AWS 白皮書

使用 Amazon Elastic File System 加密檔案資料

使用 Amazon Elastic File System 加密檔案資料: AWS 白皮書

Table of Contents

使用 Amazon Elastic File System 加密檔案資料

出版日期：2021 年 2 月 22 日 (文件歷史記錄與貢獻者)

摘要

安全對 AWS 來說是首要任務，我們為客戶提供了將安全作為其企業首要任務的工具。政府法規與產業或公司合規性政策，可能需要藉由使用加密政策、密碼編譯演算法與適當的金鑰管理，來保護不同機密等級的資料。此白皮書概述加密 Amazon Elastic File System (Amazon EFS) 的最佳實務。

簡介

Amazon Elastic File System (Amazon EFS) 在雲端中提供簡單且可調整規模，同時又有高可用性與耐久性的共享檔案系統。使用 Amazon EFS 所建立的檔案系統具有彈性，可讓該檔案系統在新增及刪除資料時，自動放大及縮小。其大小可放大到 PB，從而可在多個可用區域 (AZ) 中數目不受限制的存放區伺服器上散發資料。

使用 Amazon EFS 可為儲存於這些檔案系統中之靜態資料與傳輸中資料進行加密。針對靜態資料加密，您可以透過 AWS 管理主控台或 AWS Command Line Interface (AWS CLI)，建立加密的檔案系統。或者，您也可以透過 Amazon EFS API 或其中一個 AWS 開發套件，以程式設計方式建立加密的檔案系統。

針對靜態資料加密，Amazon EFS 會與 AWS Key Management Service (AWS KMS) 相整合，進行金鑰管理。您也可以掛載檔案系統，並透過傳輸層安全性 (TLS) 傳輸所有 NFS 流量，藉此啟用傳輸中資料的加密。

此白皮書概述了 Amazon EFS 的加密最佳實務。其描述如何在用戶端連線層啟用傳輸中資料的加密，以及如何在 AWS 管理主控台與 AWS CLI 中建立加密的檔案系統。

> **Note**
>
> 使用 API 與開發套件建立加密檔案系統，不在此白皮書的範圍內。如需如何完成此動作的詳細資訊，請參閱《Amazon EFS 使用者指南》或開發套件文件中的 Amazon EFS API。

基本概念與術語

本節定義此白皮書中參考的概念與術語。

- Amazon Elastic File System (Amazon EFS) – 具有高可用性與耐用性的服務，可以在 AWS 雲端中提供簡單、可擴展的共享檔案儲存體。Amazon EFS 提供標準的檔案系統界面與檔案系統語意。您可以在多個可用區域中數目不受限制的存放區伺服器上，儲存幾乎無限量的資料。
- AWS Identity and Access Management (IAM) – 這項服務可讓您安全地控制 AWS 服務 API 的細微存取權。建立原則並將其用於限制個別使用者、群組與角色的存取權。您可以通過 IAM 主控台管理您的 AWS KMS 金鑰。
- AWS KMS – 受控服務，可讓您輕鬆地建立及控制客戶主金鑰 (CMK)，其為用於加密資料的加密金鑰。AWS KMS CMK 是由 FIPS 140-2 Cryptographic Module Validation Program 驗證的硬體安全模組 (HSM) 所保護，但中國 (北京) 與中國 (寧夏) 區域除外。AWS KMS 會與其他為您資料加密的 AWS 服務整合。其也會與 AWS CloudTrail 完全整合，以提供 AWS KMS 代表您所進行的 API 呼叫記錄，這有助於滿足適用於您組織的合規或法規要求。
- 客戶主金鑰 (CMK) – 代表金鑰階層的頂端。其包含用於為資料加密及解密的金鑰材料。AWS KMS 可產生此金鑰材料；也可由您產生金鑰材料後，將其匯入 AWS KMS。CMK 專門用於 AWS 帳戶與 AWS 區域，可由客戶或 AWS 進行管理。
- AWS 管理的 CMK – 由 AWS 代表您所產生的 CMK。當您為整合式 AWS 服務的資源啟用加密時，就會建立 AWS 管理的 CMK。AWS 管理的 CMK 金鑰原則會由 AWS 管理，而且您無法加以變更。建立或儲存 AWS 管理的 CMK 不需付費。
- 客戶管理的 CMK – 您使用 AWS 管理主控台、API、AWS CLI 或軟體開發套件所建立的 CMK。當您需要對 CMK 進行更細微的控制時，可以使用客戶管理的 CMK。
- KMS 金鑰原則 – 資源原則，可控制客戶管理之 CMK 的存取權。客戶會使用金鑰原則或 IAM 原則與金鑰原則的組合，定義這些許可。如需詳細資訊，請參閱《AWS KMS 開發人員指南》中的管理存取權概觀。
- 資料金鑰 – 由 AWS KMS 所產生的密碼編譯金鑰，用於為 AWS KMS 外部的資料加密。AWS KMS 可讓授權實體 (使用者或服務) 取得受 CMK 保護的資料金鑰。
- Transport Layer Security (TLS) – TLS 是 Secure Sockets Layer (SSL) 的新一代技術，是透過網路交換的資訊加密所需的密碼編譯協定。
- EFS 裝載協助程式 – Linux 用戶端代理程式 (`amazon-efs-utils`)，用於簡化 EFS 檔案系統裝載。其可用於透過 TLS 通道設定、維護及路由所有 NFS 流量。

如需基本概念與術語的相關詳細資訊，請參閱《AWS KMS 開發人員指南》中的 AWS 金鑰管理服務概念。

靜態資料加密

AWS 提供有建立加密檔案系統的工具，您可使用業界標準的 AES-256 加密演算法，加密所有靜態資料與中繼資料。加密檔案系統的設計訴求，是自動且透明地處理加密與解密，您完全無須修改您的應用程序。若您的組織受到需要靜態資料與中繼資料加密之公司或法規政策的限制，建議您建立加密檔案系統。

主題

管理金鑰

Amazon EFS 可與 AWS KMS 相整合，管理加密檔案系統的加密金鑰。AWS KMS 也支援其他 AWS 服務的加密，例如：Amazon Simple Storage Service (Amazon S3)、Amazon Elastic Block Store (Amazon EBS)、Amazon Relational Database Service (Amazon RDS)、Amazon Aurora、Amazon Redshift、Amazon WorkMail、WorkSpaces 等。對加密檔案系統內容來說，Amazon EFS 會使用具有 XTS 模式與 256 位元金鑰 (XTS-AES-256) 的進階加密標準演算法。

考慮如何藉由採用所有加密政策來保護靜態資料時，要回答三個重要的問題。這些問題對於儲存於受管與非受管的服務 (如 Amazon EBS) 中的資料都同樣有效。

金鑰儲存在哪裡？

AWS KMS 會以加密的格式將您的主金鑰儲存於具有高耐用性的儲存體中，以協助確保需要時即可擷取。

哪裡會使用金鑰？

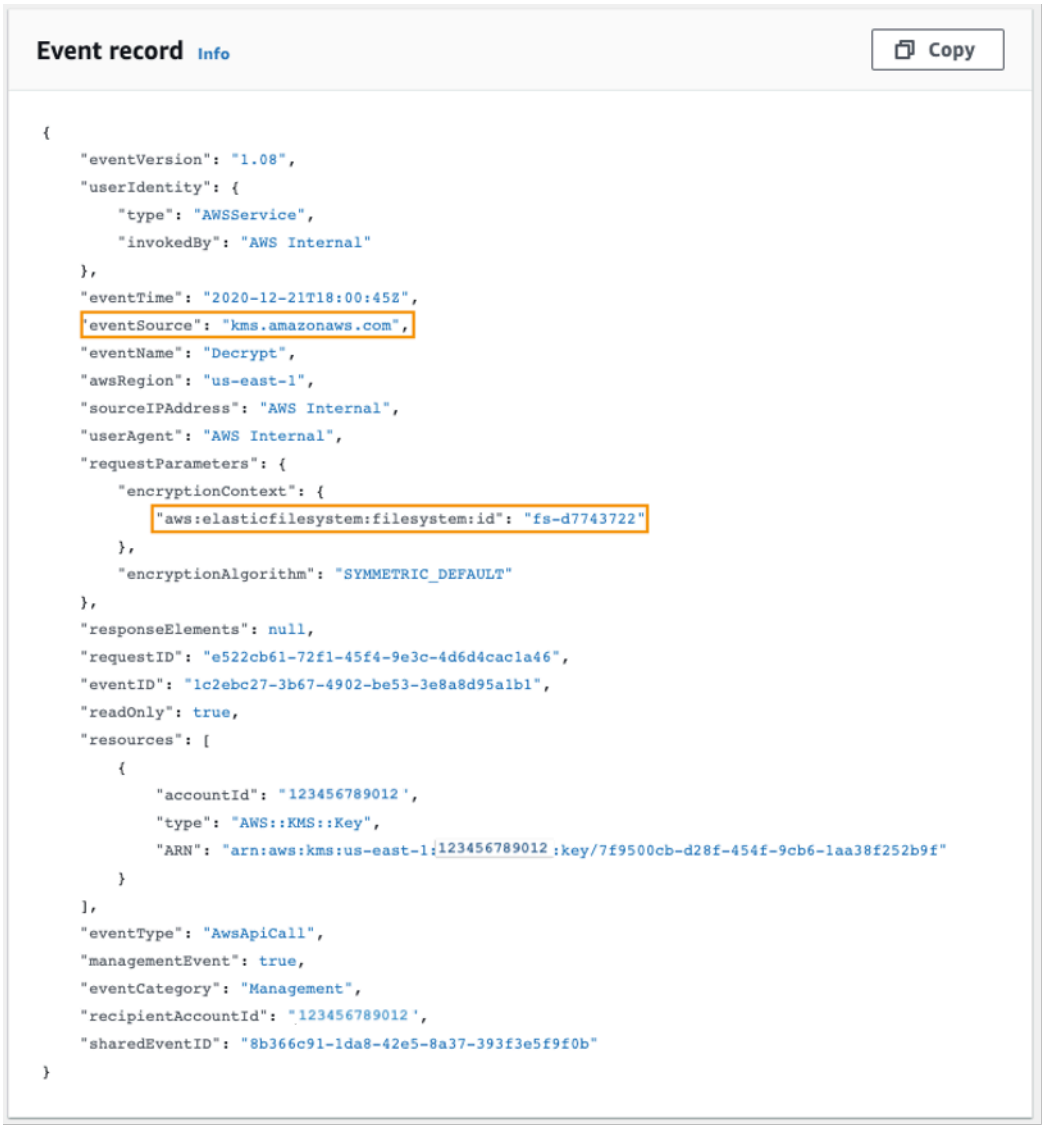
使用加密的 Amazon EFS 檔案系統，不會讓掛載該檔案系統的用戶端感到任何不同。所有密碼編譯作業都發生在 EFS 服務中，資料會在寫入磁碟之前進行加密，並會在用戶端發出讀取請求後進行解密。

誰可以使用金鑰？

AWS KMS 金鑰政策可控制對加密金鑰的存取。

建議您將這些政策與 IAM 政策相結合，以提供另一層控制。每個金鑰都有一個金鑰政策。若金鑰是 AWS 管理的 CMK，則 AWS 會管理該金鑰政策。若金鑰是客戶管理的 CMK，則您可管理該金鑰政策。這些金鑰政策是控制 CMK 存取權的主要方式。其定義了控管使用及管理金鑰的許可。

當您使用 Amazon EFS 建立加密檔案系統時，將會為 Amazon EFS 授與代表您使用 CMK 的存取權。Amazon EFSS 代表您對 AWS KMS 進行的呼叫，會出現在您的 CloudTrail 記錄中，一如來自於您 AWS 帳戶一般。下列螢幕擷取畫面顯示由 Amazon EFS 所進行 KMS 解密呼叫的範例 CloudTrail 事件。



KMS 解密的 CloudTrail 記錄

如需 AWS KMS 的詳細資訊以及如何管理加密金鑰的存取權，請參閱《AWS KMS 開發人員指南》中的管理 AWS KMS CMK 存取權。

如需 AWS KMS 如何管理密碼編譯的詳細資訊，請參閱《AWS KMS 密碼編譯詳細資訊》白皮書。

如需如何建立系統管理員 IAM 使用者與群組的詳細資訊，請參閱《IAM 使用者指南》中的建立您的第一個 IAM 系統管理員使用者與群組。

建立加密檔案系統

您可以使用 AWS 管理主控台、AWS CLI、Amazon EFS API 或 AWS 開發套件，建立加密檔案系統。您只能在建立檔案系統時為其啟用加密。

Amazon EFS 與 AWS KMS 相整合，可進行金鑰管理，並會使用 CMK 為檔案系統加密。檔案系統中繼資料 (如檔案名稱、目錄名稱與目錄內容) 使用 AWS 管理的 CMK 進行加密與解密。

您的檔案或檔案資料的內容，將使用您選擇的 CMK 進行加密與解密。該 CMK 可以是下列三種類型之一：

- 適用於 Amazon EFS 之 AWS 管理的 CMK
- 來自 AWS 帳戶之客戶管理的 CMK
- 來自不同 AWS 帳戶之客戶管理的 CMK

您的組織可能受到公司或法規政策的限制，需要完全控制 CMK 的建立、輪換、刪除，以及存取控制與使用政策。若是如此，建議您使用客戶管理的 CMK。在其他情況下，可以使用 AWS 管理的 CMK。

所有使用者都有適用於 Amazon EFS 之 AWS 管理的 CMK，其別名是 `aws/elasticfilesystem`。AWS 可管理此 CMK 的金鑰政策，且您無法對其進行變更。建立及儲存 AWS 管理的 CMK 不會產生任何費用。

若您決定使用客戶管理的 CMK 來加密您的檔案系統，請選取您擁有之客戶管理的 CMK 的金鑰別名。或者，可以輸入客戶管理的 CMK 的 Amazon Resource Name (ARN)。有了您所擁有之客戶管理的 CMK 之後，即可透過金鑰政策與金鑰授予來控制可使用該金鑰的使用者與服務。

您也可以藉由選擇停用、重新啟用、刪除或撤銷對這些金鑰的存取權，來控制這些金鑰的週期與輪換。如需管理其他 AWS 帳戶中金鑰存取權的資訊，請參閱《AWS KMS 開發人員指南》中的變更金鑰政策。

如需如何管理客戶管理的 CMK 的詳細資訊，請參閱《AWS KMS 開發人員指南》中的客戶主金鑰 (CMK)。

下列章節會討論如何使用 AWS 管理主控台與使用 AWS CLI，建立加密檔案系統。

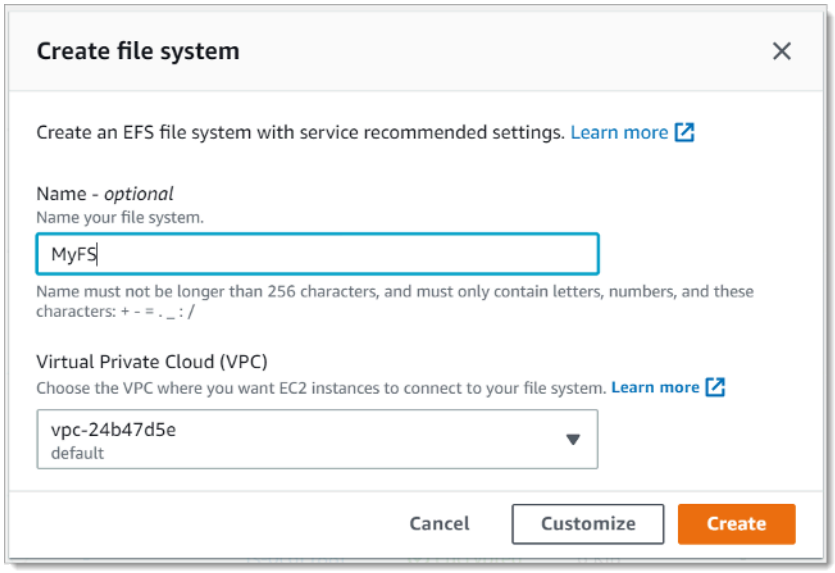
使用 AWS 管理主控台建立加密檔案系統

使用下列程序可以利用 AWS 管理主控台來建立加密 Amazon EFS 檔案系統。

步驟 1.設定檔案系統設定

您在此步驟中會設定一般的檔案系統設定，包括生命週期管理、效能與輸送量模式，以及靜態資料加密。

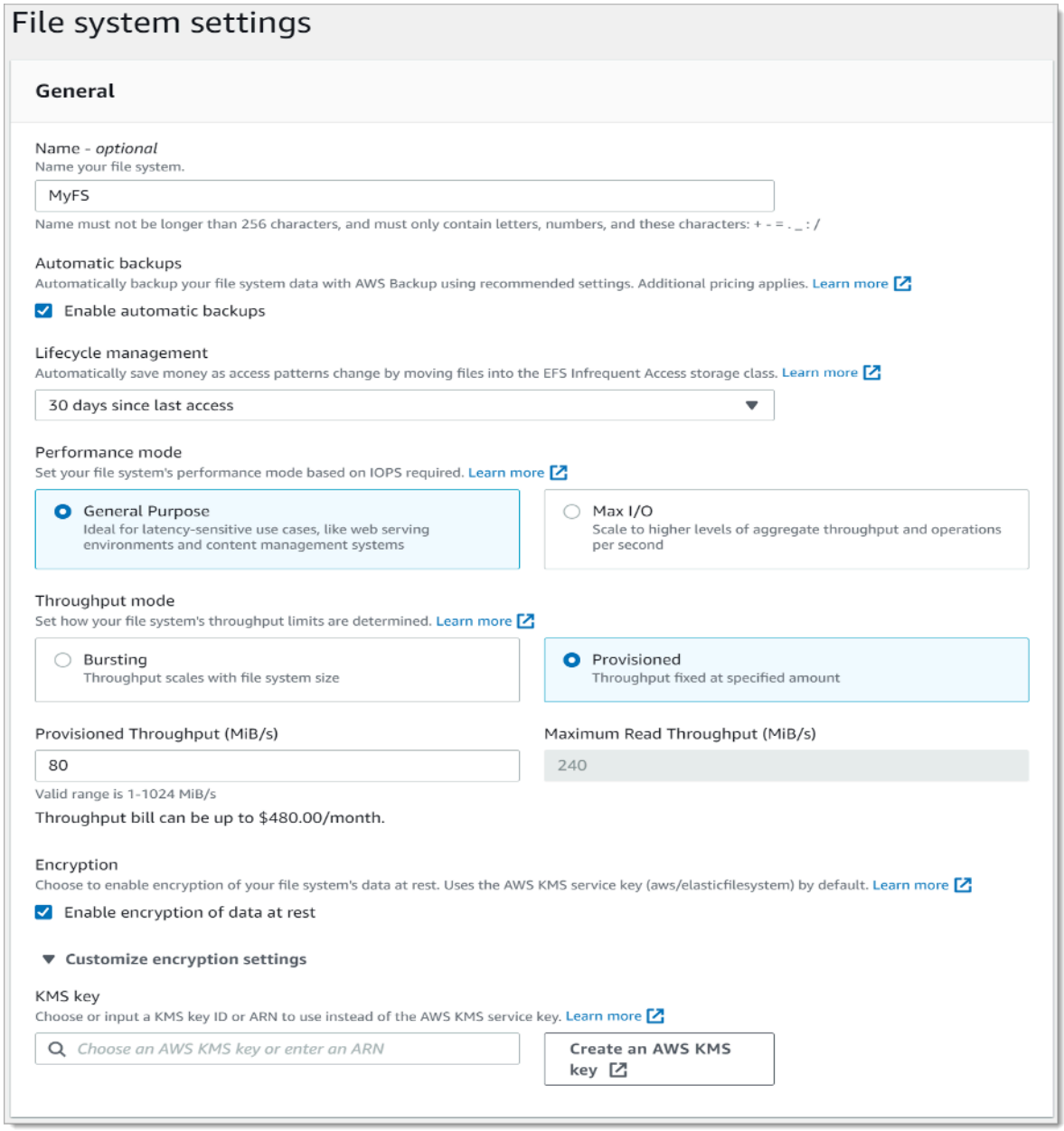
1. 登入 AWS 管理主控台，然後開啟 Amazon EFS 主控台。
2. 選擇 Create file system (建立檔案系統)，開啟 Create file system (建立檔案系統) 對話方塊。如需使用建議設定 (包括根據預設啟用加密) 建立檔案系統的詳細資訊，請參閱建立您的 Amazon EFS 檔案系統。



建立 EFS 檔案系統

3. (選用) 選取 Customize (自訂) 可建立自訂的檔案系統，而不使用服務建議的設定來建立檔案系統。

   File system settings (檔案系統設定) 頁面會隨即出現。



建立 EFS 檔案系統：一般設定

4. 對於 General (一般) 設定，請輸入下列詳細資訊。
   - (選用) 輸入檔案系統的 Name (名稱)。
   - Automatic backups (自動備份) 預設為開啟。您可以清除核取方塊以關閉自動備份。如需詳細資訊，請參閱搭配 Amazon EFS 一起使用 AWS Backup。
   - 選擇 Lifecycle management (生命週期管理) 政策。Amazon EFS 生命週期管理會自動管理您檔案系統中具成本效益的檔案儲存體。若加以啟用，生命週期管理會將尚未存取來設定期間的檔案，移轉至不常存取 (IA) 儲存類別。您可以使用生命週期政策來定義這段期間。若不想啟用生命週期

管理，請選擇 None (無)。如需詳細資訊，請參閱《Amazon EFS 使用者指南》中的 EFS 生命週期管理。

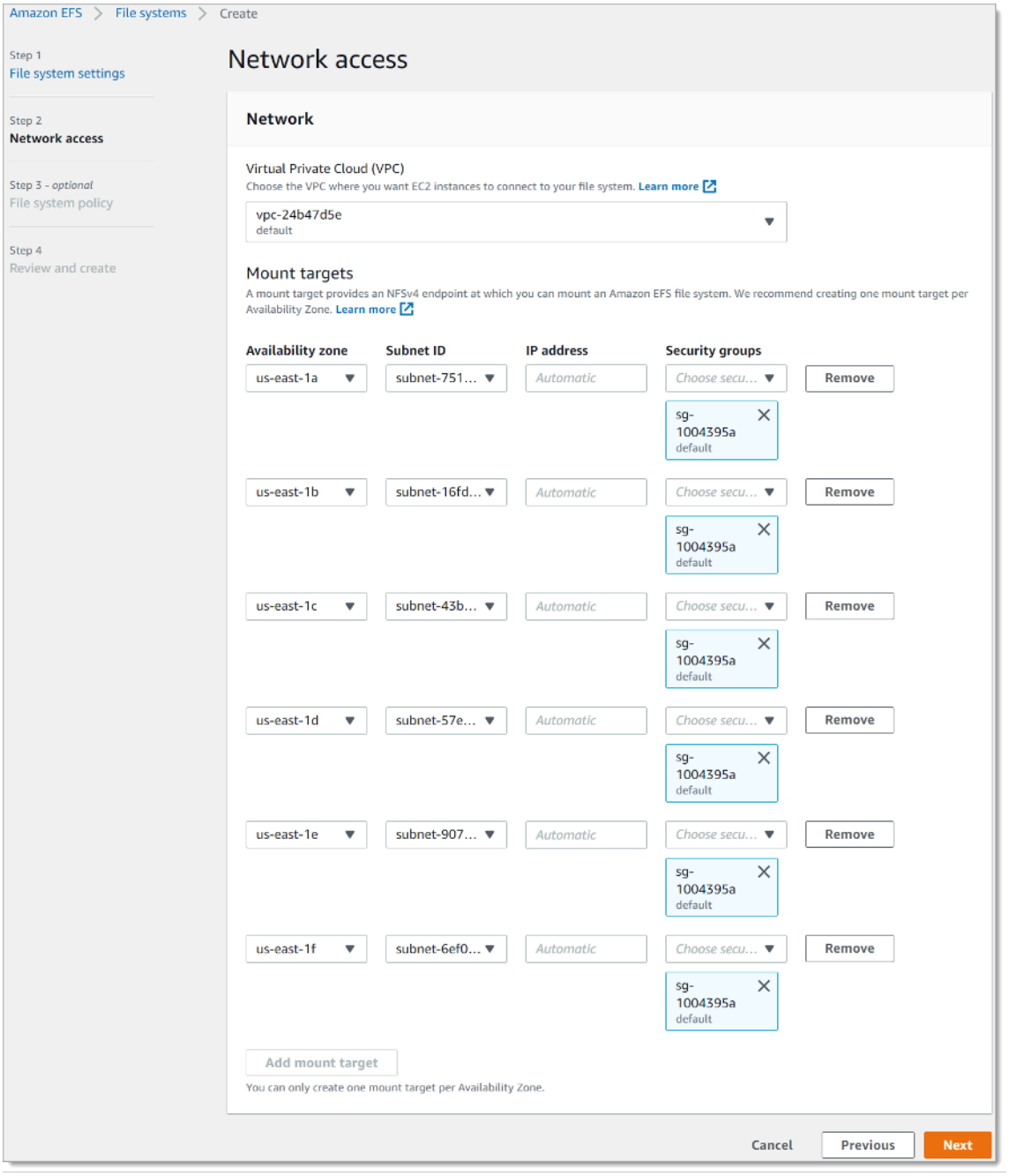
- 選擇 Performance mode (效能模式)，可以是預設的 General Purpose mode (一般用途模式) 或 Max I/O (最大 I/O)。如需詳細資訊，請參閱《Amazon EFS 使用者指南》中的 效能模式。
- 選擇 Throughput mode (輸送量模式)，可以是預設的 Bursting mode (爆量模式) 或 Provisioned mode (佈建模式)。
- 若選取了 Provisioned (佈建)，會隨即顯示Provisioned Throughput (MiB/s) (佈建輸送量 (MiB/秒) 欄位。輸入要為檔案系統佈建的輸送量。輸入輸送量後，主控台會在欄位旁顯示每月成本的估計值。如需詳細資訊，請參閱《Amazon EFS 使用者指南》中的輸送量模式。
- 根據預設，Encryption (加密) 會啟用靜態資料加密。根據預設，其會使用您的 AWS Key Management Service (AWS KMS) EFS 服務金鑰 (`aws/elasticfilesystem`)。若要選擇不同的 KMS 金鑰進行加密，請展開 Customize encryption settings (自訂加密設定)，然後從清單中選擇金鑰。或者，輸入您要使用之 KMS 金鑰的 KMS 金鑰 ID 或 Amazon Resource Name (ARN)。

  若您需要建立新金鑰，請選擇 Create an AWS KMS Key (建立 AWS KMS 金鑰)，啟動 AWS KMS 主控台並建立新金鑰。

5. (選用) 選擇 Add tag (新增標籤)，將成對的金鑰/值，新增至您的檔案系統。
6. 選擇 Next (下一步)，繼續進行組態程序中的 Network Access (網路存取) 步驟。

步驟 2.設定網路存取

在此步驟中，您將設定檔案系統的網路設定，包括虛擬私人雲端 (VPC) 與掛載目標。請為每個掛載目標，設定可用區域、子網路、IP 地址與安全性群組。



建立 EFS 檔案系統：網路存取

1. 選擇您希望 EC2 執行個體連線至您檔案系統的虛擬私人雲端 (VPC)。如需詳細資訊，請參閱《Amazon EFS 使用者指南》中的管理檔案系統網路協助工具。

   - 可用區域 – 根據預設，AWS 區域中的每個可用區域內，都設定了掛載目標。若在特定的可用區域內不希望有掛載目標，請選擇 Remove (移除) 以刪除該區域的掛載目標。在預計會存取您檔案系統的每個可用區域中，建立掛載目標。執行此動作無需付費。

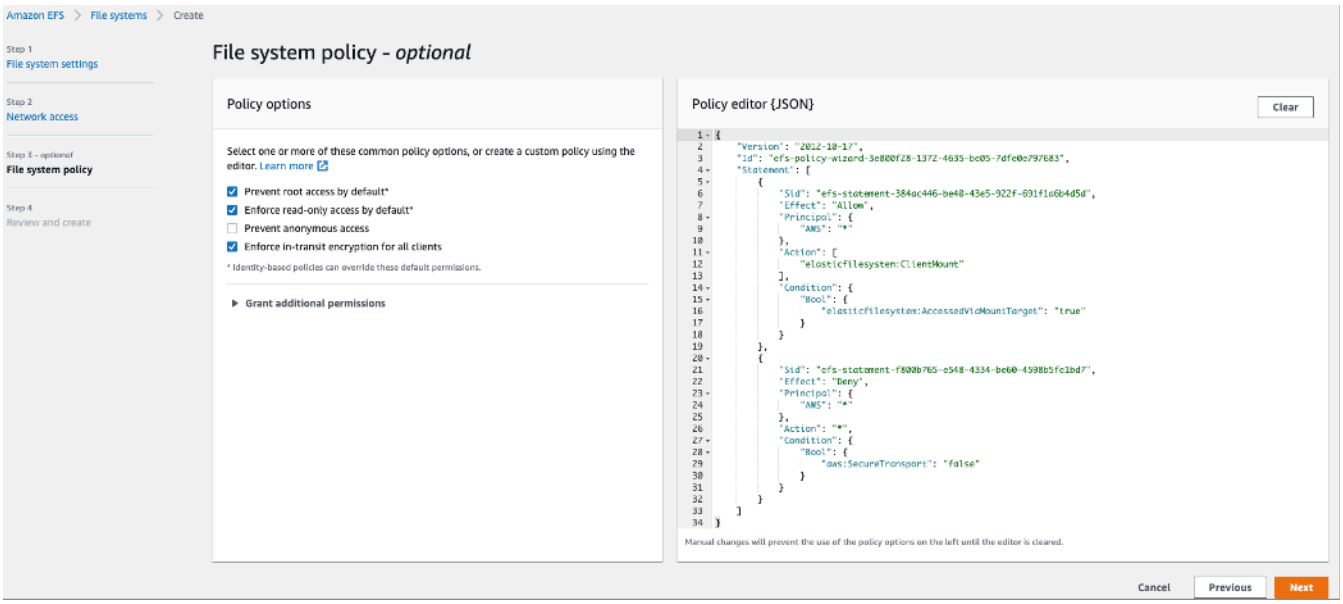
- 子網路 ID – 從可用區域中選擇可用的子網路。預先會選取預設的子網路。最佳實務是根據您的安全需求，確認所選子網路是公有或私有。
- IP 地址 – 根據預設，Amazon EFS 會從子網路的可用地址中，自動選擇 IP 地址。或者，也可以輸入該子網路中的特定 IP 地址。雖然掛載目標具有單一 IP 地址，但這些目標是具有高可用性的備援網路資源。
- 安全群組 – 您可以為掛載目標指定一或多個安全群組。最佳實務是確保安全群組僅用於 EFS 掛載用途 (NFS 連接埠 2049)，而輸入規則僅允許來自其他 VPC CIDR 區塊範圍的連接埠 2049，或是使用安全群組作為需要存取 EFS 的資源來源。如需詳細資訊，請參閱《Amazon EFS 使用者指南》中的使用 Amazon EC2 執行個體與掛載目標的安全群組。

  若要新增其他安全群組或變更安全群組，請選取 Choose security groups (選擇安全群組)，然後從清單中新增另一個安全群組。若不想使用預設的安全群組，可以將其刪除。如需詳細資訊，請參閱《Amazon EFS 使用者指南》中的建立安全群組。

2. 選擇 Add mount target (新增掛載目標) 可為沒有掛載目標的可用區域建立掛載目標。如果每個可用區域都已設定掛載目標，則無法使用此選項。
3. 選擇 Next (下一步) 即可繼續。File system policy (檔案系統政策) 頁面會隨即顯示。

步驟 3.建立檔案系統政策

在此步驟中，您會建立檔案系統政策，控制 NFS 用戶端對檔案系統的存取。EFS 檔案系統政策是 IAM 資源政策，可用於控制 NFS 用戶端對檔案系統的存取。如需詳細資訊，請參閱《Amazon EFS 使用者指南》中的使用 IAM 控制 NFS 對 Amazon EFS 的存取。

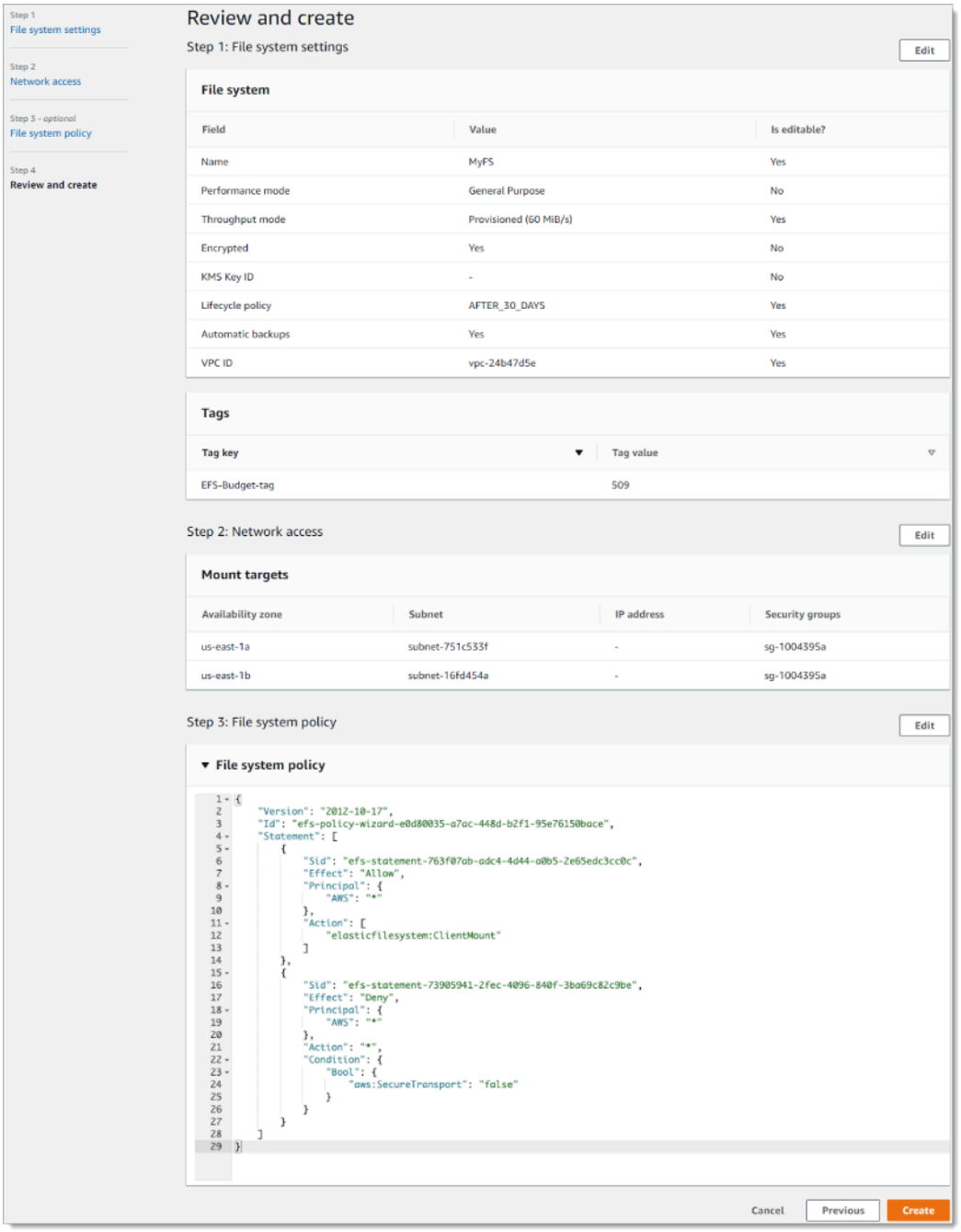


建立 EFS 檔案系統：檔案系統政策

1. 在政策選項中，建議您選擇下列預先設定的可用政策選項：
   - 根據預設防止根存取
   - 根據預設強制執行唯讀存取
   - 對所有用戶端強制執行傳輸中加密
2. 使用 Grant additional permissions (授予其他許可)，可將檔案系統許可授予給其他 IAM 主體 (包括其他 AWS 帳戶)。選擇 Add (新增)，接著輸入要為其授予許可之實體的主體 ARN，然後選擇要授予的 Permissions (許可)。
3. 根據您的需求，使用 Policy editor (政策編輯器) 自訂預先設定的政策，或是依需求建立您自己的政策。當您選擇其中一個預先設定的政策時，JSON 政策定義會隨即出現在政策編輯器中。
4. 選擇 Next (下一步) 即可繼續。Review and create (檢閱及建立) 頁面會隨即出現。

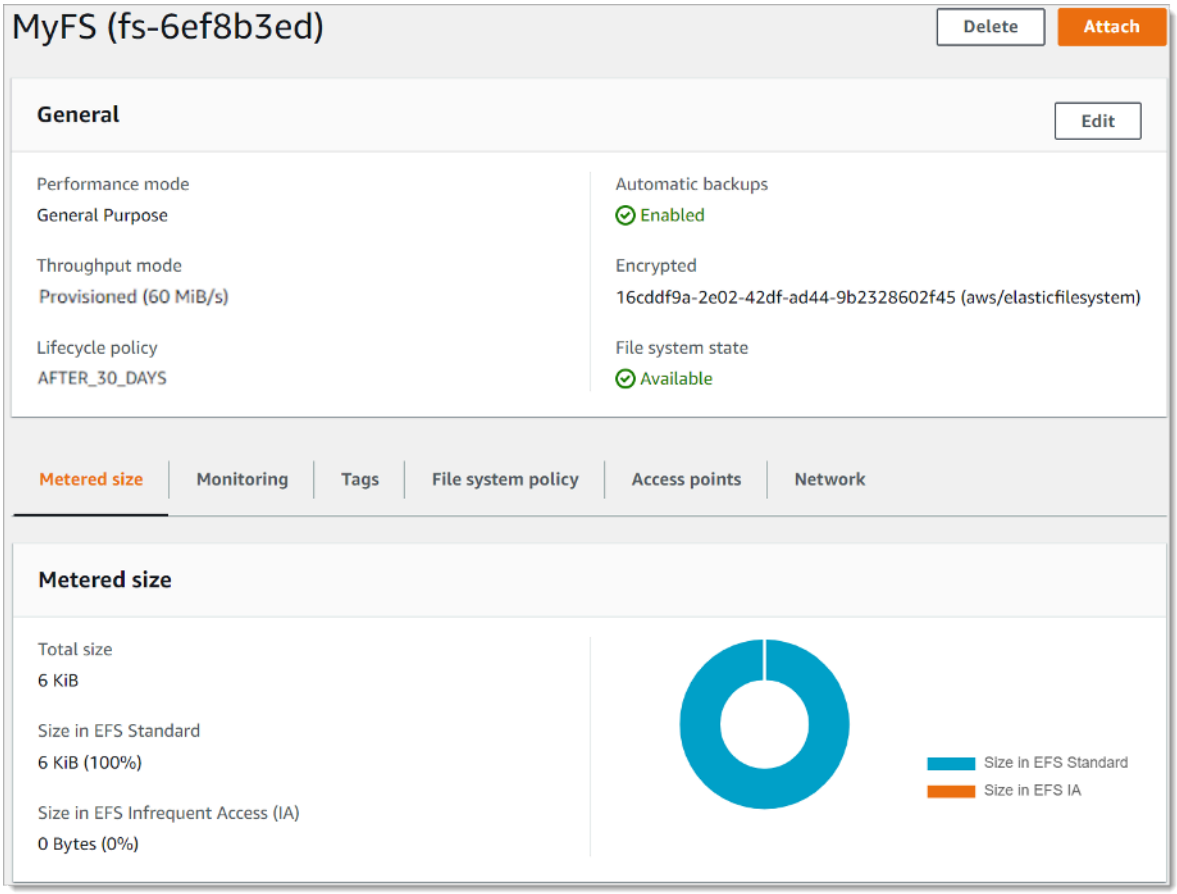
步驟 4.檢閱及建立

在此步驟中，您會檢閱檔案系統設定並進行任何修改，然後建立檔案系統。



建立 EFS 檔案系統：檢閱及建立

1. 檢閱每個檔案系統組態群組。此時，您可以選擇 Edit (編輯)，對每個群組進行變更。
2. 選擇 Create (建立) 可以建立檔案系統，並返回 File systems (檔案系統) 頁面。
3. File systems (檔案系統) 頁面會顯示檔案系統及其組態詳細資訊，如下圖所示。



檔案系統

使用 AWS CLI 建立加密檔案系統

當您使用 AWS CLI 建立加密檔案系統時，可以使用其他參數來設定加密狀態與客戶管理的 CMK。請務必使用最新版本的 AWS CLI。如需升級 AWS CLI 的資訊，請參閱《AWS 命令列界面使用者指南》中的安裝、更新及解除安裝 AWS CLI。

在 `CreateFileSystem` 作業中，`--encrypted` 參數是建立加密檔案系統所需的布林值。只有當您使用客戶管理的 CMK 且包含金鑰的別名或 ARN 時，才需要 `--kms-key-id`。若目前使用 AWS 管理的 CMK，請勿包含此參數。

```
$ aws efs create-file-system \
--creation-token $(uuidgen) \
--performance-mode generalPurpose \
--encrypted \
--kms-key-id user/customer-managedCMKalias
```

如需使用 AWS 管理主控台、AWS CLI、AWS 開發套件或 Amazon EFS API 建立 Amazon EFS 檔案系統的詳細資訊，請參閱《Amazon EFS 使用者指南》中的什麼是 Amazon Elastic File System。

強制執行靜態資料加密

加密對 I/O 延遲與輸送量的影響非常小。使用者、應用程序與服務並不會感覺到加密與解密的進行。所有資料與中繼資料在寫入磁碟之前，都會由 Amazon EFS 代表您進行加密，並會在客戶端讀取之前進行解密。您無需變更用戶端工具、應用程序或服務，即可存取加密的檔案系統。

您的組織可能需要加密所有資料，才能符合特定的機密等級，或是需要加密與特定應用程式、工作負載或環境相關聯的所有資料。您可以使用以 AWS Identity and Access Management (IAM) 身分區分的政策，為 Amazon EFS 檔案系統的資源強制執行靜態資料加密。使用 IAM 條件金鑰可以避免使用者建立未加密的 EFS 檔案系統。

例如，明確允許使用者只能建立加密 EFS 檔案系統的 IAM 政策，會使用下列效果、動作與條件的組合：

- `Effect` 為 `Allow`。
- `Action` 為 `elasticfilesystem:CreateFileSystem`。
- `Condition` `elasticfilesystem:Encrypted` 為 `true`。

下列範例說明以 IAM 身分區分的政策，其授權主體只能建立加密的檔案系統。

```
{
  “Version”: “2012-10-17”,
  “Statement”: [
    {
      “Sid”: “VisualEditior0”,
      “Effect”: “Allow”,
      “Action”: “elasticfilesystem:CreateFileSystem”,
      “Condition”: {
        “Bool”: {
          “elasticfilesystem:Encrypted”: “true”
        }
      },
      “Resource”: “*”
    }
```

```
}
```

設定為 * 的 Resource 屬性，表示將會對所有建立的 EFS 資源，套用 IAM 政策。您可以根據標籤新增其他條件屬性，以便只對具有資料機密需求的一部分 EFS 資源強制執行該屬性。

您也可以藉由對組織中的所有 AWS 帳戶或 OU 使用服務控制政策，在 AWS Organizations 層級強制執行建立加密的 Amazon EFS 檔案系統。如需 AWS Organizations 中服務控制策略的詳細資訊，請參閱《AWS Organizations 使用者指南》中的服務控制政策。

建立需要加密所有 EFS 檔案系統的 IAM 政策

您可以建立以 IAM 身分區分的政策，授權使用者使用主控台、AWS CLI 或 API 時，只能建立加密的 Amazon EFS 檔案系統。下列程序描述如何使用 IAM 主控台建立此類政策，然後再將該政策套用至您帳戶中的使用者。

建立強制執行加密 EFS 檔案系統的 IAM 政策：

1. 登入 AWS 管理主控台，並開啟 IAM 主控台。
2. 在導覽窗格的 Access management (存取管理) 下，選擇 Policies (政策)。
3. 選擇 Create policy (建立政策)，隨即會顯示 Create policy (建立政策) 頁面。
4. 在 Visual Editor (視覺化編輯器) 標籤中，輸入下列資訊。
   - 針對服務，請選擇 EFS。
   - 針對動作，請在搜尋欄位中輸入 `create`，然後選擇 CreateFileSystem (建立檔案系統)。
   - 針對 請求條件，請按一下 Add condition (新增條件) 連結，對 Condition Key (條件金鑰) 搜索 `elasticfilesystem:Encrypted`、對 Operator (運算子) 搜尋 `Bool`，以及對 Value (值) 搜尋 `true`。
5. 提供該政策的名稱與描述。確認政策摘要，包括 Encrypted (加密) 請求條件。
6. 選擇 Create policy (建立政策)，以建立政策。

對帳戶中的使用者套用政策：

1. 在 IAM 主控台中的 Access management (存取管理) 下，選擇 Users (使用者)。
2. 選取要套用該政策的使用者。
3. 選擇 Add permissions (新增許可)，隨即會顯示 Add permissions (新增許可) 頁面。
4. 選擇 Attach existing policies directly (直接連接現有政策)。

5. 輸入您於上一個程序中所建立的 EFS 政策名稱。
6. 選取並展開該政策。然後選擇 {}JSON，以確認該政策的內容。看起來應該像下列 JSON 政策。

```
{
  “Version”: “2012-10-17”,
  “Statement”: [
    {
      “Sid”: “VisualEditior0”,
      “Effect”: “Allow”,
      “Action”: “elasticfilesystem:CreateFileSystem”,
      “Condition”: {
        “Bool”: {
          “elasticfilesystem:Encrypted”: “true”
        }
      },
      “Resource”: “*”
    }
}
```

偵測未加密的檔案系統

您的組織可能有找出未加密 Amazon EFS 資源的需求。您可以使用 AWS Config 受管規則，偵測未加密的檔案系統。AWS Config 提供 AWS 受管規則，其為預先定義且可自訂的規則，AWS Config 會使用這些規則來評估您的 AWS 資源是否符合常見的最佳實務，並會將不符合規則的資源加上 NON_COMPLIANT 的旗標。

您可以使用 AWS Managed Config 規則 `efs-encrypted-check`，檢查 Amazon Elastic File System (Amazon EFS) 是否已設定為使用 AWS Key Management Service (AWS KMS) 來加密檔案資料。如需設定與啟用 AWS 受管規則的詳細資訊，請參閱使用 AWS Config 受管規則。

傳輸中資料的加密

您可以掛載檔案系統，以便使用業界標準 AES-256 加密的傳輸層安全性 1.2 (TLS)，加密傳輸中的所有 NFS 流量。TLS 是一組業界標準的密碼編譯通訊協定，用於為透過網路交換的資訊進行加密。AES-256 是 256 位元加密密碼，用於 TLS 中的資料傳輸。建議您在存取檔案系統的每個用戶端上，都設定傳輸中的加密。

您可以使用 IAM 政策，針對 NFS 用戶端存取 Amazon EFS 強制執行傳輸中的加密。當用戶端連接至檔案系統時，Amazon EFS 會評估檔案系統的 IAM 資源政策 (稱為檔案系統政策) 以及任何以身分區分的 IAM 政策，來決定要授予的適當之檔案系統存取許可。您可以在檔案系統資源政策中，使用 `aws:SecureTransport` 條件金鑰，強制 NFS 用戶端在連接至 EFS 檔案系統時，要使用 TLS。

> **Note**
>
> 您必須使用 EFS 掛載協助程式，掛載您的 Amazon EFS 檔案系統，才能使用 IAM 授權來控制 NFS 用戶端的存取權。如需詳細資訊，請參閱《Amazon EFS 使用者指南》中的使用 IAM 授權進行掛載。

下列 EFS 檔案系統政策範例，會強制執行傳輸中進行加密，並具有下列特性：

- `effect` 為 `allow`。
- 所有 IAM 實體的主體都設定為 `*`。
- 動作設定為 `ClientMount`、`ClientWrite` 與 `ClientRootAccess`。
- 授予許可的條件設定為 `SecureTransport`。只有對使用 TLS 連接至檔案系統的 NFS 用戶端，才授予存取權。

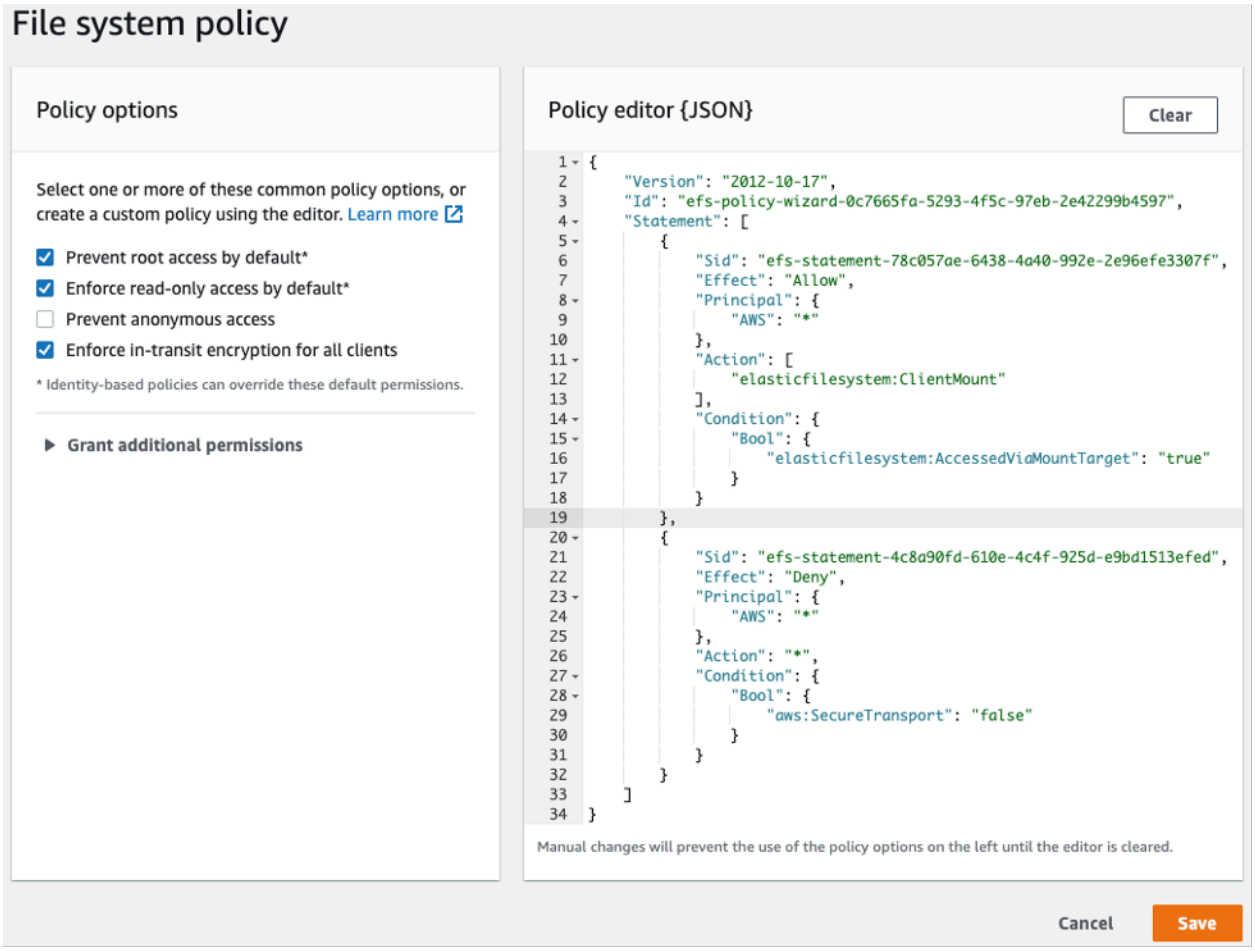
```
{
  “Version”: “2012-10-17”,
  “Id”: “ExamplePolicy01”,
  “Statement”: [
    {
      “Sid”: “VisualEditior0”,
      “Effect”: “Allow”,
      “Principal”: {
        “AWS”: “*”,
      },
      “Action”: [
```

```
“elasticfilesystem:ClientRootAccess”,
“elasticfilesystem:ClientMount”,
“elasticfilesystem:ClientWrite”
      ],
      “Condition”: {
        “Bool”: {
          “aws:SecureTransport”: “true”
        }
      }
    }
  ]
}
```

您可以使用 Amazon EFS 主控台或 AWS CLI，建立檔案系統政策。

使用 EFS 主控台建立檔案系統政策：

1. 開啟 Amazon EFS 主控台。
2. 選擇 File Systems (檔案系統)。
3. 在 File systems (檔案系統) 頁面上，選擇您要對其編輯或建立檔案系統政策的檔案系統。該檔案系統的詳細資訊頁面會隨即顯示。
4. 選擇 File system policy (檔案系統政策)，然後選擇 Edit (編輯)。 File system policy (檔案系統政策) 頁面會隨即顯示。



建立檔案系統政策

5. 在政策選項中，建議您選擇下列可用的預先設定之政策選項：

   - 根據預設防止根存取
   - 根據預設強制執行唯讀存取
   - 對所有用戶端強制執行傳輸中加密

   若您選擇預先設定的政策，則政策 JSON 物件會隨即顯示在 Policy editor (政策編輯器) 面板中。

6. 使用 Grant additional permissions (授予其他許可)，可將檔案系統許可授予給其他 IAM 主體 (包括其他 AWS 帳戶)。選擇 Add (新增)，接著輸入要為其授予許可之實體的主體 ARN，然後選擇要授予的 Permissions (許可)。

7. 根據您的需求，使用 Policy editor (政策編輯器) 自訂預先設定的政策，或是依需求建立您自己的政策。當您使用編輯器時，預先設定的政策選項會變為無法使用。若要復原政策變更，請選擇 Clear (清除)。

當您清除編輯器時，預先設定的政策會再次變為可用。

8. 完成政策的編輯或建立後，請選擇 Save (儲存)。

   檔案系統的詳細資訊頁面會隨即顯示，並會顯示 File system policy (檔案系統政策) 中的政策。

   您也可以使用 AWS CloudFormation 或 AWS 開發套件，以程式設計方式建立檔案系統政策，或是直接使用 Amazon EFS API 建立檔案系統政策。如需建立檔案系統政策的詳細資訊，請參閱《Amazon EFS 使用者指南》中的建立檔案系統政策。

設定傳輸中資料的加密

若要設定傳輸中資料的加密，建議您在每個用戶端上下載 EFS 掛載協助程式。EFS 掛載協助程式是 AWS 提供的開放原始碼公用程式，可用於簡化 EFS 的使用，包括設定傳輸中資料的加密。根據預設，掛載協助程式會使用 EFS 建議的掛載選項。

下列 Linux 發行版本支援 EFS 掛載協助程式：

- Amazon Linux 2017.09+
- Amazon Linux 2+
- Debian 9+
- Fedora 28+
- Red Hat Enterprise Linux / CentOS 7+
- Ubuntu 16.04+

設定傳輸中資料的加密：

1. 安裝 EFS 掛載協助程式：
   - 針對 Amazon Linux，請使用此命令：

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

   - 針對其他 Linux 發行版本，請從 GitHub 下載並安裝。

     amazon-efs-utils 套件會自動安裝下列相依內容：NFS 用戶端 (nfs-utils)、網路轉送 (stunnel)、OpenSSL 與 Python。
2. 掛載檔案系統：

```
sudo mount -t efs -o tls file-system-id
efs-mount-point
```

- `mount -t efs` 會叫用 EFS 掛載協助程式。
- 使用 EFS 掛載協助程式進行掛載時，不支持使用檔案系統的 DNS 名稱或使用掛載目標的 IP 地址，請改用檔案系統 ID。
- 根據預設，EFS 掛載協助程式會使用 AWS 建議的掛載選項。不建議覆寫這些預設掛載選項，但在出現情況時，我們提供執行此動作的彈性。建議您徹底測試所有覆寫的掛載選項，了解這些變更對於檔案系統存取與效能的影響。
- 下表顯示 EFS 掛載協助程式所使用的預設掛載選項。

選項	描述
nfsvers=4.1	NFS 通訊協定版本
rsize=1048576	NFS 用戶端針對每個網路 READ 請求，可接收的資料位元組上限)
wsize=1048576	NFS 用戶端針對每個網路 WRITE 請求，可傳送的資料位元組上限

選項	描述
hard	NFS 用戶端在 NFS 請求逾時後的復原行為，以便讓 NFS 請求在伺服器回覆之前無限期重試。
timeo=600	NFS 用戶端重試 NFS 請求之前，等待回應的逾時值 (單位為十秒)
retrans=2	NFS 用戶端在嘗試進一步的復原動作之前，重試請求的次數
noresvport	告訴 NFS 用戶端在重新建立網路連線時，使用新的 TCP 來源連接埠

- 將下列一行新增至 `/etc/fstab`，任一系統重新啟動之後，就會自動重新掛載您的檔案系統。

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

使用傳輸中資料的加密

若您的組織受到需要加密傳輸中資料之公司或法規政策的限制，建議您在存取檔案系統的每個用戶端上，使用傳輸中資料的加密。加密與解密設定於連接層級中，能增添另一層的安全性。

使用 EFS 掛載協助程式來掛載檔案系統，會設定及維持用戶端與 Amazon EFS 之間的 TLS 1.2 通道，並會透過此加密通道來路由所有 NFS 流量。用於建立加密 TLS 連接的憑證，由 Amazon Certificate Authority (CA) 所簽署，並受到大多數現代 Linux 發行版本的信任。EFS 掛載協助程式也繁衍出一個看門狗程序，以監視每個檔案系統的所有安全通道，並確保其正在執行。

使用 EFS 掛載協助程式建立與 Amazon EFS 的加密連線之後，不需要其他使用者輸入或組態。使用者連接與應用程序在存取檔案系統時，並不會感覺到正在進行加密。

成功掛載並使用 EFS 掛載協助程式建立 EFS 檔案系統的加密連線後，掛載命令的輸出會顯示掛載的檔案系統，並會使用 localhost (127.0.0.1) 作為網路轉送來建立加密通道。請參閱下列輸出範例。

```
     127.0.0.1:/ on efs-mount-point type nfs4

(rw,relatime,vers=4.1,rsize=1048576,wsize=1048576,namlen=255,hard,proto=tcp,port=20059,timeo=6
```

若要將 `efs-mount-point` 對應至 EFS 檔案系統，請在 `/var/log/amazon/efs` 中查詢 mount.log 檔案，並找到上次成功的掛載作業。使用下列簡單的 grep 命令即可完成。

```
     grep -E "Successfully
     mounted.*efs-mount-point"
     /var/log/amazon/efs/mount.log | tail -1
```

此 grep 命令的輸出，將會傳回掛載的 EFS 檔案系統之 DNS 名稱。請參閱以下輸出範例。

```
     2018-03-15 07:03:42,363 - INFO - Successfully mounted
     file-system-id.efs.region.amazonaws.com
     at efs-mount-point
```

結論

Amazon EFS 檔案系統待用資料與傳輸中的資料都可加密。您可以使用 CMK 為待用資料加密，並使用 AWS KMS 加以控制及管理。建立加密檔案系統非常簡單，只需在 AWS 管理主控台的 Amazon EFS 檔案系統建立精靈中選取核取方塊，或是將單一參數新增至 AWS CLI、AWS 開發套件或 Amazon EFS API 中的 `CreateFileSystem` 作業。

您可以使用以 AWS IAM 身分區分的原則與檔案系統原則，為待用與傳輸施行加密，以進一步強化您的安全需求，並有助於滿足您的合規需求。使用加密檔案系統對檔案系統效能影響最小，不會讓服務、應用程式與使用者感到任何不同。您可以使用 EFS 裝載協助程式，在每個用戶端上建立加密的 TLS 通道，為傳輸中的資料加密，藉此為用戶端與裝載的 EFS 檔案系統之間的所有 NFS 流量加密。您可以使用 IAM 身分原則，為 Amazon EFS 待用資料施行加密，並使用 EFS 檔案系統原則為 Amazon EFS 傳輸中的資料施行加密，兩者均無需額外費用。

資源

- 《AWS KMS 密碼編譯詳細資訊白皮書》
- Amazon EFS User Guide

文件歷史記錄與貢獻者

文件歷史記錄

若要收到此白皮書更新的通知，請訂閱 RSS 摘要。

update-history-change	update-history-description	update-history-date
小幅度更新	調整頁面配置	2021 年 4 月 30 日
更新白皮書	新增使用 IAM 施行待用與傳輸中的加密	2021 年 2 月 22 日
更新白皮書	新增傳輸中的資料加密	2018 年 4 月 1 日
初次出版	發佈使用 Amazon EFS 加密檔案系統為待用資料加密	2017 年 9 月 1 日

> **Note**
>
> 若要訂閱 RSS 更新，您必須為正在使用的瀏覽器啟用 RSS 外掛程式。

貢獻者

此文件的貢獻者包括：

- AWS 儲存體專家解決方案架構師 Darryl S. Osborne
- Amazon EFS 資深產品經理 Joseph Travaglini
- AWS 首席解決方案架構師 Peter Buonora
- AWS 資深解決方案架構師 Siva Rajamani