案系統。

逐步解說：使用 AWS Direct Connect 和 VPN 建立和掛載內部部署的檔案系統

本逐步解說會 AWS Management Console 使用在內部部署用戶端上建立和裝載檔案系統。您可以使用 AWS Virtual Private Network （ AWS VPN ）上的 AWS Direct Connect 連接或連接來完成此操作。

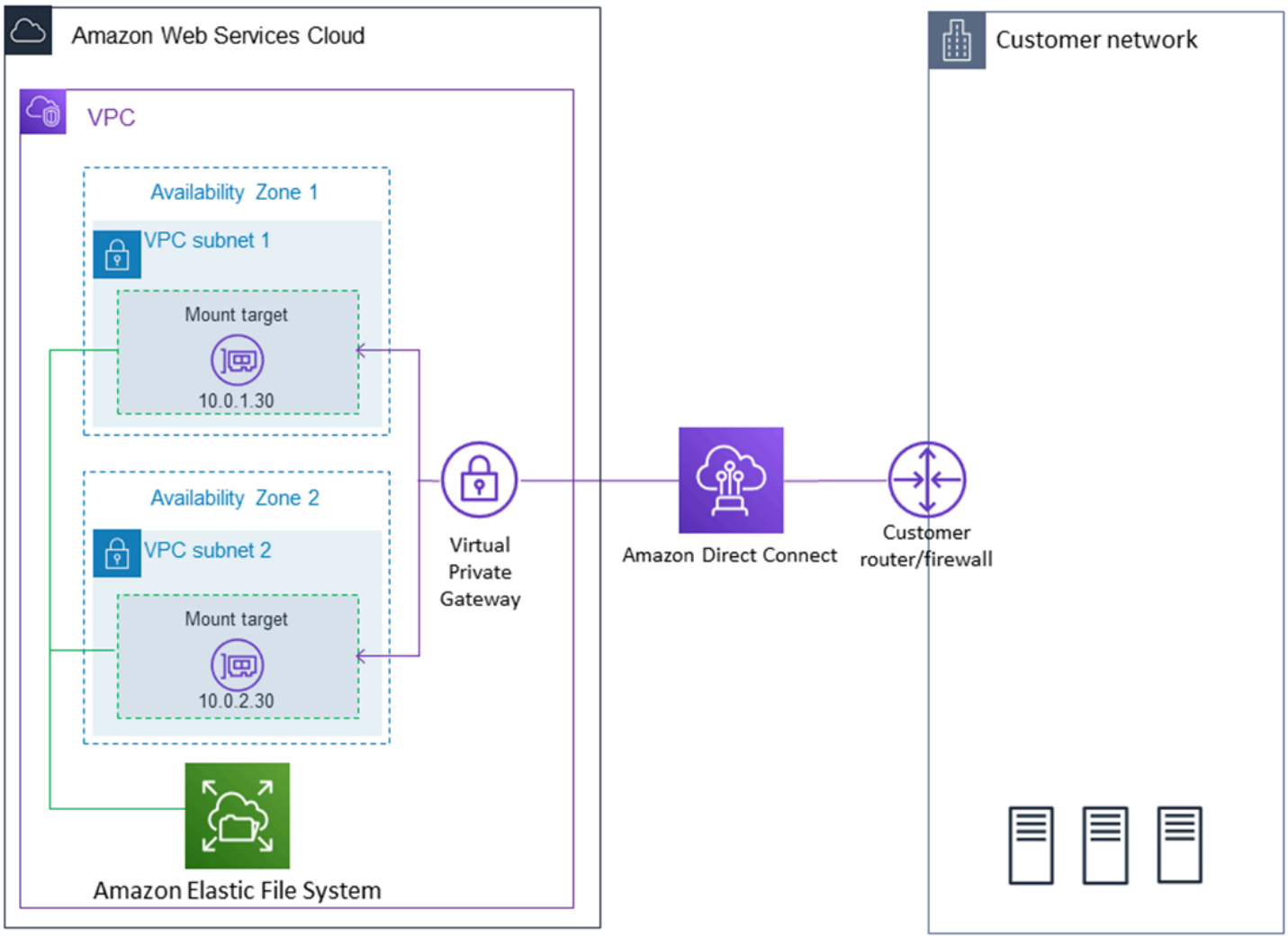
> **Note**
>
> 不支援使用 Amazon EFS 搭配以 Microsoft Windows 爲基礎的用戶端。

主題

在本逐步解說中，我們假設您已經有 AWS Direct Connect 或 VPN 連線。如果不具此連線，您可立即開始連線程序和在連線建立時回到此逐步解說。若要取得更多資訊 AWS Direct Connect，請參閱《AWS Direct Connect 使用指南》。如需有關設定 VPN 連線的詳細資訊，請參閱《Amazon VPC 使用者指南》中的 VPN 連線。

當您有 AWS Direct Connect 或 VPN 連線時，您可以在 Amazon VPC 中建立一個 Amazon EFS 檔案系統和掛載目標。之後，您下載並安裝工 amazon-efs-utils 具。然後，您從現場部署用戶端中測試檔案系統。最後，逐步解說最後的清理步驟將為您提供移除這些資源的資訊。

本逐步解說會在美國西部 (奧勒岡) 區域 (`us-west-2`) 中建立所有這些資源。無論 AWS 區域 您使用哪種方式，請務必始終如一地使用它。您的所有資源 (VPC、掛載目標和 Amazon EFS 檔案系統) 都必須位於相同的資源 AWS 區域，如下圖所示。



> **Note**
>
> 在某些情況下，本機應用程式可能需要知道該 EFS 檔案系統是否提供使用。在這些情況下，如果第一個掛載點暫時無法使用，則您的應用程式應該能夠指向不同的掛載點 IP 地址。在這個案例中，我們建議您將兩個現場部署用戶端連接到在不同可用區域 (AZ) 的檔案系統以獲得更高的可用性。

開始之前

您可以使用您的根憑證登 AWS 帳戶 入主控台並嘗試此練習。不過， AWS Identity and Access Management (IAM) 最佳做法建議您不要使用 AWS 帳戶. 反之，在帳戶中建立一個管理員使用者並使用這些憑證來管理帳戶中的資源。如需詳細資訊，請參閱使用指南中的為 IAM 身分中心使用AWS IAM Identity Center 者指派 AWS 帳戶 存取權限。

您可以使用預設 VPC 或在帳戶中建立的自訂 VPC。預設的 VPC 設定適用於此逐步解說。不過，如果您使用的是自訂 VPC，請檢查下列各項：

- 該網際網路閘道已連接至您的 VPC。如需詳細資訊，請參閱Amazon VPC 使用者指南中的網際網路閘道。
- 該 VPC 路由表包含傳送所有網際網路綁定型流量到網際網路閘道的規則。

步驟 1：建立 Amazon Elastic File System 資源

在此步驟中，您建立 Amazon EFS 檔案系統和掛載目標。

建立 Amazon EFS 檔案系統

1. 前往 https://console.aws.amazon.com/efs/ 開啟 Amazon EFS 主控台。
2. 選擇 Create File System (建立檔案系統)。
3. 從 VPC (VPC) 清單中選擇預設 VPC。
4. 選取所有可用區域的核取方塊。確保它們已選擇預設子網路、自動 IP 地址和預設安全群組。這些是您的掛載目標。如需詳細資訊，請參閱 管理掛載目標。
5. 選擇 Next Step (後續步驟)。
6. 為您的檔案系統命名，將 general purpose (一般用途) 選擇為您的預設效能模式，然後選擇 Next Step (下一步)。
7. 選擇 Create File System (建立檔案系統)。
8. 從清單中選擇您的檔案系統，並記下 Security group (安全群組) 值。您在下一個步驟中需要使用到此數值。

您剛建立的檔案系統已有掛載目標。每個掛載目標都有一個關聯的安全群組。做為虛擬防火牆的安全群組會控制網路流量。如果您在建立掛載目標未提供安全群組，Amazon EFS 會將 VPC 的預設安全群組與其相關聯。如果您完全依照上述步驟，則掛載目標使用的是預設安全群組。

接著，您將規則新增至掛載目標的安全群組，以允許對網路檔案系統 (NFS) 連接埠 (2049) 的傳入流量。您可以使用將規則新增 AWS Management Console 至 VPC 中裝載目標的安全性群組。

允許對 NFS 連接埠的傳入流量

1. 登入 AWS Management Console 並開啟 Amazon EC2 主控台，網址為 https://console.aws.amazon.com/ec2/。

2. 在網路與安全性下，選擇安全群組。
3. 選擇與您檔案系統關聯的安全群組。您在 步驟 1：建立 Amazon Elastic File System 資源 結尾時記下此資訊。
4. 在安全群組清單下方顯示的標籤窗格中，選擇傳入 索引標籤。
5. 選擇編輯。
6. 選擇 Add Rule (新增規則)，然後選擇以下其中一種類型的規則：

   - 類型 – NFS (NFS)
   - 來源 – Anywhere (隨處)

   我們建議您只使用 Anywhere (隨處) 來源進行測試。您可以建立設為在現場部署用戶端之 IP 地址的自訂來源，或從用戶端本身使用主控台，然後選擇 My IP (我的 IP)。

   > **Note**
   >
   > 您不需要新增傳出規則，因為預設的傳出規則可讓所有流量離開。如果您沒有此預設傳出規則，新增一個傳出規則，以開啟 NFS 連接埠上的 TCP 連接，以便將掛載目標安全群組識別做為目的地。

步驟 2：安裝 NFS 用戶端

在此步驟中，您將安裝 NFS 用戶端。

將 NFS 用戶端安裝在您的現場部署伺服器

> **Note**
>
> 如果您需要加密傳輸中的資料，請使用 Amazon EFS 掛載協助程式 `amazon-efs-utils`，而不要使用 NFS 用戶端。如需安裝的相關資訊 amazon-efs-utils，請參閱選用：加密傳輸中的資料一節。

1. 存取現場部署用戶端的終端機。
2. 安裝 NFS。

   如果您使用的是 Red Hat Linux，請使用下列命令來安裝 NFS。

```
$ sudo yum -y install nfs-utils
```

如果您使用的是 Ubuntu，請使用下列命令來安裝 NFS。

```
$ sudo apt-get -y install nfs-common
```

步驟 3：將 Amazon EFS 檔案系統掛載在內部部署用戶端

建立掛載目錄

1. 使用以下命令建立掛載點的目錄。

   Example

   ```
   mkdir ~/efs
   ```

2. 選擇可用區域中掛載目標的慣用 IP 地址。您可以透過現場部署 Linux 用戶端測量延遲。若要這樣做，請對在不同可用區域的 EC2 執行個體之 IP 地址使用以終端機為基礎的工具 (例如 `ping`)，以尋找具最低延遲的 IP 地址。

- 執行掛載命令，並使用掛載目標的 IP 地址進行檔案系統掛載。

  ```
  $ sudo mount -t nfs -o
   nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport mount-target-IP:/   ~/efs
  ```

現在您已掛載 Amazon EFS 檔案系統，您可以使用以下程序測試該系統。

測試 Amazon EFS 檔案系統連線

1. 使用下列命令，將目錄變更為您建立的新目錄。

   ```
   $ cd ~/efs
   ```

2. 建立子目錄，並將子目錄的擁有權變更為 EC2 執行個體使用者。接著，使用下列命令導覽至新目錄。

```
$ sudo mkdir getting-started
$ sudo chown ec2-user getting-started
$ cd getting-started
```

3. 透過下列命令建立文字檔。

```
$ touch test-file.txt
```

4. 透過以下命令列出目錄內容。

```
$ ls -al
```

因此，會建立以下檔案。

```
-rw-rw-r-- 1 username username 0 Nov 15 15:32 test-file.txt
```

您也可以透過將項目新增至 /etc/fstab 檔案以自動掛載檔案系統。如需詳細資訊，請參閱 自動掛載 Amazon EFS 檔案系統。

> **Warning**
>
> 使用 _netdev 選項，此選項用於在自動掛載檔案系統時識別網路檔案系統。若 _netdev 已遺失，EC2 執行個體可能會停止回應。此結果是因為網路檔案系統在運算執行個體開始聯網後需要初始化。如需詳細資訊，請參閱 自動掛載失敗且執行個體沒有回應。

步驟 4：清除資源和保護 AWS 帳戶

在完成此逐步解說後，或者，如果您不想探索逐步解說，您應該遵循這些步驟以清除資源並保護 AWS 帳戶。

若要清理資源並保護您的 AWS 帳戶

1. 使用下列命令卸載 Amazon EFS 檔案系統。

```
$ sudo umount ~/efs
```

2. 前往 https://console.aws.amazon.com/efs/ 開啟 Amazon EFS 主控台。

3. 選擇您要從檔案系統清單刪除的 Amazon EFS 檔案系統。
4. 針對 Actions (動作)，選擇 Delete file system (刪除檔案系統)。
5. 在永久刪除檔案系統對話方塊中，輸入要刪除的 Amazon EFS 檔案系統之檔案系統 ID，然後選擇刪除檔案系統。
6. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
7. 在導覽窗格中，選擇安全群組。
8. 選取您在此逐步解說中將規則新增至其中的安全群組名稱。

> ⚠ Warning
>
> 無法刪除 VPC 的預設安全群組。

9. 在 Actions (動作) 中，選擇 Edit inbound rules (編輯傳入規則)。
10. 選擇在您新增之傳入規則結尾的 X 並選擇 Save (儲存)。

選用：加密傳輸中的資料

若要加密傳輸中的資料，請使用 Amazon EFS 掛載協助程式 amazon-efs-utils，而非 NFS 用戶端。

此amazon-efs-utils 套件是 Amazon EFS 工具的開放原始碼集合。此 amazon-efs-utils 系列隨附掛載協助程式和工具，可讓您更輕鬆地為 Amazon EFS 加密傳輸中的資料。如需此套件的詳細資訊，請參閱安裝 Amazon EFS 工具。此套件可免費下載 GitHub，您可以透過複製套件的存放庫來取得此套件。

若要 amazon-efs-utils 從複製 GitHub

1. 存取現場部署用戶端的終端機。
2. 從終端機，使用以下命令 GitHub 將 amazon-efs-utils 工具從複製到您選擇的目錄。

```
git clone https://github.com/aws/efs-utils
```

現在您已有套件，即可進行安裝。根據現場部署用戶端的 Linux 發行版本，此安裝的處理方式會有所不同。支援以下發行版本：

- Amazon Linux 2
- Amazon Linux
- Red Hat Enterprise Linux (和例如 CentOS 之類的導數) 版本 7 和更新版本

- Ubuntu 16.04 LTS 和更新版本

若要建置並安裝 amazon-efs-utils 為 RPM 套件

1. 開啟用戶端上的終端機，然後瀏覽至具有複製 amazon-efs-utils 套件的目錄。 GitHub
2. 使用以下命令建置套件。

```
make rpm
```

> **Note**
>
> 如果您尚未這麼做，則請使用下列命令安裝 rpm-builder 套件。
>
> ```
> sudo yum -y install rpm-build
> ```

3. 使用下列命令安裝 套件。

```
sudo yum -y install build/amazon-efs-utils*rpm
```

若要建置並安裝 amazon-efs-utils 為 deb 套件

1. 開啟用戶端上的終端機，然後瀏覽至具有複製 amazon-efs-utils 套件的目錄。 GitHub
2. 使用以下命令建置套件。

```
./build-deb.sh
```

3. 使用下列命令安裝 套件。

```
sudo apt-get install build/amazon-efs-utils*deb
```

安裝套件之後，請設定 amazon-efs-utils 在您的 AWS 區域 WITH AWS Direct Connect 或 VPN 中使用。

若要設 amazon-efs-utils 定以便在您的 AWS 區域

1. 使用您選擇的文字編輯器，開啟 `/etc/amazon/efs/efs-utils.conf` 進行編輯。

2. 尋找行 “dns_name_format = {fs_id}.efs.*{region}*.amazonaws.com”。
3. 使用 AWS 區域的 ID (例如 us-west-2) 變更 *{region}*。

若要將 EFS 檔案系統掛載在內部部署用戶端上，請先開啟在內部部署 Linux 用戶端上的終端機。若要掛載系統，您需要檔案系統 ID、其中一個掛載目標的掛載目標 IP 地址，以及檔案系統的 AWS 區域。如果您建立多個檔案系統的掛載目標，則可以選擇任何其中一個。

當您擁有該資訊時，您可以使用三個步驟來掛載檔案系統：

建立掛載目錄

1. 使用以下命令建立掛載點的目錄。

   Example

   ```
   mkdir ~/efs
   ```

2. 選擇可用區域中掛載目標的慣用 IP 地址。您可以透過現場部署 Linux 用戶端測量延遲。若要這樣做，請對在不同可用區域的 EC2 執行個體之 IP 地址使用以終端機為基礎的工具 (例如 ping)，以尋找具最低延遲的 IP 地址。

更新 **/etc/hosts**

- 使用以下格式透過檔案系統 ID 和掛載目標 IP 地址，將項目新增到本機 /etc/hosts 檔案。

  ```
  mount-target-IP-Address file-system-ID.efs.region.amazonaws.com
  ```

  Example

  ```
  192.0.2.0 fs-12345678.efs.us-west-2.amazonaws.com
  ```

建立掛載目錄

1. 使用以下命令建立掛載點的目錄。

   Example

   ```
   mkdir ~/efs
   ```

2. 執行掛載命令來掛載檔案系統。

   Example

   ```
   sudo mount -t efs fs-12345678 ~/efs
   ```

   如果您想要使用傳輸中的資料加密，掛載命令看起來如下所示。

   Example

   ```
   sudo mount -t efs -o tls fs-12345678 ~/efs
   ```

逐步解說：掛載來自不同 VPC 的檔案系統

在此逐步解說中，您將設定 Amazon EC2 執行個體以掛載位於不同虛擬私有雲端 (VPC) 中的 Amazon EFS 檔案系統。您可以使用 EFS 掛載協助程式來執行此操作。掛載協助程式是 `amazon-efs-utils` 工具組的一部分。如需 `amazon-efs-utils` 的相關資訊，請參閱 安裝 Amazon EFS 工具。

請務必使用 VPC 對等連接或 VPC 傳輸閘道來連接用戶端的 VPC 和 EFS 檔案系統的 VPC。使用 VPC 對等互連或傳輸閘道來連接 VPC 時，即使 VPC 屬於不同帳戶，Amazon EC2 執行個體仍可在另一個 VPC 存取 EFS 檔案系統。

> **Note**
>
> 不支援使用 Amazon EFS 搭配以 Microsoft Windows 爲基礎的用戶端。

主題

開始之前

在這個逐步解說中，我們假設您已經有下列設定：

- 使用此程序之前，EC2 執行個體上已安裝 `amazon-efs-utils` 工具組。如需安裝 `amazon-efs-utils` 的指示，請參閱安裝 Amazon EFS 工具。
- 下列其中一項：
  - EFS 檔案系統所在的 VPC 與 EC2 執行個體所在的 VPC 之間的 VPC 對等連接。VPC 對等連接是在兩個 VPC 之間的網路連線。這種連線類型可讓您使用私有網際網路通訊協定第 4 版 (IPv4) 或網際網路通訊協定第 6 版 (IPv6) 地址，在兩者間路由流量。您可以使用 VPC 對等連線來連接相同 AWS 區域 或兩者之間的 VPC。 AWS 區域如需詳細資訊，請參閱《Amazon VPC 對等互連指南》中的建立和接受 Amazon VPC 對等互連連線。
  - EFS 檔案系統所在的 VPC 與 EC2 執行個體所在之 VPC 之間的傳輸閘道連接。傳輸閘道是網路傳輸中樞，您可以用於互相連接 VPC 和現場部署網路。如需詳細資訊，請參閱《Amazon VPC 傳輸閘道指南》中的開始使用傳輸閘道。

步驟 1：判斷 EFS 掛載目標的可用區域 ID

為確保檔案系統具備高可用性，建議您一律使用與 NFS 用戶端所在同一可用區域的 EFS 掛載目標 IP 地址。如果要掛載另一個帳戶中的 EFS 檔案系統，請確保 NFS 用戶端和 EFS 掛載目標位於相同的可用區域 ID。此要求適用的原因是，可用區域名稱在各個帳戶間可能會有不同。

決定 EC2 執行個體的可用區域。

1. 連線到您的 EC2 執行個體：

   - 若要從執行 macOS 或 Linux 的電腦連接至您的執行個體，請指定 SSH 命令的 .pem 檔案。為此，您必須使用 `-i` 選項和私密金鑰路徑。
   - 若要從執行 Windows 的電腦連線至執行個體，您可以使用 MindTerm 或 PuTTY。您需要安裝 PuTTY 並將 .pem 檔案轉換為 .ppk 檔案，才可以使用該程式。

   如需詳細資訊，請參閱 Amazon EC2 使用者指南中的下列主題：

   - 使用安全殼層從 Linux 或 macOS Connect 至您的 Linux 執行個體
   - 使用 PuTTY 從視窗 Connect 到您的 Linux 執行個體
2. 您可以使用 `describe-availability-zones` CLI 命令來判斷 EC2 執行個體所在的可用區域 ID，如下所示。

```
[ec2-user@ip-10.0.0.1] $ aws ec2 describe-availability-zones --zone-name
{
    "AvailabilityZones": [
        {
            "State": "available",
            "ZoneName": "us-east-2b",
            "Messages": [],
            "ZoneId": "use2-az2",
            "RegionName": "us-east-2"
        }
    ]
}
```

可用區域 ID 會在 ZoneId 屬性 use2-az2 中傳回。

步驟 2：判斷掛載目標 IP 地址

既然您已知道 EC2 執行個體的可用區域ID，就可以開始擷取位於相同可用區域ID 的掛載目標 IP 地址。

判斷同一個可用區域ID 中的掛載目標 IP 地址

- 您可以使用 describe-mount-targets CLI 命令來擷取 use2-az2 AZ ID 中的檔案系統掛載目標 IP 地址，如下所示。

```
$ aws efs describe-mount-targets --file-system-id file_system_id
{
    "MountTargets": [
        {
            "OwnerId": "111122223333",
            "MountTargetId": "fsmt-11223344",
  =====>    "AvailabilityZoneId": "use2-az2",
            "NetworkInterfaceId": "eni-048c09a306023eeec",
            "AvailabilityZoneName": "us-east-2b",
            "FileSystemId": "fs-01234567",
            "LifeCycleState": "available",
            "SubnetId": "subnet-06eb0da37ee82a64f",
            "OwnerId": "958322738406",
  =====>    "IpAddress": "10.0.2.153"
        },
```

```
...
        {
            "OwnerId": "111122223333",
            "MountTargetId": "fsmt-667788aa",
            "AvailabilityZoneId": "use2-az3",
            "NetworkInterfaceId": "eni-0edb579d21ed39261",
            "AvailabilityZoneName": "us-east-2c",
            "FileSystemId": "fs-01234567",
            "LifeCycleState": "available",
            "SubnetId": "subnet-0ee85556822c441af",
            "OwnerId": "958322738406",
            "IpAddress": "10.0.3.107"
        }
    ]
}
```

use2-az2可用區域ID 中的掛載目標 IP 地址為 10.0.2.153。

步驟 3：新增掛載目標的主機項目

您現在可以在 EC2 執行個體的 /etc/hosts 檔案中建立一個項目，以便將掛載目標 IP 地址對應至 EFS 檔案系統的主機名稱。

新增掛載目標的主機項目

1. 請在 EC2 執行個體的 /etc/hosts 檔案中新增一行掛載目標 IP 地址。該項目使用的格式為 m*ount-target-IP-Address file-system-ID*.efs.*region*.amazonaws.com。您可以利用下列命令來將該行新增至檔案。

   ```
   echo "10.0.2.153 fs-01234567.efs.us-east-2.amazonaws.com" | sudo tee -a /etc/hosts
   ```

2. 確保 EC2 執行個體和掛載目標的 VPC 安全群組具有允許存取 EFS 系統的規則 (視需要)。如需詳細資訊，請參閱 針對 Amazon EC2 執行個體和掛載目標使用 VPC 安全群組。

步驟 4：使用 EFS 掛載協助程式掛載檔案系統

若要掛載 EFS 檔案系統，首先您必須在 EC2 執行個體上建立掛載目錄。然後，使用 EFS 掛載協助程式透過 IAM 授權或 EFS 存取點來掛載檔案系統。如需詳細資訊，請參閱 使用 IAM 控制檔案系統資料存取 及 使用 Amazon EFS 存取點。

建立掛載目錄

- 您可以使用下列命令來建立掛載檔案系統的目錄。

```
$ sudo mkdir /mnt/efs/
```

使用 IAM 授權掛載檔案系統

- 您可以使用下列命令來透過 IAM 授權掛載檔案系統。

```
$ sudo mount -t efs -o tls,iam file-system-id /mnt/efs/
```

使用 EFS 存取點掛載檔案系統

- 您可以使用下列命令來透過 EFS 存取點掛載檔案系統。

```
$ sudo mount -t efs -o tls,accesspoint=access-point-id file-system-id /mnt/efs/
```

現在您已掛載 Amazon EFS 檔案系統，您可以使用以下程序測試該系統。

測試 Amazon EFS 檔案系統連線

1. 使用下列命令，將目錄變更為您建立的新目錄。

```
$ cd ~/mnt/efs
```

2. 建立子目錄，並將子目錄的擁有權變更為 EC2 執行個體使用者。接著，使用下列命令導覽至新目錄。

```
$ sudo mkdir getting-started
$ sudo chown ec2-user getting-started
$ cd getting-started
```

3. 透過下列命令建立文字檔。

```
$ touch test-file.txt
```

4. 透過以下命令列出目錄內容。

```
$ ls -al
```

因此，會建立以下檔案。

```
-rw-rw-r-- 1 username username 0 Nov 15 15:32 test-file.txt
```

您也可以透過將項目新增至 /etc/fstab 檔案以自動掛載檔案系統。如需詳細資訊，請參閱 使用搭配 EFS 掛載協助程式的 /etc/fstab 自動掛載 EFS 檔案系統。

> **Warning**
>
> 使用 _netdev 選項，此選項用於在自動掛載檔案系統時識別網路檔案系統。若 _netdev 已遺失，EC2 執行個體可能會停止回應。此結果是因為網路檔案系統在運算執行個體開始聯網後需要初始化。如需詳細資訊，請參閱 自動掛載失敗且執行個體沒有回應。

步驟 5：清除資源和保護 AWS 帳戶

完成此演練後，或者，如果您不想探索各項演練，請務必遵循下述步驟。這些步驟能夠清除資源與保護 AWS 帳戶帳戶。

清理資源並保護您的 AWS 帳戶

1. 使用下列命令卸載 Amazon EFS 檔案系統。

   ```
   $ sudo umount ~/efs
   ```

2. 前往 https://console.aws.amazon.com/efs/ 開啟 Amazon EFS 主控台。
3. 選擇您要從檔案系統清單刪除的 Amazon EFS 檔案系統。
4. 針對 Actions (動作)，選擇 Delete file system (刪除檔案系統)。
5. 在永久刪除檔案系統對話方塊中，輸入要刪除的 Amazon EFS 檔案系統之檔案系統 ID，然後選擇刪除檔案系統。
6. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
7. 在導覽窗格中，選擇安全群組。
8. 選取您在此逐步解說中將規則新增至其中的安全群組名稱。

> **Warning**
>
> 無法刪除 VPC 的預設安全群組。

9. 在 Actions (動作) 中，選擇 Edit inbound rules (編輯傳入規則)。
10. 選擇在您新增之傳入規則結尾的 X 並選擇 Save (儲存)。

演練：靜態強制執行 Amazon EFS 檔案系統強制執行靜態加密

您可以在下面找到有關如何使用 Amazon CloudWatch 和AWS CloudTrail。本演練基於AWS白皮書使用 Amazon EFS 加密檔案系統加密資料。

> **Note**
>
> 本演練中介紹的強制創建靜態加密的 Amazon EFS 文件系統的方法已不建議使用。建立靜態加密的檔案系統的首選方法是使用`elasticfilesystem:Encrypted`條件鍵AWS Identity and Access Management以身分為基礎的政策。如需詳細資訊，請參閱 範例：強制建立加密檔案系統。您可以使用此演練創建 CloudWatch 警報，以驗證您的 IAM 策略是否阻止創建未加密文件系統。

強制執行靜態加密

您的組織可能需要對符合特定分類所有資料進行靜態加密，或是與特定應用程式、工作負載或環境相關聯。您可以使用偵測控制，對 Amazon EFS 檔案系統強制執行靜態資料加密政策。這些控制會偵測檔案系統的建立和驗證靜態加密是否已啟用。

如果偵測到未靜態加密的檔案系統，您可以多種方式來回應。方法從刪除檔案系統和掛載目標，到通知管理員都可以。

如果您要刪除未加密的靜態檔案系統，但想要保留資料，請先建立新的加密靜態檔案系統。接著，將資料複製到新的加密靜態檔案系統。複製資料之後，您可以刪除未加密的檔案系統。

檢測靜態處於未加密狀態的文件系統

您可以建立 CloudWatch 警示 CloudTrail 以監控`CreateFileSystem`事件。然後，如果已建立的檔案系統未受到靜態加密，您可以觸發警示來通知系統管理員。

建立指標篩選條件

建立未加密的 Amazon EFS 檔案系統時，若要建立 CloudWatch 警示，請使用下列步驟。

開始之前，您必須擁有已建立的現有追蹤，以便將 CloudTrail 日誌傳送到 CloudWatch Logs 日誌組。如需詳細資訊，請參閱「」傳送事件到 CloudWatch Logs中的AWS CloudTrail使用者指南。

建立指標篩選條件

1. 在 https://console.aws.amazon.com/cloudwatch/ 開啟 CloudWatch 主控台。
2. 在導覽窗格中，選擇 Logs (日誌)。
3. 在日誌群組清單中，選擇您針對 CloudTrail 日誌事件所建立之日誌群組。
4. 選擇 Create Metric Filter (建立指標篩選條件)。
5. 在 Define Logs Metric Filter (定義日誌指標篩選條件) 頁面上，選擇 Filter Pattern (篩選條件模式)，然後輸入下列命令：

   ```
   { ($.eventName = CreateFileSystem) && ($.responseElements.encrypted IS FALSE) }
   ```
6. 選擇 Assign Metric (指派指標)。
7. 針對 Filter Name (篩選條件名稱)，輸入 **UnencryptedFileSystemCreated**。
8. 針對 Metric Namespace (指標命名空間)，輸入 **CloudTrailMetrics**。
9. 針對 Metric Name (指標名稱)，輸入 **UnencryptedFileSystemCreatedEventCount**。
10. 選擇 Show advanced metric settings (顯示進階指標設定)。
11. 在 Metric Value (指標值) 中，輸入 **1**。
12. 選擇 Create Filter (建立篩選條件)。

建立警示

在您建立指標篩選條件之後，請使用下列程序來建立警示。

欲建立警示

1. 在 Log_Group_Name (Log_Group_Name) 頁面的 Filters (篩選條件) 的 UnencryptedFileSystemCreated (UnencryptedFileSystemCreated) 篩選名稱旁，選擇 Create Alarm (建立警示)。
2. 在 Create Alarm (建立警示) 頁面上，設定下列參數：

- 在 Name (名稱) 中，輸入 **`Unencrypted File System Created`**。
- 對於 Whenever (隨時)，執行下列動作：
  - 將 is (是) 設定為 *`> = 1`*
  - 將 for: (對於：) 設為 *`1`* 連續期間。
- 對於 Treat missing data as (將缺少資料視為)，選擇 good (not breaching threshold) (良好 (不違反閾值))。
- 對於 Actions (動作)，執行下列動作：
  - 在 Whenever this alarm (每當此警示) 中選擇 State is ALARM (狀態為警示)。
  - 對於 Send notification to (發送通知至)，選擇 NotifyMe (通知我)，選擇 New list (新增清單)，然後輸入此清單的唯一主題名稱。
  - 選擇 Email list (電子郵件清單)，然後輸入您要收到通知的電子郵件地址。您應會收到一封這個地址的電子郵件，確認您已建立此警示。
- 對於 Alarm Preview (警示預覽)，請執行下列動作：
  - 對於 Period (期間)，選擇 1 Minute (1 分鐘)。
  - 對於 Statistic (統計資料)，選擇 Standard (標準) 和 Sum (總和)。

3. 選擇 Create Alarm (建立警示)。

測試加密檔案系統之建立的警示

您可以建立未加密的檔案系統來測試警示，如下所示。

建立未加密的檔案系統來測試警示

1. 登入AWS Management Console，然後打開亞馬遜 EFS 控制台https://console.aws.amazon.com/efs/。
2. 選擇建立檔案系統顯示建立檔案系統對話方塊。
3. 要創建靜態未加密的文件系統，請選擇自訂顯示檔案系統設定(憑證已建立！) 頁面上的名稱有些許差異。
4. 適用於將軍設定，輸入以下內容。
   a. (選用) 輸入名稱對於檔案系統。
   b. 維持生命週期管理、效能模式，以及傳輸量模式設定為預設值。
   c. 關閉Encryption (加密)通過清除啟用靜態資料加密。

5. 選擇下一頁繼續網路存取步驟中的配置過程。
6. 選擇預設值Virtual Private Cloud (VPC)。
7. 適用於掛載目標下，選擇預設安全群組對於每個掛載目標。
8. 選擇下一頁顯示檔案系統政策(憑證已建立！) 頁面上的名稱有些許差異。
9. 選擇下一頁繼續Review and create (檢閱和建立)(憑證已建立！) 頁面上的名稱有些許差異。
10. 查看文件系統，然後選擇建立創建您的文件系統並返回檔案系統(憑證已建立！) 頁面上的名稱有些許差異。

您的線索記錄`CreateFileSystem`操作，並將事件傳送至 CloudWatch Logs 日誌組。事件會觸發指標警示，CloudWatch Logs 會將變更通知傳送給您。

逐步解說：使用 NFS 用戶端的 IAM 授權啟用根擠壓

在本逐步解說中，您將設定 Amazon EFS 以防止所有AWS主體的根目錄存取 Amazon EFS 檔案系統，但單一管理工作站除外。您可以透過為網路檔案系統AWS Identity and Access Management (NFS) 用戶端設定 (IAM) 授權來執行此操作。如需 EFS 中 NFS 用戶端 IAM 授權的詳細資訊，請參閱使用 IAM 控制檔案系統資料存取。

若要執行這項操作，需要設定兩個 IAM 許可政策，如下所示：

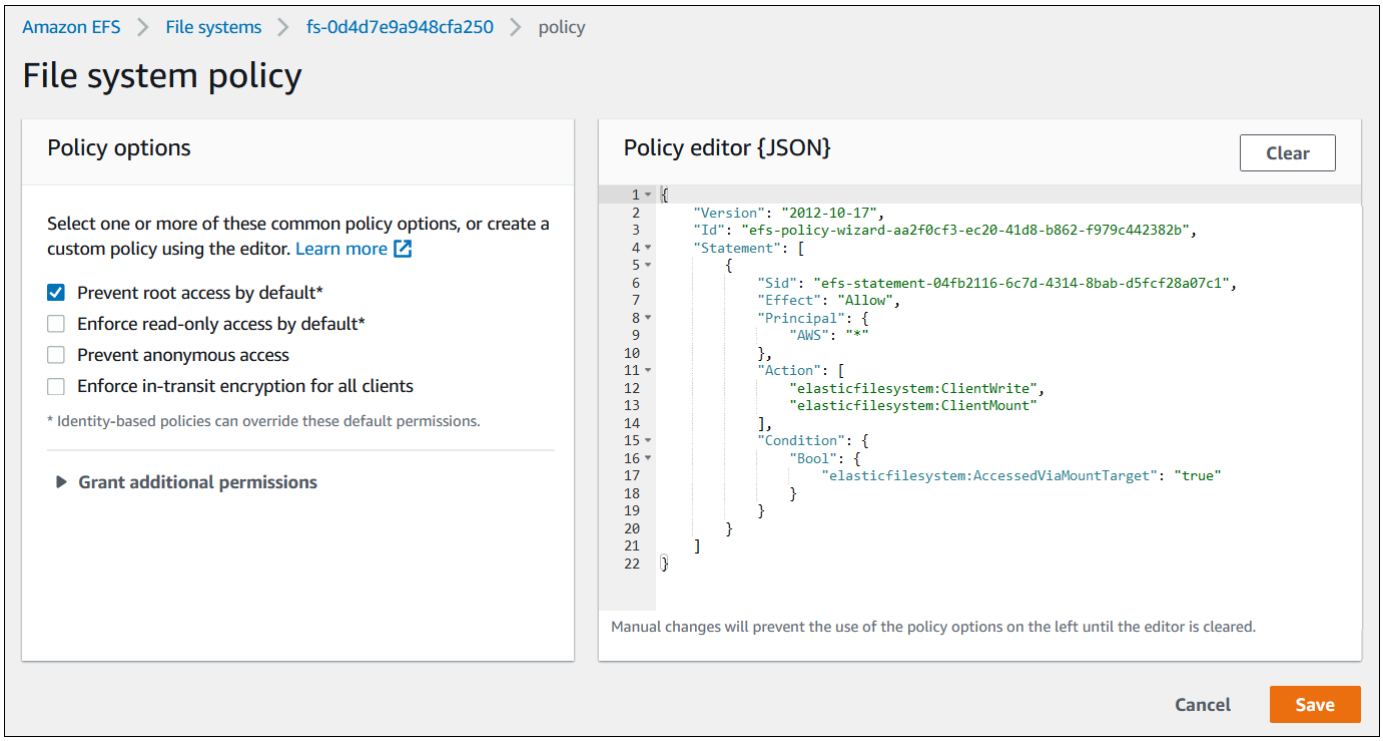
- 建立 EFS 檔案系統政策，此政策會明確允許檔案系統的讀取和寫入存取權，並隱含拒絕根存取權。
- 使用 Amazon EC2 執行個體設定檔，將 IAM 身分指派給需要檔案系統根存取權的 Amazon EC2 管理工作站。如需 Amazon EC2 執行個體設定檔的詳細資訊，請參閱使用AWS Identity and Access Management者指南中的使用執行個體設定檔。
- 將 `AmazonElasticFileSystemClientFullAccess` AWS 受管理政策指派給管理工作站的 IAM 角色。如需 EFSAWS 受管政策的詳細資訊，請參閱Amazon Elastic File System 的身分與存取管理。

若要針對 NFS 用戶端使用 IAM 授權來啟用根權限壓縮，請使用下列程序。

若要防止 root 存取檔案系統

1. 開啟 Amazon Elastic File System 主控台，網址為 https://console.aws.amazon.com/efs/。
2. 選擇檔案系統。
3. 在 File systems (檔案系統) 頁面上，選擇您要啟用根權限壓縮的檔案系統。

4. 在 [檔案系統詳細資料] 頁面上，選擇 [檔案系統原則]，然後選擇 [編輯]。File system policy (檔案系統政策) 頁面隨即顯示。



5. 選擇 [原則選項] 下的 [預設防止 root 存取權限] *。原則 JSON 物件會顯示在 [原則編輯器] 中。
6. 選擇 Save (儲存) 以儲存檔案系統政策。

非匿名用戶端可以透過以身分為基礎的政策取得檔案系統的根存取權。當您將`AmazonElasticFileSystemClientFullAccess`受管政策附加到工作站的角色時，IAM 會根據工作站的身分識別政策授予工作站的 root 存取權。

透過管理工作站啟用根存取權

1. 前往網址 https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。
2. 建立 Amazon EC2 EC2 的大型`EFS-client-root-access`。IAM 建立與您建立的 EC2 角色名稱相同的執行個體設定檔。
3. 將 AWS 受管政策指派 `AmazonElasticFileSystemClientFullAccess` 給您建立的 EC2 角色。本政策的內容如下所示。

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

```
            "Effect": "Allow",
            "Action": [
                    "elasticfilesystem:ClientMount",
                    "elasticfilesystem:ClientRootAccess",
                    "elasticfilesystem:ClientWrite",
                    "elasticfilesystem:DescribeMountTargets"
            ],
            "Resource": "*"
        }
    ]
}
```

4. 將執行個體描述檔連接至您用來做為管理工作站的 EC2 執行個體，如下所述。如需詳細資訊，請參閱《適用於 Linux 執行個體的 Amazon EC2 使用者指南》中的可用的執行個體類型。

   a. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。

   b. 在導覽窗格中，選擇 Instances (執行個體)。

   c. 選擇執行個體。針對 Actions (動作)，選擇 Instance Settings (執行個體設定)，然後選擇 Attach/Replace IAM role (連接/取代 IAM 角色)。

   d. 選擇您在第一個步驟中建立的 IAM 角色 `EFS-client-root-access`，然後選擇 Apply (套用)。

5. 在管理工作站上安裝 EFS 掛載協助程式。如需 EFS 掛載協助程式和 amazon-efs-utils 套件的詳細資訊，請參閱安裝 Amazon EFS 工具。

6. 透過使用下列命令搭配 `iam` 掛載選項，在管理工作站上掛載 EFS 檔案系統。

```
$ sudo mount -t efs -o tls,iam file-system-id:/ efs-mount-point
```

   您可以將 Amazon EC2 執行個體設定為使用 IAM 授權自動掛接檔案系統。如需詳細 EFS 訊，請參閱使用 IAM 授權掛載。

Amazon EFS 中的安全

AWS 共同責任模型適用於 Amazon Elastic File System 中的資料保護。如此模型中所述， AWS 負責保護執行所有 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，我們建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 登入資料並設定個別使用者。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 資源進行通訊。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。
- 使用 AWS 加密解決方案以及其中的所有默認安全控制 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。
- 如果您在透過命令列介面或 API 存取時需要經 AWS 過 FIPS 140-2 驗證的加密模組，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) 140-2 概觀。

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。這包括當您使用主控台、API 或 AWS SDK AWS 服務 使用 EFS 或其他工作時。AWS CLI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。

主題

- Amazon EFS 中的彈性
- Amazon EFS 的網路隔離

Amazon EFS 的資料加密

Amazon EFS 支援兩種檔案系統加密形式：傳輸中加密和靜態加密。您可在 Amazon EFS 檔案系統建立時啟用靜態資料加密。當您掛載檔案系統時，可以啟用對傳輸中的資料加密。

如果您在透過命令列介面或 API 存取時需要經 AWS 過 FIPS 140-2 驗證的加密模組，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) 140-2 概觀。

如果您的組織需要遵守公司或法規政策，該政策要求對靜態資料和中繼資料進行加密，我們建議建立一個靜態加密的檔案系統，並使用傳輸中的資料加密來掛載您的檔案系統。

加密靜態資料

您可以使用 AWS Management Console、或透過 Amazon EFS API 或其中 AWS CLI一個 AWS 開發套件以程式設計方式建立加密的檔案系統。您的組織可能需要對符合特定分類所有資料進行加密，或是與特定應用程式、工作負載或環境相關聯。

建立 EFS 檔案系統之後，您無法變更其加密設定。這表示您無法修改未加密的檔案系統，使其加密。反之，您需要建立新的加密檔案系統。

> **Note**
>
> AWS 金鑰管理基礎架構使用聯邦資訊處理標準 (FIPS) 140-2 核准的加密演算法。基礎設施符合國家標準技術研究所 (NIST) 800-57 的建議。

在 Amazon EFS 檔案系統上強制執行靜態加密。

您可以在 AWS Identity and Access Management (IAM) 身分型政策中使用 `elasticfilesystem:Encrypted` IAM 條件索引鍵，以控制使用者是否可以建立靜態加密的 Amazon EFS 檔案系統。如需有關使用條件索引鍵的詳細資訊，請參閱 範例：強制建立加密檔案系統。

您也可以在內部 AWS Organizations 定義服務控制政策 (SCP)，為組織中的所有 AWS 帳戶人強制執行 EFS 加密。如需有關中的服務控制策略的詳細資訊 AWS Organizations，請參閱《AWS Organizations 使用指南》中的服務控制策略。

使用主控台對靜態的檔案系統進行加密

使用 Amazon EFS 主控台建立新檔案系統時，預設下會啟用靜態加密。下列程序說明當您從主控台建立新的檔案系統時，如何為其啟用加密。

> **Note**
>
> 使用 AWS CLI、API 和 SDK 建立新檔案系統時，預設下不會啟用靜態加密。如需詳細資訊，請參閱 建立檔案系統 (AWS CLI)。

使用 EFS 主控台加密新的檔案系統

1. 前往 https://console.aws.amazon.com/efs/ 開啟 Amazon Elastic File System 主控台。
2. 選擇建立檔案系統以開啟建立檔案系統對話方塊。
3. (選用) 輸入您的檔案系統名稱。
4. 對於虛擬私有雲端 (VPC)，請選擇您的 VPC，或將其設定為預設 VPC。
5. 選擇建立以建立使用下列服務建議設定的檔案系統：
   - 使用 Amazon EFS (`aws/elasticfilesystem`) 的預設值 AWS KMS key 啟用靜態資料加密功能。
   - 開啓自動備份：如需詳細資訊，請參閱 備份 Amazon EFS 檔案系統。
   - 掛載：Amazon EFS 會使用下列設定建立掛載目標：
     - 位於建立檔案系統 AWS 區域 的每個可用區域中。
     - 位於所選 VPC 的預設子網路中。
     - 使用 VPC 的預設安全群組。建立檔案系統之後，您可以管理安全群組。

     如需詳細資訊，請參閱 管理檔案系統網路存取權限。
   - 「一般用途」效能模式：如需詳細資訊，請參閱 效能模式。
   - 「彈性輸送量」模式：如需詳細資訊，請參閱 輸送量模式。
   - 使用 30 天政策啟用「生命週期」管理：如需詳細資訊，請參閱 管理檔案系統儲存。
6. 檔案系統頁面上方會出現一個橫幅，顯示您建立的檔案系統狀態。當檔案系統可供使用時，橫幅中會出現存取檔案系統詳細資訊頁面的連結。

您現在有了新的 encrypted-at-rest 檔案系統。

靜態加密的運作方式

在加密的檔案系統中，資料和中繼資料會自動加密後再寫入檔案系統。同樣地，隨著資料和中繼資料受到讀取，會自動將他們解密再顯示給應用程式。這些程序是由 Amazon EFS 以透明方式處理，因此您不必修改應用程式。

Amazon EFS 使用產業標準的 AES-256 加密演算法來靜態加密 EFS 資料和中繼資料。如需詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的密碼編譯基礎。

Amazon EFS 如何使用 AWS KMS

Amazon EFS 與 AWS Key Management Service (AWS KMS) 整合以進行金鑰管理。Amazon EFS 使用客戶金鑰來加密檔案系統，方式如下：

- 靜態中繼資料加密 — Amazon EFS 使 AWS 受管金鑰 用 Amazon EFS 來加密和解密檔案系統中繼資料 (也就是檔案名稱、目錄名稱和目錄內容)。`aws/elasticfilesystem`
- 加密靜態檔案資料：您選擇用於加密和解密檔案資料的客戶受管金鑰(也就是檔案的內容)。您可以啟用、停用或撤銷對此客戶自管金鑰的授予。此客戶受管金鑰可以是下列兩種類型之一：
  - AWS 受管金鑰 適用於 Amazon EFS — 這是預設的客戶受管金鑰`aws/elasticfilesystem`。客戶受管金鑰建立和儲存時不會產生費用，但使用會產生費用。如需進一步了解，請參閱 AWS Key Management Service 定價。
  - 客戶受管金鑰：這是使用起來最靈活的 KMS 金鑰，因為您可以設定它的金鑰政策和授予多個使用者或服務。如需建立客戶受管金鑰的詳細資訊，請參閱 AWS Key Management Service 開發人員指南中的建立金鑰。

    如果您為檔案資料加密和解密使用客戶受管金鑰，則可以啓用金鑰輪換。當您啟用按鍵輪換時，每年 AWS KMS 會自動旋轉金鑰一次。此外，使用客戶受管金鑰后，您可以選擇隨時停用、重新啟用、刪除或撤銷對客戶受管金鑰的存取。如需詳細資訊，請參閱 管理檔案系統 KMS 金鑰的存取權。

> **Important**
>
> Amazon EFS 僅接受對稱的客戶受管金鑰。您無法在 Amazon EFS 中使用非對稱的客戶受管金鑰。

靜態資料加密和解密都會以透明方式處理。不過，Amazon EFS 專屬的 AWS 帳戶 ID 會顯示在與 AWS KMS 動作相關的 AWS CloudTrail 日誌中。如需詳細資訊，請參閱 適用於檔案系統的 Amazon EFS 日誌 encrypted-at-rest檔項目。

Amazon EFS 關鍵政策 AWS KMS

金鑰政策是控制對客戶受管金鑰存取的主要方式。如需關於金鑰政策的詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的在 AWS KMS中使用金鑰政策。下列清單說明 Amazon EFS 對於靜態檔案系統加密所需或以其他方式支援的所有 AWS KMS與 — 相關許可：

- kms:Encrypt：(選用) 將純文字加密為加密文字。此許可會納入預設的金鑰政策中。
- kms:Decrypt：(必要) 對密文進行解密。加密文字為之前已加密的純文字。此許可會納入預設的金鑰政策中。
- kms: ReEncrypt — (選用) 使用新的客戶管理金鑰對伺服器端的資料進行加密，而不會在用戶端公開資料的明文。資料會先解密，然後重新加密。此許可會納入預設的金鑰政策中。
- kms：GenerateDataKeyWithout純文字 — (必要) 傳回以客戶管理金鑰加密的資料加密金鑰。此權限包含在 kms: K GenerateData ey* 下的預設金鑰原則中。
- kms: CreateGrant — (必要) 將授權新增至金鑰，以指定誰可以使用金鑰，以及在何種情況下可以使用金鑰。授予是金鑰政策的備用許可機制。如需授權的詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的使用授權。此許可會納入預設的金鑰政策中。
- kms: DescribeKey — (必要) 提供有關指定客戶管理金鑰的詳細資訊。此許可會納入預設的金鑰政策中。
- kms: ListAliases — (選用) 列出帳戶中的所有金鑰別名。當您使用主控台來建立加密的檔案系統時，此許可會填入選擇 KMS 金鑰清單。我們建議您使用此許可，以提供最佳使用者體驗。此許可會納入預設的金鑰政策中。

AWS 受管金鑰 Amazon EFS KMS 政策

Amazon EFS 的 AWS 受管金鑰 KMS 政策 JSON，`aws/elasticfilesystem`如下所示：

```
{
    "Version": "2012-10-17",
    "Id": "auto-elasticfilesystem-1",
    "Statement": [
        {
            "Sid": "Allow access to EFS for all principals in the account that are
 authorized to use EFS",
            "Effect": "Allow",
```

```
            "Principal": {
                "AWS": "*"
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:CreateGrant",
                "kms:DescribeKey"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "elasticfilesystem.us-east-2.amazonaws.com",
                    "kms:CallerAccount": "111122223333"
                }
            }
        },
        {
            "Sid": "Allow direct 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": "*"
        }
    ]
}
```

加密傳輸中的資料

已在使用 Amazon EFS 掛載協助程式來掛載檔案系統時，透過啟用 Transport Layer Security (TLS) 來完成對 Amazon EFS 檔案系統之傳輸中的資料啟用加密。如需詳細資訊，請參閱 使用 EFS 掛載協助程式掛載 EFS 檔案系統。

將傳輸中的資料加密宣告為 Amazon EFS 檔案系統的掛載選項時，掛載協助程式會初始化用戶端 stunnel 程序。Stunnel 是一種開放原始碼多功能網路轉送。用戶端 stunnel 程序會在本機連接埠上監聽傳入流量，以及掛載協助程式會將網路檔案系統 (NFS) 用戶端流量重新導向到這個本機連接埠。掛載協助程式使用 TLS 版本 1.2 來與檔案系統通訊。

在啟用傳輸中的資料加密的狀態下，若要使用掛載協助程式掛載 Amazon EFS 檔案系統

1. 透過安全殼層 (SSH) 存取執行個體的終端機，並使用適當的使用者名稱登入。有關如何執行此操作的詳細資訊，請參閱使用安全殼層從 Linux 或 macOS Connect 到您的 Linux 執行個體。
2. 執行下列命令來掛載檔案系統。

```
sudo mount -t efs  -o tls fs-12345678:/ /mnt/efs
```

傳輸中加密的運作方式

若要啟用傳輸中的資料加密，請使用 TLS 連線到 Amazon EFS。我們建議您使用 EFS 掛載協助程式來掛載檔案系統，因為與使用 NFS `mount` 掛載相比，該程式可以簡化掛載程序。EFS 掛載協助程式會使用 `stunnel` TLS 來管理程序。如果您不是使用掛載協助程式，您仍然可以啟用對傳輸中的資料加密。高階執行步驟如下。

若要在不需 EFS 掛載協助程式的情況下啟用對傳輸中的資料加密

1. 下載並安裝 `stunnel`，並注意該應用程式所接聽的連接埠。請參閱 升級 `stunnel` 以取得執行此動作的指示。
2. 執行 `stunnel` 來使用 TLS 在連接埠 2049 上連接到 Amazon EFS 檔案系統。
3. 使用 NFS 用戶端，掛載 `localhost:`*`port`*，其中 *`port`* 是您在第一個步驟所記下的連接埠。

由於對傳輸中的資料加密是根據每個連線所設定，每個設定的掛載擁有在執行個體上執行的專門 `stunnel` 程序。預設情況下，由 EFS 掛載協助程式使用的 `stunnel` 程序會在本機連接埠上從 20049 到 21049 進行監聽，並連接至連接埠 2049 上的 Amazon EFS。

> **Note**
>
> 預設情況下，當使用 Amazon EFS 掛載協助程式搭配 TLS 時，掛載協助程式會強制執行憑證主機名稱檢查。Amazon EFS 掛載協助程式使用其 TLS 功能的 `stunnel` 程式。有些版本的 Linux 不包含預設支援這些 TLS 功能的 stunnel 版本。使用其中一個 Linux 版本時，使用 TLS 掛載 Amazon EFS 檔案系統。

> 你已經安裝了 amazon-efs-utils 軟件包後，升級你的系統版本 stunnel 看升級 stunnel到。對於加密的問題，請參閱 故障診斷加密。

使用傳輸中的資料加密時，您的 NFS 用戶端設定會隨之變更。檢查您的主動掛載檔案系統時，您會看到一個掛載至 127.0.0.1 或 `localhost` 的檔案系統，如下列範例。

```
$ mount | column -t
127.0.0.1:/  on  /home/ec2-user/efs        type  nfs4
 (rw,relatime,vers=4.1,rsize=1048576,wsize=1048576,namlen=255,hard,proto=tcp,port=20127,timeo=6
```

使用 TLS 和 Amazon EFS 掛載協助程式進行掛載時，則將 NFS 用戶端重新設定為掛載到本機連接埠。EFS 掛載協助程式會開始用戶端 `stunnel` 程序，其會在本機連接埠上進行監聽，`stunnel` 會使用 TLS 開啟對 EFS 檔案系統的加密連線。EFS 掛載協助程式負責設定和維護此加密連線和關聯的組態。

若要判斷 Amazon EFS 檔案系統 ID 所對應的是哪個本機掛載點，您可以使用以下命令。將 *`efs-mount-point`* 取代為您已掛載檔案系統的本機路徑。

```
grep -E "Successfully mounted.*efs-mount-point" /var/log/amazon/efs/mount.log | tail -1
```

使用掛載協助程式以加密傳輸中的資料時，它也會建立名為 `amazon-efs-mount-watchdog` 的程序。此程序可確保每個掛載的 stunnel 程序為執行中，並在 Amazon EFS 檔案系統卸載時停止 stunnel。如果因為某些原因而導致 stunnel 程序意外終止，監視程式程序會將其重新啟動。

故障診斷加密

您可以在下面找到如何排解 Amazon EFS 加密問題的相關資訊。

- 以傳輸中的資料加密進行的掛載失敗
- 以傳輸中的資料加密進行的掛載已中斷
- E ncrypted-at-rest 檔案系統無法建立
- 無法使用加密的檔案系統

以傳輸中的資料加密進行的掛載失敗

預設情況下，當您使用 Amazon EFS 掛載協助程式搭配 Transport Layer Security (TLS) 時，它會強制執行主機名稱檢查。有些系統不支援此功能，例如當您使用 Red Hat Enterprise Linux 或 CentOS 時。在這些情況下，使用 TLS 來掛載 EFS 檔案系統會失敗。

採取動作

我們建議在您的用戶端升級 stunnel 版本以支援主機名稱檢查。如需詳細資訊，請參閱 升級 stunnel。

以傳輸中的資料加密進行的掛載已中斷

您的 Amazon EFS 檔案系統已加密連線可能會因為用戶端事件而停止回應或中斷，這是有可能發生的事，但機率不高。

採取動作

如果您的以傳輸中的資料加密的 Amazon EFS 檔案系統連線被中斷，請執行以下步驟：

1. 請確認 stunnel 服務正在用戶端上執行。
2. 請確認監視程式應用程式 amazon-efs-mount-watchdog 正在用戶端上執行。此應用程式正在執行，您可以找出是否使用下列命令：

```
ps aux | grep [a]mazon-efs-mount-watchdog
```

3. 檢查您的支援日誌。如需詳細資訊，請參閱 取得支援日誌。
4. 或者，您也可以啟用您的 stunnel 日誌並檢查那些資訊。您可以在 /etc/amazon/efs/efs-utils.conf 中變更您的日誌組態以啟用 stunnel 日誌。然而如此一來，您就必須使用掛載協助程式卸載該檔案系統，然後再重新掛載以讓該變更生效。

> **Important**
>
> 啟用 stunnel 日誌可能會在您的檔案系統佔用極大的空間。

如果中斷繼續，請聯絡 Sup AWS port 部門。

E ncrypted-at-rest 檔案系統無法建立

您已嘗試建立新的 encrypted-at-rest 檔案系統。但是，您會收到一條錯誤消息，指出 AWS KMS 無法使用。

採取動作

此錯誤可能發生在極少數情況下暫 AWS KMS 時無法在您的 AWS 區域. 如果發生這種情況，請等到 AWS KMS 恢復完整的可用性，然後再試一次建立檔案系統。

無法使用加密的檔案系統

加密檔案系統持續傳回 NFS 伺服器錯誤。當 EFS 因 AWS KMS 為下列其中一個原因而無法從擷取主金鑰時，可能會發生這些錯誤：

- 該金鑰已停用。
- 該金鑰已刪除。
- Amazon EFS 使用金鑰的許可已被撤銷。
- AWS KMS 暫時無法使用。

採取動作

首先，確認 AWS KMS 金鑰已啟用。您可以在主控台中檢視金鑰是否已啟用。如需詳細資訊，請在《AWS Key Management Service 開發人員指南》中的檢視金鑰。

如果該金鑰未啟用，請將其啟用。如需詳細資訊，請參閱在《AWS Key Management Service 開發人員指南》中的啟用和停用金鑰。

如果該金鑰正在等待刪除，則此狀態會停用金鑰。您可以取消刪除並重新啟用該金鑰。如需詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的排程和取消金鑰刪除。

如果金鑰已啟用，而您仍然遇到問題，或者重新啟用金鑰時遇到問題，請聯絡 Sup AWS port 部門。

Amazon Elastic File System 的身分與存取管理

AWS Identity and Access Management (IAM) 是一種 AWS 服務，讓管理員能夠安全地控制對 AWS 資源的存取權。IAM 管理員可控制哪些人員可進行身分驗證 (登入) 並獲得授權 (具有許可) 以使用 Amazon MSK 資源。IAM 是一種您可以免費使用的 AWS 服務。

主題

對象

AWS Identity and Access Management (IAM) 的使用方式會不同，取決於您在 Amazon EFS 中所執行的工作。

服務使用者：如果您使用 Amazon EFS 執行任務，您的管理員會為您提供您需要的憑證和許可。隨著您為了執行作業而使用的 Amazon EFS 功能數量變多，您可能會需要額外的許可。瞭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 Amazon EFS 中的功能，請參閱 Amazon Elastic File System 身分識別和存取疑難排解。

服務管理員：若您在公司負責管理 Amazon EFS 資源，您應該擁有 Amazon EFS 的完整存取權。您的任務是判斷服務使用者應存取的 Amazon EFS 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可搭配 Amazon EFS 使用 IAM 的方式，請參閱 Amazon Elastic File System 如何與 IAM 協同工作。

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 Amazon SNS 存取權的詳細資訊。若要檢視您可以在 IAM 中使用的基於 Amazon EFS 身分的政策範例，請參閱 Amazon Elastic File System 的身分型政策範例。

使用身分驗證

身分驗證是使用身分憑證登入 AWS 的方式。您必須以 AWS 帳戶根使用者、IAM 使用者身分，或擔任 IAM 角色進行 驗證（登入至 AWS）。

您可以使用透過身分來源 AWS IAM Identity Center 提供的憑證，以聯合身分登入 AWS。(IAM Identity Center) 使用者、貴公司的單一登入身分驗證和您的 Google 或 Facebook 憑證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。您 AWS 藉由使用聯合進行存取時，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。如需有關登入至 AWS 的詳細資訊，請參閱《AWS 登入 使用者指南》中的如何登入您的 AWS 帳戶。

如果您是以程式設計的方式存取 AWS，AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以便使用您的憑證透過密碼編譯方式簽署您的請求。如果您不使用 AWS 工具，您必須自行簽署請求。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》中的簽署 AWS API 請求。

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) 以提高帳戶的安全。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》中的在 AWS 中使用多重要素驗證 (MFA)。

AWS 帳戶 根使用者

如果是建立 AWS 帳戶，您會先有一個登入身分，可以完整存取帳戶中所有 AWS 服務 與資源。此身分稱為 AWS 帳戶 根使用者，使用建立帳戶時所使用的電子郵件地址和密碼即可登入並存取。強烈建議您不要以根使用者處理日常作業。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）搭配身分提供者使用聯合功能，使用暫時憑證來存取 AWS 服務。

聯合身分是來自您企業使用者目錄的使用者、Web 身分供應商、AWS Directory Service、Identity Center 目錄或透過身分來源提供的憑證來存取 AWS 服務 的任何使用者。聯合身分存取 AWS 帳戶時，會擔任角色，並由角色提供暫時憑證。

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，也可以連線並同步到自己身分來源中的一組使用者和群組，以便在您的所有 AWS 帳戶和應用程式中使用。如需 IAM Identity Center 的相關資訊，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 使用者是您 AWS 帳戶 中的一種身分，具備單一人員或應用程式的特定許可。建議您盡可能依賴暫時憑證，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。如需詳細資訊，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。您無法以群組身分登入。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過程變得更為容易。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，但角色僅提供暫時憑證。如需進一步了解，請參閱《IAM 使用者指南》中的建立 IAM 使用者 (而非角色) 的時機。

IAM 角色

IAM 角色是您 AWS 帳戶 中的一種身分，具備特定許可。它類似 IAM 使用者，但不與特定的人員相關聯。您可以在 AWS Management Console 中透過切換角色來暫時取得 IAM 角色。您可以透過呼叫 AWS CLI 或 AWS API 操作，或是使用自訂 URL 來取得角色。如需使用角色的方法詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM 角色。

使用暫時憑證的 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，並取得由角色定義的許可。如需有關聯合角色的詳細資訊，請參閱《IAM 使用者指南》中的為第三方身分供應商建立角色。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。
- 跨帳户存取權 – 您可以使用 IAM 角色，允許不同帳戶中的某人（信任的委託人）存取您帳戶中的資源。角色是授予跨帳户存取權的主要方式。但是，針對某些 AWS 服務，您可以將政策直接連接到資源（而非使用角色作為代理）。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 角色與資源類型政策的差異。
- 跨服務存取 – 有些 AWS 服務 會使用其他 AWS 服務 中的功能。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。

- 轉發存取工作階段 (FAS)：當您使用 IAM 使用者或角色在 AWS 中執行動作時，系統會將您視為主體。當您使用某些服務時，您可能會執行一個動作，而該動作之後會在不同的服務中啟動另一個動作。FAS 使用主體的許可呼叫 AWS 服務，搭配請求 AWS 服務 以向下游服務發出請求。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之後，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》https://docs.aws.amazon.com/IAM/latest/UserGuide/access_forward_access_sessions.html。
- 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給 AWS 服務 服務。
- 服務連結角色 – 服務連結角色是一種連結到 AWS 服務 的服務角色類型。服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的 AWS 帳戶 中，並由該服務所擁有。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 – 針對在 EC2 執行個體上執行並提出 AWS CLI 和 AWS API 請求的應用程式，您可以使用 IAM 角色來管理暫時憑證。這是在 EC2 執行個體內儲存存取金鑰的較好方式。如需指派 AWS 角色給 EC2 執行個體並提供其所有應用程式使用，您可以建立連接到執行個體的執行個體設定檔。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暫時憑證。如需詳細資訊，請參閱《IAM 使用者指南》中的利用 IAM 角色來授予許可給 Amazon EC2 執行個體上執行的應用程式。

如需了解是否要使用 IAM 角色或 IAM 使用者，請參閱《IAM 使用者指南》中的建立 IAM 角色 (而非使用者) 的時機。

使用政策管理存取權

您可以透過建立政策並將其附加到 AWS 身分或資源，在 AWS 中控制存取。政策是 AWS 中的一個物件，當其和身分或資源建立關聯時，便可定義其許可。AWS 會在主體（使用者、根使用者或角色工作階段）發出請求時評估這些政策。政策中的許可，決定是否允許或拒絕請求。大部分政策以 JSON 文件形式儲存在 AWS 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哪些內容。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。若要授與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。具備該政策的使用者便可以從 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。若要了解如何建立身分類型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

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。受管政策則是獨立的政策，您可以將這些政策附加到 AWS 帳戶 中的多個使用者、群組和角色。受管政策包含 AWS 管理政策和客戶管理政策。如需瞭解如何在受管政策及內嵌政策間選擇，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。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。主體可以包括帳戶、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) 可控制哪些委託人（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 Simple Storage Service (Amazon S3)、AWS WAF 和 Amazon VPC 是支援 ACL 的服務範例。若要進一步了解 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 支援其他較少見的政策類型。這些政策類型可設定較常見政策類型授與您的最大許可。

- 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。如需許可範圍的更多相關資訊，請參閱《IAM 使用者指南》中的 IAM 實體許可範圍。

- 服務控制政策 (SCP) – SCP 是 JSON 政策，可指定 AWS Organizations 中組織或組織單位 (OU) 的最大許可。AWS Organizations 服務可用來分組和集中管理您企業所擁有的多個 AWS 帳戶。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 AWS 帳戶根使用者。如需組織和 SCP 的更多相關資訊，請參閱《AWS Organizations 使用者指南》中的 SCP 運作方式。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合使用者的暫時工作階段時，作為參數傳遞。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。如需更多資訊，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 AWS 在涉及多種政策類型時如何判斷是否允許一項請求，請參閱《IAM 使用者指南》中的政策評估邏輯。

Amazon Elastic File System 如何與 IAM 協同工作

在您使用 IAM 管理對 Amazon EFS 的存取權之前，請瞭解哪些 IAM 功能可以與 Amazon EFS 搭配使用。

您可以搭配 Amazon Elastic File System 使用的 IAM 功能

IAM 功能	Amazon EFS 支援
身分型政策	是
資源型政策	是
政策動作	是
政策資源	是
政策條件索引鍵 (服務特定)	是
ACL	否

IAM 功能	Amazon EFS 支援
ABAC(政策中的標籤)	部分
臨時憑證	是
主體許可	是
服務角色	是
服務連結角色	是

如要全面瞭解 Amazon EFS 和其他 AWS 服務如何與大多數的 IAM 功能搭配使用，請參閱《IAM 使用者指南》中的可搭配 IAM 運作的 AWS 服務。

Amazon EFS 身分型政策

支援身分型政策	是

身分型政策是可以連接到身分 (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。若要瞭解如何建立身分類型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

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，因為這會套用至附加的使用者或角色。如要瞭解您在 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。

Amazon EFS 的身分型政策範例

若要檢視 Amazon EFS 身分類型政策的範例，請參閱Amazon Elastic File System 的身分型政策範例。

Amazon EFS 中的資源型政策

支援以資源基礎的政策	是

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。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。主體可以包括帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

若要啟用跨帳戶存取權，您可以指定在其他帳戶內的所有帳戶或 IAM 實體，作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。當主體和資源在不同的 AWS 帳戶 中時，受信任帳戶中的 IAM 管理員也必須授與主體實體 (使用者或角色) 存取資源的許可。其透過將身分型政策附加到實體來授予許可。不過，如果資源型政策會為相同帳戶中的主體授與存取，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 角色與資源型政策有何差異。

若要了解如何使用資源政策來控制檔案系統資料存取，請參閱 使用 IAM 控制檔案系統資料存取。若要了解如何將資源型政策連接到檔案系統，請參閱 建立檔案系統原則。

Amazon EFS 中的資源型政策範例

若要檢視 Amazon EFS 資源型政策的範例，請參閱 Amazon Elastic File System 的資源型政策範例。

Amazon EFS 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哪些內容。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。政策動作的名稱通常會和相關聯的 AWS API 操作相同。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。也有一些操作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與執行相關聯操作的許可。

若要查看 Amazon VPC 動作的清單，請參閱《服務授權參考》中的 Amazon EC2 定義的動作。

Amazon EFS 中的政策動作會在動作之前使用下列字首：

```
elasticfilesystem
```

如需在單一陳述式中指定多個動作，請用逗號分隔。

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

若要檢視 Amazon EFS 身分型政策的範例，請參閱 Amazon Elastic File System 的身分型政策範例。

Amazon EFS 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哪些內容。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 (例如列出作業)，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 Amazon EFS 資源類型及其 ARN 的詳細資訊，請參閱《服務授權參考》中的 Amazon Elastic File System 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 Amazon Elastic File System 定義的動作。

若要檢視 Amazon EFS 身分型政策的範例，請參閱 Amazon Elastic File System 的身分型政策範例。

Amazon EFS 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哪些內容。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。若您為單一條件索引鍵指定多個值，AWS 會使用邏輯 OR 操作評估條件。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與該 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 AWS 全域條件金鑰，請參閱《IAM 使用者指南》中的 AWS 全域條件內容金鑰。

若要查看 Amazon EFS 條件金鑰的清單，請參閱《服務授權參考》中的 Amazon Elastic File System 的條件金鑰。若要了解您可以搭配哪些動作和資源使用條件金鑰，請參閱 Amazon Elastic File System 定義的動作。

若要檢視 Amazon EFS 身分型政策的範例，請參閱 Amazon Elastic File System 的身分型政策範例。

Amazon EFS 中的 ACL

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。

在 Amazon EFS 中使用 ABAC

支援 ABAC (政策中的標籤)	部分

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 AWS 中，這些屬性稱為標籤。您可以將標籤附加到 IAM 實體 (使用者或角色)，以及許多 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。

若要根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件金鑰，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》中的什麼是 ABAC?。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)。

將暫時憑證與 Amazon EFS 搭配使用

支援臨時憑證	是

您使用臨時憑證進行登入時，某些 AWS 服務 無法運作。如需詳細資訊，包括那些 AWS 服務 搭配臨時憑證運作，請參閱《IAM 使用者指南》中的可搭配 IAM 運作的 AWS 服務。

如果您使用使用者名稱和密碼之外的任何方法登入 AWS Management Console，則您正在使用臨時憑證。例如，當您使用公司的單一登入(SSO)連結存取 AWS 時，該程序會自動建立臨時憑證。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 使用者指南中的切換至角色 (主控台)。

您可使用 AWS CLI 或 AWS API，手動建立臨時憑證。接著，您可以使用這些臨時憑證來存取 AWS。AWS 建議您動態產生臨時憑證，而非使用長期存取金鑰。如需詳細資訊，請參閱 IAM 中的暫時性安全憑證。

Amazon EFS 的跨服務主體許可

支援轉寄存取工作階段 (FAS)	是

當您使用 IAM 使用者或角色在 AWS 中執行動作時，您會被視為主體。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 使用主體的許可呼叫 AWS 服務，搭配請求 AWS 服務 以向下游服務發出請求。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

之後，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》。

Amazon SNS 的服務角色

支援服務角色	是

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給 AWS 服務。

> **Warning**
>
> 變更服務角色的許可可能會中斷 Amazon EFS 功能。只有在 Amazon EFS 提供指引時，才能編輯服務角色。

Amazon EFS 的服務連結角色

支援服務連結角色	是

服務連結角色是一種連結到 AWS 服務 的服務角色類型。服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的 AWS 帳戶 中，並由該服務所擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

如需關於建立或管理 Amazon EFS 服務連結角色的詳細資訊，請參閱 使用 Amazon EFS 的服務連結角色。

Amazon Elastic File System 的身分型政策範例

依預設，IAM 使用者和角色不具備建立或修改 Amazon EFS 資源的許可。他們也無法使用 AWS Management Console、AWS Command Line Interface (AWS CLI) 或 AWS API 執行任務。若要授與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。

若要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。

如需 Amazon EFS 所定義之動作和資源類型的詳細資訊，包括每種資源類型的 ARN 格式，請參閱《服務授權參考》中的 Amazon Elastic Container Registry 的動作、資源和條件索引鍵。

主題

政策最佳實務

身分型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 Amazon EFS 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 受管政策並朝向最低權限許可的目標邁進：如需開始授予許可給使用者和工作負載，請使用 AWS 受管政策，這些政策會授予許可給許多常用案例。它們可在您的 AWS 帳戶 中使用。我們建議您定義特定於使用案例的 AWS 客戶管理政策，以便進一步減少許可。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。
- 套用最低許可許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的權限。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。您也可以使用條件來授予對服務動作的存取權，前提是透過特定 AWS 服務（例如 AWS CloudFormation）使用條件。如需更多資訊，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，可協助您編寫安全且實用的政策。如需更多資訊，請參閱 IAM 使用者指南中的 IAM Access Analyzer 政策驗證。
- 需要多重要素驗證 (MFA)：如果存在需要 AWS 帳戶中 IAM 使用者或根使用者的情況，請開啟 MFA 提供額外的安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需更多資訊，請參閱 IAM 使用者指南中的設定 MFA 保護的 API 存取。

有關 IAM 中最佳實務的詳細資訊，請參閱《IAM 使用者指南》中的 IAM 安全最佳實務。

使用 Amazon EFS 主控台

若要存取 Amazon Elastic File System 主控台，您必須擁有最基本的一組許可。這些許可必須允許您列出和檢視您 AWS 帳戶 中 Amazon EFS 資源的詳細資訊。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，您不需要允許其最基本主控台許可。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。

為確保使用者和角色仍可使用 Amazon EFS 主控台，還請將 Amazon EFS `AmazonElasticFileSystemReadOnlyAccess` AWS 受管政策連接至實體。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。

您可以在 Amazon EFS 的 AWS 受管政策 中查看`AmazonElasticFileSystemReadOnlyAccess`和其他 Amazon EFS 受管服務政策。

範例：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，或是使用 AWS CLI 或 AWS API 透過編寫程式的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": "*"
        }
    ]
}
```

範例：強制建立加密檔案系統

下列範例說明了身分型政策，該政策授予主體只能建立加密檔案系統的權力。

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "elasticfilesystem:CreateFileSystem",
            "Condition": {
                "Bool": {
                    "elasticfilesystem:Encrypted": "true"
                }
            },
            "Resource": "*"
        }
    ]
}
```

如果將此政策指派給嘗試建立未加密檔案系統的使用者，則請求會失敗。無論使用者是否正在使用 AWS Management Console、AWS CLI、AWS API 或 SDK，都會看到類似下列內容的訊息：

```
User: arn:aws:iam::111122223333:user/username is not authorized to
      perform: elasticfilesystem:CreateFileSystem on the specified resource.
```

範例：強制建立未加密檔案系統

下列範例說明了身分型政策，該政策授予主體只能建立未加密檔案系統的權力。

```
{
```

```
    "Statement": [
      {
          "Effect": "Allow",
          "Action": "elasticfilesystem:CreateFileSystem",
          "Condition": {
              "Bool": {
                  "elasticfilesystem:Encrypted": "false"
              }
          },
          "Resource": "*"
      }
  ]
}
```

如果將此政策指派給嘗試建立加密檔案系統的使用者，則請求會失敗。無論使用者是否正在使用 AWS Management Console、AWS CLI、AWS API 或 SDK，都會看到類似下列內容的訊息：

```
User: arn:aws:iam::111122223333:user/username is not authorized to
      perform: elasticfilesystem:CreateFileSystem on the specified resource.
```

您也可以通過建立 AWS Organizations 服務控制政策 (SCP) 來強制建立加密或未加密的 Amazon EFS 檔案系統。如需關於在 AWS Organizations 中的 SCP 控制政策的詳細資訊，請參閱《AWS Organizations 使用者政策》 中的服務控制政策。

Amazon Elastic File System 的資源型政策範例

在本節中，您可以找到授予或拒絕各種 Amazon EFS 動作許可的範例檔案系統政策。Amazon EFS 檔案系統政策字元限制在 20,000 以內。如需資訊行政策元素的資訊，請參閱 Amazon EFS 中的資源型政策。

> **Important**
>
> 如您將許可授予給檔案系統政策中的個別 IAM 使用者或角色，則請勿在該政策於檔案系統有效期間內刪除或重新建立該使用者或角色。如果上述情況發生，該使用者或角色將遭檔案系統鎖定，且將無法存取。如需詳細資訊，請參閱《IAM 使用者指南》中的指定主體。

如需關於如何建立檔案系統政策的詳細資訊，請參閱 建立檔案系統原則。

主題

範例：授與特定 AWS 角色的讀取和寫入存取權

在此範例中，EFS 檔案系統政策具有下列特性：

- 效果是 `Allow`。
- 主體設定為在 AWS 帳戶 中的 Testing_Role。
- 動作設定為 `ClientMount` (可讀) 和 `ClientWrite`。
- 授與許可的條件設定為 `AccessedViaMountTarget`。

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/Testing_Role"
            },
            "Action": [
                "elasticfilesystem:ClientWrite",
                "elasticfilesystem:ClientMount"
            ],
            "Resource": "arn:aws:elasticfilesystem:us-east-2:111122223333:file-system/
fs-1234abcd",
            "Condition": {
                "Bool": {
                    "elasticfilesystem:AccessedViaMountTarget": "true"
                }
            }
        }
    ]
}
```

範例：授予只讀存取權

下列檔案系統政策僅授予 `ClientMount` EfsReadOnly IAM 角色或唯讀許可。

```
{
    "Id": "read-only-example-policy02",
    "Statement": [
        {
            "Sid": "efs-statement-example02",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/EfsReadOnly"
            },
            "Action": [
                "elasticfilesystem:ClientMount"
            ],
            "Resource": "arn:aws:elasticfilesystem:us-east-2:111122223333:file-system/
fs-12345678"
        }
    ]
}
```

若要了解如何設定其他檔案系統政策，包括拒絕對所有 IAM 主體的根存取權 (特定管理工作站除外)，請參閱 逐步解說：使用 NFS 用戶端的 IAM 授權啟用根擠壓。

範例：授予 EFS 存取點存取權

您可以使用 EFS 存取政策，為 NFS 客戶端提供應用程式專屬的檢視，以查看 EFS 檔案系統中以共用檔案為基礎的資料集。您可以使用檔案系統政策授予檔案系統上的存取點權限。

此檔案政策範例使用條件元素來授予特定存取點，該存取點由其 ARN 對檔案系統的完整存取權限識別。

如需關於使用 EFS 存取點的詳細資訊，請參閱 使用 Amazon EFS 存取點。

```
{
    "Id": "access-point-example03",
    "Statement": [
        {
            "Sid": "access-point-statement-example03",
            "Effect": "Allow",
            "Principal": {"AWS": "arn:aws:iam::555555555555:role/
EfsAccessPointFullAccess"},
            "Action": "elasticfilesystem:Client*",
            "Resource": "arn:aws:elasticfilesystem:us-east-2:111122223333:file-system/
fs-12345678",
```

```
            "Condition": {
                "StringEquals": {
                    "elasticfilesystem:AccessPointArn":"arn:aws:elasticfilesystem:us-
east-2:555555555555:access-point/fsap-12345678" }
            }
        }
    ]
}
```

Amazon EFS 的 AWS 受管政策

AWS 管理的政策是由 AWS 建立和管理的獨立政策。AWS 管理的政策的設計在於為許多常見使用案例提供許可，如此您就可以開始將許可指派給使用者、群組和角色。

請謹記，AWS 管理的政策可能不會授予您特定使用案例的最低權限許可，因為它們可供所有 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。

您無法更改 AWS 管理的政策中定義的許可。如果 AWS 更新 AWS 管理的政策中定義的許可，更新會影響政策連接的所有主體身分 (使用者、群組和角色)。在推出新的 AWS 服務 或有新的 API 操作可供現有服務使用時，AWS 很可能會更新 AWS 管理的政策。

如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

AWS受管理的策略： AmazonElasticFileSystemFullAccess

您可將 `AmazonElasticFileSystemFullAccess` 政策連接到 IAM 身分。

此政策會授予管理許可，該許可允許通過 AWS Management Console 將政策完整存取到 Amazon EFS 和相關的 AWS 服務中。

許可詳細資訊

此政策包含以下許可。

- `elasticfilesystem`：允許主體在 Amazon EFS 主控台中執行所有動作。也允許主體使用 AWS Backup 建立 (`elasticfilesystem:Backup`) 和還原 (`elasticfilesystem:Restore`) 備份。
- `cloudwatch`— 允許校長在 Amazon EFS 主控台中描述 Amazon CloudWatch 檔案系統指標和指標的警示。
- `ec2`：允許主體在 Amazon EFS 主控台中建立、刪除和描述網路介面、描述和修改網路介面屬性、描述「可用區域」、安全群組、子網路、虛擬私有雲端 (VPC) 和與 Amazon EFS 檔案系統相關聯的 VPC 屬性。

- kms：允許主體列出 AWS Key Management Service (AWS KMS) 金鑰的別名，並在 Amazon EFS 主控台中描述 KMS 金鑰。
- iam：授予建立服務連結角色的許可，以允許 Amazon EFS 代表使用者管理 AWS 資源。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "cloudwatch:DescribeAlarmsForMetric",
                "cloudwatch:GetMetricData",
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcAttribute",
                "ec2:DescribeVpcs",
                "ec2:ModifyNetworkInterfaceAttribute",
                "elasticfilesystem:Backup",
                "elasticfilesystem:CreateFileSystem",
                "elasticfilesystem:CreateMountTarget",
                "elasticfilesystem:CreateTags",
                "elasticfilesystem:CreateAccessPoint",
                "elasticfilesystem:CreateReplicationConfiguration",
                "elasticfilesystem:DeleteFileSystem",
                "elasticfilesystem:DeleteMountTarget",
                "elasticfilesystem:DeleteTags",
                "elasticfilesystem:DeleteAccessPoint",
                "elasticfilesystem:DeleteFileSystemPolicy",
                "elasticfilesystem:DeleteReplicationConfiguration",
                "elasticfilesystem:DescribeAccountPreferences",
                "elasticfilesystem:DescribeBackupPolicy",
                "elasticfilesystem:DescribeFileSystems",
                "elasticfilesystem:DescribeFileSystemPolicy",
                "elasticfilesystem:DescribeLifecycleConfiguration",
                "elasticfilesystem:DescribeMountTargets",
                "elasticfilesystem:DescribeMountTargetSecurityGroups",
                "elasticfilesystem:DescribeReplicationConfigurations",
                "elasticfilesystem:DescribeTags",
```

```
                "elasticfilesystem:DescribeAccessPoints",
                "elasticfilesystem:ModifyMountTargetSecurityGroups",
                "elasticfilesystem:PutAccountPreferences",
                "elasticfilesystem:PutBackupPolicy",
                "elasticfilesystem:PutLifecycleConfiguration",
                "elasticfilesystem:PutFileSystemPolicy",
                "elasticfilesystem:UpdateFileSystem",
                "elasticfilesystem:UpdateFileSystemProtection",
                "elasticfilesystem:TagResource",
                "elasticfilesystem:UntagResource",
                "elasticfilesystem:ListTagsForResource",
                "elasticfilesystem:Restore",
                "kms:DescribeKey",
                "kms:ListAliases"
            ],

            "Sid": "ElasticFileSystemFullAccess",
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": "iam:CreateServiceLinkedRole",
            "Sid": "CreateServiceLinkedRoleForEFS",
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": [
                        "elasticfilesystem.amazonaws.com"
                    ]
                }
            }
        }
    ]
}
```

AWS受管理的策略： AmazonElasticFileSystemReadOnlyAccess

您可將 AmazonElasticFileSystemReadOnlyAccess 政策連接到 IAM 身分。

此政策通過 AWS Management Console 授予對 Amazon SageMaker 的只讀存取權。

許可詳細資訊

此政策包含以下許可。

- elasticfilesystem：允許主體在 Amazon EFS 主控台描述 Amazon EFS 檔案系統的屬性，包括帳戶偏好、備份和檔案系統政策、生命週期組態、掛載目標及其安全群組、標籤和存取點。
- cloudwatch— 允許主體在 Amazon EFS 主控台擷取 CloudWatch 指標並描述指標的警示。
- ec2：允許主體在 Amazon EFS 主控台中檢視「可用區域」、網路介面及其屬性、安全群組、子網路、VPC 及其屬性。
- kms：允許主體在 Amazon EFS 主控台中列出 AWS KMS 金鑰別名。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:DescribeAlarmsForMetric",
                "cloudwatch:GetMetricData",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcAttribute",
                "ec2:DescribeVpcs",
                "elasticfilesystem:DescribeAccountPreferences",
                "elasticfilesystem:DescribeBackupPolicy",
                "elasticfilesystem:DescribeFileSystems",
                "elasticfilesystem:DescribeFileSystemPolicy",
                "elasticfilesystem:DescribeLifecycleConfiguration",
                "elasticfilesystem:DescribeMountTargets",
                "elasticfilesystem:DescribeMountTargetSecurityGroups",
                "elasticfilesystem:DescribeTags",
                "elasticfilesystem:DescribeAccessPoints",
                "elasticfilesystem:DescribeReplicationConfigurations",
                "elasticfilesystem:ListTagsForResource",
                "kms:ListAliases"
            ],

            "Resource": "*"
```

```
        }
    ]
}
```

AWS受管政策： AmazonElasticFileSystemClientReadWrite存取

您可以將 `AmazonElasticFileSystemClientReadWriteAccess` 政策附加到 IAM 身分中。

此政策會授予 Amazon EFS 檔案系統的讀寫用戶端存取權。此政策允許 NFS 用戶端掛載、讀取和寫入到 Amazon EFS 檔案系統中。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "elasticfilesystem:ClientMount",
                "elasticfilesystem:ClientWrite",
                "elasticfilesystem:DescribeMountTargets"
            ],
            "Resource": "*"
        }
    ]
}
```

Amazon EFS 的 AWS 受管政策更新

檢視自 Amazon EFS 開始追蹤其 AWS 受管政策變更以來的政策更新詳細資訊。如需有關此頁面變更的自動提醒，請訂閱 Amazon EFS 文件歷史紀錄 頁面的 RSS 摘要。

變更	描述	日期
更新至現有政策	政策：AmazonElasticFileSystemFullAccess Amazon EFS 新增許可，以允許主體在檔案系統上停用和啟用保護。需要許可才能允許 Amazon EFS 複寫到現有檔案系統中。	2023 年 11 月 27 日
更新至現有政策	政策：AmazonElasticFileSystemServiceRolePolicy	2022 年 1 月 25 日

變更	描述	日期
	Amazon EFS 新增許可，以允許主體建立、描述和刪除 Amazon EFS 複寫，以及建立 Amazon EFS 檔案系統。需要許可才能允許 Amazon EFS 代表使用者管理檔案系統複寫組態。	
更新至現有政策	政策：AmazonElasticFileSystemReadOnlyAccess Amazon EFS 新增許可，以允許主體描述 Amazon EFS 複寫。需要許可才能允許使用者檢視檔案系統複寫組態。	2022 年 1 月 25 日
更新至現有政策	政策：AmazonElasticFileSystemFullAccess Amazon EFS 新增許可，以允許主體建立、描述和刪除 Amazon EFS 複寫。需要許可才能允許使用者管理檔案系統複寫組態。	2022 年 1 月 25 日
開始追蹤政策	政策：AmazonElasticFileSystemClientReadWrite存取 授與 NFS 用戶端在 Amazon EFS 檔案系統上讀取和寫入的權限。	2022 年 1 月 3 日
開始追蹤政策	政策：AmazonElasticFileSystemServiceRolePolicy Amazon EFS 的服務連結角色許可	2021 年 10 月 8 日
更新至現有政策	政策：AmazonElasticFileSystemFullAccess Amazon EFS 新增許可，以允許主體修改和描述 Amazon EFS 帳戶偏好。需要許可才能允許使用者在 Amazon EFS 主控台中檢視和設定帳戶偏好設定。	2021 年 5 月 7 日
更新至現有政策	政策：AmazonElasticFileSystemReadOnlyAccess Amazon EFS 新增許可，以允許主體描述 Amazon EFS 帳戶偏好。需要許可才能允許使用者在 Amazon EFS 主控台中檢視帳戶偏好設定。	2021 年 5 月 7 日

變更	描述	日期
Amazon EFS 開始追蹤變更	Amazon EFS 開始追蹤其 AWS 受管政策的變更	2021 年 5 月 7 日

搭配亞馬遜 EFS 使用標籤

您可以使用標籤來控制對 Amazon EFS 資源的存取，以及實作屬性型存取控制 (ABAC)。如需詳細資訊，請參閱：

- 標記 Amazon EFS 資源
- 根據資源的標籤控制存取
- 的 ABAC 是什麼AWS？ 在 IAM 使用者指南中的〈〉

> **Note**
>
> Amazon EFS 複寫不支援使用標籤進行屬性型存取控制 (ABAC)。

若要在建立期間將標籤套用至 Amazon EFS 資源，使用者必須擁有特定AWS Identity and Access Management (IAM) 許可。

在建立期間授予標籤資源的許可

以下標籤建立 Amazon EFS API 動作可讓您在建立資源時指定標籤。

- `CreateAccessPoint`
- `CreateFileSystem`

若要讓使用者在建立期間標籤資源，他們必須具備使用者在建立資源時標籤資源，例如`elasticfilesystem:CreateAccessPoint`或`elasticfilesystem:CreateFileSystem`。若標籤於資源建立動作指定，請針對動作AWS執行其他授權，以確認使用者具備建立標籤的許可。`elasticfilesystem:TagResource`因此，使用者必須同時具備使用 `elasticfilesystem:TagResource` 動作的明確許可。

在 elasticfilesystem:TagResource 動作的 IAM 政策定義中，搭配 elasticfilesystem:CreateAction 條件金鑰使用 Condition 元素，將標記許可給與建立資源的動作。

Example 政策：只允許在建立期間將標籤新增至檔案系統

以下範例政策可讓使用者只在建立期間建立檔案系統，並將標籤套用至檔案系統。使用者沒有標記現有資源的權限 (他們不能直接呼叫 elasticfilesystem:TagResource 動作)。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "elasticfilesystem:CreateFileSystem"
      ],
      "Resource": "arn:aws:elasticfilesystem:region:account-id:file-system/*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "elasticfilesystem:TagResource"
      ],
      "Resource": "arn:aws:elasticfilesystem:region:account-id:file-system/*",
      "Condition": {
         "StringEquals": {
             "elasticfilesystem:CreateAction": "CreateFileSystem"
          }
       }
    }
  ]
}
```

使用標籤來控制對 Amazon EFS 資源的存取

若要控制對 Amazon EFS 資源和動作的存取，您可以根據標籤使用 IAM 政策。您可以在以兩種方式提供此控制：

- 您可以根據這些資源上的標籤來控制對 Amazon EFS 資源的存取。
- 您可以控制您可以在 IAM 請求條件中傳遞哪些標籤。

如需如何使用標籤來控制AWS資源存取權的詳細資訊，請參閱 IAM 使用者指南中的使用標籤控制存取。

根據資源的標籤控制存取

若要控制使用者或角色可在 Amazon EFS 資源上執行哪些動作，您可以在資源上使用標籤。例如，您可能想要根據資源上標籤的索引鍵值配對，允許或拒絕檔案系統資源上的特定 API 作業。

Example 策略：只有在使用特定標記時才建立檔案系統

下列範例原則只允許使用者在使用特定標籤索引鍵值組標記檔案系統時建立檔案系統，在此範例中為key=Department、value=Finance。

```
{
    "Effect": "Allow",
    "Action": [
        "elasticfilesystem:CreateFileSystem",
        "elasticfilesystem:TagResource"
    ],
    "Resource": "arn:aws:elasticfilesystem:region:account-id:file-system/*",
    "Condition": {
        "StringEquals": {
            "aws:RequestTag/Department": "Finance"
        }
    }
}
```

Example 原則：刪除具有特定標記的檔案系統

以下範例政策可讓使用者只刪除標籤為標籤為標籤的檔案系統Department=Finance。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "elasticfilesystem:DeleteFileSystem"
            ],
            "Resource": "arn:aws:elasticfilesystem:region:account-id:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
```

```
                }
            }
        }
    ]
}
```

使用 Amazon EFS 的服務連結角色

Amazon Elastic File System 使用AWS Identity and Access Management (IAM) 服務連結角色。Amazon EFS 服務連結角色是直接連結至 Amazon EFS 的一種特殊 IAM 角色類型。預先定義的 Amazon EFS 服務連結角色包含該服務代表您呼叫其他所需AWS 服務的許可。

服務連結角色可讓設定 Amazon EFS 更為簡單，因為您不必手動新增必要的許可。Amazon EFS 定義其服務連結角色的許可，僅有 Amazon EFS 能夠擔任其角色。定義的許可包括信任政策和許可政策，並且該許可政策不能連接到任何其他 IAM 實體。

您必須先刪除 Amazon EFS 檔案系統，才能刪除 Amazon EFS 服務連結角色。如此可保護您的 Amazon EFS 資源，避免您不小心移除資源的存取許可。

服務連結角色可透過 AWS CloudTrail 顯示所有 API 呼叫。因為這可讓您追蹤 Amazon EFS 代表您執行的所有動作，所以有助於監控和稽核要求。如需詳細資訊，請參閱EFS 服務連結角色的日誌項目。

Amazon EFS 的服務連結角色許可

Amazon EFS 使用名為的服務連結角色，`AWSServiceRoleForAmazonElasticFileSystem`允許 Amazon EFS 代表您的 EFS 檔案系統呼叫和管理AWS資源。

AWSServiceRoleForAmazonElasticFileSystem 服務連結角色信任下列服務以擔任角色：

- `elasticfilesystem.amazonaws.com`

此角色許可政策允許 Amazon EFS 完成政策定義 JSON 中包含的動作：

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

```
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:ModifyNetworkInterfaceAttribute",
                "tag:GetResources"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey"
            ],
            "Resource": "arn:aws:kms:*:*:key/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "backup:CreateBackupVault",
                "backup:PutBackupVaultAccessPolicy"
            ],
            "Resource": [
                "arn:aws:backup:*:*:backup-vault:aws/efs/automatic-backup-vault"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "backup:CreateBackupPlan",
                "backup:CreateBackupSelection"
            ],
            "Resource": [
                "arn:aws:backup:*:*:backup-plan:*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": [
```

```
                        "backup.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/aws-service-role/backup.amazonaws.com/
AWSServiceRoleForBackup"
            ],
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": "backup.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticfilesystem:DescribeFileSystems",
                "elasticfilesystem:CreateReplicationConfiguration",
                "elasticfilesystem:DescribeReplicationConfigurations",
                "elasticfilesystem:DeleteReplicationConfiguration"
            ],
            "Resource": "*"
        }
    ]
}
```

> **Note**
>
> 建立新的靜態加密 Amazon EFS 檔案系統AWS KMS時，您必須手動設定 IAM 許可。如需進一步了解，請參閱 加密靜態資料。

建立 Amazon EFS 的服務連結角色

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立服務連結角色。若要這麼做，IAM 實體新增`iam:CreateServiceLinkedRole`許可，IAM 實體如下列範例所示。

```
{
    "Action": "iam:CreateServiceLinkedRole",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "iam:AWSServiceName": [
                "elasticfilesystem.amazonaws.com"
            ]
        }
    }
}
```

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。

您不需要手動建立一個服務連結角色。在AWS Management Console、或AWS API 中為 EFS 檔案系統建立掛載目標或複寫組態時AWS CLI，Amazon EFS 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 EFS 檔案系統的掛載目標或複寫組態時，Amazon EFS 會再次為您建立服務連結角色。

編輯 Amazon EFS 的服務連結角色

Amazon EFS 不允許您編輯`AWSServiceRoleForAmazonElasticFileSystem`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，您可使用 IAM 來編輯角色描述。如需更多資訊，請參閱 IAM 使用者指南中的編輯服務連結角色。

刪除 Amazon EFS 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。然而，在手動刪除服務連結角色之前，您必須先清除資源。

> **Note**
>
> 若 Amazon EFS 服務在您試圖刪除資源時正在使用該角色，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。

若要刪除亞馬遜 EFS 資源AWSServiceRoleForAmazonElasticFileSystem

完成下列步驟 EFS 以刪除AWSServiceRoleForAmazonElasticFileSystem. 如需詳細程序，請參閱清理資源並保護您的 AWS 帳戶。

1. 在 Amazon EC2 執行個體上，卸載 Amazon EFS 檔案系統。
2. 刪除 Amazon EFS 檔案系統。
3. 刪除檔案系統的自訂安全性群組。

> **Warning**
> 若您使用虛擬私有雲 (VPC) 的預設安全群組，請勿刪除該安全群組。

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 AWSServiceRoleForAmazonElasticFileSystem 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。

Amazon Elastic File System 身分識別和存取疑難排解

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

主題

- 我未獲授權，不得在 Amazon EFS 中執行動作
- 我沒有授權執行 iam：PassRole
- 我想要允許 AWS 帳戶 外的人員存取我的 Amazon EFS 資源

我未獲授權，不得在 Amazon EFS 中執行動作

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 elasticfilesystem:*GetWidget* 許可時發生。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 elasticfilesystem: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 elasticfilesystem:*GetWidget* 動作存取 *my-example-widget* 資源。

如需任何協助，請聯絡您的 AWS 管理員。您的管理員提供您的登入憑證。

我沒有授權執行 iam：PassRole

如果您收到錯誤，告知您無權執行 iam:PassRole 動作，您的政策必須更新，允許您將角色傳遞給 Amazon EFS。

有些 AWS 服務 允許您傳遞現有的角色至該服務，而無須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。

當名為 marymajor 的 IAM 使用者嘗試使用主控台在 Amazon EFS 中執行動作時，發生下列範例錯誤。但是，該動作要求服務具備服務角色授與的許可。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。

如需任何協助，請聯絡您的 AWS 管理員。您的管理員提供您的登入憑證。

我想要允許 AWS 帳戶 外的人員存取我的 Amazon EFS 資源

您可以建立一個角色，讓其他帳戶中的使用者或您的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對象取得該角色。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 Amazon EFS 是否支援這些功能，請參閱 Amazon Elastic File System 如何與 IAM 協同工作。
- 如需了解如何存取您擁有的所有 AWS 帳戶 所提供的資源，請參閱《IAM 使用者指南》中的將存取權提供給您所擁有的另一個 AWS 帳戶 中的 IAM 使用者。
- 如需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擁有的 AWS 帳戶。
- 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)。

- 若要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 角色與資源型政策的差異。

使用 IAM 控制檔案系統資料存取

您可以採取一種適用於雲端環境可擴充和最佳化的方式，使用 IAM 身分政策和資源政策來控制用戶端對 Amazon EFS 資源的存取。您可以使用 IAM，允許用戶端在檔案系統上執行特定動作，包括唯讀、寫入和根存取。IAM 身分識別政策或檔案系統資源政策中的動作具有「允許」許可，可允許存取該動作。身分識別和資源政策均不需要同時授與許可。

NFS 用戶端可以在連線到 EFS 檔案系統時，使用 IAM 角色來識別自己。當用戶端連線至檔案系統時，Amazon EFS 會評估檔案系統中稱為檔案系統政策的 IAM 資源政策，以及任何身分型 IAM 政策，以決定要授予的適當檔案系統存取權限。

使用 NFS 用戶端的 IAM 授權時，用戶端連線和 IAM 授權決策會紀錄於 AWS CloudTrail。如需如何使用記錄 Amazon EFS API 呼叫的詳細資訊 CloudTrail，請參閱使用記錄 Amazon EFS API 呼叫 AWS CloudTrail。

> **Important**
>
> 您必須使用 EFS 掛載協助程式掛載 Amazon EFS 檔案系統，才能使用 IAM 授權來控制用戶端的存取權。如需詳細資訊，請參閱 使用 IAM 授權掛載。

預設 EFS 檔案系統政策

預設的 EFS 檔案系統政策不使用 IAM 進行驗證，並且會將完全存取權授予任何可以使用掛載目標連線至檔案系統的匿名用戶端。每當使用者設定的檔案系統政策未生效時，預設政策就會生效，包括在建立檔案系統時。每當預設檔案系統政策生效時，`DescribeFileSystemPolicy` API 操作便會傳回 `PolicyNotFound` 回應。

用戶端的 EFS 動作

您可以使用檔案系統政策，為存取檔案系統的用戶端指定下列動作。

動作	描述
`elasticfilesystem:ClientMount`	提供檔案系統的唯讀存取權。

動作	描述
elasticfilesystem:ClientWrite	在檔案系統上提供具有寫入權限。
elasticfilesystem:ClientRootAccess	存取檔案系統時，提供使用根使用者的功能。

用戶端的 EFS 條件金鑰

欲表示條件，您可以使用預先定義的條件金鑰。Amazon EFS 為 NFS 用戶端提供下列預先定義的條件金鑰。使用 IAM 控制安全存取 EFS 檔案系統時，不會強制執行任何其他條件金鑰。

EFS 條件金鑰	描述	運算子
aws:SecureTransport	在連線到 EFS 檔案系統時，使用此金鑰要求用戶端使用 TLS。	Boolean
aws:SourceIp	存取 EFS 檔案系統之用戶端的私人 IP 位址。	字串
elasticfilesystem:AccessPointArn	用戶端連線到的 EFS 存取點 ARN。	字串
elasticfilesystem:AccessedViaMountTarget	客戶端未使用檔案系統掛載目標時，可使用此金鑰防止其存取到 EFS 檔案系統中。	Boolean

檔案系統政策範例

若要檢視 Amazon EFS 檔案系統政策範例，請參閱 Amazon Elastic File System 的資源型政策範例。

控制 NFS 用戶端對 Amazon EFS 檔案系統的網路存取

您可以使用網路層安全性和 Amazon EFS 檔案系統原則來控制 NFS 用戶端對 EFS 檔案系統的存取。您可以使用可搭配 Amazon EC2 的網路層安全性機制，例如 VPC 安全群組規則和網路 ACL。您也可以使用 AWS IAM 透過 EFS 檔案系統政策和身分識別型政策來控制 NFS 存取。

主題

針對 Amazon EC2 執行個體和掛載目標使用 VPC 安全群組

使用 Amazon EFS 時，您需要為Amazon EC2 執行個體指定 Amazon EFS 安全群組和為與檔案系統關聯之 EFS 掛載目標指定安全群組。安全群組會做為防火牆，且您新增的規則會定義流量。在「入門」練習中，在啟動 EC2 執行個體時您已建立一個安全群組。然後，使用 EFS 掛載目標與另一個安全群組建立關聯 (也就是在預設 VPC 中的預設安全群組)。這種方法適用於「入門」練習。不過，對於生產系統，您應該設定安全群組搭配最低許可以與 EFS 搭配使用。

您可以授予對 EFS 檔案系統的傳入和傳出存取。若要這樣做，您新增的規則可讓 EC2 執行個體使用網路檔案系統 (NFS) 連接埠，透過掛載目標連接到 Amazon EFS 檔案系統。請依照下列步驟來建立和更新安全群組。

建立 EC2 執行個體和掛載目標的安全群組

1. 在 VPC 中建立兩個安全群組。

   如需詳細資訊，請參閱《Amazon VPC 使用者指南》中建立安全群組的「建立安全群組」部分。
2. 前往 https://console.aws.amazon.com/vpc/ 開啟「Amazon VPC 人雲端管理主控台」，然後驗證這些安全群組的預設規則。兩個安全群組應該只有讓流量離開的傳出規則。

更新安全群組的必要存取

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 為 EC2 安全群組新增規則，以允許從任何主機使用 Secure Shell (SSH) 的傳入存取。或者，限制 Source (來源) 地址。

   您不需要新增傳出規則，因為預設的傳出規則可讓所有流量離開。如果事實不是如此，您需要新增一個傳出規則，以開啟 NFS 連接埠上的 TCP 連接，以便將掛載目標安全群組識別做為目的地。

   如需說明，請參閱《Amazon VPC 使用者指南》中的新增和移除規則。
3. 新增掛載目標的輸入和輸出規則。

- 為掛載目標安全群組新增輸入規則，以便允許該安全群組從 EC2 安全群組中傳入存取。會將 EC2 安全群組識別做為來源。
- 新增輸出規則以在所有 NFS 連接埠上開啟 TCP 連線。會將 EC2 安全群組識別做為目的地。

如需說明，請參閱《Amazon VPC 使用者指南》中的新增和移除規則。

4. 驗證現在兩個安全群組皆授權傳入和傳出存取。

如需有關安全群組的詳細資訊，請參閱適用於 Linux 執行個體的 Amazon EC2 安全群組。

使用 EFS 的來源連接埠

若要支援一組廣泛的 NFS 用戶端，Amazon EFS 允許從任何來源連接埠的連線。如果您要求只有具有特殊權限的使用者可以存取 Amazon EFS，我們建議您使用以下用戶端防火牆規則。使用 SSH 連線至檔案系統，並執行下列命令：

```
iptables -I OUTPUT 1 -m owner --uid-owner 1-4294967294 -m tcp -p tcp --dport 2049 -j
 DROP
```

此命令會在 OUTPUT 鏈 (`-I OUTPUT 1`) 的開始處插入新規則。該規則可防止任何未具特殊權限、非核心的程序 (`-m owner --uid-owner 1-4294967294`) 開啟對 NFS 連接埠的連線 (`-m tcp -p tcp –dport 2049`)。

網路存取的安全性考量

如果 NFS 版本 4.1 (NFSv4.1) 用戶端可對其中一個檔案系統之掛載目標的 NFS 連接埠 (TCP 連接埠 2049) 進行網路連線，其只能掛載檔案系統。同樣地，如果 NFSv4.1 用戶端進行網路連線而存取檔案系統時，其只能宣告使用者和群組 ID。

您是否能夠進行此網路連線的能力，會同時受到以下項目的影響：

- 掛載目標 VPC 提供的網路隔離：檔案系統掛載目標無法讓公有 IP 地址與其相關聯。唯一可以掛載檔案系統的目標如下所示：
  - 本機 Amazon VPC 中的 Amazon EC2 執行個體
  - 已連接 VPC 中的 EC2 執行個體
  - 使用 AWS Direct Connect 和 AWS Virtual Private Network (VPN) 連接到 Amazon VPC 的現場部署伺服器

- 用戶端和掛載目標之 VPC 子網路的網路存取控制清單 (ACL)，適用於從掛載目標之子網路外部進行存取 – 為了掛載檔案系統，用戶端必須能夠讓 TCP 連接到 NFS 連接埠的掛載目標，並獲得傳回流量。
- 用戶端和掛載目標 VPC 安全群組的規則，適用於所有存取：用於 EC2 執行個體掛載檔案系統時，以下安全群組規則必須有效：
  - 檔案系統掛載目標的網路介面必須擁有的安全群組規則，讓傳入連線從執行個體在 NFS 連接埠。您可以依 IP 地址 (CIDR 範圍) 或安全群組啟用傳入連線。掛載目標的網路介面上傳入 NFS 連接埠的安全群組規則來源，對檔案系統存取控制而言是很關鍵的要素。檔案系統掛載目標的網路介面不會使用非 NFS 連接埠的傳入規則和任何傳出規則。
  - 掛載執行個體擁有的網路介面必須具有安全群組規則，這些規則會啟用對其中一個檔案系統掛載目標上 NFS 連接埠的傳出連線。您可以根據 IP 地址 (CIDR 範圍) 或安全群組來允許傳出連線。

如需詳細資訊，請參閱 管理掛載目標。

在 Amazon EFS 中使用界面 VPC 人雲端端點

若要建立虛擬私有雲端 (VPC) 和 Amazon EFS API 之間的私有連線，您可以建立介面 VPC 端點。端點可提供 Amazon EFS API 的安全連線，而不需要網際網路閘道、NAT 執行個體或虛擬私有網路 (VPN) 連線。如需詳細資訊，請參閱 Amazon VPC 使用者指南中的介面 VPC 端點。

介面 VPC 端點的支援功能可讓您使用私有 IP 位址在 AWS 服務之間進行私人通訊。 AWS PrivateLink 若要使用 AWS PrivateLink，請使用 Amazon VPC 主控台、API 或 CLI 在 VPC 中為 Amazon EFS 建立介面 VPC 擬私人雲端端點。這會在您的子網路中建立包含私有 IP 地址的彈性網路介面，用於完成 Amazon EFS API 要求。您也可以使用 AWS VPN、 AWS Direct Connect或 VPC 對等，從內部部署環境或其他 VPC 存取 VPC 端點。若要進一步了解，請參閱 Amazon VPC 使用者指南 AWS PrivateLink中的透過存取服務。

為 Amazon EFS 建立界面端點

若要為 Amazon EFS 建立介面 VPC 端點，請使用以下其中一種方式：

- **com.amazonaws.*region*.elasticfilesystem**：為 Amazon EFS API 操作建立一個端點。
- **com.amazonaws.*region*.elasticfilesystem-fips**：建立 Amazon EFS API 端點時，應遵守聯邦資訊處理標準 (FIPS) 140-2。

如需 Amazon EFS 端點的完整清單，請參閱 Amazon Web Services 一般參考 中的 Amazon Elastic File System。

有關如何建立界面端點的詳細資訊，請參閱 Amazon VPC 使用者指南中的建立界面端點。

為 Amazon EFS 建立 VPC 私人雲端端點政策

若要控制對 Amazon EFS API 的存取，您可以將 AWS Identity and Access Management (IAM) 政策附加到 VPC 端點。此政策會指定以下項目：

- 可執行動作的主體。
- 可執行的動作。
- 可供執行動作的資源。

如需詳細資訊，請參閱 Amazon VPC 使用者指南中的使用 VPC 端點控制服務的存取。

下列範例顯示 VPC 端點政策，拒絕所有人透過端點建立 EFS 檔案系統的權限。範例政策也會授予所有人執行所有其他動作的許可。

```
{
   "Statement": [
        {
            "Action": "*",
            "Effect": "Allow",
            "Resource": "*",
            "Principal": "*"
        },
        {
            "Action": "elasticfilesystem:CreateFileSystem",
            "Effect": "Deny",
            "Resource": "*",
            "Principal": "*"
        }
    ]
}
```

如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的使用 VPC 端點政策。

在網路檔案系統 (NFS) 層級處理使用者、群組和權限

根據預設，在建立檔案系統之後，只有根使用者 (UID 0) 具備讀取、寫入和執行的權限。若要讓其他使用者能夠修改檔案系統，根使用者必須明確地授予存取權給這些使用者。您可以使用存取點來自動建立非根使用者可寫入的目錄。如需詳細資訊，請參閱 使用 Amazon EFS 存取點。

Amazon EFS 檔案系統物件具有相關的 Unix 風格模式。此模式值定義了對該物件執行動作的許可。若是熟悉 Unix 風格系統的使用者，就能輕易地了解 Amazon EFS 對這些許可的相關動作。

此外，在 Unix 風格的系統上，會將使用者和群組對應到數字識別符，Amazon EFS 會利用這些識別符來表示檔案所有權。對於 Amazon EFS，檔案系統物件 (即檔案、目錄等) 由單個擁有者和單一群組擁有。當使用者嘗試存取檔案系統物件時，Amazon EFS 會利用這些對應的數字 ID 來檢查權限。

> **Note**
>
> NFS 通訊協定為每個使用者最多支援 16 個群組 ID (GID)，超出的任何 GID 都會從 NFS 用戶端請求處截斷。如需詳細資訊，請參閱 拒絕在 NFS 檔案系統上存取允許的檔案。

您可以在下面找到許可範例以及 Amazon EFS 的 NFS 許可考量相關討論。

主題

檔案和目錄許可

除非已由 EFS 存取點覆寫，否則在 EFS 檔案系統的檔案和目錄根據掛載 NFSv4.1 用戶端所宣告的使用者和群組 ID 將支援標準 Unix 樣式讀取、寫入和執行許可。 如需詳細資訊，請參閱 在網路檔案系統 (NFS) 層級處理使用者、群組和權限。

> **Note**
>
> 依預設，這一層的存取控制取決於在使用者和群組 ID 之其宣告中的信任 NFSv4.1 用戶端。您可以使用 AWS Identity and Access Management (IAM) 以資源為基礎的政策和身分政策來授權 NFS 用戶端，並提供唯讀、寫入和根存取權限。您可以使用 EFS 存取點來覆寫 NFS 用戶

端所提供的作業系統使用者和群組身分資訊。如需詳細資訊，請參閱 使用 IAM 控制檔案系統資料存取 及 建立存取點。

以檔案和目錄的讀取、寫入和執行許可為例，Alice 可能有權在檔案系統的目錄 (/alice) 中讀取和寫入任何她想要的檔案。不過，在此範例中，Alice 未獲允許可讀取或寫入在相同檔案系統 (/mark) 上 Mark 個人目錄中的任何檔案。Alice 和 Mark 兩人都獲允許，可讀取但不得寫入共用目錄 (/share) 中的檔案。

Amazon EFS 檔案系統使用案例與權限的範例

在建立 Amazon EFS 檔案系統，並掛載 VPC 中檔案系統的目標之後，您就可以將遠端的檔案系統，掛載於本機的 Amazon EC2 執行個體上。mount 指令可以掛載檔案系統中的任何目錄。不過，當您首次建立檔案系統時，只會有一個位於 / 的根目錄。根使用者和根群組擁有掛載的目錄。

下列 mount 命令會將 Amazon EFS 檔案系統的根目錄 (以檔案系統的 DNS 名稱辨識)，掛載於 /efs-mount-point 本機目錄。

```
sudo mount -t nfs -o
 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport file-system-id.efs.aws-region.amazonaws.com:/ efs-mount-point
```

最初的權限模式允許：

- 對擁有者read-write-execute根的 權限
- 對群組read-execute根的 權限
- 對其他項目的 read-execute 權限

只有根使用者能修改此目錄。根使用者還能授予其他使用者寫入此目錄的許可，例如：

- 建立可寫入的每個使用者子目錄。如需 step-by-step 指示，請參閱逐步解說：建立可寫入的每個使用者子目錄與設定重新啟動時自動重新掛載。
- 允許使用者寫入 Amazon EFS 檔案系統根。具備根權限的使用者，可以授予其他使用者對檔案系統的存取權限。
  - 若要將 Amazon EFS 檔案系統的所有者變更為非根使用者和群組，請使用下列程式碼：

```
$ sudo chown user:group /EFSroot
```

- 若要讓檔案系統的權限變得更加寬鬆，請使用下列程式碼：

```
$ sudo chmod 777 /EFSroot
```

此命令將 read-write-execute 權限授予所有已掛載檔案系統的 EC2 執行個體上的所有使用者。

檔案系統內檔案和目錄的使用者和群組 ID 權限

Amazon EFS 檔案系統中的檔案和目錄可支援標準根據使用者 ID 和群組 ID 的 Unix 式讀取、寫入和執行許可。當 NFS 用戶端在不使用存取點的情況下掛載 EFS 檔案系統時，則用戶端提供的使用者 ID 和群組 ID 會受到信任。您可以使用 EFS 存取點來覆寫 NFS 用戶端所使用的使用者 ID 和群組 ID。當使用者嘗試存取檔案和目錄時，Amazon EFS 會檢查其使用者 ID 和群組 ID，來驗證每個使用者是否具有存取這些物件的權限。針對使用者所建立的新檔案和目錄，Amazon EFS 也會使用這些 ID 做為這些項目的擁有者和群組擁有者。Amazon EFS 不會檢查使用者或群組的名稱，而只使用數字識別符。

> **Note**
>
> 當您在 EC2 執行個體上建立使用者時，可以將任意的數字使用者 ID (UID) 和群組 ID (GID) 指派給使用者。數字使用者 ID 會在 Linux 系統上的 `/etc/passwd` 檔案中設定。數字群組 ID 會在 `/etc/group` 檔案中設定。這些檔案定義了名稱與 ID 之間的對應關係。在 EC2 執行個體外部，Amazon EFS 不會對這些 ID 進行任何身分驗證 (包括 0 的根 ID)。

如果使用者從兩個不同的 EC2 執行個體來存取 Amazon EFS 檔案系統，則取決於這些執行個體上使用者的 UID 是否相同，可能會產生如下的不同結果：

- 如果這兩個 EC2 執行個體上的使用者 ID 皆相同，則無論其所用的 EC2 執行個體為何，Amazon EFS 都會將這些 ID 視為代表同一個使用者。從這兩個 EC2 執行個體存取檔案系統時，使用者的使用體驗是相同的。
- 如果兩個 EC2 執行個體上的使用者 ID 不同，則 Amazon EFS 會將這些使用者視為不同的使用者。從這兩個不同的 EC2 執行個體存取 Amazon EFS 檔案系統時，使用者體驗不同。
- 如果不同 EC2 執行個體上的兩個不同使用者共用一個 ID，Amazon EFS 會將這兩者視為同一個使用者。

您可以考慮用一致的方式，來管理各個 EC2 執行個體的使用者 ID 對應。使用者可以使用 `id` 指令來查看自己的數字 ID。

```
$ id

uid=502(joe) gid=502(joe) groups=502(joe)
```

關閉 ID 映射器

在作業系統中的 NFS 公用程式，包含了稱為 ID Mapper (ID 映射器) 的背景行程，可用來管理使用者名稱與 ID 之間的對應。在 Amazon Linux 中，背景行程稱為 `rpc.idmapd`；在 Ubuntu 上，背景行程稱為 `idmapd`。此背景行程會將使用者和群組的 ID 轉譯為名稱，反之亦然。不過，Amazon EFS 只會處理數字 ID。我們建議您在 EC2 執行個體上關閉此程序。在 Amazon Linux 上，ID 映射器通常是停用的，如果已停用，請勿將其啟用。若要關閉 ID 映射器，請使用如下所示的命令。

```
$  service rpcidmapd status
$  sudo service rpcidmapd stop
```

不要進行根權限壓縮

依預設，EFS 檔案系統上會停用根權限壓縮。使用 `no_root_squash` 時，Amazon EFS 就會如同 Linux NFS 伺服器一般運作。如果使用者或群組的 ID 為 0，Amazon EFS 會將該使用者視為 `root` 根使用者，並略過權限檢查 (允許存取和修改所有的檔案系統物件)。當 AWS Identity and Access Management (AWS IAM) 身分識別或資源政策不允許存取`ClientRootAccess`動作時，可以在用戶端連線上啟用根擠壓。啟用根權限壓縮時，會將根使用者轉換為在 NFS 伺服器上具備有限權限的使用者。

如需詳細資訊，請參閱 使用 IAM 控制檔案系統資料存取 及 逐步解說：使用 NFS 用戶端的 IAM 授權啟用根擠壓。

權限快取

Amazon EFS 會在一小段時間內建立檔案權限的快取。因此，使用者存取權最近已被撤銷，但可能會有一段短暫的時間，使用者仍可存取該物件。

變更檔案系統物件的所有權

Amazon EFS 會強制執行 POSIX `chown_restricted` 屬性。這表示只有根使用者可以變更檔案系統物件的擁有者。根使用者或擁有者使用者可以變更檔案系統物件的擁有者群組。不過，但除非使用者為根使用者，否則只能將群組變更為擁有者使用者所屬的群組。

EFS 存取點

「存取點」會使用存取點，將作業系統使用者、群組和檔案系統路徑套用至請求提出的任何檔案系統。存取點的作業系統使用者和群組會覆寫 NFS 用戶端提供的任何身分資訊。檔案系統路徑會公開給用戶端作為存取點的根目錄。此方法可確保每個應用程式在存取共用檔案型資料集時，一律使用正確的作業系統身分和正確的目錄。使用存取點的應用程式只能在其專屬目錄及子目錄中存取資料。如需存取點的詳細資訊，請參閱 使用 Amazon EFS 存取點。

使用 Amazon EFS 存取點

Amazon EFS 存取點是應用程式特定的 EFS 檔案系統進入點，此進入點可讓您更輕鬆地管理共用資料集的應用程式存取。存取點可以針對透過存取點提出的所有檔案系統要求，強制執行使用者身分 (包括使用者的 POSIX 群組)。存取點也可以針對檔案系統強制執行不同的根目錄，讓用戶端只能存取指定目錄或其子目錄中的資料。

您可以使用 AWS Identity and Access Management (IAM) 政策強制執行特定應用程式使用特定存取點。透過結合 IAM 政策與存取點，您可以輕鬆地為應用程式提供特定資料集的安全存取權。

> **Note**
>
> 您需要在 EFS 檔案系統上建立至少一個掛載目標，才能使用存取點。

如需建立存取點的詳細資訊，請參閱建立存取點。

主題

- 建立存取點
- 使用存取點掛載檔案系統
- 使用存取點強制執行使用者身分
- 使用存取點強制採用根目錄
- 在 IAM 政策中使用存取點

建立存取點

您可以使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 和 EFS API 為現有的 Amazon EFS 檔案系統建立存取點。Amazon EFS 檔案系統最多可以有 1,000 個存取點。存取點建立後，您無法修改該存取點。

如需建立存取點的 step-by-step 程序，請參閱建立存取點。

使用存取點掛載檔案系統

使用存取點掛載檔案系統時，您可以使用 EFS 掛載協助程式。在掛載命令中，包含檔案系統 ID、存取點 ID 和 `tls` 掛載選項，如下列範例所示。

```
$ mount -t efs -o tls,iam,accesspoint=fsap-abcdef0123456789a fs-
abc0123def456789a: /localmountpoint
```

如需使用存取點掛載檔案系統的詳細資訊，請參閱 使用 EFS 存取點進行掛載。

使用存取點強制執行使用者身分

您可以使用存取點，來強制執行透過存取點提出之所有檔案系統要求的使用者和群組資訊。若要啟用此功能，您必須在建立存取點時指定要強制採用的作業系統身分。

做為此程序的一部分，請提供下列資訊：

- 使用者 ID：使用者的數字 POSIX 使用者 ID。
- 群組 ID：使用者的數字 POSIX 群組 ID。
- 次要群組 ID：選填的次要群組 ID 清單。

啟用使用者強制執行時，Amazon EFS 會將 NFS 用戶端的使用者和群組 ID 取代為在所有檔案系統操作的存取點上設定的身分。使用者強制執行也會執行下列項目：

- 新檔案和目錄的擁有者和群組會設定為存取點的使用者 ID 和群組 ID。
- 在評估檔案系統許可時，EFS 會考慮使用者 ID、群組 ID 和存取點的次要群組 ID。EFS 會忽略 NFS 用戶端的 ID。

> **Important**
>
> 強制執行使用者身分必須遵守 `ClientRootAccess` IAM 許可。
> 例如，在某些情況下，您可能會將存取點使用者 ID、群組 ID 或這兩者同時設定為根 (也就是說，將 UID、GID 或者兩者同時設定為 0)。在此類情況下，您必須將 `ClientRootAccess` IAM 許可授與 NFS 用戶端。

使用存取點強制採用根目錄

您可以使用存取點覆寫檔案系統的根目錄。強制執行根目錄時，使用存取點的 NFS 用戶端會使用存取點上設定的根目錄，而不是檔案系統的根目錄。

您可以在建立存取點時設定存取點 `Path` 屬性來啟用此功能。此 `Path` 屬性是檔案系統根目錄的完整路徑，適用於透過此存取點提出的所有檔案系統要求。完整路徑的長度不能超過 100 個字元。最多可以包含四個子目錄。

當您在存取點上指定根目錄時，它會成為掛載存取點之 NFS 用戶端之檔案系統的根目錄。例如，假設存取點的根目錄為 `/data`。在此情況下，使用存取點掛載 `fs-12345678:/` 的效果與不使用存取點掛載 `fs-12345678:/data` 的效果相同。

在存取點中指定根目錄時，請確定已設定目錄權限，以允許存取點的使用者成功掛載檔案系統。請特別確定執行位元已為存取點使用者、群組或所有人設定。例如，目錄權限值 755 可讓目錄使用者擁有者列出檔案、建立檔案和裝載，以及所有其他使用者列出檔案和裝載。

建立存取點的根目錄

如果檔案系統上不存在存取點的根目錄路徑，Amazon EFS 會使用擁有權和許可來自動建立根目錄。如果您在建立時未指定目錄擁有權和許可權，Amazon EFS 將不會建立根目錄。此方法可以為特定使用者或應用程式佈建檔案系統存取，而無需從 Linux 主機掛載檔案系統。如需建立根目錄，您可以在建立存取點時，使用下列屬性來設定根目錄擁有權和許可：

- `OwnerUid`：用來做為根目錄擁有者的數字 POSIX 使用者 ID。
- `OwnerGiD`：用來做為根目錄擁有者群組的數字 POSIX 群組 ID。
- 許可：目錄的 Unix 模式。常見的組態是 755。確定已為存取點使用者設定執行位元，以便他們能夠掛載。此組態賦與目錄擁有者在目錄中輸入、列出和寫入新檔案的許可。也賦與所有其他使用者輸入和列出檔案的許可。如需使用 Unix 檔案和目錄模式的詳細資訊，請參閱 在網路檔案系統 (NFS) 層級處理使用者、群組和權限。

只有在為目錄指定了 OwnGID 和許可時 OwnUid，Amazon EFS 才會建立存取點根目錄。如果您未提供此資訊，則 Amazon EFS 不會建立根目錄。如果根目錄不存在，嘗試使用存取點掛載將會失敗。

當您使用存取點掛載檔案系統時，如果該目錄不存在，則會建立存取點的根目錄，前提是在建立存取點時指定了根目錄 OwnerUid 和權限。如果存取點上設定的根目錄在掛載前已經存在，存取點則不會覆寫現有的許可。如果您刪除根目錄，EFS 會在下次使用存取點掛載檔案系統時將其重新建立。

> **Note**
>
> 如果您未指定存取點擁有權和許可權，Amazon EFS 將不會建立根目錄。掛載存取點的所有嘗試都將失敗。

存取點根目錄的安全模型

當根目錄覆寫生效時，Amazon EFS 的表現就會跟啟用了 no_subtree_check 選項的 Linux NFS 伺服器一樣。

在 NFS 通訊協定中，伺服器會產生檔案控制點，用戶端在存取檔案時會使用此控制點作為唯一的參考。EFS 會安全地產生檔案控制點，EFS 檔案系統無法預測此控制點，且此控制點是 EFS 檔案系統所特有的。當根目錄覆寫準備就緒時，EFS 不會對在指定根目錄之外檔案揭露檔案控制點。不過，在某些情況下，使用者可能會使用機制取得其存取點外部檔案的檔案控 out-of-band 制代碼。例如，如果使用者可以存取第二個存取點，可能就會這麼做。如果使用者這麼做，他們可以對檔案執行讀取和寫入操作。

系統一律會強制執行檔案擁有權和存取許可，以供在使用者存取點根目錄內外存取檔案。

在 IAM 政策中使用存取點

您可以使用 IAM 政策來強制執行由其 IAM 角色識別的特定 NFS 用戶端，僅能來存取特定的存取點。若要執行此作業，請使用 `elasticfilesystem:AccessPointArn` IAM 條件金鑰。`AccessPointArn` 是用來掛載檔案系統之存取點的 Amazon Resource Name (ARN)。

以下是檔案系統政策範例，此政策允許 IAM 角色 app1 使用存取點 `fsap-01234567` 存取檔案系統。此政策也允許 app2 透過存取點 `fsap-89abcdef` 使用檔案系統。

```
{
    "Version": "2012-10-17",
    "Id": "MyFileSystemPolicy",
    "Statement": [
        {
            "Sid": "App1Access",
            "Effect": "Allow",
            "Principal": { "AWS": "arn:aws:iam::111122223333:role/app1" },
            "Action": [
                "elasticfilesystem:ClientMount",
                "elasticfilesystem:ClientWrite"
```

```
            ],
            "Condition": {
                "StringEquals": {
                    "elasticfilesystem:AccessPointArn" : "arn:aws:elasticfilesystem:us-
east-1:222233334444:access-point/fsap-01234567"
                }
            }
        },
        {
            "Sid": "App2Access",
            "Effect": "Allow",
            "Principal": { "AWS": "arn:aws:iam::111122223333:role/app2" },
            "Action": [
                "elasticfilesystem:ClientMount",
                "elasticfilesystem:ClientWrite"
            ],
            "Condition": {
                "StringEquals": {
                    "elasticfilesystem:AccessPointArn" : "arn:aws:elasticfilesystem:us-
east-1:222233334444:access-point/fsap-89abcdef"
                }
            }
        }
    ]
}
```

封鎖對 Amazon EFS 檔案系統的公開存取

Amazon EFS 封鎖公開存取功能提供設定，幫助管理 Amazon EFS 檔案系統的公開存取。依預設，新 Amazon EFS 檔案系統無法公開存取。但是，您可以修改檔案系統政策，實現公開存取。

> **Important**
>
> 啟用「封鎖公用存取」可防止透過直接附加至檔案系統的資源原則授與公用存取，以協助保護您的資源。除了啟用「封鎖公用存取」之外，請仔細檢查下列原則，以確認其未授予公用存取權：
>
> - 附加至關聯 AWS 主體 (例如 IAM 角色) 的身分識別型政策
> - 附加至關聯 AWS 資源 (例如AWS Key Management Service (KMS) 金鑰) 的以資源為基礎的政策

主題

使用 AWS Transfer Family進行封鎖公開存取

搭配使用 Amazon EFS 時 AWS Transfer Family，如果檔案系統允許公開存取，則從 Transfer Family 統伺服器所擁有的檔案系統存取請求會遭到封鎖。Amazon EFS 會評估檔案系統的 IAM 政策，如果政策是公開的，Amazon EFS 則會封鎖該請求。若要允許 AWS Transfer Family 存取您的檔案系統，請更新您的檔案系統原則，使其不被視為公開。

> **Note**
>
> 如果 EFS 檔案系統具有允許在 2021 年 1 月 6 日之前建立的公用存取政策的 EFS 檔案系統，則依預設會停用 Tran AWS 帳戶 sfer Family 與 Amazon EFS 搭配使用。若要啟用「Transfer Family」來存取您的檔案系統，請聯絡 Sup AWS port 部門。

「公有」的意義

評估檔案系統是否允許公開存取時，Amazon EFS 會假設檔案系統政策是公開狀態。然後，根據檔案系統政策評估情況判斷其是否具備非公開條件。若要視為具備非公開條件，檔案系統政策必須僅將存取授予以下一或多個項目的固定值 (不包含萬用字元的值)：

- 一組無類別網域間路由選擇 (CIDR)，使用 `aws:SourceIp`。如需 CIDR 的詳細資訊，請參閱 RFC Editor 網站上的 RFC 4632。
- AWS 主參與者、使用者、角色或服務主體 (例如，`aws:PrincipalOrgID`)
- `aws:SourceArn`
- `aws:SourceVpc`
- `aws:SourceVpce`
- `aws:SourceOwner`
- `aws:SourceAccount`
- `elasticfilesystem:AccessedViaMountTarget`
- `aws:userid, outside the pattern "AROLEID:*"`

在這些規則之下，下列範例政策視為公開狀態。

```
{
    "Version": "2012-10-17",
    "Id": "efs-policy-wizard-15ad9567-2546-4bbb-8168-5541b6fc0e55",
    "Statement": [
        {
            "Sid": "efs-statement-14a7191c-9401-40e7-a388-6af6cfb7dd9c",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Action": [
                "elasticfilesystem:ClientMount",
                "elasticfilesystem:ClientWrite",
                "elasticfilesystem:ClientRootAccess"
            ]
        }
    ]
}
```

您可以 EFS 條件索引鍵 `elasticfilesystem:AccessedViaMountTarget` 集設定為 true，即得到非公開的檔案系統政策。您可使用 `elasticfilesystem:AccessedViaMountTarget` 實現特定的 EFS 操作，這些操作通過使用檔案系統掛載目標可訪問 EFS 文件系統的客戶端。下列非公用政策會將 `elasticfilesystem:AccessedViaMountTarget` 條件索引鍵集設定為 true。

```
{
    "Version": "2012-10-17",
    "Id": "efs-policy-wizard-15ad9567-2546-4bbb-8168-5541b6fc0e55",
    "Statement": [
        {
            "Sid": "efs-statement-14a7191c-9401-40e7-a388-6af6cfb7dd9c",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Action": [
                "elasticfilesystem:ClientMount",
                "elasticfilesystem:ClientWrite",
                "elasticfilesystem:ClientRootAccess"
            ],
            "Condition": {
```

```
                "Bool": {
                    "elasticfilesystem:AccessedViaMountTarget": "true"
                }
            }
        }
    ]
}
```

如需 Amazon EFS 條件索引鍵的詳細資訊，請參閱 用戶端的 EFS 條件金鑰。如需建立檔案系統政策的詳細資訊，請參閱 建立檔案系統原則。

Amazon EFS 的合規驗證

若要瞭解 AWS 服務 是否屬於特定規範遵循方案的範圍內，請參閱AWS 服務 遵循規範計劃方案中的，並選擇您感興趣的合規方案。如需一般資訊，請參閱AWS 規範計劃AWS。

您可以使用下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱下載中的報告中的 AWS Artifact。

您在使用時的合規責任取決 AWS 服務 於您資料的敏感性、公司的合規目標以及適用的法律和法規。AWS 提供下列資源以協助遵循法規：

- 安全性與合規性快速入門指南 — 這些部署指南討論架構考量，並提供部署以安全性和合規性 AWS 為重點的基準環境的步驟。
- 在 Amazon Web Services 上架構 HIPAA 安全性與合規性 — 本白皮書說明公司如何使用建立符合 HIPAA 資格的應 AWS 用程式。

> **Note**
>
> 並非所有人 AWS 服務 都符合 HIPAA 資格。如需詳細資訊，請參閱 HIPAA 資格服務參照。

- AWS 合規資源AWS — 此工作簿和指南集合可能適用於您的產業和所在地。
- AWS 客戶合規指南 — 透過合規的角度瞭解共同的責任模式。這份指南總結了在多個架構 (包括美國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)) 中，保 AWS 服務 護指引並對應至安全控制的最佳實務。
- 使用AWS Config 開發人員指南中的規則評估資源 — 此 AWS Config 服務會評估您的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 提供了內部安全狀態的全面視圖 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 controls reference。
- Amazon GuardDuty — 透過監控環境中的 AWS 帳戶可疑和惡意活動，藉此 AWS 服務 偵測您的工作負載、容器和資料的潛在威脅。 GuardDuty 可協助您因應各種合規性需求，例如 PCI DSS，滿足特定合規性架構所規定的入侵偵測需求。
- AWS Audit Manager— 這 AWS 服務 有助於您持續稽核您的 AWS 使用情況，以簡化您管理風險的方式，以及遵守法規和業界標準的方式。

Amazon EFS 中的彈性

AWS 全球基礎架構是圍繞可 AWS 區域 用區域（AZ）構建的。 AWS 區域 提供多個物理分離和隔離的 AZ，這些 AZ 與低延遲，高輸送量和高冗餘網絡連接。使用 AZ，您可以設計和操作在區域之間自動容錯移轉的應用程式和資料庫，而不會中斷。與傳統的單一或多資料中心基礎設施相比，AZ 的可用性、容錯能力和擴充能力更高。

Amazon EFS 檔案系統在 AWS 區域內能應對一個或多個可用區域故障。掛載目標本身的設計具有高可用性。在設計高可用性並容錯移轉至其他 AZ 時，請記住，雖然每個 AZ 中掛載目標的 IP 位址和 DNS 都是靜態的，但它們是由多個資源支援的備援元件。如需詳細資訊，請參閱 如何使用 Amazon EFS 搭配 Amazon EC2 。

如需 AWS 區域 和可用區域的詳細資訊，請參閱AWS 全域基礎結構。

Amazon EFS 的網路隔離

作為受管服務，Amazon Elastic File System 受到 AWS 全球網路安全的保護。有關 AWS 安全服務以及如何 AWS 保護基礎架構的詳細資訊，請參閱AWS 雲端安全 若要使用基礎架構安全性的最佳做法來設計您的 AWS 環境，請參閱安全性支柱架構良 AWS 好的架構中的基礎結構保護。

您可以使用 AWS 已發佈的 API 呼叫透過網路存取 Amazon EFS。使用者端必須支援下列專案：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 具備完美轉送私密(PFS)的密碼套件，例如 DHE (Ephemeral Diffie-Hellman)或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。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，您可以透過 AWS Security Token Service (AWS STS) 來產生暫時安全憑證來簽署請求。

您可從任何網路位置呼叫這些 API，但 Amazon EFS 確實可支援資源型存取政策，而這類政策納入的限制會以來源 IP 地址為基礎。您也可以使用 Amazon EFS 政策，以便從特定 Amazon Virtual Private Cloud (Amazon VPC) 端點或特定 VPC 中控制存取權。實際上，這可以將對指定 Amazon EFS 資源的網路存取從網路內的特定 VPC 隔離出 AWS 來。

Amazon EFS 配額

您可以在下面找到使用 Amazon EFS 時的配額。

主題

您可以提高的 Amazon EFS 配額

「Service Quotas」是一項可協助您從單一位置管理配額或限制的 AWS 服務。在 Service Quotas 主控台中，您可以檢視所有 Amazon EFS 限制值，並請求增加 AWS 區域中 EFS 檔案系統的配額數量。

您也可以聯絡 AWS 支援部，請求提高下列 Amazon EFS 配額。如需進一步了解，請參閱請求提高配額。Amazon EFS 服務團隊會單獨審查每項請求。

- 每個客戶帳戶的檔案系統數目。
- 中所有已連線用戶端的每個 AWS 區域區域檔案系統的彈性輸送量配額
- 針對所有已連線用戶端的區域檔案系統佈建輸送量配額 AWS 區域。

下列資料表列出您可以變更的每項資源的預設配額。

每個客戶帳戶的檔案系統數量

資源	預設配額
中每個客戶帳戶的檔案系統數目 AWS 區域	1,000

區域檔案系統 — 每個檔案系統中所有連線用戶端的總預設彈性輸送量 AWS 區域

AWS 區域	最大讀取輸送量	最大寫入輸送量 (計量輸送量)
美國東部 (俄亥俄) 區域 美國東部 (維吉尼亞北部) 區域 美國西部 (奧勒岡) 區域 亞太 (東京) 區域 歐洲 (愛爾蘭) 區域	每秒 20 吉字節 () GiBps	5 GiBps
所有其他 AWS 區域	3 GiBps	1 GiBps

地區檔案系統 — 每個檔案系統中所有連線用戶端的預設佈建輸送量總計 AWS 區域

AWS 區域	最大讀取輸送量	最大寫入輸送量 (計量輸送量)
美國東部 (俄亥俄) 區域 美國東部 (維吉尼亞北部) 區域 美國西部 (奧勒岡) 區域 歐洲 (愛爾蘭) 區域	10 GiBps	3.33 GiBps
所有其他 AWS 區域	3 GiBps	1 GiBps

請求提高配額

若要透過要求提高這些配額 AWS Support，請執行下列步驟。Amazon EFS 團隊會檢視每項配額的提高請求。

若要要求增加配額，請透過 AWS Support

1. 開啟 AWS Support 中心頁面，如有必要請登入。然後選擇建立案例。
2. 在 Create case (建立案例) 下，選擇 Service Limit Increase (提高服務限制)。

3. 在 Limit Type (限制類型) 中，選擇要提高的限制類型。填寫表單中的必要欄位，然後選擇您偏好的聯絡方式。

無法變更的 Amazon EFS 資源配額

無法變更多個 Amazon EFS 資源的配額，包括：

- 一般資源的配額，例如每個檔案系統的存取點數或連線數。
- 每個區域檔案系統的彈性和佈建輸送量配額，適用於 AWS 區域.
- 針對所有連線用戶端的每個區域或單一區域檔案系統，針對 AWS 區域.

下表列出一般資源配額、單一區域檔案系統輸送量限制，以及無法變更的大量批次輸送量限制。

無法變更的一般資源配額

資源	配額
每個檔案系統的存取點數目	1,000
每個檔案系統的連線數目	25,000
在可用區域中每個檔案系統的掛載目標數量	1
每種虛擬私有雲端 (VPC)的掛載目標數	1,400
每個掛載目標的安全群組數量	5
每個檔案系統的標籤數量	50
每個檔案系統的 VPC 數量	1

> **Note**
>
> 用戶端也可以連線到與檔案系統帳戶或 VPC 不同的掛載目標。如需詳細資訊，請參閱 從另一個 AWS 帳戶 或 VPC 掛載 EFS 檔案系統。

單一區域檔案系統 — 每個檔案系統中所有連線用戶端的預設彈性和佈建輸送量總計 AWS 區域

AWS 區域	最大讀取輸送量	最大寫入輸送量 (計量輸送量)
所有 AWS 區域	3 GiBps	1 GiBps

區域和單一區域檔案系統 — 每個檔案系統中所有連線用戶端的總高載輸送量 AWS 區域

AWS 區域	最大讀取輸送量	最大寫入輸送量
美國東部 (俄亥俄) 區域 美國東部 (維吉尼亞北部) 區域 美國西部 (奧勒岡) 區域 亞太 (雪梨) 區域 歐洲 (愛爾蘭) 區域	5 GiBps	3 GiBps
所有其他 AWS 區域	3 GiBps	1 GiBps

NFS 用戶端的配額

下列配額僅適用於 NFS 用戶端，且假設您使用的是 Linux NFSv4.1 用戶端：

- 對於使用彈性輸送量的檔案系統，並使用 Amazon EFS 用戶端 (版本MiBps) 或 Amazon EFS CSI 驅動程式 (aws-efs-csi 驅動程式) 2.0 版或更新amazon-efs-utils 版本進行裝載的檔案系統，最大組合讀取和寫入輸送量為每秒 1,500 MB ()。所有其他檔案系統的最大輸送量為 500 MiBps。如需有關效能的詳細資訊，請參閱 效能摘要。NFS 用戶端輸送量的計算方式為傳送及接收的總位元組數，而 NFS 的請求大小下限是 4 KB (對讀取請求采用 1/3 計量速率后)。
- 每個用戶端最多可同時開啟 65,536 個作用中使用者。
- 最多可在執行個體上同時開啟 65,536 個檔案。列出目錄內容時不計為開啟檔案。
- 用戶端上每一個掛載在每個連線上最多可獲得 65,536 個鎖定。
- 當連接到內部部署或另一個 AWS 區域 中的 Amazon EFS、NFS 用戶端時，您可能會觀察其輸送量比連線到相同 AWS 區域的 EFS 上低些。此影響是因為網路延遲增加的關係。網路延遲需要 1 毫秒或更低，才能達到每個用戶端的最大輸送量。將大型資 DataSync 料集從內部部署 NFS 伺服器移轉至 EFS 時，請使用資料移轉服務。

- NFS 通訊協定為每個使用者最多支援 16 個群組 ID (GID)，超出的任何 GID 都會從 NFS 用戶端請求處截斷。如需詳細資訊，請參閱 拒絕在 NFS 檔案系統上存取允許的檔案。
- 不支援搭配 Microsoft Windows 使用 Amazon EFS。

Amazon EFS 檔案系統配額

下列是 Amazon EFS 檔案系統專用配額：

資源	配額
檔案名稱長度，以位元組為單位	255
符號連結 (symlink) 長度，以位元組為單位	4,080
檔案硬連結數量	177
單一檔案的大小	52,673,613,135,872 個位元組 (47.9 TiB)
目錄深度的層級數	1,000
跨所有執行個體和使用者的單一檔案鎖定數	512
每個檔案系統政策的字元限制	20,000
*「一般用途」模式每秒的檔案操作次數	250,000

* 如需關於「一般用途」模式每秒執行檔案操作次數的詳細資訊，請參閱 效能摘要。

不支援的 NFSv4.0 和 4.1 功能

雖然 Amazon EFS 不支援 NFSv4 或 NFSv3，但它確實支援 NFSv4 和 NFSv4，但下列功能除外：

- pNFS
- 任何類型的用戶端委派或回呼
  - OPEN 操作一律將 `OPEN_DELEGATE_NONE` 傳回為委派類型。

  - OPEN 操作會針對 NFSERR_NOTSUPP 和 CLAIM_DELEGATE_CUR 宣告類型傳回 CLAIM_DELEGATE_PREV。
- 強制性鎖定

  Amazon EFS 中的所有鎖定為建議性鎖定，這表示讀取和寫入操作在執行之前不會檢查有衝突的鎖定。
- 拒絕共用

  NFS 支援拒絕共用的概念。拒絕共用主要供 Windows 用戶端使用，可讓使用者拒絕其他使用者存取已開啟的特定檔案。Amazon EFS 不支援此功能，並會針對指定除 NFS4ERR_NOTSUPP 外的拒絕共用值的任何 OPEN 命令傳回 NFS 錯誤 OPEN4_SHARE_DENY_NONE。Linux NFS 用戶端除了 OPEN4_SHARE_DENY_NONE 以外皆不使用。
- 存取控制清單 (ACL)
- Amazon EFS 不會更新檔案讀取上的 time_access 屬性。Amazon EFS 會更新下列事件中的 time_access：
  - 檔案建立時 (將建立 inode)。
  - NFS 用戶端進行明確的 setattr 呼叫時。
  - 例如，檔案大小變更或檔案中繼資料變更導致的寫入 inode。
  - 任何 inode 屬性更新。
- 命名空間
- 持續回覆快取
- 以 Kerberos 為基礎的安全性
- NFSv4.1 資料保留
- 目錄上的 SetUID
- 使用 CREATE 操作時的不支援檔案類型：區塊型儲存設備 (NF4BLK)、字元裝置 (NF4CHR)、屬性目錄 (NF4ATTRDIR) 和具名屬性 (NF4NAMEDATTR)。
- 不支援的屬性：
  FATTR4_ARCHIVE、FATTR4_FILES_AVAIL、FATTR4_FILES_FREE、FATTR4_FILES_TOTAL、FATTR
  和 FATTR4_ACL。

  嘗試設定這些屬性會產生傳回用戶端的 NFS4ERR_ATTRNOTSUPP 錯誤。

其他考量

此外，請注意下列事項：

- 如需可 AWS 區域 在其中建立 Amazon EFS 檔案系統的清單，請參閱AWS 一般參考。
- Amazon EFS 不支援 `nconnect` 掛載選項。
- 您可以使用 AWS Direct Connect 和 VPN 從內部部署資料中心伺服器掛載 Amazon EFS 檔案系統。如需詳細資訊，請參閱 使用內部部署用戶端進行掛載。

疑難排解檔案操作錯誤

當您存取 Amazon EFS 檔案系統時，檔案系統中的檔案將受特定限制。超過這些限制將造成檔案操作錯誤。如需關於 Amazon EFS 中的用戶端與檔案型限制的詳細資訊，請參閱 NFS 用戶端的配額。您可以在下列資訊中找到一些常用檔案操作錯誤，以及和每個錯誤相關的限制。

主題

出現「超出磁碟配額」錯誤的命令失敗

Amazon EFS 目前不支援使用者磁碟配額。如果超出下列任何限制，則此錯誤可能發生：

- 最多可同時開啟 65,536 個作用中使用者的檔案。多次登入的使用者帳戶，將僅計為一位使用中使用者。
- 執行個體最多可以一次開啟 65,536 個檔案。列出目錄內容時不計為開啟檔案。
- 用戶端上每一個掛載在每個連線上最多可獲得 65,536 個鎖定。

採取動作

如果您遭遇此問題，您可以透過識別超出了上述哪一個限制，然後進行變更以滿足該限制來解決問題。如需詳細資訊，請參閱 NFS 用戶端的配額。

出現「I/O 錯誤」的命令失敗

此錯誤通常會因下列其中一個問題而發生：

- 每個執行個體有超過 65,536 個作用中使用者帳戶可同時開啟檔案。

  採取動作

  如果您遭遇此問題，您可以透過符合執行個體支援的檔案開啟數量限制來解決問題。若要執行此操作，請降低在執行個體中從 Amazon EFS 檔案系統同時開啟檔案的作用中使用者數目。
- 已刪除加 AWS KMS 密檔案系統的金鑰。

  採取動作

  如果您遭遇到此問題，您不再能夠對以該金鑰加密的資料進行解密，這表示該資料變得不再可用。

出現「檔案名稱太長」錯誤的命令失敗

當檔案名稱大小或其符號連結 (symlink) 太長時，將出現此錯誤。檔案名稱具有下列限制：

- 名稱長度最多可達 255 個位元組。
- 符號連結最多可達 4080 位元組。

採取動作

如果您遭遇此問題，您可以透過縮短檔名或符號連結長度以符合支援的限制來解決問題。

命令失敗，出現「找不到檔案」錯誤

因為某些較舊的 32 位元版本 Oracle 電子商務套件使用 32 位元檔案 I/O 介面，而 EFS 使用 64 位元 inode 號碼，就會發生此錯誤。可能失敗的系統呼叫包括 `stat()` 和 `readdir()`。

採取動作

如果遇到此錯誤，您可以使用 nfs.enable_ino64=0 kernel 開機選項來解決問題。此選項會將 64 位元 EFS inode 號碼壓縮為 32 位元。針對不同的 Linux 發行版，核心開機選項的處理方式不同。在 Amazon Linux 上，通過將 `nfs.enable_ino64=0 kernel` 新增到 `/etc/default/grub` 的

GRUB_CMDLINE_LINUX_DEFAULT 變數來開啟此選項。如需有關如何開啟核心開機選項的特定說明文件，請參閱您的發行版本。

出現「過多連結」錯誤的命令失敗

當檔案有太多硬連結時將發生此錯誤。一個檔案最多可以有 177 個硬連結。

採取動作

如果您遭遇此問題，您可以透過減少硬連結數量以符合支援的限制來解決問題。

出現「檔案過大」 錯誤的命令失敗

檔案太大時將發生此項錯誤。單一檔案大小最多可達 52,673,613,135,872 位元組 (47.9 TiB)。

採取動作

如果您遭遇此問題，您可以透過降低檔案大小以符合支援的限制來解決問題。

EFS S

亞馬遜 EFS API 是一種以 HTTP (RFC 2616) 為基礎的網路通訊協定。對於每個 API 呼叫，您都會向您要管理檔案系統的區域特定 Amazon EFS API 端點發出 HTTP 請求。AWS 區域此 API 會將 JSON (RFC 4627) 文件用於 HTTP 請求/回應內文。

亞馬遜 EFS API 是一種 RPC 模型。在此模型中有一組固定的操作，且每個操作的語法無須任何事先互動即會對用戶端公開。在下一節中，您可以找到使用抽象 RPC 表示法的每個 API 操作的說明。每個操作都有一個操作名稱，此名稱不會顯示在線路上。每個操作的主題都會指定映射至 HTTP 請求元素。

指定請求對應的特定 Amazon EFS 作業是由請求的方法 (GET、PUT、POST 或 DELETE) 以及要求 URI 符合哪些各種模式的組合來決定。如果作業是 PUT 或 POST，Amazon EFS 會從要求 URI 路徑區段、查詢參數和要求主體中的 JSON 物件擷取呼叫引數。

> **Note**
>
> 雖然操作名稱 (例如 `CreateFileSystem`) 不會顯示在線路上，這些名稱在 AWS Identity and Access Management (IAM) 政策中仍有其意義。如需詳細資訊，請參閱Amazon Elastic File System 的身分與存取管理。
> 操作名稱也用於命名命令行工具和AWS SDK API 的元素中的命令。例如，有一個名為 `create-file-system` 的 AWS CLI 命令映射至 `CreateFileSystem` 操作。
> 作業名稱也會出現在 Amazon EFS API 呼叫的AWS CloudTrail日誌中。

API 端點

API 端點是在 API 呼叫之 HTTP URI 中做為主機的 DNS 名稱。這些 API 端點特定於AWS 區域並採用以下形式。

```
elasticfilesystem.aws-region.amazonaws.com
```

例如，美國西部 (奧勒岡) 區域的 Amazon EFS API 端點如下。

```
elasticfilesystem.us-west-2.amazonaws.com
```

如需 Amazon EFS 支援的AWS 區域清單 (您可以在其中建立和管理檔案系統)，請參閱中的 Amazon Elastic File System AWS 一般參考。

區域特定的 API 端點定義了您進行 API 呼叫時可存取的 Amazon EFS 資源範圍。例如，當您使用上述端點呼叫`DescribeFileSystems`作業時，您會取得在您帳戶中建立的美國西部 (奧勒岡) 區域中的檔案系統清單。

API 版本

要用於呼叫的 API 版本會以請求 URI 的第一個路徑區段來識別，且其形式為 ISO 8601 日期。如需範例，請參閱 CreateFileSystem。

文件說明的是 API 2015-02-01 版。

相關主題

以下章節提供 API 操作的說明、如何建立用於請求身分驗證的簽章，以及如何使用 IAM 政策將許可授予給這些 API 操作。

- Amazon Elastic File System 的身分與存取管理
- 動作
- 資料類型

使用亞馬遜 EFS 的查詢 API 請求率

Amazon EFS API 請求會針對每個區域進AWS 帳戶行限制，以協助提升服務效能。所有 Amazon EFS API 呼叫一起呼叫 (無論是來自應用程式AWS CLI、或 Amazon EFS 主控台) 都不得超過允許的 API 請求率上限。最大 API 請求率可能會有所不同AWS 區域。發出的 API 請求歸因於基礎AWS 帳戶。

如果 API 請求超過其類別的 API 請求率，該請求將傳回 `ThrottlingException` 錯誤碼。若要避免發生這種錯誤，請確保您的應用程式不會過度頻繁地重試 API 請求。您可以謹慎使用輪詢以及使用指數退避重試，以避免此錯誤。

輪詢

您的應用程式可能需要重複呼叫 API 操作，以查看狀態的更新。在您開始輪詢前，請設定請求時間讓請求可能完成。當您開始輪詢時，請在連續的請求之間使用適當的休眠間隔。為了獲得最佳結果，請使用較長的休眠間隔。

重試或批次處理

您的應用程式可能需要在 API 請求失敗後重試，或處理多個資源 (例如，所有 Amazon EFS 檔案系統)。若要降低 API 請求的速率，請在連續的請求之間使用適當的休眠間隔。為了獲得最佳結果，請使用較長或可變的休眠間隔。

計算

當您需要輪詢或重試 API 請求時，建議您使用指數退避演算法來計算 API 呼叫之間的休眠間隔。指數退避的背後概念是，對於連續錯誤回應，讓重試之間的等待時間漸進拉長。如需詳細資訊和此演算法的實作範例，請參閱中AWS的錯誤重試和指數輪詢Amazon Web Services 一般參考。

動作

支援以下動作：

- CreateAccessPoint
- CreateFileSystem
- CreateMountTarget
- CreateReplicationConfiguration
- CreateTags
- DeleteAccessPoint
- DeleteFileSystem
- DeleteFileSystemPolicy
- DeleteMountTarget
- DeleteReplicationConfiguration
- DeleteTags
- DescribeAccessPoints
- DescribeAccountPreferences
- DescribeBackupPolicy
- DescribeFileSystemPolicy
- DescribeFileSystems
- DescribeLifecycleConfiguration
- DescribeMountTargets

- DescribeMountTargetSecurityGroups
- DescribeReplicationConfigurations
- DescribeTags
- ListTagsForResource
- ModifyMountTargetSecurityGroups
- PutAccountPreferences
- PutBackupPolicy
- PutFileSystemPolicy
- PutLifecycleConfiguration
- TagResource
- UntagResource
- UpdateFileSystem
- UpdateFileSystemProtection

CreateAccessPoint

建立 EFS 存取點。存取點是 EFS 檔案系統的應用程式特定檢視，會將作業系統使用者和群組，以及檔案系統路徑套用至透過存取點提出的任何檔案系統請求。該作業系統使用者和群組會覆寫 NFS 用戶端提供的任何身分資訊。檔案系統路徑會公開以作為存取點的根目錄。使用存取點的應用程式只能在其專屬目錄及子目錄中存取資料。若要進一步了解，請參閱使用 EFS 存取點掛載檔案系統。

> **Note**
>
> 在相同檔案系統上，如果快速連續傳送多個建立存取點的請求，而且檔案系統已接近 1,000 個存取點極限，您可能遇到系統對這些請求限流。這是為了確保檔案系統不會超過指定的存取點限制。

這項操作需要 `elasticfilesystem:CreateAccessPoint` 動作的許可。

將存取點標記在建立上。若標籤於建立動作中指定，IAM 會針對 `elasticfilesystem:TagResource` 動作執行其他授權，以確認使用者具備建立標籤的許可。因此，您必須授予使用 `elasticfilesystem:TagResource` 動作的明確許可。如需詳細資訊，請參閱在建立期間授予標記資源的許可。

請求語法

```
POST /2015-02-01/access-points HTTP/1.1
Content-type: application/json

{
   "ClientToken": "string",
   "FileSystemId": "string",
   "PosixUser": {
      "Gid": number,
      "SecondaryGids": [ number ],
      "Uid": number
   },
   "RootDirectory": {
      "CreationInfo": {
         "OwnerGid": number,
         "OwnerUid": number,
         "Permissions": "string"
      },
      "Path": "string"
```

```
   },
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

URI 請求參數

請求不會使用任何 URI 參數。

請求主體

請求接受採用 JSON 格式的下列資料。

ClientToken

Amazon EFS 用來確保等冪建立的字串 (最多 64 個 ASCII 字元)。

類型：字串

長度限制：長度下限為 1。長度上限為 64。

模式：`.+`

必要：是

FileSystemId

存取點提供存取的 EFS 檔案系統 ID。

類型：字串

長度限制：長度上限為 128。

模式：`^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

必要：是

PosixUser

適用於所有檔案系統請求的操作系統使用者和群組，其中請求使用存取點提出。

類型：PosixUser 物件

必要：否

RootDirectory

存取點在 EFS 檔案系統上公開的目錄，即爲 NFS 用戶端透過該存取點存取 EFS 檔案系統的根目錄。使用存取點的用戶端只能存取根目錄及子目錄。如果 RootDirectory > Path 指定不存在，Amazon EFS 會在用戶端連線到存取點時建立目錄並應用 CreationInfo 設定。指定 RootDirectory 時，您必須提供 Path 和 CreationInfo。

只有在您已為目錄提供下 CreationInfo列項目 OwnUid、OwnGID 和許可時，Amazon EFS 才會建立根目錄。如果您未提供此資訊，則 Amazon EFS 不會建立根目錄。如果根目錄不存在，嘗試使用存取點掛載將會失敗。

類型：RootDirectory 物件

必要：否

Tags

建立與存取點關聯的標籤。每一個標記都是金鑰對數值，每一個金鑰必須唯一。如需詳細資訊，請參閱《 AWS 一般參考指南》中的標記 AWS 資源。

類型：Tag 物件陣列

必要：否

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "AccessPointArn": "string",
   "AccessPointId": "string",
   "ClientToken": "string",
   "FileSystemId": "string",
   "LifeCycleState": "string",
   "Name": "string",
   "OwnerId": "string",
   "PosixUser": {
```

```
      "Gid": number,
      "SecondaryGids": [ number ],
      "Uid": number
   },
   "RootDirectory": {
      "CreationInfo": {
         "OwnerGid": number,
         "OwnerUid": number,
         "Permissions": "string"
      },
      "Path": "string"
   },
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

AccessPointArn

與存取點關聯的唯一 Amazon Resource Name (ARN)。

類型：字串

長度限制：長度上限為 128。

模式：`^arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:access-point/fsap-[0-9a-f]{8,40}$`

AccessPointId

由 Amazon EFS 指派的存取點 ID。

類型：字串

長度限制：長度上限為 128。

模式：^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:access-point/fsap-[0-9a-f]{8,40}|fsap-[0-9a-f]{8,40})$

ClientToken

請求中指定的不透明字串，以確保等冪建立。

類型：字串

長度限制：長度下限為 1。長度上限為 64。

模式：.+

FileSystemId

存取點套用至 EFS 檔案系統的 ID。

類型：字串

長度限制：長度上限為 128。

模式：^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$

LifeCycleState

識別存取點的生命周期階段。

類型：字串

有效值:creating | available | updating | deleting | deleted | error

Name

存取點的名稱。這是 Name 標籤的值。

類型：字串

OwnerId

識別擁 AWS 帳戶 有存取點資源的。

類型：字串

長度限制：長度上限為 14。

模式：^(\d{12})|(\d{4}-\d{4}-\d{4})$

PosixUser

完整的 POSIX 身分識別，包括存取點上的使用者 ID、群組 ID 和次要群組 ID，這些 ID 適用於 NFS 用戶端使用存取點的所有檔案作業。

類型：PosixUser 物件

RootDirectory

存取點在 EFS 檔案系統上公開的目錄，即爲 NFS 用戶端透過該存取點存取 EFS 檔案系統的根目錄。

類型：RootDirectory 物件

Tags

與存取點相關聯的標籤，顯示為「標籤」物件的陣列。

類型：Tag 物件陣列

錯誤

AccessPointAlreadyExists

如果您嘗試創建的存取點已經存在，並使用您在請求中提供的創建權杖，則傳回。

HTTP 狀態碼：409

AccessPointLimitExceeded

如果 AWS 帳戶 已經建立了每個檔案系統允許的最大存取點數，則傳回。如需詳細資訊，請參閱 https://docs.aws.amazon.com/efs/latest/ug/limits.html#limits-efs-resources-per-account-per-region。

HTTP 狀態碼：403

BadRequest

如果請求格式錯誤或包含錯誤，例如無效的參數值或缺少必要參數，則傳回。

HTTP 狀態碼：400

FileSystemNotFound

如果請求者中不存在指定的`FileSystemId` AWS 帳戶值，則返回。

HTTP 狀態碼：404

IncorrectFileSystemLifeCycleState

如果檔案系統的生命週期狀態不是「可用」，則傳回。

HTTP 狀態碼：409

InternalServerError

如果伺服器端發生錯誤，則傳回。

HTTP 狀態碼：500

ThrottlingException

當 `CreateAccessPoint` API 動作呼叫太快且檔案系統上的存取點數目接近 120 的限制，則傳回。

HTTP 狀態碼：429

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

CreateFileSystem

建立新且空白的文件系統。操作需要從請求中取得建立字符，讓 Amazon EFS 用來確保等冪建立 (使用相同建立字符呼叫操作不會有任何效果)。如果呼叫者目前不存在 AWS 帳戶 具有指定建立權杖的呼叫者所擁有的檔案系統，則此作業會執行下列動作：

- 建立新且空白的文件系統。檔案系統將會擁有 Amazon EFS 指派的 ID，並且其初期的生命週期狀態將會是 `creating`。
- 傳回所建立檔案系統的描述。

否則，此操作會傳回 `FileSystemAlreadyExists` 錯誤，其中包含現有檔案系統的 ID。

> **Note**
>
> 針對基本使用案例，您可以針對建立字符使用隨機產生的 UUID。

等冪操作可讓您重試 `CreateFileSystem` 呼叫，而無須承擔建立額外檔案系統的風險。在初始呼叫失敗，導致不確定檔案系統實際上是否已建立時，便可能會發生此狀況。其中一個範例便是發生傳輸層逾時，或是您的連線重設時。只要您使用相同的建立字符，若初始呼叫成功建立檔案系統，用戶端便會從 `FileSystemAlreadyExists` 錯誤中得知該檔案系統已存在。

如需詳細資訊，請參閱《Amazon EFS 使用者指南》中的建立檔案系統。

> **Note**
>
> `CreateFileSystem` 呼叫會在檔案系統的生命週期狀態仍處於 `creating` 時傳回。您可以透過呼叫 DescribeFileSystems 操作來檢查檔案系統的建立狀態，該操作與其他項目會一起傳回檔案系統狀態。

此操作會接受一個為檔案系統選擇的選用 `PerformanceMode` 參數。我們建議所`generalPurpose`有檔案系統使用。`PerformanceMode`該`maxIO`模式是上一代的效能類型，專為高度平行化的工作負載而設計，可以容忍比模式更高的延遲。`generalPurpose` `MaxIO`使用彈性輸送量的單一區域檔案系統或檔案系統不支援 mode。

檔案系統建立後無法變更。`PerformanceMode`如需詳細資訊，請參閱 Amazon EFS 效能模式。

您可以使用 `ThroughputMode` 參數設定檔案系統的輸送量模式。

在檔案系統完全建立後，Amazon EFS 會將其生命週期狀態設為 `available`，此時您可以為 VPC 中的檔案系統建立一或多個掛載目標。如需詳細資訊，請參閱 CreateMountTarget。您可以使用掛載目標，在您 VPC 中的 EC2 執行個體上掛載您的 Amazon EFS 檔案系統。如需詳細資訊，請參閱 Amazon EFS：運作方式。

這項操作需要 `elasticfilesystem:CreateFileSystem` 動作的許可。

檔案系統可在建立時加上標籤。若標籤於建立動作中指定，IAM 會針對 `elasticfilesystem:TagResource` 動作執行其他授權，以確認使用者具備建立標籤的許可。因此，您必須授予使用 `elasticfilesystem:TagResource` 動作的明確許可。如需詳細資訊，請參閱在建立期間授予標記資源的許可。

請求語法

```
POST /2015-02-01/file-systems HTTP/1.1
Content-type: application/json

{
   "AvailabilityZoneName": "string",
   "Backup": boolean,
   "CreationToken": "string",
   "Encrypted": boolean,
   "KmsKeyId": "string",
   "PerformanceMode": "string",
   "ProvisionedThroughputInMibps": number,
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ],
   "ThroughputMode": "string"
}
```

URI 請求參數

請求不會使用任何 URI 參數。

請求主體

請求接受採用 JSON 格式的下列資料。

AvailabilityZoneName

對於「單一區域」檔案系統，請指 AWS 定要在其中建立檔案系統的可用區域。使用格式 `us-east-1a` 來指定可用區域。如需單一區域檔案系統的詳細資訊，請參閱 Amazon EFS 使用者指南中的 EFS 檔案系統類型。

> **Note**
>
> 並非所有提供 Amazon EFS 的可用區域都可以使用一 AWS 區域 個區域檔案系統。

類型：字串

長度限制：長度下限為 1。長度上限為 64。

模式：`.+`

必要：否

Backup

指定是否在您正在建立的檔案系統上啟用自動備份。將值設定為 `true` 以啟用自動備份。如果您要建立單區域檔案系統，預設會啟用自動備份。如需詳細資訊，請參閱《Amazon EFS 使用者指南》中的啟用自動備份。

預設值為 `false`。但是，如果您指定 `AvailabilityZoneName`，預設值為 `true`。

> **Note**
>
> AWS Backup 並非所有提供 Amazon EFS 的 AWS 區域 地方均可使用。

類型：布林值

必要：否

CreationToken

字串最多為 64 個 ASCII 字元。Amazon EFS 使用這項功能來確保等冪建立。

類型：字串

長度限制：長度下限為 1。長度上限為 64。

模式：`.+`

必要：是

Encrypted

布林值，若為 True 便會建立加密檔案系統。建立加密的檔案系統時，您可以選擇指定現有金 AWS Key Management Service 鑰 (KMS 金鑰)。若您沒有指定 KMS 金鑰，則會使用 Amazon EFS 的預設 KMS 金鑰 `/aws/elasticfilesystem` 來保護加密檔案系統。

類型：布林值

必要：否

KmsKeyId

您要使用 KMS 金鑰 ID 來保護加密檔案系統。此參數只有在您希望使用非預設 KMS 金鑰時才是必要參數。若沒有指定此參數，則會使用 Amazon EFS 的預設 KMS 金鑰。您可以使用以下格式指定此 KMS 金鑰 ID。

- 金鑰 ID - 金鑰的唯一識別碼，例如 `1234abcd-12ab-34cd-56ef-1234567890ab`。
- ARN - 金鑰的 Amazon Resource Name (ARN)，例如 `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`。
- 金鑰別名 - 先前為金鑰建立的顯示名稱，例如 `alias/projectKey1`。
- 金鑰別名 ARN - 金鑰別名的 ARN，例如 `arn:aws:kms:us-west-2:444455556666:alias/projectKey1`。

如果使用`KmsKeyId`，則必須將「CreateFile系統:加密」參數設定為 true。

> **Important**
>
> EFS 只接受對稱 KMS 金鑰。Amazon EFS 檔案系統不能使用非對稱 KMS 金鑰。

類型：字串

長度限制：長度上限為 2048。

模式：`^([0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}|mrk-[0-9a-f]{32}|alias/[a-zA-Z0-9/_-]+|(arn:aws[-a-z]*:kms:[a-z0-9-]+:\d{12}:((key/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12})|(key/mrk-[0-9a-f]{32})|(alias/[a-zA-Z0-9/_-]+))))$`

必要：否

PerformanceMode

檔案系統的效能模式。我們建議針對所有的檔案系統使用 generalPurpose 效能模式。使用 maxIO 效能模式的檔案系統可擴展到更高層級的彙整輸送量及每秒操作數，其代價是針對大多數的檔案操作，會有稍高的延遲。效能模式在檔案系統建立之後便無法變更。單區域檔案系統不支援 maxIO 模式。

> **Important**
>
> 由於最大 I/O 的每個操作延遲較高，我們建議所有檔案系統使用「一般用途」效能模式。

預設值為 generalPurpose。

類型：字串

有效值:generalPurpose | maxIO

必要：否

ProvisionedThroughputInMibps

您要佈建的檔案系統輸送量，以每秒 MB (MiBps) 為單位。若將 ThroughputMode 設為 provisioned，則為必要項目。有效值為 1-3414 MiBps，上限取決於地區。若要提高此限制，請聯絡 AWS Support。如需詳細資訊，請參閱《Amazon EFS 使用者指南》中的您可以增加的 Amazon EFS 配額。

類型：Double

有效範圍：最小值為 1.0。

必要：否

Tags

用於建立一或多個與檔案系統相關聯的標籤。每個標籤都是使用者定義的鍵/值對。透過包含 "Key":"Name","Value":"{value}" 鍵/值對來在建立時為您的檔案系統命名。每個鍵都必須是唯一的。如需詳細資訊，請參閱《 AWS 一般參考指南》中的標記 AWS 資源。

類型：Tag 物件陣列

必要：否

ThroughputMode

指定檔案系統的輸送量模式。模式可以是 bursting、provisioned 或 elastic。若您將 ThroughputMode 設為 provisioned，您也必須為 ProvisionedThroughputInMibps 設定值。建立檔案系統後，在有限時間內，您可以減少佈建輸送量或變更輸送量模式。如需詳細資訊，請參閱《Amazon EFS 使用者指南》中的使用佈建模式指定輸送量。

預設值為 bursting。

類型：字串

有效值:bursting | provisioned | elastic

必要：否

回應語法

```
HTTP/1.1 201
Content-type: application/json

{
   "AvailabilityZoneId": "string",
   "AvailabilityZoneName": "string",
   "CreationTime": number,
   "CreationToken": "string",
   "Encrypted": boolean,
   "FileSystemArn": "string",
   "FileSystemId": "string",
   "FileSystemProtection": {
      "ReplicationOverwriteProtection": "string"
   },
   "KmsKeyId": "string",
   "LifeCycleState": "string",
   "Name": "string",
   "NumberOfMountTargets": number,
   "OwnerId": "string",
   "PerformanceMode": "string",
   "ProvisionedThroughputInMibps": number,
   "SizeInBytes": {
      "Timestamp": number,
      "Value": number,
      "ValueInArchive": number,
```

```
      "ValueInIA": number,
      "ValueInStandard": number
   },
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ],
   "ThroughputMode": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 201 回應。

服務會傳回下列 JSON 格式的資料。

AvailabilityZoneId

檔案系統所在可用區域的唯一且一致的識別碼僅對單區域有效。例如，use1-az1是 us-east-1 的可用區域識別碼 AWS 區域，而且它在每個項目中都有相同的位置。 AWS 帳戶

類型：字串

AvailabilityZoneName

描述檔案系統所在的 AWS 可用區域，且僅對單一區域檔案系統有效。如需詳細資訊，請參閱《Amazon EFS 使用者指南》中的使用 EFS 儲存類別。

類型：字串

長度限制：長度下限為 1。長度上限為 64。

模式：.+

CreationTime

建立檔案系統的時間，以秒為單位 (自 1970-01-01T00:00:00Z 以來)。

類型：Timestamp

CreationToken

請求中指定的不透明字串。

類型：字串

長度限制：長度下限為 1。長度上限為 64。

模式：`.+`

Encrypted

布林值，若為 true，指出加密檔案系統。

類型：布林值

FileSystemArn

Amazon EFS 檔案系統的 Amazon Resource Name (ARN)，格式為 `arn:aws:elasticfilesystem:region:account-id:file-system/file-system-id`。示例資料範例：`arn:aws:elasticfilesystem:us-west-2:1111333322228888:file-system/fs-01234567`

類型：字串

FileSystemId

由 Amazon EFS 指派的檔案系統 ID。

類型：字串

長度限制：長度上限為 128。

模式：`^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

FileSystemProtection

說明檔案系統的防護。

類型：FileSystemProtectionDescription 物件

KmsKeyId

AWS KMS key 用來保護加密檔案系統的識別碼。

類型：字串

長度限制：長度上限為 2048。

模式：^([0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}|mrk-[0-9a-f]{32}|alias/[a-zA-Z0-9/_-]+|(arn:aws[-a-z]*:kms:[a-z0-9-]+:\d{12}:((key/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12})|(key/mrk-[0-9a-f]{32})|(alias/[a-zA-Z0-9/_-]+))))$

LifeCycleState

檔案系統的生命周期階段。

類型：字串

有效值:creating | available | updating | deleting | deleted | error

Name

您可以將標籤 (包括 Name 標籤) 新增至檔案系統。如需詳細資訊，請參閱 CreateFileSystem。如果檔案系統有 Name 標籤，Amazon EFS 會傳回此欄位中的值。

類型：字串

長度限制：長度上限為 256。

模式：^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$

NumberOfMountTargets

檔案系統目前擁有的掛載目標數。如需詳細資訊，請參閱 CreateMountTarget。

類型：整數

有效範圍：最小值為 0。

OwnerId

建 AWS 帳戶 立檔案系統的。

類型：字串

長度限制：長度上限為 14。

模式：^(\d{12})|(\d{4}-\d{4}-\d{4})$

PerformanceMode

檔案系統的效能模式。

類型：字串

有效值:generalPurpose | maxIO

ProvisionedThroughputInMibps

檔案系統的佈建輸送量量 MiBps，以測量單位。對使用 ThroughputMode 設定為 provisioned 的檔案系統有效。

類型：Double

有效範圍：最小值為 1.0。

SizeInBytes

儲存在檔案系統、Value 欄位中的資料最新已知計量大小 (以位元組為單位)，以及在 Timestamp 欄位中決定該大小的時間。Timestamp 值是自 1970-01-01T00:00:00Z 以來的整數秒數。SizeInBytes 值不代表檔案系統的一致快照集大小，但是在沒有寫入檔案系統時，它最終會保持一致。也就是說，只有超過幾個小時未修改檔案系統，SizeInBytes 才能表示實際大小。否則，該值并不能代表檔案系統在任何時間點的確切大小。

類型：FileSystemSize 物件

Tags

與檔案系統相關聯的標籤以 Tag 物件陣列形式呈現出來。

類型：Tag 物件陣列

ThroughputMode

顯示檔案系統的輸送量模式。如需詳細資訊，請參閱《Amazon EFS 使用者指南》中的輸送量模式。

類型：字串

有效值:bursting | provisioned | elastic

錯誤

BadRequest

如果請求格式錯誤或包含錯誤，例如無效的參數值或缺少必要參數，則傳回。

HTTP 狀態碼：400

FileSystemAlreadyExists

如果您嘗試建立的檔案系統已經存在，並使用了您提供的建立權杖，則傳回。

HTTP 狀態碼：409

FileSystemLimitExceeded

如果 AWS 帳戶 已經建立了每個帳戶允許的最大檔案系統數，則傳回。

HTTP 狀態碼：403

InsufficientThroughputCapacity

如果沒有足夠容量佈建其他輸送量，則傳回。當您嘗試以佈建輸送量模式建立檔案系統、嘗試增加現有檔案系統的佈建輸送量，或嘗試將現有檔案系統從「爆增輸送量」變更為「佈建輸送量」模式時，系統可能會傳回此值。請稍後再試。

HTTP 狀態碼：503

InternalServerError

如果在伺服器端發生錯誤，則傳回。

HTTP 狀態碼：500

ThroughputLimitExceeded

如果因為已達到 1024 MB 的輸送量限制而無法變更輸送量模式或佈建輸送量總量，則傳回。

HTTP 狀態碼：400

UnsupportedAvailabilityZone

如果請求的 Amazon EFS 功能在指定的可用區域中不可用，則傳回。

HTTP 狀態碼：400

範例

建立加密檔案系統

下列範例會傳送 POST 要求，以在啟用自動備份的 `us-west-2` 區域中建立檔案系統。該請求指定 `myFileSystem1` 為等冪性的建立權杖。

請求範例

```
POST /2015-02-01/file-systems HTTP/1.1
Host: elasticfilesystem.us-west-2.amazonaws.com
x-amz-date: 20140620T215117Z
Authorization: <...>
Content-Type: application/json
Content-Length: 42

{
  "CreationToken" : "myFileSystem1",
  "PerformanceMode" : "generalPurpose",
  "Backup": true,
  "Encrypted": true,
  "Tags":[
      {
         "Key": "Name",
         "Value": "Test Group1"
      }
   ]
}
```

回應範例

```
HTTP/1.1 201 Created
x-amzn-RequestId: 01234567-89ab-cdef-0123-456789abcdef
Content-Type: application/json
Content-Length: 319

{
   "ownerId":"251839141158",
   "CreationToken":"myFileSystem1",
   "Encrypted": true,
   "PerformanceMode" : "generalPurpose",
   "fileSystemId":"fs-01234567",
   "CreationTime":"1403301078",
   "LifeCycleState":"creating",
   "numberOfMountTargets":0,
   "SizeInBytes":{
       "Timestamp": 1403301078,
       "Value": 29313618372,
       "ValueInArchive": 201156,
       "ValueInIA": 675432,
```

```
        "ValueInStandard": 29312741784
    },
    "Tags":[
       {
         "Key": "Name",
         "Value": "Test Group1"
       }
    ],
    "ThroughputMode": "elastic"
}
```

建立單區域可用的加密 EFS 檔案系統

下列範例會傳送 POST 要求，以在啟用自動備份的 us-west-2 區域中建立檔案系統。檔案系統在 us-west-2b可用區域中有單區域儲存。

請求範例

```
POST /2015-02-01/file-systems HTTP/1.1
Host: elasticfilesystem.us-west-2.amazonaws.com
x-amz-date: 20140620T215117Z
Authorization: <...>
Content-Type: application/json
Content-Length: 42

{
  "CreationToken" : "myFileSystem2",
  "PerformanceMode" : "generalPurpose",
  "Backup": true,
  "AvailabilityZoneName": "us-west-2b",
  "Encrypted": true,
  "ThroughputMode": "elastic",
  "Tags":[
      {
         "Key": "Name",
         "Value": "Test Group1"
      }
   ]
}
```

回應範例

```
HTTP/1.1 201 Created
```

```
x-amzn-RequestId: 01234567-89ab-cdef-0123-456789abcdef
Content-Type: application/json
Content-Length: 319

{
   "ownerId":"251839141158",
   "CreationToken":"myFileSystem1",
   "Encrypted": true,
   "AvailabilityZoneId": "usew2-az2",
   "AvailabilityZoneName": "us-west-2b",
   "PerformanceMode" : "generalPurpose",
   "fileSystemId":"fs-01234567",
   "CreationTime":"1403301078",
   "LifeCycleState":"creating",
   "numberOfMountTargets":0,
   "SizeInBytes":{
       "Timestamp": 1403301078,
       "Value": 29313618372,
       "ValueInArchive": 201156,
       "ValueInIA": 675432,
       "ValueInStandard": 29312741784
   },
   "Tags":[
      {
        "Key": "Name",
        "Value": "Test Group1"
      }
   ],
   "ThroughputMode": "elastic"
}
```

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK

- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

CreateMountTarget

建立文件系統的掛載目標。您接著可以使用掛載目標，在 EC2 執行個體上掛載檔案系統。

您可以在 VPC 中的每個可用區域內建立一個掛載目標。指定可用區域內 VPC 中的所有 EC2 執行個體都會針對指定的檔案系統共享單一掛載目標。若您在可用區域中有多個子網路，您會在其中一個子網路內建立掛載目標。EC2 執行個體不需要位於和掛載目標相同的子網路中，也能存取其檔案系統。

您只能為單區域檔案系統建立一個掛載目標。您必須在檔案系統所在的同一可用區域中掛載目標。請在 DescribeFileSystems 回應物件中使用 `AvailabilityZoneName` 和 `AvailabiltyZoneId` 屬性來取得此資訊。建立掛載目標時，請使用與檔案系統的可用區域相關聯的 `subnetId`。

如需詳細資訊，請參閱 Amazon EFS：運作方式。

若要建立檔案系統的掛載目標，檔案系統的生命週期狀態必須是 `available`。如需詳細資訊，請參閱 DescribeFileSystems。

請在請求中提供下列資訊：

- 正在建立掛載目標的檔案系統 ID。
- 子網路 ID 決定了下列內容：
  - VPC (Amazon EFS 在其中建立掛載目標)
  - 可用區域 (Amazon EFS 在其中建立掛載目標)
  - IP 地址隨 Amazon EFS 選取掛載目標的 IP 地址而變化(若您沒有在請求中指定 IP 地址)

在建立掛載目標後，Amazon EFS 會傳回回應，其中包含 `MountTargetId` 和 `IpAddress`。您會在 EC2 執行個體中掛載檔案系統時使用此 IP 地址。您也會在掛載檔案系統時使用掛載目標的 DNS 名稱。您使用掛載目標於其上掛載檔案系統的 EC2 執行個體，可將掛載目標的 DNS 名稱解析為其 IP 地址。如需詳細資訊，請參閱運作方式：實作概觀。

請注意，您只能在一個 VPC 內為檔案系統建立掛載目標，並且每個可用區域中只能有一個掛載目標。也就是，若已為檔案系統建立一或多個掛載目標，則在新增另一個掛載目標請求中所指定的子網路必須符合下列需求：

- 必須屬於和現有掛載目標子網路相同的 VPC。
- 不得位於和現有掛載目標任何子網路相同的可用區域內。

若請求滿足需求，Amazon EFS 會執行下列作業：

- 在指定子網路中建立新的掛載目標。
- 也會透過以下方式，在子網路中建立新的網路介面：
  - 若請求提供 IpAddress，則 Amazon EFS 會將該 IP 地址指派給網路介面。否則，Amazon EFS 會指派子網路中的可用地址 (其方式與請求沒有指定主要私有 IP 地址時，Amazon EC2 CreateNetworkInterface 呼叫執行的作業相同)。
  - 若請求提供 SecurityGroups，則此網路介面會和那些安全群組建立關聯。否則，它會屬於子網路 VPC 的預設安全群組。
  - 指派描述 Mount target *fsmt-id* for file system *fs-id* ，其中 *fsmt-id* 是掛載目標 ID， *fs-id* 則是 FileSystemId。
  - 將網路介面的 requesterManaged 屬性設為 true，並將 requesterId 值設為 EFS。

  每個 Amazon EFS 掛載目標都有一個對應的申請者受管 EC2 網路介面。在建立網路介面後，Amazon EFS 會將掛載目標描述中的 NetworkInterfaceId 欄位設為網路介面 ID，並將 IpAddress 欄位設為其地址。若網路介面建立失敗，整個 CreateMountTarget 操作都會失敗。

> **Note**
>
> CreateMountTarget 呼叫只會在建立網路介面後傳回，但當掛載目標狀態仍為 creating 時，您可以透過呼叫操作檢查掛載目標的建立狀態，DescribeMountTargets 操作和其他項目會一起傳回掛載目標的狀態。

我們建議您在每個可用區域中建立一個掛載目標。透過在另一個可用區域建立的掛載目標，於一個可用區域中使用檔案系統時，有成本上的考量。如需詳細資訊，請參閱 Amazon EFS。此外，透過一律使用位於執行個體可用區域的掛載目標，您會消除部分故障情形。若建立掛載目標的可用區域停止運作，您便無法透過該掛載目標存取您的檔案系統。

此操作需要在檔案系統上具備以下動作的許可：

- elasticfilesystem:CreateMountTarget

此操作也需要以下 Amazon EC2 動作的許可：

- ec2:DescribeSubnets
- ec2:DescribeNetworkInterfaces
- ec2:CreateNetworkInterface

請求語法

```
POST /2015-02-01/mount-targets HTTP/1.1
Content-type: application/json

{
   "FileSystemId": "string",
   "IpAddress": "string",
   "SecurityGroups": [ "string" ],
   "SubnetId": "string"
}
```

URI 請求參數

請求不會使用任何 URI 參數。

請求主體

請求接受採用 JSON 格式的下列資料。

FileSystemId

要建立掛載目標的檔案系統 ID。

類型：字串

長度限制：長度上限為 128。

模式：`^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

必要：是

IpAddress

指定子網路地址範圍內的有效 IPv4 地址。

類型：字串

長度限制：長度下限為 7。長度上限為 15。

模式：`^[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}$`

必要：否

SecurityGroups

最多五個 VPC 安全群組 ID，其形式為 sg-xxxxxxxx。這些必須是適用於子網路指定的相同 VPC。

類型：字串陣列

陣列成員：最多 100 個項目。

長度限制：長度下限為 11。長度上限為 43。

模式：^sg-[0-9a-f]{8,40}

必要：否

SubnetId

要在其中新增掛載目標的子網路 ID。對於單區域檔案系統，請使用與檔案系統的可用區域相關聯的子網路。

類型：字串

長度限制：長度下限為 15。長度上限為 47。

模式：^subnet-[0-9a-f]{8,40}$

必要：是

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "AvailabilityZoneId": "string",
   "AvailabilityZoneName": "string",
   "FileSystemId": "string",
   "IpAddress": "string",
   "LifeCycleState": "string",
   "MountTargetId": "string",
   "NetworkInterfaceId": "string",
   "OwnerId": "string",
   "SubnetId": "string",
```

```
   "VpcId": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

AvailabilityZoneId

掛載目標所在可用區域的唯一且一致的識別碼。例如，use1-az1是 us-east-1 區域的 AZ ID，且每個區域都有相同的位置。 AWS 帳戶

類型：字串

AvailabilityZoneName

掛載目標所在可用區域名稱。可用區域會獨立對應至每個區域的名稱 AWS 帳戶。例如，您的 AWS 帳戶 可us-east-1a用區域可能與其他位置不同 AWS 帳戶。us-east-1a

類型：字串

長度限制：長度下限為 1。長度上限為 64。

模式：.+

FileSystemId

指定掛載目標所屬的檔案系統 ID。

類型：字串

長度限制：長度上限為 128。

模式：^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$

IpAddress

使用掛載目標掛載檔案系統的地址。

類型：字串

長度限制：長度下限為 7。長度上限為 15。

模式：^[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}$

LifeCycleState

掛載目標的生命週期狀態。

類型：字串

有效值:creating | available | updating | deleting | deleted | error

MountTargetId

系統指定的掛載目標 ID。

類型：字串

長度限制：長度下限為 13。長度上限為 45。

模式：^fsmt-[0-9a-f]{8,40}$

NetworkInterfaceId

Amazon EFS 建立掛載目標時建立的網路介面 ID。

類型：字串

OwnerId

AWS 帳戶 擁有資源的 ID。

類型：字串

長度限制：長度上限為 14。

模式：^(\d{12})|(\d{4}-\d{4}-\d{4})$

SubnetId

掛載目標子網路的 ID。

類型：字串

長度限制：長度下限為 15。長度上限為 47。

模式：^subnet-[0-9a-f]{8,40}$

VpcId

掛載目標所在的虛擬私有雲端 (VPC)。

類型：字串

錯誤

AvailabilityZonesMismatch

如果為掛載目標指定的可用區域與為單區域儲存指定的可用區域不同，則傳回。如需詳細資訊，請參閱區域和單區域儲存冗餘。

HTTP 狀態碼：400

BadRequest

如果請求格式錯誤或包含錯誤，例如無效的參數值或缺少必要參數，則傳回。

HTTP 狀態碼：400

FileSystemNotFound

如果請求者中不存在指定的`FileSystemId` AWS 帳戶值，則返回。

HTTP 狀態碼：404

IncorrectFileSystemLifeCycleState

如果檔案系統的生命週期狀態不是「可用」，則傳回。

HTTP 狀態碼：409

InternalServerError

如果伺服器端發生錯誤，則傳回。

HTTP 狀態碼：500

IpAddressInUse

如果請求指定了已在子網路中使用的請求 `IpAddress`，則傳回。

HTTP 狀態碼：409

MountTargetConflict

如果掛載目標違反以檔案系統現有的掛載目標為基礎的其中一個指定限制，則傳回。

HTTP 狀態碼：409

NetworkInterfaceLimitExceeded

呼叫帳戶已達到指定 AWS 區域區域彈性網絡介面的限制。刪除某些網路介面，或請求提高帳戶配額。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的 Amazon VPC 配額 (請參閱網路介面資料表中的每個區域的網路介面項目)。

HTTP 狀態碼：409

NoFreeAddressesInSubnet

如果在請求中未指定 IpAddress 且在子網路中沒有可用的 IP 地址，則傳回。

HTTP 狀態碼：409

SecurityGroupLimitExceeded

如果請求中指定的 SecurityGroups 大小大於五，則傳回。

HTTP 狀態碼：400

SecurityGroupNotFound

如果子網路的虛擬私有雲端 (VPC) 中沒有其中一個指定的安全群組，則傳回。

HTTP 狀態碼：400

SubnetNotFound

如果在請求中沒有提供 ID SubnetId 的子網路，則傳回。

HTTP 狀態碼：400

UnsupportedAvailabilityZone

如果請求的 Amazon EFS 功能在指定的可用區域中不可用，則傳回。

HTTP 狀態碼：400

範例

將掛載目標新增至檔案系統

下列請求會建立檔案系統的掛載目標。請求僅指定必要 FileSystemId 和 SubnetId 參數的值。請求不提供可選的 IpAddress 和 SecurityGroups 參數。對於 IpAddress，此操作會使用指定子網

路中的其中一個可用 IP 地址。而且，此操作會使用與 SecurityGroups 的 VPC 相關聯的預設安全群組。

請求範例

```
POST /2015-02-01/mount-targets HTTP/1.1
Host: elasticfilesystem.us-west-2.amazonaws.com
x-amz-date: 20140620T221118Z
Authorization: <...>
Content-Type: application/json
Content-Length: 160

{"SubnetId": "subnet-748c5d03", "FileSystemId": "fs-01234567"}
```

回應範例

```
HTTP/1.1 200 OK
x-amzn-RequestId: 01234567-89ab-cdef-0123-456789abcdef
Content-Type: application/json
Content-Length: 252

{
    "MountTargetId": "fsmt-55a4413c",
    "NetworkInterfaceId": "eni-01234567",
    "FileSystemId": "fs-01234567",
    "LifeCycleState": "available",
    "SubnetId": "subnet-01234567",
    "OwnerId": "231243201240",
    "IpAddress": "172.31.22.183"
}
```

將掛載目標新增至檔案系統

下面的請求指定創建一個掛載目標的所有請求參數。

請求範例

```
POST /2015-02-01/mount-targets HTTP/1.1
Host: elasticfilesystem.us-west-2.amazonaws.com
x-amz-date: 20140620T221118Z
Authorization: <...>
Content-Type: application/json
```

```
Content-Length: 160

{
   "FileSystemId":"fs-01234567",
   "SubnetId":"subnet-01234567",
   "IpAddress":"10.0.2.42",
   "SecurityGroups":[
      "sg-01234567"
   ]
}
```

回應範例

```
HTTP/1.1 200 OK
x-amzn-RequestId: 01234567-89ab-cdef-0123-456789abcdef
Content-Type: application/json
Content-Length: 252

{
   "OwnerId":"251839141158",
   "MountTargetId":"fsmt-9a13661e",
   "FileSystemId":"fs-01234567",
   "SubnetId":"subnet-fd04ff94",
   "LifeCycleState":"available",
   "IpAddress":"10.0.2.42",
   "NetworkInterfaceId":"eni-1bcb7772"
}
```

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK

- AWS 適用於紅寶石 V3 的 SDK

CreateReplicationConfiguration

建立複寫組態，將現有 EFS 檔案系統複寫到新的只讀檔案系統中。如需詳細資訊，請參閱《Amazon EFS 使用者指南》中的 Amazon EFS 複寫。複寫組態指定以下內容：

- 來源檔案系統：您要複寫的 EFS 檔案系統。在現有複寫組態中，來源檔案系統不能為目的地檔案系統。
- AWS 區域 — 建 AWS 區域 立目標檔案系統的位置。所有可使用 EFS 的部分都 AWS 區域 可以使用 Amazon EFS 複寫。必須啟用區域。如需詳細資訊，請參閱《 AWS 一般參考參考指南》 AWS 區域中的〈管理〉。
- 目的地檔案系統組態：複寫來源檔案系統的目的地檔案系統組態。在複寫組態中只能作爲目的地檔案系統。

  複寫組態的參數包括：

  - 檔案系統 ID：複寫的目的地檔案系統 ID。如果未提供任何 ID，那麼 EFS 會建立具有預設設定的新檔案系統。對於現有檔案系統，必須停用檔案系統的複寫覆寫保護。如需詳細資訊，請參閱複寫至現有檔案系統。
  - 可用區域：如果您希望目的地檔案系統使用單區域儲存，則必須指定可在其中建立檔案系統的可用區域。如需詳細資訊，請參閱《Amazon EFS 使用者指南》中的 EFS 檔案系統類型。
  - 加密：所有目的地檔案系統都會在啟用靜態加密的情況下建立。您可以指定用來加密目的檔案系統的 AWS Key Management Service (AWS KMS) 金鑰。如不指定 KMS 金鑰，則會使用 Amazon EFS 的服務管理 KMS 金鑰。

    > **Note**
    >
    > 建立目的地檔案系統之後，您無法變更 KMS 金鑰。

對於新目的地檔案系統，預設會設定下列屬性：

- 效能模式：目的地檔案系統的效能模式與來源檔案系統的模式相符，除非目的地檔案系統使用 EFS 單區域儲存。在這種情況下，會使用「一般用途效能」模式。無法變更效能模式。
- 輸送量模式：目的地檔案系統的輸送量模式匹配來源檔案系統的輸送量模式。建立檔案系統之後，您可以修改輸送量模式。

- 生命週期管理 — 未在目標檔案系統上啟用生命週期管理。建立目的地檔案系統之後，您可以啟用生命週期管理。
- 自動備份：在目的地檔案系統上啟用自動每日備份。建立檔案系統之後，您可以變更此設定。

如需詳細資訊，請參閱《Amazon EFS 使用者指南》中的 Amazon EFS 複寫。

請求語法

```
POST /2015-02-01/file-systems/SourceFileSystemId/replication-configuration HTTP/1.1
Content-type: application/json

{
   "Destinations": [
      {
         "AvailabilityZoneName": "string",
         "FileSystemId": "string",
         "KmsKeyId": "string",
         "Region": "string"
      }
   ]
}
```

URI 請求參數

請求會使用下列 URI 參數。

SourceFileSystemId

指定您要複寫的 Amazon EFS 檔案系統。在另一個複寫組態中，此檔案系統已不能成爲來源或目的地檔案系統。

長度限制：長度上限為 128。

模式：`^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

必要：是

請求主體

請求接受採用 JSON 格式的下列資料。

Destinations

目的地組態物件陣列。僅支援一個目的地組態物件。

類型：DestinationToCreate 物件陣列

必要：是

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "Destinations": [
      {
         "FileSystemId": "string",
         "LastReplicatedTimestamp": number,
         "Region": "string",
         "Status": "string"
      }
   ],
   "OriginalSourceFileSystemArn": "string",
   "SourceFileSystemArn": "string",
   "SourceFileSystemId": "string",
   "SourceFileSystemRegion": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

CreationTime

說明建立複寫組態的時間。

類型：Timestamp

Destinations

目的地物件陣列。僅支援一個目的地物件。

類型：Destination 物件陣列

OriginalSourceFileSystemArn

複寫組態中原始來源 EFS 檔案系統的 Amazon Resource Name (ARN)。

類型：字串

SourceFileSystemArn

複寫組態中當前來源檔案系統的 Amazon Resource Name (ARN)。

類型：字串

SourceFileSystemId

要複寫的來源 Amazon EFS 檔案系統 ID。

類型：字串

長度限制：長度上限為 128。

模式：`^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

SourceFileSystemRegion

來源 EFS 檔案系統所 AWS 區域 在的位置。

類型：字串

長度限制：長度下限為 1。長度上限為 64。

模式：`^[a-z]{2}-((iso[a-z]{0,1}-)|(gov-)){0,1}[a-z]+-{0,1}[0-9]{0,1}$`

錯誤

BadRequest

如果請求格式錯誤或包含錯誤，例如無效的參數值或缺少必要參數，則傳回。

HTTP 狀態碼：400

ConflictException

如果複寫中的來源檔案系統已加密，但目的地檔案系統未加密，則傳回。

HTTP 狀態碼：409

FileSystemLimitExceeded

如果 AWS 帳戶 已經建立了每個帳戶允許的最大檔案系統數，則傳回。

HTTP 狀態碼：403

FileSystemNotFound

如果請求者中不存在指定的`FileSystemId` AWS 帳戶值，則返回。

HTTP 狀態碼：404

IncorrectFileSystemLifeCycleState

如果檔案系統的生命週期狀態不是「可用」，則傳回。

HTTP 狀態碼：409

InsufficientThroughputCapacity

如果沒有足夠容量佈建其他輸送量，則傳回。當您嘗試以佈建輸送量模式建立檔案系統、嘗試增加現有檔案系統的佈建輸送量，或嘗試將現有檔案系統從「爆增輸送量」變更為「佈建輸送量」模式時，系統可能會傳回此值。請稍後再試。

HTTP 狀態碼：503

InternalServerError

如果在伺服器端發生錯誤，則傳回。

HTTP 狀態碼：500

ReplicationNotFound

如果指定的檔案系統沒有複寫組態，則傳回。

HTTP 狀態碼：404

ThroughputLimitExceeded

如果因為已達到 1024 MiB/s 的輸送量限制而無法變更輸送量模式或佈建輸送量總量，則傳回。

HTTP 狀態碼：400

UnsupportedAvailabilityZone

如果請求的 Amazon EFS 功能在指定的可用區域中不可用，則傳回。

HTTP 狀態碼：400

ValidationException

如果提出請求的 AWS Backup 服務不可用，則返回。 AWS 區域

HTTP 狀態碼：400

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK
- AWS SDK for Java V2 的开发
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

CreateTags

> **Note**
>
> 棄用：CreateTags 已棄用且未維護。若要從 EFS 資源建立標籤，請使用 TagResource API 動作。

建立或覆寫與檔案系統相關聯的標籤。每個標籤都是金鑰值對。如果要求中指定的標籤鍵已存在於檔案系統上，此操作會以要求中提供的值覆寫其值。如果您將 Name 標籤新增至檔案系統，Amazon EFS 會在 DescribeFileSystems 回應操作時傳回該標籤。

這項操作需要 elasticfilesystem:CreateTags 動作的許可。

請求語法

```
POST /2015-02-01/create-tags/FileSystemId HTTP/1.1
Content-type: application/json

{
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

URI 請求參數

請求會使用下列 URI 參數。

FileSystemId

您要修改其標籤的 ID (字串)。此操作只會修改標籤，而不會修改檔案系統。

長度限制：長度上限為 128。

模式：^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$

必要：是

請求主體

請求接受採用 JSON 格式的下列資料。

Tags

新增的 Tag 物件陣列。每個 Tag 物件都是一個鍵值對。

類型：Tag 物件陣列

必要：是

回應語法

```
HTTP/1.1 204
```

回應元素

如果動作成功，則服務會送回具有空 HTTP 主體的 HTTP 204 回應。

錯誤

BadRequest

如果請求格式錯誤或包含錯誤，例如無效的參數值或缺少必要參數，則傳回。

HTTP 狀態碼：400

FileSystemNotFound

如果請求者中不存在指定的FileSystemId AWS 帳戶值，則返回。

HTTP 狀態碼：404

InternalServerError

如果伺服器端發生錯誤，則傳回。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

DeleteAccessPoint

刪除指定的存取點。刪除完成後，新用戶端將無法再連線至存取點。刪除時連線至存取點的用戶端將繼續運作，直到終止連線為止。

這項操作需要 elasticfilesystem:DeleteAccessPoint 動作的許可。

請求語法

```
DELETE /2015-02-01/access-points/AccessPointId HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

AccessPointId

您要刪除的存取點 ID。

長度限制：長度上限為 128。

模式：^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:access-point/fsap-[0-9a-f]{8,40}|fsap-[0-9a-f]{8,40})$

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 204
```

回應元素

如果動作成功，則服務會送回具有空 HTTP 主體的 HTTP 204 回應。

錯誤

AccessPointNotFound

如果請求者中不存在指定的AccessPointId AWS 帳戶值，則返回。

HTTP 狀態碼：404

BadRequest

如果請求格式錯誤或包含錯誤，例如無效的參數值或缺少必要參數，則傳回。

HTTP 狀態碼：400

InternalServerError

如果伺服器端發生錯誤，則傳回。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

DeleteFileSystem

刪除檔案系統，永久伺服其內容的存取。傳回時，文件系統不再存在，您無法存取已刪除文件系統的任何內容。

您必須先手動刪除附加至檔案系統的掛載目標，才能刪除 EFS 檔案系統。當您使用 AWS 主控台刪除檔案系統時，會為您執行此步驟。

> **Note**
>
> 您無法刪除屬於 EFS 複寫組態一部分的檔案系統。您需要先刪除複寫組態。

您無法刪除正在使用的檔案系統。也就是說，如果檔案系統有任何掛載目標，您必須先刪除它們。如需詳細資訊，請參閱 DescribeMountTargets 及 DeleteMountTarget。

> **Note**
>
> `DeleteFileSystem` 呼叫會在檔案系統狀態仍處於 `deleting` 時傳回。因 DescribeFileSystems 操作會傳回您帳戶中的檔案系統清單，所以您可以通過呼叫該操作來檢查檔案系統刪除狀態。如果您傳遞檔案系統 ID 或已刪除檔案系統的建立權杖，則 DescribeFileSystems 會傳回 `404 FileSystemNotFound` 錯誤。

這項操作需要 `elasticfilesystem:DeleteFileSystem` 動作的許可。

請求語法

```
DELETE /2015-02-01/file-systems/FileSystemId HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

FileSystemId

您要刪除的檔案系統 ID。

長度限制：長度上限為 128。

模式：^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 204
```

回應元素

如果動作成功，則服務會送回具有空 HTTP 主體的 HTTP 204 回應。

錯誤

BadRequest

如果請求格式錯誤或包含錯誤，例如無效的參數值或缺少必要參數，則傳回。

HTTP 狀態碼：400

FileSystemInUse

如果檔案系統有掛載目標，則傳回。

HTTP 狀態碼：409

FileSystemNotFound

如果請求者中不存在指定的`FileSystemId` AWS 帳戶值，則返回。

HTTP 狀態碼：404

InternalServerError

如果伺服器端發生錯誤，則傳回。

HTTP 狀態碼：500

範例

刪除檔案系統

下列範例將 DELETE 請求傳送至 file-systems 端點 (elasticfilesystem.us-west-2.amazonaws.com/2015-02-01/file-systems/fs-01234567)，以刪除 ID 為 fs-01234567 的檔案系統。

請求範例

```
DELETE /2015-02-01/file-systems/fs-01234567 HTTP/1.1
Host: elasticfilesystem.us-west-2.amazonaws.com
x-amz-date: 20140622T233021Z
Authorization: <...>
```

回應範例

```
HTTP/1.1 204 No Content
x-amzn-RequestId: a2d125b3-7ebd-4d6a-ab3d-5548630bff33
Content-Length: 0
```

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

DeleteFileSystemPolicy

為指定檔案系統刪除 FileSystemPolicy。刪除現有策略後，預設 FileSystemPolicy 便會生效。如需關於預設檔案系統政策的詳細資訊，請參閱在 EFS 中使用以資源為基礎的政策。

這項操作需要 elasticfilesystem:DeleteFileSystemPolicy 動作的許可。

請求語法

```
DELETE /2015-02-01/file-systems/FileSystemId/policy HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

FileSystemId

指定要刪除的 FileSystemPolicy 的 EFS 檔案系統。

長度限制：長度上限為 128。

模式：^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
```

回應元素

如果動作成功，則服務會傳回具空 HTTP 內文的 HTTP 200 回應。

錯誤

BadRequest

如果請求格式錯誤或包含錯誤，例如無效的參數值或缺少必要參數，則傳回。

HTTP 狀態碼：400

FileSystemNotFound

如果請求者中不存在指定的`FileSystemId` AWS 帳戶值，則返回。

HTTP 狀態碼：404

IncorrectFileSystemLifeCycleState

如果檔案系統的生命週期狀態不是「可用」，則傳回。

HTTP 狀態碼：409

InternalServerError

如果伺服器端發生錯誤，則傳回。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

DeleteMountTarget

刪除指定的掛載目標。

如果您刪除了掛載目標，該操作會強制中斷任何掛載的檔案系統掛載，此舉可能會中斷使用該掛載的執行個體或應用程式。為避免應用程式突然切斷，如果可行，您可以考慮卸載掛載目標的任何掛載。此操作也會刪除相關聯的網路介面。寫入未遞交時可能會遺失，但是借此操作中斷掛載目標並不會損毀檔案系統本身。您建立的檔案系統仍存在。您可以使用另一個掛載目標在 VPC 中掛載 EC2 執行個體。

此操作需要在檔案系統上具備以下動作的許可：

- `elasticfilesystem:DeleteMountTarget`

> **Note**
>
> `DeleteMountTarget` 呼叫會在掛載目標狀態仍處於 `deleting` 時傳回。因 DescribeMountTargets 操作會傳回給定文件系統的掛載目標描述列表，所以您可以呼叫該操作來檢查掛載目標刪除情況。

此操作還需要在掛載目標網路介面上獲得下列 Amazon EC2 動作的許可：

- `ec2:DeleteNetworkInterface`

請求語法

```
DELETE /2015-02-01/mount-targets/MountTargetId HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

MountTargetId

要刪除的掛載目標 ID (字串)。

長度限制：長度下限為 13。長度上限為 45。

模式：`^fsmt-[0-9a-f]{8,40}$`

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 204
```

回應元素

如果動作成功，則服務會送回具有空 HTTP 主體的 HTTP 204 回應。

錯誤

BadRequest

如果請求格式錯誤或包含錯誤，例如無效的參數值或缺少必要參數，則傳回。

HTTP 狀態碼：400

DependencyTimeout

嘗試處理請求時服務逾時，那麼用戶端應該再次嘗試呼叫。

HTTP 狀態碼：504

InternalServerError

如果伺服器端發生錯誤，則傳回。

HTTP 狀態碼：500

MountTargetNotFound

如果在發起人的 AWS 帳戶帳戶中找不到指定 ID 的掛載目標，則傳回。

HTTP 狀態碼：404

範例

移除檔案系統的掛載目標

下列範例會傳送 DELETE 請求以刪除特定掛載目標。

請求範例

```
DELETE /2015-02-01/mount-targets/fsmt-9a13661e HTTP/1.1
Host: elasticfilesystem.us-west-2.amazonaws.com
x-amz-date: 20140622T232908Z
Authorization: <...>
```

回應範例

```
HTTP/1.1 204 No Content
x-amzn-RequestId: 01234567-89ab-cdef-0123-456789abcdef
```

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

DeleteReplicationConfiguration

刪除複寫組態。刪除複寫組態，結束複寫程序。刪除複寫組態之後，目的地檔案系統變成 `Writeable`，同時系統重新啟用其複寫保護。如需詳細資訊，請參閱刪除複寫組態。

這項操作需要 `elasticfilesystem:DeleteReplicationConfiguration` 動作的許可。

請求語法

```
DELETE /2015-02-01/file-systems/SourceFileSystemId/replication-configuration HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

SourceFileSystemId

複寫組態中的來源檔案系統 ID。

長度限制：長度上限為 128。

模式：`^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 204
```

回應元素

如果動作成功，則服務會送回具有空 HTTP 主體的 HTTP 204 回應。

錯誤

BadRequest

如果請求格式錯誤或包含錯誤，例如無效的參數值或缺少必要參數，則傳回。

HTTP 狀態碼：400

FileSystemNotFound

如果請求者中不存在指定的`FileSystemId` AWS 帳戶值，則返回。

HTTP 狀態碼：404

InternalServerError

如果伺服器端發生錯誤，則傳回。

HTTP 狀態碼：500

ReplicationNotFound

如果指定的檔案系統沒有複寫組態，則傳回。

HTTP 狀態碼：404

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

DeleteTags

> **Note**
>
> 已作廢：DeleteTags 已棄用且不受維護。若要從 EFS 資源移除標籤，請使用 UntagResource API 動作。

從檔案系統刪除指定的標籤。如果 DeleteTags 請求包含不存在的標籤金鑰，那麼 Amazon EFS 會忽略該金鑰，避免造成錯誤。如需有關標籤和相關限制的詳細資訊，請參閱 AWS Billing and Cost Management 使用指南中的標籤限制。

這項操作需要 elasticfilesystem:DeleteTags 動作的許可。

請求語法

```
POST /2015-02-01/delete-tags/FileSystemId HTTP/1.1
Content-type: application/json

{
   "TagKeys": [ "string" ]
}
```

URI 請求參數

請求會使用下列 URI 參數。

FileSystemId

您要刪除標籤的檔案系統 ID (字串)。

長度限制：長度上限為 128。

模式：^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$

必要：是

請求主體

請求接受採用 JSON 格式的下列資料。

TagKeys

要刪除的標籤索引鍵清單。

類型：字串陣列

陣列成員：項目數下限為 1。項目數上限為 50。

長度限制：長度下限為 1。長度上限為 128。

模式：^(?![aA]{1}[wW]{1}[sS]{1}:)([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$

必要：是

回應語法

```
HTTP/1.1 204
```

回應元素

如果動作成功，則服務會送回具有空 HTTP 主體的 HTTP 204 回應。

錯誤

BadRequest

如果請求格式錯誤或包含錯誤，例如無效的參數值或缺少必要參數，則傳回。

HTTP 狀態碼：400

FileSystemNotFound

如果請求者中不存在指定的`FileSystemId` AWS 帳戶值，則返回。

HTTP 狀態碼：404

InternalServerError

如果伺服器端發生錯誤，則傳回。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

DescribeAccessPoints

傳回特定 Amazon EFS 存取點的說明 (如果 AccessPointId 已提供)。如果您提供 EFS FileSystemId，則會傳回該檔案系統所有存取點的說明。您可以在請求中提供 AccessPointId 或 FileSystemId，但不能同時提供兩者。

這項操作需要 elasticfilesystem:DescribeAccessPoints 動作的許可。

請求語法

```
GET /2015-02-01/access-points?
AccessPointId=AccessPointId&FileSystemId=FileSystemId&MaxResults=MaxResults&NextToken=NextToken
 HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

AccessPointId

(選用) 指定要在回應中描述的 EFS 存取點；與 FileSystemId 互斥。

長度限制：長度上限為 128。

模式：^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:access-point/fsap-[0-9a-f]{8,40}|fsap-[0-9a-f]{8,40})$

FileSystemId

(選用) 如果您提供 FileSystemId，EFS 會傳回該檔案系統的所有存取點；與 AccessPointId 互斥。

長度限制：長度上限為 128。

模式：^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$

MaxResults

(選用) 擷取檔案系統的所有存取點時，您可以選擇性地指定 MaxItems 參數，以限制回應中傳回的物件數目。預設值為 100.

有效範圍：最小值為 1。

NextToken

如果是分頁回應，那麼將會出現 NextToken。您可以在後續請求中使用 NextMarker 來擷取下一頁的存取點描述。

長度限制：長度下限為 1。長度上限為 128。

模式：.+

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "AccessPoints": [
      {
         "AccessPointArn": "string",
         "AccessPointId": "string",
         "ClientToken": "string",
         "FileSystemId": "string",
         "LifeCycleState": "string",
         "Name": "string",
         "OwnerId": "string",
         "PosixUser": {
            "Gid": number,
            "SecondaryGids": [ number ],
            "Uid": number
         },
         "RootDirectory": {
            "CreationInfo": {
               "OwnerGid": number,
               "OwnerUid": number,
               "Permissions": "string"
            },
            "Path": "string"
         },
         "Tags": [
            {
```

```
            "Key": "string",
            "Value": "string"
         }
      ]
   }
],
"NextToken": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

AccessPoints

存取點描述的陣列。

類型：AccessPointDescription 物件陣列

NextToken

如果存取點超過回應中傳回的存取點，則顯示此陣列。您可以使用後續要求 NextMarker 中的來擷取其他描述。

類型：字串

長度限制：長度下限為 1。長度上限為 128。

模式：`.+`

錯誤

AccessPointNotFound

如果請求者中不存在指定的`AccessPointId` AWS 帳戶值，則返回。

HTTP 狀態碼：404

BadRequest

如果請求格式錯誤或包含錯誤，例如無效的參數值或缺少必要參數，則傳回。

HTTP 狀態碼：400

FileSystemNotFound

如果請求者中不存在指定的`FileSystemId` AWS 帳戶值，則返回。

HTTP 狀態碼：404

InternalServerError

如果伺服器端發生錯誤，則傳回。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

DescribeAccountPreferences

傳回目前與提出要求之使用者 AWS 帳戶 相關聯的帳戶偏好設定設定 AWS 區域。

請求語法

```
GET /2015-02-01/account-preferences HTTP/1.1
Content-type: application/json

{
   "MaxResults": number,
   "NextToken": "string"
}
```

URI 請求參數

請求不會使用任何 URI 參數。

請求主體

請求接受採用 JSON 格式的下列資料。

MaxResults

(選用) 擷取帳戶偏好設定時，您可以選擇性地指定 MaxItems 參數，以限制回應中傳回的物件數目。預設值為 100.

類型：整數

有效範圍：最小值為 1。

必要：否

NextToken

(選用) 如果回應裝載已分頁，您可以 NextToken 在後續要求中使用來擷取 AWS 帳戶 偏好設定的下一頁。

類型：字串

長度限制：長度下限為 1。長度上限為 128。

模式：.+

必要：否

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "ResourceIdPreference": {
      "ResourceIdType": "string",
      "Resources": [ "string" ]
   }
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

NextToken

如果有更多的記錄超過響應返回的存在。您可以在後續請求中使用 NextToken 來擷取其他描述。

類型：字串

長度限制：長度下限為 1。長度上限為 128。

模式：.+

ResourceIdPreference

描述目前中與提出請求之使用者 AWS 帳戶 相關聯的資源 ID 偏好設定設定 AWS 區域。

類型：ResourceIdPreference 物件

錯誤

InternalServerError

如果伺服器端發生錯誤，則傳回。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

DescribeBackupPolicy

傳回指定 EFS 檔案系統的備份政策。

請求語法

```
GET /2015-02-01/file-systems/FileSystemId/backup-policy HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

FileSystemId

指定要擷取 BackupPolicy 的 EFS 檔案系統。

長度限制：長度上限為 128。

模式：^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPolicy": {
      "Status": "string"
   }
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

BackupPolicy

描述檔案系統的備份政策，指出自動備份是開啟還是關閉。

類型：BackupPolicy 物件

錯誤

BadRequest

如果請求格式錯誤或包含錯誤，例如無效的參數值或缺少必要參數，則傳回。

HTTP 狀態碼：400

FileSystemNotFound

如果請求者中不存在指定的`FileSystemId` AWS 帳戶值，則返回。

HTTP 狀態碼：404

InternalServerError

如果伺服器端發生錯誤，則傳回。

HTTP 狀態碼：500

PolicyNotFound

如果指定 EFS 檔案系統的預設檔案系統政策生效，則傳回。

HTTP 狀態碼：404

ValidationException

如果提出請求的 AWS Backup 服務不可用，則返回。 AWS 區域

HTTP 狀態碼：400

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面

- AWS SDK for .NET
- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK
- AWS SDK for Java V2 的开发
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

DescribeFileSystemPolicy

傳回指定 EFS 檔案系統的 FileSystemPolicy。

這項操作需要 elasticfilesystem:DescribeFileSystemPolicy 動作的許可。

請求語法

```
GET /2015-02-01/file-systems/FileSystemId/policy HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

FileSystemId

指定要擷取 FileSystemPolicy 的 EFS 檔案系統。

長度限制：長度上限為 128。

模式：^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "FileSystemId": "string",
   "Policy": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

FileSystemId

指定 FileSystemPolicy 套用的 EFS 檔案系統。

類型：字串

長度限制：長度上限為 128。

模式：^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$

Policy

適用於 EFS 檔案系統的 JSON 格式化 FileSystemPolicy。

類型：字串

長度限制：長度下限為 1。長度上限為 20,000。

模式：[\s\S]+

錯誤

BadRequest

如果請求格式錯誤或包含錯誤，例如無效的參數值或缺少必要參數，則傳回。

HTTP 狀態碼：400

FileSystemNotFound

如果請求者中不存在指定的FileSystemId AWS 帳戶值，則返回。

HTTP 狀態碼：404

InternalServerError

如果伺服器端發生錯誤，則傳回。

HTTP 狀態碼：500

PolicyNotFound

如果指定 EFS 檔案系統的預設檔案系統政策生效，則傳回。

HTTP 狀態碼：404

範例

範例

此範例說明的一種用法 DescribeFileSystemPolicy。

請求範例

```
GET /2015-02-01/file-systems/fs-01234567/policy HTTP/1.1
```

回應範例

```
{
    "FileSystemId": "fs-01234567",
    "Policy": "{
        "Version": "2012-10-17",
        "Id": "efs-policy-wizard-cdef0123-aaaa-6666-5555-444455556666",
        "Statement": [
            {
                "Sid": "efs-statement-abcdef01-1111-bbbb-2222-111122224444",
                "Effect" : "Deny",
                "Principal": {
                "AWS": "*"
                },
                "Action": "*",
                "Resource": "arn:aws:elasticfilesystem:us-east-2:111122223333:file-
system/fs-01234567",
                "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                    }
                }
            },
            {
                "Sid": "efs-statement-01234567-aaaa-3333-4444-111122223333",
                "Effect": "Allow",
                "Principal": {
                    "AWS": "*"
                },
                "Action": [
```

```
                    "elasticfilesystem:ClientMount",
                    "elasticfilesystem:ClientWrite"
                ],
                "Resource" : "arn:aws:elasticfilesystem:us-east-2:111122223333:file-
system/fs-01234567"
            }
        ]
    }
}
```

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

DescribeFileSystems

如果提供了檔案系統 CreationToken 或 FileSystemId，則傳回特定 Amazon EFS 檔案系統的說明。否則，它將返回調用者在您調用的端點 AWS 帳戶 中擁有 AWS 區域 的所有文件系統的描述。

擷取所有檔案系統描述時，您可以選擇性地指定 MaxItems 參數，以限制回應中的描述數目。此數字會自動設定為 100。如果要保留更多檔案系統描述，Amazon EFS 會在回應中傳回 NextMarker (不透明權杖)。在這種情況下，您應該使用 Marker 請求參數 (設定為 NextMarker 的值) 傳送後續請求。

若要擷取檔案系統描述清單，則要在反覆程序中使用如下操作，即先呼叫 DescribeFileSystems 而不包含 Marker，然後使用 Marker 參數繼續呼叫，直至沒有 NextMarker 回應爲止。其中，參數設定為先前回應的 NextMarker 值。

未指定一次 DescribeFileSystems 呼叫回應中傳回的檔案系統順序，也未指定跨多路呼叫重複回應傳回的檔案系統順序。

這項操作需要 elasticfilesystem:DescribeFileSystems 動作的許可。

請求語法

```
GET /2015-02-01/file-systems?
CreationToken=CreationToken&FileSystemId=FileSystemId&Marker=Marker&MaxItems=MaxItems
 HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

CreationToken

(可選) 使用此建立權杖 (字串) 將列表限制為檔案系統。建立 Amazon EFS 檔案系統時，您要指定建立權杖。

長度限制：長度下限為 1。長度上限為 64。

模式：.+

FileSystemId

(選用) 您要擷取其說明的檔案系統 ID (字串)。

長度限制：長度上限為 128。

模式：^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$

Marker

(選用) 從先前的 DescribeFileSystems 操作中傳回不透明分頁權杖 (字串)。如果存在，則指定從傳回呼叫中斷的地方繼續列表。

長度限制：長度下限為 1。長度上限為 128。

模式：.+

MaxItems

(選用) 指定回應中傳回的檔案系統數量上限。此數字會自動設定為 100。如果您有 100 多個檔案系統，那麼回應會以每頁 100 進行分頁。

有效範圍：最小值為 1。

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "FileSystems": [
      {
         "AvailabilityZoneId": "string",
         "AvailabilityZoneName": "string",
         "CreationTime": number,
         "CreationToken": "string",
         "Encrypted": boolean,
         "FileSystemArn": "string",
         "FileSystemId": "string",
         "FileSystemProtection": {
            "ReplicationOverwriteProtection": "string"
         },
         "KmsKeyId": "string",
         "LifeCycleState": "string",
```

```
         "Name": "string",
         "NumberOfMountTargets": number,
         "OwnerId": "string",
         "PerformanceMode": "string",
         "ProvisionedThroughputInMibps": number,
         "SizeInBytes": {
            "Timestamp": number,
            "Value": number,
            "ValueInArchive": number,
            "ValueInIA": number,
            "ValueInStandard": number
         },
         "Tags": [
            {
               "Key": "string",
               "Value": "string"
            }
         ],
         "ThroughputMode": "string"
      }
   ],
   "Marker": "string",
   "NextMarker": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

FileSystems

檔案系統描述陣列。

類型：FileSystemDescription 物件陣列

Marker

如果在請求中由發起人提供了相應的信息 (字串)，那麼這個信息就會在響應中呈現。

類型：字串

長度限制：長度下限為 1。長度上限為 128。

模式：.+

NextMarker

如果在回應中傳回的文件系統數量少於所有存在的文件系統，那麼相應的信息 (字串)就會在響應中呈現。您可以在後續請求中使用 NextMarker 來擷取下一頁描述。

類型：字串

長度限制：長度下限為 1。長度上限為 128。

模式：.+

錯誤

BadRequest

如果請求格式錯誤或包含錯誤，例如無效的參數值或缺少必要參數，則傳回。

HTTP 狀態碼：400

FileSystemNotFound

如果請求者中不存在指定的FileSystemId AWS 帳戶值，則返回。

HTTP 狀態碼：404

InternalServerError

如果伺服器端發生錯誤，則傳回。

HTTP 狀態碼：500

範例

擷取 10 個檔案系統清單

下列範例會將 GET 請求傳送至 file-systems 端點 (elasticfilesystem.us-west-2.amazonaws.com/2015-02-01/file-systems)。請求會指定 MaxItems 查詢參數，以便將檔案系統描述的數目限制為 10。

請求範例

```
GET /2015-02-01/file-systems?MaxItems=10 HTTP/1.1
```

```
Host: elasticfilesystem.us-west-2.amazonaws.com
x-amz-date: 20140622T191208Z
Authorization: <...>
```

回應範例

```
HTTP/1.1 200 OK
x-amzn-RequestId: 01234567-89ab-cdef-0123-456789abcdef
Content-Type: application/json
Content-Length: 499
{
   "FileSystems":[
      {
         "OwnerId":"251839141158",
         "CreationToken":"MyFileSystem1",
         "FileSystemId":"fs-01234567",
         "PerformanceMode" : "generalPurpose",
         "CreationTime":"1403301078",
         "LifeCycleState":"created",
         "Name":"my first file system",
         "NumberOfMountTargets":1,
         "SizeInBytes":{
            "Timestamp": 1403301078,
            "Value": 29313618372,
            "ValueInArchive": 201156,
            "ValueInIA": 675432,
            "ValueInStandard": 29312741784
         }
      }
   ]
}
```

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK
- AWS 適用於 Java V2 的 SDK

- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

DescribeLifecycleConfiguration

傳回指定 Amazon EFS 檔案系統的目前 LifecycleConfiguration 物件。生命週期管理使用 LifecycleConfiguration 物件來識別在儲存類別之間移動檔案的時間。對於沒有 LifecycleConfiguration 物件的檔案系統，呼叫會在回應中傳回空陣列。

這項操作需要 elasticfilesystem:DescribeLifecycleConfiguration 動作許可。

請求語法

```
GET /2015-02-01/file-systems/FileSystemId/lifecycle-configuration HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

FileSystemId

您要擷取其 LifecycleConfiguration 物件的檔案系統 ID (字串)。

長度限制：長度上限為 128。

模式：^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "LifecyclePolicies": [
      {
         "TransitionToArchive": "string",
         "TransitionToIA": "string",
```

```
        "TransitionToPrimaryStorageClass": "string"
      }
   ]
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

LifecyclePolicies

生命週期管理政策陣列。EFS 最多為每個檔案系統支援一個政策。

類型：LifecyclePolicy 物件陣列

陣列成員：最多 3 個項目。

錯誤

BadRequest

如果請求格式錯誤或包含錯誤，例如無效的參數值或缺少必要參數，則傳回。

HTTP 狀態碼：400

FileSystemNotFound

如果請求者中不存在指定的`FileSystemId` AWS 帳戶值，則返回。

HTTP 狀態碼：404

InternalServerError

如果伺服器端發生錯誤，則傳回。

HTTP 狀態碼：500

範例

擷取檔案系統的生命週期組態

下列請求會擷取指定檔案系統的 `LifecycleConfiguration` 物件。

請求範例

```
GET /2015-02-01/file-systems/fs-01234567/lifecycle-configuration HTTP/1.1
Host: elasticfilesystem.us-west-2.amazonaws.com
x-amz-date: 20181120T221118Z
Authorization: <...>
```

回應範例

```
HTTP/1.1 200 OK
        x-amzn-RequestId: 01234567-89ab-cdef-0123-456789abcdef
        Content-Type: application/json
        Content-Length: 86
{
  "LifecyclePolicies": [
    {
        "TransitionToArchive": "AFTER_270_DAYS"
    },
    {
        "TransitionToIA": "AFTER_14_DAYS"
    },
    {
        "TransitionToPrimaryStorageClass": "AFTER_1_ACCESS"
    }
  ]
}
```

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP

- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

DescribeMountTargets

傳回所有目前掛載目標的說明，或檔案系統的特定掛載目標。當請求所有目前的掛載目標時，未指定回應中傳回的掛載目標順序。

在 FileSystemId 中指定的檔案系統 ID 上或在 MountTargetId 中指定的掛載目標檔案系統上，此操作需要獲得 elasticfilesystem:DescribeMountTargets 動作的許可。

請求語法

```
GET /2015-02-01/mount-targets?
AccessPointId=AccessPointId&FileSystemId=FileSystemId&Marker=Marker&MaxItems=MaxItems&MountTarg
 HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

AccessPointId

(選用) 您要列出其掛載目標的存取點 ID。如果您的請求中不包含 FileSystemId 或 MountTargetId，則其必須包含在您的請求中。接受作為輸入的存取點 ID 或 ARN。

長度限制：長度上限為 128。

模式：^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:access-point/fsap-[0-9a-f]{8,40}|fsap-[0-9a-f]{8,40})$

FileSystemId

(選用) 您要列出其掛載目標的檔案系統 ID (字串)。如果您的請求中不包含 AccessPointId 或 MountTargetId，則其必須包含在您的請求中。接受作為輸入的檔案系統 ID 或 ARN。

長度限制：長度上限為 128。

模式：^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$

Marker

(選用) 從先前的 DescribeMountTargets 操作中傳回不透明分頁權杖 (字串)。如果存在，則指定從先前傳回呼叫中斷的地方繼續列表。

長度限制：長度下限為 1。長度上限為 128。

模式：`.+`

MaxItems

(選用) 在回應中傳回的掛載目標數量上限。目前，此數字會自動設定為 10，而忽略其他值。如果您有 100 多個掛載目標，那麼回應會以每頁 100 進行分頁。

有效範圍：最小值為 1。

MountTargetId

(選用) 您要描述的掛載目標 ID (字串)。如果您的請求中不包含 `FileSystemId`，則其必須包含在您的請求中。接受作為輸入的掛載目標 ID 或 ARN。

長度限制：長度下限為 13。長度上限為 45。

模式：`^fsmt-[0-9a-f]{8,40}$`

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "Marker": "string",
   "MountTargets": [
      {
         "AvailabilityZoneId": "string",
         "AvailabilityZoneName": "string",
         "FileSystemId": "string",
         "IpAddress": "string",
         "LifeCycleState": "string",
         "MountTargetId": "string",
         "NetworkInterfaceId": "string",
         "OwnerId": "string",
         "SubnetId": "string",
         "VpcId": "string"
```

```
      }
   ],
   "NextMarker": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

Marker

如果請求包含 Marker，則回應會在此欄位中傳回該值。

類型：字串

長度限制：長度下限為 1。長度上限為 128。

模式：.+

MountTargets

將文件系統的掛載目標作為 MountTargetDescription 對象陣列傳回。

類型：MountTargetDescription 物件陣列

NextMarker

如果值存在，則會有更多要傳回的掛載目標。在後續請求中，您可以在請求中使用此值來提供 Marker，以擷取下一組掛載目標。

類型：字串

長度限制：長度下限為 1。長度上限為 128。

模式：.+

錯誤

AccessPointNotFound

如果請求者中不存在指定的AccessPointId AWS 帳戶值，則返回。

HTTP 狀態碼：404

BadRequest

如果請求格式錯誤或包含錯誤，例如無效的參數值或缺少必要參數，則傳回。

HTTP 狀態碼：400

FileSystemNotFound

如果請求者中不存在指定的`FileSystemId` AWS 帳戶值，則返回。

HTTP 狀態碼：404

InternalServerError

如果伺服器端發生錯誤，則傳回。

HTTP 狀態碼：500

MountTargetNotFound

如果在發起人的 AWS 帳戶帳戶中找不到指定 ID 的掛載目標，則傳回。

HTTP 狀態碼：404

範例

擷取為檔案系統建立的掛載目標說明

下列請求會擷取針對指定檔案系統建立的掛載目標說明。

請求範例

```
GET /2015-02-01/mount-targets?FileSystemId=fs-01234567 HTTP/1.1
Host: elasticfilesystem.us-west-2.amazonaws.com
x-amz-date: 20140622T191252Z
Authorization: <...>
```

回應範例

```
HTTP/1.1 200 OK
x-amzn-RequestId: 01234567-89ab-cdef-0123-456789abcdef
Content-Type: application/json
```

```
Content-Length: 357

{
   "MountTargets":[
      {
         "OwnerId":"251839141158",
         "MountTargetId":"fsmt-01234567",
         "FileSystemId":"fs-01234567",
         "SubnetId":"subnet-01234567",
         "LifeCycleState":"added",
         "IpAddress":"10.0.2.42",
         "NetworkInterfaceId":"eni-1bcb7772"
      }
   ]
}
```

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

DescribeMountTargetSecurityGroups

傳回掛載目標目前作用中的安全群組。此操作要求已建立掛載目標的網路介面，且掛載目標的生命週期狀態不是「已刪除 (deleted)」 。

此操作需要以下動作的許可：

- 掛載目標檔案系統上的 elasticfilesystem:DescribeMountTargetSecurityGroups 動作。
- ec2:DescribeNetworkInterfaceAttribute 掛載目標網路介面上的動作。

請求語法

```
GET /2015-02-01/mount-targets/MountTargetId/security-groups HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

MountTargetId

您要擷取其安全群組的掛載目標 ID。

長度限制：長度下限為 13。長度上限為 45。

模式：^fsmt-[0-9a-f]{8,40}$

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "SecurityGroups": [ "string" ]
```

```
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

SecurityGroups

安全群組陣列。

類型：字串陣列

陣列成員：最多 100 個項目。

長度限制：長度下限為 11。長度上限為 43。

模式：`^sg-[0-9a-f]{8,40}`

錯誤

BadRequest

如果請求格式錯誤或包含錯誤，例如無效的參數值或缺少必要參數，則傳回。

HTTP 狀態碼：400

IncorrectMountTargetState

如果掛載目標並未處於操作的正確狀態，則傳回。

HTTP 狀態碼：409

InternalServerError

如果伺服器端發生錯誤，則傳回。

HTTP 狀態碼：500

MountTargetNotFound

如果在發起人的 AWS 帳戶帳戶中找不到指定 ID 的掛載目標，則傳回。

HTTP 狀態碼：404

範例

擷取對檔案系統有效的安全群組

下列範例會擷取安全群組，這些安全群組對與掛載目標相關聯的網路介面有效。

請求範例

```
GET /2015-02-01/mount-targets/fsmt-9a13661e/security-groups HTTP/1.1
Host: elasticfilesystem.us-west-2.amazonaws.com
x-amz-date: 20140620T223513Z
Authorization: <...>
```

回應範例

```
HTTP/1.1 200 OK
x-amzn-RequestId: 01234567-89ab-cdef-0123-456789abcdef
Content-Length: 57

{
"SecurityGroups" : [
"sg-188d9f74"
]
}
```

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

DescribeReplicationConfigurations

擷取特定檔案系統的複寫組態。如果未指定檔案系統，則會擷取 AWS 帳戶 中的所有複製組態。 AWS 區域

請求語法

```
GET /2015-02-01/file-systems/replication-configurations?
FileSystemId=FileSystemId&MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

FileSystemId

您可以提供特定檔案系統的 ID，來擷取特定檔案系統的複寫組態。

長度限制：長度上限為 128。

模式：`^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

MaxResults

(選用) 若要限制傳回在回應中的物件數目，您可以指定 MaxItems 參數。預設值為 100.

有效範圍：最小值為 1。

NextToken

如果是分頁回應，那麼將會出現 NextToken。您可以在後續請求中使用 NextToken 來擷取下一頁輸出。

長度限制：長度下限為 1。長度上限為 128。

模式：`.+`

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "Replications": [
      {
         "CreationTime": number,
         "Destinations": [
            {
               "FileSystemId": "string",
               "LastReplicatedTimestamp": number,
               "Region": "string",
               "Status": "string"
            }
         ],
         "OriginalSourceFileSystemArn": "string",
         "SourceFileSystemArn": "string",
         "SourceFileSystemId": "string",
         "SourceFileSystemRegion": "string"
      }
   ]
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

NextToken

您可以在後續請求中使用先前回應裏的 NextToken 來擷取下一頁的存取點描述。

類型：字串

長度限制：長度下限為 1。長度上限為 128。

模式：.+

Replications

傳回的複寫組態集合。

類型：ReplicationConfigurationDescription 物件陣列

錯誤

BadRequest

如果請求格式錯誤或包含錯誤，例如無效的參數值或缺少必要參數，則傳回。

HTTP 狀態碼：400

FileSystemNotFound

如果請求者中不存在指定的`FileSystemId` AWS 帳戶值，則返回。

HTTP 狀態碼：404

InternalServerError

如果伺服器端發生錯誤，則傳回。

HTTP 狀態碼：500

ReplicationNotFound

如果指定的檔案系統沒有複寫組態，則傳回。

HTTP 狀態碼：404

ValidationException

如果提出請求的 AWS Backup 服務不可用，則返回。 AWS 區域

HTTP 狀態碼：400

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET

- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

DescribeTags

> **Note**
>
> 已作廢：DescribeTags 動作已作廢且不受維護。若要檢視與 EFS 資源相關聯的標籤，請使用 ListTagsForResource API 動作。

傳回與檔案系統相關聯的所有標籤。未指定一次 DescribeTags 呼叫回應中傳回的標籤順序，也未指定跨多路呼叫 (使用分頁時) 重複回應傳回的標籤順序。

這項操作需要 elasticfilesystem:DescribeTags 動作的許可。

請求語法

```
GET /2015-02-01/tags/FileSystemId/?Marker=Marker&MaxItems=MaxItems HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

FileSystemId

您要擷取其標籤的檔案系統 ID。

長度限制：長度上限為 128。

模式：^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$

必要：是

Marker

(選用) 從先前的 DescribeTags 操作中傳回不透明分頁權杖 (字串)。如果存在，則指定從先前呼叫中斷的地方繼續列表。

長度限制：長度下限為 1。長度上限為 128。

模式：.+

MaxItems

(選用) 在回應中傳回的檔案系統數量上限。目前，此數字會自動設定為 100，而忽略其他值。如果您有 100 多個標籤，那麼回應會以每頁 100 進行分頁。

有效範圍：最小值為 1。

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "Marker": "string",
   "NextMarker": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

Marker

如果請求包含 `Marker`，則回應會在此欄位中傳回該值。

類型：字串

長度限制：長度下限為 1。長度上限為 128。

模式：`.+`

NextMarker

如果值存在，則會有更多要傳回的標籤。在後續請求中，您可以在下一個請求中提供 NextMarker 的值作為 Marker 參數值的值，以擷取下一組標籤。

類型：字串

長度限制：長度下限為 1。長度上限為 128。

模式：.+

Tags

傳回與檔案系統相關聯的標籤做為 Tag 物件陣列的檔案系統。

類型：Tag 物件陣列

錯誤

BadRequest

如果請求格式錯誤或包含錯誤，例如無效的參數值或缺少必要參數，則傳回。

HTTP 狀態碼：400

FileSystemNotFound

如果請求者中不存在指定的FileSystemId AWS 帳戶值，則返回。

HTTP 狀態碼：404

InternalServerError

如果伺服器端發生錯誤，則傳回。

HTTP 狀態碼：500

範例

擷取與檔案系統相關聯的所有標籤

下列請求會擷取與指定檔案系統相關聯的標籤 (鍵值對)。

請求範例

```
GET /2015-02-01/tags/fs-01234567/ HTTP/1.1
Host: elasticfilesystem.us-west-2.amazonaws.com
x-amz-date: 20140620T215404Z
Authorization: <...>
```

回應範例

```
HTTP/1.1 200 OK
x-amzn-RequestId: 01234567-89ab-cdef-0123-456789abcdef
Content-Type: application/json
Content-Length: 288

{
    "Tags":[
        {
            "Key":"Name",
            "Value":"my first file system"
        },
        {
            "Key":"Fleet",
            "Value":"Development"
        },
        {
            "Key":"Developer",
            "Value":"Alice"
        }
    ]
}
```

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK
- AWS SDK for Java V2 的軟件

- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

ListTagsForResource

列出頂層 EFS 資源的所有標籤。您必須提供要擷取標籤的資源 ID。

這項操作需要 elasticfilesystem:DescribeAccessPoints 動作的許可。

請求語法

```
GET /2015-02-01/resource-tags/ResourceId?MaxResults=MaxResults&NextToken=NextToken
 HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

MaxResults

(選用) 指定回應中傳回的檔案系統數量上限。預設值為 100.

有效範圍：最小值為 1。

NextToken

(選用) 如果回應承載已分頁，您可以在後續請求中使用 NextToken 來擷取下一頁存取點描述。

長度限制：長度下限為 1。長度上限為 128。

模式：.+

ResourceId

指定您要擷取標籤的 EFS 資源。您可以使用此 API 端點擷取 EFS 檔案系統和存取點的標籤。

長度限制：長度上限為 128。

模式：^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:(access-point/fsap|file-system/fs)-[0-9a-f]{8,40}|fs(ap)?-[0-9a-f]{8,40})$

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

NextToken

如果對回應承載進行分頁，那麼將會出現 NextToken。您可以在後續請求中使用 NextToken 來擷取下一頁的存取點描述。

類型：字串

長度限制：長度下限為 1。長度上限為 128。

模式：.+

Tags

指定 EFS 資源的標籤陣列。

類型：Tag 物件陣列

錯誤

AccessPointNotFound

如果請求者中不存在指定的AccessPointId AWS 帳戶值，則返回。

HTTP 狀態碼：404

BadRequest

如果請求格式錯誤或包含錯誤，例如無效的參數值或缺少必要參數，則傳回。

HTTP 狀態碼：400

FileSystemNotFound

如果請求者中不存在指定的`FileSystemId` AWS 帳戶值，則返回。

HTTP 狀態碼：404

InternalServerError

如果伺服器端發生錯誤，則傳回。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

ModifyMountTargetSecurityGroups

修改掛載目標的作用中的安全群組。

當您建立掛載目標時，Amazon EFS 也會建立新的網路介面。如需詳細資訊，請參閱 CreateMountTarget。此作業會以要求中提供的，取代與掛載目標相關聯之網路介面的 SecurityGroups 有效安全群組。此操作要求已建立掛載目標的網路介面，且掛載目標的生命週期狀態不是「已刪除 (deleted)」 。

此作業需要下列動作的權限：

- 掛載目標檔案系統上的 elasticfilesystem:ModifyMountTargetSecurityGroups 動作。
- ec2:ModifyNetworkInterfaceAttribute 掛載目標網路介面上的動作。

請求語法

```
PUT /2015-02-01/mount-targets/MountTargetId/security-groups HTTP/1.1
Content-type: application/json

{
   "SecurityGroups": [ "string" ]
}
```

URI 請求參數

請求會使用下列 URI 參數。

MountTargetId

您要修改其安全群組的掛載目標 ID。

長度限制：長度下限為 13。長度上限為 45。

模式：^fsmt-[0-9a-f]{8,40}$

必要：是

請求主體

請求接受採用 JSON 格式的下列資料。

SecurityGroups

最多五個 VPC 安全群組 ID 陣列。

類型：字串陣列

陣列成員：最多 100 個項目。

長度限制：長度下限為 11。長度上限為 43。

模式：`^sg-[0-9a-f]{8,40}`

必要：否

回應語法

```
HTTP/1.1 204
```

回應元素

如果動作成功，則服務會送回具有空 HTTP 主體的 HTTP 204 回應。

錯誤

BadRequest

如果請求格式錯誤或包含錯誤，例如無效的參數值或缺少必要參數，則傳回。

HTTP 狀態碼：400

IncorrectMountTargetState

如果掛載目標並未處於操作的正確狀態，則傳回。

HTTP 狀態碼：409

InternalServerError

如果伺服器端發生錯誤，則傳回。

HTTP 狀態碼：500

MountTargetNotFound

如果在發起人的 AWS 帳戶帳戶中找不到指定 ID 的掛載目標，則傳回。

HTTP 狀態碼：404

SecurityGroupLimitExceeded

如果請求中指定的 SecurityGroups 大小大於五，則傳回。

HTTP 狀態碼：400

SecurityGroupNotFound

如果子網路的虛擬私有雲端 (VPC) 中沒有其中一個指定的安全群組，則傳回。

HTTP 狀態碼：400

範例

取代裝載目標的安全群組

下列範例會取代與掛載目標相關聯之網路介面的有效安全群組。

請求範例

```
PUT /2015-02-01/mount-targets/fsmt-9a13661e/security-groups HTTP/1.1
Host: elasticfilesystem.us-west-2.amazonaws.com
x-amz-date: 20140620T223446Z
Authorization: <...>
Content-Type: application/json
Content-Length: 57

{
  "SecurityGroups" : [
  "sg-188d9f74"
  ]
}
```

回應範例

```
HTTP/1.1 204 No Content
x-amzn-RequestId: 01234567-89ab-cdef-0123-456789abcdef
```

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

PutAccountPreferences

使用此操作可設定目前 AWS 區域 區域中的帳戶偏好，以便為新 EFS 檔案系統使用長至 17 個字元 (63 位元) 或短至 8 個字元 (32 位元) 的資源 ID，並掛載目標資源。您所做的任何變更都不會影響所有現有資源 ID。當 EFS 轉移至長資源 ID 時，您可以在加入期間設定 ID 偏好。如需詳細資訊，請參閱管理 Amazon EFS 資源 ID。

> **Note**
>
> 從 2021 年 10 月開始，如果您嘗試將帳戶偏好設定為使用簡短的 8 字元格式資源 ID，將會收到錯誤訊息。如果您收到錯誤訊息，且必須針對檔案系統使用短 ID 並掛載目標資源，請連絡 AWS 支援部門。

請求語法

```
PUT /2015-02-01/account-preferences HTTP/1.1
Content-type: application/json

{
   "ResourceIdType": "string"
}
```

URI 請求參數

請求不會使用任何 URI 參數。

請求主體

請求接受採用 JSON 格式的下列資料。

ResourceIdType

指定要為使用者設定的 EFS 資源 ID 偏好設定 AWS 區域，其中包括 LONG_ID (17 個字元) 或 SHORT_ID (8 個字元)。 AWS 帳戶

> **Note**
>
> 從 2021 年 10 月開始，將帳戶偏好設定為 SHORT_ID 時，您將收到錯誤信息。如果您收到錯誤訊息，且必須針對檔案系統使用短 ID 並掛載目標資源，請連絡 AWS 支援部門。

類型：字串

有效值:LONG_ID | SHORT_ID

必要：是

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "ResourceIdPreference": {
      "ResourceIdType": "string",
      "Resources": [ "string" ]
   }
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

ResourceIdPreference

描述目前使用者的 AWS 帳戶資源類型及其 ID 偏好設定 AWS 區域。

類型：ResourceIdPreference 物件

錯誤

BadRequest

如果請求格式錯誤或包含錯誤，例如無效的參數值或缺少必要參數，則傳回。

HTTP 狀態碼：400

InternalServerError

如果伺服器端發生錯誤，則傳回。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

PutBackupPolicy

更新檔案系統備份政策。使用此動作可啟動或停止檔案系統的自動備份。

請求語法

```
PUT /2015-02-01/file-systems/FileSystemId/backup-policy HTTP/1.1
Content-type: application/json

{
   "BackupPolicy": {
      "Status": "string"
   }
}
```

URI 請求參數

請求會使用下列 URI 參數。

FileSystemId

指定要更新備份政策的 EFS 檔案系統。

長度限制：長度上限為 128。

模式：`^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

必要：是

請求主體

請求接受採用 JSON 格式的下列資料。

BackupPolicy

包含在 PutBackupPolicy 請求中的備份政策。

類型：BackupPolicy 物件

必要：是

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPolicy": {
      "Status": "string"
   }
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

BackupPolicy

描述檔案系統的備份政策，指出自動備份是開啟還是關閉。

類型：BackupPolicy 物件

錯誤

BadRequest

如果請求格式錯誤或包含錯誤，例如無效的參數值或缺少必要參數，則傳回。

HTTP 狀態碼：400

FileSystemNotFound

如果請求者中不存在指定的FileSystemId AWS 帳戶值，則返回。

HTTP 狀態碼：404

IncorrectFileSystemLifeCycleState

如果檔案系統的生命週期狀態不是「可用」，則傳回。

HTTP 狀態碼：409

InternalServerError

如果伺服器端發生錯誤，則傳回。

HTTP 狀態碼：500

ValidationException

如果提出請求的 AWS Backup 服務不可用，則返回。 AWS 區域

HTTP 狀態碼：400

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK
- AWS SDK for Java V2 的开发
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

PutFileSystemPolicy

將 Amazon EFS FileSystemPolicy 套用至 Amazon EFS 檔案系統。檔案系統政策是以 IAM 資源為基礎的政策，可包含多個政策聲明。檔案系統一律只有一個檔案系統政策，這些政策可以是預設原則或顯式政策集，或使用此 API 操作更新的政策。EFS 檔案系統政策字元限制為 20,000 以內。設定顯式政策時，該政策會覆寫預設政策。如需有關預設檔案系統原則的詳細資訊，請參閱預設 EFS 檔案系統原則。

> **Note**
>
> EFS 檔案系統政策字元限制為 20,000 以內。

這項操作需要 elasticfilesystem:PutFileSystemPolicy 動作的許可。

請求語法

```
PUT /2015-02-01/file-systems/FileSystemId/policy HTTP/1.1
Content-type: application/json

{
   "BypassPolicyLockoutSafetyCheck": boolean,
   "Policy": "string"
}
```

URI 請求參數

請求會使用下列 URI 參數。

FileSystemId

您要建立或更新 FileSystemPolicy 的 EFS 檔案系統 ID。

長度限制：長度上限為 128。

模式：^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$

必要：是

請求主體

請求接受採用 JSON 格式的下列資料。

BypassPolicyLockoutSafetyCheck

(選用) 用於指定是否繞過 FileSystemPolicy 政策鎖定安全檢查的布林值。鎖定安全檢查會決定請求中的政策是否鎖定 (阻止) 提出請求的 IAM 主體在此檔案系統上提出未來的 PutFileSystemPolicy 請求。僅當您打算阻止提出請求的 IAM 主體在此檔案系統上提出後續的 PutFileSystemPolicy 請求時，才將 BypassPolicyLockoutSafetyCheck 設定為 True。預設值為 False。

類型：布林值

必要：否

Policy

您正在建立 FileSystemPolicy。接受 JSON 格式化政策定義。EFS 檔案系統政策字元限制為 20,000 以內。若要深入瞭解組成檔案系統政策的元素，請參閱 Amazon EFS 中以資源為基礎的政策。

類型：字串

長度限制：長度下限為 1。長度上限為 20,000。

模式：[\s\S]+

必要：是

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "FileSystemId": "string",
   "Policy": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

FileSystemId

指定 FileSystemPolicy 套用的 EFS 檔案系統。

類型：字串

長度限制：長度上限為 128。

模式：^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$

Policy

適用於 EFS 檔案系統的 JSON 格式化 FileSystemPolicy。

類型：字串

長度限制：長度下限為 1。長度上限為 20,000。

模式：[\s\S]+

錯誤

BadRequest

如果請求格式錯誤或包含錯誤，例如無效的參數值或缺少必要參數，則傳回。

HTTP 狀態碼：400

FileSystemNotFound

如果請求者中不存在指定的FileSystemId AWS 帳戶值，則返回。

HTTP 狀態碼：404

IncorrectFileSystemLifeCycleState

如果檔案系統的生命週期狀態不是「可用」，則傳回。

HTTP 狀態碼：409

InternalServerError

如果伺服器端發生錯誤，則傳回。

HTTP 狀態碼：500

InvalidPolicyException

如果 FileSystemPolicy 格式錯誤或包含錯誤，例如無效的參數值或缺少必要參數，則傳回。如果出現政策鎖定安全檢查錯誤，則傳回。

HTTP 狀態碼：400

範例

建立一個 EFS FileSystemPolicy

下列要求會建立可FileSystemPolicy讓所有 AWS 主體以讀取和寫入權限裝載指定的 EFS 檔案系統。

請求範例

```
PUT /2015-02-01/file-systems/fs-01234567/file-system-policy HTTP/1.1
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "elasticfilesystem:ClientMount",
                "elasticfilesystem:ClientWrite"
            ],
            "Principal": {
                "AWS": ["*"]
            },
        }
    ]
}
```

回應範例

```
{
    "Version": "2012-10-17",
    "Id": "1",
    "Statement": [
        {
```

```
            "Sid": "efs-statement-abcdef01-1111-bbbb-2222-111122224444",
            "Effect": "Allow",
            "Action": [
                "elasticfilesystem:ClientMount",
                "elasticfilesystem:ClientWrite"
            ],
            "Principal": {
                "AWS": ["*"]
            },
            "Resource":"arn:aws:elasticfilesystem:us-east-1:1111222233334444:file-
system/fs-01234567"
        }
    ]
}
```

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

PutLifecycleConfiguration

使用此動作可管理檔案系統的儲存空間。LifecycleConfiguration 由定義下列項目的一或多個 LifecyclePolicy 物件組成：

- **TransitionToIA**：何時將檔案系統中的檔案從主要儲存 (標準儲存類別) 移至 Infrequent Access (IA) 儲存類別。
- **TransitionToArchive**：何時將檔案系統中的檔案從目前主要儲存類別 (IA 或標準儲存) 移至「封存」儲存。

  檔案系統在轉移至 IA 儲存之前，無法轉移至「封存」儲存。因此，不 TransitionToArchive 得設定或必須晚於 TransitionTo IA。

  > **Note**
  >
  > 封存儲存體類別僅適用於使用彈性輸送量模式和一般目的效能模式的檔案系統。

- **TransitionToPrimaryStorageClass**：在檔案系統中的檔案存取到 IA 或「封存」儲存后，是否將其移回主要存儲 (標準存儲類別)。

如需詳細資訊，請參閱管理檔案系統儲存。

每個 Amazon EFS 檔案系統都支援一個生命週期組態，該組態適用於檔案系統中的所有檔案。如果指定的檔案系統已存在 LifecycleConfiguration 物件，則 PutLifecycleConfiguration 呼叫會修改現有組態。請求主體中含有空 LifecyclePolicies 陣列的 PutLifecycleConfiguration 呼叫會刪除任何現有的 LifecycleConfiguration。在請求中，指定下列項目：

- 您要啟用、停用或修改生命週期管理之檔案系統的 ID。
- LifecyclePolicy 物件的 LifecyclePolicies 陣列用於定義將檔案移至 IA 儲存、「封存」儲存，以及移回主要儲存的時間。

> **Note**
>
> Amazon EFS 要求每個 `LifecyclePolicy` 物件只能轉移一次，因此 `LifecyclePolicies` 陣列需要使用不同的 `LifecyclePolicy` 物件進行結構化。如需詳細資訊，請參閱下文中的請求範例。

這項操作需要 `elasticfilesystem:PutLifecycleConfiguration` 操作許可。

若要將`LifecycleConfiguration`物件套用至加密的檔案系統，您需要與建立加密檔案系統時相同的 AWS Key Management Service 權限。

請求語法

```
PUT /2015-02-01/file-systems/FileSystemId/lifecycle-configuration HTTP/1.1
Content-type: application/json

{
   "LifecyclePolicies": [
      {
         "TransitionToArchive": "string",
         "TransitionToIA": "string",
         "TransitionToPrimaryStorageClass": "string"
      }
   ]
}
```

URI 請求參數

請求會使用下列 URI 參數。

FileSystemId

正在建立 `LifecycleConfiguration` 物件的檔案系統 ID (字串)。

長度限制：長度上限為 128。

模式：`^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

必要：是

請求主體

請求接受採用 JSON 格式的下列資料。

LifecyclePolicies

用於定義檔案系統 `LifecycleConfiguration` 物件的 `LifecyclePolicy` 物件陣列。`LifecycleConfiguration`物件會通知下列事項的生命週期管理：

- **`TransitionToIA`**：何時將檔案系統中的檔案從主要儲存 (標準儲存類別) 移至 Infrequent Access (IA) 儲存類別。
- **`TransitionToArchive`**：何時將檔案系統中的檔案從目前主要儲存類別 (IA 或標準儲存) 移至「封存」儲存。

  檔案系統在轉移至 IA 儲存之前，無法轉移至「封存」儲存。因此，不 TransitionToArchive 得設定或必須晚於 TransitionTo IA。

  > **Note**
  >
  > 封存儲存體類別僅適用於使用彈性輸送量模式和一般目的效能模式的檔案系統。

- **`TransitionToPrimaryStorageClass`**：在檔案系統中的檔案存取到 IA 或「封存」儲存后，是否將其移回主要存儲 (標準存儲類別)。

> **Note**
>
> 使用 `put-lifecycle-configuration` CLI 命令或 `PutLifecycleConfiguration` API 動作時，Amazon EFS 要求每個 `LifecyclePolicy` 物件只能有一次轉移。這意味著在請求內文中，`LifecyclePolicies` 必須結構化為 `LifecyclePolicy` 物件陣列，每次儲存轉移對應一個物件。如需詳細資訊，請參閱下文中的請求範例。

類型：LifecyclePolicy 物件陣列

陣列成員：最多 3 個項目。

必要：是

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "LifecyclePolicies": [
      {
         "TransitionToArchive": "string",
         "TransitionToIA": "string",
         "TransitionToPrimaryStorageClass": "string"
      }
   ]
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

LifecyclePolicies

生命週期管理政策陣列。EFS 最多為每個檔案系統支援一個政策。

類型：LifecyclePolicy 物件陣列

陣列成員：最多 3 個項目。

錯誤

BadRequest

如果請求格式錯誤或包含錯誤，例如無效的參數值或缺少必要參數，則傳回。

HTTP 狀態碼：400

FileSystemNotFound

如果請求者中不存在指定的`FileSystemId` AWS 帳戶值，則返回。

HTTP 狀態碼：404

IncorrectFileSystemLifeCycleState

如果檔案系統的生命週期狀態不是「可用」，則傳回。

HTTP 狀態碼：409

InternalServerError

如果伺服器端發生錯誤，則傳回。

HTTP 狀態碼：500

範例

建立生命週期組態

下列範例會使用 PutLifecycleConfiguration 動作建立 LifecyclePolicy 物件。此範例建立生命週期政策，以便指示 EFS 執行以下操作：

- 將過去 30 天內未在標準儲存中存取過的檔案系統中的所有檔案移至封存儲存。
- 將過去 90 天內未在標準儲存中存取過的檔案系統中的所有檔案移至封存儲存。
- 檔案儲存到 IA 或「封存」儲存中后，再移回標準存儲。封存儲存體類別僅適用於使用彈性輸送量模式和一般目的效能模式的檔案系統。

如需詳細資訊，請參閱 EFS 儲存類別和管理檔案系統儲存。

請求範例

```
PUT /2015-02-01/file-systems/fs-0123456789abcdefb/lifecycle-configuration HTTP/1.1
Host: elasticfilesystem.us-west-2.amazonaws.com
x-amz-date: 20181122T232908Z
Authorization: <...>
Content-type: application/json
Content-Length: 86

{
   "LifecyclePolicies": [
      {
         "TransitionToArchive": "AFTER_90_DAYS"
      },
```

```
      {
         "TransitionToIA": "AFTER_30_DAYS"
      },
      {
         "TransitionToPrimaryStorage": "AFTER_1_ACCESS"
      }
   ]
}
```

回應範例

```
HTTP/1.1 200 OK
x-amzn-RequestId: 01234567-89ab-cdef-0123-456789abcdef
Content-type: application/json
Content-Length: 86

{
    "LifecyclePolicies": [
      {
         "TransitionToArchive": "AFTER_90_DAYS"
      },
      {
         "TransitionToIA": "AFTER_30_DAYS"
      },
      {
         "TransitionToPrimaryStorage": "AFTER_1_ACCESS"
      }
    ]
}
```

put-lifecycle-configuration CLI 要求範例

此範例說明的一種用法 PutLifecycleConfiguration。

請求範例

```
aws efs put-lifecycle-configuration \
   --file-system-id fs-0123456789abcdefb \
   --lifecycle-policies "[{"TransitionToArchive":"AFTER_90_DAYS"},
     {"TransitionToIA":"AFTER_30_DAYS"},
     {"TransitionToPrimaryStorageClass":"AFTER_1_ACCESS"}]
   --region us-west-2 \
   --profile adminuser
```

回應範例

```
{
   "LifecyclePolicies": [
       {
           "TransitionToArchive": "AFTER_90_DAYS"
       },
       {
           "TransitionToIA": "AFTER_30_DAYS"
       },
       {
           "TransitionToPrimaryStorageClass": "AFTER_1_ACCESS"
       }
   ]
}
```

停用生命週期管理

下列範例會停用指定檔案系統的生命週期管理。

請求範例

```
PUT /2015-02-01/file-systems/fs-01234567/lifecycle-configuration HTTP/1.1
Host: elasticfilesystem.us-west-2.amazonaws.com
x-amz-date: 20181122T232908Z
Authorization: <...>
Content-type: application/json
Content-Length: 86

{
   "LifecyclePolicies": [ ]
}
```

回應範例

```
HTTP/1.1 200 OK
```

```
x-amzn-RequestId: 01234567-89ab-cdef-0123-456789abcdef
Content-type: application/json
Content-Length: 86

{
   "LifecyclePolicies": [ ]
}
```

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK
- AWS SDK for Java V2 的开发
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

TagResource

建立 EFS 資源標籤。您可以使用此 API 操作建立 EFS 檔案系統標籤和存取點。

這項操作需要 `elasticfilesystem:TagResource` 動作的許可。

請求語法

```
POST /2015-02-01/resource-tags/ResourceId HTTP/1.1
Content-type: application/json

{
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

URI 請求參數

請求會使用下列 URI 參數。

ResourceId

指定您要為其建立標籤的 EFS 資源的 ID。

長度限制：長度上限為 128。

模式：`^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:(access-point/fsap|file-system/fs)-[0-9a-f]{8,40}|fs(ap)?-[0-9a-f]{8,40})$`

必要：是

請求主體

請求接受採用 JSON 格式的下列資料。

Tags

新增的 Tag 物件陣列。每個 Tag 物件都是一個鍵值對。

類型：Tag 物件陣列

必要：是

回應語法

```
HTTP/1.1 200
```

回應元素

如果動作成功，則服務會傳回具空 HTTP 內文的 HTTP 200 回應。

錯誤

AccessPointNotFound

如果請求者中不存在指定的AccessPointId AWS 帳戶值，則返回。

HTTP 狀態碼：404

BadRequest

如果請求格式錯誤或包含錯誤，例如無效的參數值或缺少必要參數，則傳回。

HTTP 狀態碼：400

FileSystemNotFound

如果請求者中不存在指定的FileSystemId AWS 帳戶值，則返回。

HTTP 狀態碼：404

InternalServerError

如果伺服器端發生錯誤，則傳回。

HTTP 狀態碼：500

範例

建立檔案系統標籤

下列請求會在指定的檔案系統上建立三個標籤 ("key1"、"key2"、和 "key3")。

請求範例

```
POST /2015-02-01/tag-resource/fs-01234567 HTTP/1.1
Host: elasticfilesystem.us-west-2.amazonaws.com
x-amz-date: 20140620T221118Z
Authorization: <...>
Content-Type: application/json
Content-Length: 160

{
    "Tags": [
        {
            "Key": "key1",
            "Value": "value1"
        },
        {
            "Key": "key2",
            "Value": "value2"
        },
        {
            "Key": "key3",
            "Value": "value3"
        }
    ]
}
```

回應範例

```
HTTP/1.1 204 no content
x-amzn-RequestId: 01234567-89ab-cdef-0123-456789abcdef
```

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK
- AWS SDK for Java V2 的軟件

- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

UntagResource

從 EFS 資源移除標籤。您可以使用此 API 操作移除 EFS 檔案系統標籤和存取點。

這項操作需要 `elasticfilesystem:UntagResource` 動作的許可。

請求語法

```
DELETE /2015-02-01/resource-tags/ResourceId?tagKeys=TagKeys HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

ResourceId

指定要移除其中標籤的 EFS 資源。

長度限制：長度上限為 128。

模式：`^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:(access-point/fsap|file-system/fs)-[0-9a-f]{8,40}|fs(ap)?-[0-9a-f]{8,40})$`

必要：是

TagKeys

要從指定 EFS 資源中移除的鍵值標籤對的索引鍵。

陣列成員：項目數下限為 1。項目數上限為 50。

長度限制：長度下限為 1。長度上限為 128。

模式：`^(?![aA]{1}[wW]{1}[sS]{1}:)([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
```

回應元素

如果動作成功，則服務會傳回具空 HTTP 內文的 HTTP 200 回應。

錯誤

AccessPointNotFound

如果請求者中不存在指定的`AccessPointId` AWS 帳戶值，則返回。

HTTP 狀態碼：404

BadRequest

如果請求格式錯誤或包含錯誤，例如無效的參數值或缺少必要參數，則傳回。

HTTP 狀態碼：400

FileSystemNotFound

如果請求者中不存在指定的`FileSystemId` AWS 帳戶值，則返回。

HTTP 狀態碼：404

InternalServerError

如果伺服器端發生錯誤，則傳回。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK

- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

UpdateFileSystem

更新輸送量模式或現有檔案系統的佈建輸送量。

請求語法

```
PUT /2015-02-01/file-systems/FileSystemId HTTP/1.1
Content-type: application/json

{
   "ProvisionedThroughputInMibps": number,
   "ThroughputMode": "string"
}
```

URI 請求參數

請求會使用下列 URI 參數。

FileSystemId

您要更新的檔案系統 ID。

長度限制：長度上限為 128。

模式：`^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

必要：是

請求主體

請求接受採用 JSON 格式的下列資料。

ProvisionedThroughputInMibps

(選擇性) 您要為您建立的檔案系統佈建的輸送量 (以每秒 MB (MiBps) 為單位。若將 `ThroughputMode` 設為 `provisioned`，則為必要項目。有效值為 1-3414 MiBps，上限取決於地區。若要提高此限制，請聯絡 AWS Support。如需詳細資訊，請參閱《Amazon EFS 使用者指南》中的您可以增加的 Amazon EFS 配額。

類型：Double

有效範圍：最小值為 1.0。

必要：否

ThroughputMode

(選用) 更新檔案系統的輸送量模式。如果您不更新輸送量模式，則不需要在請求中提供此值。若您正在將 ThroughputMode 設為 provisioned，您也必須為 ProvisionedThroughputInMibps 設定值。

類型：字串

有效值:bursting | provisioned | elastic

必要：否

回應語法

```
HTTP/1.1 202
Content-type: application/json

{
   "AvailabilityZoneId": "string",
   "AvailabilityZoneName": "string",
   "CreationTime": number,
   "CreationToken": "string",
   "Encrypted": boolean,
   "FileSystemArn": "string",
   "FileSystemId": "string",
   "FileSystemProtection": {
      "ReplicationOverwriteProtection": "string"
   },
   "KmsKeyId": "string",
   "LifeCycleState": "string",
   "Name": "string",
   "NumberOfMountTargets": number,
   "OwnerId": "string",
   "PerformanceMode": "string",
   "ProvisionedThroughputInMibps": number,
   "SizeInBytes": {
      "Timestamp": number,
      "Value": number,
      "ValueInArchive": number,
```

```
      "ValueInIA": number,
      "ValueInStandard": number
   },
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ],
   "ThroughputMode": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 202 回應。

服務會傳回下列 JSON 格式的資料。

AvailabilityZoneId

檔案系統所在可用區域的唯一且一致的識別碼僅對單區域有效。例如，use1-az1是 us-east-1 的可用區域識別碼 AWS 區域，而且它在每個項目中都有相同的位置。 AWS 帳戶

類型：字串

AvailabilityZoneName

描述檔案系統所在的 AWS 可用區域，且僅對單一區域檔案系統有效。如需詳細資訊，請參閱《Amazon EFS 使用者指南》中的使用 EFS 儲存類別。

類型：字串

長度限制：長度下限為 1。長度上限為 64。

模式：.+

CreationTime

建立檔案系統的時間，以秒為單位 (自 1970-01-01T00:00:00Z 以來)。

類型：Timestamp

CreationToken

請求中指定的不透明字串。

類型：字串

長度限制：長度下限為 1。長度上限為 64。

模式：`.+`

Encrypted

布林值，若為 true，指出加密檔案系統。

類型：布林值

FileSystemArn

Amazon EFS 檔案系統的 Amazon Resource Name (ARN)，格式為 `arn:aws:elasticfilesystem:`*`region`*`:`*`account-id`*`:file-system/`*`file-system-id`*。示例資料範例：`arn:aws:elasticfilesystem:us-west-2:1111333322228888:file-system/fs-01234567`

類型：字串

FileSystemId

由 Amazon EFS 指派的檔案系統 ID。

類型：字串

長度限制：長度上限為 128。

模式：`^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

FileSystemProtection

說明檔案系統的防護。

類型：FileSystemProtectionDescription 物件

KmsKeyId

AWS KMS key 用來保護加密檔案系統的識別碼。

類型：字串

長度限制：長度上限為 2048。

模式：^([0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}|mrk-[0-9a-f]{32}|alias/[a-zA-Z0-9/_-]+|(arn:aws[-a-z]*:kms:[a-z0-9-]+:\d{12}:((key/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12})|(key/mrk-[0-9a-f]{32})|(alias/[a-zA-Z0-9/_-]+))))$

LifeCycleState

檔案系統的生命周期階段。

類型：字串

有效值:creating | available | updating | deleting | deleted | error

Name

您可以將標籤 (包括 Name 標籤) 新增至檔案系統。如需詳細資訊，請參閱 CreateFileSystem。如果檔案系統有 Name 標籤，Amazon EFS 會傳回此欄位中的值。

類型：字串

長度限制：長度上限為 256。

模式：^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$

NumberOfMountTargets

檔案系統目前擁有的掛載目標數。如需詳細資訊，請參閱 CreateMountTarget。

類型：整數

有效範圍：最小值為 0。

OwnerId

建 AWS 帳戶 立檔案系統的。

類型：字串

長度限制：長度上限為 14。

模式：^(\d{12})|(\d{4}-\d{4}-\d{4})$

PerformanceMode

檔案系統的效能模式。

類型：字串

有效值:`generalPurpose | maxIO`

ProvisionedThroughputInMibps

檔案系統的佈建輸送量量 (以計量單位)。 MiBps對使用 `ThroughputMode` 設定為 `provisioned` 的檔案系統有效。

類型：Double

有效範圍：最小值為 1.0。

SizeInBytes

儲存在檔案系統、`Value` 欄位中的資料最新已知計量大小 (以位元組為單位)，以及在 `Timestamp` 欄位中決定該大小的時間。`Timestamp` 值是自 1970-01-01T00:00:00Z 以來的整數秒數。`SizeInBytes` 值不代表檔案系統的一致快照集大小，但是在沒有寫入檔案系統時，它最終會保持一致。也就是說，只有超過幾個小時未修改檔案系統，`SizeInBytes` 才能表示實際大小。否則，該值并不能代表檔案系統在任何時間點的確切大小。

類型：FileSystemSize 物件

Tags

與檔案系統相關聯的標籤以 `Tag` 物件陣列形式呈現出來。

類型：Tag 物件陣列

ThroughputMode

顯示檔案系統的輸送量模式。如需詳細資訊，請參閱《Amazon EFS 使用者指南》中的輸送量模式。

類型：字串

有效值:`bursting | provisioned | elastic`

錯誤

BadRequest

如果請求格式錯誤或包含錯誤，例如無效的參數值或缺少必要參數，則傳回。

HTTP 狀態碼：400

FileSystemNotFound

如果請求者中不存在指定的`FileSystemId` AWS 帳戶值，則返回。

HTTP 狀態碼：404

IncorrectFileSystemLifeCycleState

如果檔案系統的生命週期狀態不是「可用」，則傳回。

HTTP 狀態碼：409

InsufficientThroughputCapacity

如果沒有足夠容量佈建其他輸送量，則傳回。當您嘗試以佈建輸送量模式建立檔案系統、嘗試增加現有檔案系統的佈建輸送量，或嘗試將現有檔案系統從「爆增輸送量」變更為「佈建輸送量」模式時，系統可能會傳回此值。請稍後再試。

HTTP 狀態碼：503

InternalServerError

如果在伺服器端發生錯誤，則傳回。

HTTP 狀態碼：500

ThroughputLimitExceeded

如果因為已達到 1024 MB 的輸送量限制而無法變更輸送量模式或佈建輸送量總量，則傳回。

HTTP 狀態碼：400

TooManyRequests

如果您在變更輸送量模式或降低佈建輸送量值之前未等待至少 24 小時，則傳回。

HTTP 狀態碼：429

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++

- AWS 適用於轉到 V2 的 SDK
- AWS SDK for Java V2 的开发
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

UpdateFileSystemProtection

更新檔案系統保護。

這項操作需要 elasticfilesystem:UpdateFileSystemProtection 動作的許可。

請求語法

```
PUT /2015-02-01/file-systems/FileSystemId/protection HTTP/1.1
Content-type: application/json

{
   "ReplicationOverwriteProtection": "string"
}
```

URI 請求參數

請求會使用下列 URI 參數。

FileSystemId

要更新的檔案系統 ID。

長度限制：長度上限為 128。

模式：^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$

必要：是

請求主體

請求接受採用 JSON 格式的下列資料。

ReplicationOverwriteProtection

檔案系統複寫覆寫保護的狀態。

- ENABLED：檔案系統不能在複寫組態中作爲目的地檔案系統。檔案系統可寫入。複寫覆寫保護預設為 ENABLED。
- DISABLED：檔案系統能在複寫組態中作爲目的地檔案系統。檔案系統為只讀，只可由 EFS 複寫修改。

- REPLICATING：檔案系統正在複寫組態中用作目的地檔案系統。檔案系統為只讀，只可由 EFS 複寫修改。

如果刪除複寫組態，則會重新啟用檔案系統的複寫覆寫保護，且檔案系統會變成可寫入。

類型：字串

有效值:ENABLED | DISABLED | REPLICATING

必要：否

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "ReplicationOverwriteProtection": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

ReplicationOverwriteProtection

檔案系統複寫覆寫保護的狀態。

- ENABLED：檔案系統不能在複寫組態中作爲目的地檔案系統。檔案系統可寫入。複寫覆寫保護預設為 ENABLED。
- DISABLED：檔案系統能在複寫組態中作爲目的地檔案系統。檔案系統為只讀，只可由 EFS 複寫修改。
- REPLICATING：檔案系統正在複寫組態中用作目的地檔案系統。檔案系統為只讀，只可由 EFS 複寫修改。

如果刪除複寫組態，那麼檔案系統的複寫覆寫保護會重新啓動，且檔案系統變為可寫入。

類型：字串

有效值:ENABLED | DISABLED | REPLICATING

錯誤

BadRequest

如果請求格式錯誤或包含錯誤，例如無效的參數值或缺少必要參數，則傳回。

HTTP 狀態碼：400

FileSystemNotFound

如果請求者中不存在指定的FileSystemId AWS 帳戶值，則返回。

HTTP 狀態碼：404

IncorrectFileSystemLifeCycleState

如果檔案系統的生命週期狀態不是「可用」，則傳回。

HTTP 狀態碼：409

InsufficientThroughputCapacity

如果沒有足夠容量佈建其他輸送量，則傳回。當您嘗試以佈建輸送量模式建立檔案系統、嘗試增加現有檔案系統的佈建輸送量，或嘗試將現有檔案系統從「爆增輸送量」變更為「佈建輸送量」模式時，系統可能會傳回此值。請稍後再試。

HTTP 狀態碼：503

InternalServerError

如果在伺服器端發生錯誤，則傳回。

HTTP 狀態碼：500

ReplicationAlreadyExists

如果檔案系統已包含在複製組態中，則傳回。>

HTTP 狀態碼：409

ThroughputLimitExceeded

如果因為已達到 1024 MB 的輸送量限制而無法變更輸送量模式或佈建輸送量總量，則傳回。

HTTP 狀態碼：400

TooManyRequests

如果您在變更輸送量模式或降低佈建輸送量值之前未等待至少 24 小時，則傳回。

HTTP 狀態碼：429

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

資料類型

目前支援下列資料類型：

- AccessPointDescription
- BackupPolicy
- CreationInfo
- Destination
- DestinationToCreate
- FileSystemDescription
- FileSystemProtectionDescription
- FileSystemSize
- LifecyclePolicy

- MountTargetDescription
- PosixUser
- ReplicationConfigurationDescription
- ResourceIdPreference
- RootDirectory
- Tag

AccessPointDescription

提供 EFS 檔案系統存取點說明。

目錄

AccessPointArn

與存取點關聯的唯一 Amazon Resource Name (ARN)。

類型：字串

長度限制：長度上限為 128。

模式：`^arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:access-point/fsap-[0-9a-f]{8,40}$`

必要：否

AccessPointId

由 Amazon EFS 指派的存取點 ID。

類型：字串

長度限制：長度上限為 128。

模式：`^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:access-point/fsap-[0-9a-f]{8,40}|fsap-[0-9a-f]{8,40})$`

必要：否

ClientToken

請求中指定的不透明字串，以確保等冪建立。

類型：字串

長度限制：長度下限為 1。長度上限為 64。

模式：`.+`

必要：否

FileSystemId

存取點套用至 EFS 檔案系統的 ID。

類型：字串

長度限制：長度上限為 128。

模式：`^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

必要：否

LifeCycleState

識別存取點的生命周期階段。

類型：字串

有效值:`creating | available | updating | deleting | deleted | error`

必要：否

Name

存取點的名稱。這是 `Name` 標籤的值。

類型：字串

必要：否

OwnerId

識別擁 AWS 帳戶 有存取點資源的。

類型：字串

長度限制：長度上限為 14。

模式：`^(\d{12})|(\d{4}-\d{4}-\d{4})$`

必要：否

PosixUser

完整的 POSIX 身分識別，包括存取點上的使用者 ID、群組 ID 和次要群組 ID，這些 ID 適用於 NFS 用戶端使用存取點的所有檔案作業。

類型：PosixUser 物件

必要：否

RootDirectory

存取點在 EFS 檔案系統上公開的目錄，作爲 NFS 用戶端通過該存取點訪問 EFS 檔案系統的根目錄。

類型：RootDirectory 物件

必要：否

Tags

與存取點相關聯的標籤，顯示為「標籤」物件的陣列。

類型：Tag 物件陣列

必要：否

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS SDK for C++
- AWS SDK for Java V2 的軟件
- AWS 適用於紅寶石 V3 的 SDK

BackupPolicy

用於建立每日自動備份的檔案系統的備份政策。如果狀態值為 ENABLED，表示正在自動備份檔案系統。如需詳細資訊，請參閱自動備份。

目錄

Status

描述檔案系統備份政策狀態。

- **ENABLED**：EFS 正在自動備份檔案系統。
- **ENABLING**：EFS 正在開啟檔案系統自動備份。
- **DISABLED**：關閉檔案系統自動備份。
- **DISABLING**：EFS 正在關閉檔案系統自動備份。

類型：字串

有效值:ENABLED | ENABLING | DISABLED | DISABLING

必要：是

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS SDK for C++
- AWS SDK for Java V2 的軟件
- AWS 適用於紅寶石 V3 的 SDK

CreationInfo

如果指定的 `RootDirectory > Path` 不存在，則需要此選項。指定要套用至存取點的 `RootDirectory > Path` 的 POSIX ID 和許可。如果存取點根目錄不存在，當用戶端連線到存取點時，EFS 會使用這些設定來建立它。指定 `CreationInfo` 時，您必須包含所有屬性的值。

只有在您已為目錄提供下 CreationInfo列項目 OwnUid、OwnGID 和許可時，Amazon EFS 才會建立根目錄。如果您未提供此資訊，則 Amazon EFS 不會建立根目錄。如果根目錄不存在，嘗試使用存取點掛載將會失敗。

> **Important**
>
> 如果您不提供 `CreationInfo` 且指定的 `RootDirectory` 不存在，則嘗試使用存取點掛載檔案系統將會失敗。

目錄

OwnerGid

指定要套用至 `RootDirectory` 的 POSIX 群組 ID。接受從 0 到 2^32 的值 (4294967295)。

類型：Long

有效範圍：最小值為 0。最大值為 4294967295。

必要：是

OwnerUid

指定要套用至 `RootDirectory` 的 POSIX 使用者 ID。接受從 0 到 2^32 的值 (4294967295)。

類型：Long

有效範圍：最小值為 0。最大值為 4294967295。

必要：是

Permissions

以表示檔案模式位元的八進位數字格式，指定要套用至 `RootDirectory` 的 POSIX 許可。

類型：字串

長度限制：長度下限為 3。長度上限為 4。

模式：^[0-7]{3,4}$

必要：是

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS SDK for C++
- AWS 適用於 Java V2 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

Destination

描述複寫組態中的目的地檔案系統。

目錄

FileSystemId

Amazon EFS 目的地檔案系統 ID。

類型：字串

長度限制：長度上限為 128。

模式：`^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

必要：是

Region

目標檔案系統所在的。 AWS 區域

類型：字串

長度限制：長度下限為 1。長度上限為 64。

模式：`^[a-z]{2}-((iso[a-z]{0,1}-)|(gov-)){0,1}[a-z]+-{0,1}[0-9]{0,1}$`

必要：是

Status

描述目的地 EFS 檔案系統狀態。

- 建立複寫組態之後，因為選擇退出來源或目標區域，系統會出現「暫停」(Paused) 狀態。若要繼續複寫檔案系統，您需要再次選擇加入 AWS 區域。如需詳細資訊，請參閱《 AWS 一般參考指南》 AWS 區域中的〈管理〉。
- 當來源檔案系統或目的檔案系統 (或兩者) 處於故障狀態且無法復原時，系統會顯示「錯誤」(`Error`) 狀態。如需詳細資訊，請參閱《Amazon EFS 使用者指南》中的監控複寫狀態。您必須刪除複寫組態，然後將故障檔案系統 (來源或目的地) 的最新備份還原至新檔案系統中。

類型：字串

有效值:ENABLED | ENABLING | DELETING | ERROR | PAUSED | PAUSING

必要：是

LastReplicatedTimestamp

在目的地檔案系統上順利完成最近一次同步的時間。在此之前，對來源檔案系統上的資料所做的任何變更都已經成功複寫到目的檔案系統中。在此之後，系統可能無法完全複寫發生的任何變更。

類型：Timestamp

必要：否

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS SDK for C++
- AWS SDK for Java V2 的軟件
- AWS 適用於紅寶石 V3 的 SDK

DestinationToCreate

描述複寫組態中的新或現有目的地檔案系統。

目錄

AvailabilityZoneName

若要建立使用單區域儲存的檔案系統，請指定要在其中建立目的地檔案系統的可用區域名稱。

類型：字串

長度限制：長度下限為 1。長度上限為 64。

模式：`.+`

必要：否

FileSystemId

作爲目的地使用的檔案系統 ID。檔案系統的複寫機制要求必須禁用複寫覆寫。如果您未提供 ID，那麼 EFS 會為複寫目的地建立新檔案系統。

類型：字串

長度限制：長度上限為 128。

模式：`^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

必要：否

KmsKeyId

指定您要用來加密目的地檔案系統的 AWS Key Management Service (AWS KMS) 金鑰。如果您並未指定 KMS 金鑰，那麼 Amazon EFS 會使用預設 KMS 金鑰 `/aws/elasticfilesystem` 為 Amazon EFS 的提供服務。此 ID 可以是下列其中一個格式：

- 金鑰 ID：金鑰的唯一識別碼，例如 `1234abcd-12ab-34cd-56ef-1234567890ab`。
- ARN：金鑰的 Amazon Resource Name (ARN)，例如 `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`。
- 金鑰別名 - 先前為金鑰建立的顯示名稱，例如 `alias/projectKey1`。

- 金鑰別名 ARN：金鑰別名的 ARN，例如 `arn:aws:kms:us-west-2:444455556666:alias/projectKey1`。

  類型：字串

  長度限制：長度上限為 2048。

  模式：`^([0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}|mrk-[0-9a-f]{32}|alias/[a-zA-Z0-9/_-]+|(arn:aws[-a-z]*:kms:[a-z0-9-]+:\d{12}:((key/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12})|(key/mrk-[0-9a-f]{32})|(alias/[a-zA-Z0-9/_-]+))))$`

  必要：否

Region

若要建立使用區域儲存區的檔案系統，請指定要 AWS 區域 在其中建立目的檔案系統。

類型：字串

長度限制：長度下限為 1。長度上限為 64。

模式：`^[a-z]{2}-((iso[a-z]{0,1}-)|(gov-)){0,1}[a-z]+-{0,1}[0-9]{0,1}$`

必要：否

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS SDK for C++
- AWS SDK for Java V2 的軟件
- AWS 適用於紅寶石 V3 的 SDK

FileSystemDescription

檔案系統描述。

目錄

CreationTime

建立檔案系統的時間，以秒為單位 (自 1970-01-01T00:00:00Z 以來)。

類型：Timestamp

必要：是

CreationToken

請求中指定的不透明字串。

類型：字串

長度限制：長度下限為 1。長度上限為 64。

模式：`.+`

必要：是

FileSystemId

由 Amazon EFS 指派的檔案系統 ID。

類型：字串

長度限制：長度上限為 128。

模式：`^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

必要：是

LifeCycleState

檔案系統的生命周期階段。

類型：字串

有效值:`creating | available | updating | deleting | deleted | error`

必要：是

NumberOfMountTargets

檔案系統目前擁有的掛載目標數。如需詳細資訊，請參閱 CreateMountTarget。

類型：整數

有效範圍：最小值為 0。

必要：是

OwnerId

建 AWS 帳戶 立檔案系統的。

類型：字串

長度限制：長度上限為 14。

模式：`^(\d{12})|(\d{4}-\d{4}-\d{4})$`

必要：是

PerformanceMode

檔案系統的效能模式。

類型：字串

有效值:`generalPurpose | maxIO`

必要：是

SizeInBytes

儲存在檔案系統、`Value` 欄位中的資料最新已知計量大小 (以位元組為單位)，以及在 `Timestamp` 欄位中決定該大小的時間。`Timestamp` 值是自 1970-01-01T00:00:00Z 以來的整數秒數。`SizeInBytes` 值不代表檔案系統的一致快照集大小，但是在沒有寫入檔案系統時，它最終會保持一致。也就是說，只有超過幾個小時未修改檔案系統，`SizeInBytes` 才能表示實際大小。否則，該值并不能代表檔案系統在任何時間點的確切大小。

類型：FileSystemSize 物件

必要：是

Tags

與檔案系統相關聯的標籤以 Tag 物件陣列形式呈現出來。

類型：Tag 物件陣列

必要：是

AvailabilityZoneId

檔案系統所在可用區域的唯一且一致的識別碼僅對單區域有效。例如，use1-az1是 us-east-1 的可用區域識別碼 AWS 區域，而且它在每個項目中都有相同的位置。 AWS 帳戶

類型：字串

必要：否

AvailabilityZoneName

描述檔案系統所在的 AWS 可用區域，且僅對單一區域檔案系統有效。如需詳細資訊，請參閱《Amazon EFS 使用者指南》中的使用 EFS 儲存類別。

類型：字串

長度限制：長度下限為 1。長度上限為 64。

模式：.+

必要：否

Encrypted

布林值，若為 true，指出加密檔案系統。

類型：布林值

必要：否

FileSystemArn

Amazon EFS 檔案系統的 Amazon Resource Name (ARN)，格式為 arn:aws:elasticfilesystem:*region*:*account-id*:file-system/*file-system-id*。示例資料範例：arn:aws:elasticfilesystem:us-west-2:1111333322228888:file-system/fs-01234567

類型：字串

必要：否

FileSystemProtection

說明檔案系統的防護。

類型：FileSystemProtectionDescription 物件

必要：否

KmsKeyId

AWS KMS key 用來保護加密檔案系統的識別碼。

類型：字串

長度限制：長度上限為 2048。

模式：`^([0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}|mrk-[0-9a-f]{32}|alias/[a-zA-Z0-9/_-]+|(arn:aws[-a-z]*:kms:[a-z0-9-]+:\d{12}:((key/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12})|(key/mrk-[0-9a-f]{32})|(alias/[a-zA-Z0-9/_-]+))))$`

必要：否

Name

您可以將標籤 (包括 Name 標籤) 新增至檔案系統。如需詳細資訊，請參閱 CreateFileSystem。如果檔案系統有 Name 標籤，Amazon EFS 會傳回此欄位中的值。

類型：字串

長度限制：長度上限為 256。

模式：`^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

必要：否

ProvisionedThroughputInMibps

檔案系統的佈建輸送量量 (以計量單位)。 MiBps對使用 ThroughputMode 設定為 provisioned 的檔案系統有效。

類型：Double

有效範圍：最小值為 1.0。

必要：否

ThroughputMode

顯示檔案系統的輸送量模式。如需詳細資訊，請參閱《Amazon EFS 使用者指南》中的輸送量模式。

類型：字串

有效值:`bursting | provisioned | elastic`

必要：否

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS SDK for C++
- AWS SDK for Java V2 的开发
- AWS 適用於紅寶石 V3 的 SDK

FileSystemProtectionDescription

說明檔案系統的防護。

目錄

ReplicationOverwriteProtection

檔案系統複寫覆寫保護的狀態。

- ENABLED：檔案系統不能在複寫組態中作爲目的地檔案系統。檔案系統可寫入。複寫覆寫保護預設為 ENABLED。
- DISABLED：檔案系統能在複寫組態中作爲目的地檔案系統。檔案系統為只讀，只可由 EFS 複寫修改。
- REPLICATING：檔案系統正在複寫組態中用作目的地檔案系統。檔案系統為只讀，只可由 EFS 複寫修改。

如果刪除複寫組態，那麼檔案系統的複寫覆寫保護會重新啓動，且檔案系統變為可寫入。

類型：字串

有效值:ENABLED | DISABLED | REPLICATING

必要：否

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS SDK for C++
- AWS SDK for Java V2 的軟件
- AWS 適用於紅寶石 V3 的 SDK

FileSystemSize

儲存在檔案系統、`Value` 欄位中的資料最新已知計量大小 (以位元組為單位)，以及在 `Timestamp` 欄位中決定該大小的時間。該值不代表檔案系統的一致快照集大小，但是在沒有寫入檔案系統時，它最終會保持一致。也就是說，只有超過幾個小時未修改檔案系統，該值才能表示實際大小。否則，并不需要用該值來代表檔案系統在任何時間點的確切大小。

目錄

Value

儲存在檔案系統中的資料的最新已知計量大小 (以位元組為單位)。

類型：Long

有效範圍：最小值為 0。

必要：是

Timestamp

在 `Value` 欄位中傳回的資料大小是在某個時間點確定的。 值是自 1970-01-01T00:00:00Z 以來的整數秒數。

類型：Timestamp

必要：否

ValueInArchive

儲存在「封存」儲存類別中的資料的最新已知計量大小 (以位元組為單位)。

類型：Long

有效範圍：最小值為 0。

必要：否

ValueInIA

儲存在 Infrequent Access 儲存類別中的資料的最新已知計量大小 (以位元組為單位)。

類型：Long

有效範圍：最小值為 0。

必要：否

ValueInStandard

儲存在「標準」儲存類別中的資料的最新已知計量大小 (以位元組為單位)。

類型：Long

有效範圍：最小值為 0。

必要：否

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS SDK for C++
- AWS SDK for Java V2 的軟件
- AWS 適用於紅寶石 V3 的 SDK

LifecyclePolicy

描述生命週期管理所使用的原則，該原則可指定何時將檔案轉移至儲存類別和移出儲存類別。如需詳細資訊，請參閱管理檔案系統儲存。

> **Note**
>
> 使用 `put-lifecycle-configuration` CLI 命令或 `PutLifecycleConfiguration` API 動作時，Amazon EFS 要求每個 `LifecyclePolicy` 物件只能有一次轉移。這意味著在請求內文中，`LifecyclePolicies` 必須結構化為 `LifecyclePolicy` 物件陣列，每次轉換對應一個物件。如需詳細資訊，請參閱 PutLifecycleConfiguration 中的請求範例。

目錄

TransitionToArchive

在主要儲存體 (標準儲存類別) 中最後一次存取檔案後的天數，以便將檔案移至封存儲存體。中繼資料操作 (例如列出目錄內容) 不計入為檔案存取事件。

類型：字串

有效值:`AFTER_1_DAY | AFTER_7_DAYS | AFTER_14_DAYS | AFTER_30_DAYS | AFTER_60_DAYS | AFTER_90_DAYS | AFTER_180_DAYS | AFTER_270_DAYS | AFTER_365_DAYS`

必要：否

TransitionToIA

檔案在最後一次存取后的一定天數內，如果位於主儲存(標準儲存類別)，則將其移動到 Infrequent Access (IA) 儲存中。中繼資料操作 (例如列出目錄內容) 不計入為檔案存取事件。

類型：字串

有效值:`AFTER_7_DAYS | AFTER_14_DAYS | AFTER_30_DAYS | AFTER_60_DAYS | AFTER_90_DAYS | AFTER_1_DAY | AFTER_180_DAYS | AFTER_270_DAYS | AFTER_365_DAYS`

必要：否

TransitionToPrimaryStorageClass

檔案儲存到 IA 或「封存」儲存中后，是否再移回主 (標準) 存儲。中繼資料操作 (例如列出目錄內容) 不計入為檔案存取事件。

類型：字串

有效值:AFTER_1_ACCESS

必要：否

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS SDK for C++
- AWS SDK for Java V2 的軟件
- AWS 適用於紅寶石 V3 的 SDK

MountTargetDescription

提供掛載目標說明。

目錄

FileSystemId

指定掛載目標所屬的檔案系統 ID。

類型：字串

長度限制：長度上限為 128。

模式：`^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

必要：是

LifeCycleState

掛載目標的生命週期狀態。

類型：字串

有效值:`creating | available | updating | deleting | deleted | error`

必要：是

MountTargetId

系統指定的掛載目標 ID。

類型：字串

長度限制：長度下限為 13。長度上限為 45。

模式：`^fsmt-[0-9a-f]{8,40}$`

必要：是

SubnetId

掛載目標子網路的 ID。

類型：字串

長度限制：長度下限為 15。長度上限為 47。

模式：^subnet-[0-9a-f]{8,40}$

必要：是

AvailabilityZoneId

掛載目標所在可用區域的唯一且一致的識別碼。例如，use1-az1是 us-east-1 區域的 AZ ID，且每個區域都有相同的位置。 AWS 帳戶

類型：字串

必要：否

AvailabilityZoneName

掛載目標所在可用區域名稱。可用區域會獨立對應至每個區域的名稱 AWS 帳戶。例如，您的 AWS 帳戶 可us-east-1a用區域可能與其他位置不同 AWS 帳戶。us-east-1a

類型：字串

長度限制：長度下限為 1。長度上限為 64。

模式：.+

必要：否

IpAddress

使用掛載目標掛載檔案系統的地址。

類型：字串

長度限制：長度下限為 7。長度上限為 15。

模式：^[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}$

必要：否

NetworkInterfaceId

Amazon EFS 建立掛載目標時建立的網路介面 ID。

類型：字串

必要：否

OwnerId

AWS 帳戶 擁有資源的 ID。

類型：字串

長度限制：長度上限為 14。

模式：`^(\d{12})|(\d{4}-\d{4}-\d{4})$`

必要：否

VpcId

掛載目標所在的虛擬私有雲端 (VPC)。

類型：字串

必要：否

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS SDK for C++
- AWS SDK for Java V2 的軟件
- AWS 適用於紅寶石 V3 的 SDK

PosixUser

存取點上的完整 POSIX 身分識別，包括使用者 ID、群組 ID 和任何次要群組 ID，該存取點用於 NFS 用戶端，系統會使用該存取點執行的所有檔案系統作業。

目錄

Gid

POSIX 群組 ID 會用於所有使用此存取點的檔案系統操作。

類型：Long

有效範圍：最小值為 0。最大值為 4294967295。

必要：是

Uid

使用此存取點的所有檔案系統作業所使用的 POSIX 使用者 ID。

類型：Long

有效範圍：最小值為 0。最大值為 4294967295。

必要：是

SecondaryGids

次要 POSIX 群組 ID 會用於所有使用此存取點的檔案系統操作。

類型：長整數陣列

陣列成員：項目數下限為 0。項目數上限為 16。

有效範圍：最小值為 0。最大值為 4294967295。

必要：否

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS SDK for C++

- AWS SDK for Java V2 的軟件
- AWS 適用於紅寶石 V3 的 SDK

ReplicationConfigurationDescription

描述特定檔案系統的複寫組態。

目錄

CreationTime

說明建立複寫組態的時間。

類型：Timestamp

必要：是

Destinations

目的地物件陣列。僅支援一個目的地物件。

類型：Destination 物件陣列

必要：是

OriginalSourceFileSystemArn

複寫組態中原始來源 EFS 檔案系統的 Amazon Resource Name (ARN)。

類型：字串

必要：是

SourceFileSystemArn

複寫組態中當前來源檔案系統的 Amazon Resource Name (ARN)。

類型：字串

必要：是

SourceFileSystemId

要複寫的來源 Amazon EFS 檔案系統 ID。

類型：字串

長度限制：長度上限為 128。

模式：^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$

必要：是

SourceFileSystemRegion

來源 EFS 檔案系統所 AWS 區域 在的位置。

類型：字串

長度限制：長度下限為 1。長度上限為 64。

模式：^[a-z]{2}-((iso[a-z]{0,1}-)|(gov-)){0,1}[a-z]+-{0,1}[0-9]{0,1}$

必要：是

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS SDK for C++
- AWS 適用於 Java V2 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

ResourceIdPreference

描述目前使用者的 AWS 帳戶資源類型及其 ID 偏好設定 AWS 區域。

目錄

ResourceIdType

識別 EFS 資源 ID 偏好設定，可以是 LONG_ID (17 個字元) 或 SHORT_ID (8 個字元) 類型的 ID。

類型：字串

有效值:LONG_ID | SHORT_ID

必要：否

Resources

ID 偏好設定將套用於同時具有 FILE_SYSTEM 和 MOUNT_TARGET 標識符的 Amazon EFS 資源。

類型：字串陣列

有效值:FILE_SYSTEM | MOUNT_TARGET

必要：否

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS SDK for C++
- AWS SDK for Java V2 的軟件
- AWS 適用於紅寶石 V3 的 SDK

RootDirectory

指定存取點提供存取權的 Amazon EFS 檔案系統上的目錄。存取點會將指定的檔案系統路徑作為檔案系統的根目錄，以公開給使用存取點的應用程式。使用存取點的 NFS 用戶端只能存取存取點RootDirectory及其子目錄中的資料。

目錄

CreationInfo

(選用) 指定要套用至存取點的 RootDirectory 的 POSIX 識別碼和權限。如果 RootDirectory > Path 指定不存在，EFS 會在用戶端連線到存取點時使用 CreationInfo 設定建立根目錄。指定時 CreationInfo，您必須提供所有屬性的值。

> **Important**
>
> 如果您未提供 CreationInfo 且指定的 RootDirectory > Path 不存在，則嘗試使用存取點掛載檔案系統將會失敗。

類型：CreationInfo 物件

必要：否

Path

指定 EFS 檔案系統上的路徑，要公開為 NFS 用戶端使用存取點存取 EFS 檔案系統的根目錄。一個路徑最多可以有四個子目錄。如果指定的路徑不存在，您必須提供 CreationInfo.

類型：字串

長度限制：長度下限為 1。長度上限為 100。

模式：^(\/|(\/(?!\.)+[^$#<>;`|&?{}^*/\n]+){1,4})$

必要：否

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS SDK for C++
- AWS 適用於 Java V2 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

Tag

標籤是索引鍵值組。系統允許的字元包括字母、空格和可以用 UTF-8 表示的數字，以及下列字元： + - = . _ : /。

目錄

Key

標籤鍵 (字串)。索引鍵無法以 aws: 開頭。

類型：字串

長度限制：長度下限為 1。長度上限為 128。

模式：^(?![aA]{1}[wW]{1}[sS]{1}:)([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$

必要：是

Value

標籤金鑰的值。

類型：字串

長度限制：長度上限為 256。

模式：^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$

必要：是

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS SDK for C++
- AWS SDK for Java V2 的軟件
- AWS 適用於紅寶石 V3 的 SDK

文件歷史紀錄

- API 版本：2015-02-01
- 最新文件更新：2024 年 5 月 15 日

下表說明 2018 年 7 月之後《Amazon Elastic File System 使用者指南》的重要變更內容。如需有關文件更新的通知，您可以訂閱 RSS 摘要。

變更	描述	日期
增加裝載目標的配額	每個虛擬私有雲 (VPC) 的裝載目標數目上限從 400 個增加到 1,400 個。如需詳細資訊，請參閱無法變更的 Amazon EFS 資源配額。	2024年5月15日
增加彈性檔案系統的合併輸送量限制	對於使用彈性輸送量的檔案系統，且使用 Amazon EFS 用戶端 (版本) 或 Amazon EFS CSI 驅動程式 (aws-efs-csi 驅動程式) 的 2.0 版或更新amazon-efs-utils 版本進行裝載的檔案系統，最大合併讀取和寫入輸送量 MiBps 為 1,500。如需詳細資訊，請參閱 Amazon EFS 效能中的效能摘要表。	2024 年 4 月 30 日
彈性輸送量限制增加	特定的彈性輸送量限制已增加 AWS 區域。如需詳細資訊，請參閱每個用戶端中所有連線用戶端的總預設彈性輸送量 AWS 區域。	2024年3月13日
提高的 IOPS	使用彈性輸送量的檔案系統最多可以為不常存取的資料驅動	2024年1月22日

	90,000 次讀取。如需詳細資訊，請參閱效能摘要。	
更新現有的 AWS 受管策略	已新elasticfilesystem:UpdateFileSystemProtection 增至現有 AmazonElasticFileSystemFullAccess 原則的權限，以允許主體更新檔案系統上的防護。如需詳細資訊，請參閱 Amazon EFS 更新 AWS 受管政策。	2023 年 11 月 27 日
複製到現有檔案系統	檔案系統現在可以複製到現有的檔案系統，讓檔案系統之間的變更進行同步化，以便於容錯恢復之用。如需詳細資訊，請參閱目標檔案系統。	2023 年 11 月 27 日
新增的檔案系統保護	複寫覆寫保護已新增至檔案系統，預設為啟用。此保護可防止檔案系統用作複寫組態中的目的地。如需詳細資訊，請參閱停止保護。	2023 年 11 月 27 日
新的儲存類別、檔案系統類型和生命週期政策	Amazon EFS 現在提供 EFS 存檔儲存類別、檔案系統類型和轉換到存檔生命週期政策。如需儲存類別的詳細資訊，請參閱和。	2023 年 11 月 26 日
提高的 IOPS	針對不常存取的資料，彈性輸送量檔案系統現在支援最多 65,000 個讀取和 50,000 個寫入作業 IOPS，現在也支援 250,000 個讀取 IOPS 來處理經常存取的資料。如需詳細資訊，請參閱效能摘要。	2023 年 11 月 26 日

從來源檔案系統刪除複製組態	現在可以從來源檔案系統中刪除複製組態。如需詳細資訊，請參閱刪除複寫設定。	2023 年 9 月 19 日
添加了其他 AWS 區域 支持	Amazon EFS 現已向以色列 (特拉維夫) 區域的所有使用者提供。	2023 年 8 月 7 日
提高一般用途模式檔案系統的效能	Amazon EFS 一般用途模式檔案系統現在支援每秒最多 55,000 個讀取操作和 25,000 個寫入操作。如需詳細資訊，請參閱 Amazon EFS 檔案系統的配額。	2023 年 8 月 3 日
佈建輸送量限制增加	針對特定的佈建輸送量限制已增加 AWS 區域。如需詳細資訊，請參閱各自中所有連線用戶端的預設佈建輸送量總計 AWS 區域。	2023 年 6 月 21 日
EFS 複寫的擴充區域支援	EFS 複寫現在可 AWS 區域 在所有可用 EFS 中使用。如需詳細資訊，請參閱 Amazon EFS 限制。	2023 年 4 月 28 日
彈性輸送量限制增加	特定的彈性輸送量限制已增加 AWS 區域。如需詳細資訊，請參閱每個表格中所有連線用戶端的總預設彈性輸送量 AWS 區域。	2023 年 4 月 17 日
彈性會取代成組分解作為預設輸送量模式	檔案系統的預設 (和建議) 輸送量模式現在是「彈性」，而不是「大量批次設定」。如需更多詳細資訊，請參閱輸送量模式。	2023 年 4 月 13 日

添加了其他 AWS 區域 支持	Amazon EFS 現已向亞太區域 (墨爾本) 的所有使用者提供。	2023 年 4 月 12 日
新增對 macOS Ventura 的支援。	Amazon EFS 現在可以安裝於 macOS Ventura 上運行的 EC2 Mac 執行個體上。如需詳細資訊，請參閱支援的發行版。	2023 年 4 月 10 日
添加了其他 AWS 區域 支持	Amazon EFS 現已向亞太區域 (海德拉巴) 的所有使用者提供。	2023 年 2 月 16 日
添加了其他 AWS 區域 支持	Amazon EFS 現已向歐洲 (西班牙) AWS 區域的所有使用者提供。	2023 年 1 月 19 日
檔案系統的存取點限制已增加	單一檔案系統可以擁有的最大存取點數從 120 個增加到 1,000 個。如需詳細資訊，請參閱資源配額。	2023 年 1 月 17 日
添加了其他 AWS 區域 支持	Amazon EFS 現在可供歐洲 (蘇黎世) 的所有使用者使用 AWS 區域。	2022 年 12 月 15 日
新增一天生命週期政策的支援	您現在可以為「轉換成 IA」生命週期政策選取一天。如需詳細資訊，請參閱生命週期政策。	2022 年 11 月 27 日
減少讀取和寫入延遲	單區儲存和標準儲存檔案系統的檔案資料讀取和寫入延遲都減少了。如需詳細資訊，請參閱效能摘要。	2022 年 11 月 27 日

新增的其他輸送量模式	彈性輸送量模式會新增為 Amazon EFS 檔案系統的輸送量選項。如需詳細資訊，請參閱彈性輸送量。	2022 年 11 月 27 日
添加了其他 AWS 區域 支持	Amazon EFS 現已向中東 (阿拉伯聯合大公國) 區域的所有使用者提供。	2022 年 10 月 17 日
新增對 EFS 複寫的支援	Amazon EFS 已移除先前 EFS 複寫不支援通訊端和具名管道或 FIFO 的限制。	2022 年 9 月 15 日
每個連接的文件鎖定數量限制已增加	每個連線的檔案鎖定數目已從 8192 增加到 65,536 個。如需詳細資訊，請參閱 NFS 用戶端的配額。	2022 年 5 月 4 日
使用檔案鎖定移除的程序限制	Amazon EFS 已移除先前的限制，其中單一執行個體上最多 256 個程序可以同時使用檔案鎖定。如需詳細資訊，請參閱 NFS 用戶端的配額。	2022 年 5 月 4 日
添加了其他 AWS 區域 支持	Amazon EFS 現已向亞太區域 (雅加達) AWS 區域的所有使用者提供。	2022 年 1 月 27 日
新增對 EFS 複寫的支援	使用 EFS 複寫將 EFS 檔案系統上的資料和中繼資料複製到您選擇 AWS 區域 的其他 EFS 檔案系統。如需詳細資訊，請參閱 Amazon EFS 複寫。	2022 年 1 月 25 日
檔案系統和掛載目標資源使用 17 個字元的資源 ID 格式	新的 Amazon EFS 檔案系統和掛載目標資源現在會指派 17 個字元的 ID。如需詳細資訊，請參閱使用 Amazon EFS 資源。	2021 年 10 月 22 日

新增對 EFS 智慧型分層的支援	EFS 智慧型分層使用 EFS 生命週期管理來監控檔案存取模式，其設計用來自動在對應的 Infrequent Access (IA) 儲存類別之間轉換檔案。如需詳細資訊，請參閱 EFS 智慧型分層和生命週期管理。	2021 年 9 月 2 日
新增對測試 17 個字元資源 ID 格式的支援	Amazon EFS 將於 2021 年 10 月 1 日從針對檔案系統使用 8 個字元的 ID 轉換為 17 個字元的 ID，並掛載目標。在此轉換期間，您可以選擇加入並開始每次 AWS 區域 使用 17 個字元的資源 ID。如需詳細資訊，請參閱 資源 ID。	2021 年 5 月 5 日
新增對使用 Amazon EFS 掛載協助程式從不同可用區域掛載單區域檔案系統的支援	您現在可以使用 EFS 掛載協助程式，將使用單區域儲存類別的 Amazon EFS 檔案系統掛載到位於不同可用區域的 EC2 執行個體。您可以使用新 az 選項來指定 Amazon EFS 檔案系統的可用區域。如需詳細資訊，請參閱使用單區域儲存類別掛載檔案系統。	2021 年 4 月 6 日
新增對 EFS 單區域儲存類別的支援	Amazon EFS 單區域儲存類別會將資料冗餘存放在 AWS 區域中的單一可用區域內。EFS 單區域和一區域不常存取 (單區域 — IA) 儲存類別是儲存資料的成本效益選項，不需要 EFS 標準和標準 — IA 儲存類別的異地同步備份復原能力。如需詳細資訊，請參閱 EFS 儲存類別。	2021 年 3 月 9 日

添加了其他 AWS 區域 支持	Amazon EFS 現已向亞太區域 (大阪) 的所有使用者提供。	2021 年 3 月 3 日
新增對執行 macOS Big Sur 的 Amazon EC2 macOS 執行個體的支援	您現在可以使用 EFS 掛載協助程式或使用 NFS 掛載命令，從執行 macOS Big Sur 的 EC2 macOS 執行個體掛載您的 Amazon EFS 檔案系統。如需詳細資訊，請參閱使用 EFS 掛載協助程式進行掛載或不使用 EFS 掛載協助程式掛載檔案系統。	2021 年 2 月 23 日
新的 Amazon EFS 主控台可在 AWS GovCloud (US) 區域使用	新的 Amazon EFS 主控台現在可在中使用 AWS GovCloud (US) AWS 區域。	2021 年 2 月 10 日
為新的 Amazon EFS CloudWatch 指標添加了 Support `MeteredIOBytes`	您可以使用 `MeteredIOBytes` 衡量每個檔案系統操作的位元組數，包括資料讀取、資料寫入及中繼資料操作。讀取操作的計量速率是其他操作速率的三分之一。如需詳細資訊，請參閱 Amazon EFS 的 Amazon CloudWatch 指標。	2021 年 1 月 28 日
Amazon EFS 將檔案系統讀取輸送量提高 300%	Amazon EFS 檔案系統現在會以其他請求率的三分之一計量讀取請求。	2021 年 1 月 28 日

為新的 Amazon EFS CloudWatch 指標添加了 Support `StorageBytes`	您可以使用 `StorageBytes` 以位元組為單位來測量和監視檔案系統的大小，包括儲存在標準和 Infrequent Access 儲存類別中的資料量。如需詳細資訊，請參閱 Amazon EFS 的 Amazon CloudWatch 指標。	2021 年 1 月 11 日
用 AWS Transfer Family 於存取 Amazon EFS 檔案系統	您可以使 AWS Transfer Family 用將檔案傳入和傳出 Amazon EFS 檔案系統。如需詳細資訊，請參閱使用 AWS Transfer Family 來存取 EFS 檔案系統中的檔案。	2021 年 1 月 6 日
用 AWS Systems Manager 於管理 Amazon EFS 客戶端 (`amazon-efs-utils`)	您可以使 AWS Systems Manager 用在 EC2 執行個體上自動安裝或更新 Amazon EFS 用戶端 (`amazon-efs-utils`)。如需詳細資訊，請參閱使用 AWS Systems Manager 自動安裝或更新 Amazon EFS 用戶端。	2020 年 9 月 29 日
強制建立加密的 EFS 檔案系統	您可以使用 `elasticfilesystem:Encrypted` AWS Identity and Access Management (IAM) 條件金鑰強制使用者建立靜態加密的 Amazon EFS 檔案系統。如需詳細資訊，請參閱逐步解說：在 Amazon EFS 檔案系統上強制執行靜態加密。	2020 年 9 月 16 日

每個用戶端的 Amazon EFS 輸送量增加 100%	EFS 現在支援每個用戶端輸送量高達 500 MB/s，比之前的 250 MB/s 上限增加 100%。如需詳細資訊，請參閱 Amazon EFS 檔案系統的配額。	2020 年 7 月 23 日
新增對 Amazon EFS 檔案系統自動每日備份的支援	使用 EFS 主控台建立檔案系統時，現在預設會啟用自動每日備份。如需詳細資訊，請參閱AWS Backup 搭配 Amazon EFS 使用。	2020 年 7 月 16 日
全新的快速建立工作流程可簡化 Amazon EFS 檔案系統	使用 EFS 主控台中的「快速建立」選項，您可以透過單一按鈕使用服務建議設定來建立 EFS 檔案系統。如需詳細資訊，請參閱 CreateyYour Amazon EFS 檔案系統。	2020 年 7 月 16日
Amazon EFS 主控台現已推出	新的 EFS 主控台可讓您更輕鬆地使用 Amazon EFS，並簡化 EFS 檔案系統的管理。	2020 年 7 月 16 日
Amazon EFS 提高檔案系統最小輸送量	使用爆量輸送量的 Amazon EFS 檔案系統現在具有 1 Mb/s 的最低輸送量。如需更多詳細資訊，請參閱輸送量模式。	2020 年 6 月 30 日
一般用途模式檔案系統的效能提升	一般用途模式檔案系統現在支援每秒高達 35,000 次讀取操作，比先前的 7,000 次限制增加 400%。如需詳細資訊，請參閱 Amazon EFS 檔案系統的配額。	2020 年 4 月 1 日
添加了其他 AWS 區域 支持	Amazon EFS 現在可供北京和寧夏 AWS 區域的所有使用者使用。	2020 年 1 月 22 日

新增對 NFS 用戶端 IAM 授權的支援	您現在可以使用 AWS Identity and Access Management (IAM) 來管理對 Amazon EFS 檔案系統的 NFS 存取。如需詳細資訊，請參閱使用 AWS IAM 控制對 Amazon EFS 的 NFS 存取。	2020 年 1 月 13 日
新增對 EFS 存取點的支援	Amazon EFS 存取點是應用程式特定的 EFS 檔案系統進入點，此進入點可讓您更輕鬆地管理共用資料集的應用程式存取。如需詳細資訊，請參閱使用 Amazon EFS 存取點。	2020 年 1 月 13 日
增加了對 AWS Backup 部分還原的 Support。	除了還原完整復原點之外，您現在可以使用部分還原來還原特定檔案和目錄。如需詳細資訊，請參閱AWS Backup 搭配 Amazon EFS 使用。	2020 年 1 月 13 日
新增對 IAM 服務連結角色的支援	Amazon EFS 現在會使用根據 IAM 的服務連結角色，讓您透過自動新增必要權限以更輕鬆地設定 EFS。如需詳細資訊，請參閱為 Amazon EFS 使用服務相關角色。	2019 年 12 月 10 日
添加了其他 AWS 區域 支持	Amazon EFS 現在可供歐洲 (斯德哥爾摩) 的所有使用者使用 AWS 區域。	2019 年 11 月 20 日
添加了其他 AWS 區域 支持	亞太區域 (香港) 的所有使用者現在都可以使用 Amazon EFS AWS 區域。	2019 年 11 月 20 日

添加了其他 AWS 區域 支持	Amazon EFS 現在可供南美洲 (聖保羅) 的所有使用者使用 AWS 區域。	2019 年 11 月 20 日
添加了其他 AWS 區域 支持	Amazon EFS 現在可供中東 (巴林) 的所有使用者使用 AWS 區域。	2019 年 11 月 20 日
已新增 7 天生命週期管理政策	生命週期管理現在有附加政策，可在 7 天後將資料移至具成本效益且不常存取的儲存類別。如需詳細資訊，請參閱 EFS 生命週期管理。	2019 年 11 月 6 日
新增對介面 VPC 端點的支援	您可以在 Virtual Private Cloud 和 Amazon EFS 之間建立私有連線以呼叫 EFS API。如需詳細資訊，請參閱使用 VPC 端點。	2019 年 10 月 22 日
啟動新的 EC2 執行個體時，掛載 EFS 檔案系統。	您現在可以設定新的 Amazon EC2 執行個體，並於啟動時，在 EC2 啟動執行個體精靈中掛載 EFS 檔案系統。如需詳細資訊，請參閱步驟 2。建立 EC2 資源和啟動 EC2 執行個體。	2019 年 10 月 17 日
新增對 Service Quotas 支援	您現在可以在 Service Quotas 主控台中檢視所有 Amazon EFS 的限制。如需詳細資訊，請參閱 Amazon EFS 限制。	2019 年 9 月 10 日

已新增新的生命週期管理政策	當使用「生命週期管理」時，您現在可以從四個生命週期政策當中選擇其中之一，以定義檔案何時轉換成經濟實惠的不常存取儲存類別。如需詳細資訊，請參閱 EFS 生命週期管理。	2019 年 7 月 9 日
EFS 生命週期管理現在適用於所有 EFS 檔案系統。	EFS 生命週期管理功能現在適用於所有 EFS 檔案系統。根據檔案系統建立日期的舊有限制現在已移除。如需詳細資訊，請參閱 EFS 生命週期管理。	2019 年 7 月 9 日
添加了其他 AWS 區域 支持	Amazon EFS 現在可供歐洲 (巴黎) 的所有使用者使用 AWS 區域。	2019 年 6 月 12 日
添加了其他 AWS 區域 支持	Amazon EFS 現在可供亞太區域 (孟買) 的所有使用者使用 AWS 區域。	2019 年 6 月 5 日
添加了其他 AWS 區域 支持	Amazon EFS 現在可供加拿大 (中部) 的所有使用者使用 AWS 區域。	2019 年 5 月 1 日
API 更新：標籤現在是 CreateFileSystem 操作有效負載的一部分	您現在可以在使用 AWS API 和 CLI CreateFileSystem 作業建立 Amazon EFS 檔案系統時包含標籤。如需詳細資訊，請參閱CreateFile系統和使用 AWS CLI 建立檔案系統。	2019 年 2 月 19 日

新功能：EFS Infrequent Access 的儲存類別和 EFS 生命週期管理	Amazon EFS Infrequent Access 的儲存類別是不常存取檔案適用的最佳成本儲存類別。EFS 生命週期管理會自動將檔案從標準轉換到不常存取的儲存。如需詳細資訊，請參閱 EFS 儲存類別。	2019 年 2 月 13 日
添加了其他 AWS 區域 支持	Amazon EFS 現在可供歐洲 (倫敦) 的所有使用者使用 AWS 區域。	2019 年 1 月 23 日
AWS Backup 與 Amazon EFS 的服務整合	Amazon EFS 檔案系統可以使用完全受管 AWS Backup、集中、自動化的備份服務進行備份，以備份雲端和內部部署 AWS 服務之間的資料。如需詳細資訊，請參閱 AWS Backup 和 Amazon EFS。	2019 年 1 月 16 日
新增傳輸閘道連線對內部部署儲存系統的支援。	您現可在內部部署儲存系統上，使用傳輸閘道連線存取 Amazon EFS 檔案系統。如需詳細資訊，請參閱從其他的帳戶或 VPC 進行掛載和逐步解說：掛載來自不同 VPC 的檔案系統。	2018 年 12 月 6 日
EFS 檔案同步現在已成為新 AWS DataSync 服務的一部分。	AWS DataSync 是一項受管資料傳輸服務，可簡化內部部署儲存系統與 AWS 儲存服務之間的大量資料同步處理作業。如需詳細資訊，請參閱使用將檔案從現場部署檔案系統傳輸到 Amazon EFS AWS DataSync。	2018 年 11 月 26 日

新增 VPN 及區域間 VPC 對等互連	Amazon EFS 現在可透過 VPN 連接及區域間 VPC 對等互連進行存取。如需詳細資訊，請參閱使用將檔案從現場部署檔案系統傳輸到 Amazon EFS AWS DataSync。	2018 年 10 月 23 日
新增 VPN 及區域間 VPC 對等互連	您現可透過 VPN 連接及區域間 VPC 對等互連存取 Amazon EFS 檔案系統。如需詳細資訊，請參閱從其他的帳戶或 VPC 進行掛載和 Amazon EFS 如何與 Direct Connect 和 VPN 協同運作。	2018 年 10 月 23 日
添加了其他 AWS 區域 支持	Amazon EFS 現已向亞太區域 (新加坡) AWS 區域的所有使用者提供。	2018 年 7 月 13 日
佈建的輸送量模式簡介	您現在可以用新的佈建輸送容量模式，為新的或現有的檔案系統佈建輸送容量。如需更多詳細資訊，請參閱輸送量模式。	2018 年 7 月 12 日
添加了其他 AWS 區域 支持	Amazon EFS 現已向亞太區域 (東京) AWS 區域的所有使用者提供。	2018 年 7 月 11 日

下表說明 2018 年 7 月前《Amazon Elastic File System 使用者指南》的重要變更。

變更	描述	變更日期
添加了其他 AWS 區域 支持	Amazon EFS 現已向亞太區域 (首爾) AWS 的所有使用者提供。	2018 年 5 月 30 日

變更	描述	變更日期
新增 CloudWatch 公制數學支援	Metric math 可讓您查詢多個 CloudWatch 量度，並使用數學運算式根據這些量度建立新的時間序列。如需詳細資訊，請參閱 使用 Amazon EFS 指標數學。	2018 年 4 月 4 日
已新增 amazon-efs-utils 開放原始碼工具組，並已新增傳輸中加密	amazon-efs-utils 工具是一組開放原始碼可執行檔案，可簡化 Amazon EFS 的使用，例如掛載。無需額外費用即可使用amazon-efs-utils ，您可以從中下載這些工具 GitHub。如需詳細資訊，請參閱 安裝 Amazon EFS 工具。 此外，在此版本中，Amazon EFS 現在透過 Transport Layer Security (TLS) 通道支援傳輸中加密。如需詳細資訊，請參閱 Amazon EFS 的資料加密。	2018 年 4 月 4 日
更新的文件系統限制 AWS 區域	Amazon EFS 在所有 AWS 區域的所有帳戶中，增加了檔案系統數量的限制。如需詳細資訊，請參閱 無法變更的 Amazon EFS 資源配額。	2018 年 3 月 15 日
添加了其他 AWS 區域 支持	Amazon EFS 現在可供美國西部 (加利佛尼亞北部) 的所有使用者使用 AWS 區域。	2018 年 3 月 14 日
靜態資料加密	Amazon EFS 現在支援靜態資料加密。如需詳細資訊，請參閱 Amazon EFS 的資料加密。	2017 年 8 月 14 日
新增其他區域支援	Amazon EFS 現已向歐洲 (法蘭克福) 區域的所有使用者提供。	2017 年 7 月 20 日
使用網域名稱系統 (DNS) 的檔案系統名稱	Amazon EFS 現在支援檔案系統的 DNS 名稱。在用於連接 Amazon EC2 執行個體的可用區域中，檔案系統的 DNS 名稱會自動解析為掛載目標的 IP 地址。如需詳細資訊，請參閱 以 DNS 名稱掛載於 Amazon EC2。	2016 年 12 月 20 日
增加檔案系統的標籤支援	Amazon EFS 現在每個檔案系統支援 50 個標籤。如需 Amazon EFS 中的標籤的詳細資訊，請參閱 標記 Amazon EFS 資源。	2016 年 8 月 29 日

變更	描述	變更日期
一般可用性	Amazon EFS 现已在美國東部 (維吉尼亞北部)、美國西部 (奧勒岡) 及歐洲 (愛爾蘭) 區域全面發行。	2016 年 6 月 28 日
檔案系統限制提高	每個 AWS 區域 區域、每個帳戶可建立的 Amazon EFS 檔案系統數量從 5 個提高到 10 個。	2015 年 8 月 21 日
更新入門練習	入門練習已更新，簡化了入門程序。	2015 年 8 月 17 日
新指南	這是 Amazon Elastic File System 使用者指南的第一版。	2015 年 5 月 26 日

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。