使用者指南

AWS Transfer Family

AWS Transfer Family: 使用者指南

Table of Contents

什麼是 AWS Transfer Family？ 1
如何 AWS Transfer Family 工作 3
與 Transfer Family 相關的博客文章 4
必要條件 7
區域、端點和配額 7
註冊成為 AWS 7
設定儲存 8
設定 Amazon S3 儲存貯體 8
設定 Amazon EFS 檔案系統 12
建立 IAM 角色和政策 15
建立使用者角色 16
工作階段原則的運作 19
讀/寫存取政策範例 22
Transfer Family 自學課 26
開始使用伺服器端點 26
必要條件 27
登入 主控台。 27
建立啟用 SFTP 的伺服器 28
新增服務受管理的使用者 29
使用用戶端傳輸檔案 30
建立解密工作流程 31
步驟 1：設定執行角色 32
步驟 2：建立受管理的工作流程 33
步驟 3：將工作流程新增至伺服器並建立使用者 34
步驟 4：建立 PGP key pair 36
步驟 5：將 PGP 私鑰存儲在 AWS Secrets Manager 36
步驟 6：加密檔案 37
步驟 7：執行工作流程並檢視結果 38
建立和使用 SFTP 連接器 39
步驟 1：建立必要的輔助資源 40
步驟 2：建立並測試 SFTP 連接器 44
步驟 3：使用 SFTP 連接器傳送和擷取檔案 48
建立 Transfer Family 伺服器做為遠端 SFTP 伺服器的程序 52
使用自訂身分識別提供者 54

必要條件 55
步驟 1：建立 CloudFormation 堆疊 55
步驟 2：檢查伺服器的 API Gateway 方法設定 56
步驟 3：查看 Transfer Family 服務器詳細信息 57
步驟 4：測試您的使用者是否可以連線到伺服器 58
步驟 5：測試 SFTP 連線和檔案傳輸 58
步驟 6：限制存取值區 59
如果使用 Amazon EFS，請更新 61
設定 AS2 組態 62
步驟 1：為 AS2 建立憑證 63
步驟 2：建立使用 AS2 通訊協定的 Transfer Family 伺服器 66
步驟 3：將憑證匯入為 Transfer Family 憑證資源 69
步驟 4：為您和您的交易夥伴建立個人檔案 70
步驟 5：建立您與合作夥伴之間的協議 71
步驟 6：在您和合作夥伴之間建立連接器 72
第 7 步：使用 Transfer Family 列測試在 AS2 上交換文件 73
Transfer Family 適用於 SFTP、FTPS、FTP 76
識別提供者選項 76
AWS Transfer Family 端點類型矩陣 78
設定 Transfer Family 伺服器端點 80
建立啟用 SFTP 的伺服器 82
建立啟用 FTP 的伺服器 89
建立啟用 FTP 的伺服器 97
在 VPC 中創建服務器 104
使用自訂主機名稱 123
透過伺服器端點傳輸檔案 127
可用的SFT/FTPS/FTP 指令 129
尋找您的 Amazon VPC 端點 130
避免`setstat`錯誤 132
使用 OpenSSH 30
使用 WinSCP 133
使用網路鴨 30
使用 FileZilla 136
使用一個 Perl 客戶端 138
上傳後處理 138
管理使用者 139

服務管理使用者 141
目錄服務使用者 149
自訂身分識別提供者 165
使用邏輯目錄 191
使用邏輯目錄的規則 192
實作邏輯目錄和 chroot 193
設定邏輯目錄範例 195
設定 Amazon EFS 的邏輯目錄 196
自定義 AWS Lambda 響應 197
SFTP 連接器 198
設定 SFTP 連接器 198
建立 SFTP 連接器 199
儲存密碼以與 SFTP 連接器搭配使用 206
產生並格式化 SFTP 連接器私密金鑰 207
測試 SFTP 連接器 210
使用 SFTP 連接器傳輸檔案 212
列出遠程目錄的內容 213
管理 SFTP 連接器 215
更新 SFTP 連接器 215
檢視 SFTP 連接器詳細資料 216
SFTP 連接器的配額 218
AS2 的 Transfer Family 219
AS2 使用案例 220
配置 AS2 223
使用 Transfer Family 列主控台建立 AS2 伺服器 225
使用範本建立 AS2 伺服器 228
AS2 配置 230
AS2 特色與功能 235
設定 AS2 連接器 237
建立 AS2 連接器 237
AS2 連接器演算法 240
AS2 連接器的基本驗證 241
啟用 AS2 連接器的基本驗證 243
檢視連接器詳情 246
管理 AS2 合作夥伴 248
匯入 AS2 憑證 248

AS2 證書輪換 249
建立 AS2 設定檔 251
建立 AS2 協議 251
傳輸 AS2 訊息 252
傳送 AS2 訊息 253
接收 AS2 訊息 254
為 AS2 設定 HTTPS 255
使用 AS2 連接器傳輸檔案 260
檔案名稱和位置 261
狀態碼 263
範例 JSON 檔案 264
監視器 266
AS2 狀態碼 267
AS2 錯誤代碼 268
管理檔案處理工作流 276
建立工作流程 278
設定和執行工作流程 279
檢視工作流程詳 281
使用預定義步驟 284
複製檔案 284
解密文件 289
標籤檔案 294
刪除檔案 295
工作流程的命名變數 296
範例標記和刪除工作流程 296
使用自訂檔案處理步驟 301
連續使用多個 Lambda 函數 302
在自訂處理後存取檔案 303
檔案上傳時傳送至 AWS Lambda 的範例事件 304
自訂工作流程步驟的 Lambda 函數範例 305
自訂步驟的 IAM 許可 306
工作流程的 IAM 政策 306
工作流信任關係 308
範例執行角色：解密、複製和標記 308
示例執行角色：運行函數並刪除 310
工作流程的異常處理 311

監控工作流執行 312
CloudWatch 工作流程的記錄 312
CloudWatch 工作流程的指標 314
從範本建立工作流程 315
從轉移系列伺服器移除工作流程 318
限制和限制 320
管理伺服器 322
檢視伺服器清單 322
刪除伺服器 322
檢視 SFTP 伺服器詳細資訊 324
檢視 AS2 伺服器詳細資訊 325
編輯伺服器詳情 326
編輯檔案傳輸通訊協定 329
編輯自訂身分提供者參數 331
編輯伺服器端點 333
編輯記錄 335
編輯安全性原則 335
變更管理的工作流程 336
變更伺服器的顯示橫幅 337
讓伺服器連線或離線 338
管理伺服器主機金鑰 339
新增其他伺服器主機金鑰 339
刪除伺服器主機金鑰 341
旋轉伺服器主機金鑰 341
其他伺服器主機金鑰資訊 343
監控主控台內的使用 344
管理存取控制 347
建立 S3 儲存貯體存取政策 347
建立工作階段原則 349
防止使用者mkdir在 S3 儲存貯體中執行 352
日誌 353
CloudTrail 記錄 353
啟用 CloudTrail 記錄 354
建立伺服器的範例記錄項目 355
CloudWatch 記錄 356
Transfer Family 的 CloudWatch 日誌記錄類型 357

建立伺服器的記錄 359
管理工作流程的記錄 366
配置角色 CloudWatch 369
檢視 Transfer Family 日誌串流 371
創建 Amazon CloudWatch 警報 374
將 S3 API 呼叫記錄到 S3 存取日誌 374
限制混淆副問題的例子 375
CloudWatch 轉移系列的記錄結構 376
範例 CloudWatch 記錄項目 381
使用 CloudWatch 指標 385
使用者通知 387
CloudWatch 查詢 387
使用管理事件 EventBridge 390
Transfer Family 事件 390
SFTP、FTP 伺服器和 FTP 伺服器事件 391
SFTP 連接器事件 391
A2S 活動 392
發送 Transfer Family 事件 392
建立事件模式 393
測試事件的 Transfer Family 事件模式 394
許可 394
其他資源 394
事件詳細參照 395
伺服器事件 395
連接器事件 399
澳大事件 406
安全 412
伺服器的安全性原則 413
加密算法 414
TransferSecurity政策 423
TransferSecurity政策 424
TransferSecurity政策 425
TransferSecurity政策 426
TransferSecurity政策 427
TransferSecurity政策-通信 -2024-01 /政策-FIPS-2024-05 TransferSecurity 428
TransferSecurity政策-火災 429

TransferSecurity政策-五 431
後量子安全性原則 432
SFTP 連接器的安全性原則 436
後量子安全性原則 438
關於 SSH 中的後量子混合金鑰交換 439
使用方式 440
測試方式 441
資料保護 444
資料加密 445
Transfer Family 中的密鑰管理 446
身分與存取管理 461
物件 461
使用身分驗證 462
使用政策管理存取權 464
如何與 IAM AWS Transfer Family 搭配使用 466
身分型政策範例 470
標籤型政策範例 472
對 身分與存取進行疑難排解 475
法規遵循驗證 477
恢復能力 478
基礎架構安全 479
Web 應用防火牆 479
預防跨服務混淆代理人 480
Transfer Family 使用者角色 481
「Transfer Family」工作流 483
Transfer Family 記錄/調用角色 484
AWS 受管理政策 486
AWSTransferConsoleFullAccess 486
AWSTransferFullAccess 488
AWSTransferLoggingAccess 489
AWSTransferReadOnlyAccess 490
政策更新 491
疑難排解 Transfer Family 492
服務管理使用者疑難 492
疑難排解 Amazon EFS 服務受管使用 492
公開金鑰主體太長的疑難排解 493

疑難排解無法新增 SSH 公開金鑰 493
Amazon API Gateway 問題的疑難 494
驗證失敗次數太多 494
連接已關閉 495
疑難排解加密 Amazon S3 儲存貯體的政策 496
排解驗證問題 496
驗證失敗 — SS/sFTP 496
受管理 AD 不相符範圍問題 497
其他驗證問題 497
排解受管理工作流程 498
使用 Amazon 疑難排解工作流程相關錯誤 CloudWatch 498
排解工作流程複製錯 500
疑難排解工作流程解 500
疑難排解簽署加密檔案的錯誤 501
疑難排解 FIPS 演算法的錯誤 501
解決 Amazon EFS 問題 503
排解遺失的 POSIX 設定檔 503
使用 Amazon EFS 疑難排解邏輯目錄 504
疑難排解測試身分提供者 505
疑難排解為 SFTP 連接器新增受信任的主機金鑰 505
排解檔案上傳問題 506
疑難排解 Amazon S3 檔案上傳錯誤 506
疑難排解無法讀取的檔名 506
ResourceNotFound例外疑難排 507
SFTP 連接器問題疑難排解 507
金鑰交涉失敗 507
其他 SFTP 連接器問題 508
疑難排解 AS2 問題 508
API 參考 509
歡迎 509
動作 511
CreateAccess 514
CreateAgreement 521
CreateConnector 527
CreateProfile 534
CreateServer 538

CreateUser 550
CreateWorkflow 558
DeleteAccess 566
DeleteAgreement 569
DeleteCertificate 572
DeleteConnector 574
DeleteHostKey 576
DeleteProfile 579
DeleteServer 581
DeleteSshPublicKey 584
DeleteUser 587
DeleteWorkflow 590
DescribeAccess 592
DescribeAgreement 596
DescribeCertificate 599
DescribeConnector 602
DescribeExecution 605
DescribeHostKey 610
DescribeProfile 613
DescribeSecurityPolicy 616
DescribeServer 620
DescribeUser 625
DescribeWorkflow 630
ImportCertificate 635
ImportHostKey 640
ImportSshPublicKey 644
ListAccesses 649
ListAgreements 653
ListCertificates 657
ListConnectors 660
ListExecutions 663
ListHostKeys 668
ListProfiles 672
ListSecurityPolicies 676
ListServers 680
ListTagsForResource 684

ListUsers 688
ListWorkflows 693
SendWorkflowStepState 696
StartDirectoryListing 699
StartFileTransfer 705
StartServer 711
StopServer 714
TagResource 717
TestConnection 720
TestIdentityProvider 724
UntagResource 731
UpdateAccess 734
UpdateAgreement 741
UpdateCertificate 746
UpdateConnector 750
UpdateHostKey 755
UpdateProfile 759
UpdateServer 762
UpdateUser 774
資料類型 781
As2ConnectorConfig 783
CopyStepDetails 787
CustomStepDetails 789
DecryptStepDetails 791
DeleteStepDetails 793
DescribedAccess 794
DescribedAgreement 797
DescribedCertificate 801
DescribedConnector 805
DescribedExecution 809
DescribedHostKey 812
DescribedProfile 815
DescribedSecurityPolicy 817
DescribedServer 820
DescribedUser 828
DescribedWorkflow 832

EfsFileLocation 834
EndpointDetails 835
ExecutionError 838
ExecutionResults 840
ExecutionStepResult 841
FileLocation 843
HomeDirectoryMapEntry 844
IdentityProviderDetails 846
InputFileLocation 848
ListedAccess 849
ListedAgreement 852
ListedCertificate 855
ListedConnector 858
ListedExecution 860
ListedHostKey 862
ListedProfile 864
ListedServer 866
ListedUser 869
ListedWorkflow 872
LoggingConfiguration 874
PosixProfile 875
ProtocolDetails 877
S3FileLocation 880
S3InputFileLocation 882
S3StorageOptions 884
S3Tag 885
ServiceMetadata 886
SftpConnectorConfig 887
SshPublicKey 889
Tag 891
TagStepDetails 892
UserDetails 894
WorkflowDetail 896
WorkflowDetails 898
WorkflowStep 900
提出 API 要求 902

Transfer Family 必要的要求標頭 902
Transfer Family 請求輸入和簽名 904
錯誤回應 904
可用程式庫 906
常見參數 907
常見錯誤 909
文件歷史紀錄 911
AWS 詞彙表 920
..... cmxxi

什麼是 AWS Transfer Family？

AWS Transfer Family 是一種安全的傳輸服務，可讓您將文件傳入和傳出 AWS 存儲服務。Transfer Family 是 AWS 雲端 平台的一部分。 AWS Transfer Family 為透過 SFTP、AS2、FTPS 和 FTP 直接傳入和傳出 Amazon S3 或 Amazon EFS 的檔案提供全受管支援。您可以維護用於驗證、存取和防火牆的現有用戶端設定，順暢地移轉、自動化和監控檔案傳輸工作流程，因此您的客戶、合作夥伴、內部團隊或其應用程式不會有任何變更。

請參閱入門 AWS以進一步了解並開始使用 Amazon Web Services 建置雲端應用程式。

AWS Transfer Family 支持從以下 AWS 存儲服務傳輸數據或傳輸數據。

- Amazon Simple Storage Service (Amazon S3) 存儲。如需 Amazon S3 的相關資訊，請參閱開始使用 Amazon 簡單儲存服務。
- Amazon Elastic File System (Amazon EFS) 網路檔案系統 (NFS) 檔案系統。如需 Amazon EFS 的相關資訊，請參閱什麼是 Amazon Elastic File System？

AWS Transfer Family 支持通過以下協議傳輸數據：

- 安全檔案傳輸通訊協定 (SFTP)：第 3 版

  官方的 IETF 文檔在這裡：SSH 文件傳輸協議 draft-ietf-secsh-filexfer -02.txt.
- 安全檔案傳輸通訊協定 (FTPS)
- 檔案傳輸通訊協定 (FTP)
- 適用性聲明 2 (AS2)

> **Note**
>
> 對於 FTP 和 FTPS 資料連線，傳輸系列用來建立資料通道的連接埠範圍為 8192—8200。

檔案傳輸通訊協定用於不同產業的資料交換工作流程，例如金融服務、醫療保健、廣告和零售等。「轉移族群」可簡化檔案傳輸工作流程至的移轉作 AWS業

以下是 Transfer Family 列與 Amazon S3 搭配使用的一些常見使用案例：

- 資料湖可 AWS 供從第三方 (例如廠商和合作夥伴) 上傳。

- 針對您客戶的訂閱類型資料分發。
- 您組織的內部傳輸。

以下是 Transfer Family 列與 Amazon EFS 搭配使用的一些常見使用案例：

- 資料分佈
- 供應鏈
- 內容管理
- Web 服務應用程式

以下是 Transfer Family 列與 AS2 搭配使用的一些常見使用案例：

- 符合法規要求的工作流程，仰賴通訊協定內建資料保護和安全性功能
- 供應鏈物流
- 付款流程
- B usiness-to-business (B2B) 交易
- 與企業資源規劃（ERP）和客戶關係管理（CRM）系統集成

有了 Transfer Family，您就可以存取已啟用檔案傳輸通訊協定的伺服器， AWS 而不需要執行任何伺服器基礎結構。您可以使用此服務將以檔案傳輸為基礎的工作流程移轉至， AWS 同時依原狀維護使用者的用戶端和設定。首先，您將主機名稱與伺服器端點建立關聯，然後新增使用者並提供適當的存取層級。執行此操作之後，您的使用者傳送要求就會直接從 Transfer Family 伺服器端點提供服務。

Transfer Family 列提供以下好處：

- 完全受管的服務，可即時擴展以符合您的需求。
- 您不需要修改應用程式或執行任何檔案傳輸通訊協定基礎結構。
- 將資料放在耐用的 Amazon S3 儲存中，您可以將原生用 AWS 服務 於處理、分析、報告、稽核和存檔功能。
- 使用 Amazon EFS 做為資料存放區，您將獲得可與 AWS 雲端 服務和現場部署資源搭配使用的全受管彈性檔案系統。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。這有助於消除佈建和管理容量以適應成長的需求。
- 完全受控的無伺服器檔案傳輸工作流程服務，可讓您輕鬆設定、執行、自動化和監控使用 AWS Transfer Family上傳檔案的處理。

- 沒有預付成本，您只需要為您的服務用量支付費用。

在以下各節中，您可以找到 Transfer Family 不同功能的說明、入門教學課程、如何設定不同啟用通訊協定的伺服器、如何使用不同類型的身分提供者，以及服務的 API 參考的詳細說明。

若要開始使用 Transfer Family，請參閱下列內容：

- 如何 AWS Transfer Family 工作
- 必要條件
- 開始使用 AWS Transfer Family 伺服器端點

如何 AWS Transfer Family 工作

AWS Transfer Family 這是一項全受管 AWS 服務，可用來透過下列協定將檔案傳入和傳出 Amazon 簡單儲存服務 (Amazon S3) 儲存或 Amazon 彈性檔案系統 (Amazon EFS) 檔案系統：

- 安全檔案傳輸通訊協定 (SFTP)：第 3 版

  官方的 IETF 文檔在這裡：SSH 文件傳輸協議 draft-ietf-secsh-filexfer -02.txt.
- 安全檔案傳輸通訊協定 (FTPS)
- 檔案傳輸通訊協定 (FTP)
- 適用性聲明 2 (AS2)

AWS Transfer Family 最多支援 3 個可用區域，並由 auto 擴展的備援叢集支援，適用於您的連線和傳輸要求。如需如何透過使用延遲型路由來建置更高冗餘並將網路延遲降至最低的範例，請參閱部落格文章將 SFTP 伺服器的 AWS 傳輸時的網路延遲降至最低。

Transfer Family 受管理的檔案傳輸工作流程 (MFTW) 是全受管、無伺服器檔案傳輸工作流程服務，可讓您輕鬆設定、執行、自動化和監控使用上傳檔案的處理。 AWS Transfer Family客戶可以使用 MFTW 自動執行各種處理步驟，例如複製、標記、掃描、篩選、壓縮/解壓縮，以及加密/解密使用 Transfer Family 傳輸的資料。這為追蹤和可稽核性提供端對端的可見性。如需詳細資訊，請參閱AWS Transfer Family 管理工作流。

AWS Transfer Family 支持任何標準文件傳輸協議客戶端。一些常用的客戶端如下：

- OpenSSH — 一個麥金塔和 Linux 命令列公用程式。
- WinSCP — 僅限視窗的圖形用戶端。

- 網絡鴨-一個 Linux，麥金塔和 Microsoft 視窗圖形客戶端。
- FileZilla— 一個 Linux, 麥金塔, 和視窗圖形客戶端.

AWS 提供以下 Transfer Family 工作坊。

- 建置檔案傳輸解決方案，利用 AWS Transfer Family 受管 SFP/FTPS 端點和 Amazon Cognito 和 DynamoDB 進行使用者管理。您可以在此處查看此工作坊的詳細信息。
- 在啟用 AS2 的情況下建立 Transfer Family 端點，以及 Transfer Family AS2 連接器您可以在這裡檢視此研討會的詳細資料。
- 建置解決方案，提供規範指引，並提供實驗室，協助您建置可擴充且安全的檔案傳輸架構， AWS 而不需要修改現有應用程式或管理伺服器基礎結構。您可以在此處查看此工作坊的詳細信息。

與 Transfer Family 相關的博客文章

下表列出包含「Transfer Family 列」客戶的實用資訊的部落格文章。該表格按時間順序反向排列，因此最近的帖子位於表格的開頭。

博客文章標題和鏈接	日期
使用 AWS Transfer Family SFTP 連接器和 PGP 加密架構安全且合規的受管理檔案傳輸	2024年5月16日
使用 Amazon Cognito 作為身份提供商 AWS Transfer Family 和 Amazon S3	2024 年 5 月 14 日
Transfer Family 如何協助您建置安全、合規的受管理檔案傳輸解決方案	2024 年 1 月 3 日
偵測惡意程式威脅 AWS Transfer Family	2023 年 7 月 20 日
擴充 SAP 工作負載， AWS Transfer Family	2023 年 7 月 13 日
使用 PGP 加密和解密文件 AWS Transfer Family	2023 年 6 月 21 日
AWS Transfer Family 使用 Azure 作用中目錄進行驗證，以及 AWS Lambda	2022 年 12 月 15 日

博客文章標題和鏈接	日期
使用 AWS Transfer Family 受管理工作流程自訂檔案傳遞	2022 年 10 月 14 日
使用工作流程建立雲端原生檔案傳輸平台 AWS Transfer Family	2022 年 1 月 5 日
透過 A AWS Transfer Family 和啟用使用者自助式金鑰管理 AWS Lambda。	2021 年 12 月 17 日
使用 AWS Transfer Family 和 Amazon S3 加強資料存取控制	2021 年 10 月 5 日
使用 AWS Global Accelerator 和 AWS Transfer Family 服務改善網際網路對向檔案傳輸的輸送量	2021 年 6 月 7 日
AWS Transfer Family 使用 AWS Web 應用程式防火牆和 Amazon API Gateway 進行保護	2021 年 5 月 5 日
AWS Transfer Family 使用 AWS Web 應用程式防火牆和 Amazon API Gateway 進行保護	2021 年 1 月 15 日
AWS Transfer Family 支援 Amazon Elastic File System	2021 年 1 月 7 日
啟用密碼驗證以便 AWS Transfer Family 使用 AWS Secrets Manager	2020 年 11 月 5 日
使用和集中資料存取 AWS Transfer FamilyAWS Storage Gateway	2020 年 6 月 22 日
在無伺服器應用程式 AWS Lambda 中使用 Amazon EFS	2020 年 6 月 18 日
使用 IP 允許清單來保護您的 AWS Transfer Family 伺服器	2020 年 4 月 8 日

博客文章標題和鏈接	日期
透過 AWS 傳輸 SFTP 伺服器，將網路延遲降至最低	2020 年 2 月 19 日
將 SFTP 伺服器移轉至 AWS	2020 年 2 月 12 日
使用 chroot 和邏輯目錄簡化您的 AWS SFTP 結構	2019 年 9 月 26 日
使用 Okta 做為身分識別提供者 AWS Transfer Family	2019 年 5 月 30 日

必要條件

下列各節說明使用 AWS Transfer Family 服務所需的先決條件。您至少需要建立 Amazon 簡單儲存服務 (Amazon S3) 儲存貯體，並透過 AWS Identity and Access Management (IAM) 角色提供該儲存貯體的存取權。您的角色也需要建立信任關係。這種信任關係允許 Transfer Family 擔任 IAM 角色來存取您的儲存貯體，以便為使用者的檔案傳輸請求提供服務。

主題

- 支援的 AWS 地區、端點和配額
- 註冊成為 AWS
- 設定要搭配使用的儲存區 AWS Transfer Family
- 建立 IAM 角色和政策

支援的 AWS 地區、端點和配額

若要以程式設計方式連線到 AWS 服務，請使用端點。例如，美國東部 (俄亥俄) 區域 (us-east-2) 的客戶端點為`transfer.us-east-2.amazonaws.com`。服務配額 (也稱為限制) 是您的服務資源或作業數目上限 AWS 帳戶。在本指南中，您可以在配額和中找到配額SFTP 連接器的配額。

如需有關支援的 AWS 區域、端點和服務配額的詳細資訊，請參閱AWS Transfer FamilyAmazon Web Services 一般參考.

註冊成為 AWS

當您註冊 Amazon Web Services (AWS) 時，您的 AWS 帳戶將自動註冊為中的所有服務 AWS，包括 AWS Transfer Family. 您只需支付實際使用服務的費用。

如果您已經有 AWS 帳號，請跳至下一個工作。若您尚未擁有 AWS 帳戶，請使用下列程序建立帳戶。

如果您沒有 AWS 帳戶，請完成以下步驟來建立一個。

若要註冊成為 AWS 帳戶

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

部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

當您註冊一個時 AWS 帳戶，將創建AWS 帳戶根使用者一個。根使用者有權存取該帳戶中的所有 AWS 服務 和資源。安全性最佳做法是將管理存取權指派給使用者，並僅使用 root 使用者來執行需要 root 使用者存取權的工作。

有關定價以及用 AWS Pricing Calculator 於估算 Transfer Family 成本的資訊，請參閱AWS Transfer Family 定價。

如需 AWS 區域可用性的AWS Transfer Family 相關資訊，請參閱 AWS 一般參考.

設定要搭配使用的儲存區 AWS Transfer Family

本主題說明您可以搭配使用的儲存選項 AWS Transfer Family。您可以使用 Amazon S3 或 Amazon EFS 做為 Transfer Family 伺服器的儲存。

內容

- 設定 Amazon S3 儲存貯體
  - Amazon S3 存取點
  - Amazon S3 HeadObject 行為
    - 授予僅寫入和列出檔案的能力
    - 造成延遲問題的大量零位元組物件
- 設定 Amazon EFS 檔案系統
  - Amazon EFS 檔案擁有
  - 為 Transfer Family 設定 Amazon EFS 使用者
    - 在 Amazon EFS 上設定 Transfer Family 使用者
    - 建立 Amazon EFS 根使用者
  - 支援 Amazon EFS 命令

設定 Amazon S3 儲存貯體

AWS Transfer Family 存取 Amazon S3 儲存貯體以服務使用者的傳輸請求，因此您需要提供 Amazon S3 儲存貯體，作為設定已啟用檔案傳輸協定的伺服器的一部分。您可以使用現有的儲存貯體，或是建立新的。

> **Note**
>
> 您不必使用位於相同 AWS 區域的伺服器和 Amazon S3 儲存貯體，但我們建議您使用此作為最佳實務。

設定使用者時，您可以為每個使用者指派一個 IAM 角色。此角色決定他們對 Amazon S3 儲存貯體的存取層級。

如需建立新儲存貯體的相關資訊，請參閱如何建立 S3 儲存貯體？ 在 Amazon 簡單存儲服務用戶指南。

> **Note**
>
> 您可以使用 Amazon S3 物件鎖定來防止物件遭到固定時間或無限期覆寫。這與 Transfer Family 的工作方式與其他服務相同。如果物件存在且受到保護，則不允許寫入該檔案或刪除該物件。如需 Amazon S3 物件鎖定的詳細資訊，請參閱 Amazon 簡單儲存服務使用者指南中的使用 Amazon S3 物件鎖定。

Amazon S3 存取點

AWS Transfer Family 支援 Amazon S3 存取點，這是 Amazon S3 的一項功能，可讓您輕鬆管理對共用資料集的精細存取。您可以在任何使用 S3 儲存貯體名稱的地方使用 S3 存取點別名。您可以在 Amazon S3 中為具有不同權限存取 Amazon S3 儲存貯體中共用資料的使用者建立數百個存取點。

例如，您可以使用存取點允許三個不同的團隊存取相同的共用資料集，其中一個團隊可以從 S3 讀取資料，第二個團隊可以將資料寫入 S3，第三個團隊可以從 S3 讀取、寫入和刪除資料。若要實作如上所述的精細存取控制，您可以建立 S3 存取點，其中包含可讓不同團隊非對稱存取權的政策。您可以將 S3 存取點與 Transfer Family 伺服器搭配使用，以實現精細的存取控制，而無需建立跨越數百個使用案例的複雜 S3 儲存貯體政策。若要進一步了解如何將 S3 存取點與 Transfer Family 伺服器搭配使用，請參閱使用AWS Transfer Family 和 Amazon S3 增強資料存取控制部落格文章。

> **Note**
>
> AWS Transfer Family 目前不支援 Amazon S3 多區域存取點。

Amazon S3 HeadObject 行為

> **Note**
>
> 當您建立或更新 Transfer Family 伺服器時，可以優化 Amazon S3 目錄的效能，進而消除`HeadObject`呼叫。

在 Amazon S3 中，儲存貯體與物件是主要資源，而且物件會存放在儲存貯體中。Amazon S3 可模擬階層式檔案系統，但有時可能與典型檔案系統的行為不同。例如，目錄不是 Amazon S3 中的一流概念，而是以物件金鑰為基礎。 AWS Transfer Family 透過將物件的索引鍵分割為正斜線字元 (/)，將最後一個元素視為檔案名稱，然後在相同路徑下將具有相同前置詞的檔案名稱群組在一起，來推斷目錄路徑。當您使用`mkdir`或使用 Amazon S3 主控台建立空目錄時，會建立零位元組物件來表示資料夾的路徑。這些物件的索引鍵會以尾端的正斜線結尾。這些零位元組物件的說明請參閱使用 Amazon S3 使用者指南中的資料夾在 Amazon S3 主控台中組織物件。

當您執行`ls`命令時，有些結果是 Amazon S3 零位元組物件 (這些物件具有以正斜線字元結尾的金鑰)，Transfer Family 會針對這些物件發出`HeadObject`要求 (請參閱 Amazon 簡單儲存服務 API 參考HeadObject中的詳細資訊)。使用 Amazon S3 做為 Transfer Family 列的儲存時，這可能會導致下列問題。

授予僅寫入和列出檔案的能力

在某些情況下，您可能只想提供對 Amazon S3 物件的寫入存取權。例如，您可能想要提供值區中寫入 (或上傳) 和列出物件的存取權，但不想要讀取 (下載) 物件。若要使用檔案傳輸用戶端執行`ls`和`mkdir`命令，您必須擁有 Amazon S3 `ListObjects` 和`PutObject`許可。但是，當 Transfer Family 需要對寫入或列出檔案進行呼`HeadObject`叫時，呼叫會失敗並顯示拒絕存取的錯誤，因為此呼叫需要`GetObject`權限。

> **Note**
>
> 當您建立或更新 Transfer Family 伺服器時，可以優化 Amazon S3 目錄的效能，進而消除`HeadObject`呼叫。

在此情況下，您可以新增 AWS Identity and Access Management (IAM) 政策條件來授予存取`GetObject`權，該條件僅針對以斜線 (/) 結尾的物件新增權限。這種情況可以防止對文件進行`GetObject`調用（以便無法讀取它們），但允許用戶列出和遍歷文件夾。下列範例政策僅提供對

Amazon S3 儲存貯體的寫入和列出存取。若要使用此政策，請*DOC-EXAMPLE-BUCKET*以儲存貯體的名稱取代。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowListing",
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
        },
        {
            "Sid": "AllowReadWrite",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
            ]
         },
      {
            "Sid": "DenyIfNotFolder",
            "Effect": "Deny",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "NotResource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*/"
            ]
         }
      ]
}
```

> **Note**
>
> 此原則不允許使用者附加檔案。換句話說，指派此原則的使用者無法開啟檔案來新增內容或修改檔案。此外，如果您的使用案例需要在上傳檔案之前進行`HeadObject`呼叫，則此原則不適用於您。

造成延遲問題的大量零位元組物件

如果您的 Amazon S3 儲存貯體包含大量這些零位元組物件，Transfer Family 會發出許多`HeadObject`呼叫，這可能會導致處理延遲。此問題的建議解決方案是啟用最佳化目錄以減少延遲。

例如，假設您進入您的主目錄，並且您有 10,000 個子目錄。換句話說，您的 Amazon S3 存儲桶有 10,000 個文件夾。在這個案例中，如果您執行 `ls` (list) 命令，清單作業需要六到八分鐘之間。但是，如果您最佳化您的目錄，此作業只需要幾秒鐘的時間。您可以在伺服器建立或更新程序期間，在「設定其他詳細資料」畫面中設定此選項。這些程序會在設定 SFTP、FTPS 或 FTP 伺服器端點主題下詳細說明。

> **Note**
>
> GUI 用戶端可能會在您的控制範圍之外發出`ls`指令，因此如果可以的話，請務必啟用此設定。

如果您不優化或無法優化目錄，則此問題的替代解決方案是刪除所有零字節對象。注意下列事項：

- 空目錄將不再存在。目錄僅因為名稱位於物件的索引鍵中而存在。
- 不會阻止某人再次打電話`mkdir`和破壞事情。您可以通過制定防止目錄創建的策略來緩解此問題。
- 某些情況下使用這些 0 字節的對象。例如，您有一個像/收件箱/客戶 1000 這樣的結構，並且每天都會清理收件箱目錄。

最後，還有一個可能的解決方案是限制政策條件中可見的物件數目，以減少`HeadObject`呼叫次數。為了使這是一個可行的解決方案，您需要接受，您可能只能查看有限的所有子目錄集。

設定 Amazon EFS 檔案系統

AWS Transfer Family 存取 Amazon Elastic File System (Amazon EFS) 來為使用者的傳輸請求提供服務。因此，在設定已啟用檔案傳輸通訊協定的伺服器時，您必須提供 Amazon EFS 檔案系統。您可以使用現有的檔案系統，也可以建立新檔案系統。

注意下列事項：

- 當您使用 Transfer Family 伺服器和 Amazon EFS 檔案系統時，伺服器和檔案系統必須位於相同的位置 AWS 區域。
- 伺服器和檔案系統不需要位於相同的帳戶中。如果伺服器和檔案系統不在同一個帳戶中，檔案系統策略必須將明確的權限授予使用者角色。

  如需如何設定多個帳戶的詳細資訊，請參閱AWS Organizations 使用者指南中的管理組織中的 AWS 帳戶。
- 設定使用者時，您可以為每個使用者指派一個 IAM 角色。此角色決定了他們對 Amazon EFS 檔案系統的存取層級。
- 如需掛接 Amazon EFS 檔案系統的詳細資訊，請參閱裝載 Amazon EFS 檔案系統。

如需 Amazon EFS 如何 AWS Transfer Family 協同運作的詳細資訊，請參閱 Amazon 彈性檔案系統使用 AWS Transfer Family 者指南中的使用存取 Amazon EFS 檔案系統中的檔案。

Amazon EFS 檔案擁有

Amazon EFS 使用可攜式作業系統界面 (POSIX) 檔案權限模型來代表檔案擁有權。

在 POSIX 中，系統中的使用者分為三個不同的權限類別：當您允許使用者使用存取儲存在 Amazon EFS 檔案系統中的檔案時 AWS Transfer Family，必須為他們指派「POSIX 設定檔」。此設定檔用於判斷其對 Amazon EFS 檔案系統中檔案和目錄的存取權限。

- 使用者 (u)：檔案或目錄的擁有者。通常，文件或目錄的創建者也是所有者。
- 群組 (g)：需要相同存取其共用檔案和目錄的使用者集合。
- 其他 (o)：除了擁有者和群組成員以外，可存取系統的所有其他使用者。此權限類別也稱為「公用」。

在 POSIX 權限模型中，每個檔案系統物件 (檔案、目錄、符號連結、命名管道和通訊端) 都與前面提到的三組權限相關聯。Amazon EFS 物件具有與其相關聯的 UNIX 樣式模式。此模式值定義了對該物件執行動作的許可。

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，物件由單一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。

為 Transfer Family 設定 Amazon EFS 使用者

在設定 Amazon EFS 使用者之前，您可以執行下列任一項作業：

- 您可以在 Amazon EFS 中建立使用者並設定其主資料夾。如需詳細資訊，請參閱 在 Amazon EFS 上設定 Transfer Family 使用者。
- 如果您想要新增 root 使用者，您可以建立 Amazon EFS 根使用者。

> **Note**
>
> Transfer Family 伺服器不支援 Amazon EFS 存取點來設定 POSIX 許可。Transfer Family 用戶的 POSIX 配置文件（在上一節中描述）提供設置 POSIX 權限的功能。這些權限是根據 UID、GID 和次要 gID 在使用者層級設定，以進行細微存取。

在 Amazon EFS 上設定 Transfer Family 使用者

Transfer Family 會將使用者對應至 UID/GID 和您指定的目錄。如果 UID/GID/ 目錄不存在於 EFS 中，則應先建立它們，然後再將它們指派給使用者。有關建立 Amazon EFS 使用者的詳細資訊，請參閱 Amazon Elastic File System 檔案系統使用者指南中的網路檔案系統 (NFS) 層級處理使用者、群組和許可。

在 Transfer Family 列中設定 Amazon EFS 使用者的步驟

1. 使用這些欄位，在「Transfer Family」中為您的使用者對應 EFS UID 和 GID。`PosixProfile`
2. 如果您希望使用者在登入時從特定資料夾啟動，可以在`HomeDirectory`欄位下指定 EFS 目錄。

您可以使用 CloudWatch 規則和 Lambda 函數將程序自動化。如需與 EFS 互動的 Lambda 函數範例，請參閱在無伺服器應用程式 AWS Lambda 中使用 Amazon EFS。

此外，您還可以為 Transfer Family 使用者設定邏輯目錄。如需詳細資訊，請參設定 Amazon EFS 的邏輯目錄閱使用邏輯目錄簡化您的 Transfer Family 目錄結構主題中的一節。

建立 Amazon EFS 根使用者

如果您的組織很適合您透過 SFTP/FTPS 啟用 root 使用者存取權以進行使用者的設定，您可以建立 UID 和 GID 為 0 的使用者 (root 使用者)，然後使用該 root 使用者建立資料夾並為其他使用者指派 POSIX ID 擁有者。此選項的優點是不需要掛載 Amazon EFS 檔案系統。

執行中所述的步驟新增 Amazon EFS 服務受管使用者，對於「使用者 ID」和「群組 ID」，輸入 0 (零)。

支援 Amazon EFS 命令

下列命令支援的 Amazon EFS AWS Transfer Family。

- `cd`
- `ls/dir`
- `pwd`
- `put`
- `get`
- `rename`
- `chown`：只有 root (即具有 uid=0 的使用者) 可以變更檔案和目錄的擁有權和權限。
- `chmod`：只有 root 可以更改文件和目錄的所有權和權限。
- `chgrp`：支援 root 或檔案擁有者，只能將檔案群組變更為其次要群組之一。
- `ln -s/symlink`
- `mkdir`
- `rm/delete`
- `rmdir`
- `chmtime`

建立 IAM 角色和政策

本主題說明可搭配使用的原則和角色類型 AWS Transfer Family，並逐步介紹建立使用者角色的程序。它也說明工作階段原則的運作方式，並提供範例使用者角色。

AWS Transfer Family 使用下列類型的角色：

- 使用者角色 — 允許服務管理的使用者存取必要的「Transfer Family」資源。 AWS Transfer Family 在「Transfer Family」使用者 ARN 的內容中擔任此角色。
- 存取角色 — 僅提供對正在傳輸的 Amazon S3 檔案的存取權。對於輸入 AS2 傳輸，存取角色使用 Amazon 資源名稱 (ARN) 作為協議。對於輸出 AS2 傳輸，存取角色會使用 ARN 作為連接器。

- 叫用角色 — 可搭配 Amazon API Gateway 作為伺服器的自訂身分提供者使用。「Transfer Family」會在「轉 Transfer Family」伺服器 ARN 的內容中擔任此角色。
- 記錄角色 — 用於將項目記錄到 Amazon CloudWatch。Transfer Family 會使用此角色記錄成功和失敗詳細資料，以及檔案傳輸的相關資訊。「Transfer Family」會在「轉 Transfer Family」伺服器 ARN 的內容中擔任此角色。對於輸出 AS2 傳輸，記錄角色會使用連接器 ARN。
- 執行角色 — 允許「Transfer Family」使用者呼叫和啟動工作流程。「Transfer Family」會在「Transfer Family」工作流程 ARN 的內容中擔任此角色。

除了這些角色之外，您也可以使用工作階段原則。會話策略用於在必要時限制訪問。請注意，這些原則是獨立的：也就是說，您不會將這些原則新增至角色。相反地，您可以直接將工作階段原則新增至「Transfer Family」使用者。

> **Note**
>
> 當您建立由服務管理的「Transfer Family」使用者時，可以選取「根據主資料夾自動產生原則」。如果您想限制用戶訪問自己的文件夾，這是一個有用的快捷方式。此外，您也可以檢視有關工作階段原則的詳細資訊以及中的範例工作階段原則的運作。您也可以在 IAM 使用者指南中的工作階段政策中找到有關工作階段政策的詳細資訊。

主題

- 建立使用者角色
- 工作階段原則的運作
- 讀/寫存取政策範例

建立使用者角色

建立使用者時，您會做出一些關於使用者存取權的決定。這些決策包括使用者可以存取哪些 Amazon S3 儲存貯體或 Amazon EFS 檔案系統、每個 Amazon S3 儲存貯體的哪些部分以及檔案系統中的哪些檔案可以存取，以及使用者擁有的許可 (例如，PUT或GET)。

若要設定存取權，您可以建立以身分識別為基礎的 AWS Identity and Access Management (IAM) 政策和角色，以提供該存取資訊。在此程序中，您可以為使用者提供 Amazon S3 儲存貯體或 Amazon EFS 檔案系統的存取權，該系統是檔案操作的目標或來源。若要執行此作業，請遵循下列高層級步驟，稍後會詳細進行說明：

建立使用者角色

1. 建立的 AWS Transfer Family身分與存取權管理政策 這在中有所描述若要為以下項目建立 IAM 政策 AWS Transfer Family。
2. 建立 IAM 角色並附加新的 IAM 政策。如需範例，請參閱讀/寫存取政策範例。
3. 在 AWS Transfer Family 和 IAM 角色之間建立信任關係。這在中有所描述建立信任關係。

下列程序說明如何建立 IAM 政策和角色。

若要為以下項目建立 IAM 政策 AWS Transfer Family

1. 在 https://console.aws.amazon.com/iam/ 中開啟 IAM 主控台。
2. 在導覽窗格中，選擇 Policies (政策)，然後選擇 Create policy (建立政策)。
3. 在 Create Policy (建立政策) 頁面上，選擇 JSON 標籤。
4. 在出現的編輯器中，將編輯器的內容取代為要附加到 IAM 角色的 IAM 政策。

   您可以授與讀取/寫入存取權，或限制使用者存取其主目錄。如需詳細資訊，請參閱 讀/寫存取政策範例。
5. 選擇 [檢閱原則] 並提供原則的名稱和說明，然後選擇 [建立原則]。

接下來，您會建立 IAM 角色並將新的 IAM 政策連接到它。

若要為以下項目建立 IAM 角色 AWS Transfer Family

1. 在導覽窗格中，選擇 Roles (角色)，然後選擇 Create role (建立角色)。

   在 [建立角色] 頁面上，確定已選取AWS 服務。
2. 從服務清單選擇 Transfer (傳輸)，然後選擇 Next: Permissions (下一步：許可)。這會在 AWS Transfer Family 和之間建立信任關係 AWS。
3. 在 [附加權限原則] 區段中，找出並選擇您剛建立的原則，然後選擇 [下一步：標籤]。
4. (選用) 輸入標籤的金鑰和值，然後選擇 Next: Review (下一步：檢閱)。
5. 在 Review (檢閱) 頁面上，輸入您新角色的名稱和描述，然後選擇 Create role (建立角色)。

接下來，您可以在 AWS Transfer Family 和之間建立信任關係 AWS。

建立信任關係

> **Note**
>
> 在我們的範例中，我們同時使用ArnLike和ArnEquals。它們在功能上是相同的，因此您可以在構建策略時使用任何一種。「Transfer Family」文件會在條件包含萬用字元ArnLike時使用，並ArnEquals指出完全相符的條件。

1. 在 IAM 主控台中，選擇您剛建立的角色。
2. 在 Summary (摘要) 頁面上，選擇 Trust relationships (信任關係)，然後選擇 Edit trust relationship (編輯信任關係)。
3. 在 「編輯信任關係」編輯器中，確定服務為"transfer.amazonaws.com"。訪問策略如下所示。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

建議您使用 aws:SourceAccount 和 aws:SourceArn 條件金鑰，保護自己免受混淆代理人問題的困擾。來源帳戶是伺服器的擁有者，而來源 ARN 是使用者的 ARN。例如：

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account_id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:transfer:region:account_id:user/*"
    }
}
```

如果您希望限制到特定服務器而不是用戶帳戶中的任何服務器，也可以使用該ArnLike條件。例如：

```
"Condition": {
    "ArnLike": {
        "aws:SourceArn": "arn:aws:transfer:region:account-id:user/server-id/*"
    }
}
```

> **Note**
>
> 在上面的例子中，用您自己的信息替換每個#######。

有關混淆的副問題和更多示例的詳細信息，請參閱預防跨服務混淆代理人。

4. 選擇 [更新信任原則] 以更新存取原則。

您現在已建立可 AWS Transfer Family 代表您呼叫 AWS 服務的 IAM 角色。您已將您建立的 IAM 政策附加至角色，以授予使用者存取權。在此開始使用 AWS Transfer Family 伺服器端點區段中，會將此角色和原則指派給您的一或多個使用者。

另請參閱

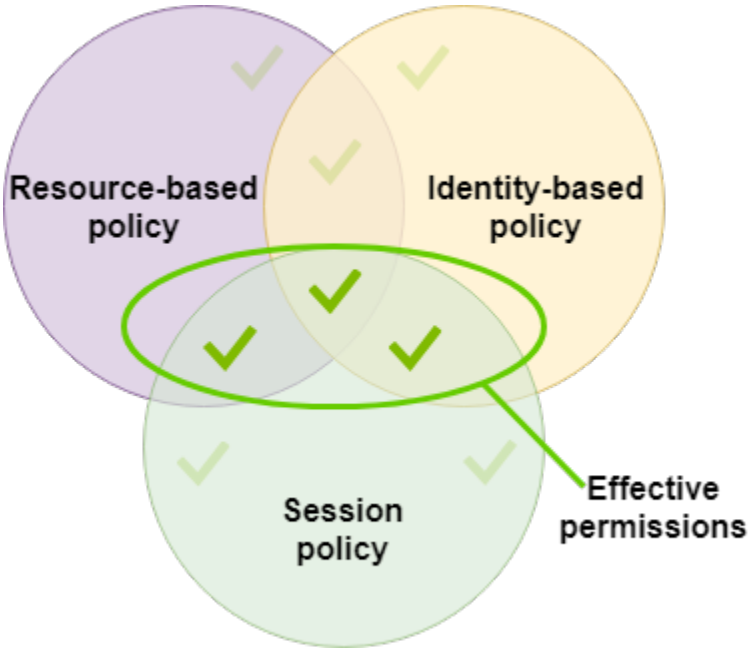
- 如需 IAM 角色的詳細一般資訊，請參閱 IAM 使用者指南中的建立角色以將許可委派給 AWS 服務。
- 若要進一步了解 Amazon S3 資源的身分型政策，請參閱 Amazon 簡單儲存服務使用者指南中的 Amazon S3 中的身分識別和存取管理。
- 若要進一步了解 Amazon EFS 資源的身分型政策，請參閱 Amazon 彈性檔案系統使用者指南中的使用 IAM 控制檔案系統資料存取。

工作階段原則的運作

當管理員建立角色時，角色通常會包含涵蓋多個使用案例或專案團隊成員的廣泛權限。如果管理員設定主控台 URL，則可以使用工作階段原則來降低結果工作階段的權限。例如，如果您建立具有讀取/寫入存取權的角色，您可以設定 URL 來限制使用者只能存取其主目錄。

工作階段原則是當您以程式設計方式為角色或使用者建立暫時工作階段時，作為參數傳遞的進階原則。工作階段政策對於鎖定使用者非常有用，以便他們只能存取物件首碼包含其使用者名稱的值區部分。下

圖顯示工作階段原則的權限是工作階段原則和以資源為基礎的原則的交集，以及工作階段原則和身分識別型原則的交集。



如需詳細資訊，請參閱 IAM 使用者指南中的工作階段政策。

在中 AWS Transfer Family，只有在您傳入 Amazon S3 或從 Amazon S3 傳輸時，才支援工作階段政策。下列範例原則是工作階段原則，僅限使用者存取其home目錄。注意下列事項：

- 只有在您需要啟用「跨帳戶存取」時，才需要GetObjectACL和對帳PutObjectACL單。也就是說，您的 Transfer Family 服務器需要訪問不同帳戶中的存儲桶。
- 工作階段原則的最大長度為 2048 個字元。如需詳細資訊，請參閱 API 參考資料中CreateUser動作的原則要求參數。
- 如果您的 Amazon S3 儲存貯體使用 AWS Key Management Service (AWS KMS) 加密，則必須在政策中指定其他許可。如需詳細資訊，請參閱 Amazon S3 中的資料加密。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowListingOfUserFolder",
            "Action": [
                "s3:ListBucket"
            ],
            "Effect": "Allow",
```

```
            "Resource": [
                "arn:aws:s3:::${transfer:HomeBucket}"
            ],
            "Condition": {
                "StringLike": {
                    "s3:prefix": [
                        "${transfer:HomeFolder}/*",
                        "${transfer:HomeFolder}"
                    ]
                }
            }
        },
        {
            "Sid": "HomeDirObjectAccess",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:GetObjectVersion",
                "s3:GetObjectACL",
                "s3:PutObjectACL"
            ],
            "Resource": "arn:aws:s3:::${transfer:HomeDirectory}/*"
        }
    ]
}
```

> **Note**
>
> 上述原則範例假設使用者的主目錄設定為包含尾隨斜線，表示該目錄為目錄。另一方面，如果您在沒有尾部斜杠的HomeDirectory情況下設置了用戶，那麼您應該將其作為策略的一部分包括在內。

在上一個範例原則中，請注意transfer:HomeFoldertransfer:HomeBucket、和transfer:HomeDirectory原則參數的使用。這些參數是針對HomeDirectory為使用者設定的設定，如HomeDirectory和中所述實作您的 API Gateway 方法。這些參數具有下列定義：

- transfer:HomeBucket參數會取代為的第一個元件HomeDirectory。

- transfer:HomeFolder參數會被參數的剩餘部分取HomeDirectory代。
- 該transfer:HomeDirectory參數已移除前導正斜線 (/)，以便在Resource陳述式中用作 S3 Amazon 資源名稱 (ARN) 的一部分。

> **Note**
>
> 如果您使用的是邏輯目錄 (也就是使用者homeDirectoryType是)，則不支援LOGICAL這些原則參數 (HomeBucketHomeDirectory、和HomeFolder)。

例如，假設為「Transfer Family」使用者設定的HomeDirectory參數為/home/bob/amazon/stuff/。

- transfer:HomeBucket設定為/home。
- transfer:HomeFolder設定為/bob/amazon/stuff/。
- transfer:HomeDirectory變成home/bob/amazon/stuff/。

第一個"Sid"允許用戶列出從開始的所有目錄/home/bob/amazon/stuff/。

第二個"Sid"限制了用戶put和get訪問相同的路徑，/home/bob/amazon/stuff/.

讀/寫存取政策範例

授與Amazon S3 儲存桶的讀取/寫入

下列範例政策 AWS Transfer Family 授與 Amazon S3 儲存貯體中物件的讀取/寫入存取權。

注意下列事項：

- 使用您 Amazon S3 儲存貯體的名稱來取代 *DOC-EXAMPLE-BUCKET*。
- 只有在您需要啟用「跨帳戶存取」時，才需要GetObjectACL和對帳PutObjectACL單。也就是說，您的 Transfer Family 服務器需要訪問不同帳戶中的存儲桶。
- 只有在正在存取的 Amazon S3 儲存貯體上啟用版本控制時，才需要GetObjectVersion和DeleteObjectVersion陳述式。

> **Note**
>
> 如果您曾經為儲存貯體啟用版本控制，則需要這些許可，因為您只能在 Amazon S3 中暫停版本控制，而不能完全關閉它。如需詳細資訊，請參閱未建立版本控制、啟用版本控制和版本控制暫停的值區。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowListingOfUserFolder",
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
            ]
        },
        {
            "Sid": "HomeDirObjectAccess",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:GetObjectVersion",
                "s3:GetObjectACL",
                "s3:PutObjectACL"
            ],
            "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
        }
    ]
}
```

授予檔案系統存取權限給 Amazon EFS 檔案系統中的檔案

> **Note**
>
> 除了該策略之外，您還必須確保您的 POSIX 文件權限授予適當的訪問權限。如需詳細資訊，請參閱《Amazon Elastic File System 使用者指南》中的使用網路檔案系統 (NFS) 層級的使用者、群組和許可。

下列範例政策授與根檔案系統存取 Amazon EFS 檔案系統中檔案的權限。

> **Note**
>
> 在下列範例中，請將*##*取代為您的區域、*## ID* 替換為檔案所在的帳戶，以及 *file-system-id*Amazon 彈性檔案系統 (Amazon EFS) 的 ID 取代。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RootFileSystemAccess",
            "Effect": "Allow",
            "Action": [
                "elasticfilesystem:ClientRootAccess",
                "elasticfilesystem:ClientMount",
                "elasticfilesystem:ClientWrite"
            ],
            "Resource": "arn:aws:elasticfilesystem:region:account-id:file-system/file-system-id"
        }
    ]
}
```

下列範例政策授予使用者檔案系統存取 Amazon EFS 檔案系統中檔案的權限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "UserFileSystemAccess",
            "Effect": "Allow",
```

```
            "Action": [
                "elasticfilesystem:ClientMount",
                "elasticfilesystem:ClientWrite"
            ],
            "Resource": "arn:aws:elasticfilesystem:region:account-id:file-system/file-system-id"
        }
    ]
}
```

Transfer Family 自學課

使用 AWS Transfer Family 者指南提供多種使用案例的詳細逐步解說。

- 開始使用 AWS Transfer Family 伺服器端點：本教學課程將逐步引導您建立 SFTP Transfer Family 伺服器和服務管理的使用者，然後說明如何使用用戶端傳輸檔案。
- 設定和使用 SFTP 連接器：本教學課程說明如何設定 SFTP 連接器，然後在 Amazon S3 儲存和 SFTP 伺服器之間傳輸檔案。
- 將 Amazon API Gateway 方法設定為自訂身分供應商：本教學課程說明如何設定 Amazon API Gateway 方法，並將其用作自訂身分供應商，將檔案上傳到 AWS Transfer Family 伺服器。
- 設定受管理的工作流程以解密檔案：本教學課程說明如何設定包含解密步驟的受管工作流程，以及如何將加密檔案上傳到 Amazon S3 儲存貯體，然後檢視解密的檔案。
- 設定 AS2 組態：本自學課程逐步介紹設定 AS2 Transfer Family 伺服器所需的步驟。這裡有匯入憑證、建立設定檔和合約、選擇性地建立 AS2 連接器，然後測試組態的指示。

主題

- 開始使用 AWS Transfer Family 伺服器端點
- 設定受管理的工作流程以解密檔案
- 設定和使用 SFTP 連接器
- 將 Amazon API Gateway 方法設定為自訂身分供應商
- 設定 AS2 組態

開始使用 AWS Transfer Family 伺服器端點

使用此自學課程可以開始使用 AWS Transfer Family (Transfer Family)。您將學習如何使用 Amazon S3 儲存建立具有可公開存取的端點啟用 SFTP 的伺服器、新增具有服務管理身份驗證的使用者，以及使用 Cyberduck 傳輸檔案。

主題

- 必要條件
- 步驟 1：登入 AWS Transfer Family 主控台
- 步驟 2：建立啟用 SFTP 的伺服器

- 步驟 3：新增服務受管理的使用者
- 步驟 4：使用用戶端傳輸檔案

必要條件

在開始之前，請務必完成中的需求必要條件。在此設定中，您可以建立 Amazon Simple Storage Service (Amazon S3) 儲存貯體和 AWS Identity and Access Management (IAM) 使用者角色。

使用 AWS Transfer Family 主控台需要許可，並且設定 Transfer Family 使用的其他 AWS 服務 (例如 Amazon 簡單儲存服務 AWS Certificate Manager、Amazon 彈性檔案系統和 Amazon Route 53) 時需要許可。例如，對於使用傳輸系列傳入和傳出檔案的 AWS 使用者，AmazonS3 會FullAccess授予設定和使用 Amazon S3 儲存貯體的許可。建立 Amazon S3 儲存貯體需要此政策中的某些許可。

若要使用「Transfer Family」主控台，您需要下列項目：

- AWSTransferConsoleFullAccess授予 SFTP 使用者建立 Transfer Family 資源的權限。
- 只有當您希望 Transfer Family 在 Amazon Lo CloudWatch gs 中為伺服器自動建立記錄角色，或是為登入伺服器的使用者建立使用者角色時，才需要 IAM FullAccess (或特別是允許建立 IAM 角色的政策)。
- 要創建和刪除 VPC 服務器類型，您需要將操作 ec2：CreateVpc端點和 ec2：DeleteVpc端點添加到策略中。

> **Note**
>
> 亞馬遜 S3 FullAccess 和 IAM FullAccess 政策本身並不需要一般使用. AWS Transfer Family這裡會以簡單的方式呈現，以確保涵蓋您需要的所有權限。此外，這些是 AWS 受管理的政策，也就是可供所有 AWS 客戶使用的標準政策。您可以檢視這些原則中的個別權限，並決定您的目的所需的最小權限集。

步驟 1：登入 AWS Transfer Family 主控台

若要登入以 Transfer Family

1. 請登入 AWS Management Console 並開啟 AWS Transfer Family 主控台，網址為 https://console.aws.amazon.com/transfer/。
2. 對於帳戶 ID 或別名，請輸入您的 ID AWS 帳戶。

3. 對於 IAM 使用者名稱，請輸入您為 Transfer Family 建立的使用者角色名稱。
4. 在「密碼」中，輸入您的 AWS 帳戶密碼。
5. 選擇 Sign In (登入)。

步驟 2：建立啟用 SFTP 的伺服器

安全殼層 (SSH) 檔案傳輸通訊協定 (SFTP) 是用於透過網際網路安全傳輸資料的網路通訊協定。該協議支持 SSH 的完整安全性和身份驗證功能。它廣泛用於交換數據，包括金融服務，醫療保健，零售和廣告等各種行業的業務合作夥伴之間的敏感信息。

若要建立已啟用 SFTP 的伺服器

1. 從功能窗格中選取伺服器，然後選擇建立伺服器。
2. 在 [選擇通訊協定] 中選取 [SFTP]，然後選擇 [下一步]。
3. 在 [選擇身分識別提供者] 中，選擇 [Transfer Family] 中的 [受管理以儲存使用者身分識別和金鑰的服務]，然後選
4. 在 [選擇端點] 中，執行下列動作：
   a. 對於端點類型，請選擇可公開存取的端點類型。
   b. 對於自訂主機名稱，請選擇無。
   c. 選擇下一步。
5. 在 [選擇網域] 中，選擇 Amazon S3。
6. 在設定其他詳細資料中，針對密碼編譯演算法選項，選擇包含伺服器啟用的加密演算法的安全性原則。我們最新的安全性政策為預設值：如需詳細資訊，請參閱AWS Transfer Family 伺服器的安全性原則。

   > **Note**
   >
   > 只有當您為伺服器新增受管理的工作流程時，請選擇 [建立新角色以進行CloudWatch記錄]。若要記錄伺服器事件，您不需要建立 IAM 角色。

7. 在 [檢閱並建立] 中選擇 [建立伺服器]。系統會將您帶到「伺服器」頁面。

新伺服器的狀態變更為「線上」可能需要幾分鐘的時間。此時，您的伺服器可以執行檔案作業，但您必須先建立使用者。如需建立使用者的詳細資訊，請參閱管理伺服器端點的使用者。

步驟 3：新增服務受管理的使用者

將使用者新增至啟用 SFTP 的伺服器

1. 在 [伺服器] 頁面上，選取要新增使用者的伺服器。
2. 選擇新增使用者。
3. 在 [使用者設定] 區段中，輸入使用者名稱做為使用者名稱。此使用者名稱必須至少為 3 個字元且最多 100 個字元。您可以在使用者名稱中使用下列字元：a—z、A-Z、0—9、底線 '_'、連字號 '-'、句號 ' 。 '和符號 (@)。使用者名稱不能以連字號、句點或位於符號開頭。
4. 對於「存取」，請選擇您在中建立的 IAM 角色建立 IAM 角色和政策。此 IAM 角色包括 IAM 政策，其中包含存取 Amazon S3 儲存貯體的許可，以及與 AWS Transfer Family 服務之間的信任關係。中概述的程序建立信任關係顯示了如何建立適當的信任關係。
5. 針對「策略」，選擇「無」。
6. 對於主目錄，請選擇您要用來存放傳輸資料的 Amazon S3 儲存貯體 AWS Transfer Family。輸入home目錄的路徑。這是您的使用者使用其用戶端登入時所看到的目錄。

   建議您使用包含使用者名稱的目錄路徑，以便您可以選擇使用工作階段原則。工作階段政策會限制使用者在 Amazon S3 儲存貯體中存取該使用者home目錄的權限。如需使用工作階段原則的詳細資訊，請參閱工作階段原則的運作。

   如果您願意，您可以將此參數保留空白，以使用 Amazon S3 儲存貯體的`root`目錄。如果選擇此選項，請確保您的 IAM 角色可提供`root`目錄的存取權。
7. 選取 [受限制] 核取方塊可防止使用者存取其home目錄以外的任何內容。這也可以防止使用者看到 Amazon S3 儲存貯體名稱或資料夾名稱。
8. 對於 SSH 公開金鑰，請以`ssh-rsa` *`<string>`*格式輸入安全殼層 key pair 的公開安全殼層金鑰部分。

   您的金鑰必須經過服務驗證，才能新增新使用者。如需如何產生 SSH key pair 的詳細資訊，請參閱為服務管理的使用者產生 SSH 金鑰。
9. (選擇性) 在「機碼和值」中，輸入一或多個標籤作為鍵值配對，然後選擇「新增標籤」。
10. 選擇 Add (新增) 將新使用者新增至您選擇的伺服器。

    新使用者會顯示在 [伺服器詳細資訊] 頁面的 [使用者] 區段中。

步驟 4：使用用戶端傳輸檔案

您可以透過在用戶端中指定傳輸作業，透過 AWS Transfer Family 服務傳輸檔案。 AWS Transfer Family 支持多個客戶端。如需詳細資訊，請參閱使用用戶端透過伺服器端點傳輸檔案

本節包含使用網路鴨和 OpenSSH 的程序。

主題

- 使用網路鴨
- 使用 OpenSSH

使用網路鴨

AWS Transfer Family 使用網絡鴨傳輸文件

1. 打開網絡鴨客戶端。
2. 選擇「開啟連線」。
3. 在「開啟連線」對話方塊中，選擇「SFTP (SSH 檔案傳輸通訊協定)」。
4. 在伺服器中，輸入您的伺服器端點。伺服器端點位於 [伺服器詳細資訊] 頁面上，請參閱檢視 SFTP、FTP 伺服器和 FTP 伺服器的詳細資訊。
5. 針對「連接埠號碼」，輸入 **22** SFTP。
6. 針對 Username (使用者名稱)，輸入您在管理伺服器端點的使用者中建立的使用者名稱。
7. 對於 SSH 私密金鑰，請選擇或輸入安全殼層私密金鑰。
8. 選擇連線。
9. 執行檔案傳輸。

   根據檔案所在位置，執行以下其中一項：

   - 在本機目錄 (來源) 中，選擇要傳輸的檔案，然後將檔案拖放到 Amazon S3 目錄 (目標)。
   - 在 Amazon S3 目錄 (來源) 中，選擇要傳輸的檔案，然後將檔案拖放到本機目錄 (目標) 中。

使用 OpenSSH

使用下列說明使用 OpenSSH 從命令列傳輸檔案。

> **Note**
>
> 此用戶端僅適用於啟用 SFTP 的伺服器。

若要使用 OpenSSH 命令列公 AWS Transfer Family 用程式來傳輸檔案

1. 在 Linux 或 Macintosh 上，開啟命令終端機。
2. 在提示符下，輸入以下命令：`% sftp -i transfer-key sftp_user@service_endpoint`

   在前面的命令中，`sftp_user`是用戶名，`transfer-key`是 SSH 私鑰。這裡`service_endpoint`是所選伺服器的 AWS Transfer Family 主控台中所示的伺服器端點。

   應會出現 `sftp` 提示。
3. (選擇性) 若要檢視使用者的主目錄，請在提示下輸入下列命`sftp`令：`sftp> pwd`
4. 在下一行中，輸入下列文字：`sftp> cd /mybucket/home/sftp_user`

   在這個開始的練習中，此 Amazon S3 儲存貯體是檔案傳輸的目標。
5. 在下一行中，輸入下列命令：`sftp> put filename.txt`

   該`put`命令會將檔案傳輸到 Amazon S3 儲存貯體。

   即會顯示類似下面的訊息，指出正在傳輸檔案或已完成。

   ```
   Uploading filename.txt to /my-bucket/home/sftp_user/filename.txt

   some-file.txt 100% 127 0.1KB/s 00:00
   ```

設定受管理的工作流程以解密檔案

本教學課程說明如何設定包含解密步驟的受管理工作流程。本教學也會示範如何將加密檔案上傳到 Amazon S3 儲存貯體，然後檢視該儲存貯體中的解密檔案。

> **Note**
>
> AWS 存儲博客有一篇文章，描述瞭如何簡單地解密文件而不使用 Transfer Family 託管工作流程編寫任何代碼，使用 PGP 和 AWS Transfer Family.

主題

- 步驟 1：設定執行角色
- 步驟 2：建立受管理的工作流程
- 步驟 3：將工作流程新增至伺服器並建立使用者
- 步驟 4：建立 PGP key pair
- 步驟 5：將 PGP 私鑰存儲在 AWS Secrets Manager
- 步驟 6：加密檔案
- 步驟 7：執行工作流程並檢視結果

步驟 1：設定執行角色

建立 Transfer Family 可用來啟動工作流程的 AWS Identity and Access Management (IAM) 執行角色。建立執行角色的程序如中所述工作流程的 IAM 政策。

> **Note**
>
> 在建立執行角色時，請務必在執行角色與「Transfer Family」之間建立信任關係，如中所述建立信任關係。

下列執行角色原則包含啟動您在本教學課程中建立之工作流程所需的所有必要權限。若要使用此範例政策，請以您自己的資訊取代 *user input placeholders*。以您上傳加密檔案的 Amazon S3 儲存貯體名稱取DOC-EXAMPLE-BUCKET代。

> **Note**
>
> 並非每個工作流程都需要此範例中列出的每個權限。您可以根據特定工作流程中的步驟類型來限制權限。每個預先定義步驟類型所需的權限會在中說明使用預定義步驟。自訂步驟所需的權限在中說明自訂步驟的 IAM 許可。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "WorkflowsS3Permissions",
```

```
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectTagging",
                "s3:GetObjectVersion",
                "s3:PutObject",
                "s3:PutObjectTagging",
                "s3:ListBucket",
                "s3:PutObjectTagging",
                "s3:PutObjectVersionTagging",
                "s3:DeleteObjectVersion",
                "s3:DeleteObject"
            ],
            "Resource": ["arn:aws:s3:::DOC-EXAMPLE-BUCKET/*",
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET"]
            "Condition": {
                "StringEquals": {
                    "s3:RequestObjectTag/Archive": "yes"
                }
            }
        },
        {
            "Sid": "DecryptSecret",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/transfer/
*"
        }
    ]
}
```

步驟 2：建立受管理的工作流程

現在您需要建立包含解密步驟的工作流程。

若要建立包含解密步驟的工作流程

1. 請在以下位置開啟 AWS Transfer Family 主控台。 https://console.aws.amazon.com/transfer/
2. 在左側導覽窗格中，選擇 [工作流程]，然後選擇 [建立工作流程]。
3. 輸入下列詳細資訊：

- 輸入說明，例如**Decrypt workflow example**。
- 在「標稱步驟」區段中，選擇「新增步驟」。

4. 針對 [選擇步驟類型] 選擇 [解密檔案]，然後選擇 [下一步]。
5. 在「設定參數」對話方塊中，指定下列項目：

   - 輸入描述性步驟名稱，例如**decrypt-step**。步驟名稱中不允許使用空格。
   - 對於解密檔案的目的地，請選擇 Amazon S3。
   - 對於目的地儲存貯體名稱，選擇您在步驟 1 中建立的 IAM 政策DOC-EXAMPLE-BUCKET中指定的相同 Amazon S3 儲存貯體。
   - 針對「目的地 key prefix」，輸入您要在目的地值區中儲存解密檔案的前置字元 (資料夾) 名稱，**decrypted-files/**例如。

     > **Note**
     >
     > 確保在前綴中添加尾隨斜杠（**/**）。

   - 在此自學課程中，請清除「覆寫現有的」。如果清除此設定，如果您嘗試解密具有與現有檔案相同名稱的檔案，工作流程處理會停止，且不會處理新檔案。

   選擇 [下一步] 以移至檢閱畫面。
6. 檢閱步驟的詳細資訊。如果一切正確，請選擇 [建立步驟]。
7. 您的工作流程只需要單一解密步驟，因此不需要設定其他步驟。選擇 [建立工作流程] 以建立新工作流程。

記下新工作流程的工作流程 ID。在下一步中，您將需要此 ID。本教學課程使用*w-1234abcd5678efghi*做為工作流程 ID 範例。

步驟 3：將工作流程新增至伺服器並建立使用者

現在您已經有了解密步驟的工作流程，您必須將其與「Transfer Family」伺服器建立關聯。本自學課程展示如何將工作流程貼附至現有的 Transfer Family 伺服器。或者，您也可以建立新的伺服器來搭配工作流程使用。

將工作流程附加到伺服器之後，您必須建立一個可以 SFTP 到伺服器的使用者，並觸發工作流程以執行。

規劃 Transfer Family 伺服器以執行工作流程的步驟

1. 請在以下位置開啟 AWS Transfer Family 主控台。 https://console.aws.amazon.com/transfer/
2. 在左側導覽窗格中，選擇 [伺服器]，然後從清單中選擇伺服器。請確定此伺服器支援 SFTP 通訊協定。
3. 在伺服器的詳細資訊頁面上，向下捲動至 [其他詳細資料] 區段，然後選擇 [編輯]。
4. 在 [編輯其他詳細資料] 頁面的 [受管理的工作流程] 區段中，選擇您的工作流程，然後選擇對應的執行角色。
   - 對於完整檔案上傳的工作流程，請選擇您在中建立的工作流程步驟 2：建立受管理的工作流程，例如，**w-1234abcd5678efghi**。
   - 對於受管工作流程執行角色，請選擇您在中建立的 IAM 角色步驟 1：設定執行角色。
5. 捲動至頁面底部，然後選擇 [儲存] 以儲存變更。

請記下您使用之伺服器的 ID。您用來儲存 PGP 金鑰的 AWS Secrets Manager 密碼名稱部分取決於伺服器 ID。

若要新增可觸發工作流程的使用者

1. 請在以下位置開啟 AWS Transfer Family 主控台。 https://console.aws.amazon.com/transfer/
2. 在左側導覽窗格中，選擇 [伺服器]，然後選擇要用於解密工作流程的伺服器。
3. 在伺服器詳細資訊頁面上，向下捲動至「使用者」區段，然後選擇「新增使用者」。
4. 針對您的新使用者，請輸入下列詳細資訊：
   - 對於 User name (使用者名稱)，請輸入 **decrypt-user**。
   - 在 [角色] 中，選擇可存取您伺服器的使用者角色。
   - 對於主目錄，請選擇您先前使用的 Amazon S3 儲存貯體，例如DOC-EXAMPLE-BUCKET。
   - 如果是 SSH 公開金鑰，請貼上與您擁有的私密金鑰對應的公開金鑰。如需詳細資訊，請參閱 為服務管理的使用者產生 SSH 金鑰。
5. 選擇 [新增] 以儲存您的新使用者。

請記下此伺服器的 Transfer Family 使用者名稱。密碼部分取決於使用者的名稱。為了簡單起見，本教程使用了可以由服務器的任何用戶使用的默認密鑰。

步驟 4：建立 PGP key pair

使用其中一個支援的 PGP 用戶端來產生 PGP key pair。此程序會在中詳細說明產生 PGP 金鑰。

若要產生 PGP key pair

1. 在本教學課程中，您可以使用 gpg (GnuPG) 版本 2.0.22 用戶端來產生使用 RSA 做為加密演算法的 PGP key pair。對於此客戶端，運行以下命令，並提供電子郵件地址和密碼。您可以使用任何您喜歡的名稱或電子郵件地址。請務必記住您使用的值，因為您稍後需要在自學課程中輸入這些值。

   ```
   gpg --gen-key
   ```

   > **Note**
   >
   > 如果您使用的是 2.3.0 或更高GnuPG版本，則必須運行`gpg --full-gen-key`。當系統提示您輸入要建立的金鑰類型時，請選擇 RSA 或 ECC。但是，如果您選擇 ECC，請務必BrainPool為橢圓曲線選擇NIST或。不要選擇Curve 25519。

2. 執行下列命令以匯出私密金鑰。*user@example.com*以產生金鑰時使用的電子郵件地址取代。

   ```
   gpg --output workflow-tutorial-key.pgp --armor --export-secret-key user@example.com
   ```

   這個命令會將私密金鑰匯出到**workflow-tutorial-key.pgp**檔案中。您可以將輸出檔案命名為任何您喜歡的名稱。您也可以在將私密金鑰檔案新增至之後刪除該檔案 AWS Secrets Manager。

步驟 5：將 PGP 私鑰存儲在 AWS Secrets Manager

您需要以非常特定的方式將私密金鑰儲存在 Secrets Manager 中，以便工作流程在上傳的檔案上執行解密步驟時，工作流程才能找到私密金鑰。

> **Note**
>
> 當您將密碼儲存在「Secrets Manager 中時， AWS 帳戶 會產生費用。如需定價的資訊，請參閱 AWS Secrets Manager 定價。

在密碼管理員中儲存 PGP 私密金鑰

1. 請登入 AWS Management Console 並開啟 AWS Secrets Manager 主控台，網址為 https://console.aws.amazon.com/secretsmanager/。
2. 在左側導覽窗格中，選擇秘密。
3. 在「密碼」頁面上，選擇「儲存新密碼」。
4. 在 [選擇密碼類型] 頁面上，對於 [密碼類型]，選擇 [其他密碼類型]。
5. 在「鍵/值對」區段中，選擇「鍵/值」標籤。
   - 鍵-輸入**PGPPrivateKey**。
   - value — 將私鑰的文本粘貼到值字段中。
6. 選擇添加行，然後在「鍵/值對」部分中，選擇「鍵/值」選項卡。
   - 鍵-輸入**PGPPassphrase**。
   - value — 輸入您在中產生 PGP key pair 時所使用的複雜密碼。步驟 4：建立 PGP key pair
7. 選擇下一步。
8. 在 [設定密碼] 頁面上，輸入密碼的名稱和說明。您可以為特定使用者或可供所有使用者使用的密碼建立密碼。如果您的服務器 ID 是 *s-11112222333344445*，則按如下方式命名密碼。
   - 若要為所有使用者建立預設密碼，請為密碼命名**aws/transfer/*s-11112222333344445*/@pgp-default**。
   - 若只要為先前建立的使用者建立密碼，請為密碼命名**aws/transfer/*s-11112222333344445*/decrypt-user**。
9. 選擇 [下一步]，然後接受 [設定旋轉] 頁面上的預設值。然後選擇下一步。
10. 在「檢閱」頁面上，選擇「儲存」以建立並儲存密碼。

如需將 PGP 私密金鑰新增至 Secrets Manager 的詳細資訊，請參閱用 AWS Secrets Manager 來儲存您的 PGP 金鑰。

步驟 6：加密檔案

使用此gpg程式加密檔案，以便在工作流程中使用。執行下列命令來加密檔案：

```
gpg -e -r marymajor@example.com --openpgp testfile.txt
```

執行此命令之前，請注意下列事項：

- 對於-r引數，請*marymajor@example.com*以建立 PGP key pair 時使用的電子郵件地址取代。
- 該--openpgp標誌是可選的。這個旗標可讓加密的檔案符合 RFC4880 標準。
- 此指令會在與之相同的**testfile.txt.gpg**位置建立一個名為的檔案**testfile.txt**。

步驟 7：執行工作流程並檢視結果

若要執行工作流程，請使用您在步驟 3 中建立的使用者連接至「Transfer Family」伺服器。然後，您可以查看在步驟 2.5 中指定的 Amazon S3 儲存貯體，設定目標參數以查看解密的檔案。

執行解密工作流程

1. 開啟命令終端機。
2. 運行以下命令，*your-endpoint*替換為實際端點以及*transfer-key*用戶的 SSH 私鑰：

   ```
   sftp -i transfer-key decrypt-user@your-endpoint
   ```

   例如，如果私鑰存儲在中~/.ssh/decrypt-user，而您的端點是s-11112222333344445.server.transfer.us-east-2.amazonaws.com，則命令如下：

   ```
   sftp -i  ~/.ssh/decrypt-user decrypt-user@s-11112222333344445.server.transfer.us-east-2.amazonaws.com
   ```

3. 執行 pwd 命令。如果成功，此命令將返回以下內容：

   ```
   Remote working directory: /DOC-EXAMPLE-BUCKET/decrypt-user
   ```

   您的目錄會反映您的 Amazon S3 儲存貯體的名稱。
4. 執行下列命令以上傳檔案並觸發工作流程以執行：

   ```
   put testfile.txt.gpg
   ```

5. 對於解密檔案的目的地，您在建立工作流程時指定了decrypted-files/資料夾。現在，您可以導航到該文件夾並列出內容。

   ```
   cd ../decrypted-files/
   ls
   ```

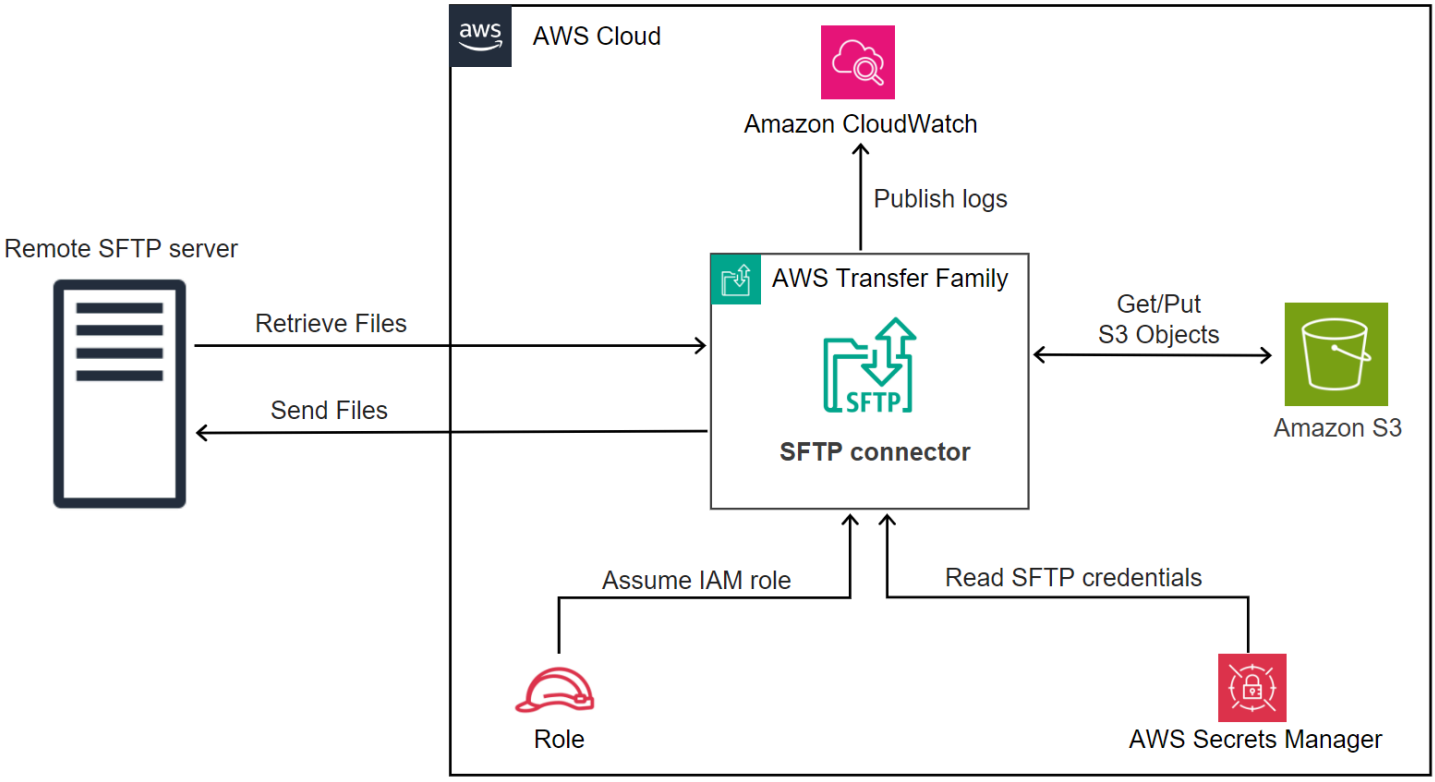
如果成功，該`ls`命令將列出該`testfile.txt`文件。您可以下載此檔案，並確認它與您之前加密的原始檔案相同。

設定和使用 SFTP 連接器

連接器的目的是在 AWS 儲存裝置與合作夥伴的 SFTP 伺服器之間建立關係。您可以將檔案從 Amazon S3 傳送到合作夥伴擁有的外部目的地。您也可以使用 SFTP 連接器從合作夥伴的 SFTP 伺服器擷取檔案。

本教學課程說明如何設定 SFTP 連接器，然後在 Amazon S3 儲存和 SFTP 伺服器之間傳輸檔案。

SFTP 連接器會從中擷取 SFTP 認證， AWS Secrets Manager 以驗證到遠端 SFTP 伺服器並建立連線。連接器會將檔案傳送到遠端伺服器或從遠端伺服器擷取檔案，並將檔案存放在 Amazon S3 中。IAM 角色是用來允許存取 Amazon S3 儲存貯體以及存放在 Secrets Manager 中的登入資料。你可以登錄到 Amazon CloudWatch。



下列部落格文章提供使用 SFTP 連接器建立 MFT 工作流程的參考架構，包括在使用 SFTP 連接器將檔案傳送至遠端 SFTP 伺服器之前先使用 PGP 加密檔案：使用 SFTP 連接器和 PGP 加[密架構安全且符合規範的受管理檔案傳輸](#)。 AWS Transfer Family

主題

- 步驟 1：建立必要的輔助資源
- 步驟 2：建立並測試 SFTP 連接器
- 步驟 3：使用 SFTP 連接器傳送和擷取檔案
- 建立 Transfer Family 伺服器做為遠端 SFTP 伺服器的程序

步驟 1：建立必要的輔助資源

您可以使用 SFTP 連接器在 Amazon S3 和任何遠端 SFTP 伺服器之間複製檔案。在本教程中，我們使用 AWS Transfer Family 服務器作為我們的遠程 SFTP 服務器。我們需要創建和配置以下資源：

- 建立 Amazon S3 儲存貯體以將檔案存放在您的 AWS 環境中，以及從遠端 SFTP 伺服器傳送和擷取檔案：創建 Amazon S3 存儲桶。
- 建立用於存取 Amazon S3 儲存的 AWS Identity and Access Management 角色，以及我們在秘密管理員中的秘密：建立具有必要權限的 IAM 角色。
- 建立使用 SFTP 通訊協定的 Transfer Family 伺服器，以及使用 SFTP 連接器在 SFTP 伺服器之間傳輸檔案的服務管理使用者：。建立 Transfer Family SFTP 伺服器和使用者
- 建立 AWS Secrets Manager 密碼，以儲存 SFTP 連接器用來登入遠端 SFTP 伺服器的認證：。在中建立並儲存密碼 AWS Secrets Manager

創建 Amazon S3 存儲桶

建立 Amazon S3 儲存貯體

1. 請在以下位置登入 AWS Transfer Family 主控台：https://console.aws.amazon.com/s3/。
2. 選擇「區域」並輸入名稱。

   在本教學課程中，我們的儲存貯體位於中**US East (N. Virginia) us-east-1**，名稱為**sftp-server-storage-east**。
3. 接受預設值，然後選擇 [建立值區]。

如需建立 Amazon S3 儲存貯體的完整詳細資訊，請參閱如何建立 S3 儲存貯體？ 在 Amazon 簡單存儲服務用戶指南。

建立具有必要權限的 IAM 角色

針對存取角色，建立具有下列權限的原則。

下列範例授與必要的權限，以存取 Amazon S3 中的*## EXAMPLE* 儲存貯體，以及存放在秘 Secrets Manager 中的指定密碼。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
        "Sid": "AllowListingOfUserFolder",
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
        ]
    },
    {
        "Sid": "HomeDirObjectAccess",
        "Effect": "Allow",
        "Action": [
            "s3:PutObject",
            "s3:GetObject",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion",
            "s3:GetObjectVersion",
            "s3:GetObjectACL",
            "s3:PutObjectACL"
        ],
        "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
    },
    {
        "Sid": "GetConnectorSecretValue",
        "Effect": "Allow",
        "Action": [
            "secretsmanager:GetSecretValue"
        ],
        "Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/
transfer/SecretName-6RandomCharacters"
```

```
    }
  ]
}
```

取代項目，如下所示：

- 對於*########*程使用。**s3-storage-east**
- 對於*##*，自學課程會使用**us-east-1**。
- 對於*## ID*，請使用您的 AWS 帳戶 ID。
- 對於 *SecretName-6 RandomCharacters*，我們是**using sftp-connector1**名字（您將擁有自己的六個隨機字符作為秘密）。

您也必須確定此角色包含信任關係，可讓連接器在為使用者的傳輸要求提供服務時存取您的資源。如需建立信任關係的詳細資訊，請參閱建立信任關係。

> **Note**
>
> 要查看我們在本教程中使用的角色的詳細信息，請參閱結合使用者和存取角色。

在中建立並儲存密碼 AWS Secrets Manager

我們需要在 Secrets Manager 器中存儲密碼，以存儲 SFTP 連接器的用戶憑據。您可以使用密碼、SSH 私密金鑰，或同時使用兩者。在本教程中，我們使用的是私鑰。

> **Note**
>
> 當您將密碼儲存在「Secrets Manager 中時， AWS 帳戶 會產生費用。如需定價的資訊，請參閱 AWS Secrets Manager 定價。

在開始存儲密鑰的過程之前，請檢索並格式化您的私鑰。私密金鑰必須對應於遠端 SFTP 伺服器上為使用者設定的公開金鑰。在我們的教程中，私鑰必須對應於我們用作遠程服務器的 Transfer Family SFTP 服務器上為測試用戶存儲的公鑰。

若要這麼做，請執行下列命令：

```
jq -sR . path-to-private-key-file
```

例如，如果您的私密金鑰檔案位於中~/.ssh/sftp-testuser-privatekey，則指令如下所示。

```
jq -sR . ~/.ssh/sftp-testuser-privatekey
```

這會以正確的格式（帶有嵌入換行符）將密鑰輸出到標準輸出。將此文本複製到某個地方，因為您需要將其粘貼到以下過程中（在步驟 6 中）。

若要將使用者認證儲存在 SFTP 連接器的 Secrets Manager 中

1. 請登入 AWS Management Console 並開啟 AWS Secrets Manager 主控台，網址為 https://console.aws.amazon.com/secretsmanager/。
2. 在左側導覽窗格中，選擇秘密。
3. 在「密碼」頁面上，選擇「儲存新密碼」。
4. 在 [選擇密碼類型] 頁面上，對於 [密碼類型]，選擇 [其他密碼類型]。
5. 在「鍵/值對」區段中，選擇「鍵/值」標籤。
   - 鍵-輸入**Username**。
   - 值 — 輸入我們的使用者名稱**sftp-testuser**。
6. 若要輸入金鑰，建議您使用「純文字」頁籤。
   a. 選擇「新增列」，然後輸入**PrivateKey**。
   b. 選擇「純文字」標籤。此欄位現在包含下列文字：

      ```
      {"Username":"sftp-testuser","PrivateKey":""}
      ```

   c. 在空雙引號（「」）之間粘貼私鑰的文本（以前保存）。

      您的屏幕應如下所示（關鍵數據顯示為灰色）。

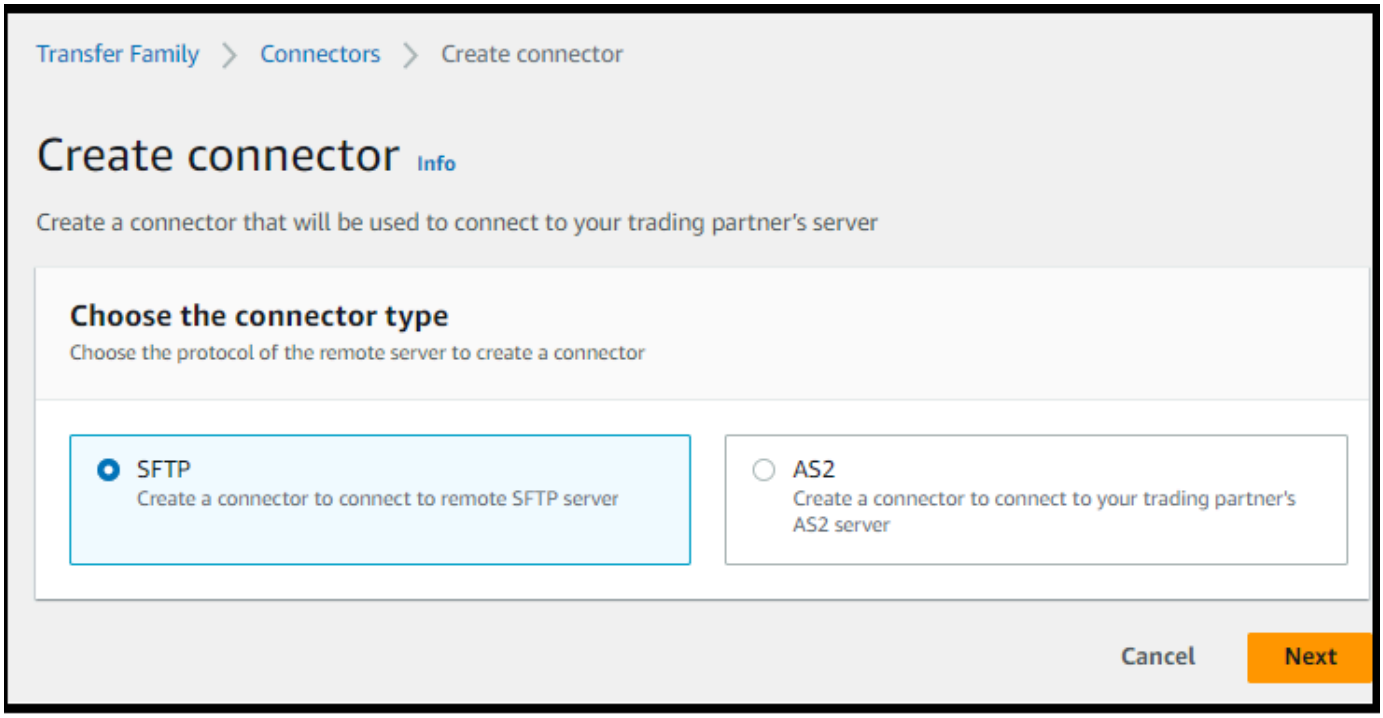
7. 選擇下一步。
8. 在 [設定密碼] 頁面上，輸入密碼的名稱。在本自學課程中，我們將秘密命名為名稱**aws/transfer/sftp-connector1**。
9. 選擇 [下一步]，然後接受 [設定旋轉] 頁面上的預設值。然後選擇下一步。
10. 在「檢閱」頁面上，選擇「儲存」以建立並儲存密碼。

步驟 2：建立並測試 SFTP 連接器

在本節中，我們會建立 SFTP 連接器，該連接器會使用先前建立的所有資源。如需詳細資訊，請參閱設定 SFTP 連接器。

若要建立 SFTP 連接器

1. 開啟主 AWS Transfer Family 控台，網址為 https://console.aws.amazon.com/transfer/。
2. 在左側導覽窗格中，選擇「連接器」，然後選擇「建立連接器」。
3. 為連接器類型選擇 SFTP 以建立 SFTP 連接器，然後選擇 [下一步]。



4. 在 [連接器組態] 區段中，提供下列資訊：

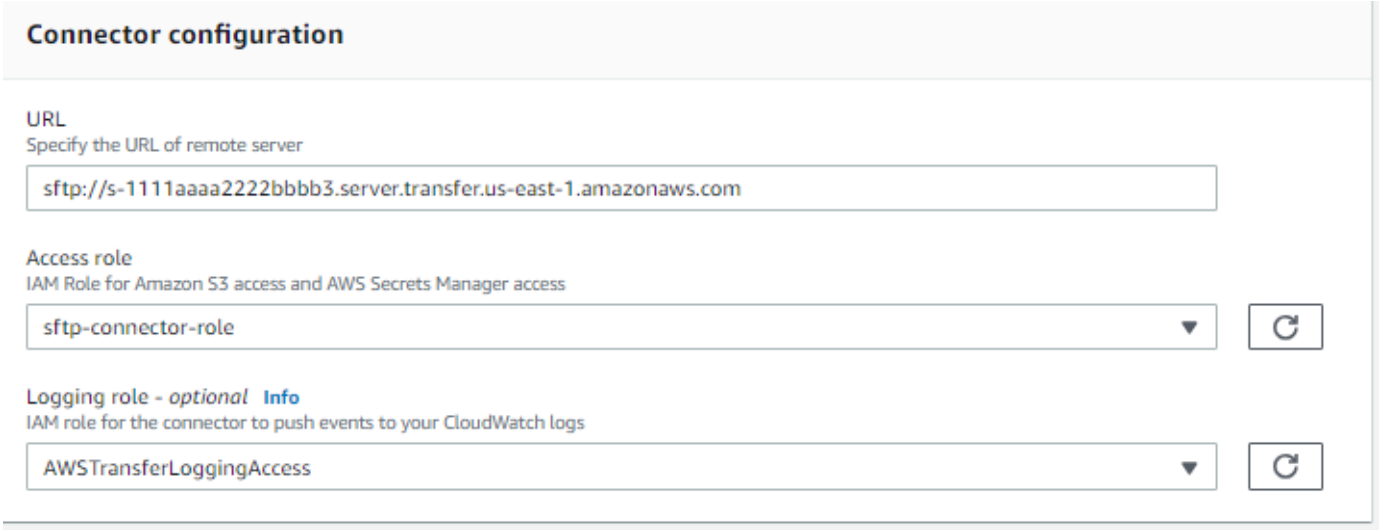
   - 對於網址，請輸入遠端 SFTP 伺服器的網址。在本教程中，我們輸入我們用作遠程 SFTP 服務器的 Transfer Family 服務器的 URL。

     ```
     sftp://s-1111aaaa2222bbbb3.server.transfer.us-east-1.amazonaws.com
     ```

     使用您*# Transfer Family ########*

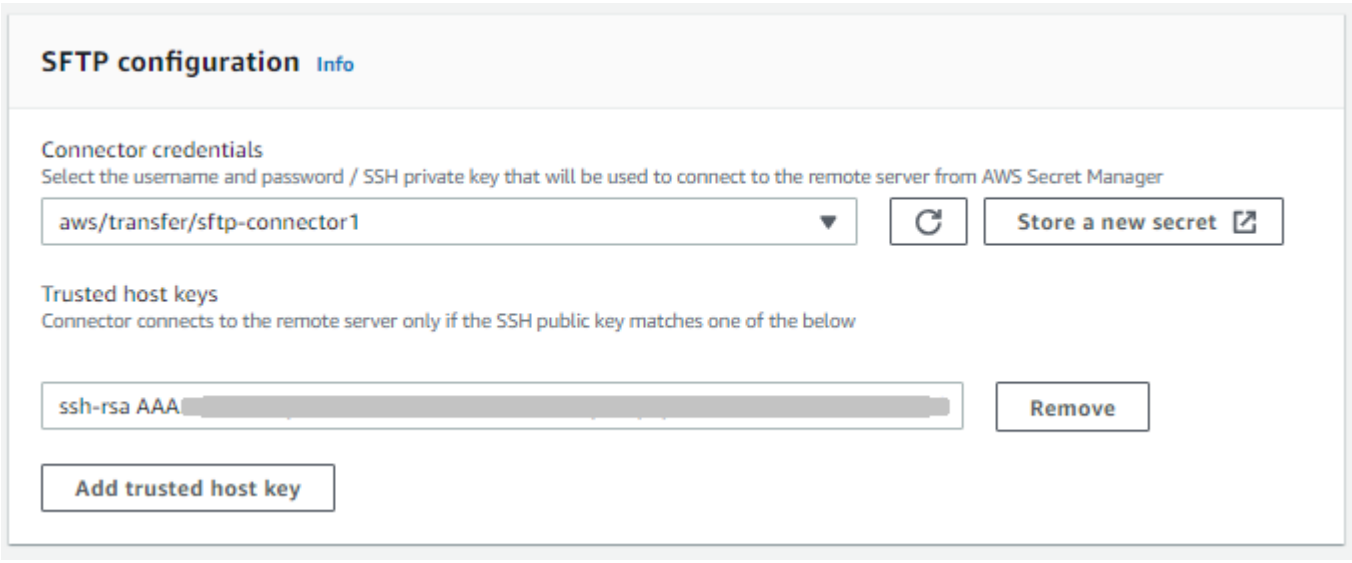
   - 對於 Access 角色，請輸入我們先前建立的角色**sftp-connector-role**。
   - 對於「記錄日誌」角色，請選擇**AWSTransferLoggingAccess**。

     > **Note**
     >
     > AWSTransferLoggingAccess 是 AWS 受管理的策略。此政策在中有詳細描述AWS 受管理的策略： AWSTransferLoggingAccess。



5. 在「SFTP 組態」區段中，提供下列資訊：

   - 對於連接器認證，請選擇包含 SFTP 認證的 Secrets Manager 資源名稱。對於教學課程，請選擇**aws/transfer/sftp-connector1**。
   - 對於受信任的主機金鑰，請貼到主機金鑰的公開部分。您可以透過針對 SFTP 伺服器執`ssh-keyscan`行來擷取此金鑰。如需有關如何格式化和儲存受信任主機金鑰的詳細資訊，請參閱SftpConnectorConfig資料類型文件。



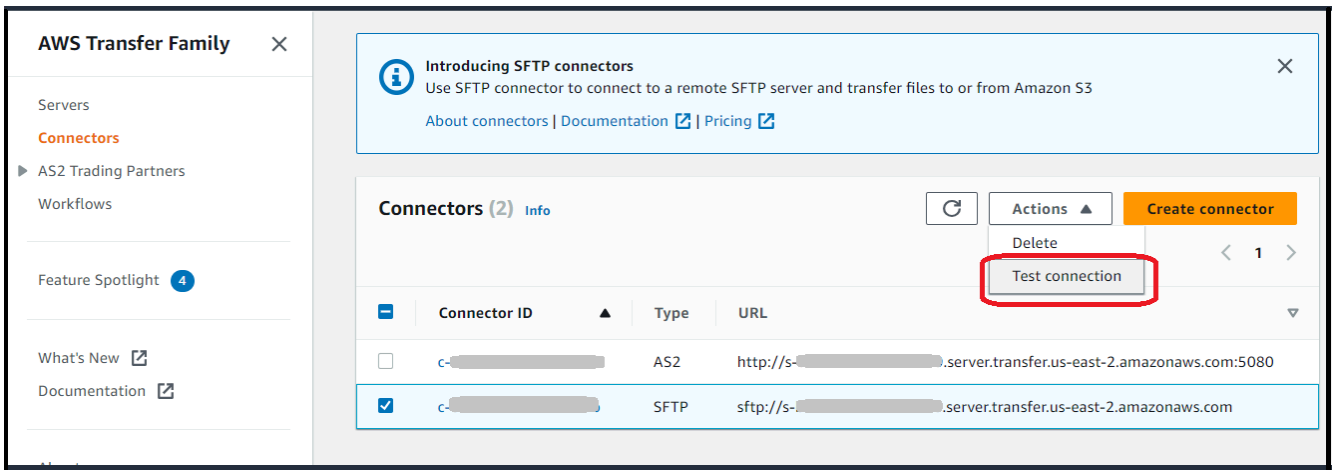
6. 確認所有設定後，請選擇 [建立連接器] 以建立 SFTP 連接器。

建立 SFTP 連接器之後，建議您先對其進行測試，然後再嘗試使用新連接器傳輸任何檔案。

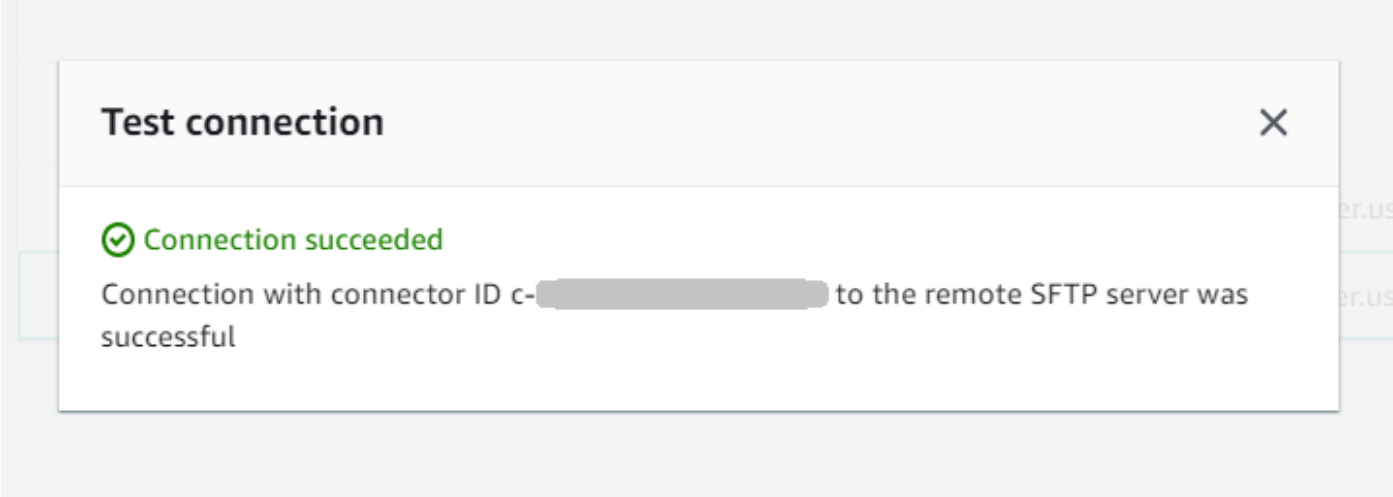
Test a connector using the console

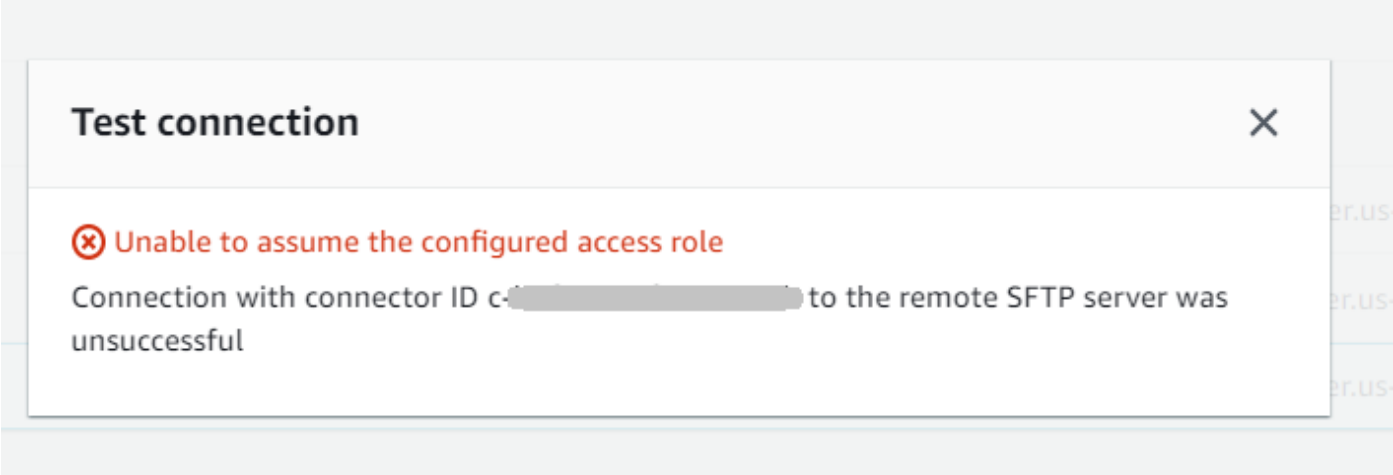
若要測試 SFTP 連接器

1. 開啟主 AWS Transfer Family 控台，網址為 https://console.aws.amazon.com/transfer/。
2. 在左側導覽窗格中，選擇 [連接器]，然後選取連接器。
3. 從「動作」功能表中，選擇「測試連線」。



系統返回一條消息，指示測試是通過還是失敗。如果測試失敗，系統會根據測試失敗的原因提供錯誤訊息。





Test a connector using the CLI

若要使用測試連接器 AWS Command Line Interface，請在命令提示字元中執行下列命令 (以實際的*###############*)：

```
aws transfer test-connection --connector-id c-connector-id
```

如果測試成功，則返回以下幾行：

```
{
   "Status": "OK",
   "StatusMessage": "Connection succeeded"
}
```

如果測試失敗，您會收到描述性錯誤訊息，例如：

```
{
   "Status": "ERROR",
   "StatusMessage": "Unable to assume the configured access role"
}
```

步驟 3：使用 SFTP 連接器傳送和擷取檔案

為了簡單起見，我們假設您的 Amazon S3 儲存貯體中已有檔案。

> **Note**
>
> 本教學針對來源和目的地儲存位置使用 Amazon S3 儲存貯體。如果您的 SFTP 伺服器不使用 Amazon S3 儲存，則無論您在以下命令`sftp-server-storage-east`中看到的任何位置，都可以使用可從 SFTP 伺服器存取的檔案位置路徑來取代路徑。

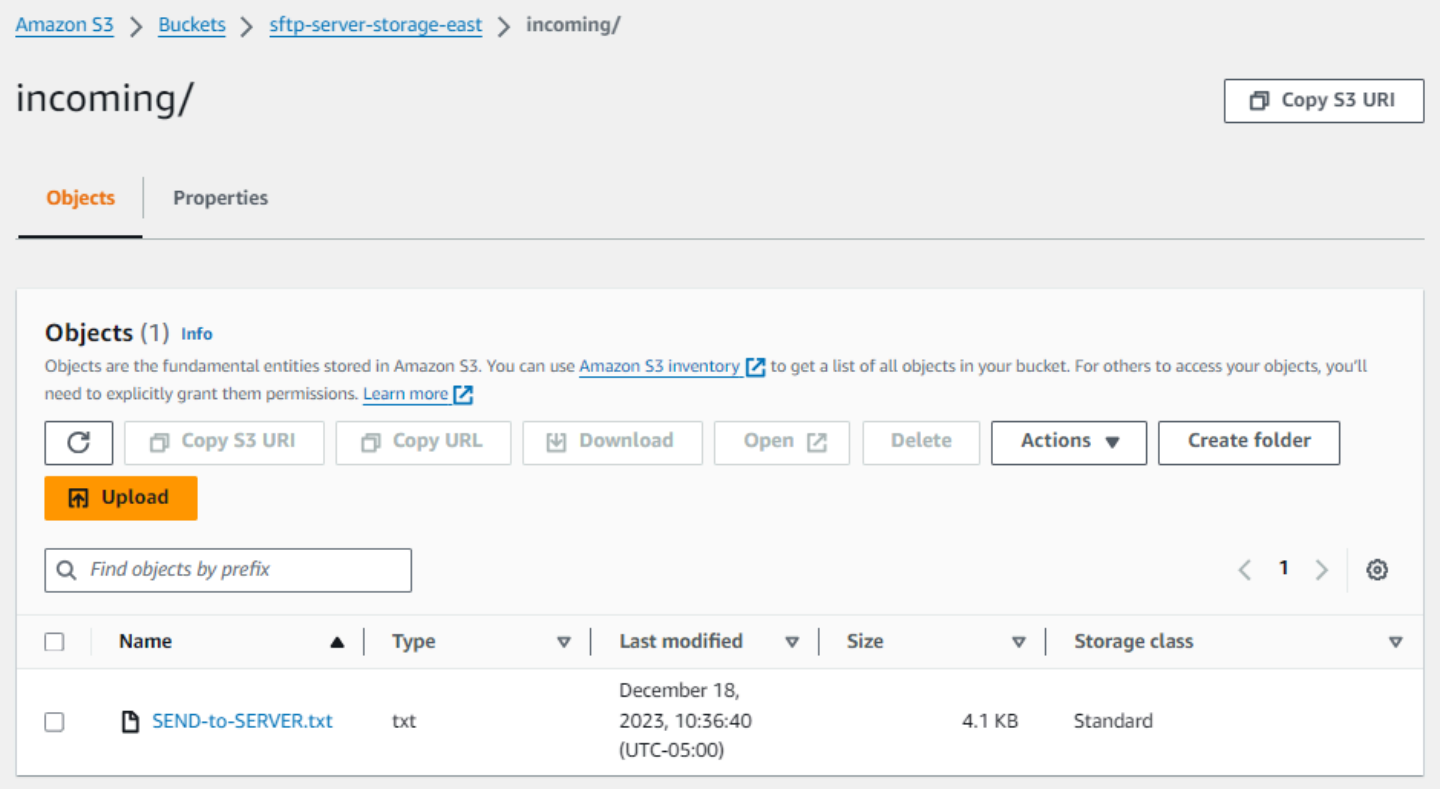
- 我們將`SEND-to-SERVER.txt`從 Amazon S3 存儲命名的文件發送到 SFTP 服務器。
- 我們會將`RETRIEVE-to-S3.txt`從 SFTP 伺服器命名的檔案擷取到 Amazon S3 儲存。

> **Note**
>
> 在下列指令中，將*############## ID*。

首先，我們將檔案從 Amazon S3 儲存貯體傳送到遠端 SFTP 伺服器。從命令提示字元執行下列命令：

```
aws transfer start-file-transfer --connector-id c-connector-id --send-file-paths "/s3-
storage-east/SEND-to-SERVER.txt" /
   --remote-directory-path "/sftp-server-storage-east/incoming"
```

您的`sftp-server-storage-east`桶現在應該看起來像這樣。



如果您看不到預期的檔案，請檢查記 CloudWatch 錄檔。

若要檢查您的 CloudWatch 記錄

1. 打開 Amazon CloudWatch 控制台 https://console.aws.amazon.com/cloudwatch/
2. 從左側導覽功能表中選取 [記錄群組]。
3. 在搜尋列中輸入您的連接器 ID，以尋找您的記錄。
4. 選取從搜尋傳回的記錄資料流。
5. 展開最新的記錄項目。

如果成功，記錄項目會如下所示：

```
{
    "operation": "SEND",
    "timestamp": "2023-12-18T15:26:57.346283Z",
    "connector-id": "connector-id",
    "transfer-id": "transfer-id",
    "file-transfer-id": "transfer-id/file-transfer-id",
    "url": "sftp://server-id.server.transfer.us-east-1.amazonaws.com",
    "file-path": "/s3-storage-east/SEND-to-SERVER.txt",
```

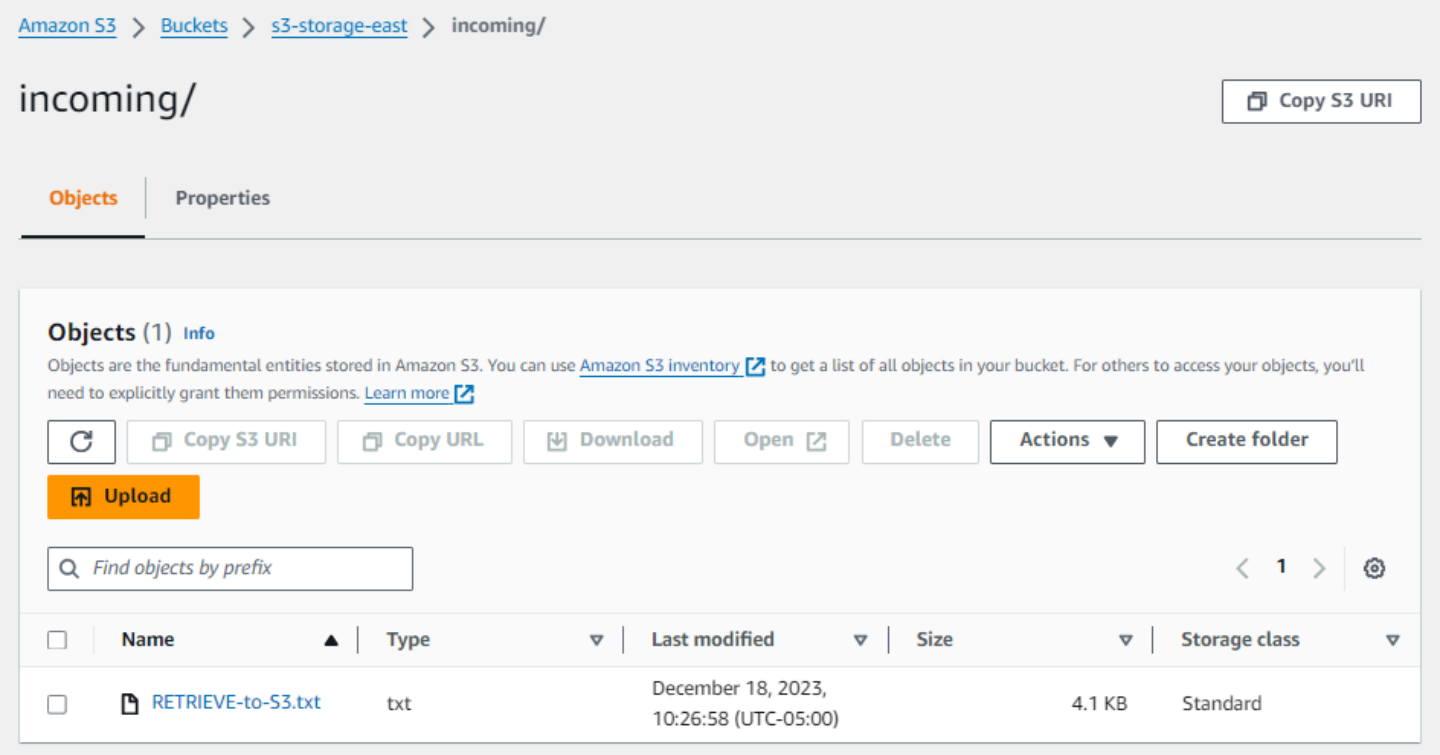
```
    "status-code": "COMPLETED",
    "start-time": "2023-12-18T15:26:56.915864Z",
    "end-time": "2023-12-18T15:26:57.298122Z",
    "account-id": "500655546075",
    "connector-arn": "arn:aws:transfer:us-east-1:500655546075:connector/connector-id",
    "remote-directory-path": "/sftp-server-storage-east/incoming"
}
```

如果檔案傳輸失敗，記錄項目會包含指定問題的錯誤訊息。發生錯誤的常見原因是 IAM 許可和不正確的檔案路徑發生問題。

接下來，我們將檔案從 SFTP 伺服器擷取到 Amazon S3 儲存貯體。從命令提示字元執行下列命令：

```
aws transfer start-file-transfer --connector-id c-connector-id --retrieve-file-paths "/sftp-server-storage-east/RETRIEVE-to-S3.txt" --local-directory-path "/s3-storage-east/incoming"
```

如果傳輸成功，您的 Amazon S3 儲存貯體會包含傳輸的檔案，如下所示。



如果成功，記錄項目會如下所示：

```
{
    "operation": "RETRIEVE",
```

```
    "timestamp": "2023-12-18T15:36:40.017800Z",
    "connector-id": "c-connector-id",
    "transfer-id": "transfer-id",
    "file-transfer-id": "transfer-id/file-transfer-id",
    "url": "sftp://s-server-id.server.transfer.us-east-1.amazonaws.com",
    "file-path": "/sftp-server-storage-east/RETRIEVE-to-S3.txt",
    "status-code": "COMPLETED",
    "start-time": "2023-12-18T15:36:39.727626Z",
    "end-time": "2023-12-18T15:36:39.895726Z",
    "account-id": "500655546075",
    "connector-arn": "arn:aws:transfer:us-east-1:500655546075:connector/c-connector-
id",
    "local-directory-path": "/s3-storage-east/incoming"
}
```

建立 Transfer Family 伺服器做為遠端 SFTP 伺服器的程序

接下來，我們概述了創建一個 Transfer Family 服務器作為本教程的遠程 SFTP 服務器的步驟。注意下列事項：

- 我們使用 Transfer Family 服務器來代表遠程 SFTP 服務器。典型的 SFTP 連接器使用者擁有自己的遠端 SFTP 伺服器。請參閱建立 Transfer Family SFTP 伺服器和使用者。
- 因為我們使用的是 Transfer Family 伺服器，所以我們也使用服務管理的 SFTP 使用者。此外，為了簡單起見，我們將此使用者存取 Transfer Family 伺服器所需的權限與使用連接器所需的權限結合在一起。同樣地，大多數 SFTP 連接器使用案例都有一個與 Transfer Family 伺服器無關聯的獨立 SFTP 使用者。請參閱建立 Transfer Family SFTP 伺服器和使用者。
- 在本教學中，由於我們將 Amazon S3 儲存用於遠端 SFTP 伺服器，因此我們需要建立第二個儲存貯體**s3-storage-east**，以便我們可以將檔案從一個儲存貯體傳輸到另一個儲存貯體。

建立 Transfer Family SFTP 伺服器和使用者

大多數使用者不需要建立 Transfer Family SFTP 伺服器和使用者，因為您已經擁有 SFTP 伺服器與使用者，而且您可以使用此伺服器來傳送檔案。但是，在本教程中，為了簡單起見，我們使用 Transfer Family 服務器作為遠程 SFTP 服務器。

按照中所述的步驟建立啟用 SFTP 的伺服器來建立伺服器並新步驟 3：新增服務受管理的使用者增使用者。這些是我們在本教程中使用的用戶詳細信息：

- 建立您的服務管理使用者。`sftp-testuser`

  - 將主目錄設定為 /sftp-server-storage-east/sftp-testuser
  - 當您建立使用者時，您會儲存公開金鑰。稍後，當您在 Secret Manager 中建立密碼時，您需要提供對應的私密金鑰。
- 角色：sftp-connector-role. 在本教學課程中，我們為 SFTP 使用者和存取 SFTP 連接器使用相同的 IAM 角色。當您為組織建立連接器時，您可能會有個別的使用者和存取角色。
- 伺服器主機金鑰：您需要在建立連接器時使用伺服器主機金鑰。您可以通過ssh-keyscan為服務器運行來檢索此密鑰。例如，如果您的伺服器 ID 為s-1111aaaa2222bbbb3，且其端點位於中us-east-1，則下列命令會擷取伺服器主機金鑰：

  ```
  ssh-keyscan s-1111aaaa2222bbbb3.server.transfer.us-east-1.amazonaws.com
  ```

  將此文本複製到某個地方，因為您需要將其粘貼到該步驟 2：建立並測試 SFTP 連接器過程中。

結合使用者和存取角色

在本教學課程中，我們使用單一的組合角色。我們將此角色用於 SFTP 使用者以及存取連接器。下列範例包含此角色的詳細資訊，以便您想要執行教學課程中的工作。

下列範例授予存取 Amazon S3 中兩個儲存貯體的必要許可，以及aws/transfer/sftp-connector1存放在秘 Secrets Manager 中名為的密碼。在教學課程中，此角色被命名為sftp-connector-role。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowListingOfUserFolder",
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::sftp-server-storage-east",
                "arn:aws:s3:::s3-storage-east"
            ]
        },
        {
            "Sid": "HomeDirObjectAccess",
```

```
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:GetObjectVersion",
                "s3:GetObjectACL",
                "s3:PutObjectACL"
            ],
            "Resource": [
                "arn:aws:s3:::sftp-server-storage-east/*",
                "arn:aws:s3:::s3-storage-east/*"
            ]
        },
        {
            "Sid": "GetConnectorSecretValue",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": "arn:aws:secretsmanager:us-east-1:500655546075:secret:aws/
transfer/sftp-connector1-6RandomCharacters"
        }
    ]
}
```

如需建立「Transfer Family」角色的完整詳細資訊，請遵循建立角色中建立使用者角色所述的程序。

將 Amazon API Gateway 方法設定為自訂身分供應商

本教學課程說明如何設定 Amazon API Gateway 方法，並將其用作自訂身分供應商，將檔案上傳到 AWS Transfer Family 伺服器。本教學課程僅使用 Basic 堆疊範本和其他基本功能作為範例。

主題

- 必要條件
- 步驟 1：建立 CloudFormation 堆疊
- 步驟 2：檢查伺服器的 API Gateway 方法設定
- 步驟 3：查看 Transfer Family 服務器詳細信息
- 步驟 4：測試您的使用者是否可以連線到伺服器

- 步驟 5：測試 SFTP 連線和檔案傳輸
- 步驟 6：限制存取值區
- 如果使用 Amazon EFS，請更新

必要條件

在中建立 Transfer Family 資源之前 AWS CloudFormation，請先建立儲存空間和使用者角色。

若要指定儲存區和建立使用者角色

1. 視您使用的儲存裝置而定，請參閱下列文件：
   - 若要建立 Amazon S3 儲存貯體，請參閱如何建立 S3 儲存貯體？ 在 Amazon 簡單存儲服務用戶指南。
   - 若要建立 Amazon EFS 檔案系統，請參閱設定 Amazon EFS 檔案系統。
2. 若要建立使用者角色，請參閱 建立 IAM 角色和政策

您可以在下一節中建立 AWS CloudFormation 堆疊時，輸入儲存和使用者角色的詳細資料。

步驟 1：建立 CloudFormation 堆疊

若要從提供的範本建立 AWS CloudFormation 堆疊

1. 請在以下位置開啟 AWS CloudFormation 主控台。 https://console.aws.amazon.com/cloudformation
2. 選取 [建立堆疊]，然後選擇 [使用新資源 (標準)]。
3. 在 [先決條件-準備範本] 窗格中，選擇 [範本已就緒]。
4. 複製此連結 (基本堆疊範本)，然後將其貼到 Amazon S3 URL 欄位中。
5. 按一下 Next (下一步)。
6. 指定參數，包括堆疊的名稱。請務必執行以下操作：
   - 取代UserName和的預設值UserPassword。
   - 在中 UserHomeDirectory，輸入您先前建立的儲存 (Amazon S3 儲存貯體或 Amazon EFS 檔案系統) 的詳細資訊。

- 將預設值UserRoleArn取代為您之前建立的使用者角色。 AWS Identity and Access Management (IAM) 角色必須具有適當的許可。如需 IAM 角色和值區政策範例，請參閱步驟 6：限制存取值區。
- 如果您要使用公開金鑰而非密碼進行驗證，請在 UserPublicKey1 欄位中輸入您的公開金鑰。第一次使用 SFTP 連線到伺服器時，您會提供私密金鑰而非密碼。

7. 選擇 [下一步]，然後在 [設定堆疊選項] 頁面上再選擇 [下一步]。
8. 檢閱您要建立之堆疊的詳細資料，然後選擇 [建立堆疊]。

> **Note**
>
> 在頁面底部的「功能」下，您必須確認 AWS CloudFormation 可能會建立 IAM 資源。

步驟 2：檢查伺服器的 API Gateway 方法設定

> **Note**
>
> 若要提高安全性，您可以設定 Web 應用程式防火牆。 AWS WAF 這是一種網頁應用程式防火牆，可讓您監控轉寄至 Amazon API Gateway 的 HTTP 和 HTTPS 請求。如需詳細資訊，請參閱 新增 Web 應用程式防火牆。

若要檢查伺服器的 API Gateway 方法組態並加以部署

1. 在以下網址開啟 API Gateway 主控台：https://console.aws.amazon.com/apigateway/。
2. 選擇範本產生的「移轉自訂身分識別提供者」基本 AWS CloudFormation 範本 API。
3. 在 [資源] 窗格中，選擇 [GET]，然後選擇 [方法要求]。
4. 針對「動作」，選擇「部署 API」。針對「部署」階段，選擇 prod，然後選擇「部署」。

   成功部署 API Gateway 方法之後，請在階段編輯器區段中檢視其效能。

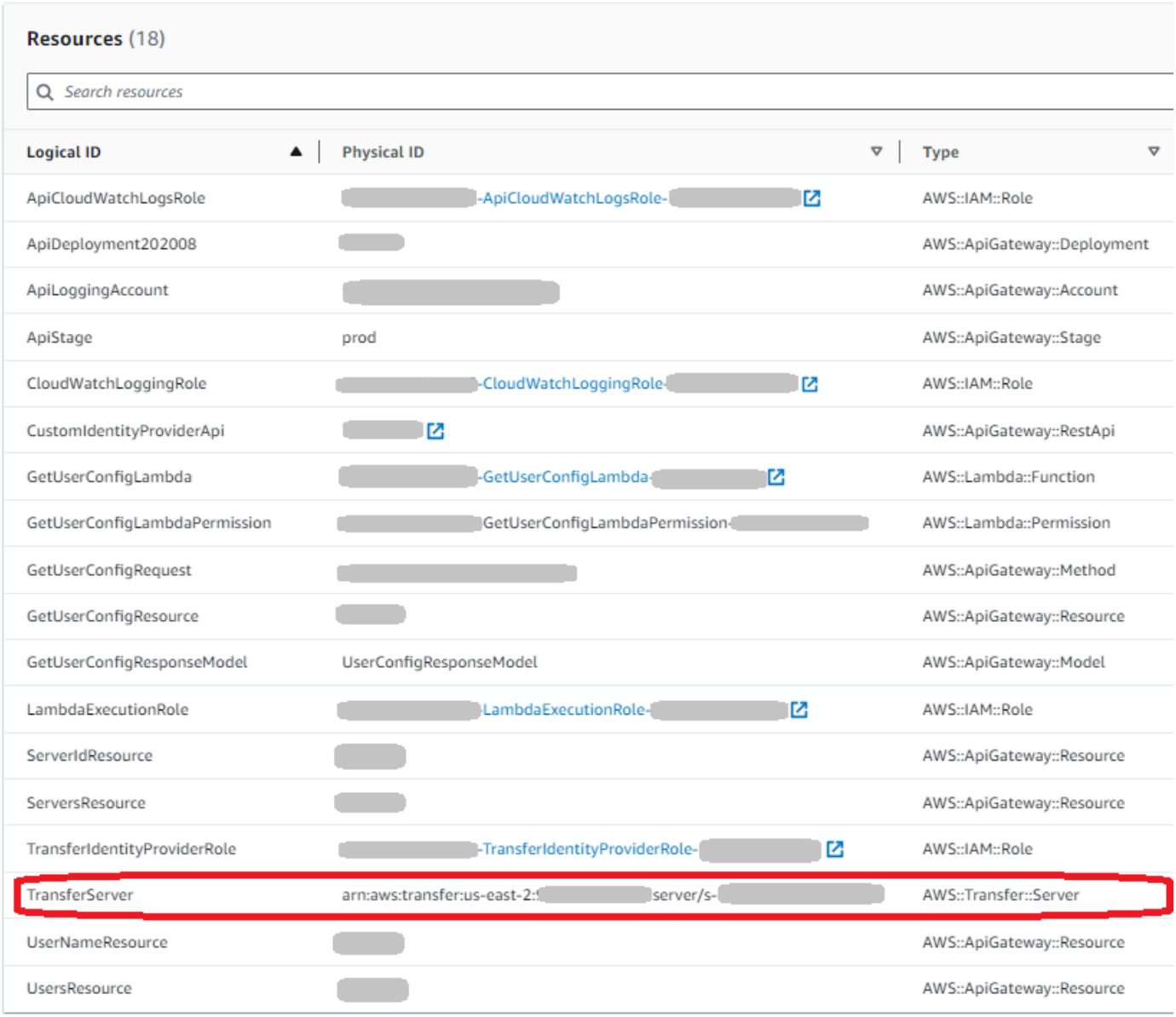
> **Note**
>
> 複製顯示在頁面頂端的呼叫 URL 位址。您將需要它進行下一步。

步驟 3：查看 Transfer Family 服務器詳細信息

當您使用範本建立 AWS CloudFormation 堆疊時，會自動建立 Transfer Family 伺服器。

若要檢視 Transfer Family 伺服器詳細資料

1. 請在以下位置開啟 AWS CloudFormation 主控台。 https://console.aws.amazon.com/cloudformation
2. 選擇您建立的堆疊。
3. 選擇 Resources (資源) 標籤。



伺服器 ARN 會顯示在TransferServer資料列的「實體 ID」欄中。伺服器識別碼包含在 ARN 中，例如：

4. 在 https://console.aws.amazon.com/transfer/ 開啟 AWS Transfer Family 主控台，然後在「伺服器」頁面上選擇新伺服器。

   伺服器 ID 與中顯示的TransferServer資源 ID 相符 AWS CloudFormation。

步驟 4：測試您的使用者是否可以連線到伺服器

若要測試使用者是否可以連線到伺服器，請使用 Transfer Family 主控台

1. 請在以下位置開啟 AWS Transfer Family 主控台。 https://console.aws.amazon.com/transfer/
2. 在 [伺服器] 頁面上，選擇新伺服器，選擇 [動作]，然後選擇 [測試]。
3. 在「使用者名稱」欄位和「密碼」欄位中輸入您的登入認證文字。這些是您在部署 AWS CloudFormation 堆疊時設定的值。
4. 在「伺服器通訊協定」中，選取 SFTP，然後輸入**127.0.0.1**做為來源 IP。
5. 選擇 測試。

   如果使用者驗證成功，則測試會傳回 `StatusCode: 200` HTML 回應，以及包含使用者角色和權限詳細資訊的 JSON 物件。例如：

```
{
    "Response": "{\"Role\": \"arn:aws:iam::123456789012:role/my-user-role\",
\"HomeDirectory\": \"/${transfer:HomeBucket}/\"}",
    "StatusCode": 200,
    "Message": "",
    "Url": "https://1a2b3c4d5e.execute-api.us-east-2.amazonaws.com/prod/servers/
s-1234abcd5678efgh0/users/myuser/config"
}
```

   如果測試失敗，請將其中一個 API Gateway AWS 管理的政策新增至您用於 API 的角色。

步驟 5：測試 SFTP 連線和檔案傳輸

若要測試 SFTP 連線

1. 在 Linux 或 macOS 裝置上，開啟命令終端機。

2. 根據您使用的是密碼還是 key pair 進行驗證，輸入下列其中一個命令。

   - 如果您使用的是密碼，請輸入以下指令：

     ```
     sftp -o PubkeyAuthentication=no myuser@server-ID.server.transfer.region-code.amazonaws.com
     ```

     出現提示時，輸入您的密碼。
   - 如果您使用的是 key pair，請輸入以下指令：

     ```
     sftp -i private-key-file myuser@server-ID.server.transfer.region-code.amazonaws.com
     ```

   > **Note**
   >
   > 對於這些`sftp`指令，請插入 Transfer Family 伺服器所 AWS 區域 在位置的代碼。例如，如果您的伺服器位於美國東部 (俄亥俄州)，請輸入**`us-east-2`**。

3. 出現`sftp>`提示時，請確定您可以上傳 (`put`)、download (`get`) 以及檢視目錄和檔案 (`pwd`和`ls`)。

步驟 6：限制存取值區

您可以限制誰可以存取特定的 Amazon S3 儲存貯體。下列範例顯示要在 CloudFormation 堆疊中以及您為使用者選取的原則中使用的設定。

在這個例子中，我們為 AWS CloudFormation 堆棧設置了以下參數：

- CreateServer: `true`
- UserHomeDirectory: `/myuser-bucket`
- UserName: `myuser`
- UserPassword: `MySuperSecretPassword`

> **Important**
>
> 這是一個示例密碼。設定 API Gateway 方法時，請務必輸入強式密碼。

- UserPublicKey1: *`your-public-key`*
- UserRoleArn: `arn:aws:iam::`*`role-id`*`:role/myuser-api-gateway-role`

UserPublicKey1 是您作為公鑰/私鑰對的一部分生成的公 key pair。

對*role-id*於您所建立的使用者角色而言，是唯一的。附加至的myuser-api-gateway-role原則如下：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::myuser-bucket"
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObjectAcl",
                "s3:GetObject",
                "s3:DeleteObjectVersion",
                "s3:DeleteObject",
                "s3:PutObjectAcl",
                "s3:GetObjectVersion"
            ],
            "Resource": "arn:aws:s3:::myuser-bucket/*"
        }
    ]
}
```

若要使用 SFTP 連線至伺服器，請在提示下輸入下列其中一個指令。

- 如果您使用密碼進行驗證，請執行下列命令：

  ```
  sftp -o PubkeyAuthentication=no myuser@transfer-server-ID.server.transfer.region-id.amazonaws.com
  ```

  出現提示時，輸入您的密碼。
- 如果您使用 key pair 進行驗證，請執行下列命令：

```
sftp -i private-key-file myuser@transfer-server-
ID.server.transfer.region-id.amazonaws.com
```

> **Note**
>
> 對於這些sftp指令，請使用 Transfer Family 伺服器所 AWS 區域 在位置的 ID。例如，如果您的伺服器位於美國東部 (俄亥俄州)，請使用us-east-2。

出現sftp提示時，系統會將您導向至主目錄，您可以透過執行pwd命令來檢視該目錄。例如：

```
sftp> pwd
Remote working directory: /myuser-bucket
```

使用者無法檢視主目錄上方的任何目錄。例如：

```
sftp> pwd
Remote working directory: /myuser-bucket
sftp> cd ..
sftp> ls
Couldn't read directory: Permission denied
```

如果使用 Amazon EFS，請更新

如果您選取 Amazon EFS 做為 Transfer Family 伺服器的儲存選項，則需要編輯堆疊的 Lambda 函數。

若要將 Posix 設定檔新增至您的 Lambda 函數

1. 開啟 Lambda 主控台，網址為 https://console.aws.amazon.com/lambda/。
2. 選取您先前建立的 Lambda 函數。Lambda 函數具有*####*的格式-GetUserConfigLambda-*lambda ###*，其中堆棧名是 CloudFormation 堆棧*##*和 *lambda* 標識符是該函數的標識符。
3. 在「程式碼」索引標籤中，選取 index.js 以顯示函數的程式碼。
4. 在中response，在Policy和之間加入下列行HomeDirectory：

   ```
   PosixProfile: {"Uid": uid-value, "Gid": gid-value},
   ```

   其中的 *UID #*和 *GID #*是整數，0 或更大，分別代表用戶 ID 和組 ID。

例如，在您新增 Posix 設定檔之後，回應欄位可能如下所示：

```
response = {
     Role: 'arn:aws:iam::123456789012:role/api-gateway-transfer-efs-role', // The
user will be authenticated if and only if the Role field is not blank
     Policy: '', // Optional JSON blob to further restrict this user's permissions
     PosixProfile: {"Gid": 65534, "Uid": 65534},
     HomeDirectory: '/fs-fab2c234' // Not required, defaults to '/'
   };
```

設定 AS2 組態

本教學課程將逐步介紹如何使用設定適用性陳述式 2 (AS2) 組態。 AWS Transfer Family完成此處描述的步驟後，您將擁有一台已啟用 AS2 的伺服器，可接受來自範例交易夥伴的 AS2 訊息。您也將擁有一個連接器，可用來傳送 AS2 訊息給範例交易夥伴。

> **Note**
>
> 範例設定的某些部分使用 AWS Command Line Interface (AWS CLI)。如果您尚未安裝 AWS CLI，請參閱《使用指南》 AWS CLI中的〈安裝或更新最新版本的AWS Command Line Interface〉。

1. 為您自己和交易夥伴建立憑證。如果您有可以使用的現有憑證，則可以略過本節。

   此程序會在中描述步驟 1：為 AS2 建立憑證。
2. 建立使用 AS2 通訊協定的 AWS Transfer Family 伺服器。或者，您可以將彈性 IP 地址添加到服務器以使其面向互聯網。

   此程序會在中描述步驟 2：建立使用 AS2 通訊協定的 Transfer Family 伺服器。

   > **Note**
   >
   > 您必須建立 Transfer Family 伺服器，只能用於輸入轉移作業。如果您只執行對外傳輸，則不需要 Transfer Family 伺服器。
3. 匯入您在步驟 1 中建立的憑證。

此程序會在中描述步驟 3：將憑證匯入為 Transfer Family 憑證資源。

4. 若要設定您的交易夥伴，請建立當地個人檔案和合作夥伴個人檔案。

   此程序會在中描述步驟 4：為您和您的交易夥伴建立個人檔案。

5. 建立您與交易夥伴之間的協議。

   此程序會在中描述步驟 5：建立您與合作夥伴之間的協議。

   > **Note**
   > 您必須僅針對入埠移轉建立協議。如果您只執行對外轉移，則不需要合約。

6. 在您與交易夥伴之間建立連接器。

   此程序會在中描述步驟 6：在您和合作夥伴之間建立連接器。

   > **Note**
   > 您必須僅為輸出傳輸建立連接器。如果您只執行輸入傳輸，則不需要連接器。

7. 測試 AS2 檔案交換。

   此程序會在中描述第 7 步：使用 Transfer Family 列測試在 AS2 上交換文件。

完成這些步驟後，您可以執行下列動作：

- 使用「傳送系列」`start-file-transfer` AWS Command Line Interface (AWS CLI) 指令，將檔案傳送至啟用 AS2 的遠端夥伴伺服器。
- 透過虛擬私有雲端 (VPC) 端點，從連接埠 5080 上啟用 AS2 的遠端合作夥伴伺服器接收檔案。

步驟 1：為 AS2 建立憑證

AS2 交換中的雙方都需要 X.509 憑證。您可以用任何您喜歡的方式創建這些證書。本主題說明如何從命令列使用 OpenSSL 建立根憑證，然後簽署從屬憑證。雙方必須產生自己的憑證。

> **Note**
>
> AS2 憑證的金鑰長度必須至少為 2048 位元，且最多為 4096 個。

若要與合作夥伴一起傳輸檔案，請注意下列事項：

- 您可以將憑證附加到設定檔。憑證包含公開或私密金鑰。
- 您的交易夥伴將他們的公鑰發送給您，然後您將其發送給您的密鑰。
- 您的交易夥伴會使用您的公開金鑰加密訊息，並使用他們的私密金鑰簽署訊息。相反，您可以使用合作夥伴的公鑰對消息進行加密，並使用私鑰對其進行簽名。

> **Note**
>
> 如果您喜歡使用 GUI 管理密鑰，Portecle則可以使用其中一個選項。

若要產生範例憑證

> **Important**
>
> 不要將您的私鑰發送給您的伴侶。在此範例中，您會為一方產生一組自我簽署的公開金鑰和私密金鑰。如果您要同時擔任兩個交易夥伴進行測試，您可以重複這些指示來產生兩組金鑰：每個交易夥伴各一組金鑰。在此情況下，您不需要產生兩個根憑證授權單位 (CA)。

1. 執行下列命令以產生具有 2048 位元長模數的 RSA 私密金鑰。

```
/usr/bin/openssl genrsa -out root-ca-key.pem 2048
```

2. 執行下列命令，以使用您的`root-ca-key.pem`檔案建立自我簽署憑證。

```
/usr/bin/openssl req \
-x509 -new -nodes -sha256 \
-days 1825 \
-subj "/C=US/ST=MA/L=Boston/O=TransferFamilyCustomer/OU=IT-dept/CN=ROOTCA" \
-key root-ca-key.pem \
-out root-ca.pem
```

引-subj數由下列值組成。

	名稱	描述
C	國家代碼	組織所在國家/地區的兩個字母代碼。
ST	州、地區或省	貴組織所在的州、地區或省。（在這種情況下，地區不是指您的 AWS 區域。）
L	Locality name (地區名稱)	您的組織所在的城市。
O	組織名稱	您組織的完整法定名稱，包括後綴，例如 LLC，Corp 等。
OU	組織單位名稱	您組織中處理此憑證的部門。
CN	一般名稱或完整網域名稱 (FQDN)	在這種情況下，我們正在創建一個根證書，所以值是ROOTCA。在這些例子中，我們使用CN來描述證書的目的。

3. 為您的本機設定檔建立簽署金鑰和加密金鑰。

```
/usr/bin/openssl genrsa -out signing-key.pem 2048
/usr/bin/openssl genrsa -out encryption-key.pem 2048
```

> **Note**
>
> 某些啟用 AS2 的伺服器 (例如 OpenAS2) 會要求您使用相同的憑證來進行簽署和加密。在這種情況下，您可以為這兩種目的導入相同的私鑰和證書。若要這麼做，請執行這個命令，而不是先前的兩個命令：
>
> ```
> /usr/bin/openssl genrsa -out signing-and-encryption-key.pem 2048
> ```

4. 執行下列命令，為要簽署的根金鑰建立憑證簽署要求 (CSR)。

```
/usr/bin/openssl req -new -key signing-key.pem -subj \
"/C=US/ST=MA/L=Boston/O=TransferFamilyCustomer/OU=IT-dept/CN=Signer" -out signing-
key-csr.pem
```

```
/usr/bin/openssl req -new -key encryption-key.pem -subj \
"/C=US/ST=MA/L=Boston/O=TransferFamilyCustomer/OU=IT-dept/CN=Encrypter" -out
 encryption-key-csr.pem
```

5. 接下來，您必須創建一個signing-cert.conf文件和一個encryption-cert.conf文件。

   - 使用文字編輯器建立包含下列內容的signing-cert.conf檔案：

   ```
   authorityKeyIdentifier=keyid,issuer
   keyUsage = digitalSignature, nonRepudiation
   ```

   - 使用文字編輯器建立包含下列內容的encryption-cert.conf檔案：

   ```
   authorityKeyIdentifier=keyid,issuer
   keyUsage = dataEncipherment
   ```

6. 最後，您可以執行下列命令來建立已簽署的憑證。

```
/usr/bin/openssl x509 -req -sha256 -CAcreateserial -days 1825 -in signing-key-
csr.pem -out signing-cert.pem -CA \
root-ca.pem -CAkey root-ca-key.pem -extfile signing-cert.conf
```

```
/usr/bin/openssl x509 -req -sha256 -CAcreateserial -days 1825 -in encryption-key-
csr.pem -out encryption-cert.pem \
-CA root-ca.pem -CAkey root-ca-key.pem -extfile encryption-cert.conf
```

步驟 2：建立使用 AS2 通訊協定的 Transfer Family 伺服器

此程序說明如何使用「Transfer Family」建立啟用 AS2 的伺服器。 AWS CLI

> **Note**
>
> 許多範例步驟都使用從檔案載入參數的指令。如需有關使用檔案載入參數的詳細資訊，請參閱如何從檔案載入參數。

如果您想改用主控台，請參閱使用 Transfer Family 列主控台建立 AS2 伺服器。

與建立 SFTP 或 FTPS AWS Transfer Family 伺服器的方式類似，您可以使用指令的`--protocols AS2`參數建立啟用 AS2 的伺服器。`create-server` AWS CLI 目前，Transfer Family 僅支援使用 AS2 通訊協定的 VPC 端點類型和 Amazon S3 儲存。

當您使用`create-server`指令為 Transfer Family 建立啟用 AS2 的伺服器時，系統會自動為您建立 VPC 端點。此端點會公開 TCP 連接埠 5080，以便它可以接受 AS2 訊息。

如果要將 VPC 端點公開給網際網路，可以將彈性 IP 地址與 VPC 端點建立關聯。

若要使用這些指示，您需要下列項目：

- VPC 的識別碼 (例如，虛擬私人雲端 01)。
- VPC 子網路的識別碼 (例如，子網路 -abcdef01、子網路 -021345ab)。
- 一或多個安全性群組識別碼，這些識別碼允許來自您的交易夥伴傳入 TCP 連接埠 5080 的流量 (例如，sg-123 4567890)。
- (選擇性) 您要與 VPC 端點建立關聯的彈性 IP 位址。
- 如果您的交易夥伴未透過 VPN 連接到您的 VPC，則需要網際網路閘道。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的使用網際網路閘道連接至網際網路。

若要建立已啟用 AS2 的伺服器

1. 執行下列命令。將每個 *user input placeholder* 替換成您自己的資訊。

```
aws transfer create-server --endpoint-type VPC \
--endpoint-details VpcId=vpc-abcdef01,SubnetIds=subnet-abcdef01,subnet-
abcdef01,subnet-
021345ab,SecurityGroupIds=sg-abcdef01234567890,sg-1234567890abcdef0 --protocols AS2
 \
--protocol-details As2Transports=HTTP
```

2. (選擇性) 您可以將 VPC 端點設為公用。您只能透過update-server作業將彈性 IP 位址附加至 Transfer Family 伺服器。下列命令會停止伺服器，使用彈性 IP 位址更新伺服器，然後再次啟動。

```
aws transfer stop-server --server-id your-server-id
```

```
aws transfer update-server --server-id your-server-id --endpoint-details \
AddressAllocationIds=eipalloc-abcdef01234567890,eipalloc-
1234567890abcdef0,eipalloc-abcd012345ccccccc
```

```
aws transfer start-server --server-id your-server-id
```

此start-server命令會自動為您建立包含伺服器公用 IP 位址的 DNS 記錄。為了讓交易夥伴能夠存取伺服器，您必須向他們提供下列資訊。在這種情況下，*your-region*指的是您的 AWS 區域.

s-*your-server-id*.server.transfer.*your-region*.amazonaws.com

您提供給交易夥伴的完整網址如下：

http://s-*your-server-id*.server.transfer.*your-region*.amazonaws.com:5080

3. 若要測試啟用 AS2 的伺服器是否可存取，請使用下列指令。確保您的伺服器可以透過 VPC 端點的私有 DNS 位址或透過公用端點存取 (如果您將彈性 IP 位址與端點相關聯) 存取。

   如果您的伺服器設定正確，連線就會成功。但是，您將收到 HTTP 狀態碼 400（錯誤請求）響應，因為您沒有發送有效的 AS2 消息。

   - 對於公共端點（如果您在上一步中關聯了彈性 IP 地址），請運行以下命令，替換您的服務器 ID 和 Region。

     ```
     curl -vv -X POST http://s-your-server-id.transfer.your-region.amazonaws.com:5080
     ```

   - 如果您要在 VPC 中進行連線，請執行下列命令來查找 VPC 端點的私人 DNS 名稱。

     ```
     aws transfer describe-server --server-id s-your-server-id
     ```

     此describe-server命令會在VpcEndpointId參數中傳回您的 VPC 端點識別碼。使用此值執行下列命令。

```
aws ec2 describe-vpc-endpoints --vpc-endpoint-ids vpce-your-vpc-endpoint-id
```

這個describe-vpc-endpoints命令返回一個數DNSEntries組，有幾個DnsName參數。在下列命令中使用區域 DNS 名稱 (不包含可用區域的名稱)。

```
curl -vv -X POST http://vpce-your-vpce.vpce-svc-your-vpce-svc.your-
region.vpce.amazonaws.com:5080
```

例如，下列指令展示前一個指令中預留位置的範例值。

```
curl -vv -X POST http://vpce-0123456789abcdefg-fghij123.vpce-
svc-11111aaaa2222bbbb.us-east-1.vpce.amazonaws.com:5080
```

4. (選擇性) 設定記錄角色。Transfer Family 會將以結構化 JSON 格式傳送和接收的訊息狀態記錄到 Amazon CloudWatch 日誌。若要讓 Transfer Family 能夠存取您帳戶中的記 CloudWatch 錄，您必須在伺服器上設定記錄角色。

   建立信任的 AWS Identity and Access Management (IAM) 角色transfer.amazonaws.com，並附加受AWSTransferLoggingAccess管政策。如需詳細資訊，請參閱 建立 IAM 角色和政策。請記下您剛建立的 IAM 角色的 Amazon 資源名稱 (ARN)，並透過執行下列update-server命令將其與伺服器建立關聯：

   ```
   aws transfer update-server --server-id your-server-id --logging-role
    arn:aws:iam::your-account-id:role/logging-role-name
   ```

   > **Note**
   >
   > 即使記錄角色是選用的，我們強烈建議您進行設定，以便您可以查看訊息的狀態並疑難排解組態問題。

步驟 3：將憑證匯入為 Transfer Family 憑證資源

此程序說明如何使用匯入憑證 AWS CLI。如果您想改用 Transfer Family 主控台，請參閱the section called “匯入 AS2 憑證”。

若要匯入您在步驟 1 中建立的簽署和加密憑證，請執行下列import-certificate命令。如果您使用相同的證書進行加密和簽名，請導入相同的證書兩次（一次SIGNING使用，然後再次ENCRYPTION使用）。

```
aws transfer import-certificate --usage SIGNING --certificate file://signing-cert.pem \
            --private-key file://signing-key.pem --certificate-chain file://root-ca.pem
```

此命令返回您的簽名CertificateId。在下一節中，此憑證 ID 稱為*my-signing-cert-id*。

```
aws transfer import-certificate --usage ENCRYPTION --certificate file://encryption-
cert.pem \
            --private-key file://encryption-key.pem --certificate-chain file://root-
ca.pem
```

此命令返回您的加密CertificateId。在下一節中，此憑證 ID 稱為*my-encrypt-cert-id*。

接下來，執行下列命令，匯入合作夥伴的加密和簽署憑證。

```
aws transfer import-certificate --usage ENCRYPTION --certificate file://partner-
encryption-cert.pem \
--certificate-chain file://partner-root-ca.pem
```

這個命令會傳回合作夥伴的加密CertificateId。在下一節中，此憑證 ID 稱為*partner-encrypt-cert-id*。

```
aws transfer import-certificate --usage SIGNING --certificate file://partner-signing-
cert.pem \
--certificate-chain file://partner-root-ca.pem
```

此指令會傳回合作夥伴的簽署CertificateId。在下一節中，此憑證 ID 稱為*partner-signing-cert-id*。

步驟 4：為您和您的交易夥伴建立個人檔案

此程序說明如何使用建立 AS2 設定檔 AWS CLI。如果您想改用 Transfer Family 主控台，請參閱the section called “建立 AS2 設定檔”。

執行下列命令來建立您的本機 AS2 設定檔。此命令會參考包含您的公開金鑰和私密金鑰的憑證。

```
aws transfer create-profile --as2-id MYCORP --profile-type LOCAL --certificate-ids \
```

```
my-signing-cert-id my-encrypt-cert-id
```

此指令會傳回您的設定檔 ID。在下一節中，此 ID 稱為*my-profile-id*。

現在，通過運行以下命令創建合作夥伴配置文件。這個命令只會使用合作夥伴的公開金鑰憑證。若要使用此指令，請以您自己*user input placeholders*的資訊取代；例如，您的合作夥伴的 AS2 名稱和憑證 ID。

```
aws transfer create-profile --as2-id PARTNER-COMPANY --profile-type PARTNER --
certificate-ids \
partner-signing-cert-id partner-encrypt-cert-id
```

此指令會傳回您合作夥伴的設定檔 ID。在下一節中，此 ID 稱為*partner-profile-id*。

> **Note**
>
> 在前面的命令中，將 *MYCORP* 替換為您組織的名稱，將「合作####」替換為您的交易夥伴組織的名稱。

步驟 5：建立您與合作夥伴之間的協議

此程序說明如何使用建立 AS2 合約。 AWS CLI如果您想改用 Transfer Family 主控台，請參閱the section called “建立 AS2 協議”。

協定將兩個設定檔 (本機和合作夥伴)、憑證以及允許雙方之間傳入 AS2 傳輸的伺服器組態結合在一起。您可以通過運行以下命令列出您的項目。

```
aws transfer list-profiles --profile-type LOCAL
aws transfer list-profiles --profile-type PARTNER
aws transfer list-servers
```

此步驟需要 Amazon S3 儲存貯體和 IAM 角色，具有儲存貯體的讀取/寫入存取權限。建立此角色的指示與 Transfer Family SFTP、FTP 和 FTPS 通訊協定的指示相同，可在中取得。建立 IAM 角色和政策

若要建立協議，您需要下列項目：

- Amazon S3 儲存貯體名稱 (以及物件前綴，如果指定)
- 可存取儲存貯體的 IAM 角色的 ARN

- 您的 Transfer Family 服務器 ID
- 您的個人資料 ID 和合作夥伴的個人資料 ID

執行下列命令以建立協定。

```
aws transfer create-agreement --description "ExampleAgreementName" --server-id your-server-id \
--local-profile-id your-profile-id --partner-profile-id your-partner-profile-id --base-directory /DOC-EXAMPLE-DESTINATION-BUCKET/AS2-inbox \
--access-role arn:aws:iam::111111111111:role/TransferAS2AccessRole
```

如果成功，此命令會傳回協定的 ID。然後，您可以使用下列指令來檢視合約的詳細資訊。

```
aws transfer describe-agreement --agreement-id agreement-id --server-id your-server-id
```

步驟 6：在您和合作夥伴之間建立連接器

此程序說明如何使用建立 AS2 連接器。 AWS CLI如果您想改用 Transfer Family 主控台，請參閱the section called “設定 AS2 連接器”。

您可以使用 `StartFileTransfer` API 操作，使用連接器將存放在 Amazon S3 中的檔案傳送到交易夥伴的 AS2 端點。您可以執行下列命令來尋找先前建立的設定檔。

```
aws transfer list-profiles
```

建立連接器時，您必須提供合作夥伴的 AS2 伺服器 URL。將下列文字複製到名為的檔案中`testAS2Config.json`。

```
{
"Compression": "ZLIB",
"EncryptionAlgorithm": "AES256_CBC",
"LocalProfileId": "your-profile-id",
"MdnResponse": "SYNC",
"MdnSigningAlgorithm": "DEFAULT",
"MessageSubject": "Your Message Subject",
"PartnerProfileId": "partner-profile-id",
"SigningAlgorithm": "SHA256"
}
```

> **Note**
>
> 對於EncryptionAlgorithm，除非您必須支援需要該DES_EDE3_CBC演算法的舊版用戶端，否則請勿指定演算法，因為這是弱式加密演算法。

然後執行下列命令以建立連接器。

```
aws transfer create-connector --url "http://partner-as2-server-url" \
--access-role your-IAM-role-for-bucket-access \
--logging-role arn:aws:iam::your-account-id:role/service-role/AWSTransferLoggingAccess
 \
--as2-config file:///path/to/testAS2Config.json
```

第 7 步：使用 Transfer Family 列測試在 AS2 上交換文件

接收來自交易夥伴的檔案

如果您將公用彈性 IP 位址與虛擬私人雲端端點相關聯，Transfer Family 會自動建立包含您公用 IP 位址的 DNS 名稱。子網域是您的 AWS Transfer Family 伺服器 ID (格式為s-1234567890abcdef0)。以下列格式提供您的伺服器網址給交易夥伴。

```
http://s-1234567890abcdef0.server.transfer.us-east-1.amazonaws.com:5080
```

如果您沒有將公用彈性 IP 位址與您的 VPC 端點建立關聯，請查詢 VPC 端點的主機名稱，該主機名稱可透過 HTTP POST 接受來自您的交易夥伴在連接埠 5080 上的 AS2 訊息。若要擷取 VPC 端點詳細資料，請使用下列命令。

```
aws transfer describe-server --server-id s-1234567890abcdef0
```

例如，假設上述命令傳回的 VPC 端點識別碼。vpce-1234abcd5678efghi然後，您將使用以下命令來檢索 DNS 名稱。

```
aws ec2 describe-vpc-endpoints --vpc-endpoint-ids vpce-1234abcd5678efghi
```

此命令會傳回執行下列命令所需之 VPC 端點的所有詳細資料。

DNS 名稱會列在DnsEntries陣列中。您的交易夥伴必須在您的 VPC 內才能存取您的 VPC 端點 (例如透過 AWS PrivateLink 或 VPN)。以下列格式提供您的 VPC 端點 URL 給您的合作夥伴。

```
http://vpce-your-vpce-id.vpce-svc-your-vpce-svc-id.your-region.vpce.amazonaws.com:5080
```

例如，下列 URL 顯示先前命令中預留位置的範例值。

```
http://vpce-0123456789abcdefg-fghij123.vpce-svc-11111aaaa2222bbbb.us-
east-1.vpce.amazonaws.com:5080
```

在此範例中，成功的傳輸會儲存在您在中指定的base-directory參數中指定的位置步驟 5：建立您與合作夥伴之間的協議。如果我們成功收到名為myfile1.txt和的文件myfile2.txt，文件存儲為/*path-defined-in-the-agreement*/processed/*original_filename.messageId.original_extension*. 在這裡，文件存儲為/DOC-EXAMPLE-DESTINATION-BUCKET/AS2-inbox/processed/myfile1.*messageId*.txt和/DOC-EXAMPLE-DESTINATION-BUCKET/AS2-inbox/processed/myfile2.*messageId*.txt。

如果您在建立 Transfer Family 伺服器時設定了記錄角色，也可以檢查記 CloudWatch 錄中 AS2 訊息的狀態。

傳送檔案給交易夥伴

您可以透過參考連接器 ID 和檔案的路徑，使用「Transfer Family 列」來傳送 AS2 訊息，如下列 `start-file-transfer` AWS Command Line Interface (AWS CLI) 指令所示：

```
aws transfer start-file-transfer --connector-id c-1234567890abcdef0 \
--send-file-paths "/DOC-EXAMPLE-SOURCE-BUCKET/myfile1.txt" "/DOC-EXAMPLE-SOURCE-BUCKET/
myfile2.txt"
```

若要取得連接器的詳細資料，請執行下列命令：

```
aws transfer list-connectors
```

該list-connectors命令會傳回連接器的連接器 ID、URL 和 Amazon 資源名稱 (ARN)。

若要傳回特定連接器的內容，請使用您要使用的 ID 執行下列命令：

```
aws transfer describe-connector --connector-id your-connector-id
```

命describe-connector令會傳回連接器的所有內容，包括其 URL、角色、設定檔、訊息配置通知 (MDN)、標籤和監視度量。

您可以檢視 JSON 和 MDN 檔案，確認合作夥伴已成功收到檔案。這些檔案是根據中所述的慣例來命名檔案名稱和位置。如果您在建立連接器時設定記錄角色，您也可以檢查記 CloudWatch 錄中 AS2 訊息的狀態。

設定 SFTP、FTPS 或 FTP 伺服器端點

本主題提供建立和使用使用一或多個 SFTP、FTPS 和 FTP 通訊協定之 AWS Transfer Family 伺服器端點的詳細資訊。

主題

- 識別提供者選項
- AWS Transfer Family 端點類型矩陣
- 設定 SFTP、FTPS 或 FTP 伺服器端點
- 使用用戶端透過伺服器端點傳輸檔案
- 管理伺服器端點的使用者
- 使用邏輯目錄簡化您的 Transfer Family 目錄結構

識別提供者選項

AWS Transfer Family 提供數種驗證和管理使用者的方法。下表比較可與「Transfer Family 列」搭配使用的可用身分識別提供者。

動作	AWS Transfer Family 管理的服務	AWS Managed Microsoft AD	Amazon API Gateway	AWS Lambda
支援的通訊協定	SFTP	SFTP, FTPS, FTP	SFTP, FTPS, FTP	SFTP, FTPS, FTP
基於金鑰的驗證	是	否	是	是
密碼身分驗證	否	是	是	是
AWS Identity and Access Management（IAM）和 POSIX	是	是	是	是

動作	AWS Transfer Family 管理的服務	AWS Managed Microsoft AD	Amazon API Gateway	AWS Lambda
邏輯主目錄	是	是	是	是
參數化訪問（基於用戶名）	是	是	是	是
隨機存取結構	是	否	是	是
AWS WAF	否	否	是	否

備註：

- IAM 用於控制 Amazon S3 支援儲存的存取，而 POSIX 則用於 Amazon EFS。
- Ad hoc 是指在運行時發送用戶配置文件的能力。例如，您可以將使用者名稱做為變數傳遞，將使用者登入其主目錄中。
- 如需詳細資訊 AWS WAF，請參閱新增 Web 應用程式防火牆。
- 有一篇博客文章描述了使用與 Microsoft Azure AD 集成的 Lambda 函數作為您的 Transfer Family 身份提供者。如需詳細資訊，請參閱AWS Transfer Family 使用 Azure 作用中目錄進行驗證和 AWS Lambda。
- 我們提供數個 AWS CloudFormation 範本，協助您快速部署使用自訂身分識別提供者的 Transfer Family 伺服器。如需詳細資訊，請參閱 Lambda 函數模板。

在下列程序中，您可以建立啟用 SFTP 的伺服器、啟用 FTP 的伺服器、啟用 FTP 的伺服器或啟用 AS2 的伺服器。

下一步驟

- 建立啟用 SFTP 的伺服器
- 建立啟用 FTP 的伺服器
- 建立啟用 FTP 的伺服器
- 配置 AS2

AWS Transfer Family 端點類型矩陣

建立 Transfer Family 伺服器時，您可以選擇要使用的端點類型。下表說明每種端點類型的特性。

端點類型矩陣

特性	公有	VPC-互聯網	VPC-內部	虛擬私隱端點 (已取代)
支援的協定	SFTP	SFTP, FTPS, 作為 2	SFTP, FTP, FTPS, 作為 2	SFTP
存取	從互聯網上。此端點類型不需要 VPC 中的任何特殊配置。	透過網際網路、VPC 和虛擬私人雲端連線環境 (例如透過內部部署資料中心或 VPN)。 AWS Direct Connect	從 VPC 和虛擬私人雲端連線的環境中，例如透過內部部署資料中心或 VPN。 AWS Direct Connect	從 VPC 和虛擬私人雲端連線的環境中，例如透過內部部署資料中心或 VPN。 AWS Direct Connect
靜態 IP 位址	您無法附加靜態 IP 位址。 AWS 提供可能會變更的 IP 位址。	您可以將彈性 IP 位址附加到端點。這些可以是 AWS擁有的 IP 地址或您自己的 IP 地址（攜帶自己的 IP 地址）。連接到端點的彈性 IP 位址不會變更。 連接到服務器的私有 IP 地址也不會更改。	連接到端點的私人 IP 位址不會變更。	連接到端點的私人 IP 位址不會變更。
來源 IP 允許清單	此端點類型不支援依來源 IP 位址的允許清單。	若要允許依來源 IP 位址進行存取，您可以使用連結至伺服器端	若要允許依來源 IP 位址進行存取，您可以使用連接到伺服器端	若要允許依來源 IP 位址進行存取，您可以使用連結至伺服器端

特性	公有	VPC-互聯網	VPC-內部	虛擬私隱端點 (已取代)
	端點可公開存取，並監聽連接埠 22 上的流量。 **Note** 對於 VPC 人雲端託管的端點，SFTP Transfer Family 伺服器可以透過連接埠 22 (預設值)、連接埠 2222 或連接埠 22000 進行操作。	點的安全群組，以及連結至端點所在子網路的網路 ACL。	點的安全群組，以及連結至端點所在子網路的網路存取控制清單 (網路 ACL)。	點的安全群組，以及連結至端點所在子網路的網路 ACL。
用戶端防火牆允許清	您必須允許伺服器的 DNS 名稱。 由於 IP 位址可能會變更，因此請避免將 IP 位址用於用戶端防火牆允許清單。	您可以允許伺服器的 DNS 名稱或連接到伺服器的彈性 IP 位址。	您可以允許端點的私人 IP 位址或 DNS 名稱。	您可以允許端點的私人 IP 位址或 DNS 名稱。

> **Note**
>
> VPC_ENDPOINT端點類型現已過時，無法用於建立新伺服器。請不要使EndpointType=VPC_ENDPOINT用新的 VPC 端點類型 (EndpointType=VPC)，您可以將其用作「內部」或「網際網路對向」，如上表所述。如需詳細資訊，請參閱 停止使用 VPC_ 端點。

請考慮下列選項來增加 AWS Transfer Family 伺服器的安全狀況：

- 使用具有內部存取權的 VPC 端點，以便只有 VPC 或虛擬私人雲端連線環境中的用戶端 (例如透過內部部署資料中心或 VPN) 才能存取伺服器。 AWS Direct Connect
- 若要允許用戶端透過網際網路存取端點並保護您的伺服器，請使用具有網際網路對向存取權的 VPC 端點。然後，修改 VPC 的安全群組，以僅允許來自託管使用者用戶端之特定 IP 位址的流量。
- 如果您需要以密碼為基礎的驗證，並在伺服器上使用自訂身分識別提供者，最佳做法是，您的密碼原則會防止使用者建立弱式密碼，並限制登入嘗試失敗的次數。
- AWS Transfer Family 是一個託管服務，所以它不提供 shell 訪問。您無法直接存取基礎 SFTP 伺服器，以便在轉移系列伺服器上執行作業系統原生命令。
- 在具有內部存取權的 VPC 端點前面使用 Network Load Balancer。將負載平衡器上的接聽程式連接埠從連接埠 22 變更為其他連接埠。這可以降低但不能消除連接埠掃描器和機器人偵測伺服器的風險，因為通訊埠 22 最常用於掃描。如需詳細資訊，請參閱網路負載平衡器現在支援安全群組的部落格文章。

> **Note**
>
> 如果您使用 Network Load Balancer， AWS Transfer Family CloudWatch 記錄會顯示 NLB 的 IP 位址，而不是實際的用戶端 IP 位址。

設定 SFTP、FTPS 或 FTP 伺服器端點

您可以使用該服務來創建文件傳輸 AWS Transfer Family 服務器。以下是可用的檔案傳輸通訊協定：

- 安全殼層 (SSH) 檔案傳輸通訊協定 (SFTP) — 透過 SSH 進行檔案傳輸。如需詳細資訊，請參閱 the section called “建立啟用 SFTP 的伺服器”。

> **Note**
>
> 我們提供建立 SFTP Transfer Family 伺服器的 AWS CDK 範例。此範例使用 TypeScript，且可在 GitHub 此處取得。

- 文件傳輸協議安全（FTPS）-使用 TLS 加密的文件傳輸。如需詳細資訊，請參閱 the section called "建立啟用 FTP 的伺服器"。
- 檔案傳輸通訊協定 (FTP) — 未加密的檔案傳輸。如需詳細資訊，請參閱 the section called "建立啟用 FTP 的伺服器"。
- 適用性聲明 2 (AS2) — 用於傳輸結構化資料的檔案傳輸。 business-to-business 如需詳細資訊，請參閱 the section called "配置 AS2"。對於 AS2，您可以為演示目的快速創建 AWS CloudFormation 堆棧。有關此程序的說明，請參閱使用範本建立示範 Transfer Family AS2 堆疊。

您可以建立具有多個通訊協定的伺服器。

> **Note**
>
> 如果您為同一伺服器端點啟用了多個通訊協定，並且想要透過多個通訊協定使用相同的使用者名稱來提供存取權，只要您的身分識別提供者中已設定特定於通訊協定的認證，就可以這麼做。對於 FTP，我們建議您保留與 SFTP 和 FTPS 分開的憑證。這是因為，與 SFTP 和 FTPS 不同，FTP 會以純文字形式傳輸認證。藉由將 FTP 認證與 SFTP 或 FTPS 隔離，如果 FTP 認證是共用或公開的，您使用 SFTP 或 FTPS 的工作負載將保持安全。

當您建立伺服器時，您可以選擇特定伺服器 AWS 區域 來執行指派給該伺服器的使用者的檔案作業要求。除了指派伺服器一或多個通訊協定之外，您也可以指派下列其中一種身分識別提供者類型：

- 使用 SSH 金鑰管理的服務。如需詳細資訊，請參閱 與服務管理的使用者合作。
- AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD)。 這個方法可讓您整合您的 Microsoft 作用中目錄群組，以提供 Transfer Family 伺服器的存取權。如需詳細資訊，請參閱 使用 AWS Directory Service 身分識別提供者。
- 自定義方法。自訂身分識別提供者方法使用 AWS Lambda 或 Amazon API Gateway，可讓您整合目錄服務以驗證和授權使用者。此服務會自動指派唯一識別您伺服器的識別符。如需詳細資訊，請參閱使用自訂身分識別提供者。Transfer Family 提供的 AWS CloudFormation 範本可讓您快速部署使用自訂身分識別提供者的伺服器。
  - 用於驗證的 Lambda 函說明使用 Lambda 函數進行驗證的 CloudFormation 範本。

- 使用 API Gateway 方法進行驗證說明使用 Amazon API Gateway 方法進行身份驗證的 CloudFormation範本。

您也可以使用預設伺服器端點為伺服器指派端點類型 (可公開存取或 VPC 託管) 和主機名稱，或使用 Amazon Route 53 服務或使用您選擇的網域名稱系統 (DNS) 服務來指派自訂主機名稱。伺服器主機名稱在建立 AWS 區域 位置必須是唯一的。

此外，您可以指派 Amazon CloudWatch Logging 角色來將事件推送到 CloudWatch 日誌、選擇包含伺服器啟用的加密演算法的安全政策，以及以鍵值配對的標記形式將中繼資料新增至伺服器。

> **Important**
>
> 實例化服務器和數據傳輸需要支付費用。有關定價以及用 AWS Pricing Calculator 於估算 Transfer Family 成本的資訊，請參閱AWS Transfer Family 定價。

建立啟用 SFTP 的伺服器

安全殼層 (SSH) 檔案傳輸通訊協定 (SFTP) 是一種網路通訊協定，用於透過網際網路安全傳輸資料。該協議支持 SSH 的完整安全性和身份驗證功能。它廣泛用於交換數據，包括金融服務，醫療保健，零售和廣告等各種行業的業務合作夥伴之間的敏感信息。

> **Note**
>
> Transfer Family 的 SFTP 伺服器透過連接埠 22 操作。對於 VPC 人雲端託管的端點，SFTP Transfer Family 伺服器也可以透過連接埠 2222 或連接埠 22000 進行操作。如需詳細資訊，請參閱 在虛擬私有雲中建立伺服器。

另請參閱

- 我們提供建立 SFTP Transfer Family 伺服器的 AWS CDK 範例。此範例使用 TypeScript，且可在 GitHub 此處取得。
- 如需如何在 VPC 內部署 Transfer Family 伺服器的逐步解說，請參閱使用 IP 允許清單來保護您的 AWS Transfer Family 伺服器。

若要建立已啟用 SFTP 的伺服器

1. 在 https://console.aws.amazon.com/transfer/ 開啟 AWS Transfer Family 主控台，並從導覽窗格中選取 [伺服器]，然後選擇 [建立伺服器]。
2. 在 [選擇通訊協定] 中選取 [SFTP]，然後選擇 [下一步]。
3. 在 [選擇身分識別提供者] 中，選擇您要用來管理使用者存取權的身分識別提供者。您有下列選項：

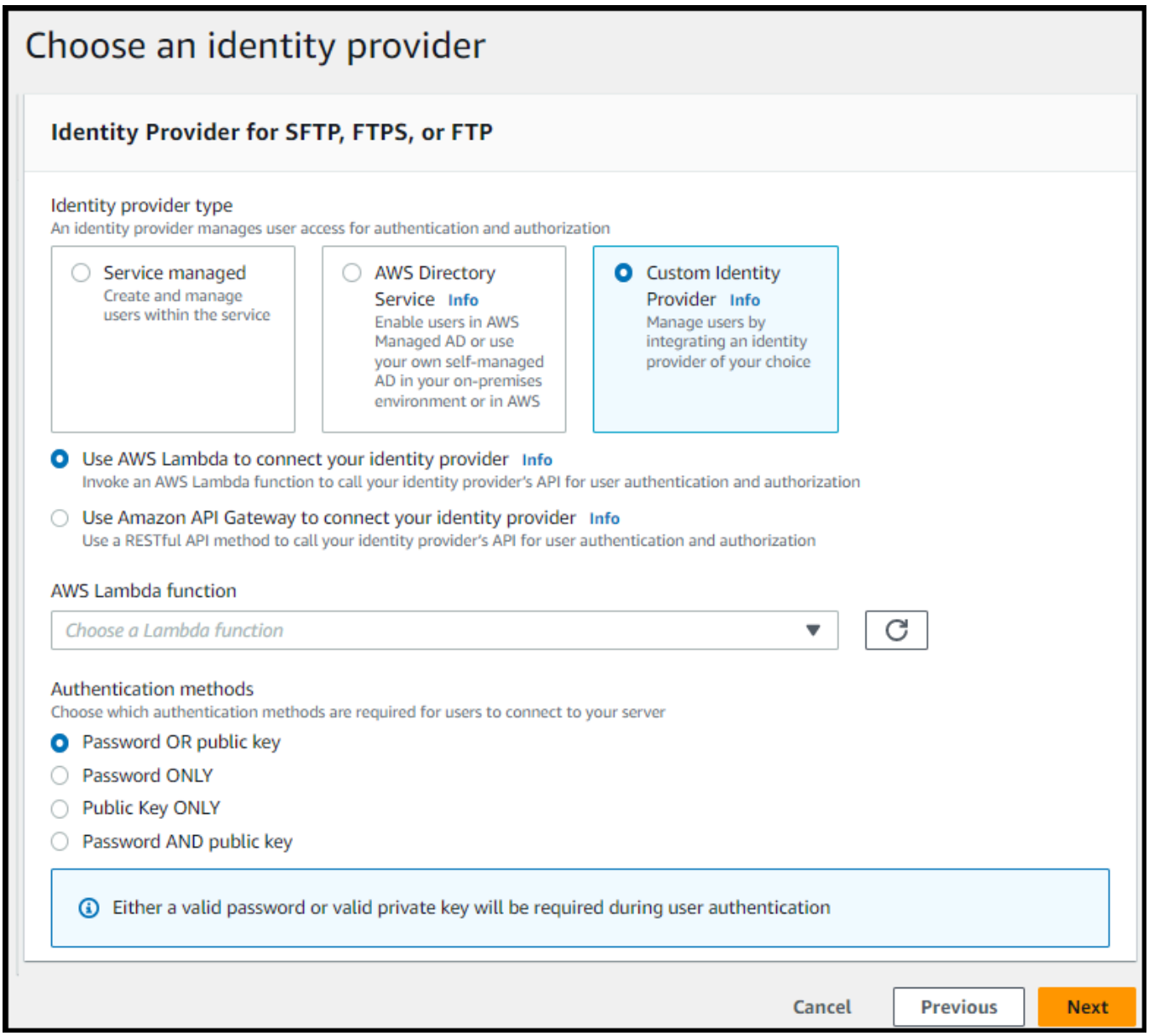
   - 服務受管理 — 您將使用者身分識別和金鑰儲存在中 AWS Transfer Family。
   - AWS Directory Service for Microsoft Active Directory— 您提供存取端點的 AWS Directory Service 目錄。如此一來，您就可以使用儲存在 Active Directory 中的認證來驗證您的使用者。若要深入瞭解如何使用 AWS Managed Microsoft AD 身分識別提供者，請參閱使用 AWS Directory Service 身分識別提供者。

     > **Note**
     > - 不支援跨帳戶和共用目錄。 AWS Managed Microsoft AD
     > - 若要將 Directory Service 設定為您的身分識別提供者的伺服器，您需要新增一些 AWS Directory Service 權限。如需詳細資訊，請參閱 開始使用之前 AWS Directory Service for Microsoft Active Directory。

   - 自訂身分識別提供者 — 選擇下列其中一個選項：
     - 用於連 AWS Lambda 接您的身分提供者 — 您可以使用由 Lambda 函數支援的現有身分識別提供者。您提供 Lambda 函數的名稱。如需詳細資訊，請參閱 用 AWS Lambda 於整合您的身分識別提供者。
     - 使用 Amazon API Gateway 連接您的身分供應商 — 您可以建立由 Lambda 函數支援的 API Gateway 方法，用作身分識別供應商。您提供 Amazon API Gateway 網址和叫用角色。如需詳細資訊，請參閱 使用 Amazon API Gateway 整合您的身分供應商。

   對於任一選項，您也可以指定如何進行驗證。

   - 密碼或金鑰 — 使用者可以使用其密碼或金鑰進行驗證。這是預設值。
   - 僅限密碼 — 使用者必須提供密碼才能連線。
   - 僅限金鑰 — 使用者必須提供私密金鑰才能連線。
   - 密碼與金鑰 — 使用者必須同時提供私密金鑰和密碼才能連線。伺服器會先檢查金鑰，然後如果金鑰有效，系統會提示輸入密碼。如果提供的私密金鑰與儲存的公開金鑰不符，驗證會失敗。



4. 選擇下一步。
5. 在 [選擇端點] 中，執行下列動作：

   a. 對於端點類型，請選擇可公開存取的端點類型。如需 VPC 託管端點的資訊，請參閱在虛擬私有雲中建立伺服器。

   b. (選擇性) 對於自訂主機名稱，請選擇無。

      您會取得由提供的伺服器主機名稱 AWS Transfer Family。伺服器主機名稱的格式為 *serverId*.server.transfer.*regionId*.amazonaws.com。

對於自訂主機名稱，您可以為伺服器端點指定自訂別名。若要進一步瞭解如何使用自訂主機名稱，請參閱使用自訂主機名稱。

c. (選擇性) 對於啟用 FIPS，請選取已啟用 FIPS 的端點核取方塊，以確保端點符合聯邦資訊處理標準 (FIPS)。

> **Note**
>
> 已啟用 FIPS 的端點僅適用於北美 AWS 地區。如需可用區AWS Transfer Family 域，請參閱 AWS 一般參考. 如需 FIPS 的詳細資訊，請參閱聯邦資訊處理標準 (FIPS) 140-2。

d. 選擇下一步。

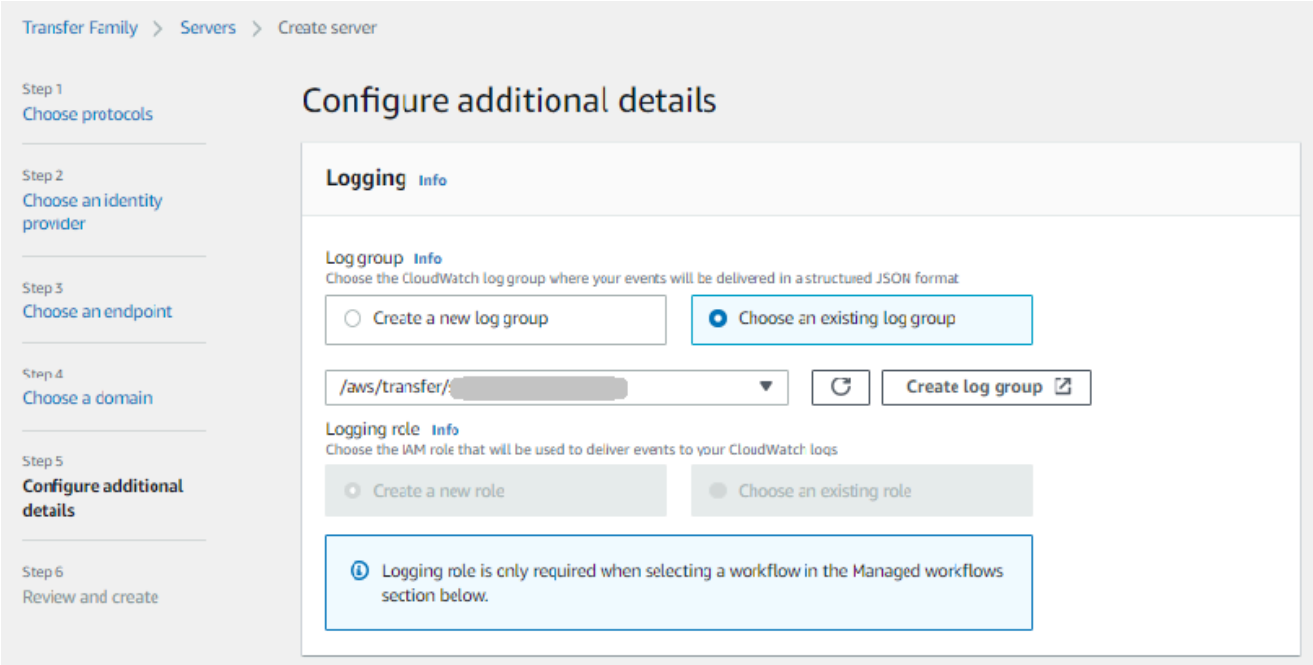
6. 在 [選擇網域] 頁面上，選擇您要用來透過所選通訊協定 AWS 儲存和存取資料的儲存服務：

   - 選擇 Amazon S3，透過所選通訊協定以物件形式存放和存取檔案。
   - 選擇 Amazon EFS，透過選取的通訊協定存放和存取 Amazon EFS 檔案系統中的檔案。

   選擇下一步。

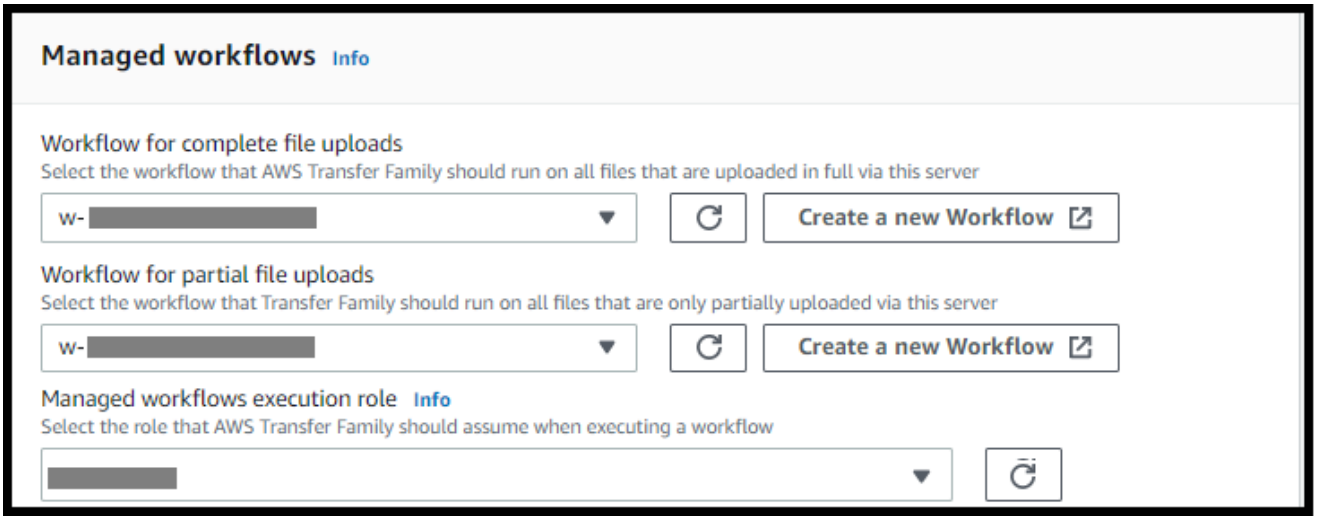
7. 在設定其他詳細資料中，執行下列動作：

   a. 若要進行記錄，請指定現有的記錄群組或建立新的記錄群組 (預設選項)。如果您選擇現有的記錄群組，則必須選取與 AWS 帳戶.



如果您選擇 [建立記錄群組]，CloudWatch 主控台 (https://console.aws.amazon.com/cloudwatch/) 會開啟 [建立記錄群組] 頁面。如需詳細資訊，請參閱在 CloudWatch 記錄檔中建立記錄群組。

b. (選擇性) 對於「受管理的工作流程」，請選擇「Transfer Family」在執行工作流程時應承擔的工作流程 ID (以及對應角色)。您可以選擇一個工作流程在完成上載時執行，另一個工作流程在部分上傳時執行。若要進一步瞭解如何使用受管理的工作流程處理檔案，請參閱AWS Transfer Family 管理工作流。



c. 對於密碼編譯演算法選項，請選擇包含伺服器啟用的加密演算法的安全性原則。我們最新的安全性政策為預設值：如需詳細資訊，請參閱AWS Transfer Family 伺服器的安全性原則。

d. (選擇性) 對於「伺服器主機金鑰」，請輸入 RSA、ED25519 或 ECDSA 私密金鑰，當用戶端透過 SFTP 連線至伺服器時，用來識別伺服器。您也可以加入描述以區分多個主機金鑰。

建立伺服器之後，您可以新增其他主機金鑰。如果您想要旋轉金鑰或想要使用不同類型的金鑰 (例如 RSA 金鑰和 ECDSA 金鑰)，則擁有多個主機金鑰非常有用。

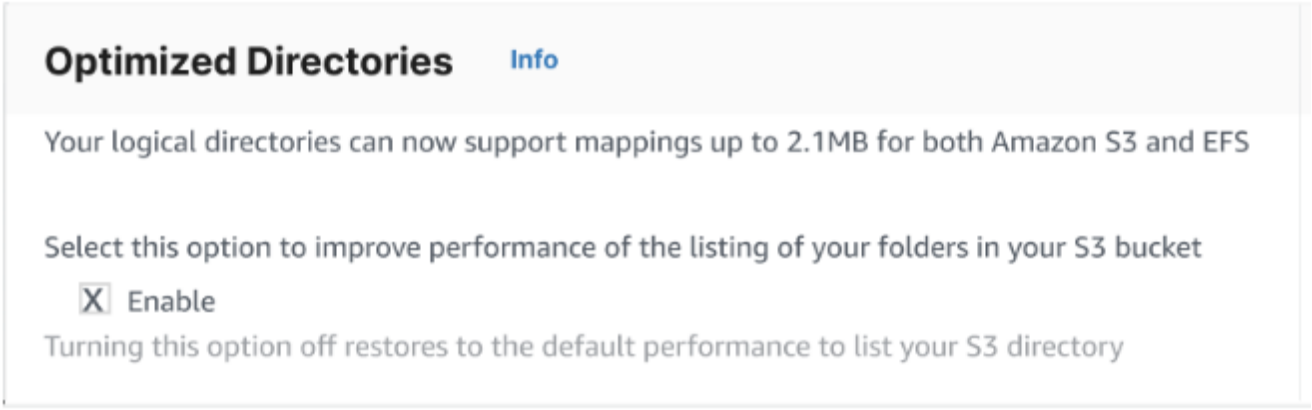
> **Note**
>
> 「伺服器主機金鑰」區段僅用於從現有啟用 SFTP 的伺服器移轉使用者。

e. (選擇性) 對於標籤，對於「鍵值」和「值」，輸入一或多個標籤作為鍵值配對，然後選擇「新增標籤」。

f. 選擇下一步。

g. 您可以優化 Amazon S3 目錄的效能。例如，假設您進入您的主目錄，並且您有 10,000 個子目錄。換句話說，您的 Amazon S3 存儲桶有 10,000 個文件夾。在這個案例中，如果您執行 `ls` (list) 命令，清單作業需要六到八分鐘之間。但是，如果您最佳化您的目錄，此作業只需要幾秒鐘的時間。

當您使用主控台建立伺服器時，依預設會啟用最佳化的目錄。如果您使用 API 建立伺服器，則預設不會啟用此行為。

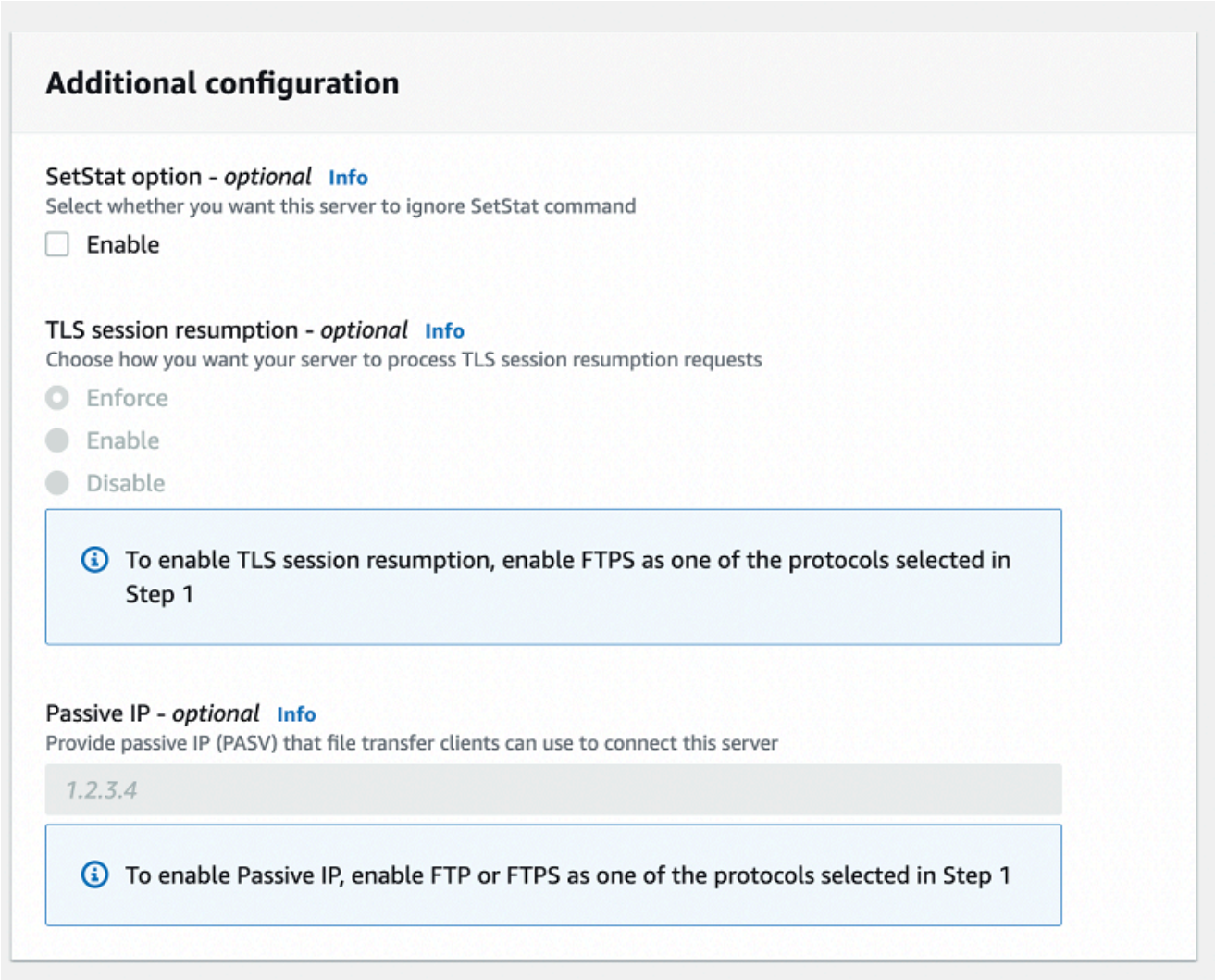


h. (選擇性) 將 AWS Transfer Family 伺服器設定為向您的使用者顯示自訂訊息，例如組織原則或條款與條件。在 [顯示橫幅] 中，在 [預先驗證顯示橫幅] 文字方塊中，輸入您要在使用者進行驗證之前顯示的文字訊息。

i. (選擇性) 您可以設定下列其他選項。

- SetStat 選項：啟用此選項可忽略用戶端嘗試在您上傳至 Amazon S3 儲存貯體的檔案`SETSTAT`上使用時產生的錯誤。如需其他詳細資訊，請參`SetStatOption`閱中的文件ProtocolDetails。

- TLS 工作階段恢復：只有在您已啟用 FTPS 作為此伺服器的其中一個通訊協定時，才能使用此選項。
- 被動 IP：只有在您已啟用 FTPS 或 FTP 作為此伺服器的其中一個通訊協定時，才能使用此選項。



8. 在「檢閱並建立」中，檢閱您的選擇。

- 如果您要編輯其中任何一個，請選擇步驟旁邊的「編輯」。

> **Note**
>
> 您必須在選擇要編輯的步驟之後檢閱每個步驟。

- 如果您沒有變更，請選擇 [建立伺服器] 來建立您的伺服器。您會前往顯示下列內容的 Servers (伺服器) 頁面，這裡會列出您的新伺服器。

新伺服器的狀態變更為「線上」可能需要幾分鐘的時間。此時，您的伺服器可以執行檔案作業，但您必須先建立使用者。如需建立使用者的詳細資訊，請參閱管理伺服器端點的使用者。

建立啟用 FTP 的伺服器

通過 SSL（FTPS）的文件傳輸協議是 FTP 的擴展。它使用傳輸層安全性 (TLS) 和安全通訊端層 (SSL) 加密通訊協定來加密流量。FTPS 允許同時或獨立地對控制和數據通道連接進行加密。

若要建立已啟用 FTP 的伺服器

1. 在 https://console.aws.amazon.com/transfer/ 開啟 AWS Transfer Family 主控台，並從導覽窗格中選取 [伺服器]，然後選擇 [建立伺服器]。
2. 在 [選擇通訊協定] 中，選取 FTPS。

   對於「伺服器憑證」，請選擇儲存於 AWS Certificate Manager (ACM) 的憑證，當用戶端透過 FTPS 連線至伺服器時，該憑證將用來識別您的伺服器，然後選擇「下一步」。

   若要要求新的公用憑證，請參閱AWS Certificate Manager 使用者指南中的要求公用憑證。

   若要將現有憑證匯入 ACM，請參閱《AWS Certificate Manager 使用指南》中的〈將憑證匯入 ACM〉。

   若要要求私有憑證以透過私有 IP 位址使用 FTPS，請參閱使用AWS Certificate Manager 者指南中的要求私人憑證。

   支援具有下列密碼編譯演算法和金鑰大小的憑證：

   - 2048 位元 RSA (RSA_2048)
   - 4096 位元 RSA (RSA_4096)
   - 橢圓定焦曲線 256 位元 (EC_prime256v1)
   - 橢圓定焦曲線 384 位元 (EC_secp384r1)
   - 橢圓定焦曲線 521 位元 (EC_secp521r1)

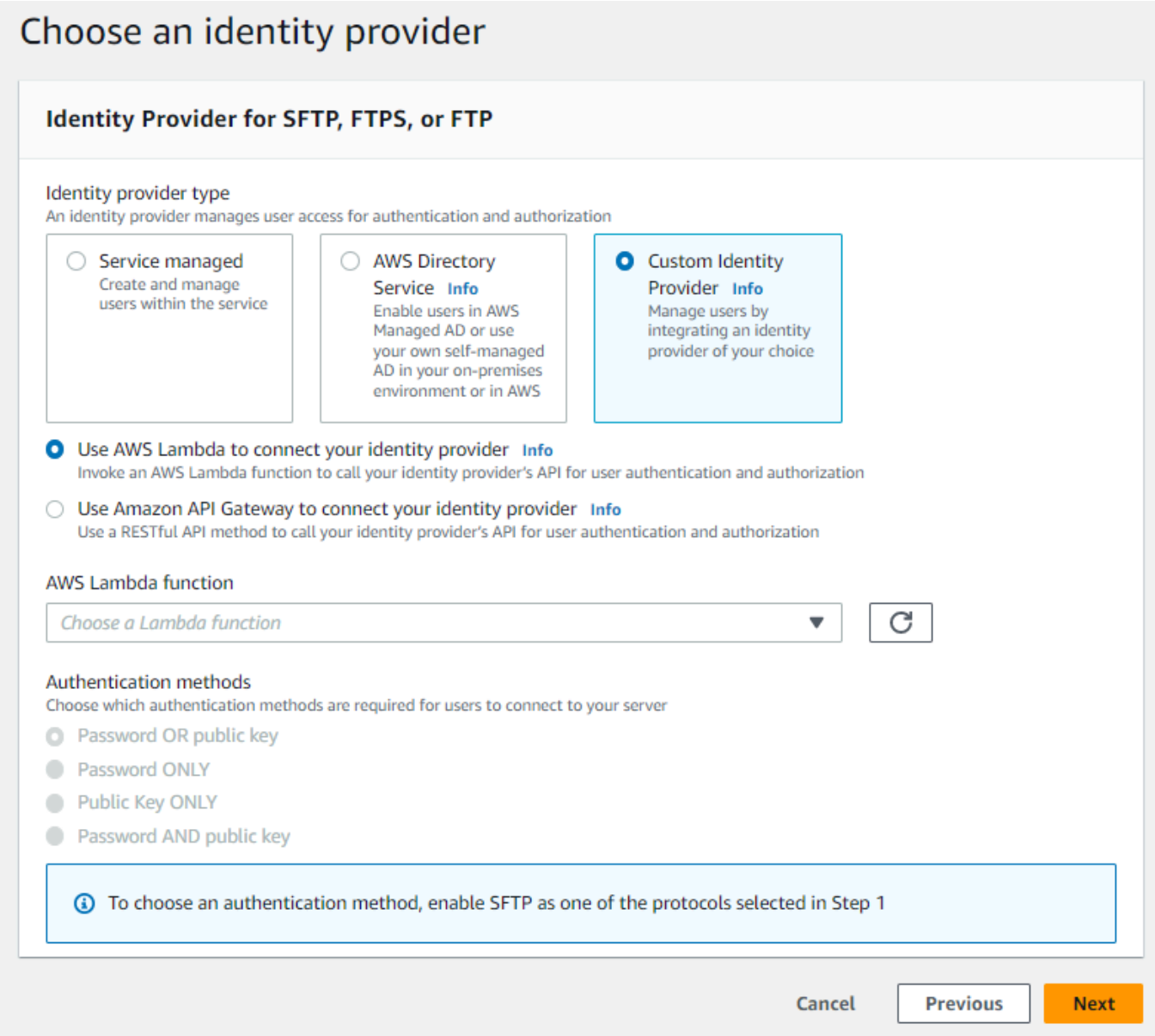
> **Note**
>
> 憑證必須是有效的 SSL/TLS X.509 第 3 版憑證，且其中指定了 FQDN 或 IP 位址，並包含發行者的相關資訊。

3. 在 [選擇身分識別提供者] 中，選擇您要用來管理使用者存取權的身分識別提供者。您有下列選項：

   - AWS Directory Service for Microsoft Active Directory— 您提供存取端點的 AWS Directory Service 目錄。如此一來，您就可以使用儲存在 Active Directory 中的認證來驗證您的使用者。若要深入瞭解如何使用 AWS Managed Microsoft AD 身分識別提供者，請參閱使用 AWS Directory Service 身分識別提供者。

     > **Note**
     >
     > - 不支援跨帳戶和共用目錄。 AWS Managed Microsoft AD
     > - 若要將 Directory Service 設定為您的身分識別提供者的伺服器，您需要新增一些 AWS Directory Service 權限。如需詳細資訊，請參閱 開始使用之前 AWS Directory Service for Microsoft Active Directory。

   - 自訂身分識別提供者 — 選擇下列其中一個選項：
     - 用於連 AWS Lambda 接您的身分提供者 — 您可以使用由 Lambda 函數支援的現有身分識別提供者。您提供 Lambda 函數的名稱。如需詳細資訊，請參閱 用 AWS Lambda 於整合您的身分識別提供者。
     - 使用 Amazon API Gateway 連接您的身分供應商 — 您可以建立由 Lambda 函數支援的 API Gateway 方法，用作身分識別供應商。您提供 Amazon API Gateway 網址和叫用角色。如需詳細資訊，請參閱 使用 Amazon API Gateway 整合您的身分供應商。



4. 選擇下一步。
5. 在 [選擇端點] 中，執行下列動作：

> **Note**
>
> 適用於 Transfer Family 的 FTPS 伺服器可在連接埠 21 (控制通道) 和連接埠範圍 8192—8200 (資料通道) 上運作。

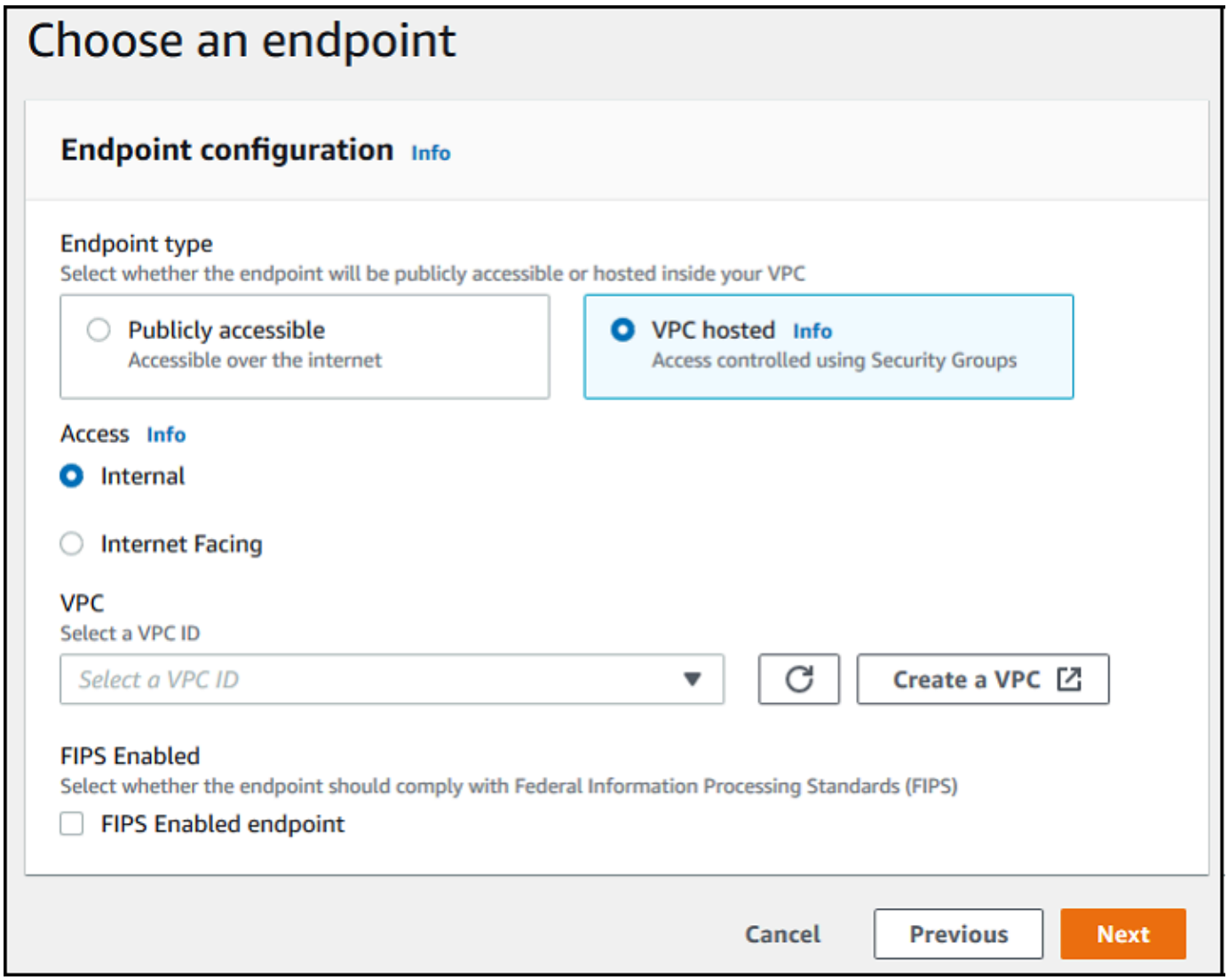
a. 對於端點類型，請選擇 VPC 託管端點類型來託管伺服器的端點。如需有關設定 VPC 託管端點的資訊，請參閱在虛擬私有雲中建立伺服器。

> **Note**
>
> 不支援可公開存取的端點。

b. (選擇性) 對於啟用 FIPS，請選取已啟用 FIPS 的端點核取方塊，以確保端點符合聯邦資訊處理標準 (FIPS)。

> **Note**
>
> 已啟用 FIPS 的端點僅適用於北美 AWS 地區。如需可用區AWS Transfer Family 域，請參閱 AWS 一般參考. 如需 FIPS 的詳細資訊，請參閱聯邦資訊處理標準 (FIPS) 140-2。

c. 選擇下一步。



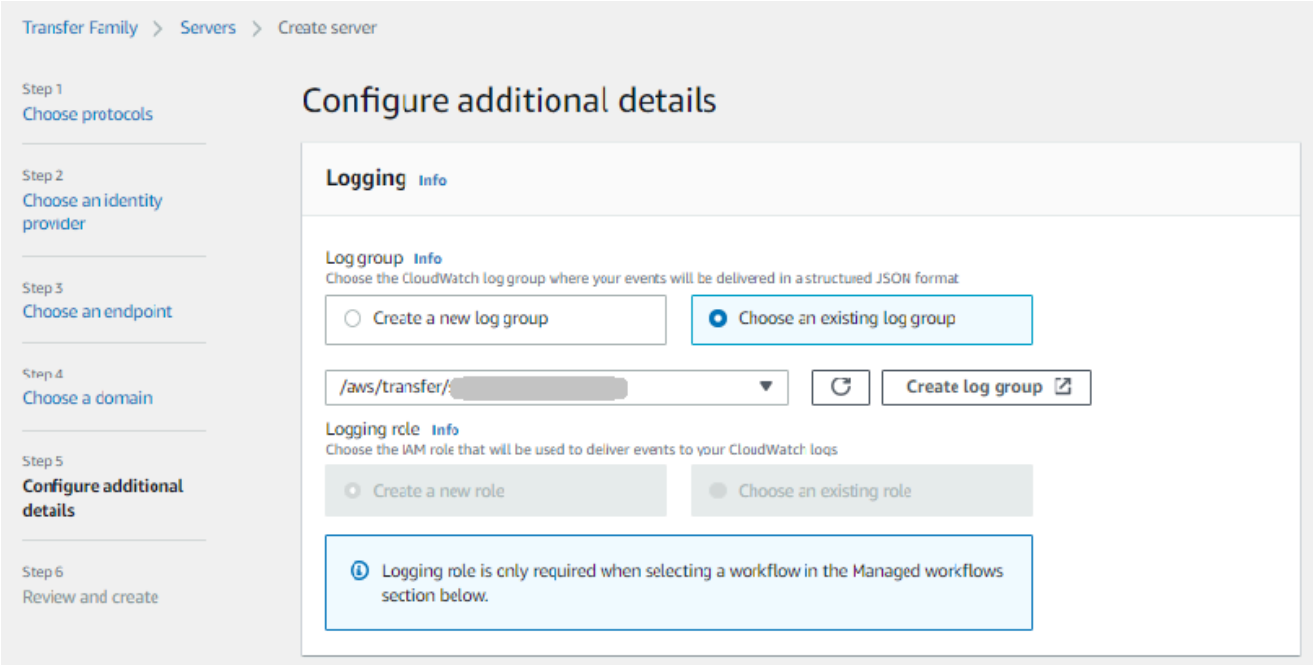
6. 在 [選擇網域] 頁面上，選擇您要用來透過所選通訊協定 AWS 儲存和存取資料的儲存服務：

   - 選擇 Amazon S3，透過所選通訊協定以物件形式存放和存取檔案。
   - 選擇 Amazon EFS，透過選取的通訊協定存放和存取 Amazon EFS 檔案系統中的檔案。

   選擇下一步。

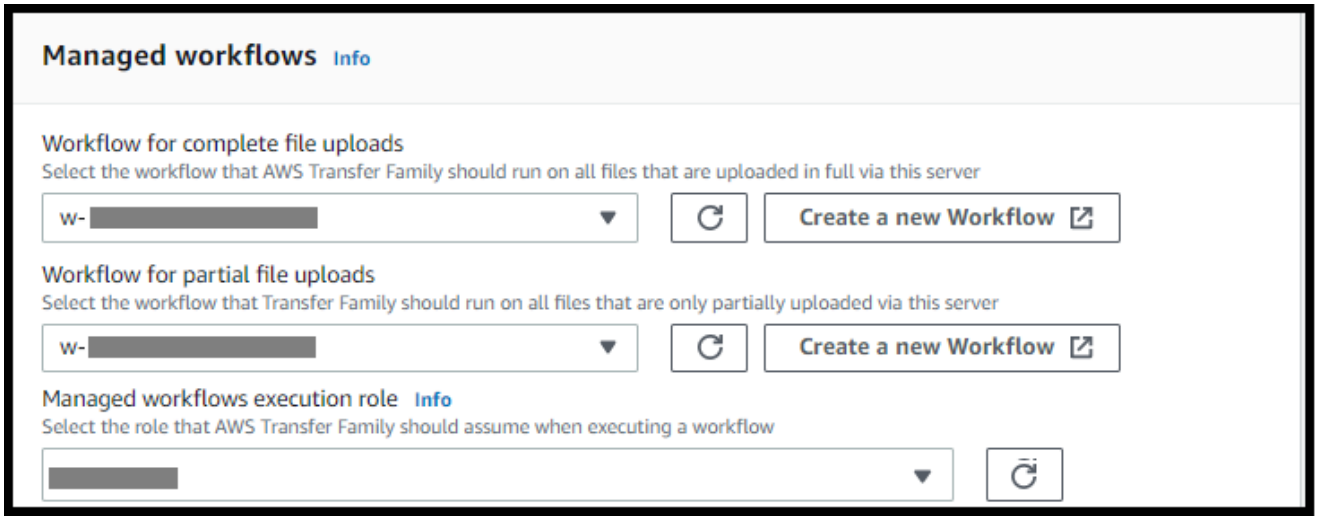
7. 在設定其他詳細資料中，執行下列動作：

   a. 若要進行記錄，請指定現有的記錄群組或建立新的記錄群組 (預設選項)。



如果您選擇 [建立記錄群組]，CloudWatch 主控台 (https://console.aws.amazon.com/cloudwatch/) 會開啟 [建立記錄群組] 頁面。如需詳細資訊，請參閱在 CloudWatch 記錄檔中建立記錄群組。

b. (選擇性) 對於「受管理的工作流程」，請選擇「Transfer Family」在執行工作流程時應承擔的工作流程 ID (以及對應角色)。您可以選擇一個工作流程在完成上載時執行，另一個工作流程在部分上傳時執行。若要進一步瞭解如何使用受管理的工作流程處理檔案，請參閱AWS Transfer Family 管理工作流。



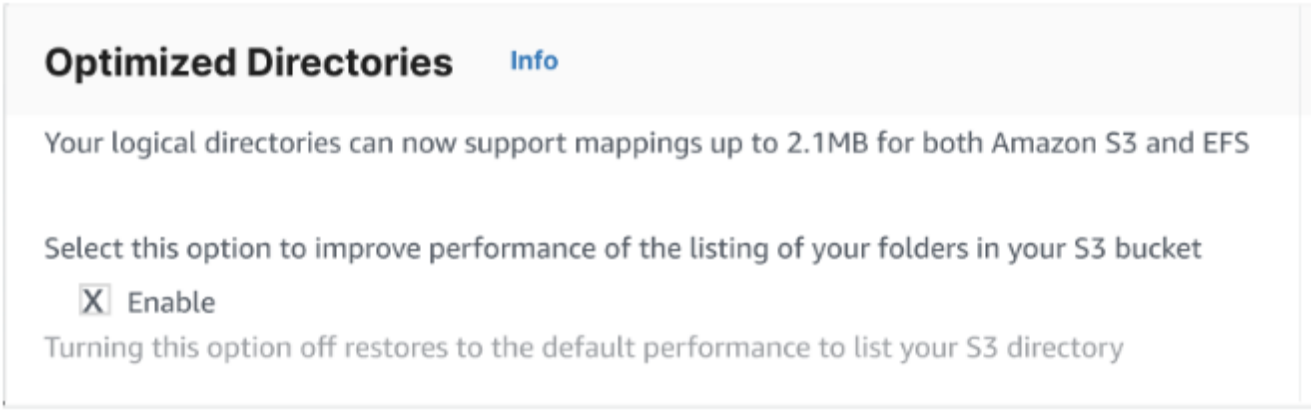
c. 對於密碼編譯演算法選項，請選擇包含伺服器啟用的加密演算法的安全性原則。我們最新的安全性政策為預設值：如需詳細資訊，請參閱AWS Transfer Family 伺服器的安全性原則。

d. 對於伺服器主機金鑰，請將其保留空白。

e. (選擇性) 對於標籤，對於「鍵值」和「值」，輸入一或多個標籤作為鍵值配對，然後選擇「新增標籤」。

f. 您可以優化 Amazon S3 目錄的效能。例如，假設您進入您的主目錄，並且您有 10,000 個子目錄。換句話說，您的 Amazon S3 存儲桶有 10,000 個文件夾。在這個案例中，如果您執行 `ls` (list) 命令，清單作業需要六到八分鐘之間。但是，如果您最佳化您的目錄，此作業只需要幾秒鐘的時間。

   當您使用主控台建立伺服器時，依預設會啟用最佳化的目錄。如果您使用 API 建立伺服器，則預設不會啟用此行為。



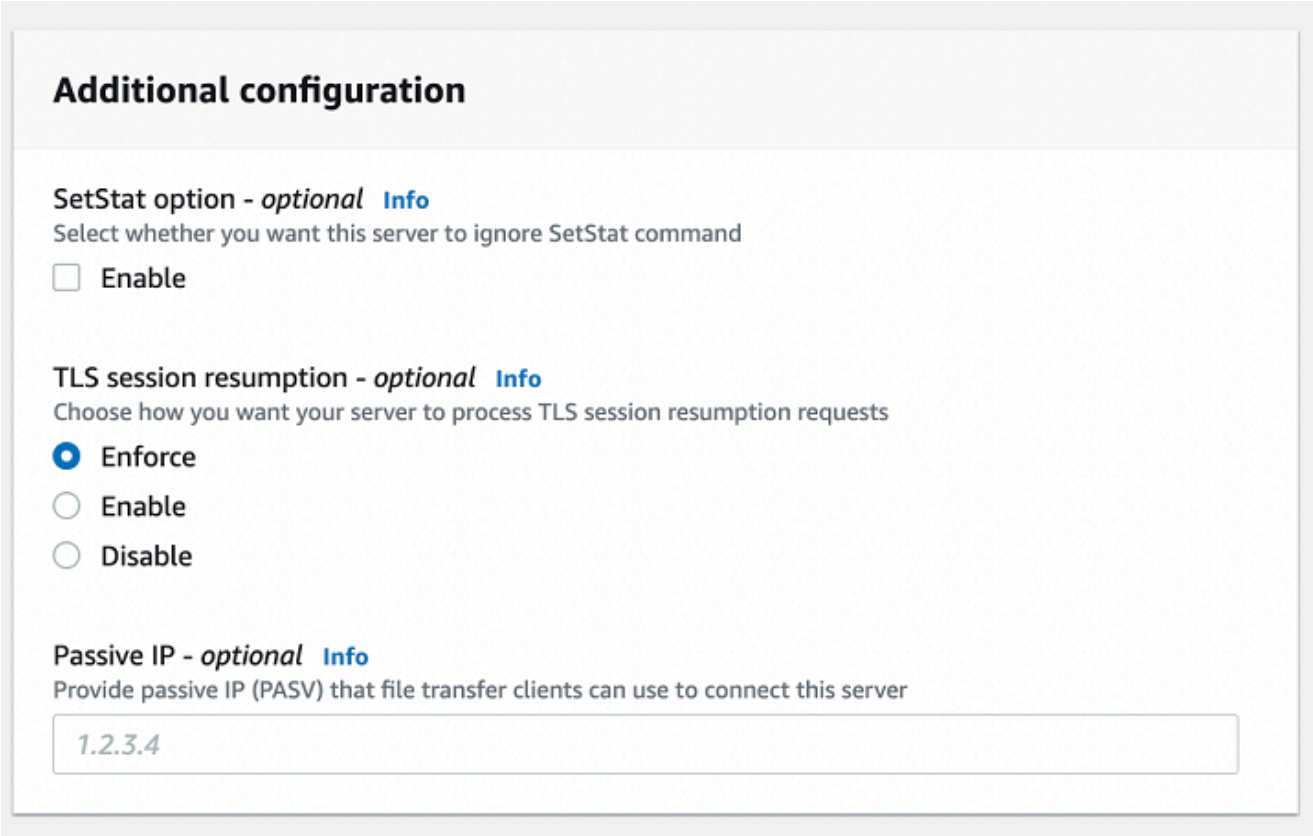
g. 選擇下一步。

h. (選擇性) 您可以將 AWS Transfer Family 伺服器設定為向使用者顯示自訂訊息，例如組織原則或條款與條件。您也可以向已成功驗證的使用者顯示自訂的每日訊息 (MOTD)。

   在 [顯示橫幅] 中，在 [驗證前顯示橫幅] 文字方塊中，輸入您要在使用者進行驗證前顯示的文字訊息，然後在驗證後顯示橫幅文字方塊中，輸入使用者成功驗證後要顯示的文字。

i. (選擇性) 您可以設定下列其他選項。

   - SetStat 選項：啟用此選項可忽略用戶端嘗試在您上傳至 Amazon S3 儲存貯體的檔案`SETSTAT`上使用時產生的錯誤。如需其他詳細資訊，請參`SetStatOption`閱ProtocolDetails主題中的文件。
   - TLS 工作階段重新開始：提供一種機制，可在 FTPS 工作階段的控制項和資料連線之間繼續或共用協商的密鑰。如需其他詳細資訊，請參`TlsSessionResumptionMode`閱ProtocolDetails主題中的文件。
   - 被動 IP：表示被動模式，用於 FTP 和 FTPS 協議。輸入單一 IPv4 地址，例如防火牆、路由器或負載平衡器的公有 IP 地址。如需其他詳細資訊，請參`PassiveIp`閱ProtocolDetails主題中的文件。



8. 在「檢閱並建立」中，檢閱您的選擇。

   - 如果您要編輯其中任何一個，請選擇步驟旁邊的「編輯」。

     > **Note**
     >
     > 您必須在選擇要編輯的步驟之後檢閱每個步驟。

   - 如果您沒有變更，請選擇 [建立伺服器] 來建立您的伺服器。您會前往顯示下列內容的 Servers (伺服器) 頁面，這裡會列出您的新伺服器。

新伺服器的狀態變更為「線上」可能需要幾分鐘的時間。此時，您的伺服器會執行您使用者的檔案操作。

後續步驟：下一步，請繼續進行使用自訂身分識別提供者以設定使用者。

建立啟用 FTP 的伺服器

檔案傳輸通訊協定 (FTP) 是用於傳輸資料的網路通訊協定。FTP 使用單獨的通道進行控制和數據傳輸。控制通道會開啟，直到終止或閒置逾時為止。資料通道在傳輸期間處於作用中狀態。FTP 使用純文本，不支持流量加密。

> **Note**
>
> 啟用 FTP 時，您必須選擇 VPC 人雲端託管端點的內部存取選項。如果您需要伺服器讓資料遍歷公用網路，則必須使用安全通訊協定，例如 SFTP 或 FTPS。

若要建立啟用 FTP 的伺服器

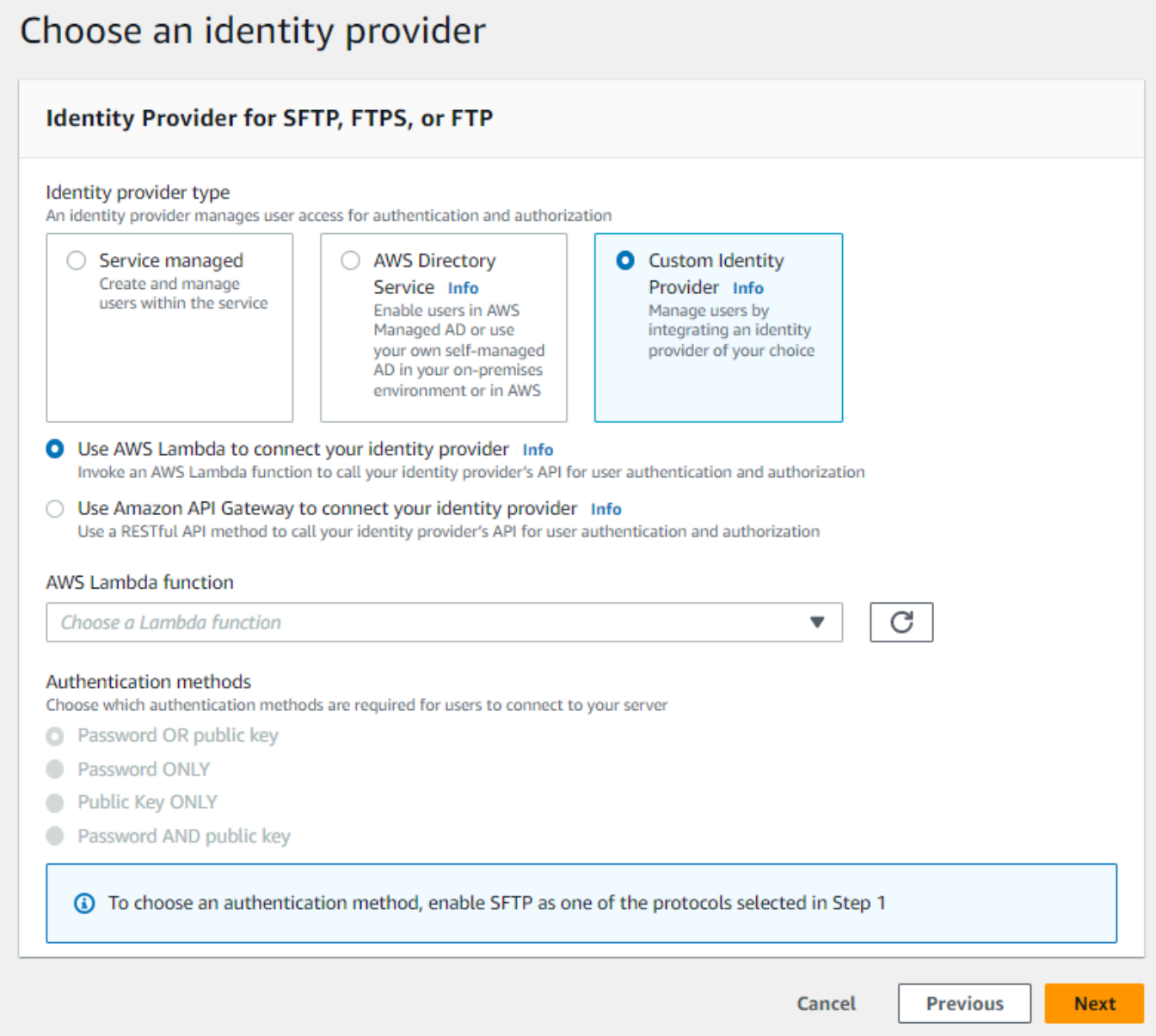
1. 在 https://console.aws.amazon.com/transfer/ 開啟 AWS Transfer Family 主控台，並從導覽窗格中選取 [伺服器]，然後選擇 [建立伺服器]。
2. 在 [選擇協定] 中，選取 [FTP]，然後選擇 [下一步]。
3. 在 [選擇身分識別提供者] 中，選擇您要用來管理使用者存取權的身分識別提供者。您有下列選項：

   - AWS Directory Service for Microsoft Active Directory— 您提供存取端點的 AWS Directory Service 目錄。如此一來，您就可以使用儲存在 Active Directory 中的認證來驗證您的使用者。若要深入瞭解如何使用 AWS Managed Microsoft AD 身分識別提供者，請參閱使用 AWS Directory Service 身分識別提供者。

     > **Note**
     >
     > - 不支援跨帳戶和共用目錄。 AWS Managed Microsoft AD
     > - 若要將 Directory Service 設定為您的身分識別提供者的伺服器，您需要新增一些 AWS Directory Service 權限。如需詳細資訊，請參閱 開始使用之前 AWS Directory Service for Microsoft Active Directory。

   - 自訂身分識別提供者 — 選擇下列其中一個選項：
     - 用於連 AWS Lambda 接您的身分提供者 — 您可以使用由 Lambda 函數支援的現有身分識別提供者。您提供 Lambda 函數的名稱。如需詳細資訊，請參閱 用 AWS Lambda 於整合您的身分識別提供者。

- 使用 Amazon API Gateway 連接您的身分供應商 — 您可以建立由 Lambda 函數支援的 API Gateway 方法，用作身分識別供應商。您提供 Amazon API Gateway 網址和叫用角色。如需詳細資訊，請參閱 使用 Amazon API Gateway 整合您的身分供應商。



4. 選擇下一步。
5. 在 [選擇端點] 中，執行下列動作：

> **Note**
>
> Transfer Family 的 FTP 伺服器在連接埠 21 (控制通道) 和連接埠範圍 8192—8200 (資料通道) 上運作。

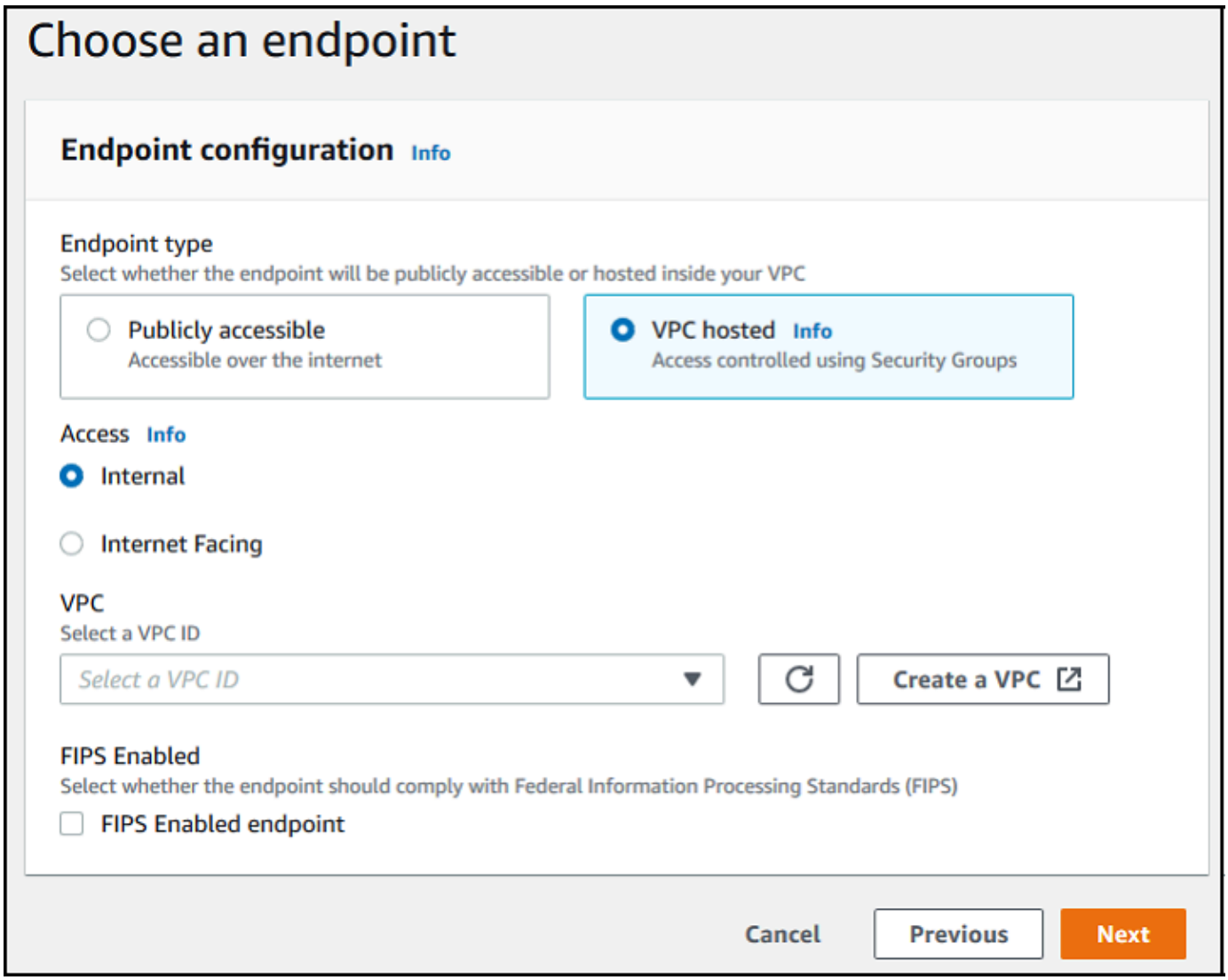
a. 對於端點類型，請選擇託管服務器端點的 VPC 託管。如需有關設定 VPC 託管端點的資訊，請參閱在虛擬私有雲中建立伺服器。

> **Note**
>
> 不支援可公開存取的端點。

b. 對於 FIPS 已啟用，請保持清除 FIPS 啟用端點核取方塊。

> **Note**
>
> FTP 伺服器不支援啟用 FIPS 的端點。

c. 選擇下一步。



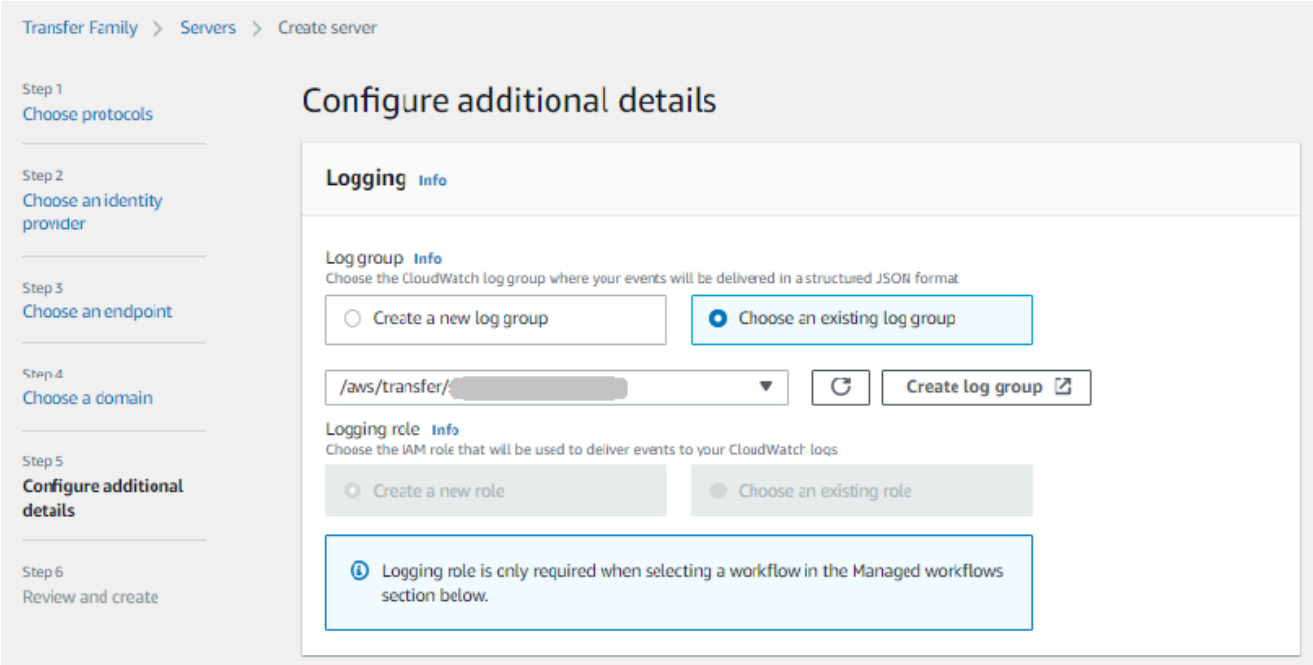
6. 在 [選擇網域] 頁面上，選擇您要用來透過所選通訊協定 AWS 儲存和存取資料的儲存服務。

   - 選擇 Amazon S3，透過所選通訊協定以物件形式存放和存取檔案。
   - 選擇 Amazon EFS，透過選取的通訊協定存放和存取 Amazon EFS 檔案系統中的檔案。

   選擇下一步。

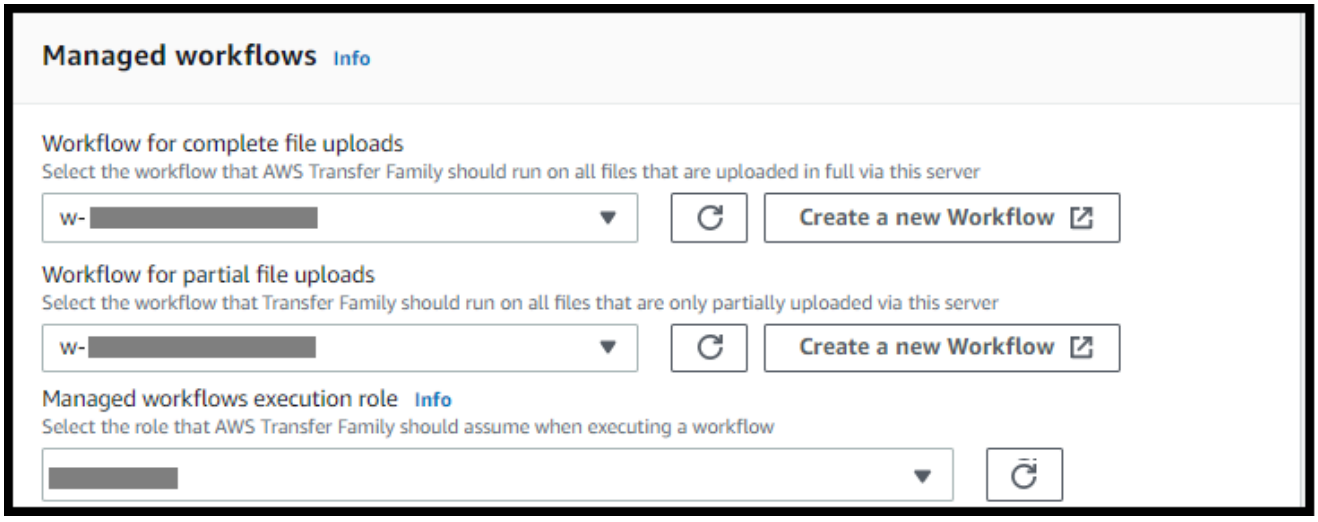
7. 在設定其他詳細資料中，執行下列動作：

   a. 若要進行記錄，請指定現有的記錄群組或建立新的記錄群組 (預設選項)。



如果您選擇 [建立記錄群組]，CloudWatch 主控台 (https://console.aws.amazon.com/cloudwatch/) 會開啟 [建立記錄群組] 頁面。如需詳細資訊，請參閱在 CloudWatch 記錄檔中建立記錄群組。

b. (選擇性) 對於「受管理的工作流程」，請選擇「Transfer Family」在執行工作流程時應承擔的工作流程 ID (以及對應角色)。您可以選擇一個工作流程在完成上載時執行，另一個工作流程在部分上傳時執行。若要進一步瞭解如何使用受管理的工作流程處理檔案，請參閱AWS Transfer Family 管理工作流。



c. 對於密碼編譯演算法選項，請選擇包含伺服器啟用的加密演算法的安全性原則。

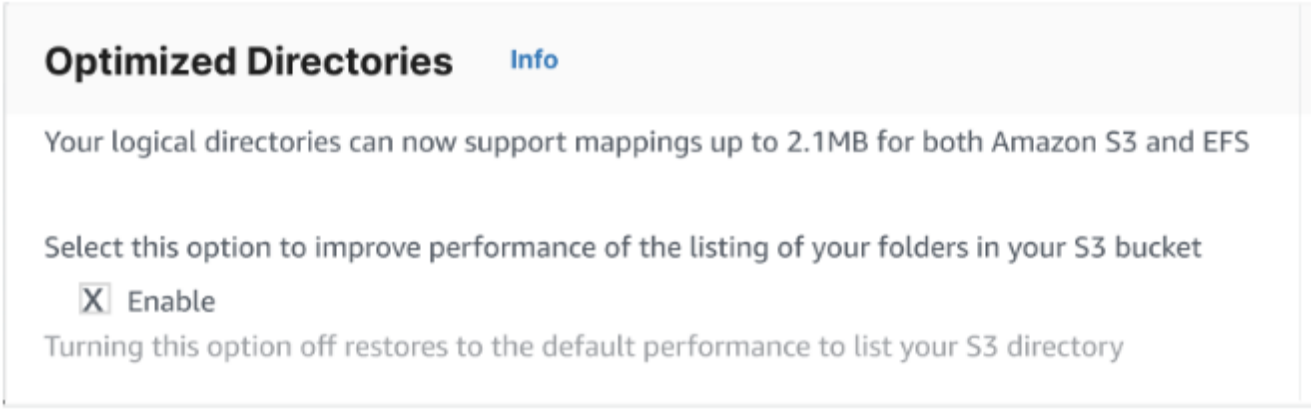
> **Note**
>
> Transfer Family 分配最新的安全策略到您的 FTP 服務器。不過，由於 FTP 通訊協定並未使用任何加密，因此 FTP 伺服器不會使用任何安全性原則演算法。除非您的伺服器也使用 FTPS 或 SFTP 通訊協定，否則安全性原則會維持未使用狀態。

d. 對於伺服器主機金鑰，請將其保留空白。

e. (選擇性) 對於標籤，對於「鍵值」和「值」，輸入一或多個標籤作為鍵值配對，然後選擇「新增標籤」。

f. 您可以優化 Amazon S3 目錄的效能。例如，假設您進入您的主目錄，並且您有 10,000 個子目錄。換句話說，您的 Amazon S3 存儲桶有 10,000 個文件夾。在這個案例中，如果您執行 `ls` (list) 命令，清單作業需要六到八分鐘之間。但是，如果您最佳化您的目錄，此作業只需要幾秒鐘的時間。

   當您使用主控台建立伺服器時，依預設會啟用最佳化的目錄。如果您使用 API 建立伺服器，則預設不會啟用此行為。



g. 選擇下一步。

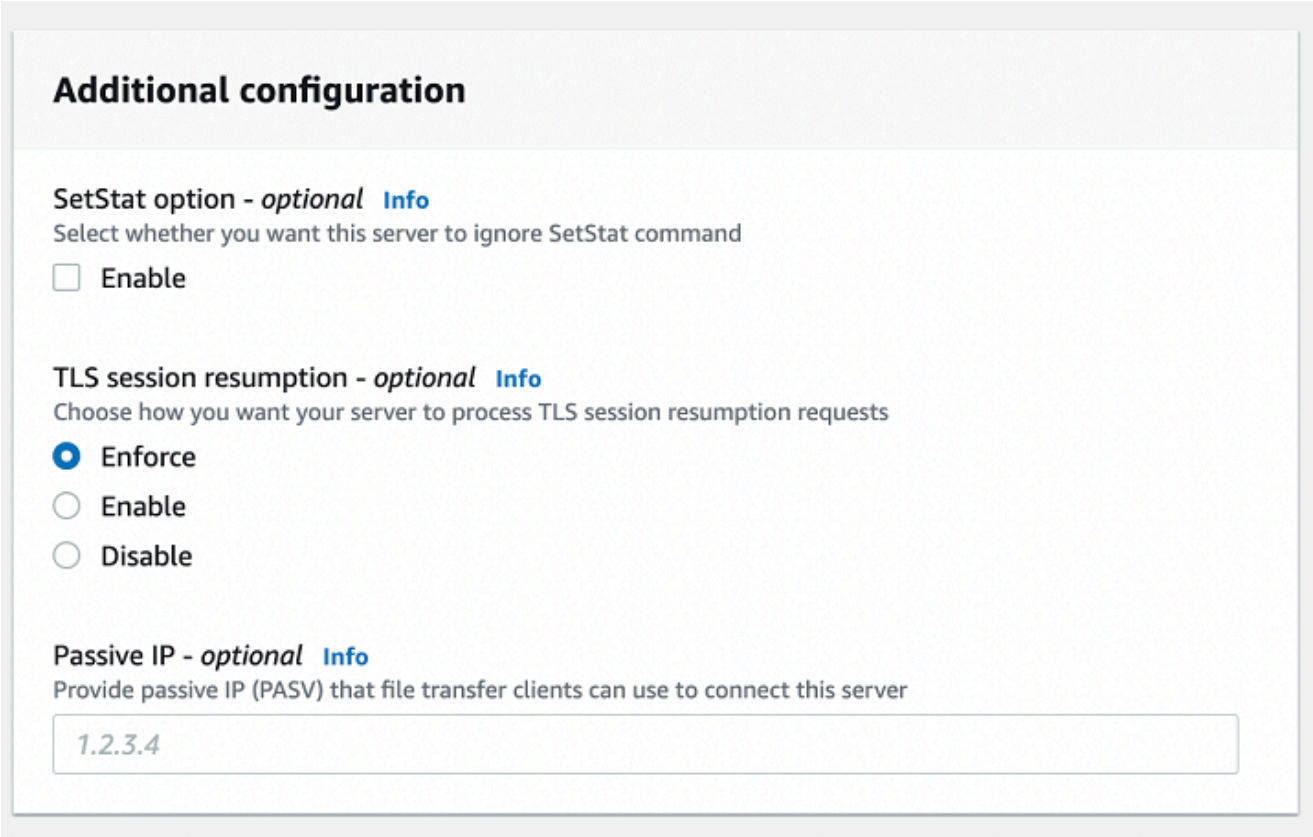
h. (選擇性) 您可以將 AWS Transfer Family 伺服器設定為向使用者顯示自訂訊息，例如組織原則或條款與條件。您也可以向已成功驗證的使用者顯示自訂的每日訊息 (MOTD)。

   在 [顯示橫幅] 中，在 [驗證前顯示橫幅] 文字方塊中，輸入您要在使用者進行驗證前顯示的文字訊息，然後在驗證後顯示橫幅文字方塊中，輸入使用者成功驗證後要顯示的文字。

i. (選擇性) 您可以設定下列其他選項。

   - SetStat 選項：啟用此選項可忽略用戶端嘗試在您上傳至 Amazon S3 儲存貯體的檔案`SETSTAT`上使用時產生的錯誤。如需其他詳細資訊，請參`SetStatOption`閱ProtocolDetails主題中的文件。

- TLS 工作階段重新開始：提供一種機制，可在 FTPS 工作階段的控制項和資料連線之間繼續或共用協商的密鑰。如需其他詳細資訊，請參`TlsSessionResumptionMode`閱ProtocolDetails主題中的文件。
- 被動 IP：表示被動模式，用於 FTP 和 FTPS 協議。輸入單一 IPv4 地址，例如防火牆、路由器或負載平衡器的公有 IP 地址。如需其他詳細資訊，請參`PassiveIp`閱ProtocolDetails主題中的文件。



8. 在「檢閱並建立」中，檢閱您的選擇。

- 如果您要編輯其中任何一個，請選擇步驟旁邊的「編輯」。

> **Note**
>
> 您必須在選擇要編輯的步驟之後檢閱每個步驟。

- 如果您沒有變更，請選擇 [建立伺服器] 來建立伺服器。您會前往顯示下列內容的 Servers (伺服器) 頁面，這裡會列出您的新伺服器。

新伺服器的狀態變更為「線上」可能需要幾分鐘的時間。此時，您的伺服器會執行您使用者的檔案操作。

後續步驟 — 對於下一步，請繼續進行使用自訂身分識別提供者以設定使用者。

在虛擬私有雲中建立伺服器

您可以在虛擬私有雲 (VPC) 內託管伺服器的端點，用於在 Amazon S3 儲存貯體或 Amazon EFS 檔案系統之間傳輸資料，而無需透過公用網際網路。

> **Note**
>
> 2021 年 5 月 19 日之後，如果您的 AWS 帳戶`EndpointType=VPC_ENDPOINT`在 2021 年 5 月 19 日之前尚未使用，您將無法使用您的帳戶建立伺服器。如果您在 2021 年 2 月 21 日或之前已經`EndpointType=VPC_ENDPOINT`在您的 AWS 帳戶中創建了服務器，則不會受到影響。在此日期之後，使用 `EndpointType` = **`VPC`**。如需詳細資訊，請參閱 the section called "停止使用 VPC_ 端點"。

如果您使用 Amazon Virtual Private Cloud (Amazon VPC) 託管資 AWS 源，則可以在 VPC 和伺服器之間建立私有連接。然後，您可以使用此伺服器透過用戶端在 Amazon S3 儲存貯體之間傳輸資料，而無需使用公有 IP 定址或需要網際網路閘道。

您可以使用 Amazon VPC 在自訂虛擬網路中啟動 AWS 資源。您可利用 VPC 來控制您的網路設定，例如 IP 地址範圍、子網路、路由表和網路閘道。如需 VPC 的詳細資訊，請參閱什麼是 Amazon V PC？在 Amazon VPC 用戶指南中。

在接下來的章節中，找到有關如何建立 VPC 並將其連接到伺服器的說明。作為概述，您可以執行以下操作：

1. 使用 VPC 端點設定伺服器。
2. 透過 VPC 端點使用 VPC 內部的用戶端 Connect 線到伺服器。這樣做可讓您透過用戶端使用傳輸存放在 Amazon S3 儲存貯體中的資料 AWS Transfer Family。即使網路與公用網際網路中斷連線，您也可以執行此傳輸。
3. 此外，如果您選擇讓伺服器的端點網際網路對向，您可以將彈性 IP 位址與端點建立關聯。這樣做可讓 VPC 以外的用戶端連線到您的伺服器。您可以使用 VPC 安全群組來控制對僅來自允許位址的要求所產生之已驗證使用者的存取。

主題

- 建立只能在 VPC 中存取的伺服器端點
- 為您的伺服器建立面向網際網路的端點
- 變更伺服器的端點類型
- 停止使用 VPC_ 端點
- 將 AWS Transfer Family 伺服器端點類型從 VPC_ 端點更新為 VPC

建立只能在 VPC 中存取的伺服器端點

在下列程序中，您會建立只有 VPC 內的資源可存取的伺服器端點。

在 VPC 內建立伺服器端點

1. 請在以下位置開啟 AWS Transfer Family 主控台。 https://console.aws.amazon.com/transfer/
2. 在導覽窗格中，選取伺服器，然後選擇建立伺服器。
3. 在 [選擇通訊協定] 中選取一或多個通訊協定，然後選擇 [下一步]。如需通訊協定的詳細資訊，請參閱步驟 2：建立啟用 SFTP 的伺服器。
4. 在 [選擇身分識別提供者] 中，選擇 [用來儲存使用者識別和金鑰的受管服務] AWS Transfer Family，然後選擇 [下一步]

   > **Note**
   >
   > 此程序使用服務管理的選項。如果選擇「自訂」，則提供 Amazon API Gateway 端點和 AWS Identity and Access Management (IAM) 角色來存取端點。這樣，您就可以整合目錄服務來驗證和授權使用者。若要進一步了解使用自訂身分提供者，請參閱使用自訂身分識別提供者。

5. 在 [選擇端點] 中，執行下列動作：

   > **Note**
   >
   > 適用於 Transfer Family 的 FTP 和 FTPS 伺服器可在連接埠 21 (控制通道) 和連接埠範圍 8192-8200 (資料通道) 上運作。

   a. 對於端點類型，請選擇 VPC 託管端點類型來託管伺服器的端點。

   b. 對於 [存取]，選擇 [內部]，讓您的端點僅供使用端點私有 IP 位址的用戶端存取。

> **Note**
>
> 如需「網際網路對接」選項的詳細資訊，請參閱 為您的伺服器建立面向網際網路的端點 在 VPC 中建立的僅供內部存取的伺服器不支援自訂主機名稱。

c. 對於 VPC，請選擇現有的 VPC ID 或選擇 [建立 VPC] 以建立新的 VPC。

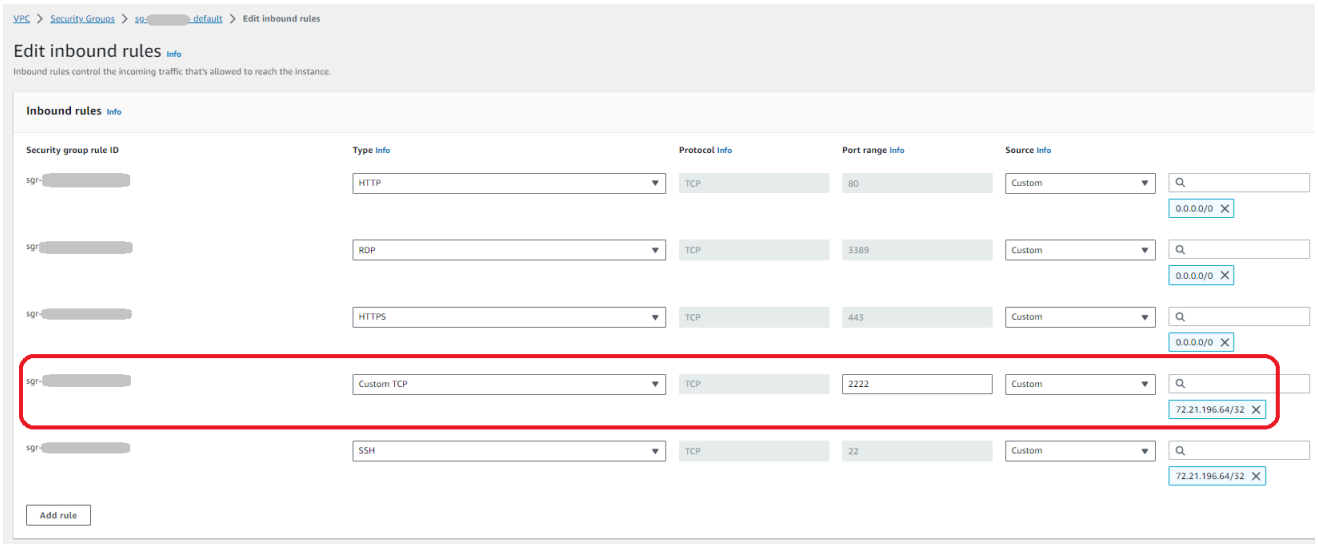
d. 在「可用區域」段落中，選擇最多三個可用區域和相關子網路。

e. 在「安全群組」區段中，選擇現有的一或多個安全性群組 ID，或選擇「建立安全性群組」以建立新的安全性群組。如需有關安全群組的詳細資訊，請參閱 Amazon Virtual Private Cloud 使用者指南中的 VPC 安全群組。若要建立安全群組，請參閱 Amazon Virtual Private Cloud 使用者指南中的建立安全群組。

> **Note**
>
> 您的 VPC 會自動具有預設安全群組。如果您在啟動伺服器時未指定不同的安全群組或群組，我們會將預設安全性群組與您的伺服器建立關聯。

對於安全性群組的輸入規則，您可以將 SSH 流量設定為使用連接埠 22、2222、22000 或任何組合。連接埠 22 是預設設定的。若要使用通訊埠 2222 或通訊埠 22000，請將輸入規則新增至安全性群組。針對類型，選擇 [自訂 TCP]，然後輸入**2222**或做**22000**為 [連接埠範圍]，然後針對來源輸入與 SSH 連接埠 22 規則相同的 CIDR 範圍。

> **Note**
>
> 您也可以針對需要 TCP「背包」ACK 的用戶端使用連接埠 2223，或 TCP 3 向握手的最終確認能力也包含資料。
> 某些用戶端軟體可能與通訊埠 2223 不相容：例如，要求伺服器在用戶端傳送 SFTP 識別字串之前的用戶端。



f. (選擇性) 對於啟用 FIPS，請選取已啟用 FIPS 的端點核取方塊，以確保端點符合聯邦資訊處理標準 (FIPS)。

> **Note**
>
> 已啟用 FIPS 的端點僅適用於北美 AWS 地區。如需可用區AWS Transfer Family 域，請參閱 AWS 一般參考. 如需 FIPS 的詳細資訊，請參閱聯邦資訊處理標準 (FIPS) 140-2。

g. 選擇下一步。

6. 在設定其他詳細資料中，執行下列動作：

a. 對於CloudWatch 記錄，請選擇下列其中一個選項來啟用 Amazon CloudWatch 記錄使用者活動：

- 建立新角色以允許 Transfer Family 自動建立 IAM 角色，只要您擁有建立新角色的適當權限即可。所建立的 IAM 角色稱為`AWSTransferLoggingAccess`。
- 選擇現有角色以從您的帳戶中選擇現有的 IAM 角色。在 [記錄角色] 底下，選擇角色。此 IAM 角色應包含將「服務」設定為的信任政策`transfer.amazonaws.com`。

  如需有關 CloudWatch 記錄的詳細資訊，請參閱設定 CloudWatch 記錄角色。

> **Note**
>
> - 如果您未指定記錄角色， CloudWatch 則無法檢視中的使用者活動。
> - 如果您不想設定 CloudWatch 記錄角色，請選取 [選擇現有角色]，但不要選取記錄角色。

b. 對於密碼編譯演算法選項，請選擇包含伺服器啟用的加密演算法的安全性原則。

> **Note**
>
> 根據預設，除非您選擇不同的`TransferSecurityPolicy-2020-06`安全性原則，否則安全性原則會附加至您的伺服器。

如需關於安全政策的詳細資訊，請參閱AWS Transfer Family 伺服器的安全性原則。

c. (選用性：本節僅適用於從現有啟用 SFTP 的伺服器移轉使用者。) 對於伺服器主機金鑰，請輸入 RSA、ED25519 或 ECDSA 私密金鑰，當用戶端透過 SFTP 連線至伺服器時，用來識別伺服器。

d. (選擇性) 對於標籤，對於「鍵值」和「值」，輸入一或多個標籤作為鍵值配對，然後選擇「新增標籤」。

e. 選擇下一步。

7. 在「檢閱並建立」中，檢閱您的選擇。如果您：

- 要編輯其中任何一個，請選擇步驟旁邊的 「編輯」。

> **Note**
>
> 您必須在選擇要編輯的步驟之後檢閱每個步驟。

- 沒有變更，請選擇 [建立伺服器] 來建立您的伺服器。您會前往顯示下列內容的 Servers (伺服器) 頁面，這裡會列出您的新伺服器。

新伺服器的狀態變更為「線上」可能需要幾分鐘的時間。此時，您的伺服器可以執行檔案作業，但您必須先建立使用者。如需建立使用者的詳細資訊，請參閱管理伺服器端點的使用者。

為您的伺服器建立面向網際網路的端點

在下列程序中，您會建立伺服器端點。只有 VPC 預設安全性群組中允許來源 IP 位址的用戶端才能透過網際網路存取此端點。此外，透過使用彈性 IP 位址讓您的端點網際網路對向，您的用戶端可以使用彈性 IP 位址來允許存取其防火牆中的端點。

> **Note**
>
> 只有 SFTP 和 FTPS 可以在面向網際網路的 VPC 託管端點上使用。

建立網際網路對向端點

1. 請在以下位置開啟 AWS Transfer Family 主控台。 https://console.aws.amazon.com/transfer/
2. 在導覽窗格中，選取伺服器，然後選擇建立伺服器。
3. 在 [選擇通訊協定] 中選取一或多個通訊協定，然後選擇 [下一步]。如需通訊協定的詳細資訊，請參閱步驟 2：建立啟用 SFTP 的伺服器。
4. 在 [選擇身分識別提供者] 中，選擇 [用來儲存使用者識別和金鑰的受管服務] AWS Transfer Family，然後選擇 [下一步]

   > **Note**
   >
   > 此程序使用服務管理的選項。如果選擇「自訂」，則提供 Amazon API Gateway 端點和 AWS Identity and Access Management (IAM) 角色來存取端點。這樣，您就可以整合目錄服務來驗證和授權使用者。若要進一步了解使用自訂身分提供者，請參閱使用自訂身分識別提供者。

5. 在 [選擇端點] 中，執行下列動作：

   a. 對於端點類型，請選擇 VPC 託管端點類型來託管伺服器的端點。

   b. 在 [存取] 中，選擇 [網際網路對向] 讓用戶端透過網際網路存取您的端點。

      > **Note**
      >
      > 當您選擇「網際網路對接」時，您可以在每個子網路或子網路中選擇現有的彈性 IP 位址。或者，您可以轉到 VPC 控制台（ https://console.aws.amazon.com/vpc/ ）以分配

一個或多個新的彈性 IP 地址。這些地址可以由您擁有，也可 AWS 以由您擁有。您無法將已在使用的彈性 IP 位址與端點建立關聯。

c. (選擇性) 對於「自訂主機名稱」，請選擇下列其中一項：

> **Note**
>
> AWS GovCloud (US) 需要直接透過彈性 IP 位址連線的客戶，或在商業路線 53 內建立指向 EIP 的主機名稱記錄。如需將 Route 53 用於 GovCloud 端點的詳細資訊，請參閱使用AWS GovCloud (US) 者指南中的使用您的 AWS GovCloud (US) 資源設定 Amazon Route 53。

- Amazon 路由 53 DNS 別名 — 如果您要使用的主機名已在 Route 53 中註冊。然後，您可以輸入主機名稱。
- 其他 DNS — 如果您要使用的主機名稱已向其他 DNS 提供商註冊。然後，您可以輸入主機名稱。
- 無 — 使用伺服器的端點，而不使用自訂主機名稱。伺服器主機名稱的格式為 `server-id.server.transfer.region.amazonaws.com`。

> **Note**
>
> 對於中的客戶 AWS GovCloud (US)，選取「無」並不會以此格式建立主機名稱。

若要深入瞭解如何使用自訂主機名稱，請參閱使用自訂主機名稱。

d. 對於 VPC，請選擇現有的 VPC ID 或選擇 [建立 VPC] 以建立新的 VPC。

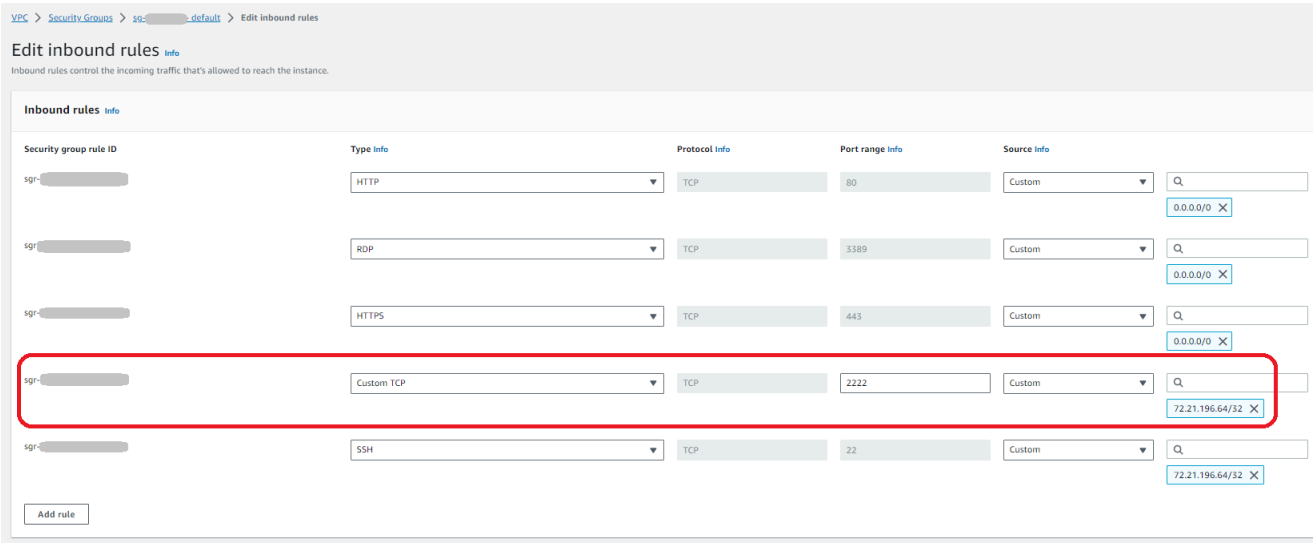
e. 在「可用區域」段落中，選擇最多三個可用區域和相關子網路。對於 IPv4 位址，請為每個子網路選擇一個彈性 IP 位址。這是您的用戶端可用來允許在其防火牆中存取端點的 IP 位址。

f. 在「安全群組」區段中，選擇現有的一或多個安全性群組 ID，或選擇「建立安全性群組」以建立新的安全性群組。如需有關安全群組的詳細資訊，請參閱 Amazon Virtual Private Cloud 使用者指南中的 VPC 安全群組。若要建立安全群組，請參閱 Amazon Virtual Private Cloud 使用者指南中的建立安全群組。

> **Note**
>
> 您的 VPC 會自動具有預設安全群組。如果您在啟動伺服器時未指定不同的安全群組或群組，我們會將預設安全性群組與您的伺服器建立關聯。

對於安全性群組的輸入規則，您可以將 SSH 流量設定為使用連接埠 22、2222、22000 或任何組合。連接埠 22 是預設設定的。若要使用通訊埠 2222 或通訊埠 22000，請將輸入規則新增至安全性群組。針對類型，選擇 [自訂 TCP]，然後輸入**2222**或做**22000**為 [連接埠範圍]，然後針對來源輸入與 SSH 連接埠 22 規則相同的 CIDR 範圍。

> **Note**
>
> 您也可以針對需要 TCP「背包」ACK 的用戶端使用連接埠 2223，或 TCP 3 向握手的最終確認能力也包含資料。
>
> 某些用戶端軟體可能與通訊埠 2223 不相容：例如，要求伺服器在用戶端傳送 SFTP 識別字串之前的用戶端。



g. (選擇性) 對於啟用 FIPS，請選取已啟用 FIPS 的端點核取方塊，以確保端點符合聯邦資訊處理標準 (FIPS)。

> **Note**
>
> 已啟用 FIPS 的端點僅適用於北美 AWS 地區。如需可用區AWS Transfer Family 域，請參閱 AWS 一般參考. 如需 FIPS 的詳細資訊，請參閱聯邦資訊處理標準 (FIPS) 140-2。

h. 選擇下一步。

6. 在設定其他詳細資料中，執行下列動作：

a. 對於CloudWatch 記錄，請選擇下列其中一個選項來啟用 Amazon CloudWatch 記錄使用者活動：

- 建立新角色以允許 Transfer Family 自動建立 IAM 角色，只要您擁有建立新角色的適當權限即可。所建立的 IAM 角色稱為`AWSTransferLoggingAccess`。
- 選擇現有角色以從您的帳戶中選擇現有的 IAM 角色。在 [記錄角色] 底下，選擇角色。此 IAM 角色應包含將「服務」設定為的信任政策`transfer.amazonaws.com`。

如需有關 CloudWatch 記錄的詳細資訊，請參閱設定 CloudWatch 記錄角色。

> **Note**
>
> - 如果您未指定記錄角色， CloudWatch 則無法檢視中的使用者活動。
> - 如果您不想設定 CloudWatch 記錄角色，請選取 [選擇現有角色]，但不要選取記錄角色。

b. 對於密碼編譯演算法選項，請選擇包含伺服器啟用的加密演算法的安全性原則。

> **Note**
>
> 根據預設，除非您選擇不同的`TransferSecurityPolicy-2020-06`安全性原則，否則安全性原則會附加至您的伺服器。

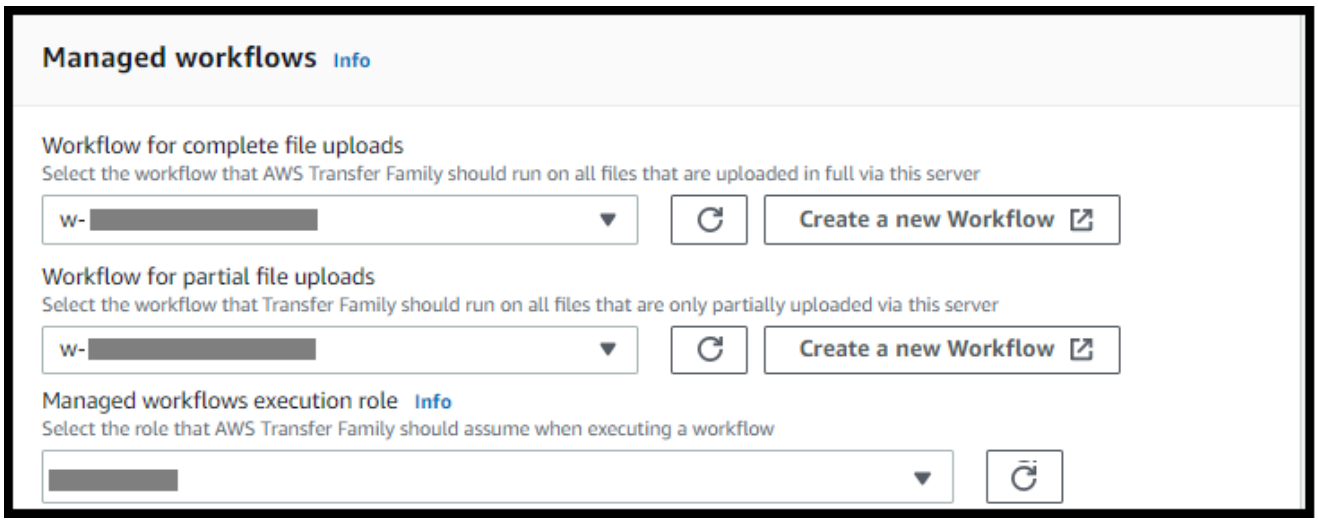
如需關於安全政策的詳細資訊，請參閱AWS Transfer Family 伺服器的安全性原則。

c. (選用性：本節僅適用於從現有啟用 SFTP 的伺服器移轉使用者。) 對於伺服器主機金鑰，請輸入 RSA、ED25519 或 ECDSA 私密金鑰，當用戶端透過 SFTP 連線至伺服器時，用來識別伺服器。

d. (選擇性) 對於標籤，對於「鍵值」和「值」，輸入一或多個標籤作為鍵值配對，然後選擇「新增標籤」。

e. 選擇下一步。

f. (選擇性) 對於「受管理的工作流程」，請選擇「Transfer Family」在執行工作流程時應承擔的工作流程 ID (以及對應角色)。您可以選擇一個工作流程在完成上載時執行，另一個工作流程在部分上傳時執行。若要進一步瞭解如何使用受管理的工作流程處理檔案，請參閱AWS Transfer Family 管理工作流。



7. 在「檢閱並建立」中，檢閱您的選擇。如果您：

- 要編輯其中任何一個，請選擇步驟旁邊的 「編輯」。

> **Note**
>
> 您必須在選擇要編輯的步驟之後檢閱每個步驟。

- 沒有變更，請選擇 [建立伺服器] 來建立您的伺服器。您會前往顯示下列內容的 Servers (伺服器) 頁面，這裡會列出您的新伺服器。

您可以選擇伺服器 ID，以查看剛建立之伺服器的詳細設定。填入 [公用 IPv4 位址] 資料行之後，您提供的彈性 IP 位址就會成功與伺服器的端點建立關聯。

> **Note**
>
> 當 VPC 中的伺服器連線時，只能透過 API 修改子網路。UpdateServer您必須停止伺服器，才能新增或變更伺服器端點的彈性 IP 位址。

變更伺服器的端點類型

如果您有可透過網際網路存取的現有伺服器 (也就是具有公用端點類型)，則可以將其端點變更為 VPC 端點。

> **Note**
>
> 如果 VPC 中的現有伺服器顯示為VPC_ENDPOINT，建議您將其修改為新的 VPC 端點類型。使用此新端點類型，您不再需要使用 Network Load Balancer (NLB) 將彈性 IP 位址與伺服器端點建立關聯。此外，您可以使用 VPC 安全群組來限制對伺服器端點的存取。不過，您可以視需要繼續使用VPC_ENDPOINT端點類型。

下列程序假設您的伺服器使用目前的公用端點類型或較舊的VPC_ENDPOINT類型。

變更伺服器的端點類型

1. 請在以下位置開啟 AWS Transfer Family 主控台。 https://console.aws.amazon.com/transfer/
2. 在導覽窗格中，選擇 Servers (伺服器)。
3. 選取要變更其端點類型之伺服器的核取方塊。

   > **Important**
   >
   > 您必須先停止伺服器，才能變更其端點。

4. 針對 Actions (動作)，選擇 Stop (停止)。
5. 在出現的確認對話方塊中，選擇「停止」以確認您要停止伺服器。

> **Note**
>
> 在繼續執行下一個步驟之前，請在端點詳細資料中等待伺服器的狀態變更為 [離線]；這可能需要幾分鐘的時間。您可能必須在「伺服器」頁面上選擇「重新整理」，才能查看狀態變更。
> 在伺服器離線之前，您將無法進行任何編輯。

6. 在端點詳細資料中，選擇編輯。
7. 在編輯端點組態中，執行下列操作：

   a. 針對 [編輯端點類型]，選擇 [VPC 託管]。

   b. 對於「存取」，請選擇下列其中一項：

      - 內部，使您的端點只能由使用端點的私有 IP 地址的客戶端訪問。
      - 「網際網路面對」可讓用戶端透過公用網際網路存取您的端點。

      > **Note**
      >
      > 當您選擇「網際網路對接」時，您可以在每個子網路或子網路中選擇現有的彈性 IP 位址。或者，您可以轉到 VPC 控制台（ https://console.aws.amazon.com/vpc/ ）以分配一個或多個新的彈性 IP 地址。這些地址可以由您擁有，也可 AWS 以由您擁有。您無法將已在使用的彈性 IP 位址與端點建立關聯。

   c. (僅適用於面向網際網路存取的選擇性) 對於自訂主機名稱，請選擇下列其中一項：

      - Amazon 路由 53 DNS 別名 — 如果您要使用的主機名已在 Route 53 中註冊。然後，您可以輸入主機名稱。
      - 其他 DNS — 如果您要使用的主機名稱已向其他 DNS 提供商註冊。然後，您可以輸入主機名稱。
      - 無 — 使用伺服器的端點，而不使用自訂主機名稱。伺服器主機名稱的格式為 *`serverId`*`.server.transfer.`*`regionId`*`.amazonaws.com`。

        若要深入瞭解如何使用自訂主機名稱，請參閱使用自訂主機名稱。

   d. 對於 VPC，請選擇現有的 VPC ID，或選擇 [建立 VPC] 以建立新的 VPC。

   e. 在「可用區域」段落中，選取最多三個可用區域和相關子網路。如果選擇「網際網路對向」，也請為每個子網路選擇一個彈性 IP 位址。

> **Note**
>
> 如果您想要最多三個可用區域，但沒有足夠的可用區域，請在 VPC 主控台 (https://console.aws.amazon.com/vpc/) 中建立它們。
> 如果您修改子網路或彈性 IP 位址，則伺服器需要幾分鐘的時間進行更新。在伺服器更新完成之前，您無法儲存變更。

f. 選擇儲存。

8. 在 [動作] 中，選擇 [開始]，然後等待伺服器狀態變更為 [線上]；這可能需要幾分鐘的時間。

> **Note**
>
> 如果您將公用端點類型變更為 VPC 端點類型，請注意您伺服器的端點類型已變更為 VPC。

預設安全群組會附加至端點。若要變更或新增其他安全性群組，請參閱建立安全性群組。

停止使用 VPC_ 端點

AWS Transfer Family 正在停止`EndpointType=VPC_ENDPOINT`為新 AWS 帳戶建立伺服器的能力。自 2021 年 5 月 19 日起，未擁有端點類型的 AWS Transfer Family 伺服器的 AWS 帳戶`VPC_ENDPOINT`將無法使用`EndpointType=VPC_ENDPOINT`. 如果您已經擁有使用`VPC_ENDPOINT`端點類型的伺服器，建議您`EndpointType=VPC`儘快開始使用。如需詳細資訊，請參閱將 AWS Transfer Family 伺服器端點類型從 VPC_ENDPOINT 更新為 VPC。

我們於 2020 年早些時候推出了新的VPC端點類型。如需詳細資訊，請參AWS Transfer Family 閱 SFTP 支援 VPC 安全群組和彈性 IP 位址。這個新的端點功能更豐富，更具成本效益，並且不 PrivateLink 收取任何費用。如需詳細資訊，請參閱AWS PrivateLink 定價。

此端點類型在功能上等同於先前的端點類型 (`VPC_ENDPOINT`)。您可以將彈性 IP 位址直接連接到端點，使其面向網際網路，並使用安全群組進行來源 IP 篩選。如需詳細資訊，請參閱使用 IP 允許清單來保護您 AWS Transfer Family 的 SFTP 伺服器部落格文章。

您也可以在共用 VPC 環境中託管此端點。如需詳細資訊，請參閱AWS Transfer Family 現在支援共用服務 VPC 環境。

除了 SFTP 之外，您還可以使用 VPC EndpointType 來啟用 FTPS 和 FTP。我們不打算將這些功能和 FTPS/FTP 支持添加到. EndpointType=VPC_ENDPOINT 我們還從 AWS Transfer Family 控制台中刪除了此端點類型作為選項。

您可以使用 Transfer Family 主控台、API AWS CLI、SDK 或 AWS CloudFormation變更伺服器的端點類型。若要變更伺服器的端點類型，請參閱將 AWS Transfer Family 伺服器端點類型從 VPC_ 端點更新為 VPC。

如果您有任何疑問，請聯絡 AWS Support 或您的 AWS 客戶團隊。

> **Note**
>
> 我們不打算將這些功能和 FTPS 或 FTP 支持添加到 EndpointType = VPC_ 端點。我們不再在 AWS Transfer Family 控制台上將其作為選項提供。

如果您還有其他問題，可以通過 AWS Support 或您的客戶團隊與我們聯繫。

將 AWS Transfer Family 伺服器端點類型從 VPC_ 端點更新為 VPC

您可以使用 AWS Management Console AWS CloudFormation、或轉移系列 API 將伺服器的EndpointType從更新VPC_ENDPOINT為VPC。以下各節提供使用上述每種方法更新伺服器端點類型的詳細程序和範例。如果您在多個 AWS 地區和多個 AWS 帳戶中有伺服器，您可以使用下一節中提供的範例指令碼，並進行修改，來識別使用您需要更新的VPC_ENDPOINT類型的伺服器。

主題

- 使用VPC_ENDPOINT端點類型識別伺服器
- 使用更新伺服器端點類型 AWS Management Console
- 使用更新伺服器端點類型 AWS CloudFormation
- EndpointType 使用 API 更新伺服器

使用**VPC_ENDPOINT**端點類型識別伺服器

您可以使用識別哪些伺服器正在VPC_ENDPOINT使用 AWS Management Console。

使用控制台識別使用**VPC_ENDPOINT**端點類型的伺服器

1. 請在以下位置開啟 AWS Transfer Family 主控台。 https://console.aws.amazon.com/transfer/

2. 在瀏覽窗格中選擇 [伺服器]，以顯示該區域中您帳戶中的伺服器清單。
3. 依端點類型排序伺服器清單，以查看所有使用的伺服器VPC_ENDPOINT。

識別**VPC_ENDPOINT**跨多個 AWS 區域和帳戶使用的伺服器

如果您在多個 AWS 地區和多個 AWS 帳戶中擁有伺服器，則可以使用下列範例指令碼進行修改，來識別使用VPC_ENDPOINT端點類型的伺服器。範例指令碼使用 Amazon EC2 DescribeRegions和 Transfer Family 列 ListServers API 呼叫來取得所使用之所有伺服器的伺服器 ID 和區域的清單VPC_ENDPOINT。如果您有許多 AWS 帳戶，如果您使用身分提供者的工作階段設定檔進行驗證，則可以使用具有唯讀稽核員存取權的 IAM 角色來迴圈您的帳戶。

1. 下面是一個簡單的例子。

```
import boto3

profile = input("Enter the name of the AWS account you'll be working in: ")
session = boto3.Session(profile_name=profile)

ec2 = session.client("ec2")

regions = ec2.describe_regions()

for region in regions['Regions']:
    region_name = region['RegionName']
    if region_name=='ap-northeast-3': #https://github.com/boto/boto3/issues/1943
        continue
    transfer = session.client("transfer", region_name=region_name)
    servers = transfer.list_servers()
    for server in servers['Servers']:
       if server['EndpointType']=='VPC_ENDPOINT':
           print(server['ServerId'], region_name)
```

2. 取得要更新的伺服器清單之後，您可以使用下列各節中描述的其中一種方法來更新EndpointType至VPC。

使用更新伺服器端點類型 AWS Management Console

1. 請在以下位置開啟 AWS Transfer Family 主控台。 https://console.aws.amazon.com/transfer/
2. 在導覽窗格中，選擇 Servers (伺服器)。
3. 選取要變更其端點類型之伺服器的核取方塊。

> **Important**
>
> 您必須先停止伺服器，才能變更其端點。

4. 針對 Actions (動作)，選擇 Stop (停止)。
5. 在出現的確認對話方塊中，選擇「停止」以確認您要停止伺服器。

> **Note**
>
> 繼續進行下一個步驟之前，請等待伺服器的 [狀態] 變更為 [離線]；這可能需要幾分鐘的時間。您可能必須在「伺服器」頁面上選擇「重新整理」，才能查看狀態變更。

6. 狀態變更為 [離線] 之後，選擇要顯示伺服器詳細資訊頁面的伺服器。
7. 在端點詳細資料區段中，選擇編輯。
8. 選擇端點類型的 VPC 託管。
9. 選擇儲存
10. 在 [動作] 中，選擇 [開始]，然後等待伺服器狀態變更為 [線上]；這可能需要幾分鐘的時間。

使用更新伺服器端點類型 AWS CloudFormation

本節說明如何使用 AWS CloudFormation 將伺服器更新`EndpointType`至`VPC`。對您使用部署的 Transfer Family 伺服器使用此程序 AWS CloudFormation。在此範例中，用於部署 Transfer Family 伺服器的原始 AWS CloudFormation 樣板如下所示：

```
AWS TemplateFormatVersion: '2010-09-09'
Description: 'Create AWS Transfer Server with VPC_ENDPOINT endpoint type'
Parameters:
  SecurityGroupId:
    Type: AWS::EC2::SecurityGroup::Id
  SubnetIds:
    Type: List<AWS::EC2::Subnet::Id>
  VpcId:
    Type: AWS::EC2::VPC::Id
Resources:
  TransferServer:
    Type: AWS::Transfer::Server
    Properties:
      Domain: S3
```

```
      EndpointDetails:
        VpcEndpointId: !Ref VPCEndpoint
      EndpointType: VPC_ENDPOINT
      IdentityProviderType: SERVICE_MANAGED
      Protocols:
        - SFTP
  VPCEndpoint:
    Type: AWS::EC2::VPCEndpoint
    Properties:
      ServiceName: com.amazonaws.us-east-1.transfer.server
      SecurityGroupIds:
        - !Ref SecurityGroupId
      SubnetIds:
        - !Select [0, !Ref SubnetIds]
        - !Select [1, !Ref SubnetIds]
        - !Select [2, !Ref SubnetIds]
      VpcEndpointType: Interface
      VpcId: !Ref VpcId
```

範本會以下列變更進行更新：

- EndpointType已變更為VPC。
- 即會移除AWS::EC2::VPCEndpoint資源。
- SecurityGroupIdSubnetIds、和VpcId已移至AWS::Transfer::Server資源的EndpointDetails區段，
- 的VpcEndpointId屬性EndpointDetails已移除。

更新後的範本如下所示：

```
AWS TemplateFormatVersion: '2010-09-09'
Description: 'Create AWS Transfer Server with VPC endpoint type'
Parameters:
  SecurityGroupId:
    Type: AWS::EC2::SecurityGroup::Id
  SubnetIds:
    Type: List<AWS::EC2::Subnet::Id>
  VpcId:
    Type: AWS::EC2::VPC::Id
Resources:
  TransferServer:
    Type: AWS::Transfer::Server
```

```
    Properties:
      Domain: S3
      EndpointDetails:
        SecurityGroupIds:
          - !Ref SecurityGroupId
        SubnetIds:
          - !Select [0, !Ref SubnetIds]
          - !Select [1, !Ref SubnetIds]
          - !Select [2, !Ref SubnetIds]
        VpcId: !Ref VpcId
      EndpointType: VPC
      IdentityProviderType: SERVICE_MANAGED
      Protocols:
        - SFTP
```

更新使用部署的 Transfer Family 伺服器的端點類型 AWS CloudFormation

1. 使用下列步驟停止您要更新的伺服器。

   a. 請在以下位置開啟 AWS Transfer Family 主控台。 https://console.aws.amazon.com/transfer/

   b. 在導覽窗格中，選擇 Servers (伺服器)。

   c. 選取要變更其端點類型之伺服器的核取方塊。

   > **Important**
   >
   > 您必須先停止伺服器，才能變更其端點。

   d. 針對 Actions (動作)，選擇 Stop (停止)。

   e. 在出現的確認對話方塊中，選擇「停止」以確認您要停止伺服器。

   > **Note**
   >
   > 繼續進行下一個步驟之前，請等待伺服器的 [狀態] 變更為 [離線]；這可能需要幾分鐘的時間。您可能必須在「伺服器」頁面上選擇「重新整理」，才能查看狀態變更。

2. 更新 CloudFormation 堆疊

   a. 請在以下位置開啟 AWS CloudFormation 主控台。 https://console.aws.amazon.com/cloudformation

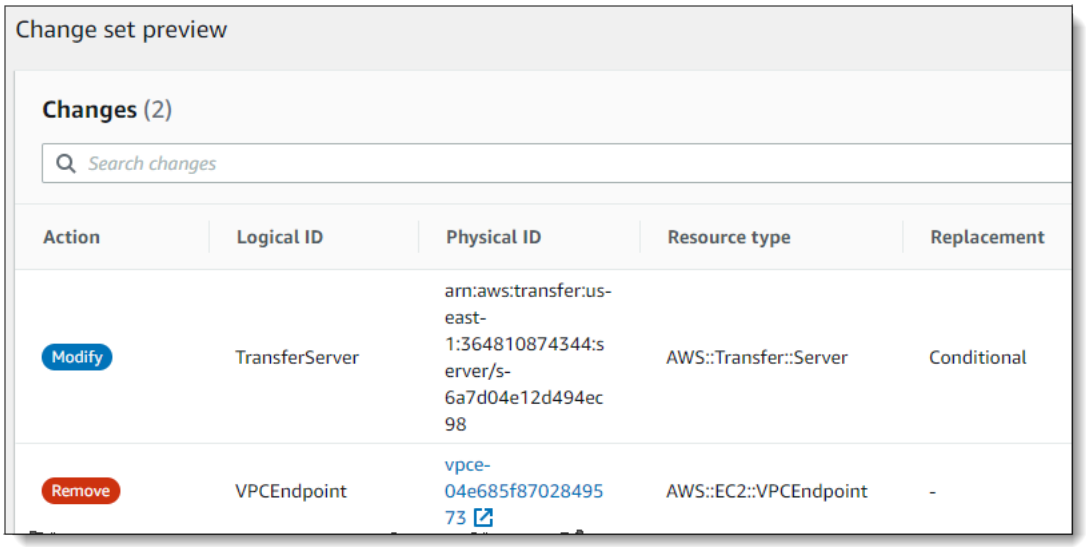
   b. 選擇用於建立 Transfer Family 伺服器的堆疊。

c. 選擇更新。

d. 選擇取代目前的範本

e. 上傳新範本。 CloudFormation 變更集可協助您在實作範本變更之前瞭解範本變更將如何影響執行中的資源。在此範例中，將會修改傳輸伺服器資源，並移除 vpcendPoint 資源。VPC 端點類型伺服器會代表您建立 VPC 端點，取代原始資源VPCEndpoint。

上傳新範本之後，變更集看起來會類似下列內容：



f. 更新堆疊。

3. 堆疊更新完成後，請瀏覽至 Transfer Family 管理主控台，網址為 https://console.aws.amazon.com/transfer/。

4. 重新啟動伺服器。選擇您在中更新的伺服器 AWS CloudFormation，然後從 [動作] 功能表選擇 [開始]。

EndpointType 使用 API 更新伺服器

您可以使用描述伺服器 AWS CLI 命令或 API 指令。UpdateServer下列範例指令碼會停止 Transfer Family 列伺服器、更新 EndpointType、移除 VPC_ENDPOINT，然後啟動伺服器。

```
import boto3
import time

profile = input("Enter the name of the AWS account you'll be working in: ")
region_name = input("Enter the AWS Region you're working in: ")
server_id = input("Enter the AWS Transfer Server Id: ")
```

```
session = boto3.Session(profile_name=profile)

ec2 = session.client("ec2", region_name=region_name)
transfer = session.client("transfer", region_name=region_name)

group_ids=[]

transfer_description = transfer.describe_server(ServerId=server_id)
if transfer_description['Server']['EndpointType']=='VPC_ENDPOINT':
    transfer_vpc_endpoint = transfer_description['Server']['EndpointDetails']
['VpcEndpointId']
    transfer_vpc_endpoint_descriptions =
 ec2.describe_vpc_endpoints(VpcEndpointIds=[transfer_vpc_endpoint])
    for transfer_vpc_endpoint_description in
 transfer_vpc_endpoint_descriptions['VpcEndpoints']:
        subnet_ids=transfer_vpc_endpoint_description['SubnetIds']
        group_id_list=transfer_vpc_endpoint_description['Groups']
        vpc_id=transfer_vpc_endpoint_description['VpcId']
        for group_id in group_id_list:
             group_ids.append(group_id['GroupId'])
    if transfer_description['Server']['State']=='ONLINE':
        transfer_stop = transfer.stop_server(ServerId=server_id)
        print(transfer_stop)
        time.sleep(300) #safe
        transfer_update =
 transfer.update_server(ServerId=server_id,EndpointType='VPC',EndpointDetails={'SecurityGroupId
        print(transfer_update)
        time.sleep(10)
        transfer_start = transfer.start_server(ServerId=server_id)
        print(transfer_start)
        delete_vpc_endpoint =
 ec2.delete_vpc_endpoints(VpcEndpointIds=[transfer_vpc_endpoint])
```

使用自訂主機名稱

您的伺服器主機名稱是使用者在連線到伺服器時在其用戶端中輸入的主機名稱。使用時，您可以使用已為伺服器主機名稱註冊的自訂網域 AWS Transfer Family。例如，您可以使用類似的自定義主機名稱`mysftpserver.mysubdomain.domain.com`。

若要將流量從已註冊的自訂網域重新導向至伺服器端點，您可以使用 Amazon Route 53 或任何網域名稱系統 (DNS) 提供者。路線 53 是本機支 AWS Transfer Family 援的 DNS 服務。

主題

- 使用 Amazon 路線 53 作為您的 DNS 提供商
- 使用其他 DNS 供應商
- 非控制台創建的服務器的自定義主機名

在主控台上，您可以選擇下列其中一個選項來設定自訂主機名稱：

- Amazon 路由 53 DNS 別名 — 如果您要使用的主機名已在 Route 53 中註冊。然後，您可以輸入主機名稱。
- 其他 DNS — 如果您要使用的主機名稱已向其他 DNS 提供商註冊。然後，您可以輸入主機名稱。
- 無 — 使用伺服器的端點，而不使用自訂主機名稱。

您可以在建立新伺服器或編輯現有伺服器的組態時設定此選項。如需建立新伺服器的詳細資訊，請參閱步驟 2：建立啟用 SFTP 的伺服器。如需編輯現有伺服器組態的詳細資訊，請參閱編輯伺服器詳情。

如需有關使用您自己的網域作為伺服器主機名稱以及如何 AWS Transfer Family 使用 Route 53 的詳細資訊，請參閱下列章節。

使用 Amazon 路線 53 作為您的 DNS 提供商

當您建立伺服器時，您可以使用 Amazon 路線 53 做為您的 DNS 供應商。在您透過 Route 53 使用網域之前，請先註冊網域。如需詳細資訊，請參閱 Amazon Route 53 開發人員指南中的網域註冊運作方式。

當您使用 Route 53 提供 DNS 路由到您的伺服器時，會 AWS Transfer Family 使用您輸入的自訂主機名稱來擷取其託管區域。 AWS Transfer Family 擷取託管區域時，可能會發生以下三種情況：

1. 如果您是 Route 53 的新手，並且沒有託管區域，請 AWS Transfer Family 添加新的託管區域和CNAME記錄。此CNAME記錄的值是伺服器的端點主機名稱。CNAME 是替代網域名稱。
2. 如果您在 Route 53 中有一個沒有任何CNAME記錄的託管區域，請將CNAME記錄 AWS Transfer Family 新增至託管區域。
3. 若服務偵測到 CNAME 記錄已存在於託管區域內，您會看到一個錯誤，指出 CNAME 記錄已存在。在此情況下，請將CNAME記錄的值變更為伺服器的主機名稱。

如需 Route 53 中託管區域的詳細資訊，請參閱 Amazon Route 53 開發人員指南中的託管區域。

使用其他 DNS 供應商

當您建立伺服器時，您也可以使用 Amazon 路線 53 以外的 DNS 供應商。若您使用替代 DNS 提供者，請確認來自您網域的流量會導向您的 伺服器端點。

若要這麼做，請將您的網域設定為伺服器的端點主機名稱。端點主機名稱在控制台中看起來像這樣：

serverid.server.transfer.*region*.amazonaws.com

> **Note**
>
> 如果您的伺服器具有 VPC 端點，則主機名稱的格式與上述格式不同。若要尋找您的 VPC 端點，請在伺服器的詳細資訊頁面上選取 VPC，然後在 VPC 儀表板上選取 VPC 端點識別碼。端點是列出的第一個 DNS 名稱。

非控制台創建的服務器的自定義主機名

當您使用 AWS Cloud Development Kit (AWS CDK)、 AWS CloudFormation或透過 CLI 建立伺服器時，如果您希望該伺服器具有自訂主機名稱，則必須新增標籤。使用控制台建立「Transfer Family」伺服器時，會自動完成標籤。

> **Note**
>
> 您也需要建立 DNS 記錄，才能將流量從您的網域重新導向至伺服器端點。如需詳細資訊，請參閱 Amazon Route 53 開發人員指南中的使用記錄。

為您的自訂主機名稱使用下列金鑰：

- 新增`transfer:customHostname`以在主控台中顯示自訂主機名稱。
- 如果您使用 Route 53 做為您的 DNS 提供者，請新增`transfer:route53HostedZoneId`. 此標記會將自訂主機名稱連結至您的 Route 53 託管區域 ID。

若要新增自訂主機名稱，請發出以下 CLI 指令。

```
aws transfer tag-resource --arn arn:aws:transfer:region:AWS ##:server/server-ID --tags
 Key=transfer:customHostname,Value="custom-host-name"
```

例如：

```
aws transfer tag-resource --arn arn:aws:transfer:us-east-1:111122223333:server/
s-1234567890abcdef0 --tags Key=transfer:customHostname,Value="abc.example.com"
```

如果您使用的是 Route 53，請執行以下指令，將您的自訂主機名稱連結至 Route 53 託管區域 ID。

```
aws transfer tag-resource --arn server-ARN:server/server-ID --tags
 Key=transfer:route53HostedZoneId,Value=HOSTED-ZONE-ID
```

例如：

```
aws transfer tag-resource --arn arn:aws:transfer:us-east-1:111122223333:server/
s-1234567890abcdef0 --tags Key=transfer:route53HostedZoneId,Value=ABCDE1111222233334444
```

假設上一個命令的範例值，請執行下列命令來檢視標籤：

```
aws transfer list-tags-for-resource --arn arn:aws:transfer:us-
east-1:111122223333:server/s-1234567890abcdef0
```

```
"Tags": [
   {
      "Key": "transfer:route53HostedZoneId",
      "Value": "/hostedzone/ABCDE1111222233334444"
   },
   {
      "Key": "transfer:customHostname",
      "Value": "abc.example.com"
   }
 ]
```

> **Note**
>
> 您的公共、託管區域及其 ID 可在 Amazon Route 53 上使用。
> 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。

使用用戶端透過伺服器端點傳輸檔案

您可以透過在用戶端中指定傳輸作業，透過 AWS Transfer Family 服務傳輸檔案。 AWS Transfer Family 支援下列用戶端：

- 我們支援 SFTP 通訊協定的第 3 版。
- OpenSSH (macOS 和 Linux)

> **Note**
>
> 此用戶端僅適用於已啟用安全殼層 (SSH) 檔案傳輸通訊協定 (SFTP) 的伺服器。

- WinSCP (僅限 Microsoft Windows)
- 數碼鴨（視窗，macOS 系統和 Linux）
- FileZilla （視窗、macOS 系統和操作系統）

下列限制適用於每個用戶端：

- 每個連線最多可同時執行多工 SFTP 工作階段數目為 10 個。
- SFTP/FTP/FTPS 連線有兩個逾時值。對於閒置連線，逾時值為 1800 秒 (30 分鐘)。如果在期限過後沒有任何活動，則用戶端可能會中斷連線。當用戶端完全沒有回應時，也會有 300 秒 (5 分鐘) 逾時。
- Amazon S3 和 Amazon EFS（由於 NFSv4 協議）要求文件名使用 UTF-8 編碼。使用不同的編碼可能會導致非預期的結果。對於 Amazon S3，請參閱物件金鑰命名指南。
- 對於透過 SSL 的檔案傳輸通訊協定 (FTPS)，僅支援「明確」模式。不支援隱含模式。
- 對於檔案傳輸通訊協定 (FTP) 和 FTPS，僅支援被動模式。
- 對於 FTP 和 FTPS，僅支援串流模式。
- 對於 FTP 和 FTPS，僅支援影像/二進位模式。
- 對於 FTP 和 FTPS，資料連線的 TLS-PROT C (未受保護) TLS 是預設的，但 FTPS 通訊協定不支援 PROT C。 AWS Transfer Family 因此，對於 FTPS，您需要發出 PROT P 以便接受數據操作。
- 如果您將 Amazon S3 用於伺服器儲存，並且客戶端包含使用多個連接進行單一傳輸的選項，請務必停用該選項。否則，大型文件上傳可能會以不可預知的方式失敗。請注意，如果您使用 Amazon EFS 做為儲存後端，EFS 確實支援單一傳輸的多個連線。

以下是 FTP 和 FTPS 的可用命令列表：

可用命令					
厭惡	功績	MLST	通過	廢棄	大型
AUTH	LANG	MKD	帕斯夫	RMD	斯托
制定的	LIST	MODE	PBSZ	RNFR	STRU
CWD	MDTM	NLST	PROT	RNTO	系統
德勒	MFMT	NOOP	PWD	SIZE	TYPE
EPSV	MLSD	選擇	結束	統計	USER

> **Note**
>
> 不支援 APPE。

對於 SFTP，在使用 Amazon 彈性檔案系統 (Amazon EFS) 的伺服器上使用邏輯主目錄的使用者，目前不支援下列操作。

不支援的 SFTP 指令			
讀取連結	符號鏈接	SSH_FXP_STAT，當請求的文件是一個符號鏈接	SSH_FXP_REALPATH 當請求的路徑包含任何符號鏈接組件

生成公鑰-私 key pair

您必須擁有可用的公開-私 key pair，才能傳輸檔案。如果您之前尚未產生 key pair，請參閱為服務管理的使用者產生 SSH 金鑰。

主題

- 可用的SFT/FTPS/FTP 指令
- 尋找您的 Amazon VPC 端點

- 避免setstat錯誤
- 使用 OpenSSH
- 使用 WinSCP
- 使用網路鴨
- 使用 FileZilla
- 使用一個 Perl 客戶端
- 上傳後處理

可用的SFT/FTPS/FTP 指令

下表說明 SFTP AWS Transfer Family、FTPS 和 FTP 通訊協定的可用命令。

> **Note**
>
> 該表提到 Amazon S3 的文件和目錄，該文件和目錄僅支持存儲桶和對象：沒有階層。但是，您可以在物件索引鍵名稱中使用前置字元來暗示階層，並以類似於資料夾的方式組織資料。有關此行為的說明，請參閱 Amazon 簡單儲存服務使用者指南中的使用物件中繼資料。

SFT/FTPS/FTP 指令

Command	Amazon S3	Amazon EFS
`cd`	支援	支援
`chgrp`	不支援	支援 (`root`或`owner`僅支援)
`chmod`	不支援	支援 (`root`僅限)
`chmtime`	不支援	支援
`chown`	不支援	支援 (`root`僅限)
`get`	支援	支援 (包括解析符號連結)
`ln -s`	不支援	支援
`ls/dir`	支援	支援

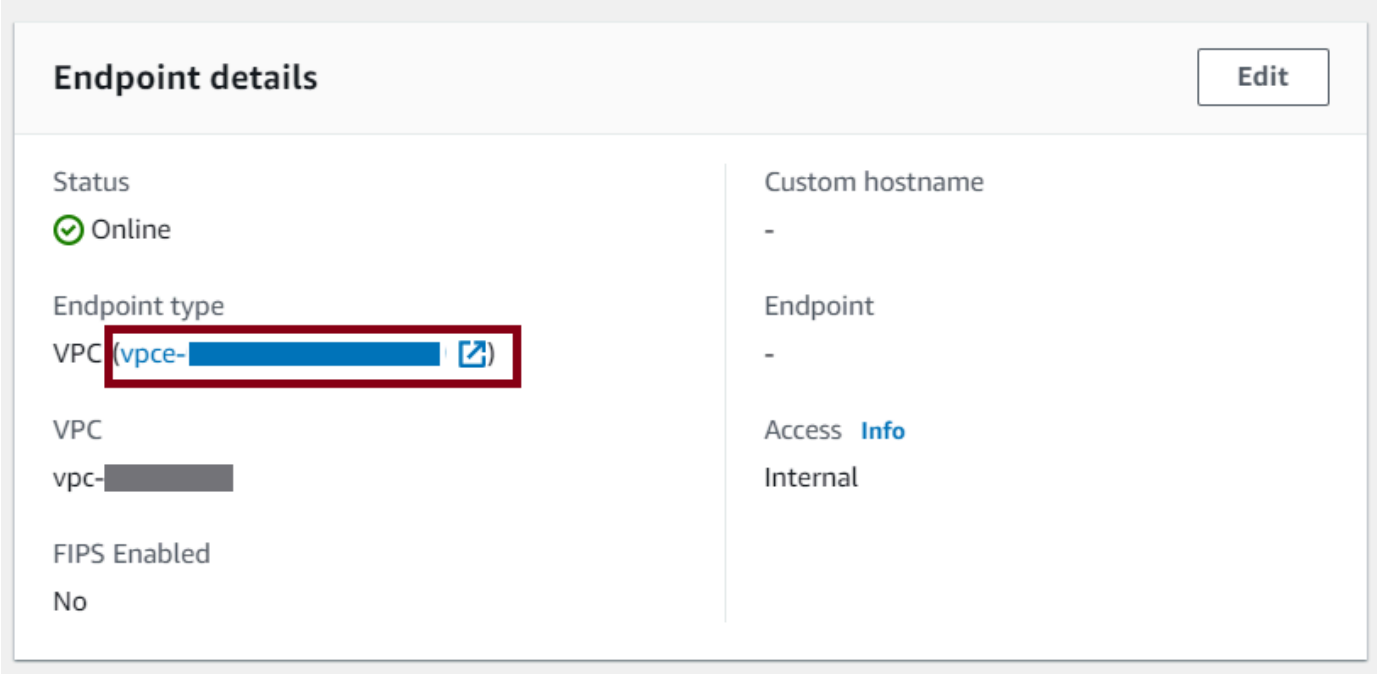
Command	Amazon S3	Amazon EFS
`mkdir`	支援	支援
`put`	支援	支援
`pwd`	支援	支援
`rename`	僅支援檔案	支援 **Note** 不支援重新命名以覆寫現有檔案或目錄。
`rm`	支援	支援
`rmdir`	支援 (僅限空目錄)	支援
`version`	支援	支援

尋找您的 Amazon VPC 端點

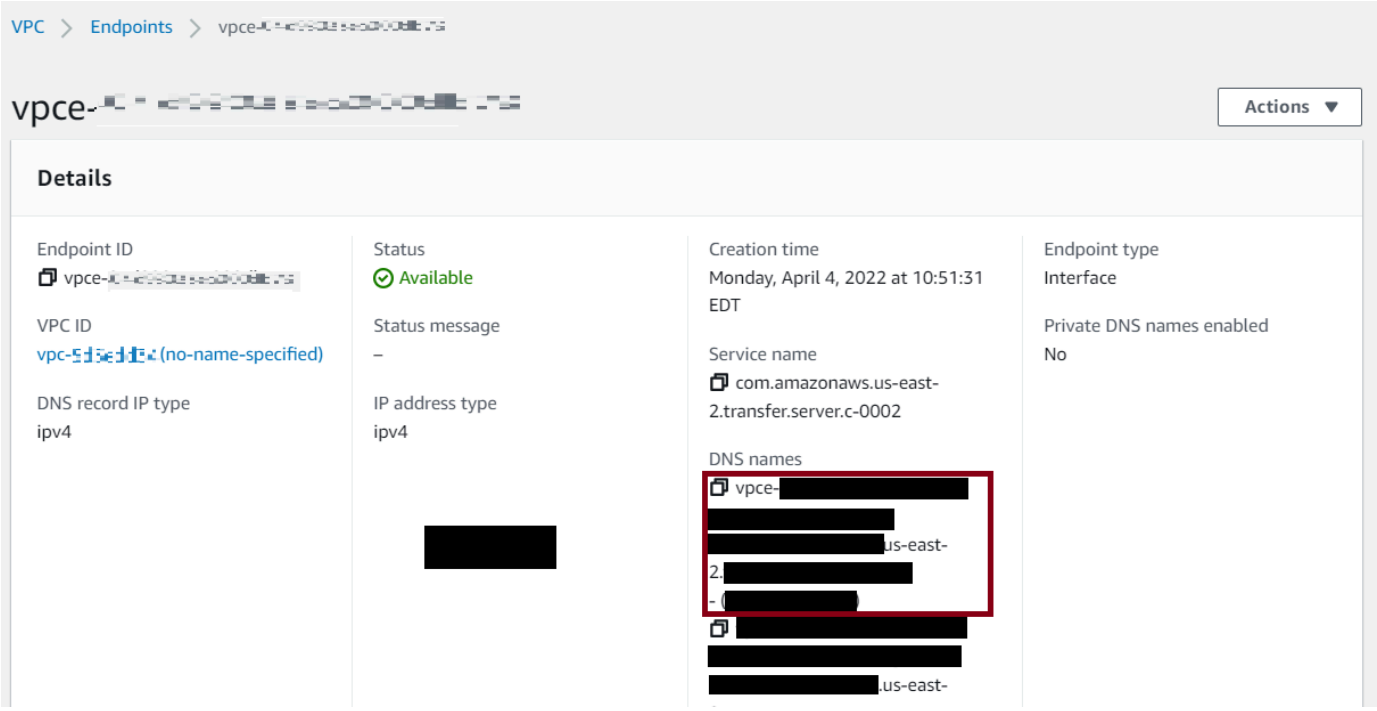
如果您的 Transfer Family 伺服器的端點類型是 VPC，識別用於傳輸檔案的端點並不簡單。在這種情況下，請使用下列程序尋找您的 Amazon VPC 端點。

尋找您的 Amazon VPC 端點

1. 瀏覽至伺服器的詳細資訊頁面。
2. 在端點詳細資料窗格中，選取 VPC。



3. 在 Amazon VPC 儀表板中，選取 VPC 端點識別碼。
4. 在 DNS 名稱清單中，您的伺服器端點是列出的第一個端點。



避免setstat錯誤

某些 SFTP 檔案傳輸用戶端可以在上傳檔案時，使用指令 (例如 SETSTAT) 嘗試變更遠端檔案的屬性，包括時間戳記和權限。不過，這些命令與 Amazon S3 等物件儲存系統並不相容。由於這種不相容性，即使已成功上傳檔案，從這些用戶端上傳檔案也可能導致錯誤。

- 當您呼叫CreateServer或 UpdateServer API 時，請使用此ProtocolDetails選項SetStatOption忽略用戶端嘗試在您上傳到 S3 儲存貯體的檔案上使用 SETSTAT 時產生的錯誤。
- 將值設定為 ENABLE_NO_OP，讓 Transfer 系列伺服器忽略 SETSTAT 命令，並上傳檔案，而不需要對 SFTP 用戶端進行任何變更。
- 請注意，雖然SetStatOptionENABLE_NO_OP設定會忽略錯誤，但會在 CloudWatch 記錄檔中產生記錄項目，因此您可以判斷用戶端何時進行 SETSTAT 呼叫。

如需此選項的 API 詳細資訊，請參閱ProtocolDetails。

使用 OpenSSH

使用下列說明使用 OpenSSH 從命令列傳輸檔案。

> **Note**
>
> 此用戶端僅適用於啟用 SFTP 的伺服器。

若要使用 OpenSSH 命令列公 AWS Transfer Family 用程式來傳輸檔案

1. 在 Linux、macOS 或視窗上，開啟命令終端機。
2. 在提示符下，輸入以下命令：

   ```
   sftp -i transfer-key sftp_user@service_endpoint
   ```

   在前面的命令中，*sftp_user*是用戶名，*transfer-key*是 SSH 私鑰。這裡*service_endpoint*是所選伺服器的 AWS Transfer Family 主控台中所示的伺服器端點。

> **Note**
>
> 此指令使用預設ssh_config檔案中的設定。除非您先前已編輯過此檔案，否則 SFTP 會使用連接埠 22。您可以透過將**-P**旗標新增至指令來指定不同的連接埠 (例如 2222)，如下所示。
>
> ```
> sftp -P 2222 -i transfer-key sftp_user@service_endpoint
> ```
>
> 或者，如果您一直想要使用連接埠 2222 或連接埠 22000，您可以更新檔案中的ssh_config預設連接埠。

應會出現 sftp 提示。

3. (選擇性) 若要檢視使用者的主目錄，請在提示下輸入下列命sftp令：

   ```
   pwd
   ```

4. 若要將檔案從檔案系統上載至轉移系列伺服器，請使用put指令。例如，若要上傳 hello.txt (假設該檔案位於檔案系統的目前目錄中)，請在提示下執行下列命sftp令：

   ```
   put hello.txt
   ```

   會出現類似下列內容的訊息，指出檔案傳輸正在進行中或已完成。

   ```
   Uploading hello.txt to /my-bucket/home/sftp_user/hello.txt

   hello.txt 100% 127 0.1KB/s 00:00
   ```

> **Note**
>
> 建立伺服器之後，您環境中的 DNS 服務可能需要幾分鐘的時間才能解析伺服器端點主機名稱。

使用 WinSCP

使用下列說明使用 WinSCP 從命令列傳輸檔案。

> **Note**
>
> 如果您使用的是 WinSCP 5.19，您可以使用 AWS 登入資料直接連線到 Amazon S3，並上傳/下載檔案。如需詳細資訊，請參閱連接至 Amazon S3 服務。

若要透過 AWS Transfer Family 使用 WinSCP 傳輸檔案

1. 開啟 WinSCP 用戶端。
2. 在「登入」對話方塊中，為「檔案通訊協定」選擇一個通訊協定：SFTP 或 FTP。

   如果您選擇 FTP，對於加密，請選擇下列其中一項：

   - 沒有 FTP 的加密
   - 適用於 FTPS 的 TLS/SSL 顯式加密
3. 針對 Host name (主機名稱)，輸入您的伺服器端點。伺服器端點位於 [伺服器詳細資料] 頁面上。如需詳細資訊，請參閱 檢視 SFTP、FTP 伺服器和 FTP 伺服器的詳細資訊。

   > **Note**
   >
   > 如果您的伺服器使用 VPC 端點，請參閱尋找您的 Amazon VPC 端點。
4. 針對連接埠號碼，輸入下列項目：

   - **22**適用於 SFTP
   - **21**適用於 FTP/FTPS
5. 在 [使用者名稱] 中，輸入您為特定身分識別提供者建立的使用者名稱。

   > **Note**
   >
   > 使用者名稱應該是您為身分提供者建立或設定的使用者之一。 AWS Transfer Family 提供下列身分識別提供者：
   >
   > - 與服務管理的使用者合作
   > - 使用 AWS Directory Service 身分識別提供者
   > - 使用自訂身分識別提供者
6. 選擇 [進階] 以開啟 [進階網站設定] 對話方塊。在 [SSH] 區段中，選擇 [驗證]。

7. 針對私密金鑰檔案，瀏覽並從檔案系統中選擇 SSH 私密金鑰檔案。

> **Note**
>
> 如果 WinSCP 提供將您的安全殼層私密金鑰轉換為 PPK 格式，請選擇 [確定]。

8. 選擇 OK (確定) 返回 Login (登入) 對話方塊，然後選擇 Save (儲存)。
9. 在 [將工作階段另存為網站] 對話方塊中，選擇 [確定] 以完成連線設定。
10. 在「登入」對話方塊中，選擇「工具」，然後選擇「偏好設定」。
11. 在「偏好設定」對話方塊中，對於「轉移」，選擇「耐久

    對於「啟用傳輸繼續/傳輸至暫存檔案名稱」選項，請選擇「停用」。

> **Note**
>
> 如果您將此選項保持啟用狀態，則會增加上傳成本，從而大幅降低上傳效能。它也可能導致大文件上傳失敗。

12. 對於傳輸，請選擇 [背景]，然後清除 [使用多個連線進行單一傳輸] 核取方塊。

> **Note**
>
> 如果您保持選取此選項，則大型檔案上傳可能會以無法預期的方式失敗。例如，可以建立產生 Amazon S3 費用的孤立分段上傳。也可能發生無訊息資料損毀。

13. 執行檔案傳輸。

    您可以使用 drag-and-drop 方法在目標視窗和來源視窗之間複製檔案。您可以使用工具列圖示來上傳、下載、刪除、編輯或修改 WinSCP 中檔案的屬性。

> **Note**
>
> 如果您使用 Amazon EFS 進行儲存，則此注意事項不適用。
> 嘗試變更遠端檔案屬性 (包括時間戳記) 的命令與物件儲存系統 (例如 Amazon S3) 不相容。因此，如果您使用 Amazon S3 進行儲存，請務必在執行檔案傳輸之前停用 WinSCP 時間戳記設定 (或`SetStatOption`如中所述使用避免`setstat`錯誤)。若要這麼做，請在 [WinSCP 傳輸設定] 對話方塊中，停用 [設定權限上傳] 選項和 [保留時間戳記一般] 選項。

使用網路鴨

使用下列說明使用 Cyberduck 從命令列傳輸檔案。

AWS Transfer Family 使用網絡鴨傳輸文件

1. 打開網絡鴨客戶端。
2. 選擇「開啟連線」。
3. 在「開啟連線」對話方塊中，選擇一個通訊協定：SFTP (SSH 檔案傳輸通訊協定)、FTP-SSL (明確驗證 TLS) 或 FTP (檔案傳輸通訊協定)。
4. 在伺服器中，輸入您的伺服器端點。伺服器端點位於 [伺服器詳細資料] 頁面上。如需詳細資訊，請參閱 檢視 SFTP、FTP 伺服器和 FTP 伺服器的詳細資訊。

   > **Note**
   >
   > 如果您的伺服器使用 VPC 端點，請參閱尋找您的 Amazon VPC 端點。

5. 針對連接埠號碼，輸入下列項目：
   - **22**適用於 SFTP
   - **21**適用於 FTP/FTPS
6. 針對 Username (使用者名稱)，輸入您在管理伺服器端點的使用者中建立的使用者名稱。
7. 如果選取了 SFTP，對於「安全殼層私密金鑰」，請選擇或輸入安全殼層私密金鑰。
8. 選擇連線。
9. 執行檔案傳輸。

   根據檔案所在位置，執行以下其中一項：
   - 在本機目錄 (來源) 中，選擇要傳輸的檔案，然後將檔案拖放到 Amazon S3 目錄 (目標)。
   - 在 Amazon S3 目錄 (來源) 中，選擇要傳輸的檔案，然後將檔案拖放到本機目錄 (目標) 中。

使用 FileZilla

請按照以下說明使用傳輸文件 FileZilla。

設定 FileZilla 檔案傳輸

1. 開啟用 FileZilla 戶端。
2. 選擇 [檔案]，然後選擇 [網站管理員]。
3. 在「網站管理員」對話方塊中，選擇「新增網站」。
4. 在 [一般] 索引標籤上，針對 [通訊協定] 選擇通訊協定：SFTP 或 FTP。

   如果您選擇 FTP，對於加密，請選擇下列其中一項：

   - 僅使用普通 FTP（不安全）-用於 FTP
   - 使用透過 TLS 的明確 FTP (如果有的話) — 適用於 FTPS
5. 在「主機名稱」中，輸入您正在使用的通訊協定，然後輸入伺服器端點。伺服器端點位於 [伺服器詳細資料] 頁面上。如需詳細資訊，請參閱 檢視 SFTP、FTP 伺服器和 FTP 伺服器的詳細資訊。

   > **Note**
   >
   > 如果您的伺服器使用 VPC 端點，請參閱尋找您的 Amazon VPC 端點。

   - 如果您使用的是 SFTP，請輸入：`sftp://`*`hostname`*
   - 如果您使用的是 FTPS，請輸入：`ftps://`*`hostname`*

   確保將*###*替換為實際服務器端點。
6. 針對連接埠號碼，輸入下列項目：

   - **22**適用於 SFTP
   - **21**適用於 FTP/FTPS
7. 如果選取了 SFTP，請選擇「金鑰檔案」做為「登入類型」。

   在金鑰檔案中，選擇或輸入安全殼層私密金鑰。
8. 在使用者中，輸入您在中建立之使用者的名稱管理伺服器端點的使用者。
9. 選擇連線。
10. 執行檔案傳輸。

> **Note**
>
> 如果您中斷正在進行的檔案傳輸， AWS Transfer Family 可能會在 Amazon S3 儲存貯體中寫入部分物件。如果您中斷上傳，請先檢查 Amazon S3 儲存貯體中的檔案大小是否與來源物件的檔案大小相符，然後再繼續。

使用一個 Perl 客戶端

如果您使用 NET::SFTP::Foreign perl 用戶端，則必須將設定`queue_size`為`1`。例如：

```
my $sftp = Net::SFTP::Foreign->new('user@s-12345.server.transfer.us-east-2.amazonaws.com', queue_size => 1);
```

> **Note**
>
> 1.92. 02 `Net::SFTP::Foreign` 之前的修訂版本需要此因應措施。

上傳後處理

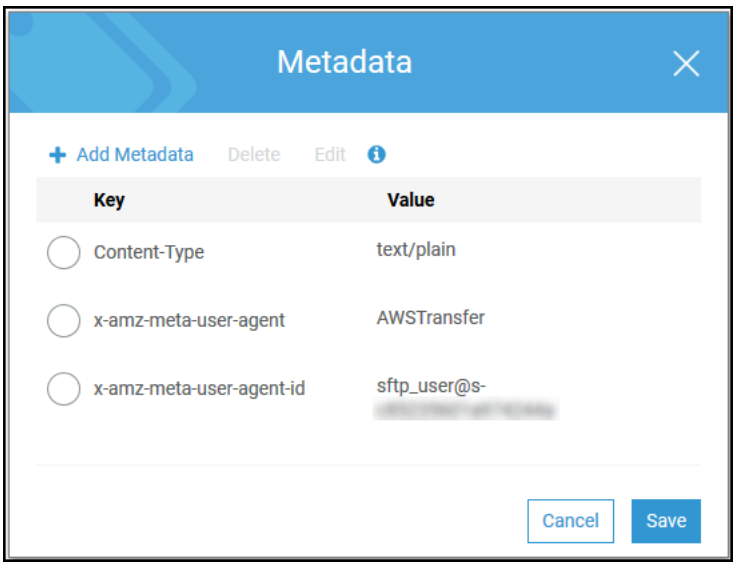
您可以檢視上傳後處理資訊，包括 Amazon S3 物件中繼資料和事件通知。

主題

- Amazon S3 對象元數據
- Amazon S3 事件通知

Amazon S3 對象元數據

作為對象元數據的一部分，您會看到一個名為`x-amz-meta-user-agent`其值的鍵`AWSTransfer`，`x-amz-meta-user-agent-id`其值為`username@server-id`。`username`是上傳檔案的「Transfer Family」使用者，`server-id`也是用於上載的伺服器。您可以使用 Lambda 函數內 S3 物件上的HeadObject作業來存取此資訊。



Amazon S3 事件通知

使用 Transfer Family 將物件上傳到 S3 儲存貯體時，會包含`RoleSessionName`在 S3 事件通知結構中的「請求者」欄位中，如`[AWS:Role Unique Identifier]/username.sessionid@server-id`下所示。例如，以下是複製到 S3 儲存貯體之檔案的 S3 存取日誌中範例請求者欄位的內容。

```
arn:aws:sts::AWS-Account-ID:assumed-role/IamRoleName/
username.sessionid@server-id
```

在上面的「請求者」欄位中，它會顯示呼叫`IamRoleName`的 IAM 角色。如需有關設定 S3 事件通知的詳細資訊，請參閱 Amazon 簡單儲存服務開發人員指南中的設定 Amazon S3 事件通知。如需有關 AWS Identity and Access Management (IAM) 角色唯一識別碼的詳細資訊，請參閱AWS Identity and Access Management 使用者指南中的唯一識別碼。

管理伺服器端點的使用者

在以下各節中，您可以找到有關如何使用AWS Directory Service for Microsoft Active Directory或自訂身分識別提供者新增使用AWS Transfer Family者的資訊。

如果您使用服務管理的身分類型，則會將使用者新增至已啟用檔案傳輸通訊協定的伺服器。當您這樣做時，每個使用者名稱在您的伺服器上都必須是唯一的。

每個使用者的屬性中也要存放該使用者的 Secure Shell (SSH) 公有金鑰。若要進行此程序使用的金鑰型驗證，則必須執行此動作。私密金鑰會儲存在使用者的電腦本機上。當您的使用者使用用戶端向您的

伺服器傳送驗證要求時，您的伺服器會先確認使用者可以存取關聯的 SSH 私密金鑰。然後，伺服器會成功驗證使用者。

此外，您可以指定使用者的主目錄或登陸目錄，並指派 AWS Identity and Access Management (IAM) 角色給使用者。或者，您可以提供工作階段政策，限制使用者只能存取 Amazon S3 儲存貯體的主目錄。

> **Important**
>
> AWS Transfer Family封鎖長度為 1 或 2 個字元的使用者名稱，無法對 SFTP 伺服器進行驗證。此外，我們也會封鎖使`root`用者名稱。
> 這背後的原因是由於密碼掃描程序大量惡意登錄嘗試。

Amazon EFS 與 Amazon S3

每個儲存選項的特性：

- 限制存取：Amazon S3 支援工作階段政策；Amazon EFS 支援 POSIX 使用者、群組和次要群組 ID
- 兩者都支持公鑰/私鑰
- 兩者都支持主目錄
- 兩者都支持邏輯目錄

> **Note**
>
> 對於 Amazon S3，邏輯目錄的大部分支援都是透過 API/CLI。您可以使用主控台中的 [受限制] 核取方塊，將使用者鎖定至其主目錄，但無法指定虛擬目錄結構。

邏輯目錄

如果您要為使用者指定邏輯目錄值，則使用的參數取決於使用者的類型。

- 對於服務管理的使用者，請在`HomeDirectoryMappings`中提供邏輯目錄值。
- 對於自訂身分識別提供者使用者，請在中`HomeDirectoryDetails`提供邏輯目錄值

主題

- 與服務管理的使用者合作

- 使用 AWS Directory Service 身分識別提供者
- 使用自訂身分識別提供者

與服務管理的使用者合作

您可以根據伺服器的網域設定，將 Amazon S3 或 Amazon EFS 服務受管使用者新增至您的伺服器。如需詳細資訊，請參閱 設定 SFTP、FTPS 或 FTP 伺服器端點。

若要以程式設計方式新增服務管理的使用者，請參閱 CreateUserAPI 的範例。

> **Note**
>
> 對於服務管理的使用者，限制為 2,000 個邏輯目錄項目。如需使用邏輯目錄的資訊，請參閱使用邏輯目錄簡化您的 Transfer Family 目錄結構。

主題

- 新增 Amazon S3 服務受管使用者
- 新增 Amazon EFS 服務受管使用者
- 管理服務管理使用者

新增 Amazon S3 服務受管使用者

> **Note**
>
> 如果您想要設定跨帳戶 Amazon S3 儲存貯體，請遵循此知識中心文章中提到的步驟：如何設定我的AWS Transfer Family伺服器使用另一個AWS帳戶中的 Amazon 簡單儲存服務儲存貯體？ 。

將 Amazon S3 服務受管使用者新增至您的伺服器

1. 在 https://console.aws.amazon.com/transfer/ 開啟AWS Transfer Family主控台，然後從導覽窗格中選取 [伺服器]。
2. 在 [伺服器] 頁面上，選取要新增使用者之伺服器的核取方塊。
3. 選擇新增使用者。

4. 在 [使用者設定] 區段中，輸入使用者名稱做為使用者名稱。此使用者名稱必須至少為 3 個字元且最多 100 個字元。您可以在使用者名稱中使用下列字元：a—z、A-Z、0—9、底線 '_'、連字號 '-'、句號 '.'。 ' ，並在符號「@」。用戶名不能以連字符 '-'，句點 '開頭 。 ' ，或在符號「@」。

5. 對於存取，請選擇您先前建立的 IAM 角色，以提供對 Amazon S3 儲存貯體的存取權限。

   您使用建立 IAM 角色和政策的程序建立此 IAM 角色。該 IAM 角色包含 IAM 政策，可讓您存取 Amazon S3 儲存貯體。它也包含在其他 IAM 政策中定義的 AWS Transfer Family 服務信任關係。如果您需要對使用者進行精細的存取控制，請參閱使用AWS Transfer Family和 Amazon S3 增強資料存取控制部落格文章。

6. (選擇性) 針對策略，選取下列其中一項：

   - 無
   - 現有政策
   - 從 IAM 選取政策：可讓您選擇現有的工作階段政策。選擇檢視以查看包含原則詳細資訊的 JSON 物件。
   - 根據主資料夾自動產生原則：為您產生工作階段原則。選擇檢視以查看包含原則詳細資訊的 JSON 物件。

   > **Note**
   >
   > 如果您選擇 [根據主資料夾自動產生原則]，請勿為此使用者選取 [限制]。

   若要進一步瞭解工作階段原則，請參閱建立 IAM 角色和政策。若要進一步瞭解如何建立工作階段原則，請參閱為 Amazon S3 儲存貯體建立工作階段政策。

7. 對於主目錄，請選擇要使用的 Amazon S3 儲存貯體存放要傳輸的資料AWS Transfer Family。輸入使用者使用其用戶端登入時所在home目錄的路徑。

   如果將此參數保持空白，則會使用 Amazon S3 儲存貯體的`root`目錄。在本例中，請確定您的 IAM 角色能夠存取此 `root` 目錄。

   > **Note**
   >
   > 建議您選擇包含使用者使用者名稱的目錄路徑，以便有效地使用階段作業原則。工作階段政策將 Amazon S3 儲存貯體中的使用者存取限制在該使用者的home目錄。

8. (選擇性) 對於「受限制」，請選取核取方塊，讓使用者無法存取該資料夾以外的任何內容，也看不到 Amazon S3 儲存貯體或資料夾名稱。

   > **Note**
   >
   > 為使用者指定主目錄並將使用者限制在該主目錄應該足以鎖定使用者對指定資料夾的存取權。如果您需要套用進一步的控制項，請使用工作階段原則。
   > 如果您為此使用者選取 [受限制]，則無法選取 [根據主資料夾自動產生原則]，因為主資料夾不是 [受限制的使用者] 定義的值。

9. 對於 SSH 公開金鑰，請輸入安全殼層 key pair 的公開安全殼層金鑰部分。

   金鑰要先經服務驗證，您才能新增新使用者。

   > **Note**
   >
   > 如需如何產生 SSH 金鑰對的說明，請參閱為服務管理的使用者產生 SSH 金鑰。

10. (選擇性) 在「機碼和值」中，輸入一或多個標籤作為鍵值配對，然後選擇「新增標籤」。
11. 選擇 Add (新增) 將新使用者新增至您選擇的伺服器。

    新使用者會顯示在 [伺服器詳細資訊] 頁面的 [使用者] 區段中。

後續步驟 — 對於下一步，請繼續執行使用用戶端透過伺服器端點傳輸檔案。

新增 Amazon EFS 服務受管使用者

Amazon EFS 使用可攜式作業系統界面 (POSIX) 檔案權限模型來代表檔案擁有權。

- 如需 Amazon EFS 檔案擁有權的詳細資訊，請參閱 Amazon EFS 檔案擁有權。
- 如需為 EFS 使用者設定目錄的詳細資訊，請參閱為 Transfer Family 設定 Amazon EFS 使用者。

將 Amazon EFS 服務受管使用者新增至您的伺服器

1. 在 https://console.aws.amazon.com/transfer/ 開啟AWS Transfer Family主控台，然後從導覽窗格中選取 [伺服器]。
2. 在「伺服器」頁面上，選取您要新增使用者的 Amazon EFS 伺服器。
3. 選擇新增使用者以顯示 [新增使用者] 頁面。

4. 在 [使用者組態] 區段中，使用下列設定。

   a. 「使用者名稱」必須至少為 3 個字元，最多 100 個字元。您可以在使用者名稱中使用下列字元：a—z、A-Z、0—9、底線 '_'、連字號 '-'、句號 ' 。 ' ，並在符號「@」。用戶名不能以連字符 '-' ，句點 '開頭 。 ' ，或在符號「@」。

   b. 對於「使用者 ID」和「群組 ID」，請注意以下事項：

      - 對於您建立的第一個使用者，我們建議您同時輸入「群組 ID」和「使用者 ID」的**0**值。這會授予使用者管理員使用 Amazon EFS 的權限。
      - 若為其他使用者，請輸入使用者的 POSIX 使用者 ID 和群組 ID。這些 ID 用於使用者執行的所有 Amazon Elastic File System 操作。
      - 對於使用者 ID 和群組 ID，請勿使用任何前導零。例如，**12345**是可以接受的，不**012345**是。

   c. (選擇性) 對於「次要群組 ID」，請為每個使用者輸入一或多個其他 POSIX 群組 ID，以逗號分隔。

   d. 對於存取權，請選擇 IAM 角色：

      - 讓使用者只能存取您希望他們存取的 Amazon EFS 資源 (檔案系統)。
      - 定義使用者可以執行和無法執行的檔案系統作業。

      我們建議您在 Amazon EFS 檔案系統選擇中使用 IAM 角色，並具有掛載存取權限和讀取/寫入許可。例如，以下兩個AWS受管理策略的組合雖然相當寬鬆，但會為您的使用者授予必要的權限：

      - AmazonElasticFileSystemClientFullAccess
      - AWSTransferConsoleFullAccess

      如需詳細資訊，請參閱 Amazon 彈性檔案系統的部落格文章AWS Transfer Family支援。

   e. 對於主目錄，請執行以下操作：

      - 選擇您要用來存放要傳輸之資料的 Amazon EFS 檔案系統AWS Transfer Family。
      - 決定是否要將主目錄設定為「受限制」。將主目錄設定為「限制」會產生下列影響：
        - Amazon EFS 使用者無法存取該資料夾外的任何檔案或目錄。
        - Amazon EFS 使用者看不到 Amazon EFS 檔案系統名稱 (fs-xxxxxxx)。

> **Note**
>
> 選取「受限制」選項時，Amazon EFS 使用者無法解析符號連結。

- (選擇性) 輸入您希望使用者使用其用戶端登入時所在的主目錄路徑。

  如果未指定主目錄，則會使用 Amazon EFS 檔案系統的根目錄。在這種情況下，請確保您的 IAM 角色可提供對此根目錄的存取權。

5. 對於 SSH 公開金鑰，請輸入安全殼層 key pair 的公開安全殼層金鑰部分。

   金鑰要先經服務驗證，您才能新增新使用者。

   > **Note**
   >
   > 如需如何產生 SSH 金鑰對的說明，請參閱為服務管理的使用者產生 SSH 金鑰。

6. (選擇性) 輸入使用者的任何標籤。在「鍵和值」中，輸入一或多個標籤作為鍵值配對，然後選擇「新增標籤」。
7. 選擇 Add (新增) 將新使用者新增至您選擇的伺服器。

   新使用者會顯示在 [伺服器詳細資訊] 頁面的 [使用者] 區段中。

當您第一次將 SFTP 轉移到 Transfer Family 伺服器時可能會遇到的問題：

- 如果您執行`sftp`命令，但沒有出現提示，您可能會遇到下列訊息：

  ```
  Couldn't canonicalize: Permission denied

  Need cwd
  ```

  在此情況下，您必須增加使用者角色的原則權限。您可以新增受AWS管理的策略，例如`AmazonElasticFileSystemClientFullAccess`。
- 如果您`pwd`在`sftp`提示下輸入以檢視使用者的主目錄，您可能會看到下列訊息，其中`######`是 SFTP 使用者的主目錄：

  ```
  remote readdir("/USER-HOME-DIRECTORY"): No such file or directory
  ```

  在此情況下，您應該能夠瀏覽至父目錄 (`cd ..`)，並建立使用者的主目錄 (`mkdir username`)。

後續步驟 — 對於下一步，請繼續執行使用用戶端透過伺服器端點傳輸檔案。

管理服務管理使用者

在本節中，您可以找到有關如何檢視使用者清單、如何編輯使用者詳細資訊，以及如何新增安全殼層公開金鑰的相關資訊。

- 檢視使用者清單
- 查看或編輯用戶詳細信息
- 刪除使用者
- 新增安全殼層公開金
- 刪除 SSH 公鑰

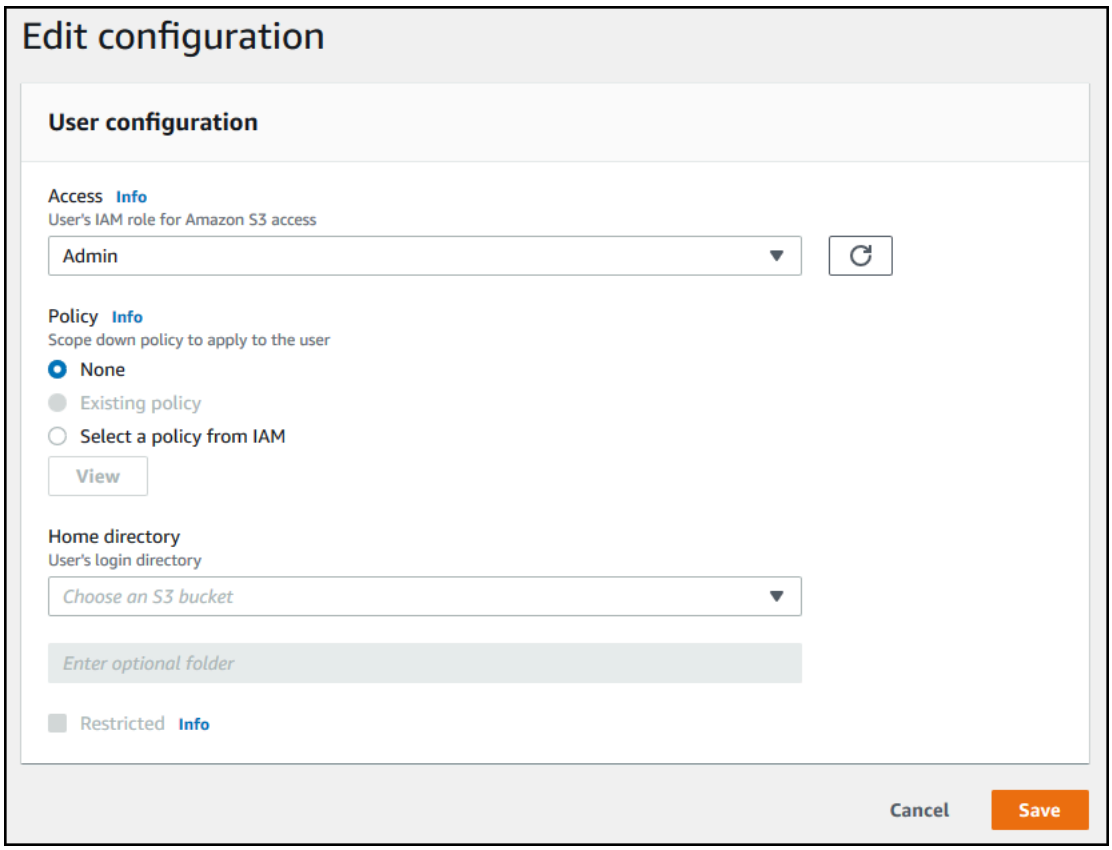
若要尋找您的使用者清單

1. 請在以下位置開啟AWS Transfer Family主控台。 https://console.aws.amazon.com/transfer/
2. 從導覽窗格中選取 [伺服器] 以顯示 [伺服器] 頁面。
3. 在「伺服器 ID」欄中選擇識別碼，以查看「伺服器詳細資訊」頁面。
4. 在「使用者」下，檢視使用者清單。

檢視或編輯使用者詳細資訊

1. 請在以下位置開啟AWS Transfer Family主控台。 https://console.aws.amazon.com/transfer/
2. 從導覽窗格中選取 [伺服器] 以顯示 [伺服器] 頁面。
3. 在「伺服器 ID」欄中選擇識別碼，以查看「伺服器詳細資訊」頁面。
4. 在 [使用者] 下，選擇使用者名稱以查看 [使用者詳細資料]

   您可以選擇 [編輯]，在此頁面上變更使用者的特性。
5. 在 [使用者詳細資料] 頁面上，選擇 [使用者組態] 旁邊的 [



6. 在「編輯組態」 頁面上，對於「存取」，選擇您先前建立的 IAM 角色，以提供對 Amazon S3 儲存貯體的存取權。

   您使用建立 IAM 角色和政策的程序建立此 IAM 角色。該 IAM 角色包含 IAM 政策，可讓您存取 Amazon S3 儲存貯體。它也包含在其他 IAM 政策中定義的 AWS Transfer Family 服務信任關係。

7. (選擇性) 針對策略，選擇下列其中一項：

   - 無
   - 現有政策
   - 從 IAM 選取政策以選擇現有政策。選擇檢視以查看包含原則詳細資訊的 JSON 物件。

   若要進一步瞭解工作階段原則，請參閱建立 IAM 角色和政策。若要進一步瞭解如何建立工作階段原則，請參閱為 Amazon S3 儲存貯體建立工作階段政策。

8. 對於主目錄，請選擇要使用的 Amazon S3 儲存貯體存放要傳輸的資料AWS Transfer Family。輸入使用者使用其用戶端登入時所在home目錄的路徑。

   如果將此參數保留空白，則會使用 Amazon S3 儲存貯體的root目錄。在本例中，請確定您的 IAM 角色能夠存取此 `root` 目錄。

> **Note**
>
> 建議您選擇包含使用者使用者名稱的目錄路徑，以便有效地使用階段作業原則。工作階段政策將 Amazon S3 儲存貯體中的使用者存取限制在該使用者的home目錄。

9. (選擇性) 對於「受限制」，請選取核取方塊，讓使用者無法存取該資料夾以外的任何內容，也看不到 Amazon S3 儲存貯體或資料夾名稱。

> **Note**
>
> 為使用者指定主目錄並將使用者限制在該主目錄時，這應該足以鎖定使用者對指定資料夾的存取權限。當您需要套用進一步控制時，請使用工作階段原則。

10. 選擇儲存，以儲存變更。

若要刪除使用者

1. 請在以下位置開啟AWS Transfer Family主控台。 https://console.aws.amazon.com/transfer/
2. 從導覽窗格中選取 [伺服器] 以顯示 [伺服器] 頁面。
3. 在「伺服器 ID」欄中選擇識別碼，以查看「伺服器詳細資訊」頁面。
4. 在 [使用者] 下，選擇使用者名稱以查看 [使用者詳細資料]
5. 在 [使用者詳細資料] 頁面上，選擇使用者名稱右邊的 [刪除]。
6. 在出現的確認對話方塊中，輸入文字**`delete`**，然後選擇 [刪除] 以確認您要刪除使用者。

這時系統會從用戶列表中刪除該用戶。

若要為使用者新增 SSH 公開金鑰

1. 請在以下位置開啟AWS Transfer Family主控台。 https://console.aws.amazon.com/transfer/
2. 在導覽窗格中，選擇 Servers (伺服器)。
3. 在「伺服器 ID」欄中選擇識別碼，以查看「伺服器詳細資訊」頁面。
4. 在 [使用者] 下，選擇使用者名稱以查看 [使用者詳細資料]
5. 選擇 Add SSH public key (新增 SSH 公有金鑰) 來將新的 SSH 公有金鑰新增至使用者。

> **Note**
>
> SSH 金鑰只能由已啟用安全殼層 (SSH) 檔案傳輸通訊協定 (SFTP) 的伺服器使用。如需如何產生 SSH key pair 的詳細資訊，請參閱為服務管理的使用者產生 SSH 金鑰。

6. 針對 SSH public key (SSH 公有金鑰)，輸入 SSH 金鑰對的 SSH 公有金鑰部分。

   金鑰要先經服務驗證，您才能新增新使用者。SSH 金鑰的格式是 `ssh-rsa string`。若要產生 SSH key pair，請參閱為服務管理的使用者產生 SSH 金鑰。
7. 選擇 Add key (新增金鑰)。

若要刪除使用者的安全殼層公開金鑰

1. 請在以下位置開啟AWS Transfer Family主控台。 https://console.aws.amazon.com/transfer/
2. 在導覽窗格中，選擇 Servers (伺服器)。
3. 在「伺服器 ID」欄中選擇識別碼，以查看「伺服器詳細資訊」頁面。
4. 在 [使用者] 下，選擇使用者名稱以查看 [使用者詳細資料]
5. 若要刪除公開金鑰，請選取其安全殼層金鑰核取方塊，然後選擇刪除。

使用 AWS Directory Service 身分識別提供者

本主題說明如何使用的 AWS Directory Service 識別提供者 AWS Transfer Family。

主題

- 使用 AWS Directory Service for Microsoft Active Directory
- 使用 Azure 作用中 AWS 目錄網域服務的 Directory Service

使用 AWS Directory Service for Microsoft Active Directory

您可以使用 AWS Transfer Family 來驗證您的檔案傳輸最終使用者 AWS Directory Service for Microsoft Active Directory。它可讓依賴 Active Directory 驗證的檔案傳輸工作流程順暢移轉，而不需要變更使用者的認證或需要自訂授權者。

您可以透過 SFTP AWS Managed Microsoft AD、FTPS 和 FTP 安全地為 AWS Directory Service 使用者和群組提供存取亞馬遜簡單儲存服務 (Amazon S3) 或亞馬遜彈性檔案系統 (Amazon EFS) 中的資

料。如果您使用 Active Directory 來儲存使用者的認證，您現在可以更輕鬆地為這些使用者啟用檔案傳輸。

您可以使用 Active Directory 連接器，提供內部部署環境或 AWS 雲端中使用中目錄群組的存取權。AWS Managed Microsoft AD 您可以授與已在 Microsoft Windows 環境中 (在 AWS 雲端或內部部署網路中) 中設定的使用者存取用 AWS Managed Microsoft AD 於識別身分的 AWS Transfer Family 伺服器。

> **Note**
>
> - AWS Transfer Family 不支援 Simple AD。
> - Transfer Family 不支援跨區域 Active Directory 設定：我們只支援與 Transfer Family 伺服器位於相同區域的 Active Directory 整合。
> - Transfer Family 不支援使用 AWS Managed Microsoft AD 或 AD Connector 為您現有的無線電式 MFA 基礎架構啟用多因素驗證 (MFA)。
> - AWS Transfer Family 不支援受管理的作用中目錄的複寫區域。

若要使用 AWS Managed Microsoft AD，您必須執行下列步驟：

1. 使用控制台創建一個或多個 AWS Managed Microsoft AD 目 AWS Directory Service 錄。
2. 使用「Transfer Family」主控台建立用 AWS Managed Microsoft AD 作其身分識別提供者的伺服器。
3. 從一個或多個 AWS Directory Service 群組新增存取權。
4. 雖然不是必要的，但我們建議您測試並驗證使用者存取權。

主題

- 開始使用之前 AWS Directory Service for Microsoft Active Directory
- 使用作用中目錄範圍
- 選擇 AWS Managed Microsoft AD 身分識別提供者
- 授予群組存取權
- 測試使用者
- 刪除群組的伺服器存取權
- 使用 SSH（安全殼層）連接到服務器

- 使用樹系和信任連線 AWS Transfer Family 至自我管理的 Active Directory

開始使用之前 AWS Directory Service for Microsoft Active Directory

為 AD 群組提供唯一識別碼

您必須為 Microsoft AD 目錄中的每個群組提供唯一識別碼 AWS Managed Microsoft AD，才能使用。您可以使用每個群組的安全性識別碼 (SID) 來執行此作業。您關聯之群組的使用者可以使用 AWS Transfer Family 列，透過已啟用的協定存取 Amazon S3 或 Amazon EFS 資源。

使用下列 Windows PowerShell 命令擷取群組的 SID，並以群組*YourGroupName*的名稱取代。

```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties * | Select
 SamAccountName,ObjectSid
```

> **Note**
>
> 如果您使用 AWS Directory Service 做為身分識別提供者，並`userPrincipalName`且`SamAccountName`具有不同的值，請 AWS Transfer Family 接受中的值`SamAccountName`。Transfer Family 不接受中指定的值`userPrincipalName`。

為您的角色新增 AWS Directory Service 權限

您還需要 AWS Directory Service API 權限才能用 AWS Directory Service 作身分提供者。下列是必要或建議的權限：

- `ds:DescribeDirectories`需要 Transfer Family 才能查找目錄
- `ds:AuthorizeApplication`需要為 Transfer Family 添加授權
- `ds:UnauthorizeApplication`建議刪除任何臨時創建的資源，以防在服務器創建過程中出現問題

將這些權限新增至您用來建立 Transfer Family 伺服器的角色。如需這些權限的詳細資訊，請參閱 AWS Directory Service API 權限：動作、資源和條件參考。

使用作用中目錄範圍

當您考慮如何讓 Active Directory 使用者存取 AWS Transfer Family 伺服器時，請記住使用者的範圍及其群組的範圍。理想情況下，使用者的範圍及其群組的範圍應該相符。也就是說，使用者和群組都在預

設範圍中，或兩者都位於信任的範圍中。如果不是這種情況，則無法通過 Transfer Family 對用戶進行身份驗證。

您可以測試使用者以確保組態正確無誤。如需詳細資訊，請參閱 測試使用者。如果使用者/群組範圍發生問題，您會收到錯誤訊息：找不到使用者群組的相關存取權。

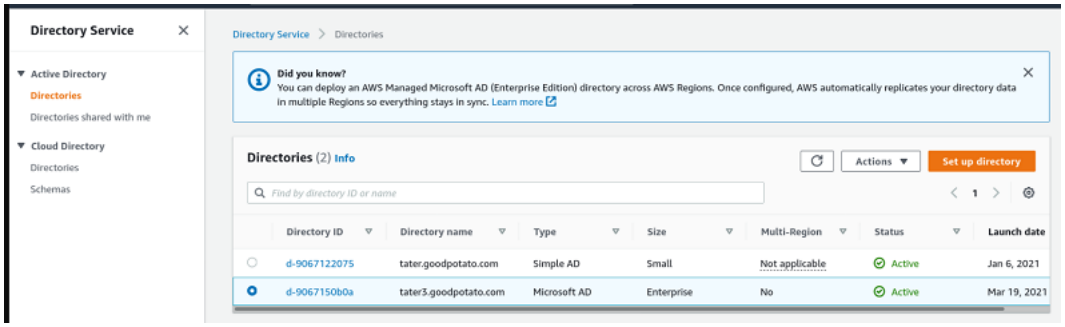
選擇 AWS Managed Microsoft AD 身分識別提供者

本節說明如何 AWS Directory Service for Microsoft Active Directory 搭配伺服器使用。

AWS Managed Microsoft AD 搭配 Transfer Family 使用

1. 請登入 AWS Management Console 並開啟 AWS Directory Service 主控台，網址為 https://console.aws.amazon.com/directoryservicev2/。

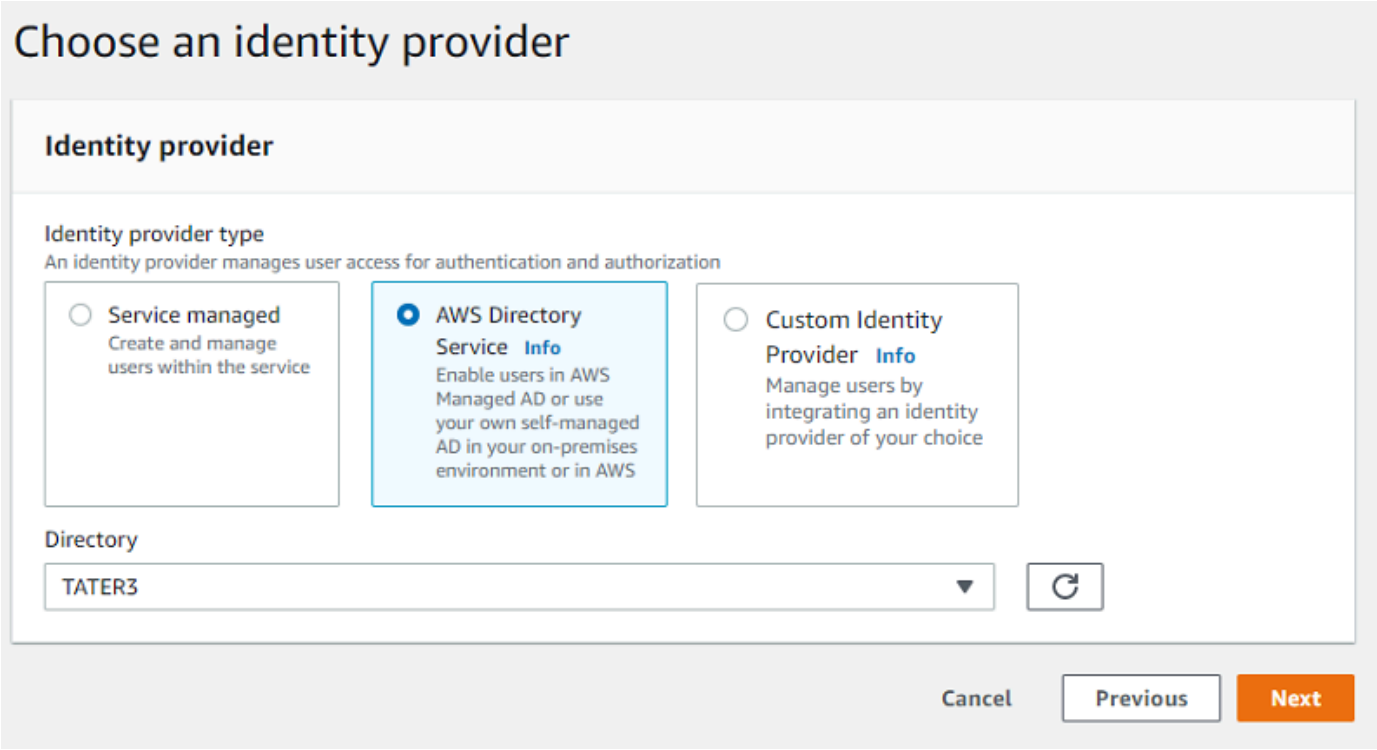
   使用主 AWS Directory Service 控台設定一或多個受管理的目錄。如需詳細資訊，請參閱《 AWS Directory Service 管理員指南》中的 AWS Managed Microsoft AD。



2. 請在 https://console.aws.amazon.com/transfer/ 開啟 AWS Transfer Family 主控台，然後選擇「建立伺服器」。
3. 在 [選擇通訊協定] 頁面上，從清單中選擇一或多個通訊協定。

   > **Note**
   >
   > 如果您選取 FTPS，則必須提供 AWS Certificate Manager 憑證。

4. 對於選擇身分識別提供者，請選擇 AWS Directory Service。



5. 目錄清單包含您已設定的所有受管理目錄。從清單中選擇目錄，然後選擇「下一步」。

> **Note**
>
> - 不支援跨帳戶和共用目錄。 AWS Managed Microsoft AD
> - 若要將 Directory Service 設定為您的身分識別提供者的伺服器，您需要新增一些 AWS Directory Service 權限。如需詳細資訊，請參閱 開始使用之前 AWS Directory Service for Microsoft Active Directory。

6. 若要完成伺服器的建立，請使用下列其中一個程序：

- 建立啟用 SFTP 的伺服器
- 建立啟用 FTP 的伺服器
- 建立啟用 FTP 的伺服器

在這些程序中，請繼續選擇身分識別提供者之後的步驟。

> **Important**
>
> 如果您在 Transfer Family 伺服器中 AWS Directory Service 使用了 Microsoft AD 目錄，則無法刪除該目錄。您必須先刪除伺服器，然後才能刪除目錄。

授予群組存取權

建立伺服器之後，您必須選擇目錄中的哪些群組應該有權透過已啟用的通訊協定上傳和下載檔案 AWS Transfer Family。您可以透過建立存取權來執行此操作。

> **Note**
>
> 使用者必須直接屬於您要授與存取權的群組。例如，假設 Bob 是一個用戶，他屬於 GroupA，並且 GroupA 本身包含在 GroupB 中。
>
> - 如果您授與 GroupA 的存取權，Bob 就會被授與存取權。
> - 如果您授予 GroupB 的存取權 (而不是 GroupA)，Bob 將無法存取。

若要授與群組存取權

1. 請在以下位置開啟 AWS Transfer Family 主控台。 https://console.aws.amazon.com/transfer/
2. 瀏覽至您的伺服器詳細資訊頁面。
3. 在「存取」區段中，選擇「新增存取權」。
4. 輸入您要存取此伺服器之 AWS Managed Microsoft AD 目錄的 SID。

   > **Note**
   >
   > 如需如何尋找群組 SID 的詳細資訊，請參閱the section called “開始使用之前 AWS Directory Service for Microsoft Active Directory”。

5. 對於存取，請選擇群組的 AWS Identity and Access Management (IAM) 角色。
6. 在「策略」區段中，選擇策略。預設設定為「無」。
7. 對於主目錄，請選擇與群組主目錄對應的 S3 儲存貯體。

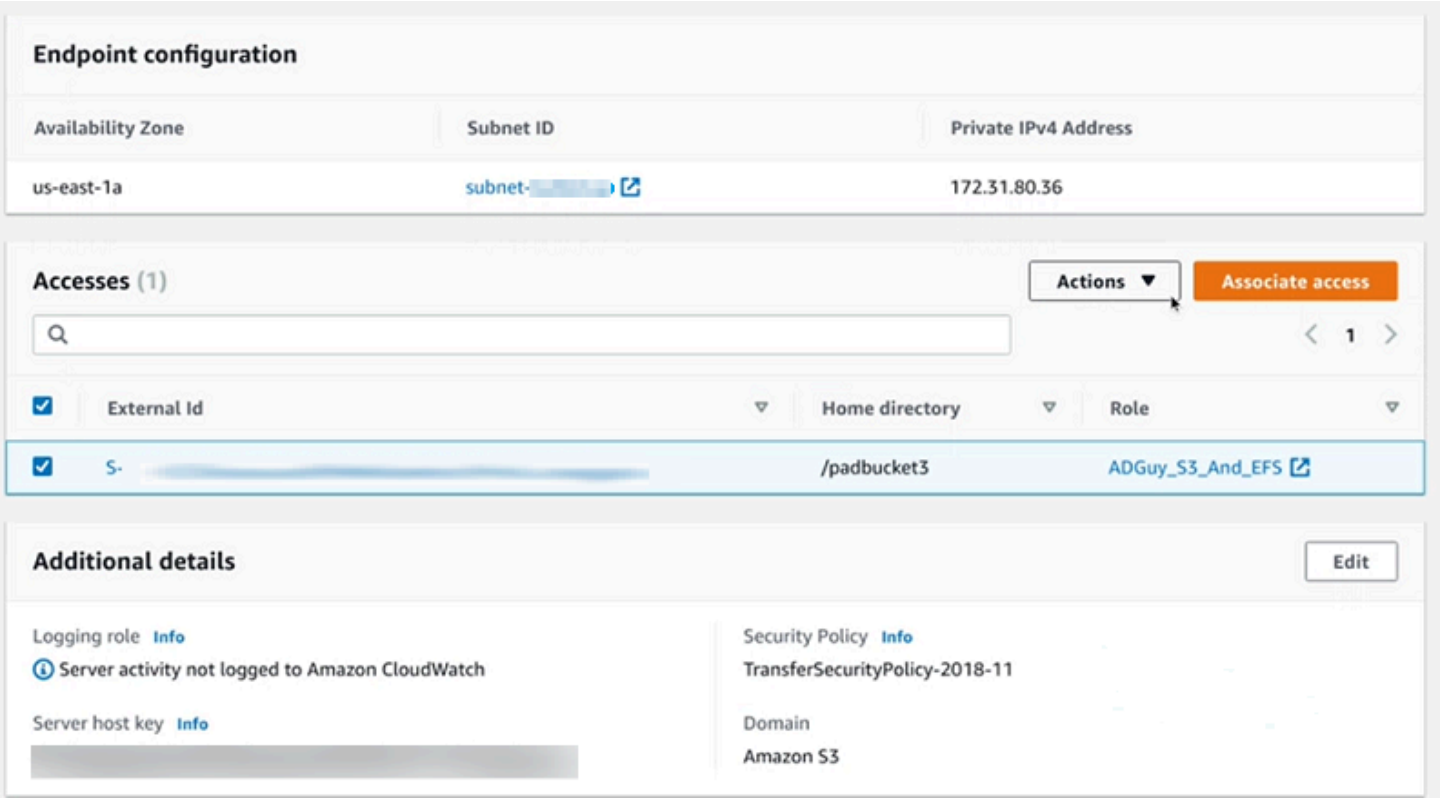
> **Note**
>
> 您可以透過建立工作階段政策來限制使用者看到的值區部分。例如，若要將使用者限制在/filetest目錄下自己的資料夾，請在方塊中輸入下列文字。
>
> ```
> /filetest/${transfer:UserName}
> ```
>
> 若要進一步瞭解如何建立工作階段原則，請參閱為 Amazon S3 儲存貯體建立工作階段政策。

8. 選擇「新增」以建立關聯。
9. 選擇您的伺服器。
10. 選擇新增存取權限。
    - 輸入群組的 SID。

    > **Note**
    >
    > 如需有關如何尋找 SID 的資訊，請參閱the section called “開始使用之前 AWS Directory Service for Microsoft Active Directory”。

11. 選擇新增存取權限。

在「存取」區段中，會列出伺服器的存取權。



測試使用者

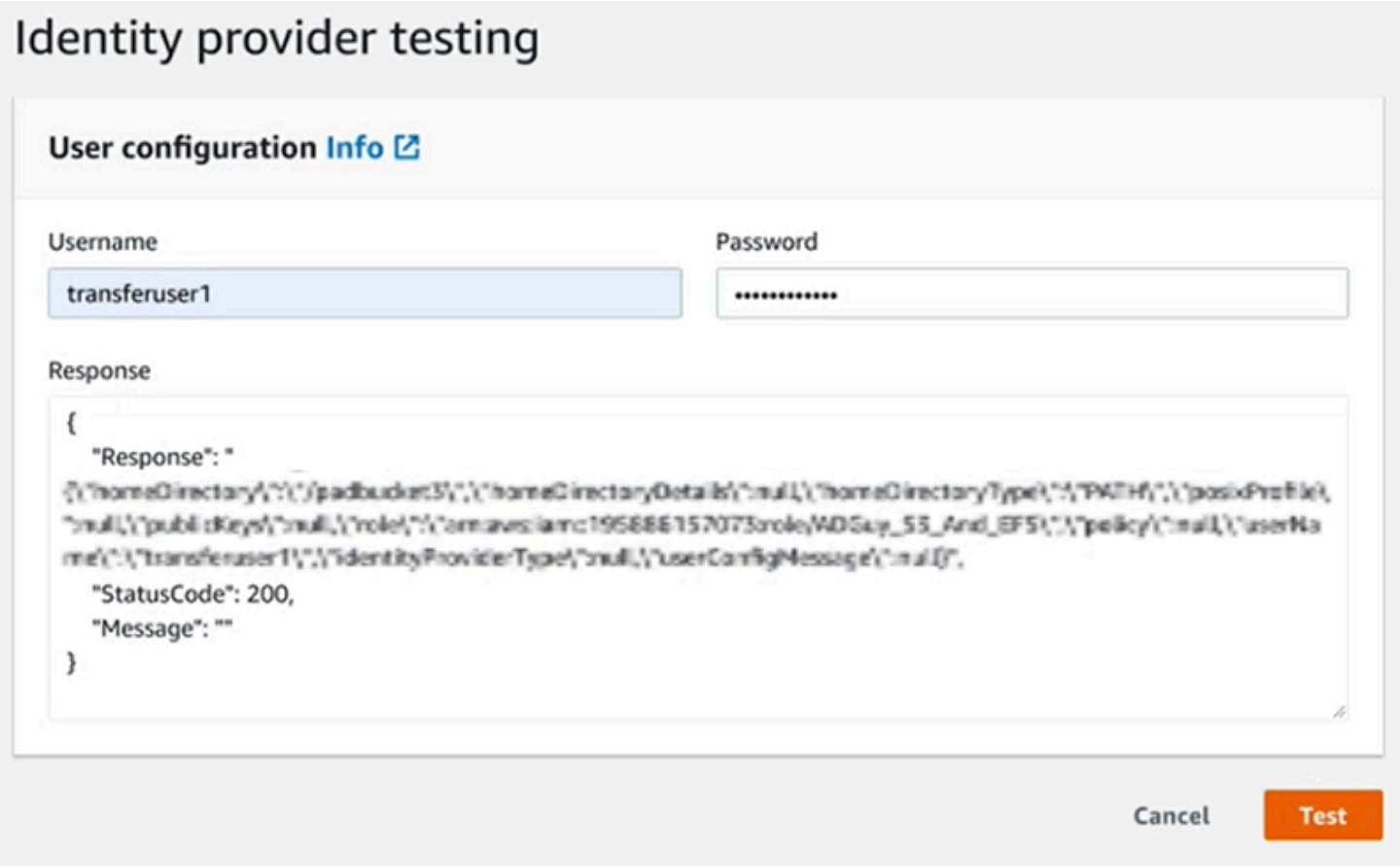
您可以測試使用者是否具有伺服器 AWS Managed Microsoft AD 目錄的存取權。

> **Note**
>
> 使用者必須位於 [端點設定] 頁面 [存取] 區段中所列的一個群組 (外部 ID) 中。如果使用者不在任何群組中，或位於多個群組中，則不會授與該使用者存取權。

測試特定使用者是否具有存取權

1. 在伺服器詳細資訊頁面上，選擇 [動作]，然後選擇 [測試]。
2. 對於身分識別提供者測試，請輸入其中一個具有存取權限之群組中之使用者的登入認證。
3. 選擇 測試。

您會看到成功的身分識別提供者測試，顯示選取的使用者已被授與伺服器的存取權。



如果使用者屬於多個具有存取權的群組，您會收到下列回應。

```
"Response":"",
"StatusCode":200,
"Message":"More than one associated access found for user's groups."
```

刪除群組的伺服器存取權

若要刪除群組的伺服器存取權

1. 在伺服器詳細資訊頁面上，選擇 [動作]，然後選擇 [刪除存取權]。
2. 在對話方塊中，確認您要移除此群組的存取權。

當您返回伺服器詳細資訊頁面時，您會看到此群組的存取權不再列出。

使用 SSH（安全殼層）連接到服務器

設定伺服器和使用者之後，您可以使用 SSH 連線到伺服器，並針對具有存取權的使用者使用完整的使用者名稱。

```
sftp user@active-directory-domain@vpc-endpoint
```

例如：transferuserexample@mycompany.com@vpce-0123456abcdef-789xyz.vpc-svc-987654zyxabc.us-east-1.vpce.amazonaws.com。

此格式會以同盟的搜尋為目標，限制搜尋可能較大的 Active Directory。

> **Note**
>
> 您可以指定簡單的使用者名稱。但是，在這種情況下，活動目錄代碼必須搜索聯合中的所有目錄。這可能會限制搜尋，而且即使使用者應具有存取權，驗證也可能會失敗。

驗證後，使用者會位於您設定使用者時指定的主目錄中。

使用樹系和信任連線 AWS Transfer Family 至自我管理的 Active Directory

您自我管理的 Active Directory (AD) 中的使用者也可以使 AWS IAM Identity Center 用單一登入存取 AWS 帳戶 和 Transfer Family 伺服器。要做到這一點， AWS Directory Service 有以下可用選項：

- 單向樹系信任 (內部部署 Active Directory 的傳出來源 AWS Managed Microsoft AD 和內送) 僅適用於根網域。
- 對於子網域，您可以使用下列任一項目：
  - 使用內部部署活動目錄 AWS Managed Microsoft AD 之間的雙向信任
  - 對每個子網域使用單向外部信任。

使用受信任的網域連線到伺服器時，使用者需要指定受信任的網域，例如transferuserexample@*mycompany.com*。

使用 Azure 作用中 AWS 目錄網域服務的 Directory Service

- 若要利用您現有的作用中目錄樹系來滿足您的 SFTP 傳輸需求，您可以使用作用中目錄連接器。
- 如果您想要在完全受管理的服務中享有 Active Directory 和高可用性的好處，您可以使用 AWS Directory Service for Microsoft Active Directory. 如需詳細資訊，請參閱 使用 AWS Directory Service 身分識別提供者。

本主題說明如何使用作用中目錄連接器和 Azure 作用中目錄網域服務 (Azure ADDS) 來驗證 SFTP 傳輸使用者與 Azure 作用中目錄。

主題

- 在您開始使用 Azure 作用中 AWS 目錄網域服務的 Directory Service 之前
- 第 1 步：添加 Azure 活動目錄域服務
- 步驟 2：建立服務帳戶
- 步驟 3：使用 AD Connector 設定 AWS 目錄
- 步驟 4：設定 AWS Transfer Family 伺服器
- 步驟 5：授予群組存取權
- 步驟 6：測試使用者

在您開始使用 Azure 作用中 AWS 目錄網域服務的 Directory Service 之前

對於 AWS，您需要以下內容：

- 您使用 Transfer Family 伺服器的 AWS 地區中的虛擬私有雲 (VPC)
- VPC 中至少有兩個私有子網路
- VPC 必須具有互聯網連接
- 客戶閘道和虛擬私有閘道，可與 Microsoft Azure 進行 site-to-site VPN 連線

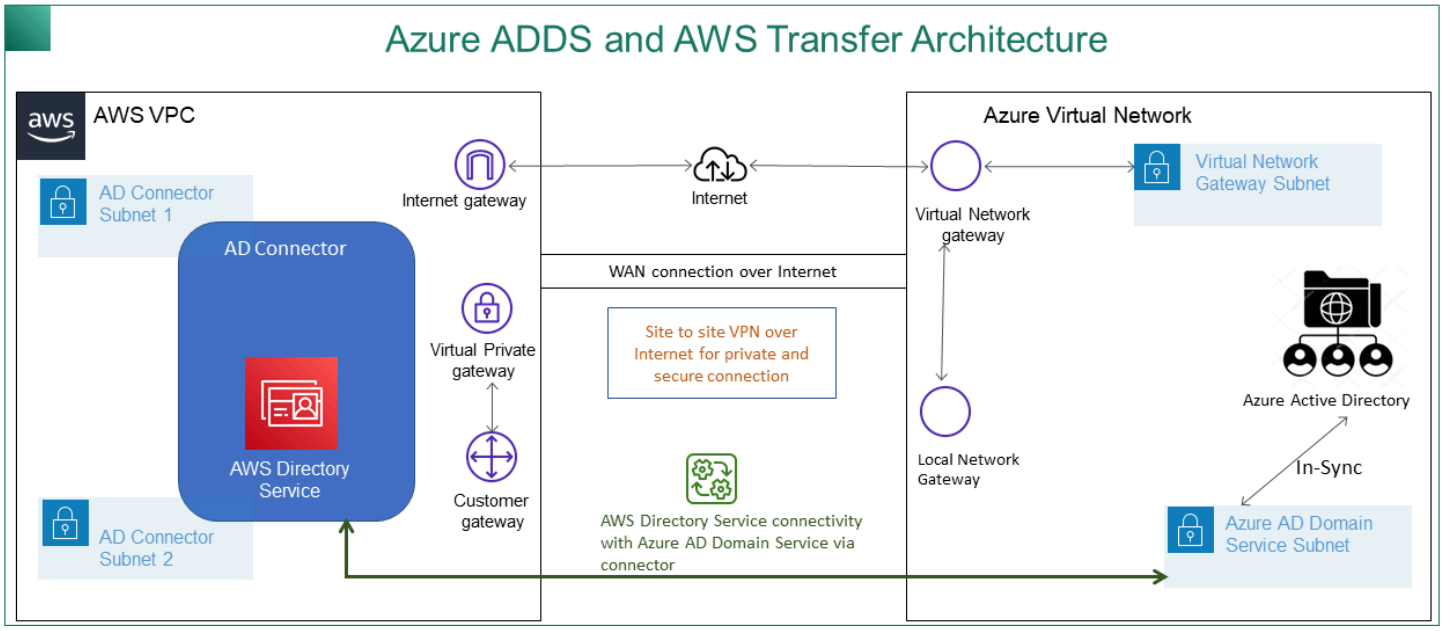
對於 Microsoft Azure，您需要以下內容：

- Azure 活動目錄和活動目錄域服務（Azure 添加）
- 一個 Azure 資源群組
- 一個 Azure 虛擬網路
- 您的 Amazon 虛擬私人雲端和 Azure 資源群組之間的 VPN 連線

> **Note**
>
> 這可以透過原生 IPSEC 通道或使用 VPN 設備進行。在本主題中，我們使用 Azure 虛擬網路閘道和本機網路閘道之間的 IPSEC 通道。通道必須設定為允許 Azure ADDS 端點與容納 AWS VPC 之子網路之間的流量。

- 客戶閘道和虛擬私有閘道，可與 Microsoft Azure 進行 site-to-site VPN 連線

下圖顯示開始之前所需的組態。

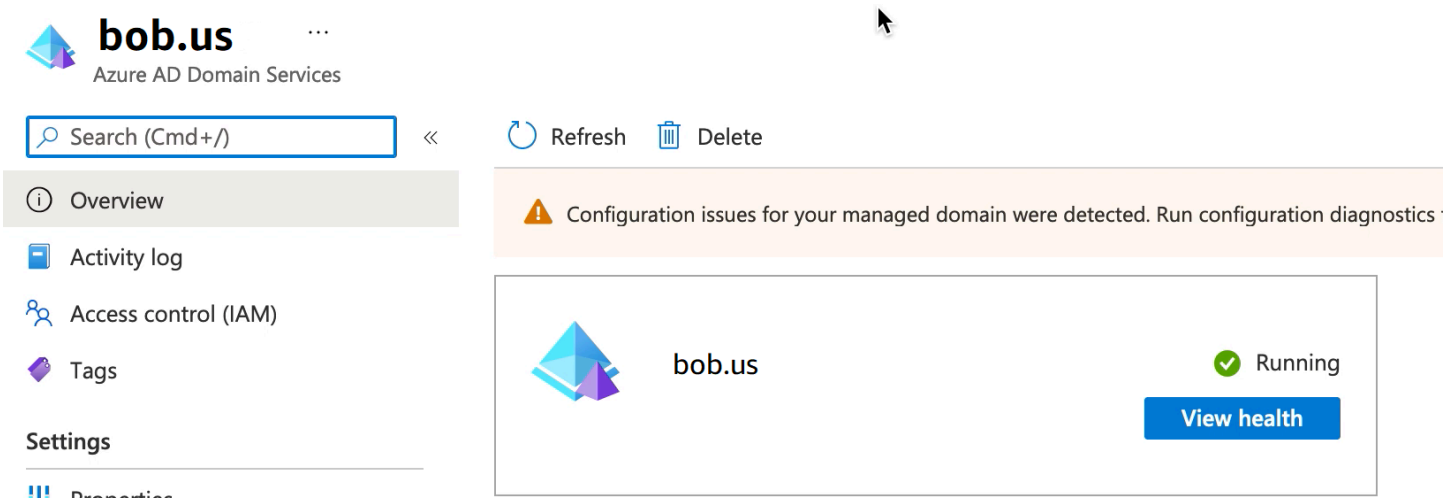


第 1 步：添加 Azure 活動目錄域服務

Azure AD 預設不支援網域加入執行個體。若要執行網域加入之類的動作，並使用群組原則等工具，系統管理員必須啟用 Azure 作用中的目錄網域服務。如果您尚未新增 Azure AD DS，或您現有的實作與您希望 SFTP 傳輸伺服器使用的網域沒有關聯，則必須新增執行個體。

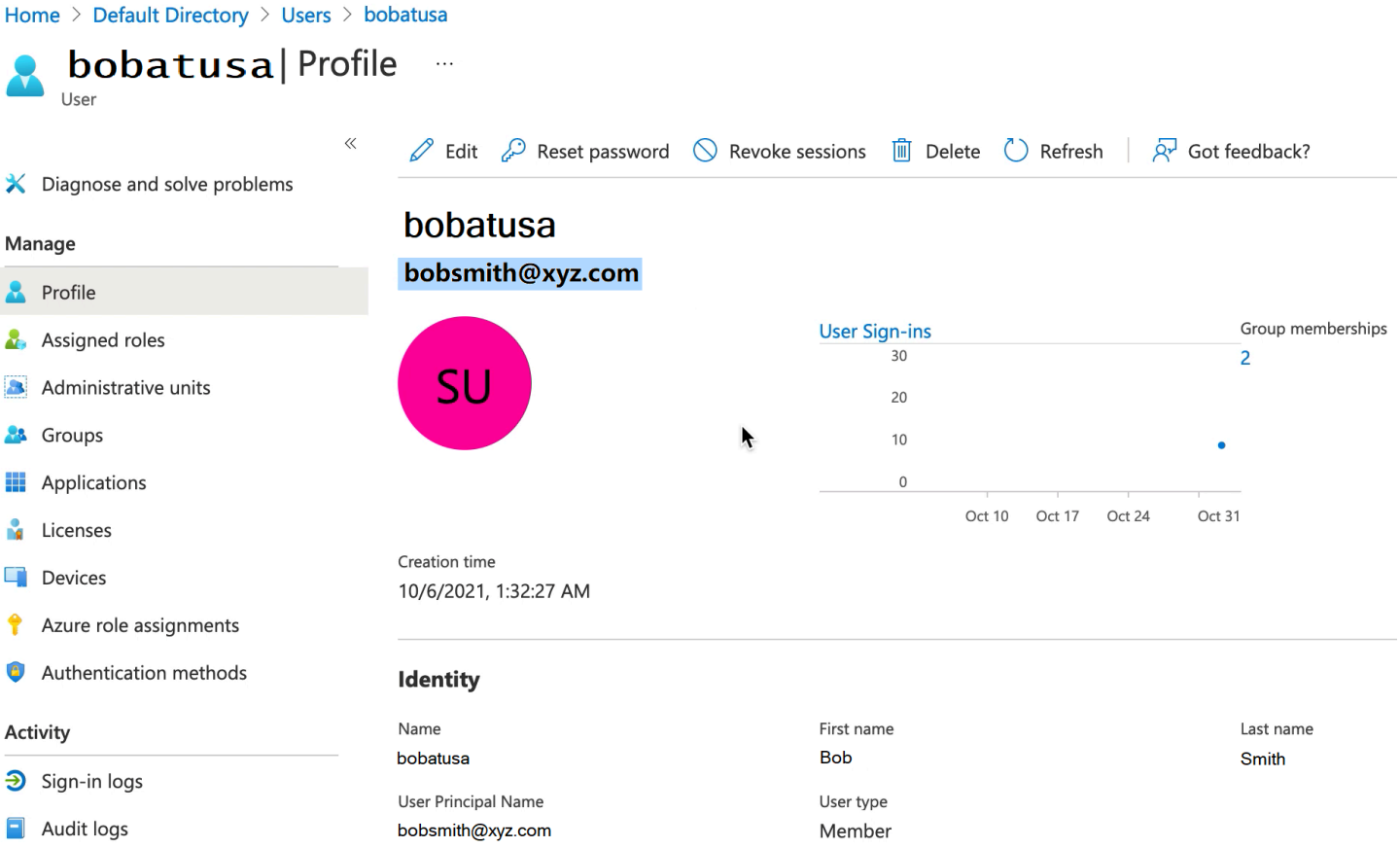
如需啟用 Azure 作用中目錄網域服務 (Azure ADDS) 的相關資訊，請參閱教學課程：建立及設定 Azure 作用中目錄網域服務受管理的網域。

> **Note**
>
> 當您啟用 Azure ADDS 時，請確定已針對您要連線 SFTP 傳輸伺服器的資源群組和 Azure AD 網域進行設定。



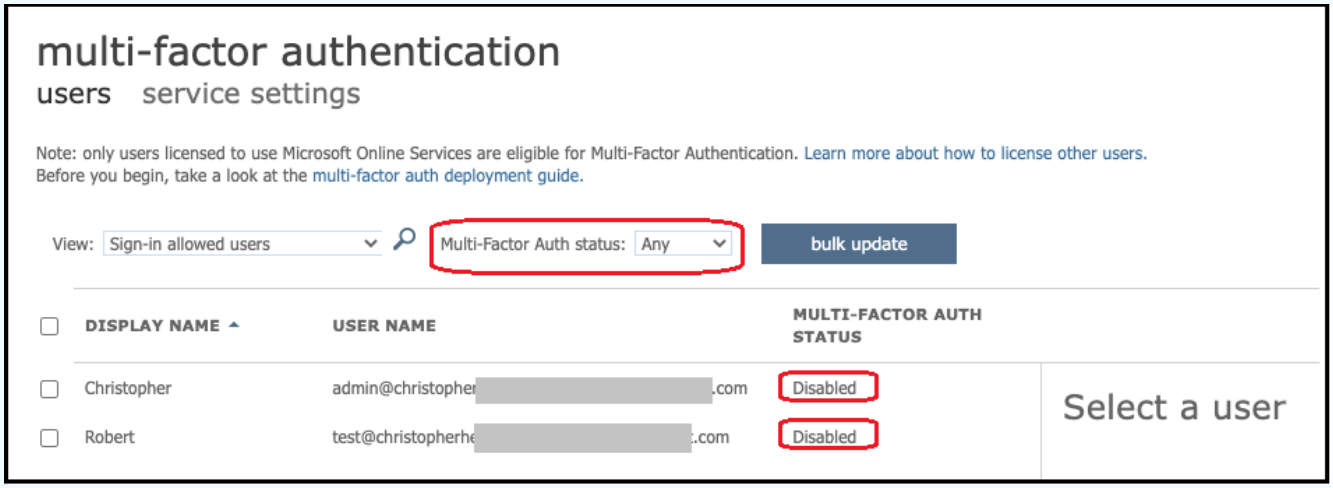
步驟 2：建立服務帳戶

Azure AD 必須有一個屬於 Azure 新增中系統管理員群組的一部分的服務帳戶。此帳戶與作用 AWS 中目錄連接器搭配使用。請確定此帳戶與 Azure 新增項目同步。



Tip

使用 SFTP 通訊協定的 Transfer Family 伺服器不支援 Azure 作用中目錄的多重要素驗證。使用者對 SFTP 進行驗證之後，Transfer Family 伺服器無法提供 MFA 權杖。在嘗試連線之前，請務必停用 MFA。



步驟 3：使用 AD Connector 設定 AWS 目錄

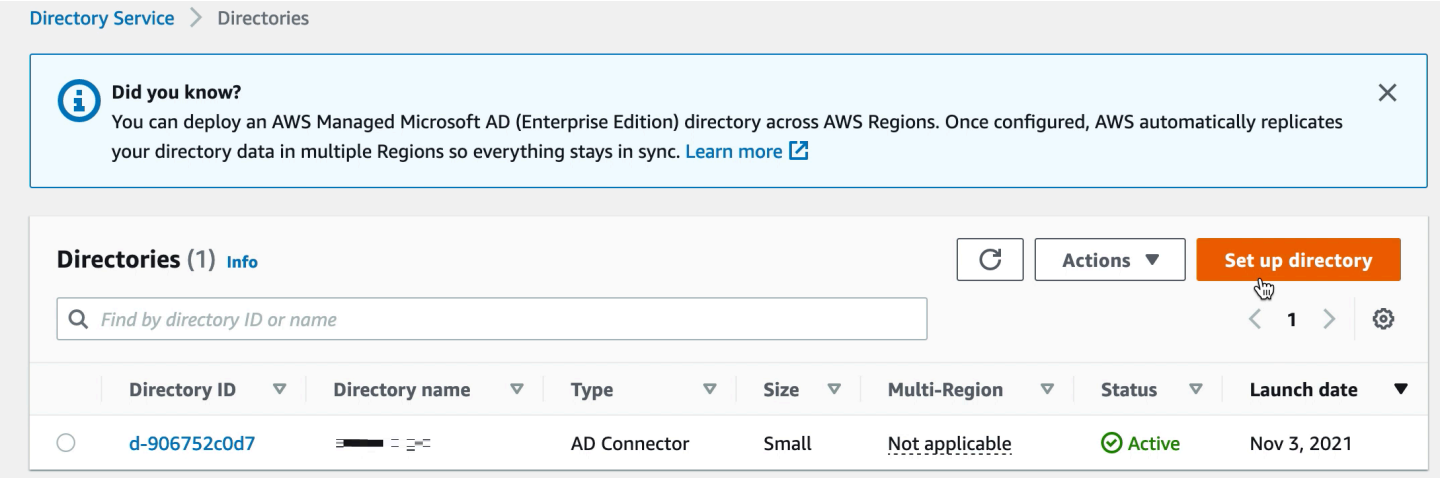
在您設定 Azure ADDS，並使用虛擬私人 AWS VPC 端和 Azure 虛擬網路之間的 IPSEC VPN 通道建立服務帳戶之後，您可以從任何 AWS EC2 執行個體偵測 Azure 新增 DNS IP 位址來測試連線。

確認連線處於作用中狀態後，您可以繼續以下步驟。

使用 AD Connector 設定 AWS 目錄

1. 開啟「Directory Service」主控台並選取「目錄」。
2. 選取 [設定目錄]。
3. 針對目錄類型，請選擇 AD Connector。
4. 選取目錄大小，選取下一步，然後選取您的 VPC 和子網路。
5. 選取「下一步」，然後依下列方式填入欄位：
   - 目錄 DNS 名稱：輸入您用於 Azure 添加的域名。
   - DNS IP 地址：輸入您的天藍添加的 IP 地址。
   - 伺服器帳戶使用者名稱和密碼：輸入您在步驟 2：建立服務帳戶中建立的服務帳戶的詳細資料。
6. 完成畫面以建立目錄服務。

現在目錄狀態應該是「作用中」，並且可以與 SFTP 傳輸伺服器搭配使用。



步驟 4：設定 AWS Transfer Family 伺服器

使用 SFTP 通訊協定和 Directory Service 的身分識別提供者類型建立 Transfer Family 列AWS 伺服器。從目錄下拉式清單中，選取您在步驟 3：使用 AD Connector 設定 AWS 目錄中新增的目錄。

> **Note**
>
> 如果您在 Transfer Family 列伺服器中使用了 Microsoft AD AWS 目錄，則無法刪除 Directory Service 中的 Microsoft AD 目錄。您必須先刪除伺服器，然後才能刪除目錄。

步驟 5：授予群組存取權

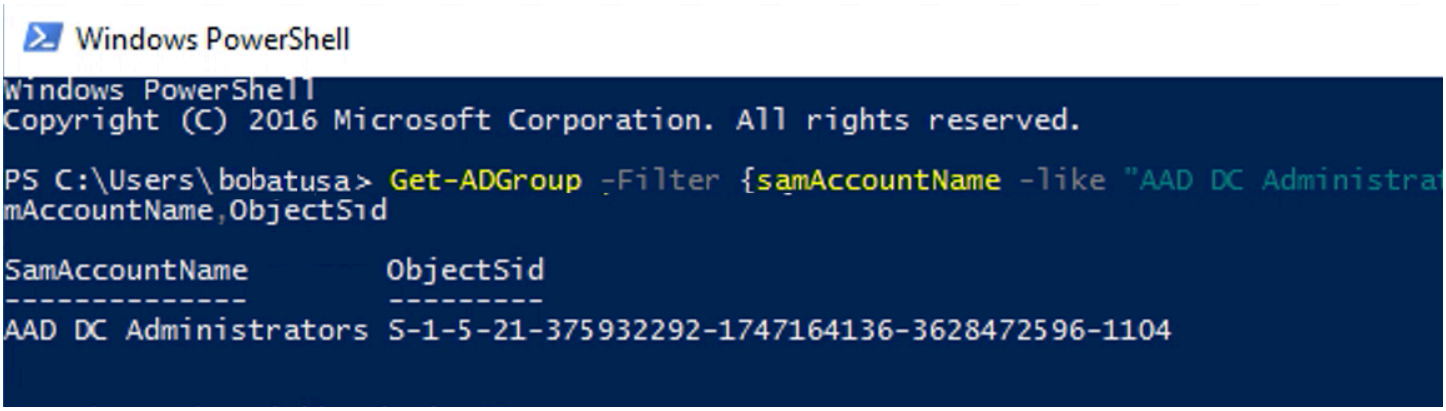
建立伺服器之後，您必須選擇目錄中的哪些群組應該有權透過已啟用的通訊協定上傳和下載檔案 AWS Transfer Family。您可以透過建立存取權來執行此操作。

> **Note**
>
> 使用者必須直接屬於您要授與存取權的群組。例如，假設 Bob 是一個用戶，他屬於 GroupA，並且 GroupA 本身包含在 GroupB 中。
>
> - 如果您授與 GroupA 的存取權，Bob 就會被授與存取權。
> - 如果您授予 GroupB 的存取權 (而不是 GroupA)，Bob 將無法存取。

若要授與存取權，您需要擷取群組的 SID。

使用下列 Windows PowerShell 命令擷取群組的 SID，並以群組*YourGroupName*的名稱取代。

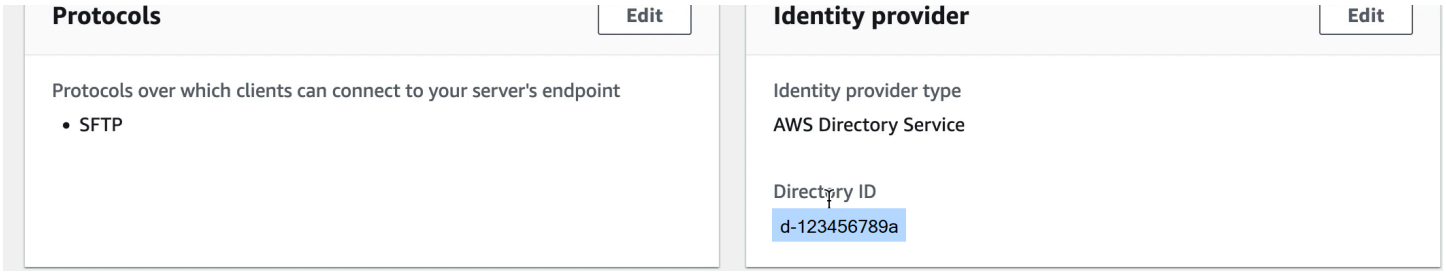
```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties * | Select
 SamAccountName,ObjectSid
```

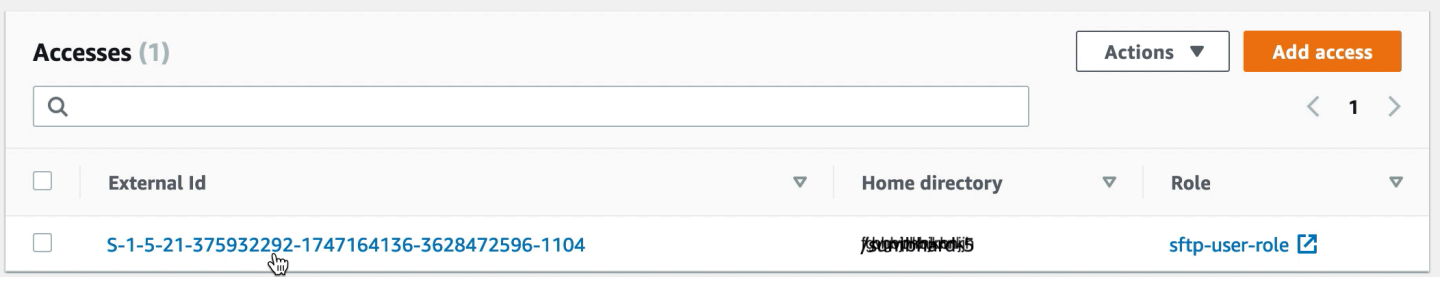


授予群組存取權

1. 打開以下位置。https://console.aws.amazon.com/transfer/
2. 導覽至伺服器詳細資訊頁面，然後在「存取」區段中選擇「新增存取權」。
3. 輸入您從上一個程序的輸出接收到的 SID。
4. 對於 [存取]，請選擇群組的 AWS Identity and Access Management 角色。
5. 在「策略」區段中，選擇策略。預設值為 None (無)。
6. 對於主目錄，請選擇與群組主目錄對應的 S3 儲存貯體。
7. 選擇「新增」以建立關聯。

傳輸伺服器的詳細資料看起來應該類似下列內容：





步驟 6：測試使用者

您可以 test (測試使用者) 使用者是否有權存取您伺服器的 AWS Managed Microsoft AD 目錄。使用者必須位於 [端點設定] 頁面 [存取] 區段中所列的一個群組 (外部 ID) 中。如果使用者不在任何群組中，或位於多個群組中，則不會授與該使用者存取權。

使用自訂身分識別提供者

若要驗證您的使用者，您可以使用現有的身分識別提供者 AWS Transfer Family。您可以使用功能整合身分供應商，該 AWS Lambda 功能會驗證並授權您的使用者存取 Amazon S3 或 Amazon Elastic File System (Amazon EFS)。如需詳細資訊，請參閱 用 AWS Lambda 於整合您的身分識別提供者。您也可以存取指標的 CloudWatch 圖形，例如在「 AWS Transfer Family 管理主控台」中傳輸的檔案數目和位元組數，讓您透過單一窗格來監控檔案傳輸，使用集中式儀表板來監控檔案傳輸。

或者，您可以使用單一 Amazon API Gateway 方法提供 RESTful 界面。Transfer Family 會呼叫此方法來連接到您的身分供應商，該供應商會對您的使用者進行身分驗證並授權存取 Amazon S3 或 Amazon EFS。如果您需要 RESTful API 來整合身分識別提供者，或者想要使用其功能來進行地理封鎖或速率限制 AWS WAF 要求，請使用此選項。如需詳細資訊，請參閱 使用 Amazon API Gateway 整合您的身分供應商。

在任何一種情況下，您都可以使用AWS Transfer Family 控制台或 CreateServerAPI 操作創建新服務器。

> **Note**
>
> Transfer Family 提供部落格文章和研討會，引導您逐步建立檔案傳輸解決方案。此解決方案利 AWS Transfer Family 用受管 SFTP/FTPS 端點和 Amazon Cognito 和 DynamoDB 進行使用者管理。
> 部落格文章可在使用 Amazon Cognito 做為身分供應商 AWS Transfer Family 和 Amazon S3 中取得。您可以在此處查看工作坊的詳細信息。

AWS Transfer Family 提供下列選項以使用自訂身分識別提供者。

- 用於連 AWS Lambda 接您的身分提供者 — 您可以使用由 Lambda 函數支援的現有身分識別提供者。您提供 Lambda 函數的名稱。如需詳細資訊，請參閱 用 AWS Lambda 於整合您的身分識別提供者。
- 使用 Amazon API Gateway 連接您的身分供應商 — 您可以建立由 Lambda 函數支援的 API Gateway 方法，用作身分識別供應商。您提供 Amazon API Gateway 網址和叫用角色。如需詳細資訊，請參閱 使用 Amazon API Gateway 整合您的身分供應商。

對於任一選項，您也可以指定如何進行驗證。

- 密碼或金鑰 — 使用者可以使用其密碼或金鑰進行驗證。這是預設值。
- 僅限密碼 — 使用者必須提供密碼才能連線。
- 僅限金鑰 — 使用者必須提供私密金鑰才能連線。
- 密碼與金鑰 — 使用者必須同時提供私密金鑰和密碼才能連線。伺服器會先檢查金鑰，然後如果金鑰有效，系統會提示輸入密碼。如果提供的私密金鑰與儲存的公開金鑰不符，驗證會失敗。

使用多種驗證方法向您的自訂身分提供者進行驗證

當您使用多種驗證方法時，Transfer Family 伺服器會控制 AND 邏輯。Transfer Family 會將此視為向您的自訂身分提供者提出的兩個個別要求：不過，這些要求的效果是合

這兩個請求必須以正確的響應成功返回，以便完成身份驗證。Transfer Family 需要完成兩個回應，這表示它們包含所有必要的元素 (如果您使用 Amazon EFS 進行儲存，則角色、主目錄、政策和 POSIX 設定檔)。Transfer Family 還要求密碼響應不能包含公鑰。

公開金鑰要求必須具有與身分識別提供者不同的回應。使用「密碼」或「金鑰」或「密碼與金鑰」時，該行為不會變更。

SSH/SFTP 通訊協定會先使用公開金鑰驗證來挑戰軟體用戶端，然後要求密碼驗證。在允許使用者完成驗證之前，此作業會要求兩者都成功。

主題

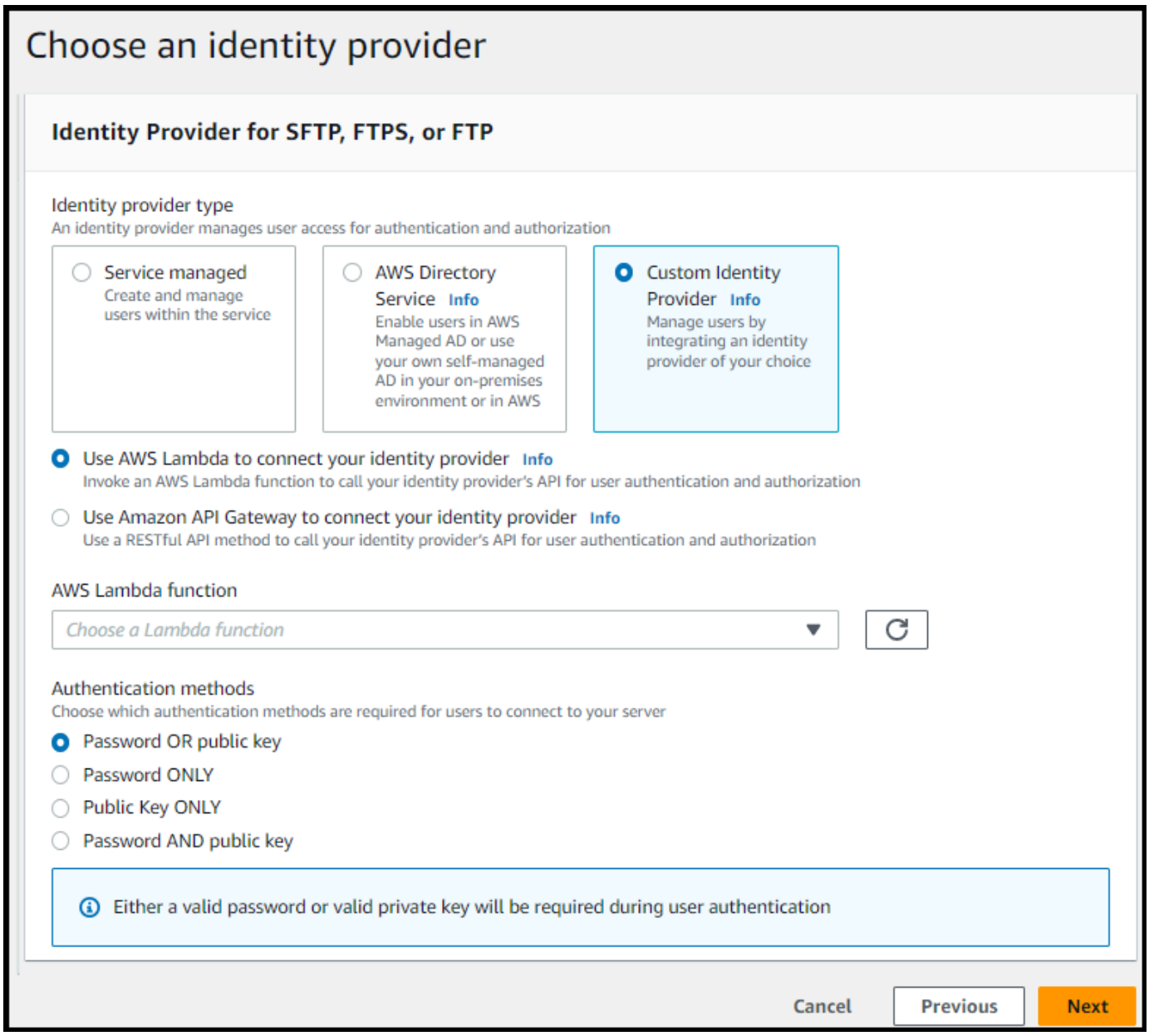
- 用 AWS Lambda 於整合您的身分識別提供者
- 使用 Amazon API Gateway 整合您的身分供應商

用 AWS Lambda 於整合您的身分識別提供者

建立連線至您的自訂身分識別提供者的 AWS Lambda 函數。您可以使用任何自訂身分識別提供者，例如 Okta、Secrets Manager 或包含授權和驗證邏輯的自訂資料存放區。 OneLogin

> **Note**
>
> 建立使用 Lambda 做為身分識別提供者的 Transfer Family 伺服器之前，您必須先建立函數。如需 Lambda 函數的範例，請參閱範例 Lambda 函數。或者，您可以部署使用Lambda 函數模板. CloudFormation 此外，請確保您的 Lambda 函數使用信任 Transfer Family 的資源型政策。如需政策範例，請參閱 以 Lambda 源為基礎的政策。

1. 開啟 AWS Transfer Family 主控台。
2. 選擇建立伺服器以開啟 [建立伺服器] 頁面。對於 [選擇身分識別提供者]，選擇 [自訂識別提供者]，如下列螢幕擷取畫面所示



> **Note**
>
> 只有當您啟用 SFTP 作為 Transfer Family 伺服器的其中一個通訊協定時，才能選擇驗證方法。

3. 確定已選取預設值「用 AWS Lambda 來連線您的身分識別提供者」。
4. 對於AWS Lambda 函數，請選擇 Lambda 函數的名稱。
5. 填入其餘的方塊，然後選擇 [建立伺服器]。如需建立伺服器的剩餘步驟的詳細資訊，請參閱設定 SFTP、FTPS 或 FTP 伺服器端點。

以 Lambda 源為基礎的政策

您必須擁有參考 Transfer Family 伺服器和 Lambda ARN 的政策。例如，您可以將下列政策與連線至身分提供者的 Lambda 函數搭配使用。原則會以字串形式逸出 JSON。

```
"Policy":
"{
  "Version": "2012-10-17",
  "Id": "default",
  "Statement": [
    {
      "Sid": "AllowTransferInvocation",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "lambda:InvokeFunction",
      "Resource": "arn:aws:transfer:region:account-id:function:my-lambda-auth-
function",
      "Condition": {
        "ArnLike": {
          "AWS:SourceArn": "arn:aws:transfer:region:account-id:server/server-id"
        }
      }
    }
  ]
}"
```

> **Note**
>
> 在上面的示例策略中，用您自己的信息替換每個*#######*。

事件訊息結構

針對自訂 IDP，傳送至授權者 Lambda 函數的 SFTP 伺服器的事件訊息結構如下。

```
{
    "username": "value",
    "password": "value",
    "protocol": "SFTP",
    "serverId": "s-abcd123456",
```

```
    "sourceIp": "192.168.0.100"
}
```

傳送至伺服器之登入認證的值在何處`username`和`password`值。

例如，您可以輸入下列指令來連線：

```
sftp bobusa@server_hostname
```

然後系統會提示您輸入密碼：

```
Enter password:
    mysecretpassword
```

您可以從 Lambda 函數中列印傳遞的事件，從 Lambda 函數進行檢查。它看起來應該類似於下面的文本塊。

```
{
    "username": "bobusa",
    "password": "mysecretpassword",
    "protocol": "SFTP",
    "serverId": "s-abcd123456",
    "sourceIp": "192.168.0.100"
}
```

FTP 和 FTPS 的事件結構類似：唯一的區別是這些值用於`protocol`參數，而不是 SFTP。

用於驗證的 Lambda 函

若要實作不同的驗證策略，請編輯 Lambda 函數。為了協助您滿足應用程式的需求，您可以部署 CloudFormation 堆疊。如需有關 Lambda 的詳細資訊，請參閱AWS Lambda 開發人員指南或使用 Node.js 建置 Lambda 函數。

主題

- Lambda 函數模板
- 有效的 Lambda 值
- 範例 Lambda 函數
- 測試您的配置

Lambda 函數模板

您可以部署使用 Lambda 函數進行驗證的 AWS CloudFormation 堆疊。我們提供數個範本，可使用登入認證來驗證和授權您的使用者。您可以修改這些範本或 AWS Lambda 程式碼，進一步自訂使用者存取權限。

> **Note**
>
> 您可以通過在模板中指定啟用 FIPS 的安全策略 AWS CloudFormation 來創建啟用 FIPS 的 AWS Transfer Family 服務器。可用的安全策略說明，請參閱 AWS Transfer Family 伺服器的安全性原則

若要建立用於驗證的 AWS CloudFormation 堆疊

1. 開啟主 AWS CloudFormation 控台，網址為 https://console.aws.amazon.com/cloudformation。
2. 請遵循《使用指南》中的「選取 AWS CloudFormation 堆疊範本」中，從現有範本部署堆疊的AWS CloudFormation 指示。
3. 使用下列其中一個範本建立 Lambda 函數，以便在 Transfer Family 中用於驗證。

   - 經典（Amazon Cognito）堆棧模板

     用於在中建立用作自訂身分識別提供者的基本範本 AWS Transfer Family。 AWS Lambda 如果使用以公開金鑰為基礎的身份驗證，則會對 Amazon Cognito 進行驗證，並從 Amazon S3 儲存貯體傳回公開金鑰。部署之後，您可以修改 Lambda 函數程式碼來執行不同的動作。

   - AWS Secrets Manager 堆疊範本

     與 AWS Transfer Family 伺服器 AWS Lambda 搭配使用的基本範本，可將 Secrets Manager 整合為身分識別提供者。它會針對格式 AWS Secrets Manager 的項目進行驗證。`aws/transfer/`*`server-id`*`/`*`username`*此外，密碼必須保留傳回至「Transfer Family」之所有使用者性質的鍵值對。部署之後，您可以修改 Lambda 函數程式碼來執行不同的動作。

   - Okta 堆疊範本：與 AWS Transfer Family 伺服器 AWS Lambda 搭配使用，將 Okta 整合為自訂身分識別提供者的基本範本。
   - Okta-MFA 堆疊範本：與 AWS Transfer Family 伺服器 AWS Lambda 搭配使用的基本範本，將 Okta 與 MultiFactor 驗證整合為自訂身分識別提供者。
   - Azure 作用中目錄範本：此堆疊的詳細資料會在部落格文章中描述AWS Transfer Family 使用 Azure 作用中目錄進行驗證，以及 AWS Lambda.

部署堆疊之後，您可以在 CloudFormation 主控台的 [輸出] 索引標籤上檢視堆疊的詳細資料。

部署其中一個堆疊是將自訂身分識別提供者整合至「Transfer Family」工作流程的最簡單方法。

有效的 Lambda 值

下表說明 Transfer Family 接受用於自訂身分識別提供者之 Lambda 函數之值的詳細資料。

Value	描述	必要
`Role`	指定 IAM 角色的亞馬遜資源名稱 (ARN)，該角色可控制使用者對 Amazon S3 儲存貯體或 Amazon EFS 檔案系統的存取權。附加到此角色的政策決定了在將檔案傳入和傳出 Amazon S3 或 Amazon EFS 檔案系統時，您希望為使用者提供的存取層級。IAM 角色也應包含信任關係，允許伺服器在處理您使用者的傳輸請求時，存取您的資源。 如需建立信任關係的詳細資訊，請參閱建立信任關係。	必要
`PosixProfile`	完整的 POSIX 身分，包括使用者 ID (`Uid`)、群組 ID (`Gid`) 和任何次要群組 ID (`SecondaryGids`)，可控制使用者對 Amazon EFS 檔案系統的存取。對檔案系統中的檔案和目錄設定的 POSIX 許可，會決定使用者在 Amazon EFS 檔案系統中傳入和傳出檔案時所取得的存取等級。	Amazon EFS 支援儲存空間所需

Value	描述	必要
PublicKeys	對此使用者有效的 SSH 公開金鑰值清單。空白清單表示這不是有效的登入。密碼驗證期間不得返回。	選用
Policy	適用於您的使用者的工作階段政策，讓您可以跨多個使用者使用相同的 IAM 角色。此政策會將使用者存取的範圍縮小到他們 Amazon S3 儲存貯體的部分。	選用
HomeDirectoryType	使用者登入伺服器時，您希望的使用者主目錄之登陸目錄 (資料夾) 類型。 • 如果將其設定為PATH，使用者會在其檔案傳輸協定用戶端中看到絕對的 Amazon S3 儲存貯體或 Amazon EFS 路徑。 • 如果將其設定為LOGICAL，則必須在HomeDirectoryDetails 參數中提供對應，讓使用者可以看到 Amazon S3 或 Amazon EFS 路徑。	選用

Value	描述	必要
HomeDirectoryDetails	邏輯目錄對應，可指定您的使用者可以看見哪些 Amazon S3 或 Amazon EFS 路徑和金鑰，以及您希望如何顯示這些路徑和金鑰。您必須指定Entry和Target配對，其中Entry顯示路徑的顯示方式，以及Target實際的 Amazon S3 或 Amazon EFS 路徑。	如果值HomeDirectoryType 為，則需要LOGICAL
HomeDirectory	使用者使用用戶端登入伺服器時的登陸目錄。	選用

> **Note**
>
> HomeDirectoryDetails是 JSON 對應的字串表示。這是相反的PosixProfile，這是一個實際的 JSON 映射對象，PublicKeys它是一個 JSON 字符串數組。如需特定語言的詳細資訊，請參閱程式碼範例。

範例 Lambda 函數

本節介紹了一些示例 Lambda 函數，在這兩個 NodeJS 和 Python。

> **Note**
>
> 在這些範例中，使用者、角色、POSIX 設定檔、密碼和主目錄詳細資料都是範例，必須以實際值取代。

Logical home directory, NodeJS

下列 NodeJS 範例函數提供具有邏輯主目錄之使用者的詳細資訊。

```
// GetUserConfig Lambda
```

```
exports.handler = (event, context, callback) => {
  console.log("Username:", event.username, "ServerId: ", event.serverId);

  var response;
  // Check if the username presented for authentication is correct. This doesn't
 check the value of the server ID, only that it is provided.
  if (event.serverId !== "" && event.username == 'example-user') {
    var homeDirectoryDetails = [
      {
        Entry: "/",
        Target: "/fs-faa1a123"
      }
    ];
    response = {
      Role: 'arn:aws:iam::123456789012:role/transfer-access-role', // The user is
 authenticated if and only if the Role field is not blank
      PosixProfile: {"Gid": 65534, "Uid": 65534}, // Required for EFS access, but
 not needed for S3
      HomeDirectoryDetails: JSON.stringify(homeDirectoryDetails),
      HomeDirectoryType: "LOGICAL",
    };

    // Check if password is provided
    if (!event.password) {
      // If no password provided, return the user's SSH public key
      response['PublicKeys'] = [ "ssh-
rsa abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789" ];
    // Check if password is correct
    } else if (event.password !== 'Password1234') {
      // Return HTTP status 200 but with no role in the response to indicate
 authentication failure
      response = {};
    }
  } else {
    // Return HTTP status 200 but with no role in the response to indicate
 authentication failure
    response = {};
  }
  callback(null, response);
};
```

Path-based home directory, NodeJS

下列 NodeJS 範例函式會提供具有路徑主目錄之使用者的詳細資訊。

```
// GetUserConfig Lambda

exports.handler = (event, context, callback) => {
  console.log("Username:", event.username, "ServerId: ", event.serverId);

  var response;
  // Check if the username presented for authentication is correct. This doesn't
 check the value of the server ID, only that it is provided.
  // There is also event.protocol (one of "FTP", "FTPS", "SFTP") and event.sourceIp
 (e.g., "127.0.0.1") to further restrict logins.
  if (event.serverId !== "" && event.username == 'example-user') {
    response = {
      Role: 'arn:aws:iam::123456789012:role/transfer-access-role', // The user is
 authenticated if and only if the Role field is not blank
      Policy: '', // Optional, JSON stringified blob to further restrict this user's
 permissions
      HomeDirectory: '/fs-faa1a123' // Not required, defaults to '/'
    };

    // Check if password is provided
    if (!event.password) {
      // If no password provided, return the user's SSH public key
     response['PublicKeys'] = [ "ssh-
rsa abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789" ];
    // Check if password is correct
    } else if (event.password !== 'Password1234') {
      // Return HTTP status 200 but with no role in the response to indicate
 authentication failure
      response = {};
    }
  } else {
    // Return HTTP status 200 but with no role in the response to indicate
 authentication failure
    response = {};
  }
  callback(null, response);
};
```

Logical home directory, Python

下列 Python 範例函數提供具有邏輯主目錄之使用者的詳細資訊。

```
# GetUserConfig Python Lambda with LOGICAL HomeDirectoryDetails
```

```
import json

def lambda_handler(event, context):
  print("Username: {}, ServerId: {}".format(event['username'], event['serverId']))

  response = {}

  # Check if the username presented for authentication is correct. This doesn't
 check the value of the server ID, only that it is provided.
  if event['serverId'] != '' and event['username'] == 'example-user':
    homeDirectoryDetails = [
      {
        'Entry': '/',
        'Target': '/fs-faa1a123'
      }
    ]
    response = {
      'Role': 'arn:aws:iam::123456789012:role/transfer-access-role', # The user will
 be authenticated if and only if the Role field is not blank
      'PosixProfile': {"Gid": 65534, "Uid": 65534}, # Required for EFS access, but
 not needed for S3
      'HomeDirectoryDetails': json.dumps(homeDirectoryDetails),
      'HomeDirectoryType': "LOGICAL"
    }

    # Check if password is provided
    if event.get('password', '') == '':
      # If no password provided, return the user's SSH public key
     response['PublicKeys'] = [ "ssh-
rsa abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789" ]
    # Check if password is correct
    elif event['password'] != 'Password1234':
      # Return HTTP status 200 but with no role in the response to indicate
 authentication failure
      response = {}
  else:
    # Return HTTP status 200 but with no role in the response to indicate
 authentication failure
    response = {}

  return response
```

Path-based home directory, Python

下列 Python 範例函式會提供具有以路徑為基礎之主目錄之使用者的詳細資訊。

```
# GetUserConfig Python Lambda with PATH HomeDirectory

def lambda_handler(event, context):
  print("Username: {}, ServerId: {}".format(event['username'], event['serverId']))

  response = {}

  # Check if the username presented for authentication is correct. This doesn't
 check the value of the server ID, only that it is provided.
  # There is also event.protocol (one of "FTP", "FTPS", "SFTP") and event.sourceIp
 (e.g., "127.0.0.1") to further restrict logins.
  if event['serverId'] != '' and event['username'] == 'example-user':
    response = {
      'Role': 'arn:aws:iam::123456789012:role/transfer-access-role', # The user will
 be authenticated if and only if the Role field is not blank
      'Policy': '', #  Optional, JSON stringified blob to further restrict this
 user's permissions
      'HomeDirectory': '/fs-fs-faa1a123',
      'HomeDirectoryType': "PATH" # Not strictly required, defaults to PATH
    }

    # Check if password is provided
    if event.get('password', '') == '':
      # If no password provided, return the user's SSH public key
     response['PublicKeys'] = [ "ssh-
rsa abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789" ]
    # Check if password is correct
    elif event['password'] != 'Password1234':
      # Return HTTP status 200 but with no role in the response to indicate
 authentication failure
      response = {}
  else:
    # Return HTTP status 200 but with no role in the response to indicate
 authentication failure
    response = {}

  return response
```

測試您的配置

建立自訂身分識別提供者之後，您應該測試您的組態。

Console

使用 AWS Transfer Family 控制台測試您的配置

1. 開啟 AWS Transfer Family 主控台。
2. 在 [伺服器] 頁面上，選擇新伺服器，選擇 [動作]，然後選擇 [測試]。
3. 輸入部署 AWS CloudFormation 堆疊時設定的「使用者名稱」和「密碼」文字。如果您保留預設選項，則使用者名稱為`myuser`，密碼為`MySuperSecretPassword`。
4. 如果您在部署 AWS CloudFormation 堆疊時設定來源 IP，請選擇伺服器通訊協定並輸入 IP 位址。

CLI

使用 AWS CLI 測試您的組態

1. 運行測試身份提供者命令。以您自己*`user input placeholder`*的資訊取代每個資訊，如後續步驟所述。

```
aws transfer test-identity-provider --server-id s-1234abcd5678efgh --user-
name myuser --user-password MySuperSecretPassword --server-protocol FTP --
source-ip 127.0.0.1
```

2. 輸入伺服器 ID。
3. 輸入您在部署 AWS CloudFormation 堆疊時設定的使用者名稱和密碼。如果您保留預設選項，則使用者名稱為`myuser`，密碼為`MySuperSecretPassword`。
4. 如果您在部署 AWS CloudFormation 堆疊時進行設定，請輸入伺服器通訊協定和來源 IP 位址。

如果使用者驗證成功，則測試會傳回 `StatusCode: 200` HTTP 回應、空字串 `Message: ""` (否則會包含失敗原因) 和`Response`欄位。

> **Note**
>
> 在下面的響應示例中，該字Response段是一個 JSON 對象，該對象已被「字符串化」（轉換為可以在程序中使用的平面 JSON 字符串），並包含用戶的角色和權限的詳細信息。

```
{
    "Response":"{\"Policy\":\"{\\\"Version\\\":\\\"2012-10-17\\\",\\\"Statement\\\":
[{\\\"Sid\\\":\\\"ReadAndListAllBuckets\\\",\\\"Effect\\\":\\\"Allow\\\",\\\"Action\\
\":[\\\"s3:ListAllMybuckets\\\",\\\"s3:GetBucketLocation\\\",\\\"s3:ListBucket\\\",\\
\"s3:GetObjectVersion\\\",\\\"s3:GetObjectVersion\\\"],\\\"Resource\\\":\\\"*\\\"}]}\",
\"Role\":\"arn:aws:iam::000000000000:role/MyUserS3AccessRole\",\"HomeDirectory\":\"/
\"}",
    "StatusCode": 200,
    "Message": ""
}
```

使用 Amazon API Gateway 整合您的身分供應商

本主題說明如何使用 AWS Lambda 函數來支援 API Gateway 方法。如果您需要 RESTful API 來整合身分識別提供者，或者想要使用其功能來進行地理封鎖或速率限制 AWS WAF 要求，請使用此選項。

使用 API Gateway 整合身分提供者的限制

- 此設定不支援自訂網域。
- 此設定不支援私有 API Gateway URL。

如果您需要其中一種，您可以在沒有 API Gateway 的情況下使用 Lambda 做為身分識別提供者。如需詳細資訊，請參閱 用 AWS Lambda 於整合您的身分識別提供者。

使用 API Gateway 方法進行驗證

您可以建立 API Gateway 方法，用作「Transfer Family」的身分識別提供者。這種方法為您提供了一種高度安全的方式來創建和提供 API。使用 API Gateway，您可以建立 HTTPS 端點，以便以更高的安全性傳輸所有內送 API 呼叫。如需 API Gateway 服務的詳細資訊，請參閱 API Gateway 開發人員指南。

API Gateway 提供了一種名為的授權方法`AWS_IAM`，該方法可為您提供與內部 AWS 使用的 AWS Identity and Access Management （IAM）相同的身份驗證。如果您使用啟用驗證`AWS_IAM`，則只有具有呼叫 API 明確權限的呼叫者才能連線到該 API 的 API Gateway 方法。

若要使用您的 API Gateway 方法做為 Transfer Family 的自訂身分提供者，請為您的 API Gateway 方法啟用 IAM。在此過程中，您提供具有許可的 IAM 角色，以便 Transfer Family 使用您的閘道。

> **Note**
>
> 若要提高安全性，您可以設定 Web 應用程式防火牆。 AWS WAF 這是一種網頁應用程式防火牆，可讓您監控轉寄至 Amazon API Gateway 的 HTTP 和 HTTPS 請求。如需詳細資訊，請參閱 新增 Web 應用程式防火牆。

使用您的 API Gateway 方法透過 Transfer Family 進行自訂驗證

1. 建立 AWS CloudFormation 堆疊。若要執行此作業：

   > **Note**
   >
   > 堆疊範本已更新為使用 Base64 編碼密碼：如需詳細資訊，請參閱。AWS CloudFormation 模板的改進

   a. 開啟主 AWS CloudFormation 控台，網址為 https://console.aws.amazon.com/cloudformation。

   b. 請遵循《使用指南》中的 「選取 AWS CloudFormation 堆疊範本」中，從現有範本部署堆疊的AWS CloudFormation 指示。

   c. 使用下列其中一個基本範本建立 AWS Lambda支援的 API Gateway 方法，以在 Transfer Family 中做為自訂身分識別提供者使用。

      - 基本堆疊範本

        根據預設，您的 API Gateway 方法會用作自訂身分識別提供者，以使用硬式編碼的 SSH (安全殼層) 金鑰或密碼來驗證單一伺服器中的單一使用者。部署之後，您可以修改 Lambda 函數程式碼來執行不同的動作。

      - AWS Secrets Manager 堆疊範本

        根據預設，您的 API Gateway 方法會針對該格式的 Secrets Manager 中的項目進行驗證。`aws/transfer/`*`server-id`*`/`*`username`*此外，密碼必須保留傳回至「Transfer Family」之所有使用者性質的鍵值對。部署之後，您可以修改 Lambda 函數程式碼來執行

不同的動作。如需詳細資訊，請參閱部落格文章啟用密碼驗證以便 AWS Transfer Family 使用 AWS Secrets Manager。

- 奧克塔堆疊範本

  您的 API Gateway 方法與 Okta 整合，做為 Transfer Family 中的自訂身分提供者。如需詳細資訊，請參閱使用 Okta 做為身分識別提供者的部落格文章。 AWS Transfer Family

部署其中一個堆疊是將自訂身分識別提供者整合至「Transfer Family」工作流程的最簡單方法。每個堆疊都會使用 Lambda 函數，根據 API Gateway 來支援您的 API 方法。然後，您可以在「Transfer Family」中使用 API 方法做為自訂身分提供者。根據預設，Lambda 函數會驗證使用的密碼呼叫`myuser`的單一使用者。`MySuperSecretPassword`部署之後，您可以編輯這些認證或更新 Lambda 函數程式碼以執行不同動作。

> **Important**
>
> 建議您編輯預設的使用者和密碼認證。

部署堆疊之後，您可以在 CloudFormation 主控台的 [輸出] 索引標籤上檢視堆疊的詳細資料。這些詳細資料包括堆疊的 Amazon 資源名稱 (ARN)、堆疊建立的 IAM 角色的 ARN，以及新閘道的 URL。

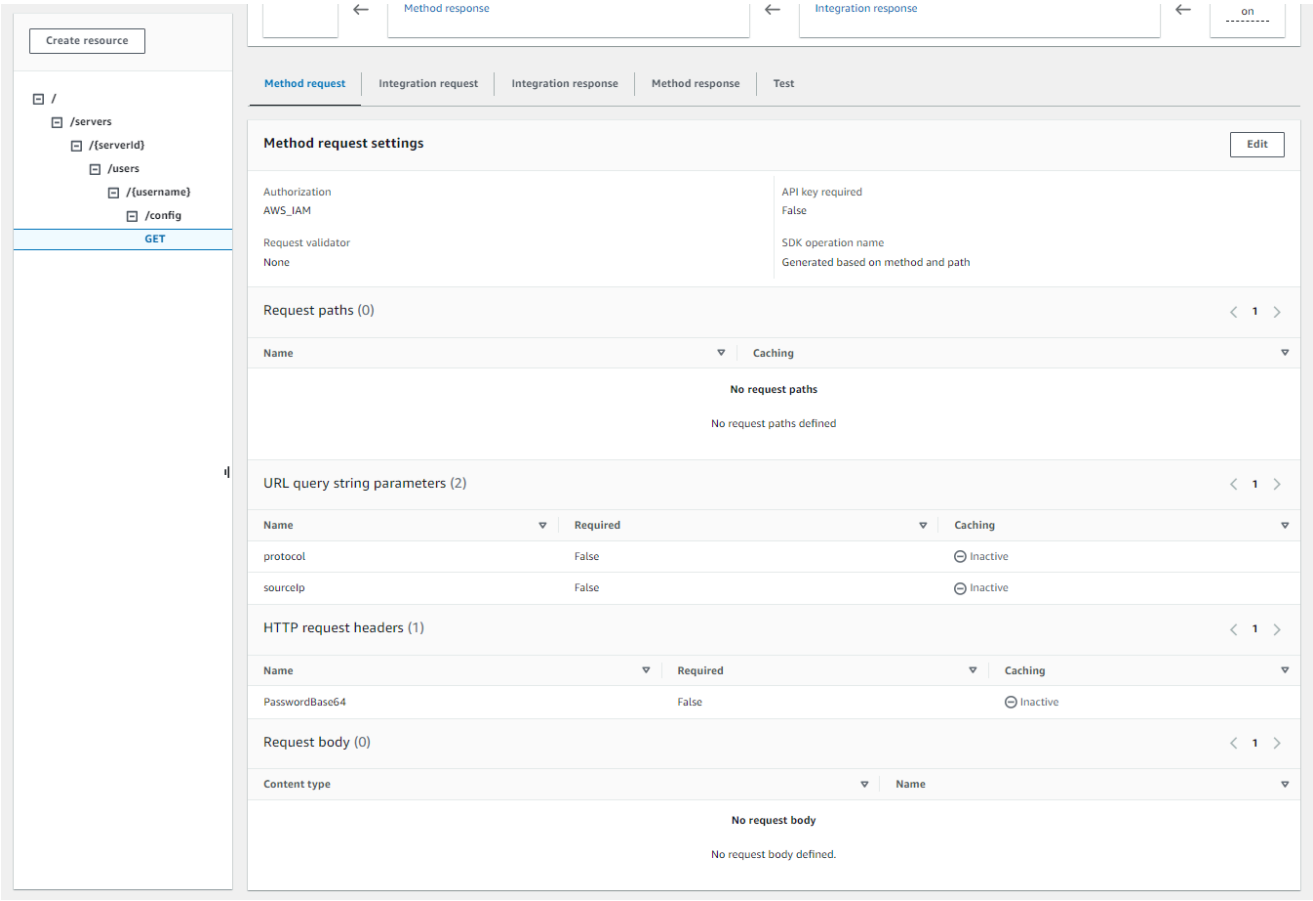
> **Note**
>
> 如果您使用自訂身分識別提供者選項為使用者啟用密碼式身份驗證，並且啟用 API Gateway 提供的請求和回應記錄，則 API Gateway 會將使用者的密碼記錄到 Amazon 日誌中。 CloudWatch 我們不建議您在生產環境中使用此日誌。如需詳細資訊，請參閱 CloudWatch API Gateway 開發人員指南中的「在 API Gateway 中設定 API 記錄」。

2. 檢查伺服器的 API Gateway 方法設定。若要執行此作業：

   a. 在以下網址開啟 API Gateway 主控台：https://console.aws.amazon.com/apigateway/。

   b. 選擇範本產生的「移轉自訂身分識別提供者」基本 AWS CloudFormation 範本 API。您可能需要選取您的區域才能查看閘道。

   c. 在 [資源] 窗格中，選擇 [GET]。下列螢幕擷取畫面顯示正確的方法設定。

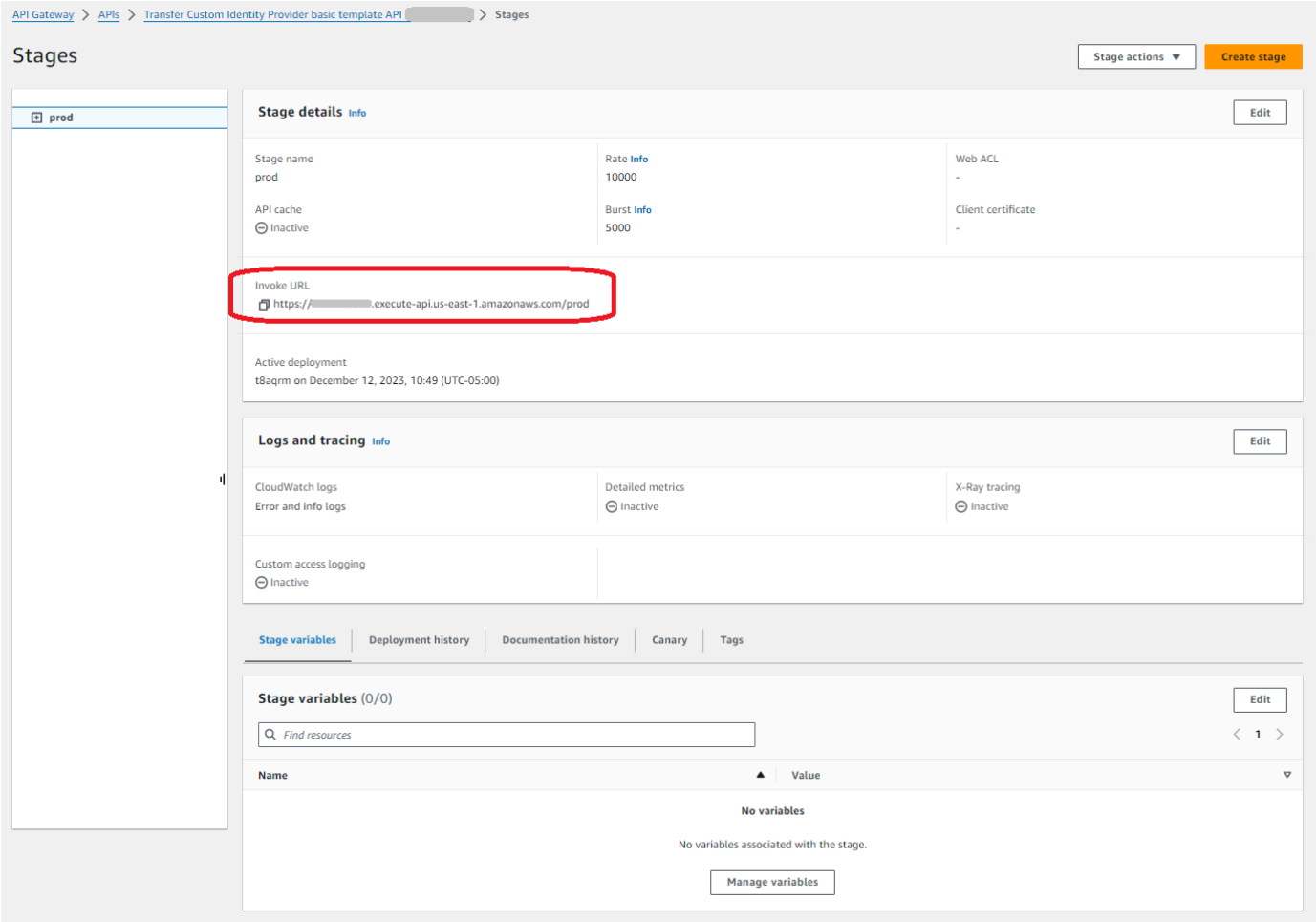


此時，您的 API 閘道已準備就緒，可供部署。

3. 針對「動作」，選擇「部署 API」。針對「部署」階段，選擇 prod，然後選擇「部署」。

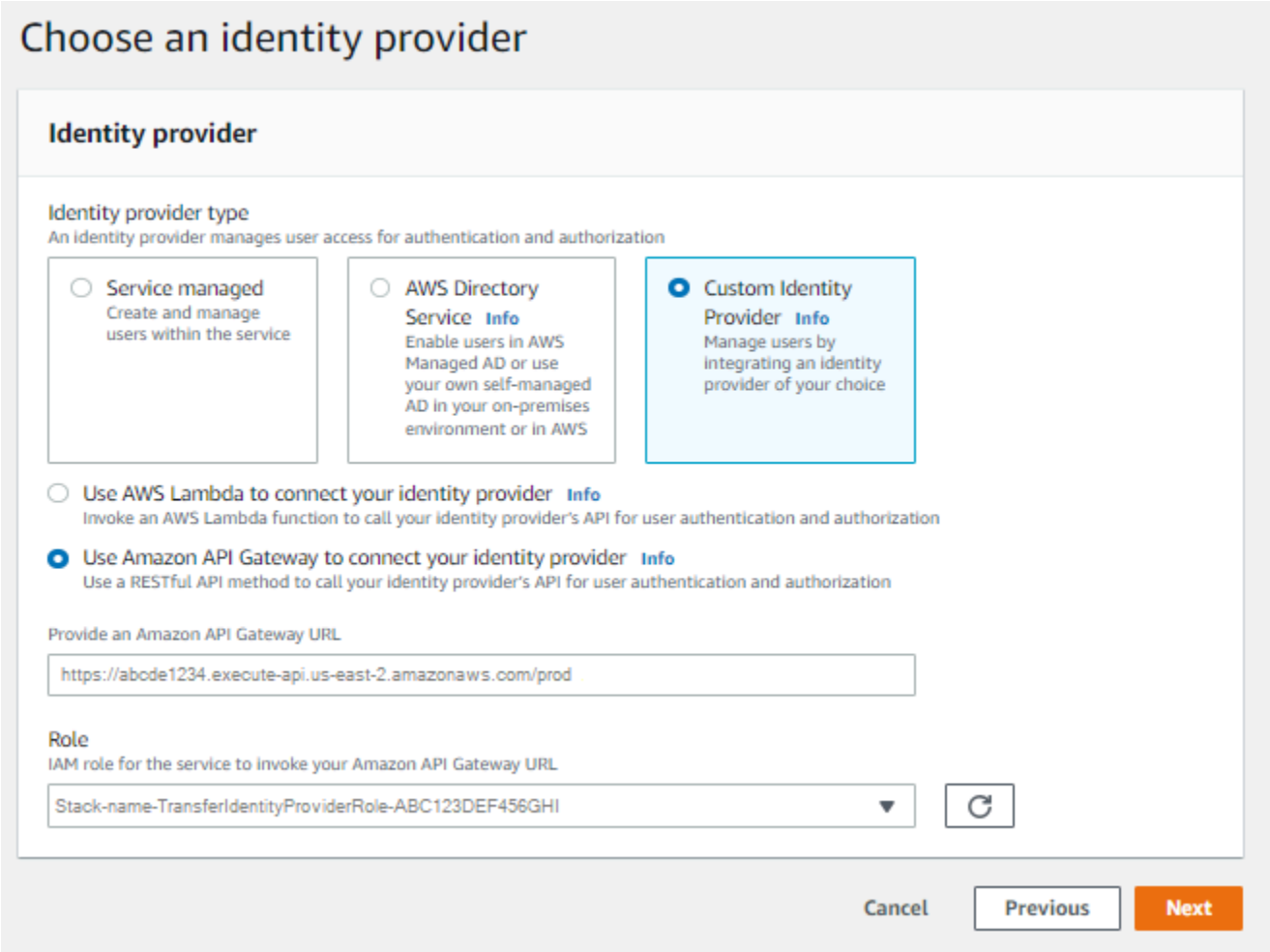
成功部署 API Gateway 方法之後，請在「階段」>「階段」詳細資料中檢視其效能，如下列螢幕擷取畫面所示。

> **Note**
>
> 複製顯示在畫面頂端的呼叫 URL 位址。您可能需要它來進行下一步。



4. 開啟主 AWS Transfer Family 控台，網址為 https://console.aws.amazon.com/transfer/。
5. 當您建立堆疊時，應該已為您建立 Transfer Family。如果沒有，請使用以下步驟設定您的伺服器。

   a. 選擇建立伺服器以開啟 [建立伺服器] 頁面。對於 [選擇身分提供者]，選擇 [自訂]，然後選取 [使用 Amazon API Gateway 連線到您的身分提供者]，如下列螢幕擷取畫面所示。



b. 在提供 Amazon API Gateway URL 文字方塊中，貼上您在此程序步驟 3 中建立之 API Gateway 端點的叫用 URL 位址。

c. 針對角色，選擇 AWS CloudFormation 範本建立的 IAM 角色。此角色允許 Transfer Family 叫用您的 API 閘道方法。

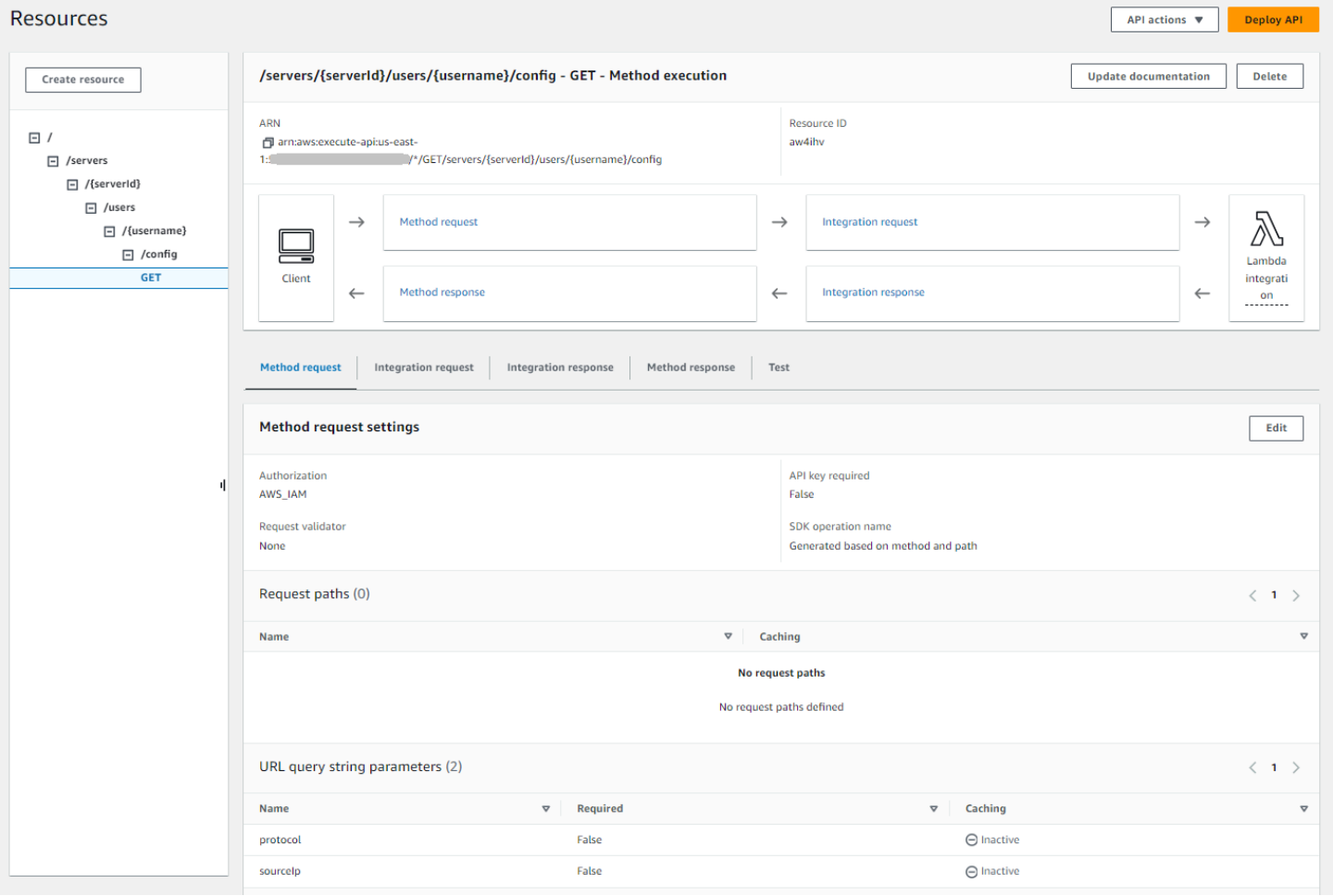
   呼叫角色包含您在步驟 1 中建立的堆疊選取的堆疊名稱。 AWS CloudFormation 它具有以下格式：*CloudFormation-stack-name*-TransferIdentityProviderRole-*ABC123DEF456GHI*。

d. 填入其餘的方塊，然後選擇 [建立伺服器]。如需建立伺服器的剩餘步驟的詳細資訊，請參閱[設定 SFTP、FTPS 或 FTP 伺服器端點]。

實作您的 API Gateway 方法

若要為 Transfer Family 建立自訂身分識別提供者，您的 API Gateway 方法必須實作資源路徑為的單一方法/servers/*serverId*/users/*username*/config。*serverId*和*username*值來自 REST 風

格的資源路徑。此外，在方法要求中新增sourceIp和protocol做為 URL 查詢字串參數，如下圖所示。



> **Note**
>
> 使用者名稱必須至少為 3 個字元，最多 100 個字元。您可以在使用者名稱中使用下列字元：a—z、A-Z、0—9、底線 (_)、連字號 (-)、句號 (.) 和 at 符號 (@)。不過，使用者名稱不能以連字號 (-)、句點 (.) 或 @符號開頭。

如果「Transfer Family」嘗試為您的使用者進行密碼驗證，則服務會提供Password:標頭欄位。如果沒有Password:標頭，Transfer Family 會嘗試使用公開金鑰驗證來驗證您的使用者。

當您使用身分識別提供者來驗證和授權使用者時，除了驗證其認證之外，您還可以根據使用者所使用的用戶端 IP 位址來允許或拒絕存取要求。您可以使用此功能來確保存放在 S3 儲存貯體或 Amazon EFS 檔案系統中的資料只能透過受支援的協定存取，只能從您指定為受信任的 IP 地址存取。若要啟用此功能，您必須sourceIp在查詢字串中加入。

如果您為伺服器啟用了多個通訊協定，並且想要透過多個通訊協定使用相同的使用者名稱提供存取權，只要您的身分識別提供者中設定了每個通訊協定特定的認證，就可以這麼做。若要啟用此功能，您必須在 RESTful 資源路徑中包含該*protocol*值。

您的 API Gateway 方法應始終返回 HTTP 狀態碼200。任何其他 HTTP 狀態碼表示存取 API 時發生錯誤。

Amazon S3 範例回應

範例回應本文是 Amazon S3 的下列格式的 JSON 文件。

```
{
 "Role": "IAM role with configured S3 permissions",
 "PublicKeys": [
     "ssh-rsa public-key1",
     "ssh-rsa public-key2"
  ],
 "Policy": "STS Assume role session policy",
 "HomeDirectory": "/bucketName/path/to/home/directory"
}
```

Note

原則會以字串形式逸出 JSON。例如：

```
"Policy":
"{
  \"Version\": \"2012-10-17\",
  \"Statement\":
     [
     {\"Condition\":
        {\"StringLike\":
            {\"s3:prefix\":
               [\"user/*\", \"user/\"]}},
     \"Resource\": \"arn:aws:s3:::bucket\",
     \"Action\": \"s3:ListBucket\",
     \"Effect\": \"Allow\",
     \"Sid\": \"ListHomeDir\"},
     {\"Resource\": \"arn:aws:s3:::*\",
        \"Action\": [\"s3:PutObject\",
        \"s3:GetObject\",
        \"s3:DeleteObjectVersion\",
```

```
        \"s3:DeleteObject\",
        \"s3:GetObjectVersion\",
        \"s3:GetObjectACL\",
        \"s3:PutObjectACL\"],
     \"Effect\": \"Allow\",
     \"Sid\": \"HomeDirObjectAccess\"}]
}"
```

下列範例回應顯示使用者具有邏輯主目錄類型。

```
{
   "Role": "arn:aws:iam::123456789012:role/transfer-access-role-s3",
   "HomeDirectoryType":"LOGICAL",
   "HomeDirectoryDetails":"[{\"Entry\":\"/\",\"Target\":\"/MY-HOME-BUCKET\"}]",
   "PublicKeys":[""]
}
```

Amazon EFS 範例回應

範例回應本文是適用於 Amazon EFS 的下列格式的 JSON 文件。

```
{
 "Role": "IAM role with configured EFS permissions",
 "PublicKeys": [
     "ssh-rsa public-key1",
     "ssh-rsa public-key2"
  ],
 "PosixProfile": {
   "Uid": "POSIX user ID",
   "Gid": "POSIX group ID",
   "SecondaryGids": [Optional list of secondary Group IDs],
 },
 "HomeDirectory": "/fs-id/path/to/home/directory"
}
```

此Role欄位顯示驗證成功。在進行密碼身份驗證時（當您提供Password:標題時），您不需要提供 SSH 公鑰。如果用戶無法通過身份驗證，例如，如果密碼不正確，則您的方法應返回沒有Role設置的響應。這種響應的一個例子是一個空的 JSON 對象。

下列範例回應顯示具有邏輯主目錄類型的使用者。

```
{
    "Role": "arn:aws:iam::123456789012:role/transfer-access-role-efs",
    "HomeDirectoryType": "LOGICAL",
    "HomeDirectoryDetails":"[{\"Entry\":\"/\",\"Target\":\"/faa1a123\"}]",
    "PublicKeys":[""],
    "PosixProfile":{"Uid":65534,"Gid":65534}
}
```

您可以在 Lambda 函數中以 JSON 格式包含使用者政策。如需有關在 Transfer Family 中設定使用者原則的詳細資訊，請參閱管理存取控制。

默認 Lambda 數

若要實作不同的驗證策略，請編輯閘道使用的 Lambda 函數。為了協助您滿足應用程式的需求，您可以在 Node.js 中使用下列 Lambda 函數範例。如需有關 Lambda 的詳細資訊，請參閱AWS Lambda 開發人員指南或使用 Node.js 建置 Lambda 函數。

下列範例 Lambda 函數會取得您的使用者名稱、密碼 (如果您正在執行密碼驗證)、伺服器 ID、通訊協定和用戶端 IP 位址。您可以使用這些輸入的組合來查詢您的身份提供者，並確定是否應該接受登錄。

> **Note**
>
> 如果您為伺服器啟用了多個通訊協定，並且想要透過多個通訊協定使用相同的使用者名稱提供存取權，只要您的身分識別提供者中設定了通訊協定特定的認證，就可以這麼做。
> 對於檔案傳輸通訊協定 (FTP)，我們建議維護與安全殼層 (SSH) 檔案傳輸通訊協定 (SFTP) 和透過 SSL (FTPS) 的檔案傳輸通訊協定分開的憑證。我們建議您保留個別的 FTP 認證，因為 FTP 與 SFTP 和 FTPS 不同，FTP 會以純文字傳輸認證。藉由將 FTP 認證與 SFTP 或 FTPS 隔離，如果 FTP 認證是共用或公開的，您使用 SFTP 或 FTPS 的工作負載將保持安全。

此示例函數返回角色和邏輯主目錄的詳細信息，以及公鑰（如果它執行公鑰身份驗證）。

當您建立服務管理的使用者時，您可以設定其主目錄 (邏輯或實體)。同樣地，我們需要 Lambda 函數結果來傳達所需的使用者實體或邏輯目錄結構。您設定的參數取決於HomeDirectoryType欄位的值。

- HomeDirectoryType設定為 PATH — HomeDirectory 欄位必須是絕對的 Amazon S3 儲存貯體前綴或 Amazon EFS 絕對路徑，讓您的使用者可以看到。
- HomeDirectoryType設定為 LOGICAL — 不要設定HomeDirectory欄位。相反地，我們會設定一個HomeDirectoryDetails欄位，提供所需的「項目/目標」對應，類似於服務管理使用者HomeDirectoryDetails參數中描述的值。

中列出了範例函數範例 Lambda 函數。

可搭配使用的 Lambda 函數 AWS Secrets Manager

若要用 AWS Secrets Manager 作身分識別提供者，您可以使用範例 AWS CloudFormation 範本中的 Lambda 函數。Lambda 函數會使用您的認證查詢 Secrets Manager 服務，如果成功，則會傳回指定的密碼。如需 Secrets Manager 的詳細資訊，請參閱 AWS Secrets Manager 使用者指南。

若要下載使用此 Lambda 函數的 AWS CloudFormation 範例範本，請前往提供的 Amazon S3 儲存貯體 AWS Transfer Family。

AWS CloudFormation 模板的改進

已對已發佈的 CloudFormation範本進行了改進 API Gateway 介面。範本現在會在 API Gateway 中使用 Base64 編碼的密碼。您現有的部署在沒有此增強功能的情況下繼續運作，但不允許使用基本 US-ASCII 字元集以外的字元的密碼。

範本中啟用此功能的變更如下：

- 資GetUserConfigRequest AWS::ApiGateway::Method源必須有這個RequestTemplates代碼（斜體行是更新的行）

```
RequestTemplates:
   application/json: |
   {
      "username": "$util.urlDecode($input.params('username'))",
      "password":
 "$util.escapeJavaScript($util.base64Decode($input.params('PasswordBase64'))).replaceAll("\
\'","'")",
      "protocol": "$input.params('protocol')",
      "serverId": "$input.params('serverId')",
      "sourceIp": "$input.params('sourceIp')"
}
```

- GetUserConfig資源必須變更才能使用標PasswordBase64題 (斜體的行是更新後的行)：RequestParameters

```
RequestParameters:
   method.request.header.PasswordBase64: false
   method.request.querystring.protocol: false
   method.request.querystring.sourceIp: false
```

若要檢查堆疊的範本是否為最新的範本

1. 開啟主 AWS CloudFormation 控台，網址為 https://console.aws.amazon.com/cloudformation。
2. 從堆疊清單中選擇您的堆疊。
3. 從詳細資料面板中，選擇「範本」標籤。
4. 查找以下內容：

   - 搜索`RequestTemplates`，並確保你有這一行：

     ```
     "password":
      "$util.escapeJavaScript($util.base64Decode($input.params('PasswordBase64'))).replaceAll(
     \'","''")",
     ```

   - 搜索`RequestParameters`，並確保你有這一行：

     ```
     method.request.header.PasswordBase64: false
     ```

如果沒有看到更新的行，請編輯堆疊。有關如何更新 AWS CloudFormation 堆疊的詳細資訊，請參閱《使用者指南》中的AWS CloudFormation〈修改堆疊範本〉。

使用邏輯目錄簡化您的 Transfer Family 目錄結構

若要簡化 AWS Transfer Family 伺服器目錄結構，您可以使用邏輯目錄。使用邏輯目錄，您可以建構虛擬目錄結構，該結構使用者使用方便使用的名稱，讓使用者在連線到 Amazon S3 儲存貯體或 Amazon EFS 檔案系統時進行瀏覽。使用邏輯目錄時，可以避免向最終使用者洩露絕對目錄路徑、Amazon S3 儲存貯體名稱和 EFS 檔案系統名稱。

> **Note**
>
> 您應該使用工作階段原則，讓使用者只能執行您允許他們執行的作業。
> 您應該使用邏輯目錄為最終使用者建立易於使用的虛擬目錄，以及抽象的離開值區名稱。邏輯目錄對應只允許使用者存取其指定的邏輯路徑和子目錄，並禁止遍歷邏輯根的相對路徑。Transfer Family 會驗證可能包含相對元素的每個路徑，並在我們將這些路徑傳遞到 Amazon S3 之前主動封鎖這些路徑；這可防止您的使用者超越其邏輯對應。
> 即使 Transfer Family 阻止使用者存取其邏輯目錄以外的目錄，我們還是建議您使用唯一的角色或工作階段原則，在儲存層級強制執行最低權限。

您可以透過執行所謂的chroot作業，使用邏輯目錄將使用者的根目錄設定為儲存階層中的所需位置。在此模式中，使用者無法瀏覽至您為其設定的主目錄或根目錄之外的目錄。

例如，雖然 Amazon S3 使用者的範圍限制為僅存取/*mybucket*/*home*/${transfer:*UserName*}，但有些用戶端允許使用者遍歷資料夾。/*mybucket*/*home*在此情況下，使用者只有在登出並重新登入 Transfer Family 伺服器後，才會重新登入其預期的主目錄。執行作chroot業可以防止發生這種情況。

您可以跨值區和前置字元建立自己的目錄結構。如果您的工作流程需要無法透過值區首碼複寫的特定目錄結構，則此功能非常有用。您也可以連結至 Amazon S3 中的多個非連續位置，類似於在 Linux 檔案系統中建立符號連結，您的目錄路徑會參照檔案系統中的不同位置。

> **邏輯目錄檔案對映**
>
> 資HomeDirectoryMapEntry料類型現在包含Type參數。在此參數存在之前，您可以建立目標為檔案的邏輯目錄對應。如果您先前已建立任何類型的邏輯目錄對映，您必須明確地將設定Type為FILE，否則這些對映將無法正常運作。
> 執行此操作的一種方法是調用 UpdateUser API，並Type將現有映射設置FILE為。

使用邏輯目錄的規則

在建立邏輯目錄對應之前，您應該瞭解下列規則：

- 如果Entry是"/"，您只能有一個對應，因為不允許重疊路徑。
- 邏輯目錄支援最大 2.1 MB 的對應 (對於服務管理的使用者，此限制為 2,000 個項目)。也就是說，包含對應的資料結構的大小上限為 2.1 MB。如果您有很多映射，則可以按如下方式計算映射的大小：
  1. 以格式寫出一個典型的映射{"Entry":"/*entry-path*","Target":"/*target-path*"}，其中*entry-path*和*target-path*是您將使用的實際值。
  2. 計算該字符串中的字符，然後添加一（1）。
  3. 將該數字乘以伺服器的近似對應數。

  如果您在步驟 3 中估計的數目小於 2.1 MB，則您的對應處於可接受的限制範圍內。
- 如果儲存貯體或檔案系統路徑已根據使用者名稱參數化，則目標可以使用該${transfer:UserName}變數。
- 目標可以是不同值區或檔案系統中的路徑，但您必須確定對應 AWS Identity and Access Management (IAM) 角色 (回應中的Role參數) 可提供對這些值區或檔案系統的存取權。

- 請勿指定HomeDirectory參數，因為當您使用參數值時，EntryTarget配對會隱含此LOGICALHomeDirectoryType值。
- 目標必須以正斜線 (/) 字元開頭，但是當您指定時，請勿使用尾隨正斜線 (/)。Target例如，/DOC-EXAMPLE-BUCKET/images是可以接受的DOC-EXAMPLE-BUCKET/images，但不/DOC-EXAMPLE-BUCKET/images/是。
- Amazon S3 是一個物件存放區，這表示資料夾是虛擬概念，而且沒有實際的目錄階層。如果您的應用程式從用戶端發出stat作業，當您使用 Amazon S3 進行儲存時，所有內容都會歸類為檔案。有關此行為的說明，請參閱使用 Amazon 簡單儲存服務使用者指南中的資料夾在 Amazon S3 主控台中組織物件。如果您的應用程式需要stat準確顯示某個項目是檔案還是資料夾，您可以使用 Amazon Elastic File System (Amazon EFS) 做為 Transfer Family 伺服器的儲存選項。
- 如果您要為使用者指定邏輯目錄值，則使用的參數取決於使用者的類型：
  - 對於服務管理的使用者，請在HomeDirectoryMappings中提供邏輯目錄值。
  - 對於自訂身分識別提供者使用者，請在中HomeDirectoryDetails提供邏輯目錄值

> **Important**
>
> 除非您選擇優化 Amazon S3 目錄的效能 (當您建立或更新伺服器時)，否則根目錄必須在啟動時存在。對於 Amazon S3，這表示您必須已建立以正斜線 (/) 結尾的零位元組物件，才能建立根資料夾。避免此問題是考慮優化 Amazon S3 效能的一個原因。

實作邏輯目錄和 chroot

若要使用邏輯目錄和chroot功能，您必須執行下列動作：

為每個使用者開啟邏輯目錄。透過在建立或更新使用者LOGICAL時將HomeDirectoryType參數設定為來執行此操作。

```
"HomeDirectoryType": "LOGICAL"
```

chroot

對於chroot，建立由每個使用者的單Entry一Target配對組成的目錄結構。根資料夾是Entry點，Target也是值區或檔案系統中要對映的位置。

Example for Amazon S3

```
[{"Entry": "/", "Target": "/mybucket/jane"}]
```

Example for Amazon EFS

```
[{"Entry": "/", "Target": "/fs-faa1a123/jane"}]
```

您可以使用上一個範例中的絕對路徑，也可以使用動態取代使用者名稱${transfer:UserName}，如下列範例所示。

```
[{"Entry": "/", "Target":
"/mybucket/${transfer:UserName}"}]
```

在上述範例中，使用者已鎖定至其根目錄，且無法在階層中向上遍歷較高的位置。

虛擬目錄結構

對於虛擬目錄結構，只要使用者的 IAM 角色對應具有存取權限，您就可以建立多EntryTarget個配對，並在 S3 儲存貯體或 EFS 檔案系統中的任何位置使用目標，包括跨多個儲存貯體或檔案系統。

在下列虛擬結構範例中，當使用者登入 AWS SFTP 時，它們位於具有、/pics/doc、和子目錄的根目錄/reporting中。/anotherpath/subpath/financials

> **Note**
>
> 除非您選擇優化 Amazon S3 目錄的效能 (當您建立或更新伺服器時)，否則使用者或管理員必須建立目錄 (如果目錄尚未存在)。避免此問題是考慮優化 Amazon S3 效能的一個原因。
> 對於 Amazon EFS，您仍然需要管理員建立邏輯對應或目/錄。

```
[
{"Entry": "/pics", "Target": "/bucket1/pics"},
{"Entry": "/doc", "Target": "/bucket1/anotherpath/docs"},
{"Entry": "/reporting", "Target": "/reportingbucket/Q1"},
{"Entry": "/anotherpath/subpath/financials", "Target": "/reportingbucket/financials"}]
```

Note

您只能將檔案上載至您對映的特定資料夾。這表示在前面的範例中，您無法僅上傳至/anotherpath或anotherpath/subpath目錄anotherpath/subpath/financials。您也無法直接對應至這些路徑，因為不允許重疊路徑。
例如，假設您建立下列對映：

```
{
   "Entry": "/pics",
   "Target": "/mybucket/pics"
},
{
   "Entry": "/doc",
   "Target": "/mybucket/mydocs"
},
{
   "Entry": "/temp",
   "Target": "/mybucket"
}
```

您只能將檔案上傳到這些值區。當您第一次透過連線時sftp，您會被放置到根目錄中/。如果您嘗試將檔案上傳到該目錄，上傳會失敗。下列指令顯示範例序列：

```
sftp> pwd
Remote working directory: /
sftp> put file
Uploading file to /file
remote open("/file"): No such file or directory
```

若要上載到任何directory/sub-directory，您必須明確地將路徑對應至sub-directory.

如需有關設定邏輯目錄和使用者的chroot詳細資訊，包括您可以下載和使用的 AWS CloudFormation 範本，請參閱 AWS S AWS torage 部落格中的使用 chroot 和邏輯目錄簡化 SFTP 結構。

設定邏輯目錄範例

在這個例子中，我們創建一個用戶，並分配兩個邏輯目錄。下列指令會建立具有邏輯目錄pics和的新使用者 (針對現有的 Transfer Family 伺服器) doc。

```
aws transfer create-user --user-name marymajor-logical --server-id s-11112222333344445
 --role arn:aws:iam::1234abcd5678:role/marymajor-role --home-directory-type LOGICAL \
 --home-directory-mappings "[{\"Entry\":\"/pics\", \"Target\":\"/DOC-EXAMPLE-BUCKET1/
pics\"}, {\"Entry\":\"/doc\", \"Target\":\"/DOC-EXAMPLE-BUCKET2/test/mydocs\"}]" \
 --ssh-public-key-body file://~/.ssh/id_rsa.pub
```

如果**marymajor**是現有使用者，且其主目錄類型為PATH，您可以使用LOGICAL與前一個類似的命令將其變更為。

```
aws transfer update-user --user-name marymajor-logical \
 --server-id s-11112222333344445 --role arn:aws:iam::1234abcd5678:role/marymajor-role \
 --home-directory-type LOGICAL --home-directory-mappings "[{\"Entry\":\"/pics\",
 \"Target\":\"/DOC-EXAMPLE-BUCKET1/pics\"}, \
 {\"Entry\":\"/doc\", \"Target\":\"/DOC-EXAMPLE-BUCKET2/test/mydocs\"}]"
```

注意下列事項：

- 如果目錄/DOC-EXAMPLE-BUCKET1/pics並/DOC-EXAMPLE-BUCKET2/test/mydocs不存在，則用戶（或管理員）需要創建它們。
- 當**marymajor**連接到服務器並運行ls -l命令時，她會看到以下內容：

  ```
  drwxr--r--   1        -        -        0 Mar 17 15:42 doc
  drwxr--r--   1        -        -        0 Mar 17 16:04 pics
  ```

- **marymajor**無法在此層級建立任何檔案或目錄。但是，在pics和中doc，她可以添加子目錄。
- 她新增pics並doc/DOC-EXAMPLE-BUCKET2/test/mydocs分別新增至 Amazon S3 路徑/DOC-EXAMPLE-BUCKET1/pics的檔案。
- 在這個例子中，我們指定了兩個不同的存儲桶來說明這種可能性。不過，您可以為使用者指定的多個或所有邏輯目錄使用同一個值區。

設定 Amazon EFS 的邏輯目錄

如果您的 Transfer Family 伺服器使用 Amazon EFS，則必須使用讀取和寫入存取權建立使用者的主目錄，使用者才能在其邏輯主目錄中工作。使用者無法自行建立此目錄，因為他們缺乏邏輯主目錄的權限。mkdir

如果使用者的主目錄不存在，且他們執行ls命令，則系統回應如下：

```
sftp> ls
```

```
remote readdir ("/"): No such file or directory
```

具有父目錄管理存取權的使用者需要建立使用者的邏輯主目錄。

自定義 AWS Lambda 響應

您可以將邏輯目錄與 Lambda 函數搭配連線至您的自訂身分提供者。若要這麼做，請在 Lambda 函數中指定HomeDirectoryDetails參數的 HomeDirectoryType as **LOGICAL**、加入Entry和Target值。例如：

```
HomeDirectoryType: "LOGICAL"
HomeDirectoryDetails: "[{\"Entry\": \"/\", \"Target\": \"/DOC-EXAMPLE-BUCKET/
theRealFolder"}]"
```

下列程式碼是自訂 Lambda 驗證呼叫成功回應的範例。

```
aws transfer test-identity-provider --server-id s-1234567890abcdef0 --user-name myuser
{
    "Url": "https://a1b2c3d4e5.execute-api.us-east-2.amazonaws.com/prod/servers/
s-1234567890abcdef0/users/myuser/config",
    "Message": "",
    "Response": "{\"Role\": \"arn:aws:iam::123456789012:role/bob-usa-role\",
\"HomeDirectoryType\": \"LOGICAL\",\"HomeDirectoryDetails\": \"[{\\\"Entry\\\":\\\"/
myhome\\\",\\\"Target\\\":\\\"/DOC-EXAMPLE-BUCKET/theRealFolder\\\"}]\",\"PublicKeys\":
 \"[ssh-rsa myrsapubkey]\"}",
    "StatusCode": 200
}
```

> **Note**
>
> 只有當您使用 API Gateway 方法做為自訂身分識別提供者時，才會傳回該"Url":行。

AWS Transfer Family SFTP 連接器

AWS Transfer Family SFTP 連接器建立了使用 SFTP 通訊協定在 Amazon 儲存和外部合作夥伴之間傳送檔案和訊息的關係。您可以將檔案從 Amazon S3 傳送到合作夥伴擁有的外部目的地。您也可以使用 SFTP 連接器從合作夥伴的 SFTP 伺服器擷取檔案。

> **Note**
>
> 目前，SFTP 連接器只能用於連接到提供網際網路存取端點的遠端 SFTP 伺服器。

下列部落格文章提供使用 SFTP 連接器建立 MFT 工作流程的參考架構，包括在使用 SFTP 連接器將檔案傳送至遠端 SFTP 伺服器之前先使用 PGP 加密檔案：使用 SFTP 連接器和 PGP 加密架構安全且符合規範的受管理檔案傳輸。 AWS Transfer Family

如需 Tran AWS Transfer Family sfer Family 列 SFTP 連接器的簡短介紹，請檢視 SFTP 連接器。

主題

- 設定 SFTP 連接器
- 使用 SFTP 連接器傳送和擷取檔案
- 列出遠程目錄的內容
- 管理 SFTP 連接器

設定 SFTP 連接器

本主題說明如何建立 SFTP 連接器、與 SFTP 連接器相關聯的安全性演算法、如何儲存密碼以保留認證、有關格式化私密金鑰的詳細資料，以及測試連接器的指示。

主題

- 建立 SFTP 連接器
- 儲存密碼以與 SFTP 連接器搭配使用
- 產生並格式化 SFTP 連接器私密金鑰
- 測試 SFTP 連接器

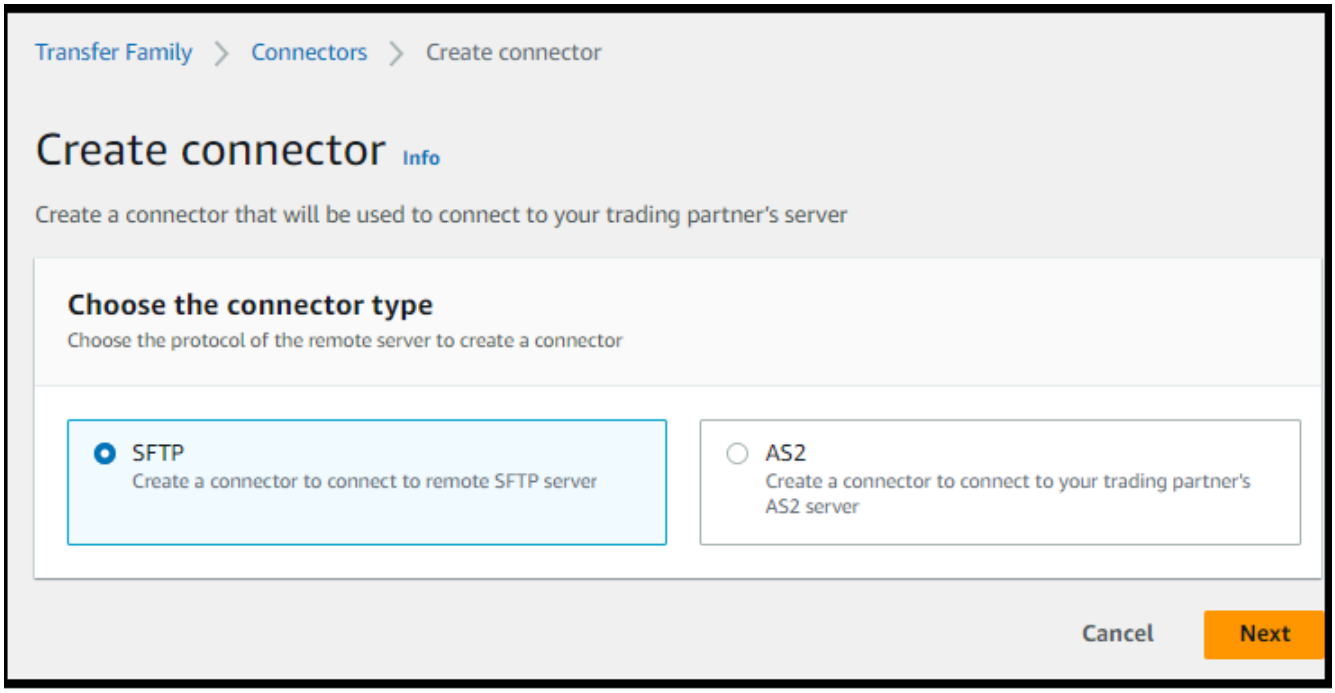
建立 SFTP 連接器

此程序說明如何使用 AWS Transfer Family 主控台或 AWS CLI建立 SFTP 連接器。

Console

建立 SFTP 連接器的步驟

1. 開啟主 AWS Transfer Family 控台，網址為 https://console.aws.amazon.com/transfer/。
2. 在左側導覽窗格中，選擇「連接器」，然後選擇「建立連接器」。
3. 為連接器類型選擇 SFTP 以建立 SFTP 連接器，然後選擇 [下一步]。



4. 在 [連接器組態] 區段中，提供下列資訊：

   - 對於 URL，請輸入遠端 SFTP 伺服器的 URL。例如`sftp://`*`partner-SFTP-server-url`*，此 URL 必須格式化為`sftp://AnyCompany.com`。

     > **Note**
     >
     > 或者，您可以在 URL 中提供連接埠號碼。格式是 `sftp://`*`partner-SFTP-server-url`*`:`*`port-number`*。預設連接埠號碼 (未指定連接埠時) 為連接埠 22。

   - 對於存取角色，請選擇要使用的 (IAM) 角色的 Amazon 資源名稱 AWS Identity and Access Management (ARN)。

- StartFileTransfer請確定此角色提供對要求中所使用之檔案位置之父目錄的讀取和寫入存取權。
- 請確定此角色提供存**secretsmanager:GetSecretValue**取密碼的權限。

> **Note**
>
> 在策略中，您必須指定秘密的 ARN。ARN 包含密碼名稱，但會將名稱附加六個隨機字母數字字元。秘密的 ARN 具有以下格式。
>
> ```
> arn:aws:secretsmanager:region:account-id:secret:aws/
> transfer/SecretName-6RandomCharacters
> ```

- 請確定此角色包含信任關係，可讓連接器在為使用者的傳輸要求提供服務時存取您的資源。如需建立信任關係的詳細資訊，請參閱建立信任關係。

下列範例授與必要的權限，以存取 Amazon S3 中的*## EXAMPLE* 儲存貯體，以及存放在秘 Secrets Manager 中的指定密碼。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
        "Sid": "AllowListingOfUserFolder",
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
        ]
    },
    {
        "Sid": "HomeDirObjectAccess",
        "Effect": "Allow",
        "Action": [
            "s3:PutObject",
            "s3:GetObject",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion",
            "s3:GetObjectVersion",
```

```
            "s3:GetObjectACL",
            "s3:PutObjectACL"
        ],
        "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
    },
    {
        "Sid": "GetConnectorSecretValue",
        "Effect": "Allow",
        "Action": [
            "secretsmanager:GetSecretValue"
        ],
        "Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/
transfer/SecretName-6RandomCharacters"
    }
  ]
}
```

> **Note**
>
> 對於存取角色，此範例會授予單一密碼的存取權。不過，您可以使用萬用字元，如果您想要對多個使用者和密碼重複使用相同的 IAM 角色，則可以節省工作。例如，下列資源陳述式會授與名稱開頭為之所有密碼的權限aws/transfer。
>
> ```
> "Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/
> transfer/*"
> ```
>
> 您也可以將包含 SFTP 認證的密碼儲存在另一個 AWS 帳戶。如需啟用跨帳戶密碼存取的詳細資訊，請參閱不同帳戶中使用者 AWS Secrets Manager 密碼的權限。

- (選擇性) 對於 Logging 角色，請為連接器選擇 IAM 角色，以用來將事件推送至記 CloudWatch 錄。下列範例原則列出 SFTP 連接器記錄事件的必要權限。

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "SFTPConnectorPermissions",
        "Effect": "Allow",
        "Action": [
            "logs:CreateLogStream",
            "logs:DescribeLogStreams",
            "logs:CreateLogGroup",
```

```
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:/aws/transfer/*"
            ]
        }]
}
```

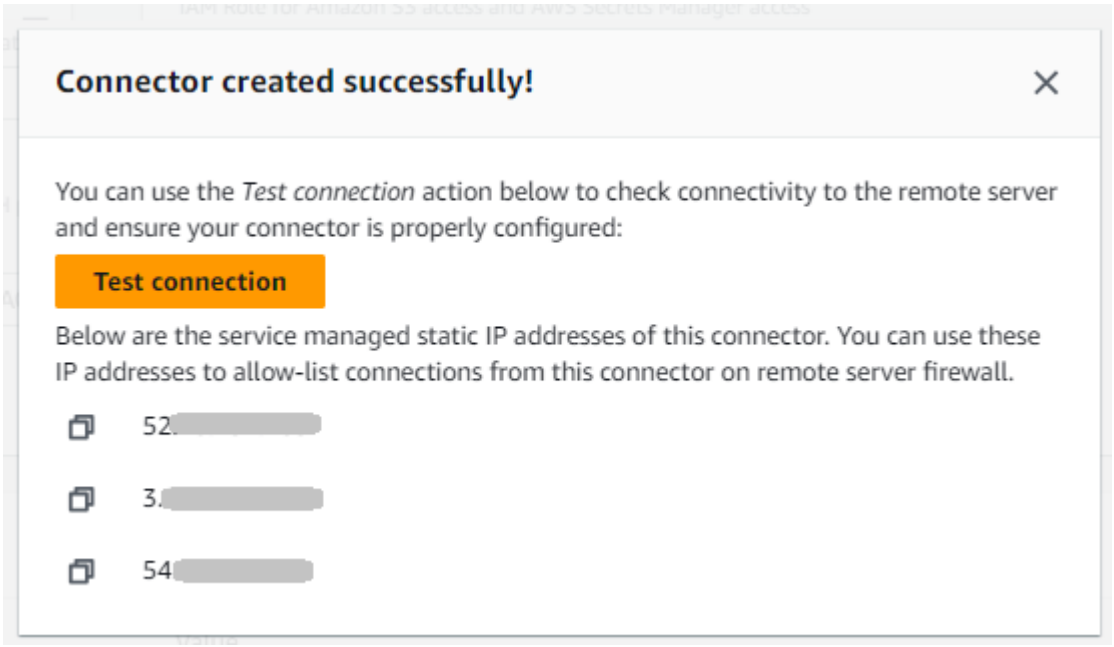
5. 在「SFTP 組態」區段中，提供下列資訊：

   - 對於連接器認證，請從下拉式清單中 AWS Secrets Manager 選擇包含 SFTP 使用者私密金鑰或密碼的密碼名稱。您必須建立密碼並以特定方式儲存。如需詳細資訊，請參閱 儲存密碼以與 SFTP 連接器搭配使用。
   - 對於受信任的主機金鑰，請貼上用來識別外部伺服器之主機金鑰的公開部分。您可以選擇新增受信任的主機金鑰來新增其他金鑰，以新增多個金鑰。您可以對 SFTP 伺服器使用`ssh-keyscan`指令來擷取必要的金鑰。如需 Transfer Family 支援之受信任主機金鑰的格式和類型的詳細資訊，請參閱SFTPConnectorConfig。

6. 在 [密碼編譯演算法選項] 區段中，從 [安全性原則] 欄位的下拉式清單中選擇安全性原則。安全性原則可讓您選取連接器支援的密碼編譯演算法。如需有關可用安全性原則和演算法的詳細資訊，請參閱AWS Transfer Family SFTP 連接器的安全性原則。

7. (選擇性) 在「標籤」區段中，對於「鍵值」，輸入一或多個標籤作為鍵值配對。

8. 確認所有設定後，請選擇 [建立連接器] 以建立 SFTP 連接器。如果成功建立連接器，會出現一個畫面，其中包含指派的靜態 IP 位址清單和 [測試連線] 按鈕。使用按鈕測試新連接器的組態。



[連接器] 頁面隨即出現，並將新 SFTP 連接器的識別碼新增至清單。若要檢視連接器的詳細資料，請參閱檢視 SFTP 連接器詳細資料。

CLI

您可以使用create-connector指令建立連接器。若要使用此指令建立 SFTP 連接器，您必須提供下列資訊。

- 遠端 SFTP 伺服器的網址。例如`sftp://partner-SFTP-server-url`，此 URL 必須格式化為`sftp://AnyCompany.com`。
- 存取角色。選擇要使用的 (IAM) 角色的 Amazon 資源名稱 AWS Identity and Access Management (ARN)。
  - `StartFileTransfer`請確定此角色提供對要求中所使用之檔案位置之父目錄的讀取和寫入存取權。
  - 請確定此角色提供存**`secretsmanager:GetSecretValue`**取密碼的權限。

    > **Note**
    >
    > 在策略中，您必須指定秘密的 ARN。ARN 包含密碼名稱，但會將名稱附加六個隨機字母數字字元。秘密的 ARN 具有以下格式。
    >
    > ```
    > arn:aws:secretsmanager:region:account-id:secret:aws/
    > transfer/SecretName-6RandomCharacters
    > ```

  - 請確定此角色包含信任關係，可讓連接器在為使用者的傳輸要求提供服務時存取您的資源。如需建立信任關係的詳細資訊，請參閱建立信任關係。

下列範例授與必要的權限，以存取 Amazon S3 中的*## EXAMPLE* 儲存貯體，以及存放在秘 Secrets Manager 中的指定密碼。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
        "Sid": "AllowListingOfUserFolder",
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Effect": "Allow",
```

```
        "Resource": [
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
        ]
    },
    {
        "Sid": "HomeDirObjectAccess",
        "Effect": "Allow",
        "Action": [
            "s3:PutObject",
            "s3:GetObject",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion",
            "s3:GetObjectVersion",
            "s3:GetObjectACL",
            "s3:PutObjectACL"
        ],
        "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
    },
    {
        "Sid": "GetConnectorSecretValue",
        "Effect": "Allow",
        "Action": [
            "secretsmanager:GetSecretValue"
        ],
        "Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/
transfer/SecretName-6RandomCharacters"
    }
  ]
}
```

Note

對於存取角色，此範例會授予單一密碼的存取權。不過，您可以使用萬用字元，如果您想要對多個使用者和密碼重複使用相同的 IAM 角色，則可以節省工作。例如，下列資源陳述式會授與名稱開頭為之所有密碼的權限`aws/transfer`。

```
"Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/transfer/
*"
```

您也可以將包含 SFTP 認證的密碼儲存在另一個 AWS 帳戶。如需啟用跨帳戶密碼存取的詳細資訊，請參閱[不同帳戶中使用者 AWS Secrets Manager 密碼的權限]。

- (選擇性) 選擇連接器的 IAM 角色，以用來將事件推送至記 CloudWatch 錄。下列範例原則列出 SFTP 連接器記錄事件的必要權限。

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "SFTPConnectorPermissions",
        "Effect": "Allow",
        "Action": [
            "logs:CreateLogStream",
            "logs:DescribeLogStreams",
            "logs:CreateLogGroup",
            "logs:PutLogEvents"
        ],
        "Resource": [
            "arn:aws:logs:*:*:log-group:/aws/transfer/*"
        ]
    }]
}
```

- 提供下列 SFTP 組態資訊。
  - 中 AWS Secrets Manager 包含 SFTP 使用者私密金鑰或密碼的秘密 ARN。
  - 用來識別外部伺服器之主機金鑰的公用部分。您可以視需要提供多個受信任的主機金鑰。

  提供 SFTP 資訊的最簡單方法是將其儲存至檔案。例如，將下列範例文字複製到名為的檔案中`testSFTPConfig.json`。

```
// Listing for testSFTPConfig.json
{
   "UserSecretId": "arn:aws::secretsmanager:us-east-2:123456789012:secret:aws/
transfer/example-username-key",
   "TrustedHostKeys": [
      "sftp.example.com ssh-rsa AAAAbbbb...EEEE="
   ]
}
```

- 指定連接器的安全性原則，並輸入安全性原則名稱。

> **Note**
>
> `SecretId`可以是整個 ARN 或密鑰的名稱（上一個列表中的*#####-##*）。

然後執行下列命令以建立連接器。

```
aws transfer create-connector --url "sftp://partner-SFTP-server-url" \
--access-role your-IAM-role-for-bucket-access \
--logging-role arn:aws:iam::your-account-id:role/service-role/
AWSTransferLoggingAccess \
--sftp-config file:///path/to/testSFTPConfig.json
--security-policy-name security-policy-name
```

儲存密碼以與 SFTP 連接器搭配使用

您可以使用 Secrets Manager 來儲存 SFTP 連接器的使用者認證。建立密碼時，您必須提供使用者名稱。此外，您可以提供密碼、私密金鑰或兩者。如需詳細資訊，請參閱 SFTP 連接器的配額。

> **Note**
>
> 當您將密碼儲存在「Secrets Manager 中時， AWS 帳戶 會產生費用。如需定價的資訊，請參閱 AWS Secrets Manager 定價。

若要將使用者認證儲存在 SFTP 連接器的 Secrets Manager 中

1. 請登入 AWS Management Console 並開啟 AWS Secrets Manager 主控台，網址為 https://console.aws.amazon.com/secretsmanager/。
2. 在左側導覽窗格中，選擇秘密。
3. 在「密碼」頁面上，選擇「儲存新密碼」。
4. 在 [選擇密碼類型] 頁面上，對於 [密碼類型]，選擇 [其他密碼類型]。
5. 在「鍵/值對」區段中，選擇「鍵/值」標籤。
   - 鍵-輸入**`Username`**。
   - value — 輸入獲得授權可連線至合作夥伴伺服器的使用者名稱。
6. 如果您要提供密碼，請選擇 [新增列]，然後在 [機碼/值配對] 區段中，選擇 [機碼/值] 索引標籤。

選擇添加行，然後在「鍵/值對」部分中，選擇「鍵/值」選項卡。

- 鍵-輸入**Password**。
- 值 — 輸入使用者的密碼。

7. 如果您想要提供私密金鑰，請參閱產生並格式化 SFTP 連接器私密金鑰，其中說明如何輸入私密金鑰資料。

> **Note**
>
> 您輸入的私密金鑰資料必須對應於遠端 SFTP 伺服器中為此使用者儲存的公開金鑰。

8. 選擇下一步。
9. 在 [設定密碼] 頁面上，輸入密碼的名稱和說明。建議您使用的字首做**aws/transfer/**為名稱。例如，您可以命名您的秘密**aws/transfer/connector-1**。
10. 選擇 [下一步]，然後接受 [設定旋轉] 頁面上的預設值。然後選擇下一步。
11. 在「檢閱」頁面上，選擇「儲存」以建立並儲存密碼。

產生並格式化 SFTP 連接器私密金鑰

有關產生公開/私 key pair 的完整詳細資訊，請參閱。在 macOS、Linux 或 Unix 上建立安全殼層金鑰

例如，若要產生與 SFTP 連接器搭配使用的私密金鑰，下列範例指令會產生正確的金鑰類型 (將 *key_name* 取代為 key pair 的實際檔案名稱)：

```
ssh-keygen -t rsa -b 4096 -m PEM -f key_name -N ""
```

> **Note**
>
> 當您建立 key pair SFTP 連接器使用時，請勿使用複雜密碼。SFTP 組態必須使用空白的複雜密碼才能正常運作。

此指令會建立 RSA key pair，金鑰大小為 4096 位元。金鑰會以舊版 PEM 格式產生，Transfer Family 需要此格式才能與 SFTP 連接器密碼搭配使用。金鑰會儲存在目前目錄中的 *key_name* *key_name*.pub (私密金鑰) 和 (公開金鑰) 中：也就是執行ssh-keygen命令的目錄。

> **Note**
>
> Transfer Family 不支援用於 SFTP 連接器之金鑰的 OpenSSH 格式 (`-----BEGIN OPENSSH PRIVATE KEY-----`)。金鑰必須是舊版 PEM 格式 (`-----BEGIN RSA PRIVATE KEY-----`或`-----BEGIN EC PRIVATE KEY-----`)。您可以在執行命令時提供`-m PEM`選項，使用此ssh-keygen工具來轉換金鑰。

產生金鑰之後，您必須確定私密金鑰的格式為 JSON 格式的內嵌換行字元 (」\ n「)。

使用命令將現有的私鑰轉換為正確的格式-帶有嵌入換行符的 JSON 格式。在這裡，我們提供了jq和 Powershell 的例子。您可以使用任何您想要將私鑰轉換為帶有嵌入換行符的 JSON 格式的工具或命令。

jq command

此範例使用jq指令，可從下載 jq 下載。

```
jq -sR . path-to-private-key-file
```

例如，如果您的私密金鑰檔案位於中`~/.ssh/my_private_key`，則指令如下所示。

```
jq -sR . ~/.ssh/my_private_key
```

這會以正確的格式（帶有嵌入換行符）將密鑰輸出到標準輸出。

PowerShell

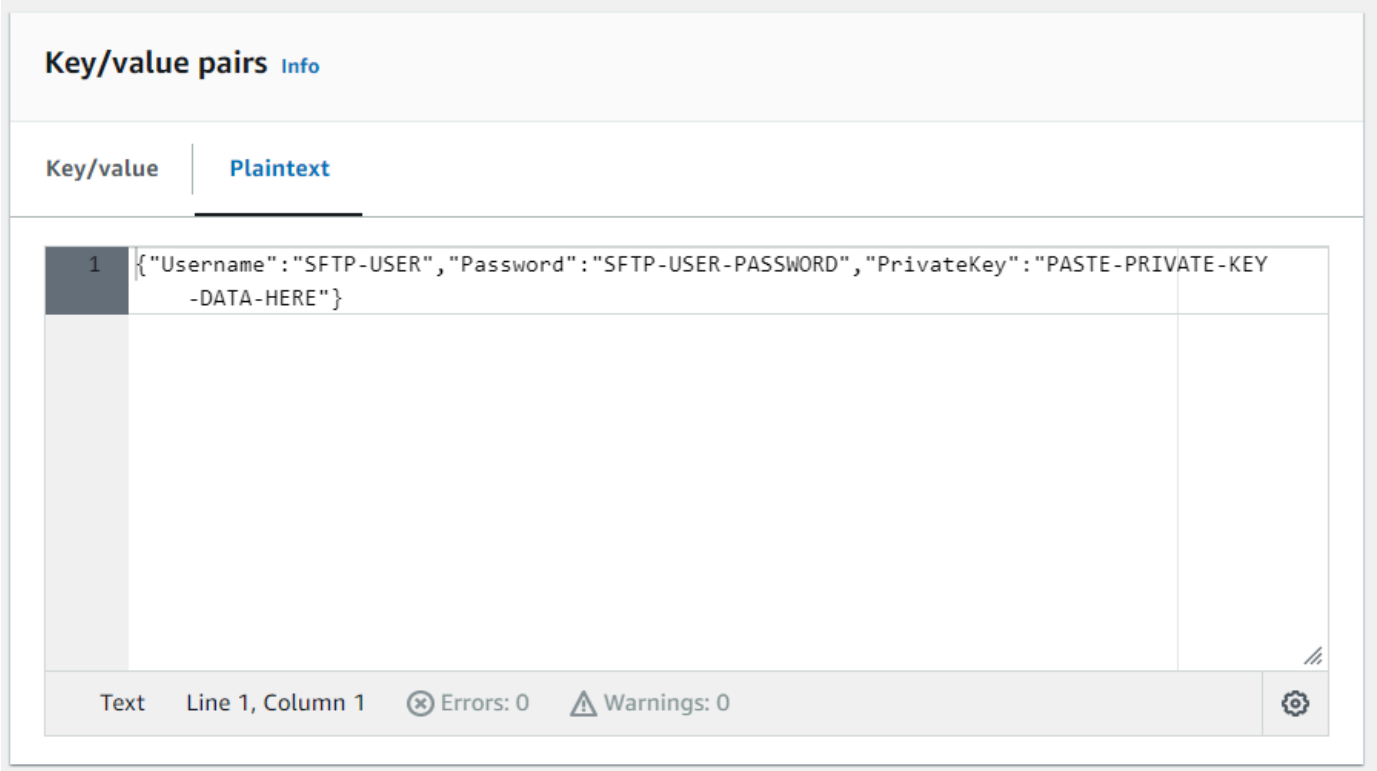
如果您使用的是 Windows，則可以使 PowerShell 用將密鑰轉換為正確的格式。下面的 Powershell 命令將私鑰轉換為正確的格式。

```
Get-Content -Raw path-to-private-key-file | ConvertTo-Json
```

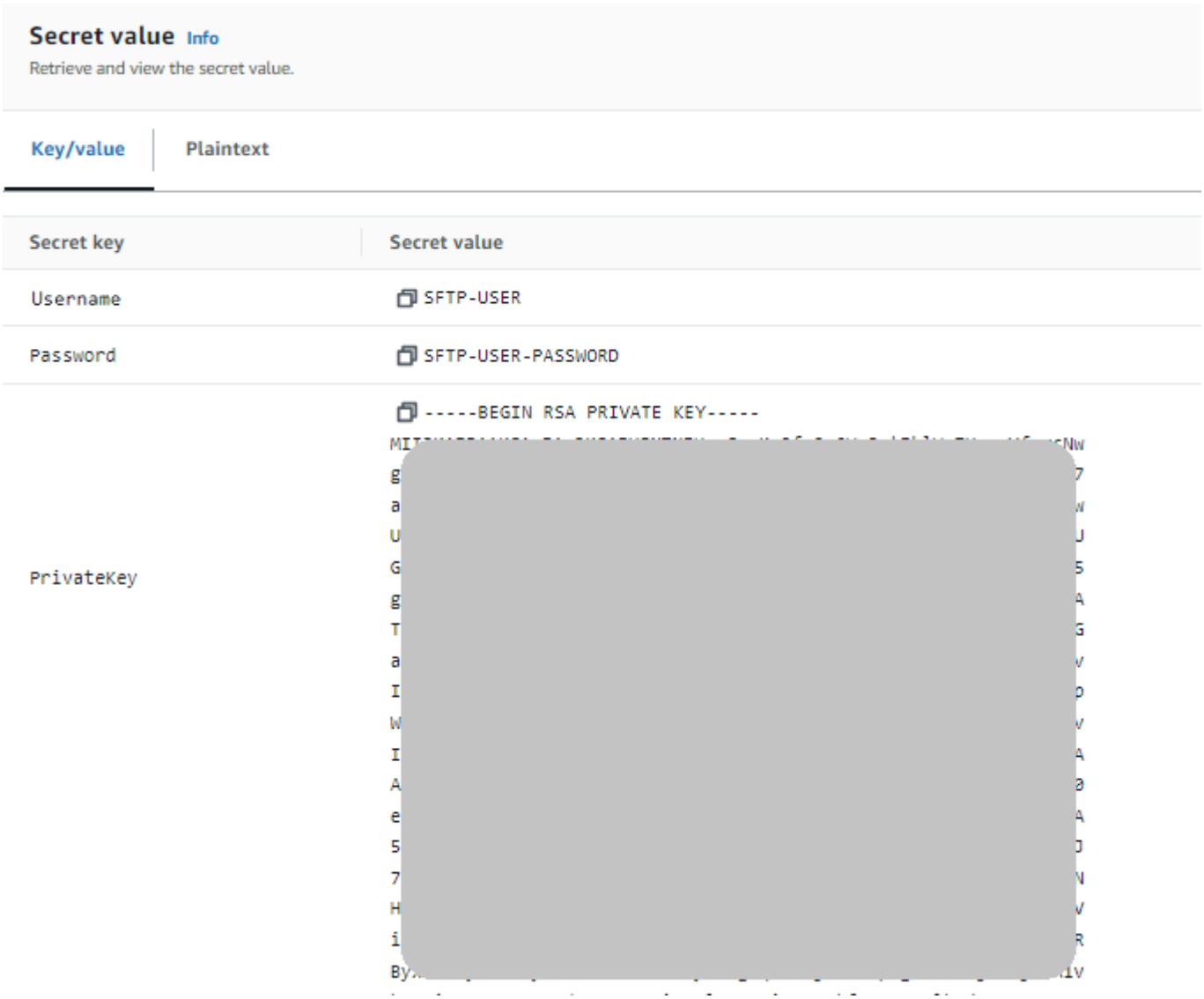
將私密金鑰資料新增至密碼以與 SFTP 連接器搭配使用

1. 在 Secrets Manager 主控台中，當儲存其他類型的密碼時，請選擇純文字索引標籤。該文本應該是空的，只有一個開放和右大括號 {}。
2. 使用以下格式粘貼您的用戶名，私鑰數據和/或密碼。針對您的私密金鑰資料，貼上您在步驟 1 中執行之命令的輸出。

```
{"Username":"SFTP-USER","Password":"SFTP-USER-PASSWORD","PrivateKey":"PASTE-PRIVATE-KEY-DATA-HERE"}
```



如果您正確貼上私密金鑰資料，您應該會在選取 [金鑰/值] 索引標籤時看到下列內容。請注意 line-by-line，會顯示私密金鑰資料，而不是連續的文字字串。



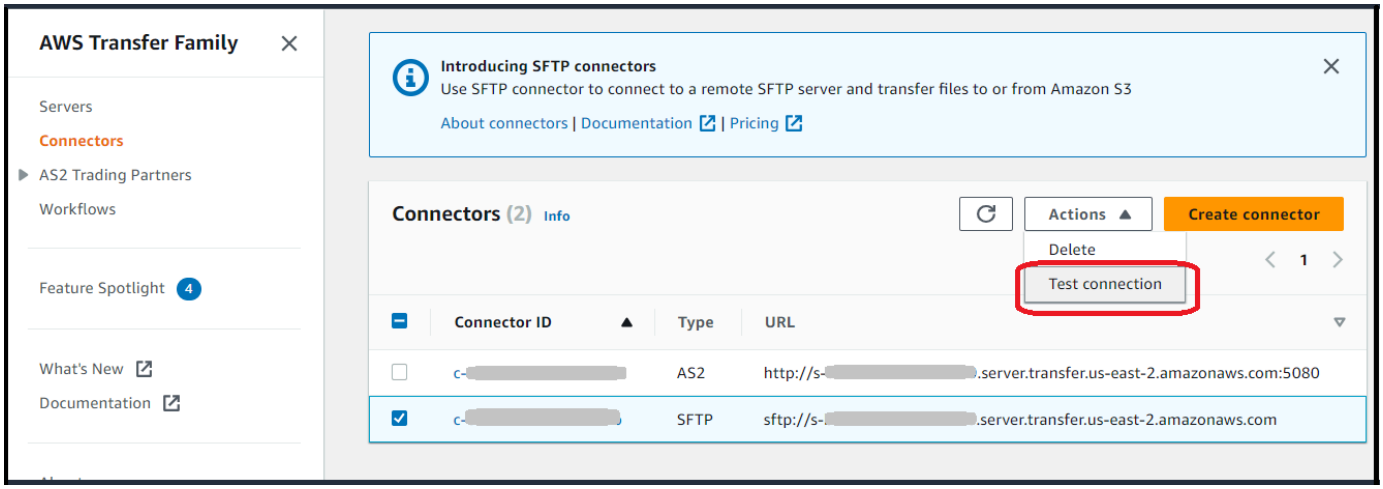
3. 繼續步驟 8 中[儲存密碼以與 SFTP 連接器搭配使用]的程序，並遵循該程序直到結束。

測試 SFTP 連接器

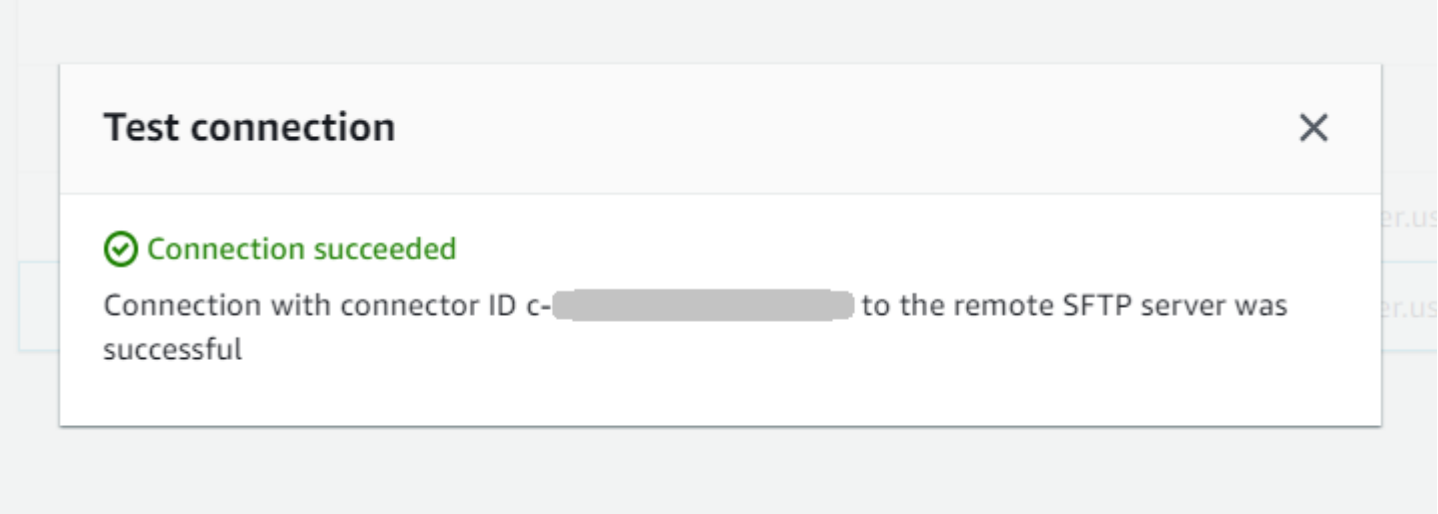
建立 SFTP 連接器之後，建議您先對其進行測試，然後再嘗試使用新連接器傳輸任何檔案。

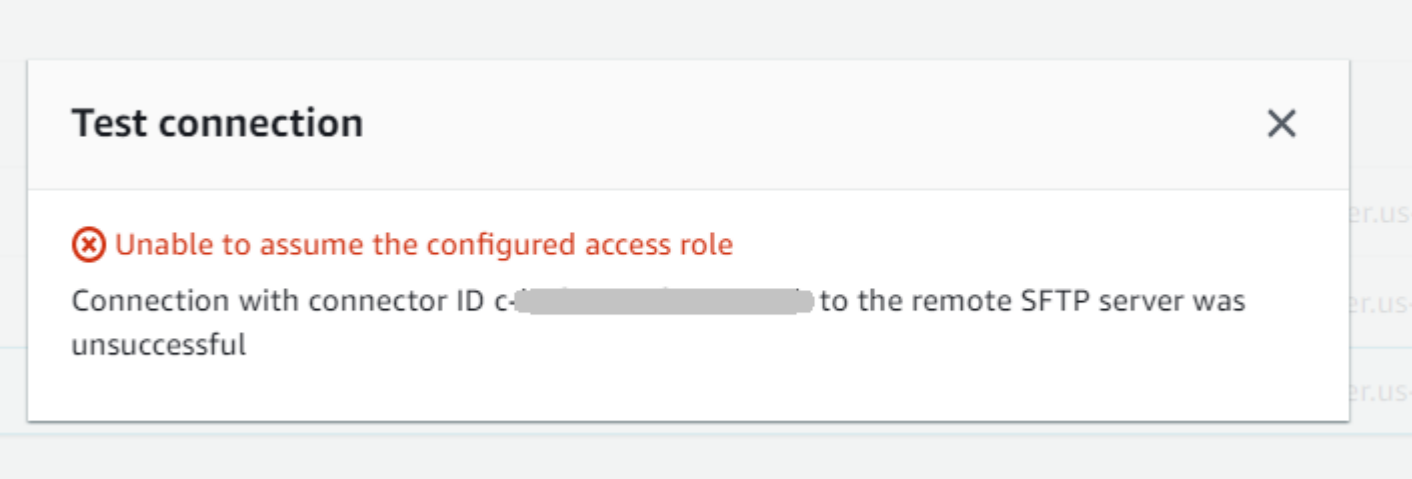
若要測試 SFTP 連接器

1. 開啟主 AWS Transfer Family 控台，[網址為 https://console.aws.amazon.com/transfer/]。
2. 在左側導覽窗格中，選擇 [連接器]，然後選取連接器。
3. 從「動作」功能表中，選擇「測試連線」。



系統返回一條消息，指示測試是通過還是失敗。如果測試失敗，系統會根據測試失敗的原因提供錯誤訊息。





> **Note**
>
> 若要使用 API 測試連接器，請參閱 TestConnectionAPI 文件。

使用 SFTP 連接器傳送和擷取檔案

SFTP 連接器可擴充與雲端和內部部署中遠端伺服器通訊的 AWS Transfer Family 功能。您可以將產生並儲存在遠端來源的資料與 AWS 託管資料倉儲整合，以進行分析、商業應用程式、報告和稽核。

若要啟動遠端 SFTP 伺服器的檔案傳輸，您可以使用 StartFileTransferAPI 作業，該作業會使用 SFTP 連接器來執行傳輸。每個`StartFileTransfer`請求可以包含 10 個不同的路徑。

您可以通過檢查服務器日誌來監視文件傳輸。連接器活動會記錄到格式為的記錄資料流`aws/transfer/`*`connector-id`*，例如`aws/transfer/c-1234567890abcdef0`。如果您看不到連接器的任何記錄檔，請確定您已指定具有連接器正確權限的記錄角色。

如需建立連接器的詳細資訊，請參閱設定 SFTP 連接器。

若要使用 SFTP 連接器傳送和擷取檔案，請使用 `start-file-transfer` AWS Command Line Interface (AWS CLI) 指令。根據您要傳送檔案 (輸出傳輸) 還是接收檔案 (入埠傳輸)，您可以指定下列參數。

- 出境轉移
  - `send-file-paths`包含一到十個來源檔案路徑，供檔案傳輸至夥伴的 SFTP 伺服器。
  - `remote-directory-path`是在客戶 SFTP 伺服器上傳送檔案的遠端路徑。
- 入境轉移
  - `retrieve-file-paths`包含一到十個遠端路徑。每個路徑都指定了一個位置，用於將檔案從合作夥伴的 SFTP 伺服器傳輸到您的 Transfer Family 伺服器。
  - `local-directory-path`是存放檔案的 Amazon S3 位置 (儲存貯體和選用前置詞)。

若要傳送檔案，請指定`send-file-paths`和`remote-directory-path`參數。您最多可以為`send-file-paths`參數指定 10 個檔案。下列範例命令會將位於 Amazon S3 儲存中名為 `/DOC-EXAMPLE-SOURCE-BUCKET/file1.txt` and `/DOC-EXAMPLE-SOURCE-BUCKET/file2.txt` 的檔案傳送到合作夥伴 SFTP 伺服器上的`/tmp`目錄。若要使用此範例指令，請以您自己*`DOC-EXAMPLE-SOURCE-BUCKET`*的值區取代。

```
aws transfer start-file-transfer --send-file-paths /DOC-EXAMPLE-SOURCE-BUCKET/
file1.txt /DOC-EXAMPLE-SOURCE-BUCKET/file2.txt \
    --remote-directory-path /tmp --connector-id c-1111AAAA2222BBBB3 --region us-east-2
```

若要接收檔案，請指定retrieve-file-paths和local-directory-path參數。*##########/my/remote/file1.txt####### SFTP ###/my/remote/file2.txt############ Amazon S3 ## /DOC/EXAMPLE-BUCKET/ ####*若要使用此範例命令，請以您自己的資訊取代 *user input placeholders*。

```
aws transfer start-file-transfer --retrieve-file-paths /my/remote/file1.txt  /my/
remote/file2.txt \
   --local-directory-path /DOC-EXAMPLE-BUCKET/prefix --connector-id c-2222BBBB3333CCCC4
 --region us-east-2
```

上述範例會指定 SFTP 伺服器上的絕對路徑。您也可以使用相對路徑：也就是說，相對於 SFTP 使用者主目錄的路徑。例如，如果 SFTP 使用者是，marymajor且他們在 SFTP 伺服器上的主目錄是/users/marymajor/，則下列指令會傳送至 /DOC-EXAMPLE-SOURCE-BUCKET/file1.txt / users/marymajor/test-connectors/file1.txt

```
aws transfer start-file-transfer --send-file-paths /DOC-EXAMPLE-SOURCE-BUCKET/file1.txt
 \
   --remote-directory-path test-connectors --connector-id c-2222BBBB3333CCCC4 --
region us-east-2
```

列出遠程目錄的內容

從遠端 SFTP 伺服器擷取檔案之前，您可以擷取遠端 SFTP 伺服器上目錄的內容。若要這麼做，您可以使用 StartDirectoryListingAPI 呼叫。

下列範例會列出遠端 SFTP 伺服器上的home資料夾內容，這是在連接器的組態中指定的。結果會放置在 Amazon S3 位置/DOC-EXAMPLE-BUCKET/connector-files，並放入名為的檔案中c-AAAA1111BBBB2222C-6666abcd-11aa-22bb-cc33-0000aaaa3333.json。

```
aws transfer start-directory-listing  \
   --connector-id c-AAAA1111BBBB2222C  \
   --output-directory-path /DOC-EXAMPLE-BUCKET/example/connector-files  \
   --remote-directory-path /home
```

此 AWS CLI 命令返回一個列表 ID 和包含結果的文件的名稱。

```
{
    "ListingId": "6666abcd-11aa-22bb-cc33-0000aaaa3333",
    "OutputFileName": "c-AAAA1111BBBB2222C-6666abcd-11aa-22bb-cc33-0000aaaa3333.json"
}
```

> **Note**
>
> 輸出檔案的命名慣例為*connector-ID*-*listing-ID*.json。

JSON 檔案包含下列資訊：

- `filePath`: 遠端檔案的完整路徑，相對於遠端伺服器上 SFTP 連接器的清單要求目錄。
- `modifiedTimestamp`: 上次修改檔案的時間，以秒為單位，國際標準時間 (UTC) 格式。此欄位為選用欄位。如果遠端檔案屬性不包含時間戳記，則會在檔案清單中省略該時間戳記。
- `size`：文件的大小，以字節為單位。此欄位為選用欄位。如果遠端檔案屬性不包含檔案大小，則會從檔案清單中省略該檔案大小。
- `path`: 遠端目錄的完整路徑，相對於遠端伺服器上 SFTP 連接器的清單要求目錄。
- `truncated`：一個標誌，指示列表輸出是否包含遠程目錄中包含的所有項目。如果您的`truncated`輸出值為 true，則可以增加可選 `max-items` input 屬性中提供的值，以便能夠列出更多項目（最多允許列表大小為 10,000 個項目）。

以下是輸出檔案 (`c-AAAA1111BBBB2222C-6666abcd-11aa-22bb-cc33-0000aaaa3333.json`) 內容的範例，其中遠端目錄包含兩個檔案和兩個子目錄 (路徑)。

```
{
    "files": [
        {
            "filePath": "/home/what.txt",
            "modifiedTimestamp": "2024-01-30T20:34:54Z",
            "size" : 2323
        },
        {
            "filePath": "/home/how.pgp",
            "modifiedTimestamp": "2024-01-30T20:34:54Z",
            "size" : 4691
```

```
        }
    ],
    "paths": [
        {
            "path": "/home/magic"
        },
        {
            "path": "/home/aws"
        },
    ],
    "truncated": "false"
}
```

管理 SFTP 連接器

本主題說明如何檢視和更新 SFTP 連接器，並列出與 SFTP 連接器相關的配額。

> **Note**
>
> 每個連接器都會自動指派靜態 IP 位址，這些 IP 位址在連接器的生命週期內保持不變。這可讓您連線至僅接受來自已知 IP 位址輸入連線的遠端 SFTP 伺服器。您的連接器會被指派一組靜態 IP 位址，這些位址由所有連接器使用相同的通訊協定 (SFTP 或 AS2) 在您的. AWS 帳戶

主題

- 更新 SFTP 連接器
- 檢視 SFTP 連接器詳細資料
- SFTP 連接器的配額

更新 SFTP 連接器

若要變更連接器的既有參數值，您可以執行update-connector指令。以下指令會更新連接器的密碼*connector-id*，在 [區域*region-id*] 中*secret-ARN*。若要使用此範例命令，請以您自己的資訊取代 *user input placeholders*。

```
aws transfer update-connector --sftp-config '{"UserSecretId":"secret-ARN"}' \
   --connector-id connector-id --region region-id
```

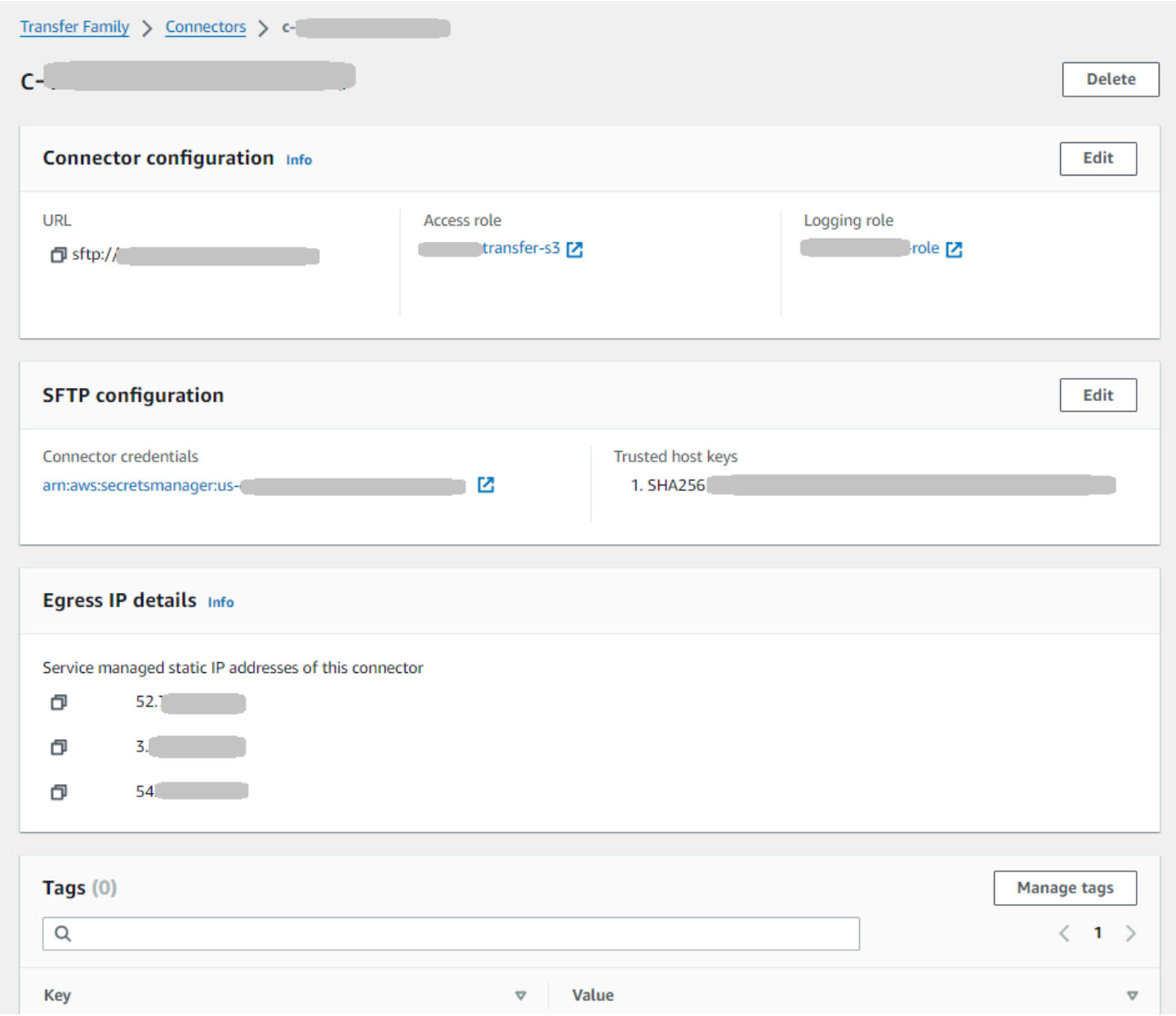
檢視 SFTP 連接器詳細資料

您可以在 AWS Transfer Family 主控台中找到 SFTP 連接器的詳細資料和內容清單。

檢視連接器詳細資料

1. 請在以下位置開啟 AWS Transfer Family 主控台。 https://console.aws.amazon.com/transfer/
2. 在左側導覽窗格中，選擇 Connectors (連接器)。
3. 在連接器識別碼資料行中選擇識別碼，以查看所選連接器的詳細資料頁面。

您可以選擇連接器詳細資料頁面上的編輯，來變更 SFTP 連接器的內容。



Note

您可以通過運行以下 AWS Command Line Interface （AWS CLI）命令獲得大部分信息，儘管格式不同。若要使用此範例命令，請以您自己的資訊取代 *user input placeholders*。

```
aws transfer describe-connector --connector-id your-connector-id
```

如需詳細資訊，請參閱 API 參考資料DescribeConnector中的。

SFTP 連接器的配額

SFTP 連接器已設定下列配額。

> **Note**
>
> SFTP 連接器的更多服務配額會列在中的AWS Transfer Family 端點和配額中Amazon Web Services 一般參考。

SFTP 連接器配額

名稱	預設	可調整
每秒測試連線交易上限 (TPS)	每個帳戶每秒 1 個請求	否
待處理檔案傳輸的佇列大小上限	1000	否
檔案大小上限	50 千兆字節 (千兆比特)	否
每個檔案的最長傳輸時間	6 小時	否
每個檔案的要求等待時間上限	6 小時	否
每個帳戶連接器的最大頻寬 (SFTP 和 AS2 連接器都有助於此值)	每秒 50 兆比特	否

為了儲存 SFTP 連接器的認證，每個密碼 Secrets Manager 碼都有關聯的配額。如果您使用相同的密鑰來存儲多種類型的密鑰，出於多種目的，您可能會遇到這些配額。

- 單一密碼的總長度：12,000 個字元
- **`Password`**字符串的最大長度：1024 個字符
- **`PrivateKey`**字符串的最大長度：8192 個字符
- **`Username`**字符串的最大長度：100 個字符

AWS Transfer Family 對於 AS2

適用性聲明 2 (AS2) 是 RFC 定義的檔案傳輸規格，其中包含強大的訊息保護和驗證機制。AS2 通訊協定對於符合性要求的工作流程至關重要，這些要求仰賴通訊協定內建資料保護和安全功能。

> **Note**
>
> Transfer Family 的 AS2 通過德拉蒙德認證。

零售業、生命科學、製造業、金融服務和公用事業等行業的客戶，依賴 AS2 進行供應鏈、物流和支付工作流程，可以使用 AWS Transfer Family AS2 端點與其業務合作夥伴進行安全交易。交易資料可在中以原生方式存取，以進 AWS 行處理、分析和機器學習。此資料也可用於與上執行的企業資源規劃 (ERP) 和客戶關係管理 (CRM) 系統的整合 AWS。使用 AS2，客戶可以大規模執行 business-to-business (B2B) 交易， AWS 同時維持現有業務合作夥伴的整合和合規性。

如果您是 Transfer Family 客戶，想要與已設定 AS2 伺服器的合作夥伴交換檔案，設定會產生一個用於加密的公開-私密金 key pair，另一組用於簽署和與合作夥伴交換公開金鑰。

Transfer Family 提供了一個您可以參加的研討會，您可以在其中配置啟用 AS2 的 Transfer Family 端點，以及 Transfer Family AS2 連接器您可以在此處查看此研討會的詳細資料。

保護傳輸中的 AS2 裝載通常涉及使用密碼編譯訊息語法 (CMS)，而且通常會使用加密和數位簽章來提供資料保護和對等驗證。已簽署的訊息處理通知 (MDN) 回應裝載可提供已收到訊息並成功解密的驗證 (不可否認)。

這些 CMS 承載和 MDN 響應的傳輸是通過 HTTP 發生的。

> **Note**
>
> 目前不支援 HTTPS AS2 伺服器端點。TLS 終止目前由客戶負責。

如需設定適用性陳述式 2 (AS2) 組態的詳細 step-by-step 逐步解說，請參閱自學課程。設定 AS2 組態

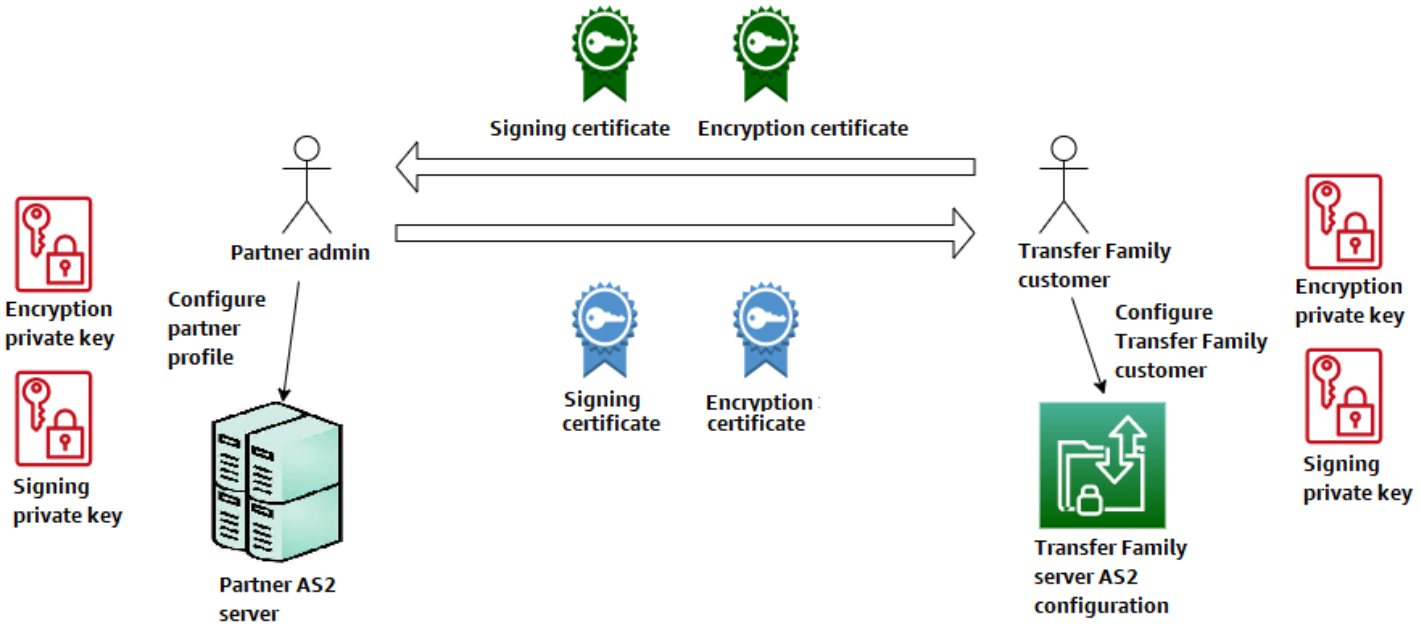
主題

- AS2 使用案例
- 配置 AS2
- 設定 AS2 連接器

- 管理 AS2 合作夥伴
- 發送和接收 AS2 消息
- 監控 AS2 使用情況

AS2 使用案例

如果您是想要與已設定 AS2 伺服器的合作夥伴交換檔案的 AWS Transfer Family 客戶，設定中最複雜的部分就是產生一個用於加密的公開-私密金 key pair，另一組用於簽署和與合作夥伴交換公開金鑰。



AWS Transfer Family 搭配 AS2 使用時，請考慮下列變化。

> **Note**
>
> 交易夥伴是與該合作夥伴設定檔相關聯的合作夥伴。
> 下表中所有 MDN 的提及都假設已簽署的 MDN。

AS2 使用案例

僅限輸入的使用案例
• 將加密的 AS2 訊息從交易夥伴傳送到 Transfer Family 伺服器。 在此情況下，請執行下列操作：

1. 為您的交易夥伴和您自己建立個人檔案。
2. 建立使用 AS2 通訊協定的 Transfer Family 伺服器。
3. 建立合約並將其新增至您的伺服器。
4. 匯入含有私密金鑰的憑證，並將其新增至您的設定檔，然後將公開金鑰匯入您的合作夥伴設定檔以進行加密。
5. 取得這些項目後，請將憑證的公開金鑰傳送給交易夥伴。

現在，您的合作夥伴可以傳送加密訊息給您，您可以將它們解密並存放在 Amazon S3 儲存貯體中。

- 將加密的 AS2 訊息從交易夥伴傳送到 Transfer Family 伺服器，並新增簽署。

  在這種情況下，您仍然只進行入站轉移作業，但現在您希望讓合作夥伴簽署他們所傳送的郵件。在此情況下，請匯入交易夥伴的簽署公開金鑰 (做為新增至合作夥伴設定檔的簽署憑證)。
- 將加密的 AS2 訊息從交易夥伴傳送到 Transfer Family 伺服器，並新增簽署和傳送 MDN 回應。

  在這種情況下，您仍然只進行入庫轉移，但是現在，除了接收已簽署的承載外，您的交易夥伴還希望收到已簽署的 MDN 回應。

  1. 匯入您的公開和私密簽署金鑰 (做為您的設定檔的簽署憑證)。
  2. 將公開簽署金鑰傳送給您的交易夥伴。

僅限輸出的使用案例

- 將加密的 AS2 訊息從 Transfer Family 伺服器傳送到交易夥伴。

  此案例與僅限輸入傳輸使用案例類似，不同之處在於您建立連接器，而不是將合約新增至 AS2 伺服器。在這種情況下，您會將交易夥伴的公開金鑰匯入他們的設定檔。
- 將加密的 AS2 訊息從 Transfer Family 伺服器傳送到交易夥伴，並新增簽署功能。

  您仍然只進行出境轉帳，但現在您的交易夥伴希望您簽署您傳送給他們的訊息。

  1. 導入您的簽名私鑰（作為添加到您的配置文件的簽名證書）。
  2. 將您的公鑰發送給交易夥伴。
- 將加密的 AS2 訊息從 Transfer Family 伺服器傳送給交易夥伴，並新增簽署並傳送 MDN 回應。

  您仍然只進行對外轉移，但是現在，除了傳送已簽署的承載外，您還希望收到交易夥伴簽署的 MDN 回應。

  1. 交易夥伴會將他們的公開簽署金鑰傳送給您。
  2. 匯入交易夥伴的公開金鑰 (作為新增至合作夥伴設定檔的簽署憑證)。

入站和出站使用案例

- 在傳輸系列伺服器與交易夥伴之間雙向傳輸加密的 AS2 訊息。

  在此情況下，請執行下列操作：

  1. 為您的交易夥伴和您自己建立個人檔案。
  2. 建立使用 AS2 通訊協定的 Transfer Family 伺服器。
  3. 建立合約並將其新增至您的伺服器。
  4. 建立連接器。
  5. 匯入含有私密金鑰的憑證，並將其新增至您的設定檔，然後將公開金鑰匯入您的合作夥伴設定檔以進行加密。
  6. 從您的交易夥伴接收公開金鑰，並將其新增至他們的設定檔以進行加密。
  7. 取得這些項目後，請將憑證的公開金鑰傳送給交易夥伴。

  現在，您和您的交易夥伴可以交換加密的消息，並且您都可以對其進行解密。您可以將收到的訊息存放在 Amazon S3 儲存貯體中，合作夥伴可以解密和存放您傳送給他們的訊息。
- 在 Transfer Family 伺服器與交易夥伴之間雙向傳輸加密的 AS2 訊息，並新增簽署功能。

  現在您和您的合作夥伴想要簽署的訊息。

  1. 導入您的簽名私鑰（作為添加到您的配置文件的簽名證書）。
  2. 將您的公鑰發送給交易夥伴。
  3. 匯入交易夥伴簽署的公開金鑰，並將其新增至他們的個人檔案。
- 在 Transfer Family 伺服器與交易夥伴之間雙向傳輸加密的 AS2 訊息，並新增簽署並傳送 MDN 回應。

  現在，您想要交換已簽署的承載，而您和交易夥伴都想要 MDN 回應。

  1. 交易夥伴會將他們的公開簽署金鑰傳送給您。
  2. 匯入交易夥伴的公開金鑰 (作為合作夥伴設定檔的簽署憑證)。
  3. 將您的公鑰發送給您的交易夥伴。

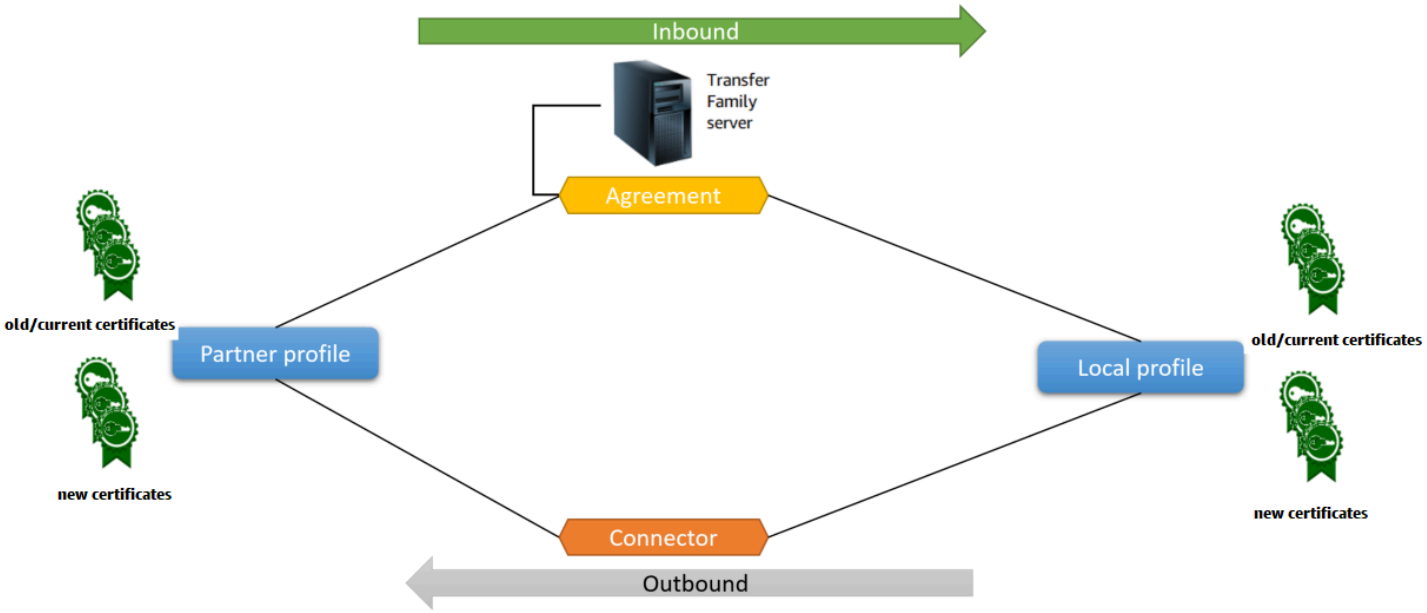
配置 AS2

若要建立啟用 AS2 的伺服器，您還必須指定下列元件：

- 協議 — 雙邊貿易夥伴協議或合作夥伴關係，定義了交換消息（文件）的雙方之間的關係。為了定義合約，Transfer Family 會結合伺服器、本機設定檔、合作夥伴設定檔和憑證資訊。Transfer Family AS2-入埠處理使用協議。
- 憑證 — 公用金鑰 (X.509) 憑證用於 AS2 通訊，以進行訊息加密和驗證。憑證也可用於連接器端點。
- 本機設定檔和合作夥伴設定檔 — 本機設定檔會定義本機 (啟用 AS2 的 Transfer Family 伺服器) 組織或「對象」。同樣地，合作夥伴設定檔定義了「Transfer Family」外部的遠端夥伴組織。

雖然並非所有啟用 AS2 的伺服器都需要，但對於輸出傳輸，您需要一個連接器。連接器會擷取輸出連線的參數。需要連接器才能將檔案傳送至客戶的外部非 AWS 伺服器。

下圖顯示了入站和出站處理程序中所涉及的 AS2 物件之間的關係。



如需 AS2 組態的 end-to-end 範例，請參閱設定 AS2 組態。

主題

- 使用 Transfer Family 列主控台建立 AS2 伺服器
- 使用範本建立示範 Transfer Family AS2 堆疊
- AS2 配置和配額
- AS2 特色與功能

使用 Transfer Family 列主控台建立 AS2 伺服器

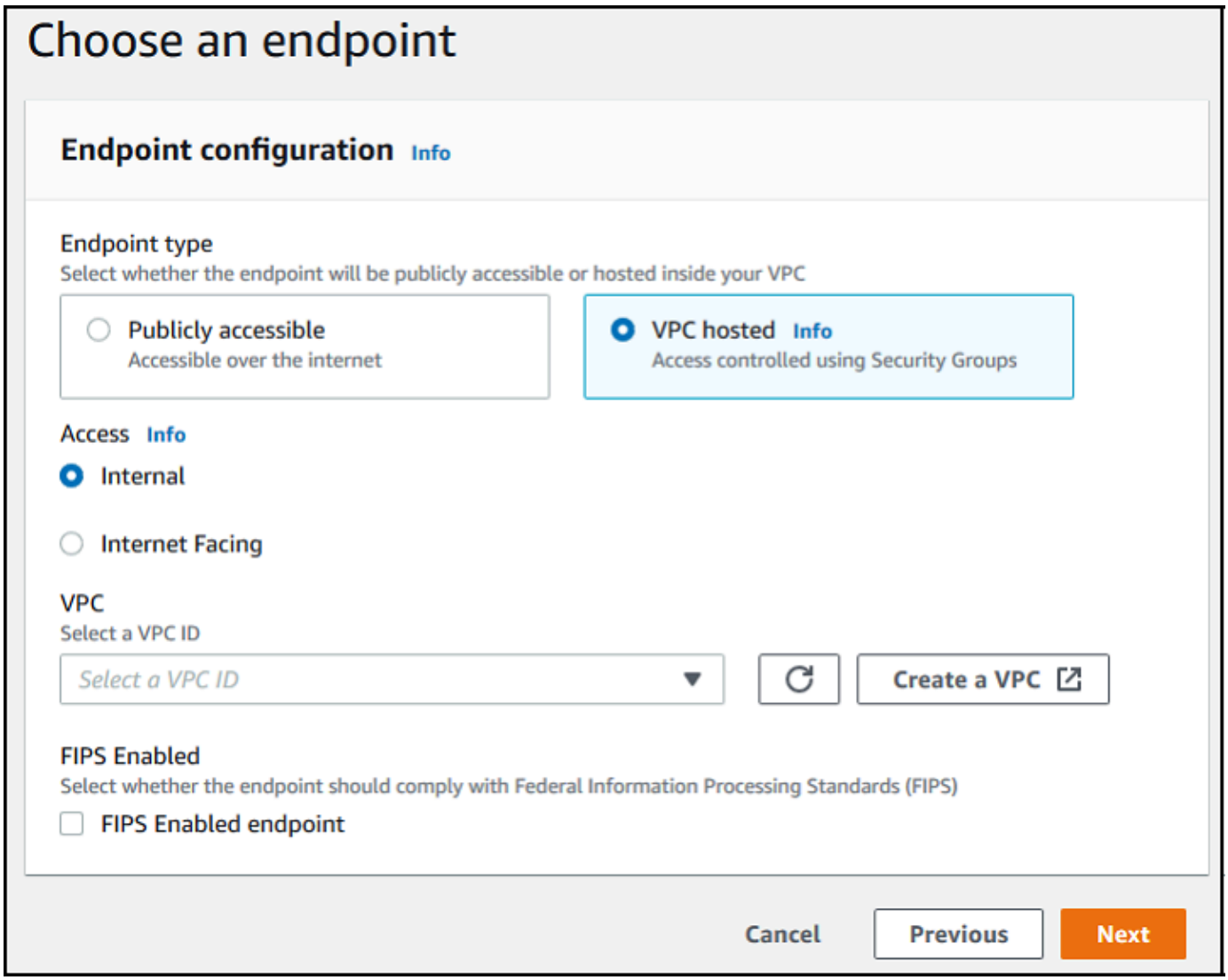
此程序說明如何使用「Transfer Family」主控台建立啟用 AS2 的伺服器。如果您想要 AWS CLI 改用，請參閱the section called “步驟 2：建立使用 AS2 通訊協定的 Transfer Family 伺服器”。

若要建立啟用 AS2 的伺服器

1. 開啟主 AWS Transfer Family 控台，網址為 https://console.aws.amazon.com/transfer/。
2. 在左側導覽窗格中，選擇 [伺服器]，然後選擇 [建立伺服器]。
3. 在 [選擇通訊協定] 頁面上，選取 AS2 (適用性陳述式 2)，然後選擇 [下一步]。
4. 在 [選擇身分識別提供者] 頁面上選擇 [下一步]。

> **Note**
>
> 對於 AS2，您無法選擇身分識別提供者，因為 AS2 通訊協定不支援基本驗證。而是透過虛擬私有雲 (VPC) 安全性群組控制存取權。

5. 在 [選擇端點] 頁面上，執行下列動作：



a. 對於端點類型，請選擇託管服務器端點的 VPC 託管。如需有關設定 VPC 託管端點的資訊，請參閱。[在虛擬私有雲中建立伺服器]

> **Note**
>
> AS2 通訊協定不支援可公開存取的端點。若要讓您的 VPC 端點可透過網際網路存取，請在 [存取] 下選擇 [網際網路對向]，然後提供您的彈性 IP 位址。

b. 針對 [存取]，選擇下列其中一個選項：

- 內部 — 選擇此選項可從 VPC 和虛擬私人雲端連線環境 (例如透過內部部署資料中心或 VPN) 提供存取權。 AWS Direct Connect

- 網際網路對接 — 選擇此選項可透過網際網路以及從 VPC 和虛擬私人雲端連線環境 (例如透過內部部署資料中心或 VPN) 提供存取權。 AWS Direct Connect

  如果您選擇「網際網路對接」，請在出現提示時提供彈性 IP 位址。

c. 對於 VPC，請選擇現有的 VPC，或選擇「建立 VPC」以建立新的 VPC。

d. 對於 FIPS 已啟用，請保持清除 FIPS 啟用端點核取方塊。

> **Note**
>
> AS2 通訊協定不支援啟用 FIPS 的端點。

e. 選擇下一步。

6. 在 [選擇網域] 頁面上，選擇 Amazon S3，使用選取的通訊協定以物件形式存放和存取檔案。

   選擇下一步。

7. 在 [設定其他詳細資料] 頁面上，選擇您需要的設定。

> **Note**
>
> 如果您要與 AS2 一起設定任何其他通訊協定，則會套用所有其他詳細資料設定。不過，對於 AS2 通訊協定，唯一套用的設定是 [CloudWatch 記錄] 和 [標籤] 區段中的設定。
> 雖然設定 CloudWatch 記錄角色是選擇性的，我們強烈建議您進行設定，以便您可以查看訊息的狀態並疑難排解組態問題。

8. 在「檢閱並建立」頁面上，檢閱您的選擇，以確定選項正確無誤。

   - 如果您要編輯任何設定，請在您要變更的步驟旁邊選擇 「編輯」。

   > **Note**
   >
   > 如果您編輯步驟，建議您在選擇要編輯的步驟後檢閱每個步驟。

   - 如果您沒有變更，請選擇 [建立伺服器] 來建立伺服器。您會前往顯示下列內容的 Servers (伺服器) 頁面，這裡會列出您的新伺服器。

     新伺服器的狀態變更為「線上」可能需要幾分鐘的時間。此時，您的伺服器會執行您使用者的檔案操作。

使用範本建立示範 Transfer Family AS2 堆疊

我們提供了一個獨立的 AWS CloudFormation 模板，以快速創建啟用 AS2 的 Transfer Family 服務器。範本使用公有 Amazon VPC 端點、憑證、本機和合作夥伴設定檔、協議和連接器來設定伺服器。

使用此範本之前，請注意下列事項：

- 如果您使用此範本建立堆疊，則需支付所使用 AWS 資源的費用。
- 範本會建立多個憑證，並將它們放入 AWS Secrets Manager 以安全地儲存。您可以視需要從 Secrets Manager 刪除這些憑證，因為您需要支付使用此服務的費用。刪除 Secrets Manager 中的這些憑證並不會從 Transfer Family 伺服器中刪除這些憑證。因此，示範堆疊的功能不會受到影響。不過，對於要搭配生產 AS2 伺服器使用的憑證，您可能會想要使用 Secrets Manager 來管理和定期輪換儲存的憑證。
- 我們建議您僅使用模板作為基礎，主要用於演示目的。如果您想要在生產環境中使用此示範堆疊，建議您修改範本的 YAML 程式碼，以建立更強大的堆疊。例如，建立生產層級憑證，並建立可在生產環境中使用的 AWS Lambda 函數。

從樣板建立已啟用 AS2 的 Transfer Family 伺服器的步驟 CloudFormation

1. 開啟主 AWS CloudFormation 控台，網址為 https://console.aws.amazon.com/cloudformation。
2. 在左側導覽窗格中，選擇 Stacks (堆疊)。
3. 選擇 Create stack (建立堆疊)，然後選擇 With new resources (standard) (使用新資源 (標準))。
4. 在 [先決條件-準備範本] 區段中，選擇 [範本已就緒]。
5. 複製此連結 AS2 示範範本，並將其貼到 Amazon S3 URL 欄位中。
6. 選擇下一步。
7. 在 [指定堆疊詳細資料] 頁面上，命名您的堆疊，然後指定下列參數：
   - 在 AS2 下，輸入本機 AS2 ID 和夥伴 AS2 ID 的值，或分別接受預設值`local`和`partner`。
   - 在 [網路] 下，輸入 [安全性群組輸入 CIDR IP] 的值，或接受預設值。`0.0.0.0/0`

   > **Note**
   >
   > 此值 (以 CIDR 格式表示) 指定允許傳入 AS2 伺服器的流量使用哪些 IP 位址。預設值允許所有 IP 位址。`0.0.0.0/0`

- 在「一般」下，輸入「字首」的值，或接受預設值`transfer-as2`。此前綴放置在由堆棧創建的任何資源名稱之前。例如，如果您使用預設前綴，則會命名您的 Amazon S3 儲存貯體`transfer-as2-`*`TransferS3BucketName`*。

8. 選擇下一步。在 [設定堆疊選項] 頁面上，再次選擇 [下一步]。
9. 檢閱您要建立之堆疊的詳細資料，然後選擇 [建立堆疊]。

> **Note**
>
> 在頁面底部的「功能」下，您必須確認 AWS CloudFormation 可能會建立 AWS Identity and Access Management (IAM) 資源。

堆疊建立之後，您可以使用 AWS Command Line Interface (AWS CLI) 將測試 AS2 訊息從合作夥伴伺服器傳送到您的本機 Transfer Family 伺服器。用於發送測試消息的示例 AWS CLI 命令與堆棧中的所有其他資源一起創建。

要使用此示例命令，請轉到堆棧的「輸出」選項卡，然後復制 TransferExampleAs2Command。然後，您可以使用執行命令 AWS CLI。如果您尚未安裝 AWS CLI，請參閱《使用指南》 AWS CLI中的〈安裝或更新最新版本的AWS Command Line Interface〉。

範例命令的格式如下：

```
aws s3api put-object --bucket TransferS3BucketName --key test.txt && aws transfer
 start-file-transfer --region aws-region --connector-id TransferConnectorId --send-
file-paths /TransferS3BucketName/test.txt
```

> **Note**
>
> 您的這個命令版本包含堆疊中*TransferS3BucketName*和*TransferConnectorId*資源的實際值。

此範例命令由兩個單獨的指令組成，這些指令會使用&&字串連在一起。

第一個命令會在值區中建立新的空白文字檔案：

```
aws s3api put-object --bucket TransferS3BucketName --key test.txt
```

然後，第二個命令會使用連接器，將檔案從夥伴設定檔傳送到本機設定檔。Transfer Family 伺服器已設定合約，允許本機設定檔接受來自合作夥伴設定檔的訊息。

```
aws transfer start-file-transfer --region aws-region --connector-id TransferConnectorId
 --send-file-paths /TransferS3BucketName/test.txt
```

執行命令後，您可以前往 Amazon S3 儲存貯體 (*TransferS3BucketName*) 並檢視內容。如果命令成功，您應該會在值區中看到下列物件：

- `processed/`— 此文件夾包含描述傳輸文件和 MDN 響應的 JSON 文件。
- `processing/`— 此資料夾會暫時包含正在處理的檔案，但傳輸完成後，此資料夾應為空白。
- *server-id*/— 此文件夾是根據您的 Transfer Family 服務器 ID 命名. 它包含`from-`*partner*（此文件夾是根據合作夥伴的 AS2 ID 動態命名），該文件夾本身包含 `failed/processed/`，和文件`processing/`夾。該文件/*server-id*/`from-`*partner*/`processed/`夾包含傳輸的文本文件的副本，以及相應的 JSON 和 MDN 文件。
- `test.txt`— 該對象是已傳送的（空）文件。

AS2 配置和配額

本主題說明使用適用性陳述式 2 (AS2) 通訊協定的移轉所支援的組態、功能和功能，包括接受的加密和摘要。本節也說明 AS2 傳輸的限制和已知問題。

主題

- AS2 支援的組態
- AS2 配額與限制

AS2 支援的組態

簽署、加密、壓縮、MDN

對於入庫和出站轉移作業，下列項目為必要或選擇性項目：

- 加密 — 必要 (HTTP 傳輸，這是目前支援的唯一傳輸方法)。僅當 TLS 終止 Proxy (例如 Application Load Balancer (ALB) 轉寄且標頭存在時，才會接受未加密的訊息。`X-Forwarded-Proto: https`
- 簽署 — 選擇性
- 壓縮 — 選用 (目前唯一支援的壓縮演算法為 ZLIB)

- 訊息處理通知 (MDN) — 選擇性

密码

輸入和出站轉移都支援下列密碼：

- 亚洲
- 俄羅斯
- 西 256_C
- 3DES (僅用於向後相容性)

消化

支持以下摘要：

- 入埠簽署和 MDN — 沙 1, SHA256, SHA384, SHA512
- 輸出簽署與 MDN — 沙 1、SHA256、SHA384、SHA512

MDN

對於 MDN 回應，支援某些類型，如下所示：

- 入站傳輸 — 同步和非同步
- 出站傳輸 — 僅同步
- 簡易郵件傳送通訊協定 (SMTP) (電子郵件 MDN) — 不支援

運輸

- 輸入傳輸 — HTTP 是目前唯一支援的傳輸，您必須明確指定。

> **Note**
>
> 如果您需要使用 HTTPS 進行輸入傳輸，可以在應用程式負載平衡器或 Network Load Balancer 上終止 TLS。這在中有所描述透過 HTTPS 接收 AS2 訊息。

- 輸出傳輸 — 如果您提供 HTTP URL，則還必須指定加密演算法。如果您提供 HTTPS 網址，您可以選擇為加密演算法指定「無」。

AS2 配額與限制

本節討論 AS2 的配額與限制

主題

- 配額
- 處理密碼的配額
- 已知限制

配額

AS2 檔案傳輸的配額如下。若要要求增加可調整的AWS 服務 配額，請參閱 AWS 一般參考.

配額

名稱	預設	可調整
每秒接收的入埠檔案數目上限	100	否
每秒傳送的輸出檔案數目上限	100	否
同時輸入檔案的最大數目	400	否
同時輸出檔案的最大數目	400	否
輸入檔案大小上限 (未壓縮)	1 GB	否
輸出檔案大小上限 (未壓縮)	1 GB	否
每個輸出要求的檔案數目上限	10	否
每秒輸出要求數目上限	100	否
每秒輸入要求數目上限	100	否
每個帳戶的最大輸出頻寬 (輸出 SFTP 和 AS2 要求都有助於此值)	每秒 50 MB	否
每部伺服器的合約數目上限	100	是

名稱	預設	可調整
每個帳戶的連接器數目上限 (SFTP 和 AS2 連接器都有助於此限制)	100	是
每個合作夥伴設定檔的最大憑證數	10	否
每個帳戶的最大憑證數	1000	是
每個帳戶的最大合作夥伴設定檔數	1000	是

處理密碼的配額

AWS Transfer Family 代表使用基本驗證的 AS2 客戶撥打電話。 AWS Secrets Manager 此外，Secrets Manager 會撥打電話給 AWS KMS。

> **Note**
>
> 這些配額不是特定於您對 Transfer Family 使用的機密：它們會在您的所有服務之間共用 AWS 帳戶。

對於 Secrets Manager`GetSecretValue`，套用的配額為合併率 DescribeSecret 和 GetSecretValue API 要求，如AWS Secrets Manager 配額中所述。

Secrets Manager **`GetSecretValue`**

名稱	值	描述
DescribeSecret 和 GetSecret Value API 請求的綜合速率	每個支援的區域：每秒 1 萬個	DescribeSecret 和 GetSecret Value API 請求的每秒最大交易量合計。

對於 AWS KMS，下列配額適用於`Decrypt`。如需詳細資訊，請參閱每個 AWS KMS API 作業的要求配額

AWS KMS **`Decrypt`**

配額名稱	預設值 (每秒請求數)

密碼編譯作業 (對稱) 要求率	這些共用配額會隨要求中使用的 AWS KMS 金鑰 AWS 區域 和類型而有所不同。每個配額會分別計算。
	• 5,500 (共用)
	• 下列區域中為 10,000 (共享)：
	  • 美國東部 (俄亥俄)，us-east-2
	  • 亞太區域 (新加坡) ap-southeast-1
	  • 亞太區域 (雪梨)，ap-southeast-2
	  • 亞太區域 (東京)，ap-northeast-1
	  • 歐洲 (法蘭克福)，eu-central-1
	  • 歐洲 (倫敦)，eu-west-2
	• 下列區域中為 50,000 (共用)：
	  • 美國東部 (維吉尼亞北部)，us-east-1
	  • 美國西部 (奧勒岡)，us-west-2
	  • 歐洲 (愛爾蘭)，eu-west-1

自訂金鑰存放區請求配額 **Note** 只有在您使用外部金鑰存放區時，才會套用此配額。	每個自訂金鑰存放區的自訂金鑰存放區要求配額會個別計算。 • 每個 AWS CloudHSM 金鑰存放區有 1,800 個 (共用) • 每個外部金鑰存放區 1800 個 (共用)

已知限制

- 不支援伺服器端 TCP 保持活動狀態。除非用戶端傳送持續使用中封包，否則連線會在 350 秒閒置後逾時。
- 若要讓服務接受並顯示在 Amazon CloudWatch 日誌中的有效協議，訊息必須包含有效的 AS2 標頭。

- 從 AWS Transfer Family AS2 接收訊息的伺服器必須支援密碼編譯訊息語法 (CMS) 演算法保護屬性，以驗證郵件簽章，如 RFC 6211 中所定義。某些舊的 IBM 英鎊產品不支援此屬性。
- 重複的郵件 ID 會導致處理/警告：重複的文件訊息。
- AS2 憑證的金鑰長度必須至少為 2048 位元，且最多為 4096 個。
- 傳送 AS2 訊息或非同步 MDN 至交易夥伴的 HTTPS 端點時，訊息或 MDN 必須使用由公開信任憑證授權單位 (CA) 簽署的有效 SSL 憑證。自我簽署憑證目前僅支援輸出傳輸。
- 端點必須支援 TLS 1.2 版通訊協定和安全性原則允許的密碼編譯演算法 (如中所述AWS Transfer Family 伺服器的安全性原則)。
- 目前不支援 AS2 1.2 版中的多個附件和憑證交換訊息 (CEM)。
- 基本驗證目前僅支援輸出郵件。

AS2 特色與功能

下表列出可用於使用 AS2 的「Transfer Family」資源的功能和功能。

AS2 功能

Transfer Family 列為 AS2 提供以下功能。

功能	支持者 AWS Transfer Family
德拉蒙德認證	是
AWS CloudFormation 支持	是
Amazon CloudWatch 指標	是
SHA-2 加密算法	是
Support Amazon S3	是
Support Amazon EFS	否
排程訊息	是
AWS Transfer Family 管理工作流	否
憑證交換訊息 (CEM)	否

功能	支持者 AWS Transfer Family
相互 TLS (MTL)	否
Support 自我簽署憑證	是

1. 使用 Amazon 的排程 AWS Lambda 功能提供輸出排程訊息 EventBridge

AS2 傳送和接收功能

下表提供 AWS Transfer Family AS2 傳送和接收功能的清單。

功能	入埠：使用伺服器接收	輸出：使用連接器傳送
TLS 加密傳輸	是[1]	是
非 TLS 傳輸 (HTTP)	是	是[2]
同步 MDN	是	是
訊息壓縮	是	是
非同步 MDN	是	否
靜態 IP 位址	是	是
攜帶您自己的 IP 位址	是	否
多個檔案附件	否	否
基本驗證	否	是
AS2 重新啟動	不適用	否
AS2 可靠性	否	否
每封郵件的自訂主旨	不適用	否

1. Network Load Balancer (NLB) 提供的輸入 TLS 加密傳輸

2. 只有在啟用加密時才能使用輸出非 TLS 傳輸

設定 AS2 連接器

連接器的目的在於建立交易夥伴之間的輸出傳輸關係 — 將 AS2 檔案從 Transfer Family 伺服器傳送到外部合作夥伴擁有的目的地。對於連接器，您可以指定本機對象、遠端夥伴及其憑證 (透過建立本機和夥伴設定檔)。

建立連接器之後，您就可以將資訊傳輸給您的交易夥伴。每個 AS2 伺服器都會指派三個靜態 IP 位址。AS2 連接器會使用這些 IP 位址，透過 AS2 傳送非同步 MDN 給您的交易夥伴。

> **Note**
>
> 交易夥伴收到的訊息大小與 Amazon S3 中的物件大小不符。發生這種差異的原因是 AS2 消息在發送之前將文件包裝在信封中。因此，即使以壓縮方式發送文件，文件大小也可能會增加。因此，請確定交易夥伴的檔案大小上限大於您傳送的檔案大小。

建立 AS2 連接器

此程序說明如何使用 AWS Transfer Family 主控台建立 AS2 連接器。如果您想要 AWS CLI 改用，請參閱the section called “步驟 6：在您和合作夥伴之間建立連接器”。

建立 AS2 連接器的步驟

1. 請在以下位置開啟 AWS Transfer Family 主控台。 https://console.aws.amazon.com/transfer/
2. 在左側導覽窗格中，選擇 [連接器]，然後選擇 [建立連接器]。
3. 在 [連接器組態] 區段中，指定下列資訊：

   - URL — 輸入輸出連線的 URL。
   - 存取角色 — 選擇要使用的 (IAM) 角色的 Amazon 資源名稱 AWS Identity and Access Management (ARN)。`StartFileTransfer`請確定此角色提供對要求中所使用之檔案位置之父目錄的讀取和寫入存取權。此外，請確定角色提供對您要傳送之檔案之父目錄的讀取和寫入存取權`StartFileTransfer`。

     > **Note**
     >
     > 如果您對連接器使用基本驗證，則存取角色需要密碼的`secretsmanager:GetSecretValue`權限。如果使用客戶管理的金鑰而不是 AWS 受管金鑰 in 來加密密碼 AWS Secrets Manager，則該角色也需要該金鑰

的kms:Decrypt權限。如果您使用前置詞命名密碼aws/transfer/，則可以使用萬用字元 (*) 新增必要的權限，如建立密碼的範例權限所示。

- 記錄角色 (選用) — 選擇連接器的 IAM 角色，以用來將事件推送至 CloudWatch 記錄。

4. 在 AS2 設定區段中，選擇本機和合作夥伴設定檔、加密和簽署演算法，以及是否壓縮傳輸的資訊。注意下列事項：

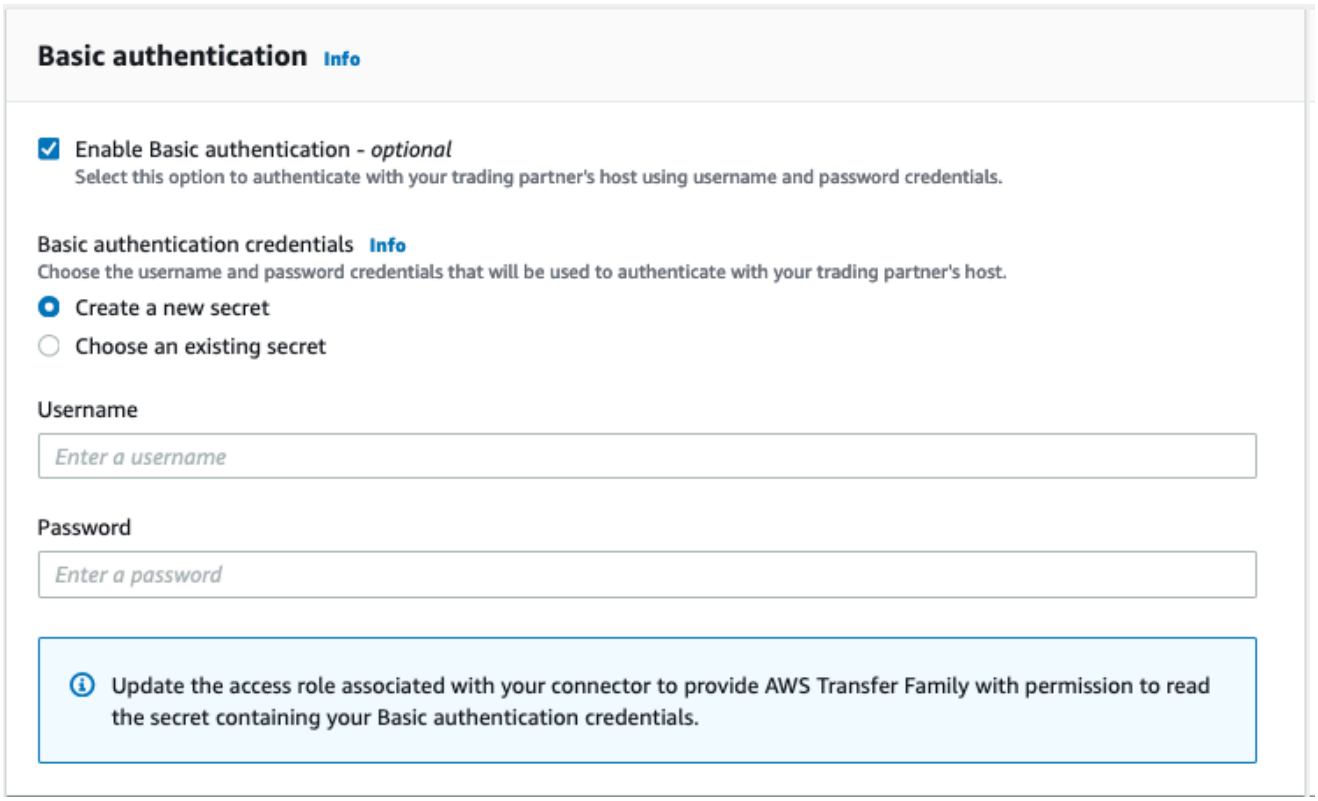
   - 對於加密演算法，DES_EDE3_CBC除非您必須支援需要此演算法的舊版用戶端，否則請勿選擇，因為它是弱式加密演算法。
   - 主旨是當做隨連接器一起傳送之 AS2 郵件中的 subject HTTP 標頭屬性使用。
   - 如果您選擇建立不含加密演算法的連接器，則必須指定HTTPS為您的通訊協定。

5. 在 MDN 組態段落中，指定下列資訊：

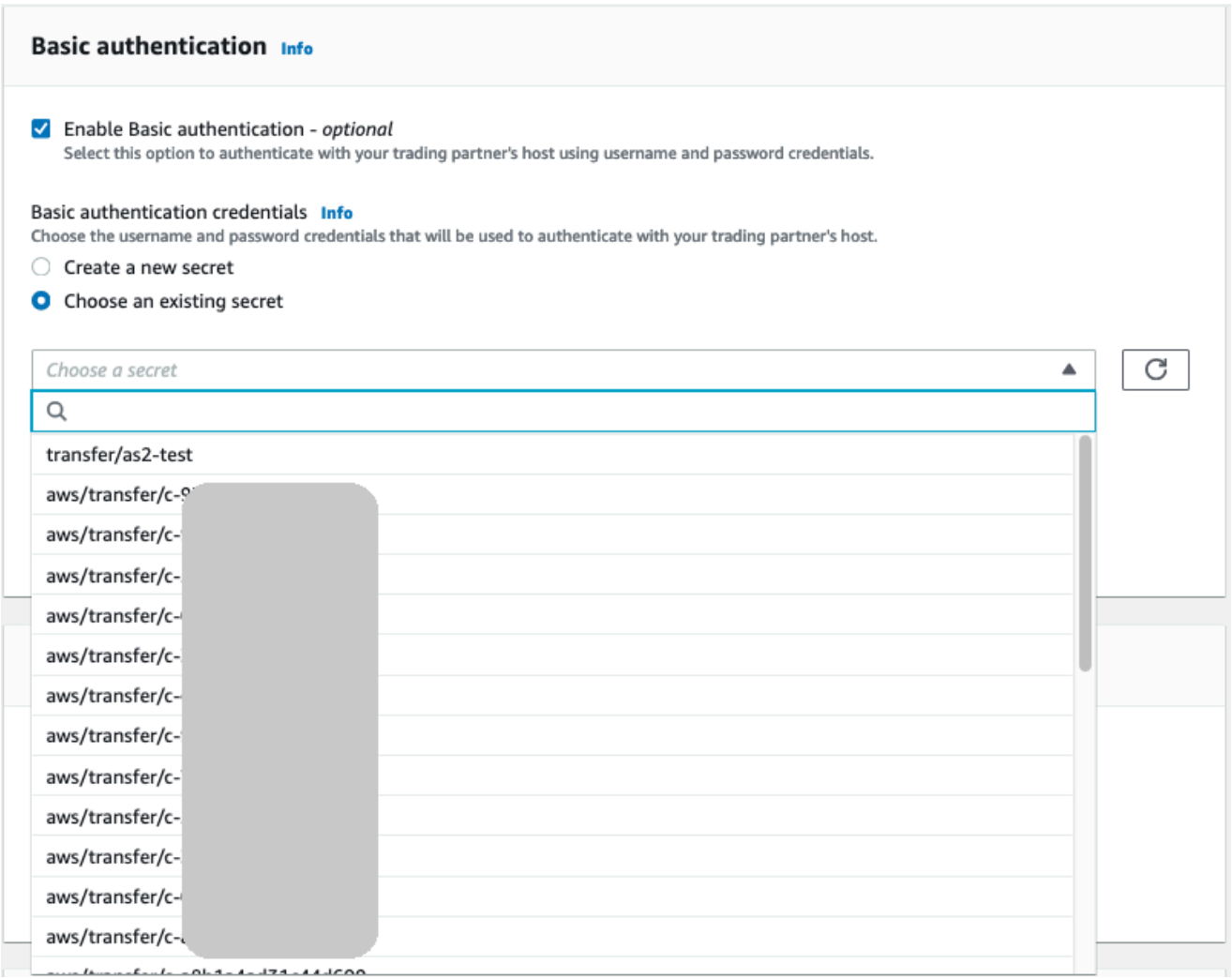
   - 申請 MDN — 您可以選擇要求您的交易夥伴在 AS2 成功收到您的訊息後，向您發送 MDN。
   - 已簽署的 MDN — 您可以選擇要求簽署 MDN。只有在您已選取要求 MDN 時，才能使用此選項。

6. 在 [基本驗證] 區段中，指定下列資訊。

   - 若要傳送登入認證以及輸出郵件，請選取啟用基本驗證。如果您不想傳送任何包含輸出郵件的認證，請將啟用基本驗證保持清除狀態。
   - 如果您使用驗證，請選擇或建立密碼。
     - 若要建立新密碼，請選擇 [建立新密碼]，然後輸入使用者名稱和密碼。這些認證必須與連線至合作夥伴端點的使用者相符。



- 若要使用現有的密碼，請選擇 [選擇現有密碼]，然後從下拉式功能表中選擇密碼。如需在 Secret Manager 中建立格式正確密碼的詳細資訊，請參閱啟用 AS2 連接器的基本驗證。



7. 確認所有設定後，請選擇 [建立連接器] 以建立連接器。

[連接器] 頁面隨即出現，並將新連接器的 ID 新增至清單。若要檢視連接器的詳細資料，請參閱檢視 AS2 連接器詳細資訊。

AS2 連接器演算法

當您建立 AS2 連接器時，連接器會附加下列安全性演算法。

Type	演算法
TLS 密碼	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

Type	演算法
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

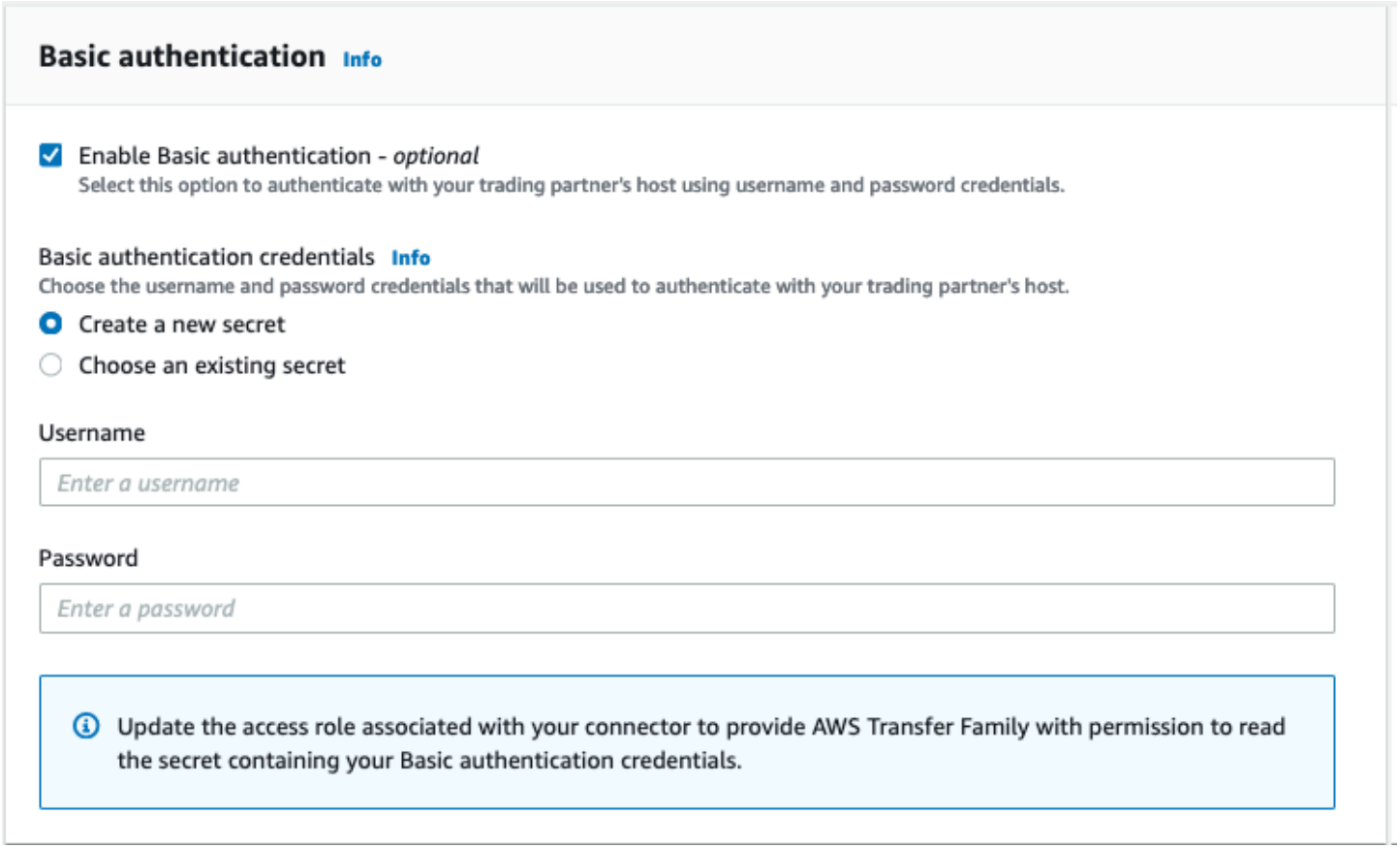
AS2 連接器的基本驗證

當您建立或更新使用 AS2 通訊協定的 Transfer Family 伺服器時，您可以為輸出郵件新增基本驗證。您可以透過將驗證資訊新增至連接器來執行此操作。

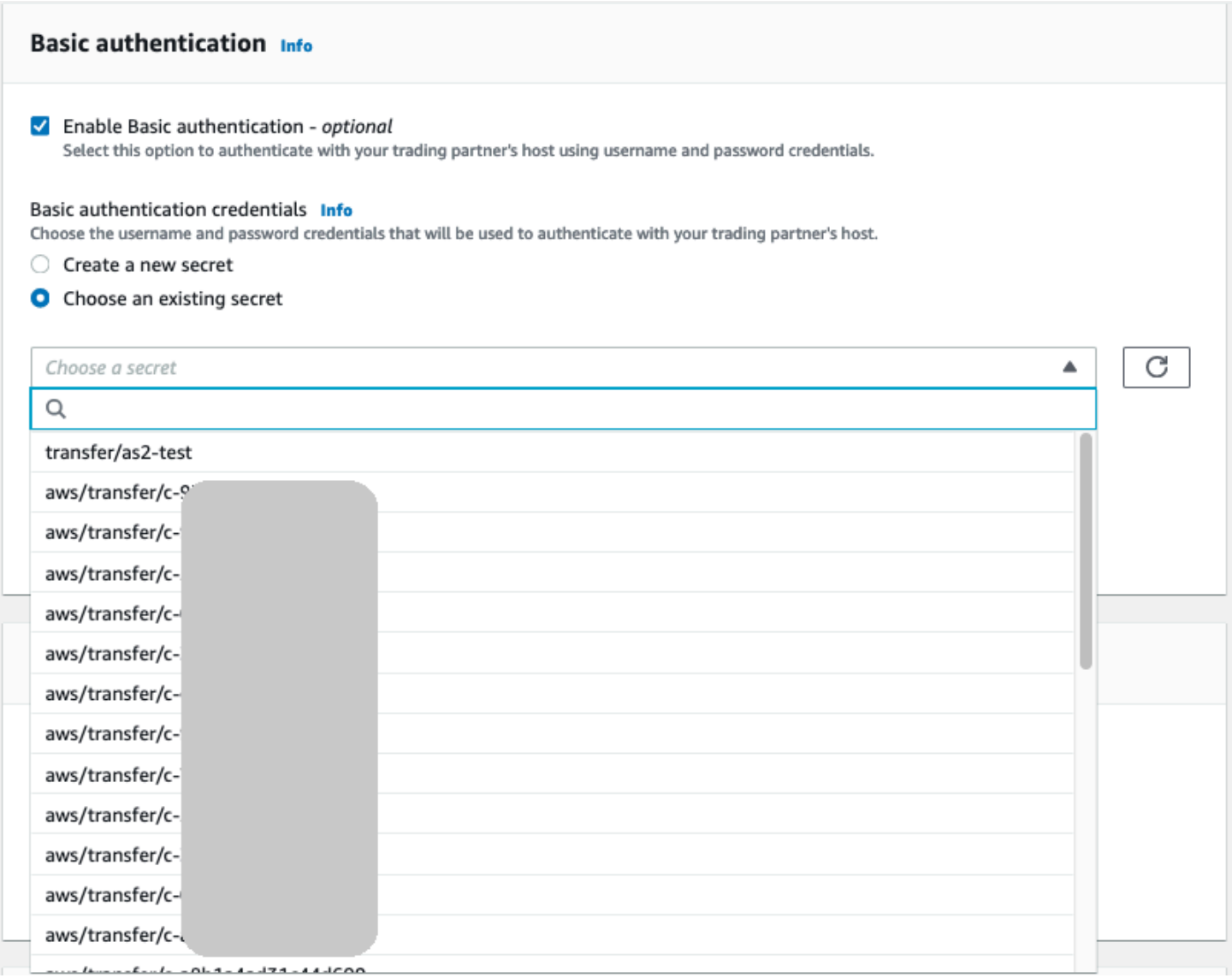
> **Note**
>
> 只有在您使用 HTTPS 時，才能使用基本驗證。

若要使用連接器的驗證，請在 [基本驗證] 區段中選取 [啟用基本驗證]。啟用基本驗證後，您可以選擇建立新密碼或使用現有密碼。在任何一種情況下，密碼中的認證都會與使用此連接器的輸出郵件一起傳送。憑證必須與嘗試連線至交易夥伴遠端端點的使用者相符。

下列螢幕擷取畫面顯示 [選取啟用基本驗證] 和 [建立新密碼]。完成這些選擇後，您可以輸入密碼的使用者名稱和密碼。



下列螢幕擷取畫面顯示 [啟用基本驗證已選取] 和 [選擇選取的現有密碼] 您的密碼必須使用正確的格式，如中所述[啟用 AS2 連接器的基本驗證](#)。



啟用 AS2 連接器的基本驗證

當您為 AS2 連接器啟用基本驗證時，您可以在 Transfer Family 主控台中建立新密碼，也可以使用在中 AWS Secrets Manager建立的密碼。在任何一種情況下，您的密碼都會儲存在 Secrets Manager 中。

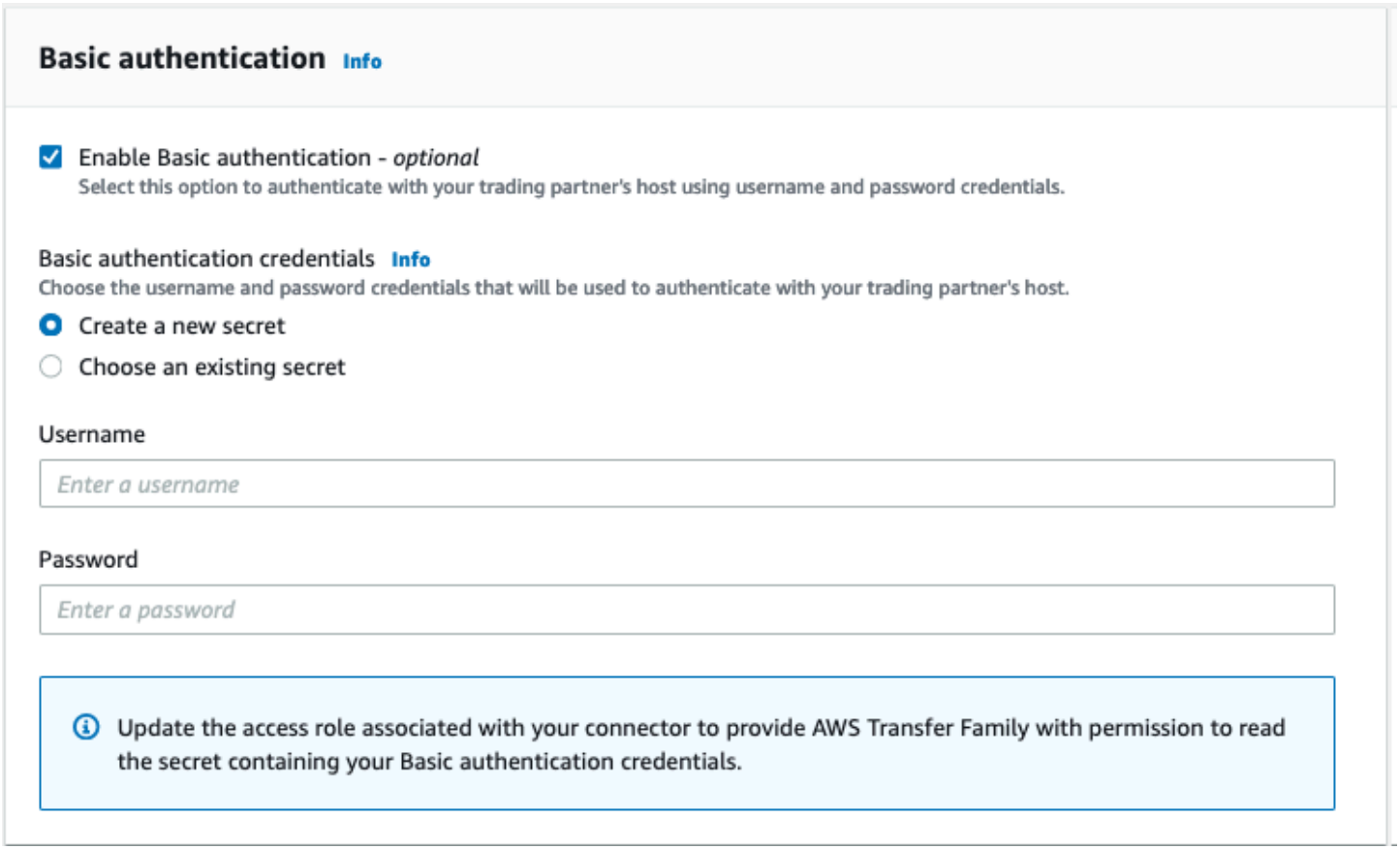
主題

- 在主控台中建立新密碼
- 使用現有的 密碼
- 在中建立密碼 AWS Secrets Manager

在主控台中建立新密碼

在主控台中建立連接器時，您可以建立新密碼。

若要建立新密碼，請選擇 [建立新密碼]，然後輸入使用者名稱和密碼。這些認證必須與連線至合作夥伴端點的使用者相符。

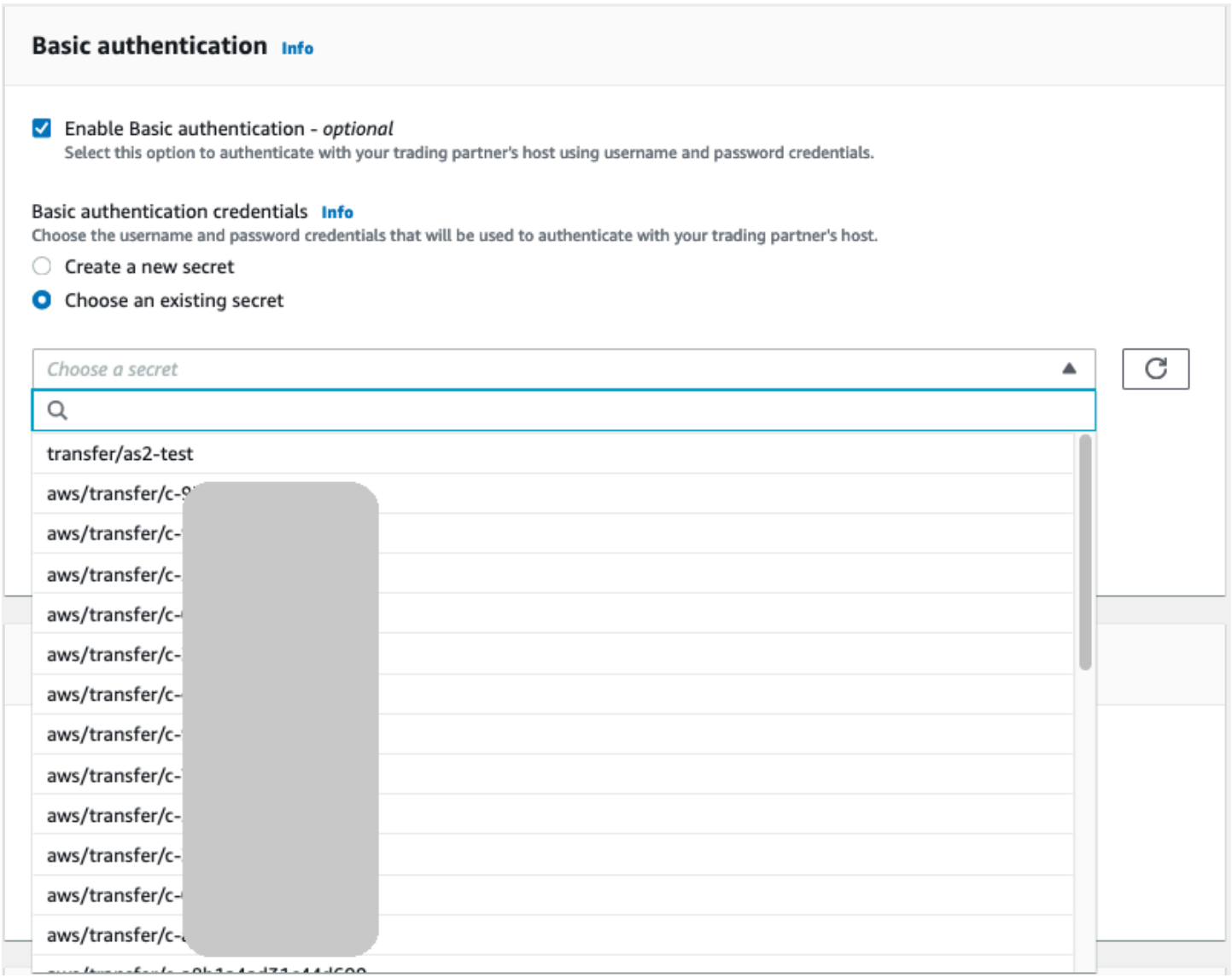


> **Note**
>
> 當您在主控台中建立新密碼時，密碼的名稱會遵循以下命名慣例：**`/aws/transfer/`*`connector-id`***，其中 *`Connector-id`* 是您所建立之連接器的識別碼。當您嘗試在中找到密碼時，請考慮這一點 AWS Secrets Manager。

使用現有的 密碼

在主控台中建立連接器時，您可以指定現有的密碼。

若要使用現有的密碼，請選擇 [選擇現有密碼]，然後從下拉式功能表中選擇密碼。如需在 Secret Manager 中建立格式正確密碼的詳細資訊，請參閱在中建立密碼 AWS Secrets Manager。



在中建立密碼 AWS Secrets Manager

下列程序說明如何建立與 AS2 連接器搭配使用的適當密碼。

> **Note**
>
> 只有在您使用 HTTPS 時，才能使用基本驗證。

將使用者認證儲存在 Secrets Manager 中以進行 AS2 基本驗證

1. 請登入 AWS Management Console 並開啟 AWS Secrets Manager 主控台，網址為 https://console.aws.amazon.com/secretsmanager/。

2. 在左側導覽窗格中，選擇秘密。
3. 在「密碼」頁面上，選擇「儲存新密碼」。
4. 在 [選擇密碼類型] 頁面上，對於 [密碼類型]，選擇 [其他密碼類型]。
5. 在「鍵/值對」區段中，選擇「鍵/值」標籤。
   - 鍵-輸入**Username**。
   - value — 輸入獲得授權可連線至合作夥伴伺服器的使用者名稱。
6. 如果您要提供密碼，請選擇 [新增列]，然後在 [機碼/值配對] 區段中，選擇 [機碼/值] 索引標籤。

   選擇添加行，然後在「鍵/值對」部分中，選擇「鍵/值」選項卡。
   - 鍵-輸入**Password**。
   - 值 — 輸入使用者的密碼。
7. 如果您要提供私密金鑰，請選擇 [新增列]，然後在 [金鑰/值配對] 區段中，選擇 [機碼/值] 索引標籤。
   - 鍵-輸入**PrivateKey**。
   - 值 — 輸入使用者的私密金鑰。此值必須以 OpenSSH 格式儲存，且必須對應於遠端伺服器中為此使用者儲存的公開金鑰。
8. 選擇下一步。
9. 在 [設定密碼] 頁面上，輸入密碼的名稱和說明。建議您使用的字首做**aws/transfer/**為名稱。例如，您可以命名您的秘密**aws/transfer/connector-1**。
10. 選擇 [下一步]，然後接受 [設定旋轉] 頁面上的預設值。然後選擇下一步。
11. 在「檢閱」頁面上，選擇「儲存」以建立並儲存密碼。

建立密碼之後，您可以在建立連接器時選擇它 (請參閱設定 AS2 連接器)。在您啟用基本驗證的步驟中，從可用密碼的下拉式清單中選擇密碼。

檢視 AS2 連接器詳細資訊

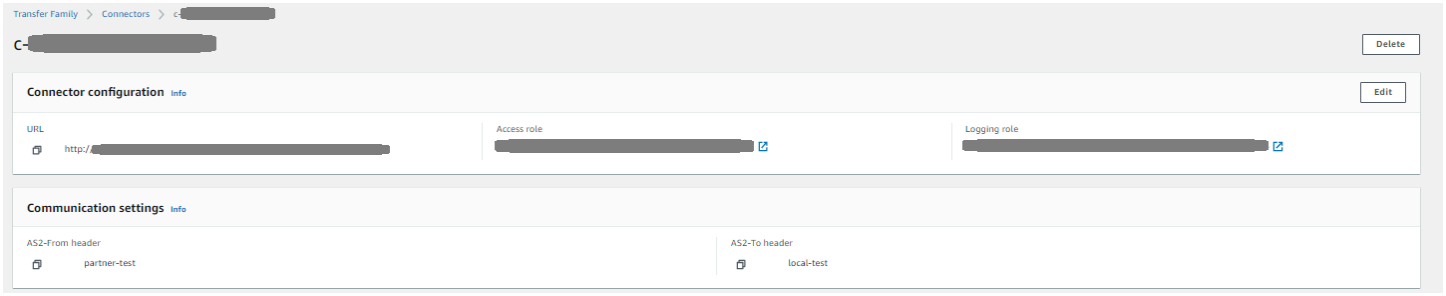
您可以在 AWS Transfer Family 主控台中找到 AS2 AWS Transfer Family 連接器的詳細資料和內容清單。AS2 連接器的內容包括其 URL、角色、設定檔、MDN、標籤和監視指標。

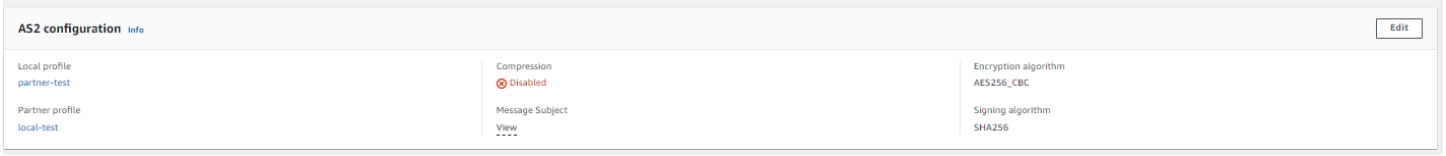
這是檢視連接器詳細資訊的程序。

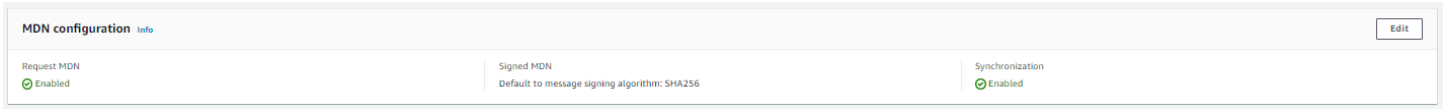
檢視連接器詳細資料

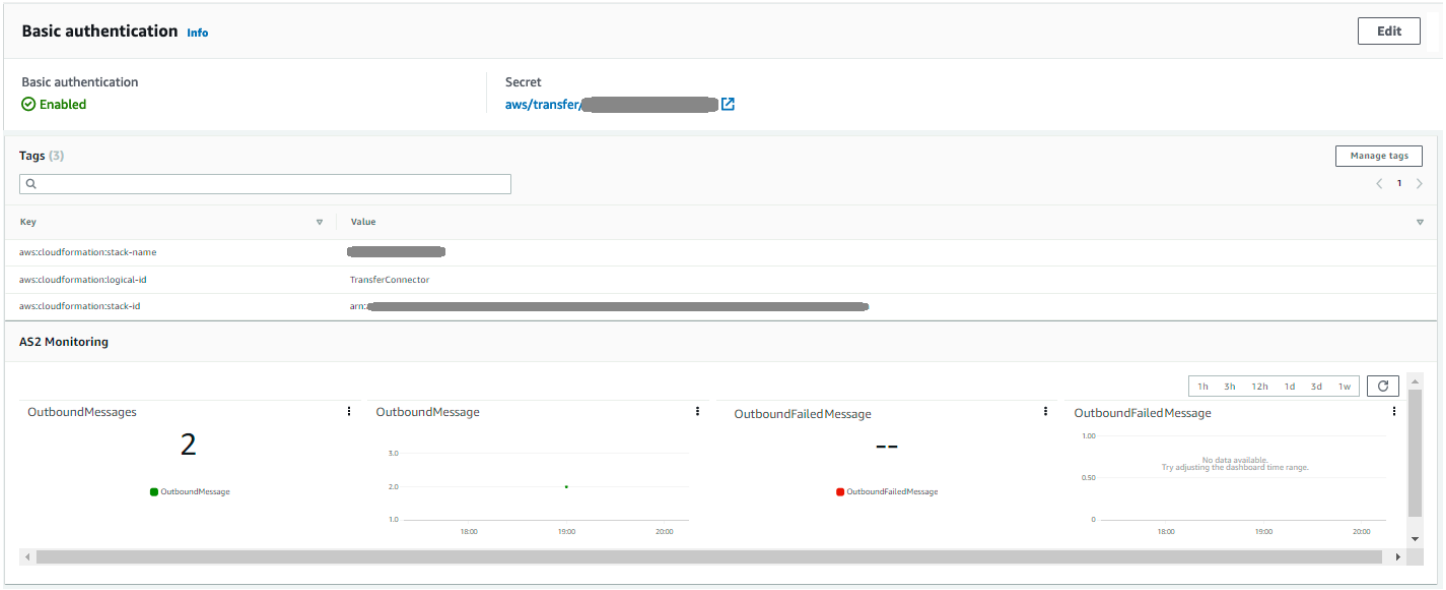
1. 請在以下位置開啟 AWS Transfer Family 主控台。 https://console.aws.amazon.com/transfer/
2. 在左側導覽窗格中，選擇 Connectors (連接器)。
3. 在連接器識別碼資料行中選擇識別碼，以查看所選連接器的詳細資料頁面。

您可以選擇編輯，在連接器的詳細資料頁面上變更 AS2 連接器的內容。









> **Note**
>
> 您可以透過執行下列命令 AWS Command Line Interface (AWS CLI 命令：

```
aws transfer describe-connector --connector-id your-connector-id
```

如需詳細資訊，請參閱 API 參考資料DescribeConnector中的。

管理 AS2 合作夥伴

本主題討論如何管理 AS2 憑證、設定檔和合約。

匯入 AS2 憑證

Transfer Family AS2 程序會使用憑證金鑰來加密和簽署傳輸的資訊。合作夥伴可以為這兩個目的使用相同的金鑰，或為每個使用個別的金鑰。如果您的通用加密金鑰由受信任的第三方保存在委託中，以便在發生災難或安全漏洞時解密資料，我們建議您使用單獨的簽署金鑰。透過使用不同的簽署金鑰 (您不會委託)，您不會損害數位簽章的不可否認性功能。

> **Note**
>
> AS2 憑證的金鑰長度必須至少為 2048 位元，且最多為 4096 個。

以下幾點詳細說明了在此過程中如何使用 AS2 證書。

- 入境
  - 交易夥伴傳送其簽署憑證的公開金鑰，而此金鑰會匯入合作夥伴設定檔。
  - 本機方傳送其加密和簽署憑證的公開金鑰。然後，合作夥伴導入一個或多個私鑰。本機方可以傳送個別的憑證金鑰進行簽署和加密，或者可以選擇使用相同的金鑰來達到這兩個目的。
- 出站 AS2
  - 合作夥伴會傳送其加密憑證的公開金鑰，而此金鑰會匯入合作夥伴設定檔。
  - 本機方傳送憑證的公開金鑰進行簽署，並匯入憑證的私密金鑰以進行簽署。
  - 如果您使用 HTTPS，則可以匯入自我簽署的傳輸層安全性 (TLS) 憑證。

如需如何建立憑證的詳細資訊，請參閱the section called “步驟 1：為 AS2 建立憑證”。

此程序說明如何使用 Transfer Family 主控台匯入憑證。如果您想要 AWS CLI 改用，請參閱the section called “步驟 3：將憑證匯入為 Transfer Family 憑證資源”。

若要指定啟用 AS2 的憑證

1. 請在以下位置開啟 AWS Transfer Family 主控台。 https://console.aws.amazon.com/transfer/
2. 在左側導覽窗格的「AS2 交易夥伴」下，選擇「憑證」。
3. 選擇 Import certificate (匯入憑證)。
4. 在「憑證說明」區段中，輸入易於識別的憑證名稱。請確定您可以透過憑證的說明來識別憑證的用途。此外，請選擇憑證的角色。
5. 在「憑證內容」區段中，提供來自交易夥伴的公開憑證，或提供本機憑證的公開和私密金鑰。
6. 在 [憑證使用] 區段中，選擇此憑證的用途。它可以用於加密，簽名，或兩者兼而有之。

   > **Note**
   >
   > 如果您選擇加密並簽署用法，Transfer Family 會建立兩個相同的憑證 (每個憑證都有自己的 ID)：一個使用值為，另一個使用值為SIGNING。ENCRYPTION

7. 在「憑證內容」區段中填入適當的詳細資料。
   - 如果您選擇自我簽署憑證，則不會提供憑證鏈結。
   - 貼上憑證的內容。
   - 如果憑證不是自我簽署憑證，請提供憑證鏈結。
   - 如果此憑證是本機憑證，請貼上其私密金鑰。
8. 選擇匯入憑證以完成程序並儲存匯入憑證的詳細資料。

> **Note**
>
> TLS 憑證只能匯入為合作夥伴的公開憑證。如果您從合作夥伴選取公用憑證，然後針對用途選取傳輸層安全性 (TLS)，您會收到警告。此外，TLS 憑證必須是自我簽署的 (也就是說，您必須選取「自我簽署憑證」才能匯入 TLS 憑證)。

AS2 證書輪換

通常，憑證的有效期為六個月到一年。您可能已設定要保留較長時間的設定檔。為了便於此，Transfer Family 提供憑證輪替。您可以為一個設定檔指定多個憑證，讓您可以持續使用該設定檔多年。Transfer Family 使用憑證進行簽署 (選用) 和加密 (強制性)。如果您願意，您可以為這兩種目的指定單一憑證。

憑證輪替是以較新的憑證取代舊即將到期的憑證的程序。此轉換是一種循序漸進的方法，以避免在合約中的合作夥伴尚未設定輸出傳輸的新憑證，或者可能會在使用較新憑證的期間傳送使用舊憑證簽署或加密的承載。新舊憑證都有效的中繼期間稱為寬限期。

X.509 憑證具有Not Before和Not After日期。但是，這些參數可能無法為管理員提供足夠的控制。Transfer Family 提供Active Date和Inactive Date設定，可控制輸出承載使用哪個憑證，以及輸入承載所接受的憑證。

輸出憑證選擇會使用傳輸日期之前的最大值作為Inactive Date。輸入程序接受範圍內的憑證，Not BeforeNot After且範圍在Active Date和範圍內Inactive Date。

下表說明針對單一設定檔設定兩個憑證的一種可能方法。

輪替中的兩個證書

名稱	NOT BEFORE(由憑證授權單位控制)	ACTIVE DATE（由 Transfer Family 設置）	INACTIVE DATE（由 Transfer Family 設置）	NOT AFTER(由憑證授權單位設定)
驗證碼 1 (較舊的憑證)	2019-11-01	2020-01-01	2020-12-31	2024-01-01
證書 2（較新的證書）	2020-11-01	2020-06-01	2021-06-01	2025-01-01

注意下列事項：

- 當您為憑證指Inactive Date定Active Date和時，範圍必須在Not Before和之間的範圍內Not After。
- 我們建議您為每個設定檔設定數個憑證，確定所有合併憑證的有效日期範圍涵蓋您要使用設定檔的時間長度。
- 我們建議您指定從舊憑證變成非作用中狀態到新憑證啟用之間的寬限時間。在前面的範例中，第一個憑證在 2020-12-31 之前不會變成非作用中狀態，而第二個憑證在 2020-06-01 上啟用，提供 6 個月的寬限期。在 2020 年 6 月 1 日至 2020 年 12 月 31 日期間，兩個憑證均處於有效狀態。

建立 AS2 設定檔

使用此程序來建立本機和合作夥伴設定檔。此程序說明如何使用「Transfer Family」主控台建立 AS2 設定檔。如果您想要 AWS CLI 改用，請參閱the section called “步驟 4：為您和您的交易夥伴建立個人檔案”。

建立 AS2 設定檔的步驟

1. 請在以下位置開啟 AWS Transfer Family 主控台。 https://console.aws.amazon.com/transfer/
2. 在左側導覽窗格的「AS2 交易夥伴」下，選擇「設定檔」，然後選擇「建立設定檔」。
3. 在「設定檔組態」區段中，輸入設定檔的 AS2 ID。此值用於 AS2 通訊協定特定的 HTTP 標頭，`as2-to`以`as2-from`及識別交易夥伴關係 (決定要使用的憑證等)。
4. 在 [設定檔類型] 區段中，選擇 [本機設定檔] 或 [合作夥伴
5. 在「憑證」區段中，從下拉式功能表中選擇一或多個憑證。

   > **Note**
   >
   > 如果您要匯入下拉式功能表中未列出的憑證，請選取「匯入新憑證」。這會在「匯入憑證」畫面上開啟新的瀏覽器視窗。如需有關匯入憑證的程序，請參閱匯入 AS2 憑證。

6. (選擇性) 在「標籤」區段中，指定一或多個索引鍵值配對，以協助識別此設定檔。
7. 選擇創建配置文件以完成該過程並保存新配置文件。

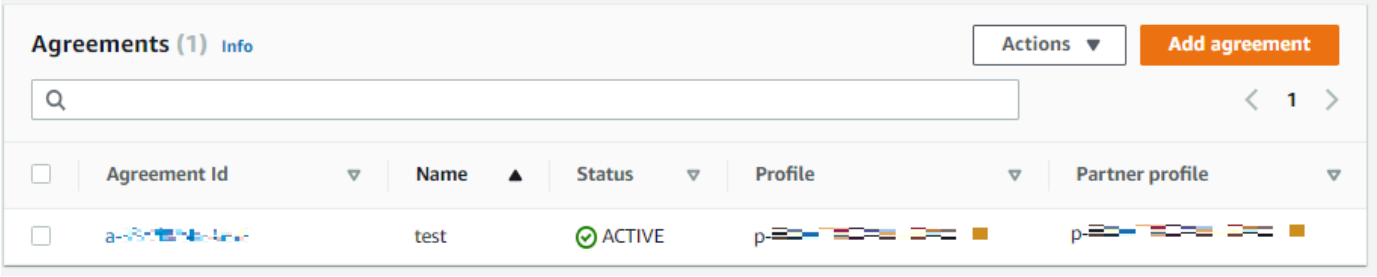
建立 AS2 協議

合約與 Transfer Family 伺服器相關聯。他們會為使用 AS2 通訊協定來交換訊息或檔案的交易夥伴指定詳細資料，使用 Transfer Family 進行輸入傳輸 — 將 AS2 檔案從外部合作夥伴擁有的來源傳送至 Transfer Family 伺服器。

此程序說明如何使用「Transfer Family」主控台建立 AS2 合約。如果您想要 AWS CLI 改用，請參閱the section called “步驟 5：建立您與合作夥伴之間的協議”。

建立 Transfer Family 伺服器的合約

1. 請在以下位置開啟 AWS Transfer Family 主控台。 https://console.aws.amazon.com/transfer/
2. 在左側導覽窗格中，選擇 [伺服器]，然後選擇使用 AS2 通訊協定的伺服器。
3. 在伺服器詳細資訊頁面上，向下捲動至「合約」區段。



4. 選擇「新增協議」。
5. 填寫協議參數，如下所示：

   a. 在「合約組態」區段中，輸入描述性名稱。請確定您可以透過合約的名稱來識別合約的用途。此外，請設定協定的「狀態」：「作用中」(預設選取) 或「非作用中」。

   b. 在「通訊設定」區段中，選擇本機設定檔和合作夥伴設定檔。

   c. 在「收件匣資料夾設定」區段中，選擇 Amazon S3 儲存貯體來存放傳入檔案，以及可存取儲存貯體的 IAM 角色。您可以選擇性地輸入字首 (資料夾)，以用來儲存值區中的檔案。

      例如，如果您**DOC-EXAMPLE-BUCKET**為值區和**incoming**字首輸入，則傳入的檔案會儲存到`/DOC-EXAMPLE-BUCKET/incoming`資料夾中。

   d. (選擇性) 在「標籤」區段中新增標籤。

   e. 輸入協議的所有資訊之後，請選擇「建立協議」。

新合約會顯示在伺服器詳細資訊頁面的「合約」區段中。

發送和接收 AS2 消息

本節說明傳送和接收 AS2 訊息的程序。它還提供了與 AS2 消息相關聯的文件名和位置的詳細信息。

下表列出 AS2 訊息可用的加密演算法，以及何時可以使用它們。

加密演算法	HTTP	HTTPS	備註
亞洲	是	是	
俄羅斯	是	是	
西 256_C	是	是	

加密演算法	HTTP	HTTPS	備註
德斯 _ 埃德 3_CBC	是	是	僅當您必須支援需要此演算法的舊版用戶端時，才使用此演算法，因為它是弱式加密演算法。
NONE	否	是	如果您要將訊息傳送至 Transfer Family 伺服器，則只能選取是NONE否使用應用程式負載平衡器 (ALB)。

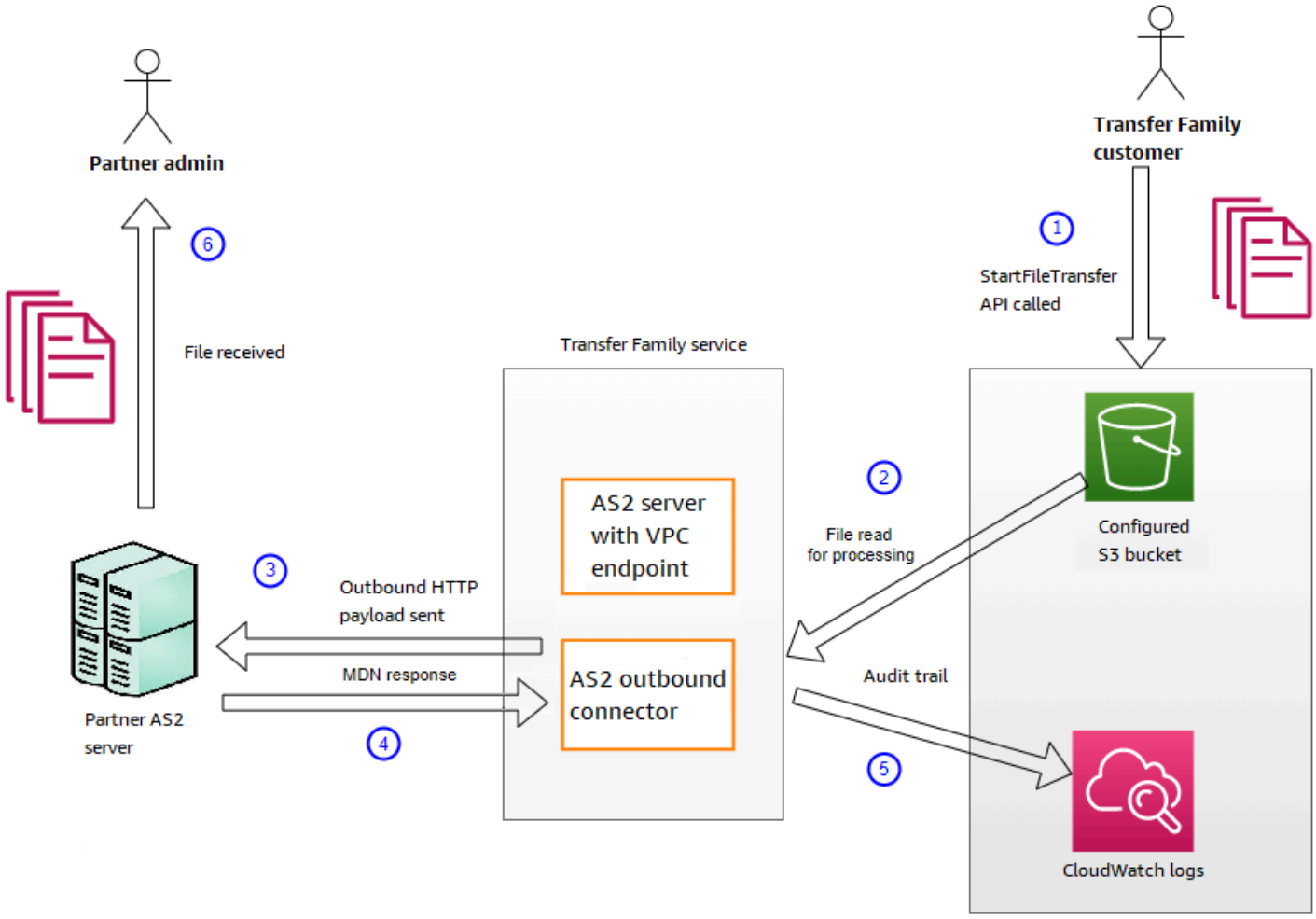
主題

- 傳送 AS2 訊息程序
- 接收 AS2 訊息程序
- 透過 HTTPS 傳送及接收 AS2 訊息
- 使用 AS2 連接器傳輸檔案
- 檔案名稱和位置
- 狀態碼
- 範例 JSON 檔案

傳送 AS2 訊息程序

輸出處理程序會定義為從 AWS 外部用戶端或服務傳送的訊息或檔案。輸出郵件的順序如下：

1. 管理員會呼叫 `start-file-transfer` AWS Command Line Interface (AWS CLI) 命令或 `StartFileTransfer` API 作業。此操作參照connector模型組態。
2. Transfer Family 會偵測到新的檔案請求並找到檔案。該文件被壓縮，簽名和加密。
3. 傳輸 HTTP 用戶端會執行 HTTP POST 要求，將承載傳輸至合作夥伴的 AS2 伺服器。
4. 該進程返回簽名的 MDN 響應，內聯 HTTP 響應（同步 MDN）。
5. 由於文件傳輸的不同階段之間移動，該過程提供 MDN 響應接收和處理詳細信息給客戶。
6. 遠端 AS2 伺服器可讓合作夥伴管理員使用已解密和驗證的檔案。



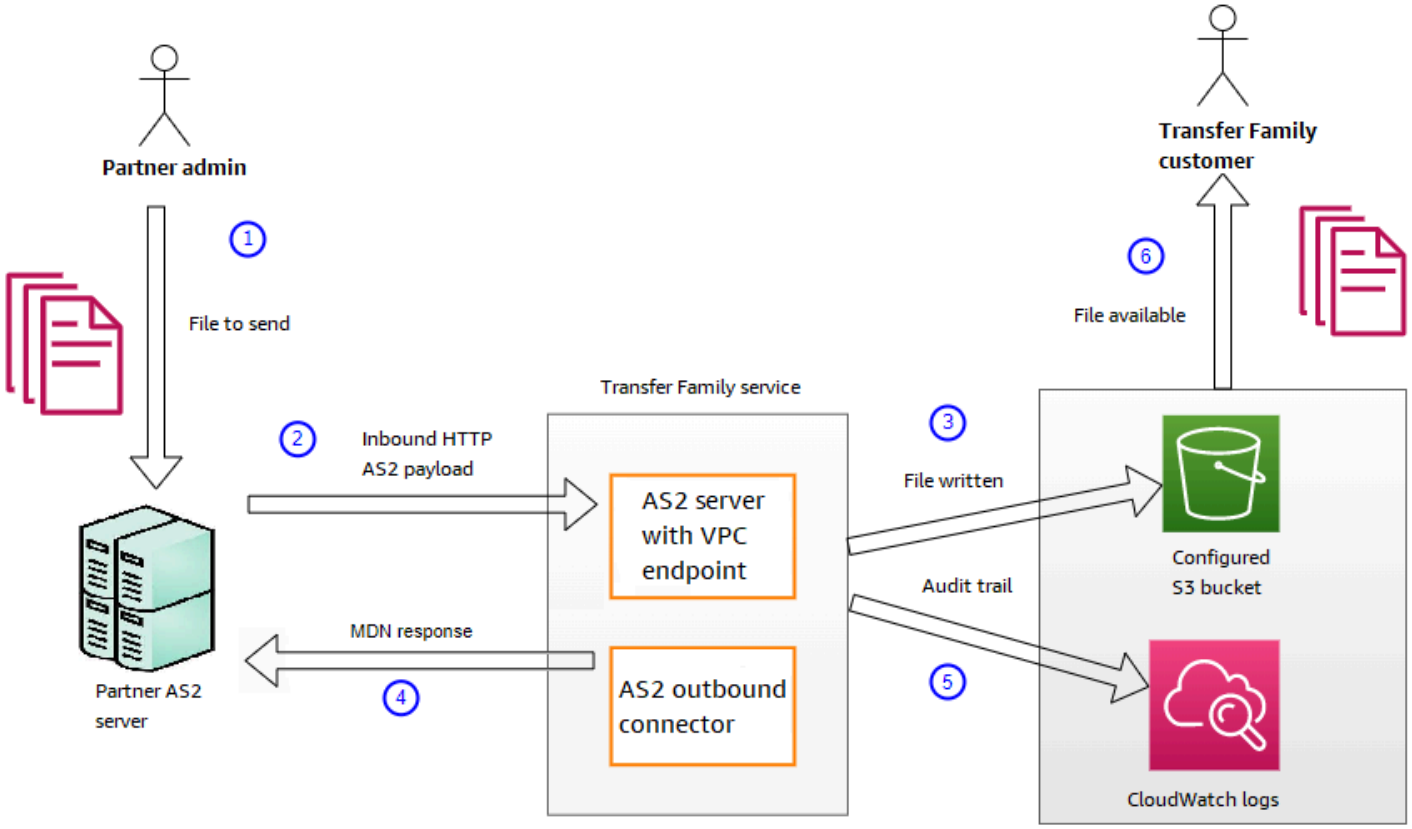
AS2 處理支援許多 RFC 4130 通訊協定，專注於常見使用案例，並與現有啟用 AS2 的伺服器實作整合。如需支援組態的詳細資訊，請參閱AS2 支援的組態。

接收 AS2 訊息程序

輸入程序會定義為正在傳輸到 AWS Transfer Family 伺服器的訊息或檔案。輸入訊息的順序如下：

1. 管理員或自動化程序會在合作夥伴的遠端 AS2 伺服器上啟動 AS2 檔案傳輸。
2. 合作夥伴的遠端 AS2 伺服器會簽署並加密檔案內容，然後將 HTTP POST 要求傳送至傳輸系列上裝載的 AS2 輸入端點。
3. Transfer Family 會使用伺服器、合作夥伴、憑證和合約的設定值，解密並驗證 AS2 承載。檔案內容存放在已設定的 Amazon S3 檔案存放區中。
4. 已簽署的 MDN 回應會以內嵌方式傳回 HTTP 回應，或透過個別的 HTTP POST 要求以非同步方式傳回原始伺服器。
5. 稽核記錄會寫入 Amazon，其中 CloudWatch 包含有關交易所的詳細資訊。

6. 解密的檔案位於名為inbox/processed的資料夾中。



透過 HTTPS 傳送及接收 AS2 訊息

本節說明如何設定使用 AS2 通訊協定透過 HTTPS 傳送及接收訊息的傳送系列伺服器。

主題

- 通過 HTTPS 發送 AS2 消息
- 透過 HTTPS 接收 AS2 訊息

通過 HTTPS 發送 AS2 消息

若要使用 HTTPS 傳送 AS2 郵件，請使用下列資訊建立連接器：

- 對於該網址，請指定一個 HTTPS 網址
- 對於加密演算法，請選取任何可用的演算法。

> **Note**
>
> 若要在不使用加密的情況下將訊息傳送至 Transfer Family 伺服器 (亦即，您NONE為加密演算法選取)，您必須使用 Application Load Balancer 器 (ALB)。

- 如中所述，提供連接器的剩餘值設定 AS2 連接器。

透過 HTTPS 接收 AS2 訊息

AWS Transfer Family AS2 服務器目前僅提供通過端口 5080 的 HTTP 傳輸。不過，您可以使用您選擇的連接埠和憑證，在 Transfer Family 伺服器 VPC 端點前面的網路或應用程式負載平衡器上終止 TLS。使用這種方法，您可以讓內送 AS2 消息使用 HTTPS。

先決條件

- VPC 必須與您的 Transfer Family 伺服器位於 AWS 區域 相同的位置。
- VPC 的子網路必須位於您要在其中使用伺服器的可用區域內。

> **Note**
>
> 每個 Transfer Family 伺服器最多可支援三個可用區域。

- 在與伺服器相同的區域中，最多配置三個彈性 IP 位址。或者，您可以選擇攜帶自己的 IP 位址範圍 (BYOIP)。

> **Note**
>
> 彈性 IP 位址的數目必須與您搭配伺服器端點使用的可用區域數目相符。

您可以設定網路負載平衡 (NLB) 或 Application Load Balancer (ALB)。下表列出了每種方法的優缺點。

下表提供當您使用 NLB 與 ALB 終止 TLS 時的功能差異。

功能	Network Load Balancer (NLB)	Application Load Balancer (ALB)
Latency (延遲)	更低的延遲，因為它在網絡層運行。	更高的延遲，因為它在應用程序層運行。
靜態 IP 支援	可以附加可以是靜態的彈性 IP 地址。	無法附加彈性 IP 位址：提供基礎 IP 位址可以變更的網域。
進階路由	不支援進階路由。	支持高級路由。可以在不加密的情況下注入 AS2 所需的`X-Forwarded-Proto` 標頭。 這個標題在 X-前進-原型在開發人員 .mozil la.org 網站上描述。
TLS/SSL 終止	支持TLS/SSL 終端	支持TLS/SSL 終端
相互 TLS	Transfer Family 目前不支援使用 NLB 進行 MTL	Support MTL

Configure NLB

此程序說明如何在 VPC 中設定面向網際網路的 Network Load Balancer (NLB)。

建立 Network Load Balancer 並將伺服器的 VPC 端點定義為負載平衡器的目標

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon 彈性運算雲端主控台。
2. 在瀏覽窗格中，選擇 [負載平衡器]，然後選擇 [建立負載平衡器]。
3. 在 Network Load Balancer 下，選擇建立。
4. 在「基本組態」區段中，輸入下列資訊：
   - 在名稱中，輸入負載平衡器的描述性名稱。
   - 對於 Scheme (結構描述)，選擇 Internet-facing (面向網際網路)。
   - 針對 [IP 位址類型]，請選擇 [IPv4]。
5. 在「網路對應」區段中，輸入下列資訊：

- 對於 VPC，請選擇您建立的虛擬私有雲 (VPC)。
- 在 [對應] 下，選擇與與伺服器端點搭配使用的相同 VPC 中可用的公用子網路相關聯的可用區域。
- 針對每個子網路的 IPv4 位址，選擇您配置的其中一個彈性 IP 位址。

6. 在「監聽器和路由」段落中，輸入下列資訊：

   - 針對通訊協定，選擇 TLS。
   - 針對連接埠，輸入 **5080**。
   - 在「預設動作」中，選擇「建立目標群組」 如需建立新目標群組的詳細資訊，請參閱若要建立目標群組。

   建立目標群組後，請在「預設」動作欄位中輸入其名稱。
7. 在 [安全接聽程式設定] 區段中，在 [預設 SSL/TLS 憑證] 區域中選擇您的憑證。
8. 選擇建立負載平衡器以建立您的 NLB。
9. （可選，但建議使用）開啟 Network Load Balancer 的存取記錄以維護完整稽核追蹤，如 Network Load Balancer 的存取記錄中所述。

   我們建議您執行此步驟，因為 TLS 連線已在 NLB 終止。因此，Transfer Family AS2 CloudWatch 記錄群組中反映的來源 IP 位址是 NLB 的私有 IP 位址，而非交易夥伴的外部 IP 位址。

Configure ALB

此程序說明如何在 VPC 中設定 Application Load Balancer (NLB)。

建立 Application Load Balancer 器，並將伺服器的 VPC 端點定義為負載平衡器的目標

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon 彈性運算雲端主控台。
2. 在瀏覽窗格中，選擇 [負載平衡器]，然後選擇 [建立負載平衡器]。
3. 在 Application Load Balancer (應用程式負載平衡器) 下，選擇 Create (建立)。
4. 在 ALB 主控台中，在連接埠 443 (HTTPS) 上建立新的 HTTP 接聽程式。
5. (選用)。如果您要設定相互驗證 (MTL)，請設定安全性設定和信任存放區。

   a. 將您的 SSL/TLS 憑證附加至接聽程式。
   b. 在 [用戶端憑證處理] 下，選取 [相互驗證 (MTL)]。

c. 選擇 [以信任存放區驗證]。

d. 在 [進階 MTL 設定] 底下，選擇或建立信任存放區，方法是上傳您的 CA 憑證。

6. 建立新的目標群組，並將 Transfer Family AS2 伺服器端點的私人 IP 位址新增為連接埠 5080 上的目標。如需建立新目標群組的詳細資訊，請參閱若要建立目標群組。
7. 設定目標群組的健全狀況檢查，以便在連接埠 5080 上使用 TCP 通訊協定。
8. 建立新規則，將 HTTPS 流量從接聽器轉寄至目標群組。
9. 設定監聽器以使用您的 SSL/TLS 憑證。

設定負載平衡器之後，用戶端會透過自訂連接埠接聽程式與負載平衡器進行通訊。然後，負載平衡器會透過連接埠 5080 與伺服器通訊。

若要建立目標群組

1. 在上一個程序中選擇建立目標群組之後，您就會移至新目標群組的「指定群組詳細資訊」頁面。
2. 在「基本組態」區段中，輸入下列資訊。

   - 針對 [選擇目標類型]，選擇 [IP 位址]。
   - 針對 Target group name (目標群組名稱)，輸入目標群組的名稱。
   - 針對 Protocol (通訊協定)，選擇 TCP。
   - 針對連接埠，輸入 **`5080`**。
   - 針對 [IP 位址類型]，請選擇 [IPv4]。
   - 對於 VPC，請選擇您為 Transfer Family AS2 伺服器建立的 VPC。
3. 在 [健全狀況檢查] 區段中，選擇 [Health 全狀況檢查通訊協定] 的 TCP
4. 選擇下一步。
5. 在「註冊目標」頁面上，輸入下列資訊：

   - 對於網路，請確認已指定為 Transfer Family AS2 伺服器建立的 VPC。
   - 對於 IPv4 位址，請輸入 Transfer Family AS2 伺服器端點的私人 IPv4 位址。

     如果您的伺服器有多個端點，請選擇 [新增 IPv4 位址] 以新增另一個資料列以輸入另一個 IPv4 位址。重複此程序，直到您輸入所有伺服器端點的私有 IP 位址為止。
   - 確定連接埠已設定為**`5080`**。
   - 選擇下方的「包含為待決」，將您的項目新增至「檢閱目標」區段。
6. 在「檢閱目標」區段中，檢閱您的 IP 目標。

7. 選擇建立目標群組，然後返回上一個建立 NLB 的程序，然後輸入指示的新目標群組。

測試從彈性 IP 地址對服務器的訪問

使用彈性 IP 位址或 Network Load Balancer 的 DNS 名稱，透過自訂 Connect 埠連線至伺服器。

> **Important**
>
> 使用負載平衡器上設定之子網路的網路存取控制清單 (網路 ACL)，管理從用戶端 IP 位址存取伺服器的存取。網路 ACL 權限是在子網路層級設定的，因此規則會套用至使用該子網路的所有資源。您無法使用安全性群組來控制來自用戶端 IP 位址的存取，因為負載平衡器的目標類型是設定為 IP 位址而非執行個體。因此，負載平衡器不會保留來源 IP 位址。如果網路負載平衡器的健康狀態檢查失敗，這表示負載平衡器無法連線到伺服器端點。若要疑難排解此問題，請檢查下列項目：
>
> - 確認伺服器端點的關聯安全性群組允許從負載平衡器上設定的子網路輸入連線。負載平衡器必須能夠透過連接埠 5080 連線到伺服器端點。
> - 確認伺服器的「狀態」為「線上」。

使用 AS2 連接器傳輸檔案

AS2 連接器會在貿易夥伴之間建立關係，以便將 AS2 訊息從 Transfer Family 伺服器傳輸到外部合作夥伴擁有的目的地。

您可以透過參考連接器 ID 和檔案的路徑，使用「Transfer Family 列」來傳送 AS2 訊息，如下列 `start-file-transfer` AWS Command Line Interface (AWS CLI) 指令所示：

```
aws transfer start-file-transfer --connector-id c-1234567890abcdef0 \
--send-file-paths "/DOC-EXAMPLE-SOURCE-BUCKET/myfile1.txt" "/DOC-EXAMPLE-SOURCE-BUCKET/myfile2.txt"
```

若要取得連接器的詳細資料，請執行下列命令：

```
aws transfer list-connectors
```

此命`list-connectors`令會傳回連接器的連接器識別碼、URL 和 Amazon 資源名稱 (ARN)。

若要傳回特定連接器的內容，請使用您要使用的 ID 執行下列命令：

```
aws transfer describe-connector --connector-id your-connector-id
```

命describe-connector令會傳回連接器的所有內容，包括其 URL、角色、設定檔、訊息配置通知 (MDN)、標籤和監視度量。

您可以檢視 JSON 和 MDN 檔案，確認合作夥伴已成功收到檔案。這些檔案是根據中所述的慣例來命名檔案名稱和位置。如果您在建立連接器時設定記錄角色，您也可以檢查記 CloudWatch 錄中 AS2 訊息的狀態。

若要檢視 AS2 連接器詳細資訊，請參閱檢視 AS2 連接器詳細資訊。若要取得有關建立 AS2 連接器的更多資訊，請參閱設定 AS2 連接器。

檔案名稱和位置

本節討論 AS2 傳輸的檔案命名慣例。

對於傳入檔案傳輸，請注意下列事項：

- 您可以在協定中指定基本目錄。基本目錄是 Amazon S3 儲存貯體名稱，並結合前置詞 (如果有的話)。例如 /DOC-EXAMPLE-BUCKET/AS2-folder。
- 如果成功處理內送檔案，則檔案 (以及對應的 JSON 檔案) 會儲存到/processed資料夾中。例如 /DOC-EXAMPLE-BUCKET/AS2-folder/processed。

  JSON 檔案包含下列欄位：

  - agreement-id
  - as2-from
  - as2-to
  - as2-message-id
  - transfer-id
  - client-ip
  - connector-id
  - failure-message
  - file-path
  - message-subject
  - mdn-message-id

  - mdn-subject
  - requester-file-name
  - requester-content-type
  - server-id
  - status-code
  - failure-code
  - transfer-size
- 如果無法成功處理內送檔案，則檔案 (以及對應的 JSON 檔案) 會儲存到/failed資料夾中。例如 /DOC-EXAMPLE-BUCKET/AS2-folder/failed。
- 傳輸的檔案會儲存在processed資料夾中的狀態*original_filename*.*messageId*.*original_extension*。也就是說，傳輸的訊息 ID 會附加至檔案名稱之前的原始副檔名。
- 系統會建立 JSON 檔案並將其另存為*original_filename*.*messageId*.*original_extension*.json。除了要新增的訊息 ID 之外，字串.json還會附加至傳輸檔案的名稱。
- 訊息處理通知 (MDN) 檔案會建立並另存為。*original_filename*.*messageId*.*original_extension*.mdn除了要新增的訊息 ID 之外，字串.mdn還會附加至傳輸檔案的名稱。
- 如果有名為的輸入檔案ExampleFileInS3Payload.dat，則會建立下列檔案：
  - 檔案 — ExampleFileInS3Payload.c4d6b6c7-23ea-4b8c-9ada-0cb811dc8b35@44313c54b0a46a36.
  - JSON ExampleFileInS3Payload.c4d6b6c7-23ea-4b8c-9ada-0cb811dc8b35@44313c54b0a46a36.
  - MDN — ExampleFileInS3Payload.c4d6b6c7-23ea-4b8c-9ada-0cb811dc8b35@44313c54b0a46a36.

對於輸出傳輸，命名類似，不同之處在於沒有內送郵件檔案，而且已傳送郵件的傳輸 ID 會新增至檔案名稱。StartFileTransferAPI 作業 (或其他程序或指令碼呼叫此作業時) 會傳回傳輸 ID。

- transfer-id是與檔案傳輸相關聯的識別碼。屬於呼叫一部分的所有要StartFileTransfer求共用一個transfer-id.
- 基本目錄與您用於來源檔案的路徑相同。也就是說，基本目錄是您在 StartFileTransfer API 作業或start-file-transfer AWS CLI 命令中指定的路徑。例如：

```
aws transfer start-file-transfer --send-file-paths /DOC-EXAMPLE-BUCKET/AS2-folder/
file-to-send.txt
```

如果您執行此指令，MDN 和 JSON 檔案會儲存在 /DOC-EXAMPLE-BUCKET/AS2-folder/processed (成功傳輸)，或 /DOC-EXAMPLE-BUCKET/AS2-folder/failed (傳輸失敗)。

- 系統會建立 JSON 檔案並將其另存為*original_filename*.*transferId*.*messageId*.*original_extension*.json。
- MDN 檔案隨即建立並另存為*original_filename*.*transferId*.*messageId*.*original_extension*.mdn。
- 如果有名為的輸出檔案ExampleFileOutTestOutboundSyncMdn.dat，則會建立下列檔案：
  - JSON ExampleFileOutTestOutboundSyncMdn.dedf4601-4e90-4043-b16b-579af35e0d83.fbe18db8-7361-42ff-8ab6-49ec1e435f34@c9c705f0baaaabaa.dat.j
  - MDN — ExampleFileOutTestOutboundSyncMdn.dedf4601-4e90-4043-b16b-579af35e0d83.fbe18db8-7361-42ff-8ab6-49ec1e435f34@c9c705f0baaaabaa.dat.m

您也可以檢查 CloudWatch 記錄以檢視轉移的詳細資料，包括任何失敗的資料。

狀態碼

下表列出當您或您的合作夥伴傳送 AS2 訊息時，可以 CloudWatch 記錄到記錄中的所有狀態碼。不同的郵件處理步驟適用於不同的郵件類型，並且僅用於監視。「已完成」和「失敗」狀態代表處理中的最後一個步驟，並且在 JSON 檔案中可見。

代碼	描述	處理完成了嗎？
處理	郵件正在轉換為最終格式。例如，解壓縮和解密步驟都具有此狀態。	否
中央傳輸	訊息處理正在傳送 MDN 回應。	否
MDN 接收	訊息處理正在接收 MDN 回應。	否

代碼	描述	處理完成了嗎？
COMPLETED (已完成)	訊息處理已成功完成。此狀態包括為輸入郵件傳送 MDN 或外寄郵件的 MDN 驗證時。	是
失敗	郵件處理失敗。如需錯誤碼的清單，請參閱AS2 錯誤代碼。	是

範例 JSON 檔案

本節列出輸入和出站傳輸的 JSON 檔案範例，包括成功傳輸和傳輸失敗的範例檔案。

已成功傳輸的範例輸出檔案：

```
{
  "requester-content-type": "application/octet-stream",
  "mesage-subject": "File xyzTest from MyCompany_OID to partner YourCompany",
  "requester-file-name": "TestOutboundSyncMdn-9lmCr79hV.dat",
  "as2-from": "MyCompany_OID",
  "connector-id": "c-c21c63ceaaf34d99b",
  "status-code": "COMPLETED",
  "disposition": "automatic-action/MDN-sent-automatically; processed",
  "transfer-size": 3198,
  "mdn-message-id": "OPENAS2-11072022063009+0000-df865189-1450-435b-9b8d-
d8bc0cee97fd@PartnerA_OID_MyCompany_OID",
  "mdn-subject": "Message be18db8-7361-42ff-8ab6-49ec1e435f34@c9c705f0baaaabaa has been
 accepted",
  "as2-to": "PartnerA_OID",
  "transfer-id": "dedf4601-4e90-4043-b16b-579af35e0d83",
  "file-path": "/DOC-EXAMPLE-BUCKET/as2testcell0000/openAs2/
TestOutboundSyncMdn-9lmCr79hV.dat",
  "as2-message-id": "fbe18db8-7361-42ff-8ab6-49ec1e435f34@c9c705f0baaaabaa",
  "timestamp": "2022-07-11T06:30:10.791274Z"
}
```

傳輸失敗的範例輸出檔案：

```
{
  "failure-code": "HTTP_ERROR_RESPONSE_FROM_PARTNER",
  "status-code": "FAILED",
```

```
  "requester-content-type": "application/octet-stream",
  "subject": "Test run from Id da86e74d6e57464aae1a55b8596bad0a to partner
 9f8474d7714e476e8a46ce8c93a48c6c",
  "transfer-size": 3198,
  "requester-file-name": "openAs2TestOutboundWrongAs2Ids-necco-3VYn5n8wE.dat",
  "as2-message-id": "9a9cc9ab-7893-4cb6-992a-5ed8b90775ff@718de4cec1374598",
  "failure-message": "http://Test123456789.us-east-1.elb.amazonaws.com:10080 returned
 status 500 for message with ID 9a9cc9ab-7893-4cb6-992a-5ed8b90775ff@718de4cec1374598",
  "transfer-id": "07bd3e07-a652-4cc6-9412-73ffdb97ab92",
  "connector-id": "c-056e15cc851f4b2e9",
  "file-path": "/testbucket-4c1tq6ohjt9y/as2IntegCell0002/openAs2/
openAs2TestOutboundWrongAs2Ids-necco-3VYn5n8wE.dat",
  "timestamp": "2022-07-11T21:17:24.802378Z"
}
```

已成功傳輸的輸入檔案範例：

```
{
  "requester-content-type": "application/EDI-X12",
  "subject": "File openAs2TestInboundAsyncMdn-necco-5Ab6bTfCO.dat sent from MyCompany
 to PartnerA",
  "client-ip": "10.0.109.105",
  "requester-file-name": "openAs2TestInboundAsyncMdn-necco-5Ab6bTfCO.dat",
  "as2-from": "MyCompany_OID",
  "status-code": "COMPLETED",
  "disposition": "automatic-action/MDN-sent-automatically; processed",
  "transfer-size": 1050,
  "mdn-subject": "Message Disposition Notification",
  "as2-message-id": "OPENAS2-11072022233606+0000-5dab0452-0ca1-4f9b-b622-
fba84effff3c@MyCompany_OID_PartnerA_OID",
  "as2-to": "PartnerA_OID",
  "agreement-id": "a-f5c5cbea5f7741988",
  "file-path": "processed/openAs2TestInboundAsyncMdn-
necco-5Ab6bTfCO.OPENAS2-11072022233606+0000-5dab0452-0ca1-4f9b-b622-
fba84effff3c@MyCompany_OID_PartnerA_OID.dat",
  "server-id": "s-5f7422b04c2447ef9",
  "timestamp": "2022-07-11T23:36:36.105030Z"
}
```

傳輸失敗的範例輸入檔案：

```
{
  "failure-code": "INVALID_REQUEST",
```

```
  "status-code": "FAILED",
  "subject": "Sending a request from InboundHttpClientTests",
  "client-ip": "10.0.117.27",
  "as2-message-id": "testFailedLogs-TestRunConfig-Default-inbound-direct-
integ-0c97ee55-af56-4988-b7b4-a3e0576f8f9c@necco",
  "as2-to": "0beff6af56c548f28b0e78841dce44f9",
  "failure-message": "Unsupported date format: 2022/123/456T",
  "agreement-id": "a-0ceec8ca0a3348d6a",
  "as2-from": "ab91a398aed0422d9dd1362710213880",
  "file-path": "failed/01187f15-523c-43ac-9fd6-51b5ad2b08f3.testFailedLogs-
TestRunConfig-Default-inbound-direct-integ-0c97ee55-af56-4988-b7b4-a3e0576f8f9c@necco",
  "server-id": "s-0582af12e44540b9b",
  "timestamp": "2022-07-11T06:30:03.662939Z"
}
```


監控 AS2 使用情況

您可以使用 Amazon CloudWatch 和AWS CloudTrail. 若要檢視其他「Transfer Family」伺服器測量結果 Amazon CloudWatch 日誌記錄 AWS Transfer Family

AS2 指標

指標	描述
InboundMessage	成功從交易夥伴收到的 AS2 訊息總數。 單位：計數 期間：5 分鐘
InboundFailedMessage	從交易夥伴收到未成功的 AS2 訊息總數。也就是說，交易夥伴發送了一條消息，但 Transfer Family 服務器無法成功處理它。 單位：計數 期間：5 分鐘
OutboundMessage	從轉移系列伺服器成功傳送給交易夥伴的 AS2 訊息總數。 單位：計數

指標	描述
	時間：5 分鐘
OutboundFailedMessage	未成功傳送給交易夥伴的 AS2 訊息總數。也就是說，它們是從 Transfer Family 服務器發送的，但交易夥伴沒有成功收到它們。 單位：計數 期間：5 分鐘

AS2 狀態碼

下表列出當您或您的合作夥伴傳送 AS2 訊息時，可以 CloudWatch 記錄到記錄中的所有狀態碼。不同的郵件處理步驟適用於不同的郵件類型，並且僅用於監視。「已完成」和「失敗」狀態代表處理中的最後一個步驟，並且在 JSON 檔案中可見。

代碼	描述	處理完成了嗎？
處理	郵件正在轉換為最終格式。例如，解壓縮和解密步驟都具有此狀態。	否
傳輸中心	訊息處理正在傳送 MDN 回應。	否
中信接收	訊息處理正在接收 MDN 回應。	否
COMPLETED (已完成)	訊息處理已成功完成。此狀態包括為輸入郵件傳送 MDN 或外寄郵件的 MDN 驗證時。	是
失敗	郵件處理失敗。如需錯誤碼的清單，請參閱AS2 錯誤代碼。	是

AS2 錯誤代碼

下表列出並說明您可能從 AS2 檔案傳輸收到的錯誤碼。

AS2 錯誤代碼

代碼	錯誤	說明和解析度
ACCESS_DENIED	• 存取遭拒。檢查您的存取角色是否具有必要的權限。 • 無效的檔案路徑 *send-file-path* • 無法取得憑證 ErrorCode：##程式碼	處理任何無效或格式錯誤SendFilePaths 的StartFileTransfer 請求時發生。也就是說，路徑缺少 Amazon S3 儲存貯體名稱，或路徑包含無效的字元。如果「Transfer Family」無法擔任存取角色或記錄角色，也會發生這種情況。 確保路徑包含有效的 Amazon S3 儲存貯體名稱和金鑰名稱。
AGREEMENT_NOT_FOUND	找不到協議。	找不到協定，或協定與非作用中的設定檔相關聯。 更新「Transfer Family」伺服器內的合約，以包含作用中的設定檔。
CONNECTOR_NOT_FOUND	找不到連接器或相關組態。	找不到連接器，或連接器與非作用中的設定檔相關聯。 更新連接器以包含作用中的設定檔。
CREDENTIALS_RETRIEVAL_FAILED	1. 密碼管理員中找不到密碼。 2. 無法存取 Secrets Manager。	對於 AS2 基本驗證，密碼必須正確格式化。下列解決方案對應於上一欄中列出的錯誤。 1. 確保密碼 ID 正確無誤。

代碼	錯誤	說明和解析度
	3. 無法解密密碼管理員中的密碼。 4. 由於節流，無法取得密碼值。	2. 請確定存取角色具有讀取密碼的適當權限。存取角色必須提供對StartFile Transfer 要求中使用之檔案位置之父目錄的讀取和寫入存取權。此外，請確定角色提供對您要傳送之檔案之父目錄的讀取和寫入存取權StartFile Transfer 。 3. 如果密碼使用客戶管理的金鑰，請確定存取角色具有 AWS Key Management Service (AWS KMS) 金鑰的權限。 4. 如需適用的配額，請參閱處理密碼的配額。
DECOMPRESSION_FAILED	無法解壓縮訊息。	發送的文件已損壞，或壓縮算法無效。 重新傳送郵件並確認已使用 ZLIB 壓縮，或重新傳送郵件而不啟用壓縮。
DECRYPT_FAILED	無法解密訊息訊*# ID*。確定合作夥伴擁有正確的公用加密金鑰。	解密失敗。 確認合作夥伴使用有效憑證傳送承載，並使用有效的加密演算法執行加密。

代碼	錯誤	說明和解析度
DECRYPT_FAILED_INVALID_SMIME_FORMAT	無法剖析封閉的 MIME 零件。	MIME 裝載已損毀或不支援的 SMIME 格式。 發送者應確保支持他們使用的格式，然後重新發送有效負載。
DECRYPT_FAILED_NO_DECRYPTION_KEY_FOUND	找不到相符的解密金鑰。	合作夥伴設定檔沒有指派符合訊息的憑證，或符合訊息的憑證現在已過期或不再有效。 您必須更新合作夥伴設定檔，並確定其中包含有效的憑證。
DECRYPT_FAILED_UNSUPPORTED_ENCRYPTION_ALG	使用具有 ID 的不支援演算法請求 SMIME 有效負載解密：## ID。	遠端傳送者已傳送具有不支援的加密演算法的 AS2 承載。 寄件者必須選擇支援的加密演算法AWS Transfer Family。
DUPLICATE_MESSAGE	重複或雙重處理步驟。	承載具有重複的處理步驟。例如，有兩個加密步驟。 透過單一步驟重新傳送郵件，以進行簽署、壓縮和加密。
ENCRYPT_FAILED_NO_ENCRYPTION_KEY_FOUND	在設定檔中找不到有效的公用加密憑證：#機設定檔 ID	Transfer Family 嘗試加密輸出郵件，但找不到本機設定檔的加密憑證。 解析度選項： • 確定本機設定檔已附加加密的憑證和私密金鑰。 • 確定加密憑證目前處於作用中狀態。

代碼	錯誤	說明和解析度
ENCRYPTION_FAILED	無法加密檔案檔*###*。	要發送的文件不可用於加密。 確認檔案位於預期的 AS2 位置，且AWS Transfer Family具有讀取檔案的權限。
FILE_SIZE_TOO_LARGE	檔案太大。	當傳送或接收超過檔案大小限制的檔案時，就會發生這種情況。
HTTP_ERROR_RESPONSE_FROM_PARTNER	*######## ID = ######## #### 400#*	與合作夥伴的 AS2 伺服器通訊會傳回未預期的 HTTP 回應碼。 合作夥伴可能能夠從其 AS2 伺服器記錄檔提供更多診斷。
INSUFFICENT_MESSAGE_SECURITY_UNENCRYPTED	需要加密。	合作夥伴將未加密的訊息傳送至「Transfer Family」，但不受支援。寄件者必須使用加密的承載。
INVALID_ENDPOINT_PROTOCOL	僅支援 HTTP 和 HTTPS。	您必須在 AS2 連接器組態中指定 HTTP 或 HTTPS 作為通訊協定。

代碼	錯誤	說明和解析度
INVALID_REQUEST	1. 郵件標頭有問題。 2. 無法剖析機密 JSON。 機密 JSON 與預期的格式不符。 3. 密碼必須是 JSON 字串。 4. 使用者名稱不得包含冒號。 使用者名稱不得包含控制字元。 使用者名稱只能包含 ASCII 字元。 密碼不得包含控制字元。 密碼只能包含 ASCII 字元。	此錯誤有幾個原因。下列解決方案對應於上一欄中列出的錯誤。 1. 檢查as2-from和as2-to欄位。請確定原始訊息識別碼與 MDN 格式相符。另外，請確保消息 ID 格式沒有缺少任何 AS2 標頭。 2. 請確保密碼值與記錄的格式相符，如中所述啟用 AS2 連接器的基本驗證。 3. 請確定密碼是以字串形式提供，而不是以二進位檔的形式提供。 4. 對使用者名稱或密碼進行必要的更正。
INVALID_URL_FORMAT	無效的網址格式：##	當您使用設定格式錯誤 URL 的連接器來傳送輸出郵件時，就會發生這個問題。 請確定連接器已設定有效的 HTTP 或 HTTPS 網址。
MDN_RESPONSE_INDICATES_AUTHENTICATION_FAILED	不適用	接收者無法驗證寄件者。協力廠商將 MDN 傳回給「Transfer Family 列」，且處置修正因子錯誤：驗證失敗。
MDN_RESPONSE_INDICATES_DECOMPRESSION_FAILED	不適用	當接收者無法解壓縮郵件內容時，就會發生這種情況。協力廠商將 MDN 傳回至「Transfer Family」，且處置修正因子錯誤：解壓縮失敗。

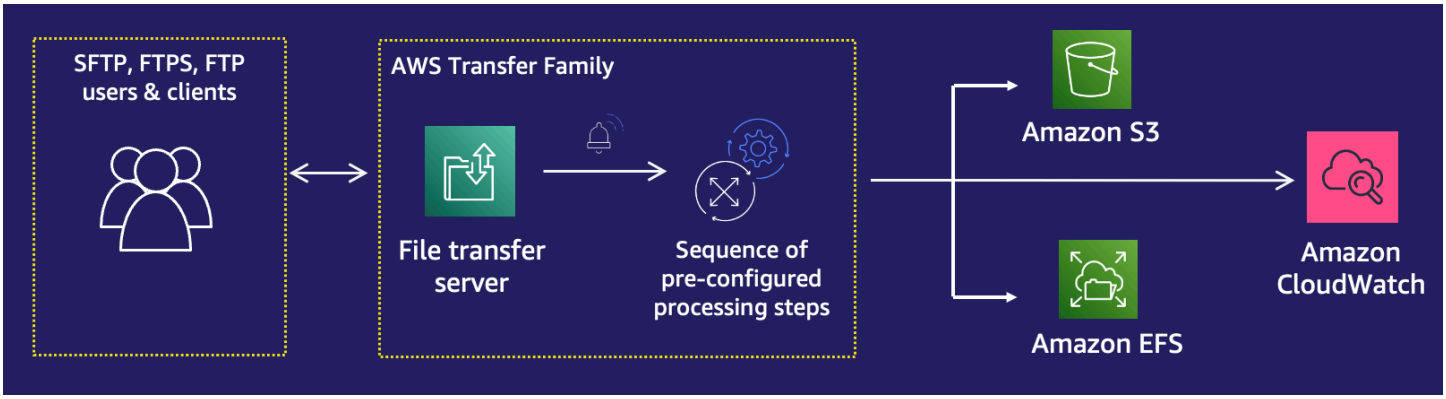
代碼	錯誤	說明和解析度
MDN_RESPONSE_INDICATES_DECRYPTION_FAILED	不適用	接收者無法解密訊息內容。協力廠商將 MDN 傳回給「Transfer Family 列」，且處置修正因子錯誤：驗證失敗。
MDN_RESPONSE_INDICATES_INSUFFICIENT_MESSAGE_SECURITY	不適用	接收者希望郵件經過簽署或加密，但事實並非如此。協力廠商將 MDN 傳回至「Transfer Family」，且處置修正因子錯誤為：。 insufficient-message-security 在連接器上啟用簽署和/或加密，以符合交易夥伴的期望。
MDN_RESPONSE_INDICATES_INTEGRITY_CHECK_FAILED	不適用	接收者無法驗證內容完整性。協力廠商將 MDN 傳回至「Transfer Family」，且處置修正因子錯誤為：。 integrity-check-failed
PATH_NOT_FOUND	無法建立目錄####。找不到父路徑。	Transfer Family 嘗試在客戶的 Amazon S3 儲存貯體中建立目錄，但找不到儲存貯體。 確保StartFile Transfer 命令中提到的每個路徑都包含現有值區的名稱。
SEND_FILE_NOT_FOUND	找不到檔###檔案路徑。	Transfer Family 無法在傳送檔案作業中找到檔案。 檢查設定的主目錄和路徑是否有效，以及 Transfer Family 具有檔案的讀取權限。

代碼	錯誤	說明和解析度
SERVER_NOT_FOUND	找不到與郵件相關聯的伺服器。	Transfer Family 在收到訊息時找不到伺服器。如果在處理內送郵件期間刪除伺服器，就會發生這種情況。
SERVER_NOT_ONLINE	######### 不在線上。	Transfer Family 伺服器處於離線狀態。 啟動伺服器，以便它可以接收和處理訊息。
SIGNING_FAILED	簽署檔案失敗。	要傳送的檔案無法進行簽署，或無法執行簽署。 確認檔案位於預期的 AS2 位置，且AWS Transfer Family具有讀取檔案的權限。
SIGNING_FAILED_NO_SIGNING_KEY_FOUND	找不到設定檔的憑證：##設定檔 ID。	嘗試簽署輸出郵件，但找不到本機設定檔的簽署憑證。 解析度選項： • 請確定本機設定檔已附加憑證和用於簽署的私密金鑰。 • 確定簽署憑證目前處於作用中狀態。
UNABLE_RESOLVE_HOST_TO_IP_ADDRESS	無法將主機名稱解析為 IP 位址。	Transfer Family 無法在 AS2 連接器中設定的公用 DNS 伺服器上執行 DNS 到 IP 位址解析。 更新連接器以指向有效的合作夥伴 URL。

代碼	錯誤	說明和解析度
UNABLE_TO_CONNECT_TO_REMOTE_HOST_OR_IP	與端點的連線逾時。	Transfer Family 無法建立通訊端連線至已設定之合作夥伴的 AS2 伺服器。 檢查合作夥伴的 AS2 伺服器是否可在設定的 IP 位址上使用。
UNABLE_TO_RESOLVE_HOSTNAME	無法解析主機名*#*。	轉移系列伺服器無法使用公用 DNS 伺服器來解析合作夥伴的主機名稱。 檢查已設定的主機是否已註冊，以及 DNS 記錄是否有時間發佈。
VERIFICATION_FAILED	AS2 訊息訊*# ID* 的簽章驗證失敗或 MIC 代碼不相符。	檢查寄件者的簽署憑證是否符合遠端設定檔的簽署憑證。同時檢查 MIC 演算法是否相容 AWS Transfer Family。
VERIFICATION_FAILED_NO_MATCHING_KEY_FOUND	• 在設定檔中找不到符合訊息簽章的公開憑證：*####*設定檔 ID。 • *#################### ID#* • 在「設定檔:*####*設定檔 ID」中找不到有效的憑證。	AWS Transfer Family正在嘗試驗證已接收郵件的簽章，但找不到合作夥伴設定檔的相符簽署憑證。 解析度選項： • 確定合作夥伴設定檔已附加簽署憑證。 • 確定憑證目前處於作用中狀態。 • 確定憑證是合作夥伴的正確簽署憑證。

AWS Transfer Family 管理工作流

AWS Transfer Family 支援受管理的檔案處理工作流程。透過受管理的工作流程，您可以在透過 SFTP、FTPS 或 FTP 傳輸檔案後開始工作流程。使用此功能，您可以協調檔案處理所需的所有必要步驟，以安全且符合成本效益的方式滿足 business-to-business (B2B) 檔案交換的合規要求。此外，您還可以從 end-to-end 稽核和可見度中受益。



透過協調檔案處理工作，受管理的工作流程可協助您在下游應用程式使用資料之前預先處理資料。此類檔案處理工作可能包括：

- 將文件移動到用戶特定的文件夾。
- 將檔案解密為工作流程的一部分。
- 為檔案加標籤。
- 透過建立函數並將 AWS Lambda 函數附加至工作流程來執行自訂處理。
- 成功傳輸檔案時傳送通知。如需詳細說明此使用案例的部落格貼文，請參閱使用 AWS Transfer Family 受管理的工作流程自訂檔案傳遞通知)。

若要快速複寫和標準化組織中多個業務單位的常見上傳後檔案處理工作，您可以使用基礎結構即程式碼 (IaC) 來部署工作流程。您可以指定要在完整上載的檔案上啟動受管理的工作流程。您也可以指定在因為工作階段過早中斷連線而僅部分上載的檔案上啟動不同的受管理工作流程。內建的例外狀況處理可協助您快速回應檔案處理結果，同時讓您控制如何處理失敗。此外，每個工作流程步驟都會產生詳細的記錄，您可以稽核這些記錄以追蹤資料歷程。

若要開始使用，請執行下列工作：

1. 根據您的需求，將工作流程設定為包含預處理動作，例如複製、標記和其他步驟。如需詳細資訊，請參閱 建立工作流程。

2. 設定「Transfer Family」用來執行工作流程的執行角色。如需詳細資訊，請參閱 工作流程的 IAM 政策。
3. 將工作流程對應至伺服器，以便在檔案到達時即時評估和啟動此工作流程中指定的動作。如需詳細資訊，請參閱 設定和執行工作流程。

相關資訊

- 若要監視工作流程執行，請參閱使用 Transfer Family 的 CloudWatch 量度。
- 如需詳細的執行記錄和疑難排解資訊，請參閱使用 Amazon 疑難排解工作流程相關錯誤 CloudWatch。
- Transfer Family 提供部落格文章和研討會，引導您逐步建立檔案傳輸解決方案。此解決方案利 AWS Transfer Family 用受管 SFTP/FTPS 端點和 Amazon Cognito 和 DynamoDB 進行使用者管理。

  部落格文章可在使用 Amazon Cognito 做為身分供應商 AWS Transfer Family 和 Amazon S3 中取得。您可以在此處查看工作坊的詳細信息。
- 檢視AWS Transfer Family 受管理的工作流程，以取得 Transfer Family 工作流程的簡要

主題

- 建立工作流程
- 使用預定義步驟
- 使用自訂檔案處理步驟
- 工作流程的 IAM 政策
- 工作流程的異常處理
- 監控工作流執行
- 從範本建立工作流程
- 從轉移系列伺服器移除工作流程
- 受管理的工作流程限制和

如需開始使用受管理工作流程的詳細說明，請參閱下列資源：

- AWS Transfer Family 受管理工作流程示範
- 使用 AWS Transfer Family 工作流程部落格文章建置雲端原生檔案傳輸平台

建立工作流程

您可以使用，建立受管理的工作流程 AWS Management Console，如本主題所述。為了盡可能簡化工作流程建立程序，主控台中的大多數區段都可以使用關聯式說明面板。

工作流程有兩種步驟：

- 標稱步驟 — 標稱步驟是您要套用至內送檔案的檔案處理步驟。如果您選取多個名義步驟，則會以線性順序處理每個步驟。
- 異常處理步驟-異常處理程序是在任何標稱步驟失敗或導致驗證錯誤時 AWS Transfer Family 執行的文件處理步驟。

建立工作流程

1. 開啟主 AWS Transfer Family 控台，網址為 https://console.aws.amazon.com/transfer/。
2. 在左側導覽窗格中，選擇「工作流程」。
3. 在 [工作流程] 頁面上選擇 [建立工作流程
4. 在 [建立工作流程] 頁面上，輸入描述。此描述顯示在 [工作流程] 頁面上。
5. 在「標稱步驟」區段中，選擇「新增步驟」。新增一或多個步驟。
   a. 從可用選項中選擇步驟類型。如需各種步驟類型的詳細資訊，請參閱the section called “使用預定義步驟”。
   b. 選擇下一步，然後設定步驟的參數。
   c. 選擇「下一步」，然後檢閱該步驟的詳細資料。
   d. 選擇 [建立步驟] 以新增步驟並繼續。
   e. 依需要繼續新增步驟。工作流程中的最大步驟數為 8。
   f. 新增所有必要的標稱步驟後，請向下捲動至 [例外處理常式 — 選用] 區段，然後選擇 [新增步驟]。

   > **Note**
   >
   > 若要即時通知您失敗，我們建議您設定例外狀況處理常式，並在工作流程失敗時執行的步驟。

6. 若要設定例外狀況處理常式，請依照先前所述的相同方式新增步驟。如果檔案導致任何步驟擲回例外狀況，則會逐一叫用您的例外狀況處理常式。

7. (選擇性) 向下捲動至「標記」區段，並新增工作流程的標籤。
8. 檢閱組態，然後選擇 [建立工作流程]。

> **Important**
>
> 建立工作流程之後，您就無法編輯它，因此請務必仔細檢閱設定。

設定和執行工作流程

您必須先將工作流程與 Transfer Family 伺服器建立關聯，才能執行工作流程。

規劃 Transfer Family 以對上載的檔案執行工作流程的步驟

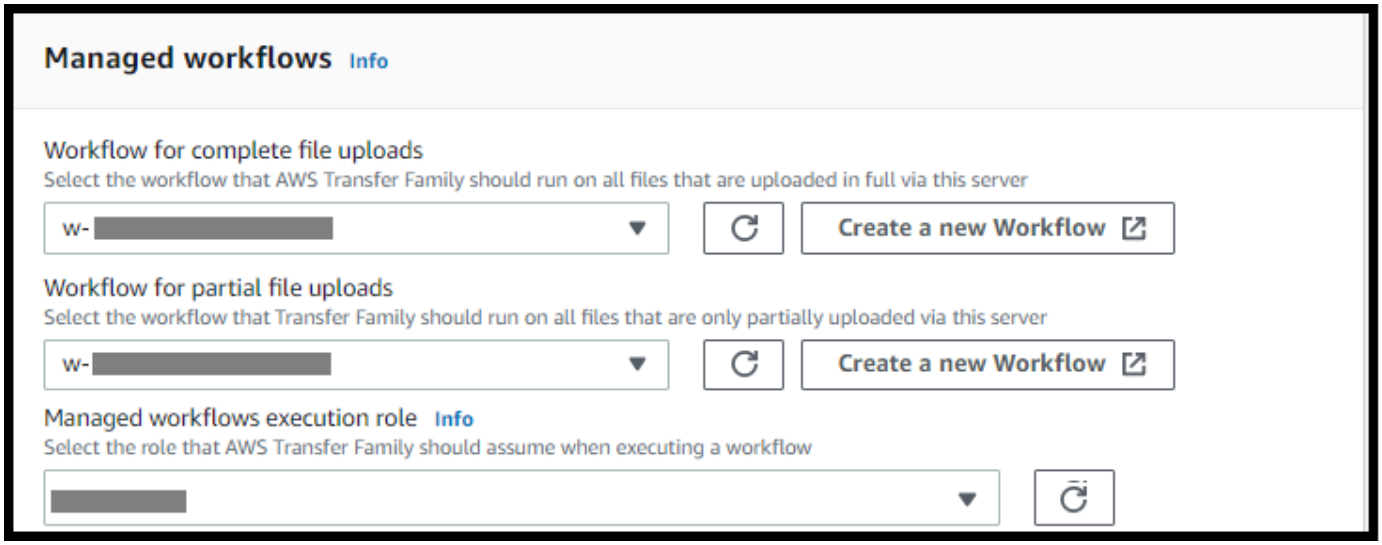
1. 開啟主 AWS Transfer Family 控台，網址為 https://console.aws.amazon.com/transfer/。
2. 在左側導覽窗格中，選擇 [伺服器]。
   - 若要將工作流程新增至現有伺服器，請選擇您要用於工作流程的伺服器。
   - 或者，建立新伺服器並將工作流程新增至該伺服器。如需詳細資訊，請參閱 設定 SFTP、FTPS 或 FTP 伺服器端點。
3. 在伺服器的詳細資訊頁面上，向下捲動至 [其他詳細資料] 區段，然後選擇 [編輯]。

> **Note**
>
> 依預設，伺服器沒有任何關聯的工作流程。您可以使用 [其他詳細資訊] 區段來建立工作流程與所選伺服器的關聯

4. 在 [編輯其他詳細資料] 頁面的 [受管理的工作流程] 區段中，選取要在所有上傳上執行的工作流程。

> **Note**
>
> 如果您還沒有工作流程，請選擇「創建一個新的工作流程」以創建一個工作流程。

   a. 選擇要使用的工作流程 ID。
   b. 選擇執行角色。這是「Transfer Family」在執行工作流程步驟時所承擔的角色。如需詳細資訊，請參閱 工作流程的 IAM 政策。選擇 Save (儲存)。



> **Note**
>
> 如果您不想再將工作流程與伺服器相關聯，您可以移除該關聯。如需詳細資訊，請參閱 從轉移系列伺服器移除工作流程。

執行工作流程的步驟

若要執行工作流程，請將檔案上傳至您使用關聯工作流程設定的 Transfer Family 伺服器。

> **Note**
>
> 每當您從伺服器中移除工作流程並以新工作流程取代，或更新伺服器組態 (這會影響工作流程的執行角色) 時，您必須等待大約 10 分鐘，才能執行新的工作流程。Transfer Family 伺服器會快取工作流程詳細資料，伺服器需要 10 分鐘才能重新整理其快取。
> 此外，您必須登出任何作用中的 SFTP 工作階段，然後在 10 分鐘的等待期後重新登入，以查看變更。

Example

```
# Execute a workflow
> sftp bob@s-1234567890abcdef0.server.transfer.us-east-1.amazonaws.com
```

```
Connected to s-1234567890abcdef0.server.transfer.us-east-1.amazonaws.com.
sftp> put doc1.pdf
Uploading doc1.pdf to /DOC-EXAMPLE-BUCKET/home/users/bob/doc1.pdf
doc1.pdf                                                                    100% 5013KB
 601.0KB/s   00:08
sftp> exit
>
```

檔案上載完成後，系統會對您的檔案執行定義的動作。例如，如果您的工作流程包含複製步驟，則會將檔案複製到您在該步驟中定義的位置。您可以使用 Amazon CloudWatch 日誌追蹤執行的步驟及其執行狀態。

檢視工作流程詳

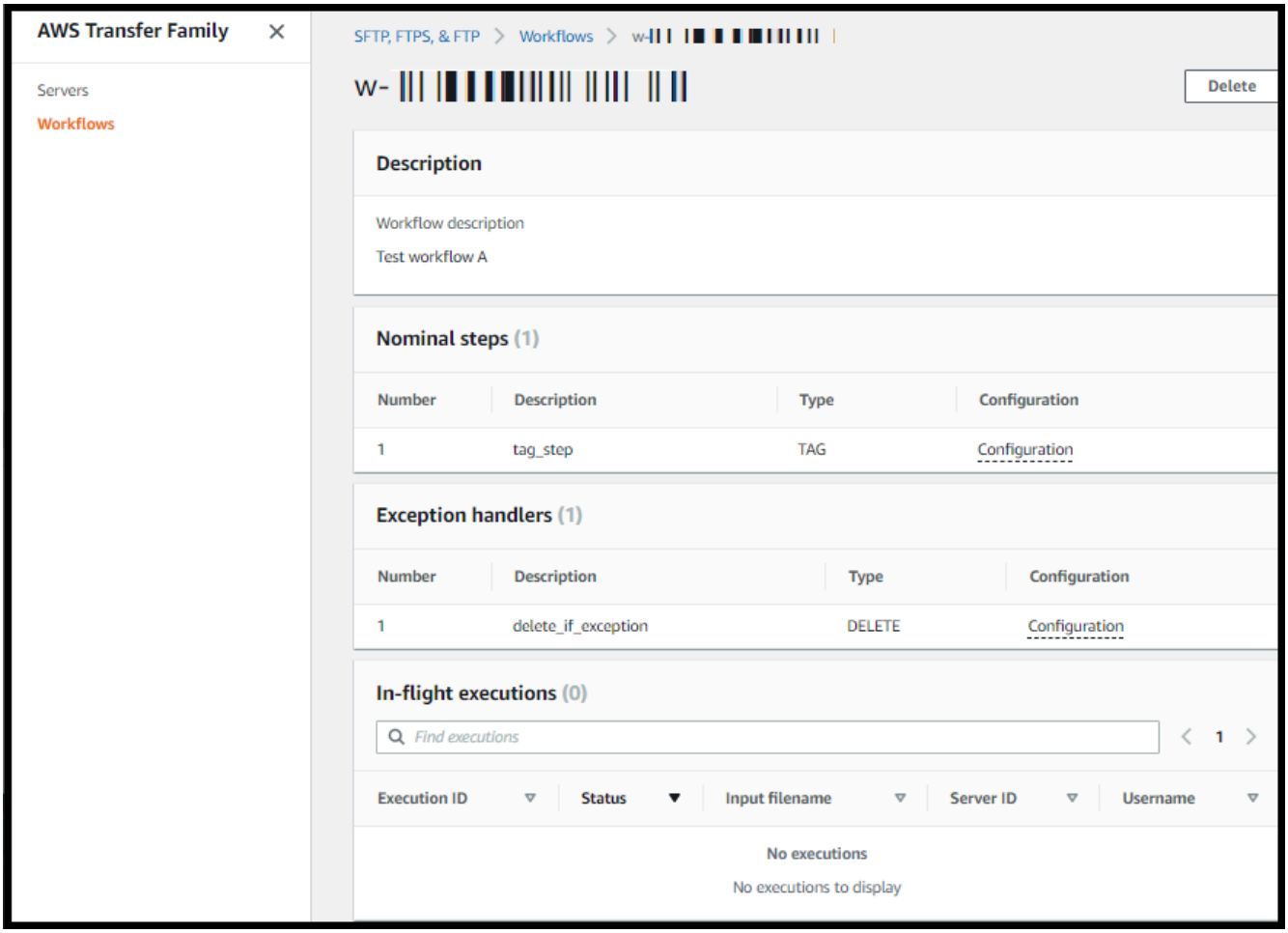
您可以檢視有關先前建立的工作流程或工作流程執行的詳細資訊。若要檢視這些詳細資訊，您可以使用主控台或 AWS Command Line Interface (AWS CLI)。

Console

檢視工作流程詳

1. 開啟主 AWS Transfer Family 控台，網址為 https://console.aws.amazon.com/transfer/。
2. 在左側導覽窗格中，選擇「工作流程」。
3. 在 [工作流程] 頁面上，選擇工作流程。

   工作流程詳細資訊頁即會開啟



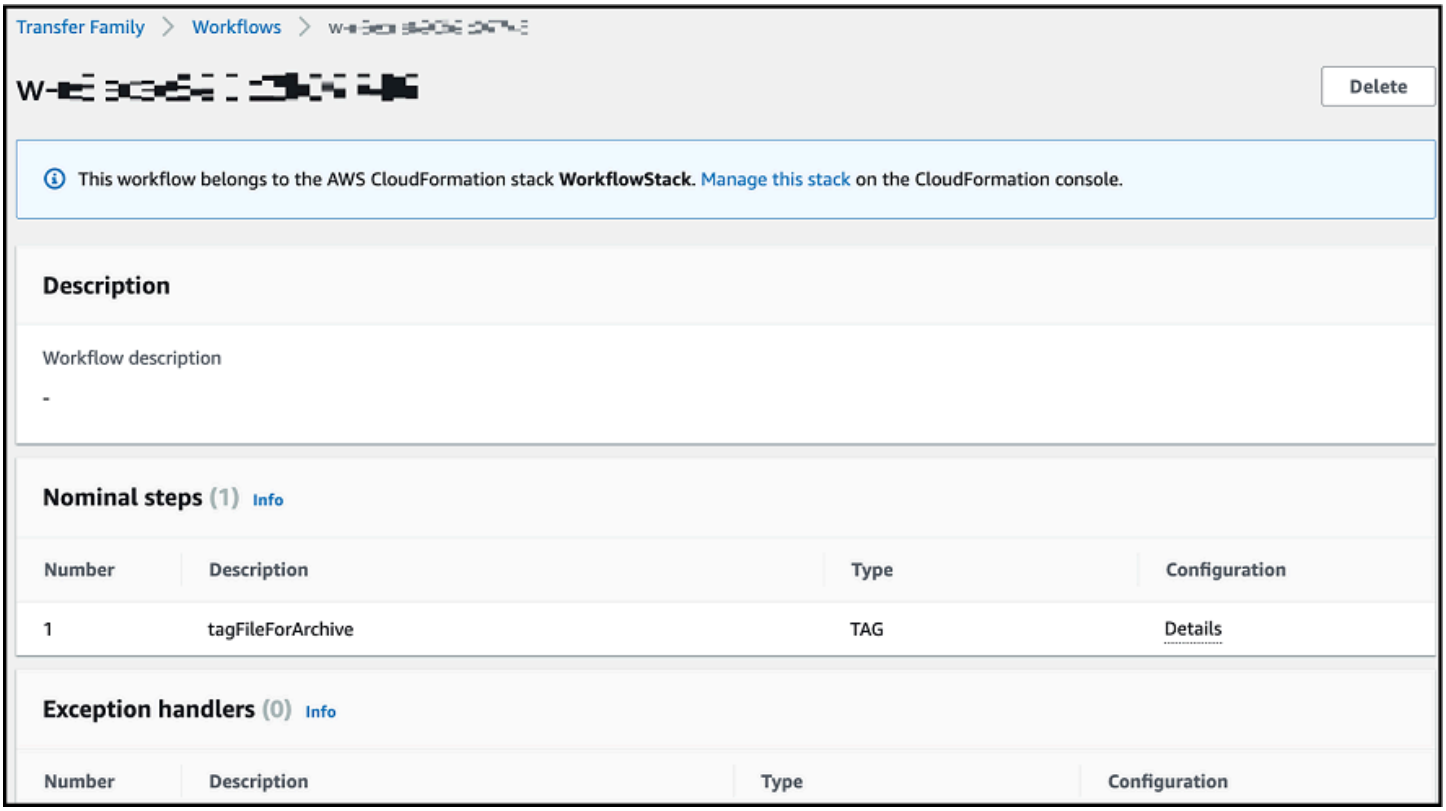
CLI

若要檢視工作流程詳細資訊，請使用 `describe-workflow` CLI 指令，如下列範例所示。將工作流程 ID *w-1234567890abcdef0* 取代為您自己的值。若要取得更多資訊，請參閱《指令參考》中的AWS CLI 描述工作流程。

```
# View Workflow details
> aws transfer describe-workflow --workflow-id w-1234567890abcdef0
{
    "Workflow": {
        "Arn": "arn:aws:transfer:us-east-1:111122223333:workflow/
w-1234567890abcdef0",
        "WorkflowId": "w-1234567890abcdef0",
        "Name": "Copy file to shared_files",
        "Steps": [
            {
                "Type": "COPY",
```

```
                "CopyStepDetails": {
                "Name": "Copy to shared",
                "FileLocation": {
                    "S3FileLocation": {
                        "Bucket": "DOC-EXAMPLE-BUCKET",
                        "Key": "home/shared_files/"
                    }
                }
                }
            }
        ],
        "OnException": {}
    }
}
```

如果您的工作流程是建立為 AWS CloudFormation 堆疊的一部分，您可以使用 AWS CloudFormation 主控台 (https://console.aws.amazon.com/cloudformation) 管理工作流程。



使用預定義步驟

當您建立工作流程時，您可以選擇新增本主題中所討論的下列預先定義步驟之一。您也可以選擇新增自己的自訂檔案處理步驟。如需詳細資訊，請參閱 the section called “使用自訂檔案處理步驟”。

主題

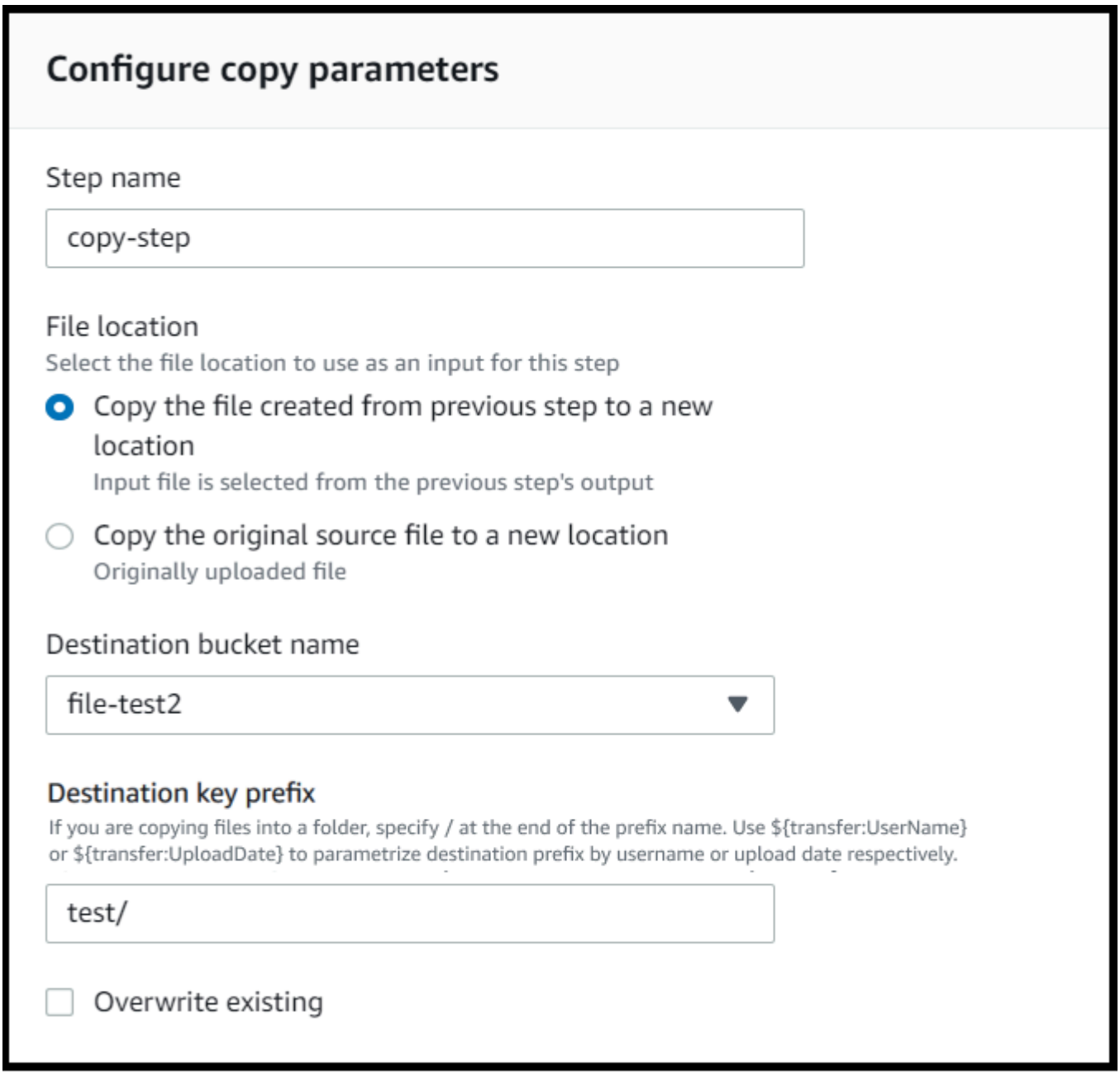
- 複製檔案
- 解密文件
- 標籤檔案
- 刪除檔案
- 工作流程的命名變數
- 範例標記和刪除工作流程

複製檔案

複製檔案步驟會在新的 Amazon S3 位置建立上傳檔案的複本。目前，您只能在 Amazon S3 使用複製檔案步驟。

下列複製檔案步驟會將檔案複製到`file-test`目標值區中的`test`資料夾中。

如果複製檔案步驟不是工作流程的第一步，您可以指定檔案位置。透過指定檔案位置，您可以複製上一個步驟中使用的檔案或上載的原始檔案。您可以使用此功能來製作原始檔案的多個副本，同時保持來源檔案不變，以便保存檔案和記錄保留。如需範例，請參閱範例標記和刪除工作流程。



提供存儲桶和密鑰詳細信息

您必須提供儲存貯體名稱和複製檔案步驟目的地的金鑰。索引鍵可以是路徑名稱或檔案名稱。金鑰是否被視為路徑名稱或檔案名稱，取決於您是否以正斜線 (/) 字元結束金鑰。

如果最後一個字元是/，您的檔案會複製到資料夾中，且其名稱不會變更。如果最後一個字元是英數字元，您上傳的檔案會重新命名為金鑰值。在這種情況下，如果具有該名稱的檔案已存在，則行為取決於 [覆寫現有欄位] 的設定。

- 如果選取「覆寫既有檔案」，則會將現有檔案取代為正在處理的檔案。

- 如果未選取「覆寫現有的」，則不會發生任何反應，工作流程處理會停止。

> **Tip**
>
> 如果同一個檔案路徑上執行並行寫入，則覆寫檔案時可能會導致非預期的行為。

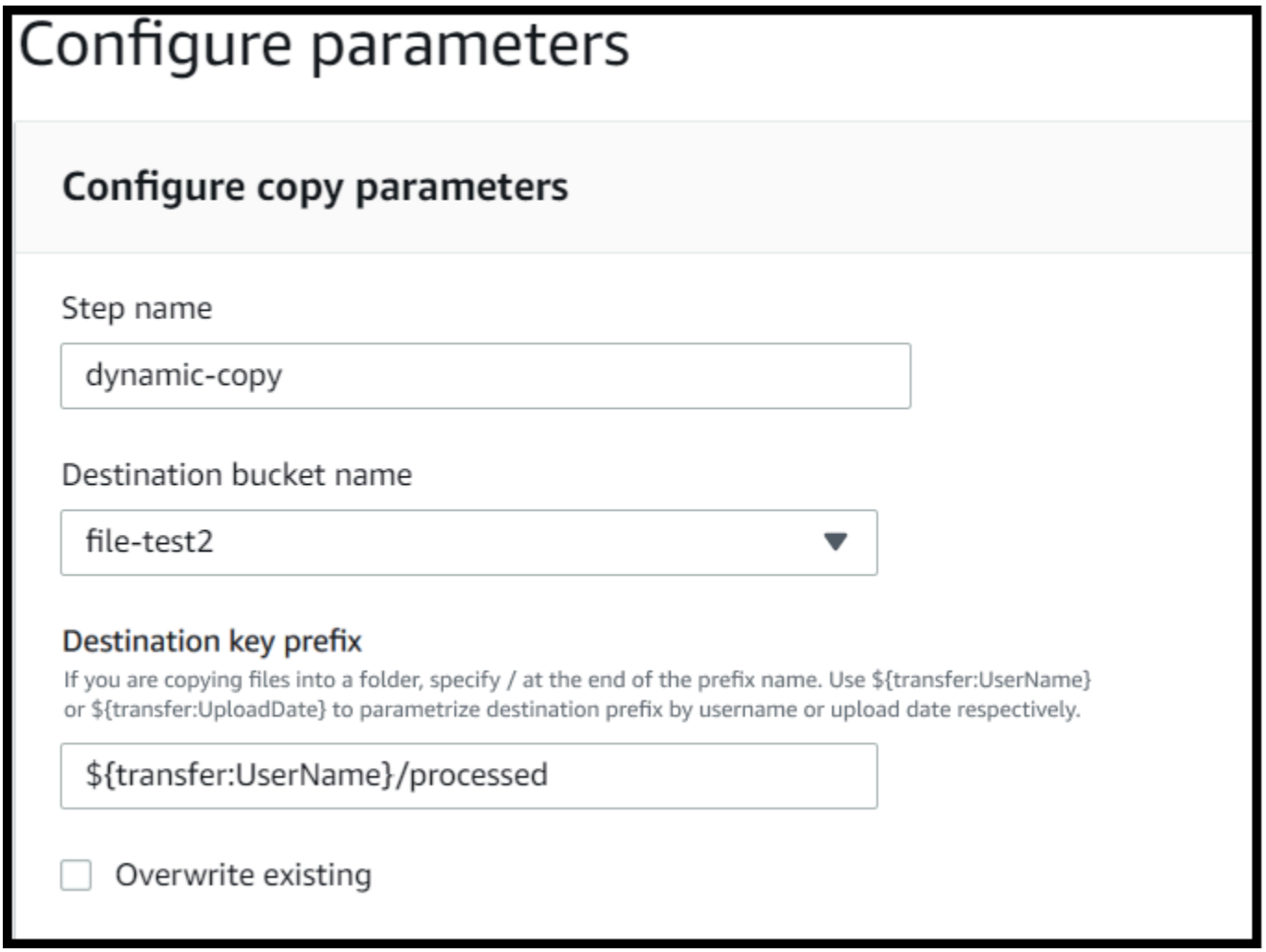
例如，如果您的金鑰值是`test/`，您上傳的檔案就會複製到資`test`料夾。如果您的索引鍵值為 (並且選取了「覆寫現有檔案」)`test/today`，則您上傳的每個檔案都會複製到`test`資料夾`today`中名為的檔案，且每個後續的檔案都會覆寫前一個檔案。

> **Note**
>
> Amazon S3 支援儲存貯體與物件，且沒有任何階層。但是，您可以在物件索引鍵名稱中使用前置字元和分隔符號來暗示階層，並以類似於資料夾的方式組織資料。

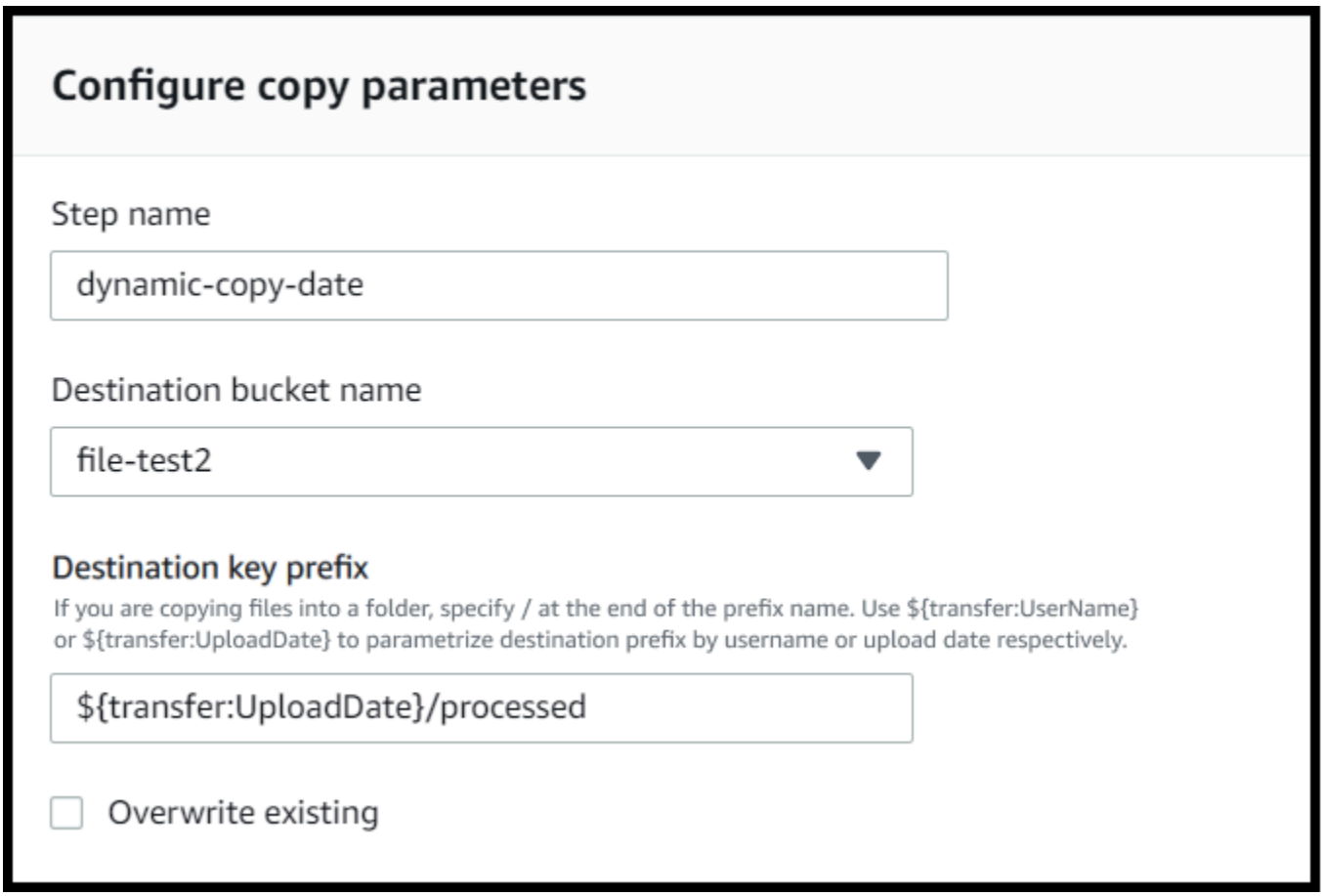
在複製檔案步驟中使用已命名變數

在複製檔案步驟中，您可以使用變數將檔案動態複製到使用者特定的資料夾中。目前，您可以使用`${transfer:UserName}`或`${transfer:UploadDate}`做為變數，將檔案複製到正在上傳檔案之指定使用者的目標位置，或根據目前日期。

在下面的例子中，如果用戶`richard-roe`上傳一個文件，它被複製到文件`file-test2/richard-roe/processed/`夾。如果用戶`mary-major`上傳文件，它將被複製到文件`file-test2/mary-major/processed/`夾中。



同樣地，您也可以用`${transfer:UploadDate}`作變數，將檔案複製到目前日期命名的目標位置。在下列範例中，如果您將目的地設定為 `${transfer:UploadDate}/processed` 2022 年 2 月 1 日，則上傳的檔案會複製到`file-test2/2022-02-01/processed/`資料夾中。



您也可以同時使用這兩個變數，結合其功能。例如：

- 例如，您可以將目標 key prefix 設定為**folder/${transfer:UserName}/${transfer:UploadDate}/**，以建立巢狀資料夾folder/marymajor/2023-01-05/。
- 例folder/marymajor-2023-01-05/如，您可以將目標 key prefix 設置為**folder/${transfer:UserName}-${transfer:UploadDate}/**，以連接兩個變量。

複製步驟的 IAM 許可

若要允許複製步驟成功，請確定工作流程的執行角色包含下列權限。

```
{
            "Sid": "ListBucket",
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": [
                "arn:aws:s3:::destination-bucket-name"
            ]
```

```
        },
        {
            "Sid": "HomeDirObjectAccess",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObjectVersion",
                "s3:DeleteObject",
                "s3:GetObjectVersion"
            ],
            "Resource": "arn:aws:s3:::destination-bucket-name/*"
        }
```

> **Note**
>
> 只有當您未選取 [覆寫現有的] 時，才需要`s3:ListBucket`使用權限。此權限會檢查您的儲存貯體，看看是否已存在具有相同名稱的檔案。如果您已選取 [覆寫現有的]，則工作流程不需要檢查檔案，只要寫入即可。
> 如果您的 Amazon S3 檔案具有標籤，則需要在 IAM 政策中新增一或兩個許可。
>
> - `s3:GetObjectTagging`為未版本控制的 Amazon S3 文件添加。
> - `s3:GetObjectVersionTagging`為版本控制的 Amazon S3 文件添加。

解密文件

AWS 存儲博客有一篇文章，描述瞭如何簡單地解密文件而不使用 Transfer Family 託管工作流程編寫任何代碼，使用 PGP 和 AWS Transfer Family.

在工作流程中使用 PGP 解密

Transfer Family 內置了對相當不錯的隱私（PGP）解密的支持。您可以對透過 SFTP、FTPS 或 FTP 上傳至亞馬遜簡單儲存服務 (Amazon S3) 或亞馬遜彈性檔案系統 (Amazon EFS) 的檔案使用 PGP 解密。

若要使用 PGP 解密，您必須建立並儲存將用於解密檔案的 PGP 私密金鑰。然後，您的使用者可以使用對應的 PGP 加密金鑰來加密檔案，然後再將檔案上傳到 Transfer Family 伺服器。收到加密檔案後，您可以在工作流程中解密這些檔案。如需詳細教學，請參閱設定受管理的工作流程以解密檔案。

若要在工作流程中使用 PGP 解密

1. 識別 Transfer Family 伺服器來託管您的工作流程，或建立新的工作流程。您必須擁有伺服器 ID，才能 AWS Secrets Manager 使用正確的密碼名稱儲存 PGP 金鑰。
2. 將您的 PGP 金鑰儲存 AWS Secrets Manager 在所需的密碼名稱下。如需詳細資訊，請參閱 管理 PGP 金鑰。工作流程可以根據密碼 Secrets Manager 中的密碼名稱，自動找出要用於解密的正確 PGP 金鑰。

   > **Note**
   >
   > 當您將密碼儲存在「Secrets Manager 中時， AWS 帳戶 會產生費用。如需定價的資訊，請參閱 AWS Secrets Manager 定價。

3. 使用 PGP key pair 加密檔案。(如需支援用戶端的清單，請參閱支援的 PGP 用戶端。) 如果您使用的是命令列，請執行下列命令。若要使用此指令，請以您用來建立 PGP key pair 的電子郵件地址取*username@example.com*代。以您要加密的檔案名稱取*testfile.txt*代。

   ```
   gpg -e -r username@example.com testfile.txt
   ```

4. 將加密的文件上傳到您的 Transfer Family 服務器。
5. 在工作流程中設定解密步驟。如需詳細資訊，請參閱 新增解密步驟。

新增解密步驟

解密步驟會將作為工作流程一部分上傳到 Amazon S3 或 Amazon EFS 的加密檔案進行解密。如需配置解密的詳細資訊，請參閱在工作流程中使用 PGP 解密。

當您為工作流程建立解密步驟時，必須指定解密檔案的目的地。您還必須選擇是否覆蓋現有文件，如果文件已存在於目標位置。您可以使用 Amazon Logs 監控解密工作流程結果，並即時取得每個檔案的稽核 CloudWatch 日誌。

選擇步驟的解密檔案類型之後，便會顯示「設定參數」頁面。填入「設定 PGP 解密參數」段落的值。

可用的選項如下：

- 步驟名稱 — 輸入步驟的描述性名稱。
- 檔案位置 — 透過指定檔案位置，您可以解密上一個步驟中使用的檔案或上傳的原始檔案。

> **Note**
>
> 如果此步驟是工作流程的第一個步驟，則無法使用此參數。

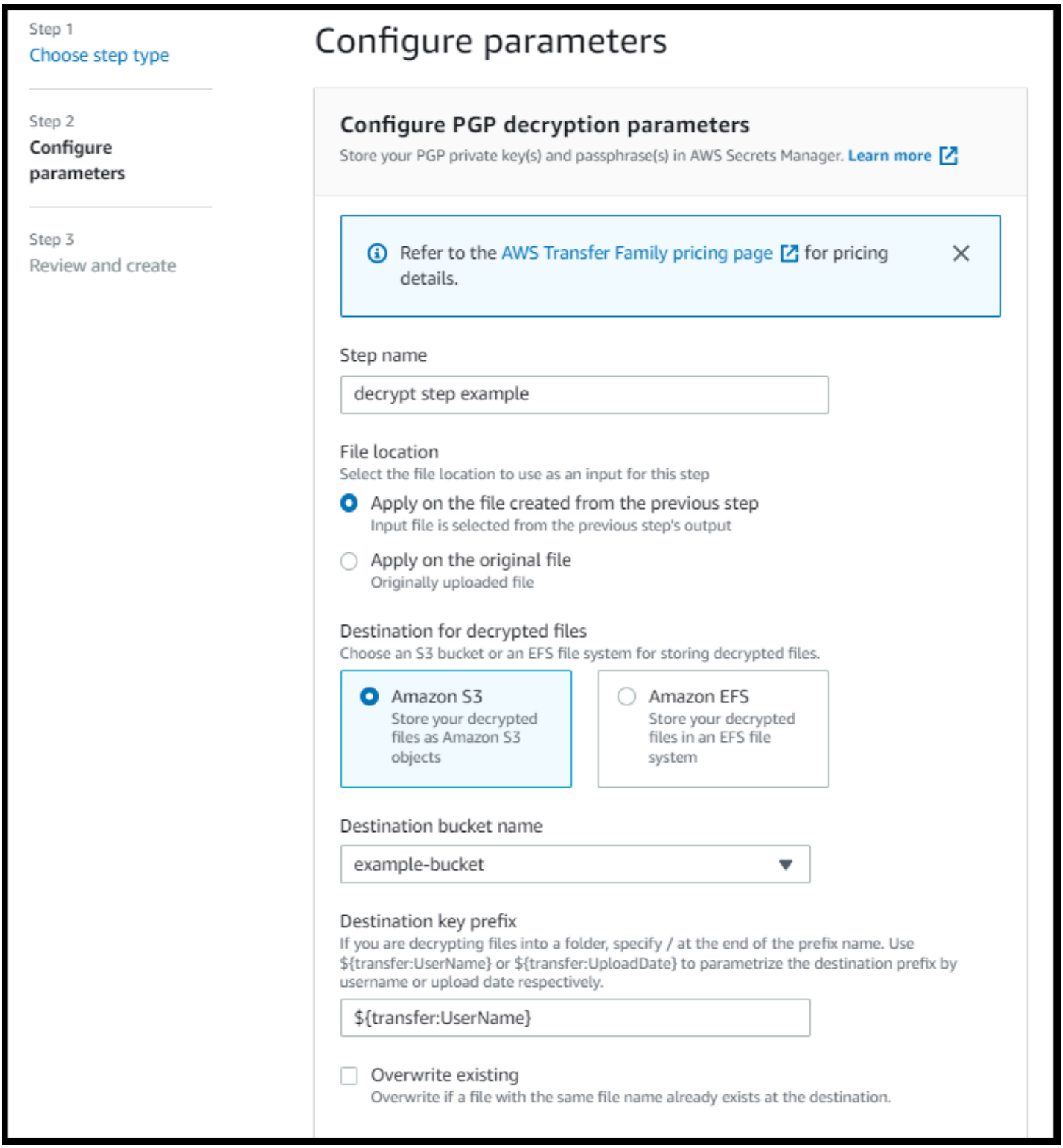
- 解密檔案的目的地 — 選擇 Amazon S3 儲存貯體或 Amazon EFS 檔案系統做為解密檔案的目的地。
  - 如果您選擇 Amazon S3，則必須提供目的地儲存貯體名稱和目的地 key prefix。若要依使用者名稱參數化目的地 key prefix，請輸入目**`${transfer:UserName}`**的地 key prefix。同樣地，若要依上傳日期參數化目的地 key prefix，請輸入目**`${Transfer:UploadDate}`**的地 key prefix。
  - 如果您選擇 Amazon EFS，則必須提供目標檔案系統和路徑。

> **Note**
>
> 您在此選擇的儲存選項必須與此工作流程相關聯的 Transfer Family 伺服器所使用的儲存系統相符。否則，當您嘗試執行此工作流程時，您將會收到錯誤訊息。

- 覆寫現有的 — 如果您上載檔案，且目的地已存在具有相同檔案名稱的檔案，則行為取決於此參數的設定：
  - 如果選取「覆寫既有檔案」，則會將現有檔案取代為正在處理的檔案。
  - 如果未選取「覆寫現有的」，則不會發生任何反應，工作流程處理會停止。

> **Tip**
>
> 如果同一個檔案路徑上執行並行寫入，則覆寫檔案時可能會導致非預期的行為。

下列螢幕擷取畫面顯示您可能會為解密檔案步驟選擇的選項範例。



解密步驟的 IAM 許可

若要允許解密步驟成功，請確定工作流程的執行角色包含下列權限。

```
{
            "Sid": "ListBucket",
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": [
                "arn:aws:s3:::destination-bucket-name"
            ]
        },
        {
            "Sid": "HomeDirObjectAccess",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObjectVersion",
                "s3:DeleteObject",
                "s3:GetObjectVersion"
            ],
            "Resource": "arn:aws:s3:::destination-bucket-name/*"
        },
        {
            "Sid": "Decrypt",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue",
            ],
            "Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/transfer/
*"
        }
```

Note

只有當您未選取 [覆寫現有的] 時，才需要`s3:ListBucket`使用權限。此權限會檢查您的儲存貯體，看看是否已存在具有相同名稱的檔案。如果您已選取 [覆寫現有的]，則工作流程不需要檢查檔案，只要寫入即可。

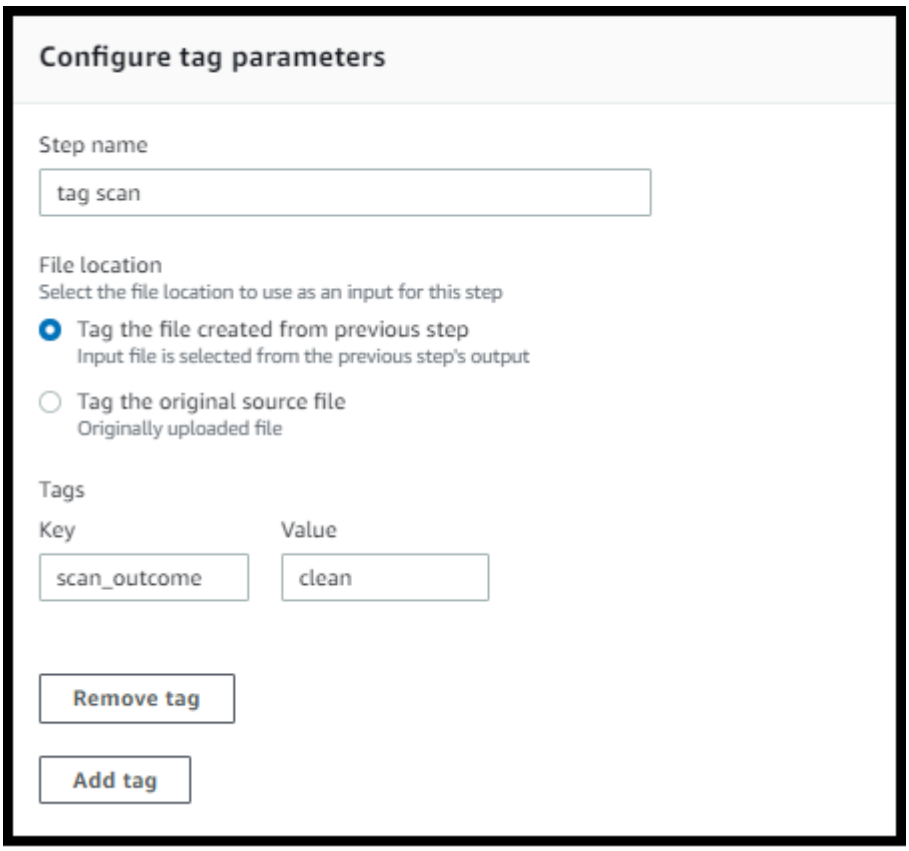
如果您的 Amazon S3 檔案具有標籤，則需要在 IAM 政策中新增一或兩個許可。

- `s3:GetObjectTagging`為未版本控制的 Amazon S3 文件添加。
- `s3:GetObjectVersionTagging`為版本控制的 Amazon S3 文件添加。

標籤檔案

若要標記傳入檔案以便進一步下游處理，請使用標籤步驟。輸入您要指定給內送檔案的標籤值。目前，只有在您將 Amazon S3 用於 Transfer Family 伺服器儲存時，才支援標籤操作。

下列範例標籤步驟會分別指派`scan_outcome`並`clean`做為標籤鍵和值。



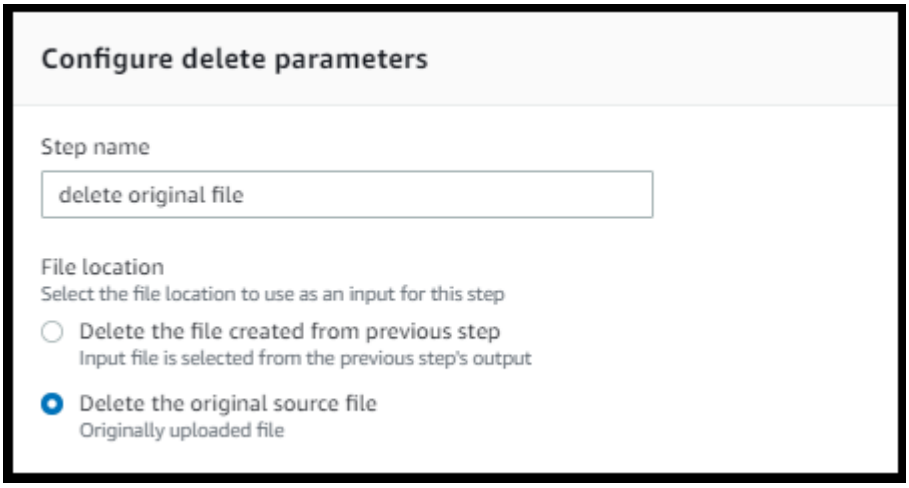
若要允許標籤步驟成功，請確定工作流程的執行角色包含下列權限。

```
{
            "Sid": "Tag",
            "Effect": "Allow",
            "Action": [
                "s3:PutObjectTagging",
                "s3:PutObjectVersionTagging"
            ],
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
            ]
}
```

> **Note**
>
> 如果您的工作流程包含在複製或解密步驟之前執行的標記步驟，則需要在 IAM 政策中新增一或兩個許可。
>
> - `s3:GetObjectTagging`為未版本控制的 Amazon S3 文件添加。
> - `s3:GetObjectVersionTagging`為版本控制的 Amazon S3 文件添加。

刪除檔案

若要從先前的工作流程步驟中刪除已處理的檔案，或刪除最初上傳的檔案，請使用刪除檔案步驟。



若要允許刪除步驟成功，請確定工作流程的執行角色包含下列權限。

```
{
            "Sid": "Delete",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteObjectVersion",
                "s3:DeleteObject"
            ],
            "Resource": "arn:aws:secretsmanager:region:account-ID:secret:aws/transfer/
*"
        }
```

工作流程的命名變數

對於複製和解密步驟，您可以使用變數來動態執行動作。目前， AWS Transfer Family 支援下列命名變數。

- 用`${transfer:UserName}`於根據上傳檔案的使用者，將檔案複製或解密到目的地。
- 用`${transfer:UploadDate}`於根據目前日期將檔案複製或解密到目標位置。

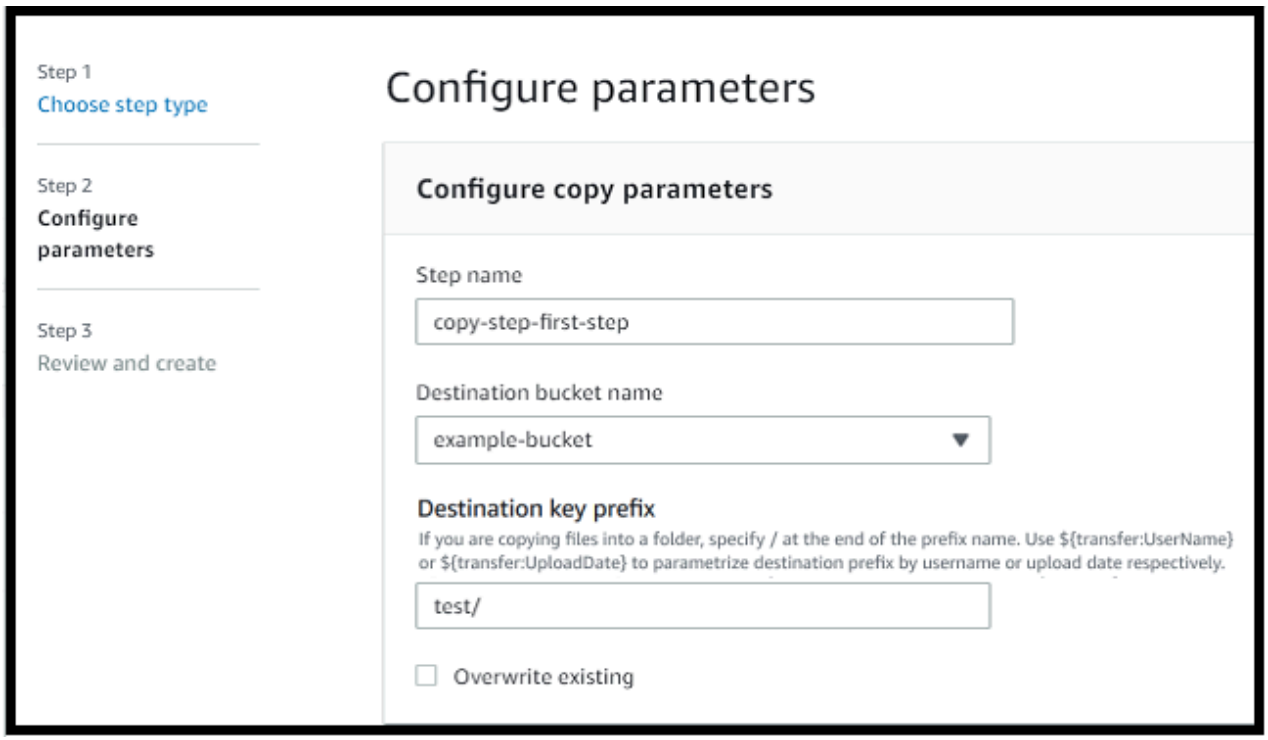
範例標記和刪除工作流程

下列範例說明工作流程，該工作流程會標記需要由下游應用程式 (例如資料分析平台) 處理的傳入檔案。標記傳入檔案後，工作流程會刪除最初上傳的檔案，以節省儲存成本。

Console

範例標籤和移動工作流程

1. 開啟主 AWS Transfer Family 控台，網址為 https://console.aws.amazon.com/transfer/。
2. 在左側導覽窗格中，選擇「工作流程」。
3. 在 [工作流程] 頁面上選擇 [建立工作流程
4. 在 [建立工作流程] 頁面上，輸入描述。此描述顯示在 [工作流程] 頁面上。
5. 新增第一個步驟 (複製)。
   a. 在「標稱步驟」區段中，選擇「新增步驟」。
   b. 選擇複製檔案，然後選擇「下一步」。
   c. 輸入步驟名稱，然後選取目的地值區和 key prefix。



d. 選擇「下一步」，然後檢閱該步驟的詳細資料。

e. 選擇 [建立步驟] 以新增步驟並繼續。

6. 新增第二個步驟 (標籤)。

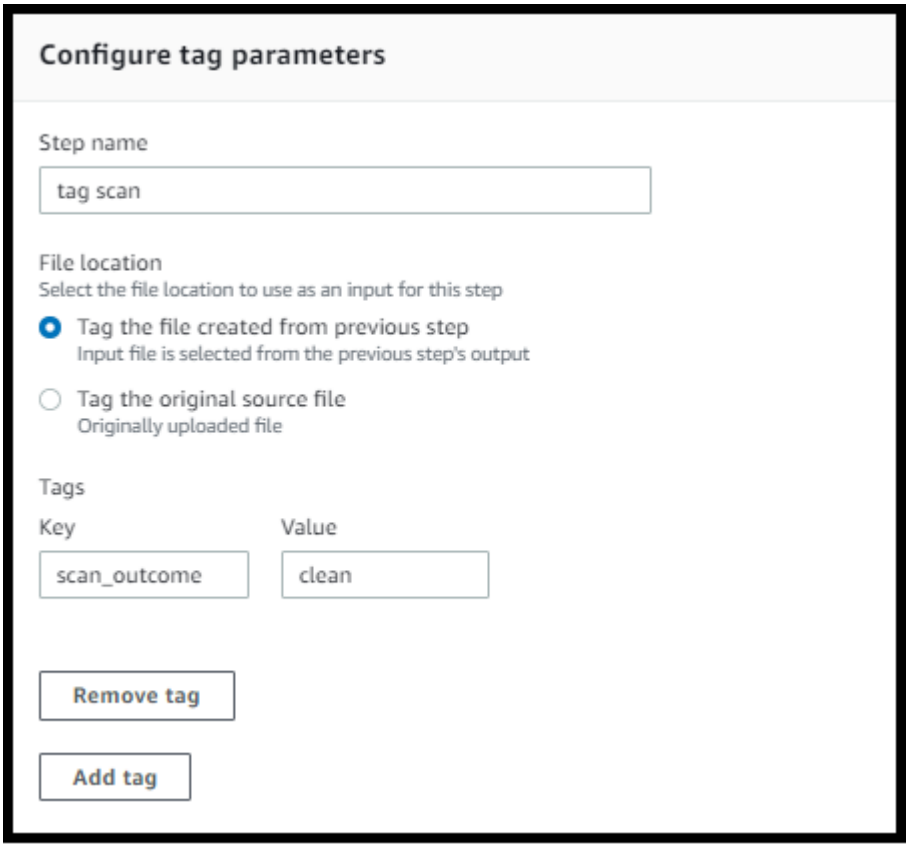
a. 在「標稱步驟」區段中，選擇「新增步驟」。

b. 選擇標記檔案，然後選擇下一步。

c. 輸入步驟名稱。

d. 對於「檔案位置」，選取「標記從上一步建立的檔案」。

e. 輸入Key (索引鍵) 和 Value (值)。



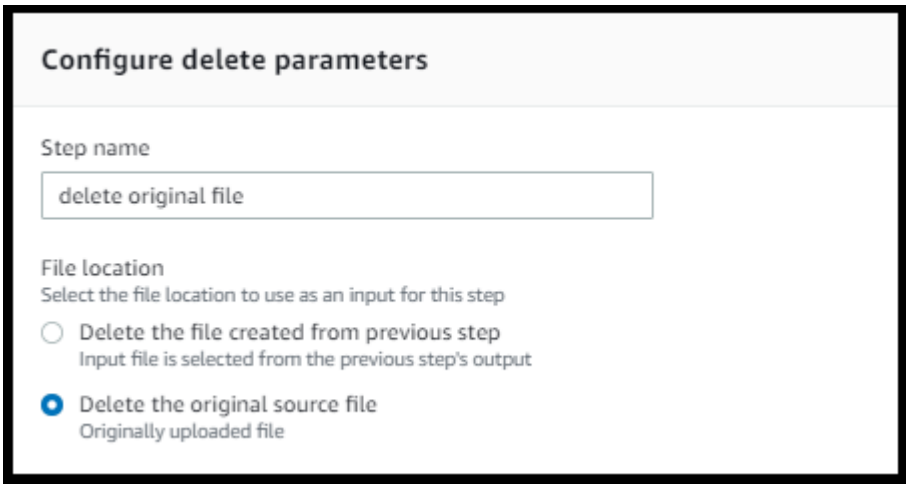
f. 選擇「下一步」，然後檢閱該步驟的詳細資料。

g. 選擇 [建立步驟] 以新增步驟並繼續。

7. 添加第三步（刪除）。

a. 在「標稱步驟」區段中，選擇「新增步驟」。

b. 選擇刪除檔案，然後選擇下一步。



c. 輸入步驟名稱。

d. 對於「檔案位置」，選取「刪除原始來源檔案」。

e. 選擇「下一步」，然後檢閱該步驟的詳細資料。

f. 選擇 [建立步驟] 以新增步驟並繼續。

8. 檢閱工作流程設定，然後選擇 [建立工作流程]。

CLI

範例標籤和移動工作流程

1. 將下列程式碼儲存到檔案中；例如，tagAndMoveWorkflow.json。將每個 *user input placeholder* 替換成您自己的資訊。

```
[
   {
       "Type": "COPY",
       "CopyStepDetails": {
          "Name": "CopyStep",
          "DestinationFileLocation": {
             "S3FileLocation": {
                "Bucket": "DOC-EXAMPLE-BUCKET",
                "Key": "test/"
             }
          }
       }
   },
   {
       "Type": "TAG",
       "TagStepDetails": {
          "Name": "TagStep",
          "Tags": [
             {
                "Key": "name",
                "Value": "demo"
             }
          ],
          "SourceFileLocation": "${previous.file}"
       }
   },
   {
      "Type": "DELETE",
      "DeleteStepDetails":{
```

```
        "Name":"DeleteStep",
        "SourceFileLocation": "${original.file}"
      }
  }
]
```

第一個步驟會將上傳的檔案複製到新的 Amazon S3 位置。第二個步驟會在複製到新位置的檔案 (`previous.file`) 加入標籤 (鍵值組)。最後，第三步刪除原始文件（`original.file`）。

2. 從儲存的檔案建立工作流程。將每個 *user input placeholder* 替換成您自己的資訊。

```
aws transfer create-workflow --description "short-description" --steps
 file://path-to-file --region region-ID
```

例如：

```
aws transfer create-workflow --description "copy-tag-delete workflow" --steps
 file://tagAndMoveWorkflow.json --region us-east-1
```

> **Note**
>
> 如需有關使用檔案載入參數的詳細資訊，請參閱如何從檔案載入參數。

3. 更新現有伺服器。

> **Note**
>
> 此步驟假設您已經擁有 Transfer Family 伺服器，並且想要將工作流程與其建立關聯。如果沒有，請參閱 設定 SFTP、FTPS 或 FTP 伺服器端點。將每個 *user input placeholder* 替換成您自己的資訊。

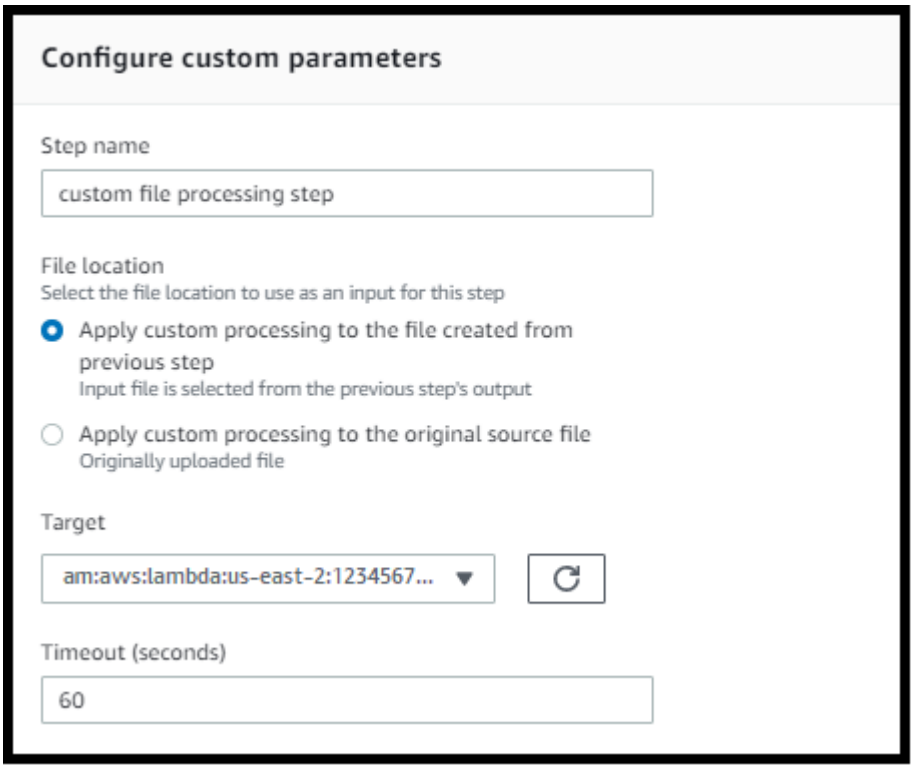
```
aws transfer update-server --server-id server-ID --region region-ID
  --workflow-details '{"OnUpload":[{ "WorkflowId": "workflow-
ID","ExecutionRole": "execution-role-ARN"}]}'
```

例如：

```
aws transfer update-server --server-id s-1234567890abcdef0 --region us-east-2
  --workflow-details '{"OnUpload":[{ "WorkflowId": "w-
abcdef01234567890","ExecutionRole": "arn:aws:iam::111111111111:role/nikki-wolf-
execution-role"}]}'
```

使用自訂檔案處理步驟

透過使用自訂檔案處理步驟，您可以使用. AWS Lambda傳送系列伺服器會在檔案送達時叫用 Lambda 函數，該函數包含自訂檔案處理邏輯，例如加密檔案、掃描惡意軟體或檢查是否有不正確的檔案類型。在下面的例子中，target AWS Lambda 函數用於處理從上一步的輸出文件。



> **Note**
>
> 如需 Lambda 函數的範例，請參閱自訂工作流程步驟的 Lambda 函數範例。如需事件範例 (包括傳遞至 Lambda 的檔案位置)，請參閱檔案上傳時傳送至 AWS Lambda 的範例事件。

透過自訂工作流程步驟，您必須設定 Lambda 函數來呼叫 SendWorkflowStepStateAPI 作業。 SendWorkflowStepState通知工作流程執行步驟已完成，且狀態為成功或失敗狀

態。SendWorkflowStepStateAPI 作業的狀態會根據 Lambda 函數的結果，叫用例外狀況處理常式步驟或線性序列中的名義步驟。

如果 Lambda 函數失敗或逾時，步驟會失敗，您會在 CloudWatch 記錄StepErrored中看到。如果 Lambda 函數是標稱步驟的一部分，且函數回應時為SendWorkflowStepStateStatus="FAILURE"或逾時，流程會繼續執行例外處理常式步驟。在此情況下，工作流程不會繼續執行剩餘 (如果有的話) 名義步驟。如需詳細資訊，請參閱工作流程的異常處理。

當您呼叫 SendWorkflowStepState API 作業時，您必須傳送下列參數：

```
{
    "ExecutionId": "string",
    "Status": "string",
    "Token": "string",
    "WorkflowId": "string"
}
```

您可以WorkflowId從執行 Lambda 函數時傳遞的輸入事件中擷取Token、和 (範例如下列各節所示)。ExecutionIdStatus值可以是SUCCESS或FAILURE。

若要從 Lambda 函數呼叫 SendWorkflowStepState API 作業，您必須使用在引入受管工作流程之後發佈的 AWS SDK 版本。

連續使用多個 Lambda 函數

當您一個接一個地使用多個自訂步驟時，「檔案位置」選項的運作方式與僅使用單一自訂步驟時不同。傳輸 Transfer Family 不支持將 Lambda 處理的文件傳回以用作下一步的輸入。因此，如果您有多個自訂步驟全部設定為使用該previous.file選項，它們都會使用相同的檔案位置 (第一個自訂步驟的輸入檔案位置)。

> **Note**
>
> 如果您在自訂步驟之後有預先previous.file定義的步驟 (標記、複製、解密或刪除)，則此設定的運作方式也會有所不同。如果將預先定義的步驟配置為使用previous.file設定，則預先定義的步驟會使用自訂步驟所使用的相同輸入檔案。自訂步驟中已處理的檔案不會傳遞至預先定義的步驟。

在自訂處理後存取檔案

如果您使用 Amazon S3 做為儲存，並且工作流程中包含對原始上傳檔案執行動作的自訂步驟，則後續步驟將無法存取該已處理的檔案。也就是說，自訂步驟之後的任何步驟都無法參照自訂步驟輸出中的更新檔案。

例如，假設您在工作流程中有以下三個步驟。

- 步驟 1 — 上傳名為的檔案`example-file.txt`。
- 第 2 步-調用以某種方式更改`example-file.txt`的 Lambda 函數。
- 步驟 3 — 嘗試對的更新版本執行進一步處理`example-file.txt`。

如果您將步驟 3 設定`sourceFileLocation`為`${original.file}`，步驟 3 會使用伺服器將檔案上傳到步驟 1 中儲存時的原始檔案位置。如果您使用`${previous.file}`的是步驟 3，步驟 3 會重複使用步驟 2 做為輸入的檔案位置。

因此，步驟 3 會導致錯誤。例如，如果步驟 3 嘗試複製更新的`example-file.txt`，您會收到下列錯誤：

```
{
    "type": "StepErrored",
    "details": {
        "errorType": "NOT_FOUND",
        "errorMessage": "ETag constraint not met (Service: null; Status Code: 412;
 Error Code: null; Request ID: null; S3 Extended Request ID: null; Proxy: null)",
        "stepType": "COPY",
        "stepName": "CopyFile"
    },
```

之`example-file.txt`所以發生這個錯誤，是因為自訂步驟會修改實體標籤 (ETag)，使其與原始檔案不符。

> **Note**
>
> 如果您使用 Amazon EFS，則不會發生此行為，因為 Amazon EFS 不會使用實體標籤來識別檔案。

檔案上傳時傳送至 AWS Lambda 的範例事件

下列範例顯示檔案上傳完成 AWS Lambda 時傳送至的事件。其中一個範例使用 Transfer Family 伺服器，該伺服器使用 Amazon S3 設定網域。另一個範例使用網域使用 Amazon EFS 的 Transfer Family 伺服器。

Custom step that uses an Amazon S3 domain

```
{
    "token": "MzI0Nzc4ZDktMGRmMi00MjFhLTgxMjUtYWZmZmRmODNkYjc0",
    "serviceMetadata": {
        "executionDetails": {
            "workflowId": "w-1234567890example",
            "executionId": "abcd1234-aa11-bb22-cc33-abcdef123456"
        },
        "transferDetails": {
            "sessionId": "36688ff5d2deda8c",
            "userName": "myuser",
            "serverId": "s-example1234567890"
        }
    },
    "fileLocation": {
        "domain": "S3",
        "bucket": "DOC-EXAMPLE-BUCKET",
        "key": "path/to/mykey",
        "eTag": "d8e8fca2dc0f896fd7cb4cb0031ba249",
        "versionId": null
    }
}
```

Custom step that uses an Amazon EFS domain

```
{
    "token": "MTg0N2Y3N2UtNWI5Ny00ZmZlLTk5YTgtZTU3YzViYjllNmZm",
    "serviceMetadata": {
        "executionDetails": {
            "workflowId": "w-1234567890example",
            "executionId": "abcd1234-aa11-bb22-cc33-abcdef123456"
        },
        "transferDetails": {
            "sessionId": "36688ff5d2deda8c",
            "userName": "myuser",
```

```
            "serverId": "s-example1234567890"
        }
    },
    "fileLocation": {
        "domain": "EFS",
        "fileSystemId": "fs-1234567",
        "path": "/path/to/myfile"
    }
}
```

自訂工作流程步驟的 Lambda 函數範例

下列 Lambda 函數擷取有關執行狀態的資訊，然後呼叫 SendWorkflowStepStateAPI 作業，將狀態傳回至該步驟的工作流程 (或) SUCCESS。FAILURE在函數呼叫 SendWorkflowStepState API 作業之前，您可以設定 Lambda 根據工作流程邏輯採取動作。

```
import json
import boto3

transfer = boto3.client('transfer')

def lambda_handler(event, context):
    print(json.dumps(event))

    # call the SendWorkflowStepState API to notify the workflow about the step's
 SUCCESS or FAILURE status
    response = transfer.send_workflow_step_state(
        WorkflowId=event['serviceMetadata']['executionDetails']['workflowId'],
        ExecutionId=event['serviceMetadata']['executionDetails']['executionId'],
        Token=event['token'],
        Status='SUCCESS|FAILURE'
    )

    print(json.dumps(response))

    return {
      'statusCode': 200,
      'body': json.dumps(response)
    }
```

自訂步驟的 IAM 許可

若要允許呼叫 Lambda 的步驟成功，請確定工作流程的執行角色包含下列權限。

```
{
            "Sid": "Custom",
            "Effect": "Allow",
            "Action": [
                "lambda:InvokeFunction"
            ],
            "Resource": [
                "arn:aws:lambda:region:account-id:function:function-name"
            ]
        }
```

工作流程的 IAM 政策

將工作流程新增至伺服器時，必須選取執行角色。伺服器會在執行工作流程時使用此角色。如果角色沒有適當的權限，則 AWS Transfer Family 無法執行工作流程。

本節說明可用於執行工作流程的一組 AWS Identity and Access Management (IAM) 許可。本主題稍後會說明其他範例。

> **Note**
>
> 如果您的 Amazon S3 檔案具有標籤，則需要在 IAM 政策中新增一或兩個許可。
>
> - `s3:GetObjectTagging`為未版本控制的 Amazon S3 文件添加。
> - `s3:GetObjectVersionTagging`為版本控制的 Amazon S3 文件添加。

若要建立工作流程的執行角色

1. 建立新的 IAM 角色，並將受 AWS 管政策新增`AWSTransferFullAccess`至角色。如需建立新 IAM 角色的詳細資訊，請參閱the section called “建立 IAM 角色和政策”。
2. 建立具有下列權限的另一個原則，並將其附加至您的角色。將每個 *user input placeholder* 替換成您自己的資訊。

   ```
   {
       "Version": "2012-10-17",
   ```

```
    "Statement": [
        {
            "Sid": "ConsoleAccess",
            "Effect": "Allow",
            "Action": "s3:GetBucketLocation",
            "Resource": "*"
        },
        {
            "Sid": "ListObjectsInBucket",
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
            ]
        },
        {
            "Sid": "AllObjectActions",
            "Effect": "Allow",
            "Action": "s3:*Object",
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
            ]
        },
        {
            "Sid": "GetObjectVersion",
            "Effect": "Allow",
            "Action": "s3:GetObjectVersion",
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
            ]
        },
        {
            "Sid": "Custom",
            "Effect": "Allow",
            "Action": [
                "lambda:InvokeFunction"
            ],
            "Resource": [
                "arn:aws:lambda:region:account-id:function:function-name"
            ]
        },
        {
            "Sid": "Tag",
            "Effect": "Allow",
```

```
            "Action": [
                "s3:PutObjectTagging",
                "s3:PutObjectVersionTagging"
            ],
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
            ]
        }
    ]
}
```

3. 儲存此角色，並在將工作流程新增至伺服器時將其指定為執行角色。

> **Note**
>
> 建構 IAM 角色時， AWS 建議您盡可能限制工作流程對資源的存取。

工作流信任關係

工作流程執行角色也需要與信任關係`transfer.amazonaws.com`。若要建立的信任關係 AWS Transfer Family，請參閱建立信任關係。

當你建立你的信任關係, 你也可以採取措施，以避免混淆的副問題. 如需此問題的說明，以及如何避免此問題的範例，請參閱the section called “預防跨服務混淆代理人”。

範例執行角色：解密、複製和標記

如果您的工作流程包含標記、複製和解密步驟，則可以使用下列 IAM 政策。將每個 *user input placeholder* 替換成您自己的資訊。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CopyRead",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectTagging",
                "s3:GetObjectVersionTagging"
            ],
```

```
            "Resource": "arn:aws:s3:::source-bucket-name/*"
        },
        {
            "Sid": "CopyWrite",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:PutObjectTagging"
            ],
            "Resource": "arn:aws:s3:::destination-bucket-name/*"
        },
        {
            "Sid": "CopyList",
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": [
                "arn:aws:s3:::source-bucket-name",
                "arn:aws:s3:::destination-bucket-name"
            ]
        },
        {
            "Sid": "Tag",
            "Effect": "Allow",
            "Action": [
                "s3:PutObjectTagging",
                "s3:PutObjectVersionTagging"
            ],
            "Resource": "arn:aws:s3:::destination-bucket-name/*",
            "Condition": {
                "StringEquals": {
                    "s3:RequestObjectTag/Archive": "yes"
                }
            }
        },
        {
            "Sid": "ListBucket",
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": [
                "arn:aws:s3:::destination-bucket-name"
            ]
        },
        {
            "Sid": "HomeDirObjectAccess",
```

```
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObjectVersion",
                "s3:DeleteObject",
                "s3:GetObjectVersion"
            ],
            "Resource": "arn:aws:s3:::destination-bucket-name/*"
        },
        {
            "Sid": "Decrypt",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": "arn:aws:secretsmanager:region:account-ID:secret:aws/transfer/
*"
        }
    ]
}
```

示例執行角色：運行函數並刪除

在此範例中，您有一個叫用 AWS Lambda 函數的工作流程。如果工作流程刪除了上傳的檔案，並且具有例外處理程式步驟來處理上一個步驟中失敗的工作流程執行，請使用下列 IAM 政策。將每個 *user input placeholder* 替換成您自己的資訊。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Delete",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteObject",
                "s3:DeleteObjectVersion"
            ],
            "Resource": "arn:aws:s3:::bucket-name"
        },
        {
            "Sid": "Custom",
            "Effect": "Allow",
```

```
            "Action": [
                "lambda:InvokeFunction"
            ],
            "Resource": [
                "arn:aws:lambda:region:account-id:function:function-name"
            ]
        }
    ]
}
```

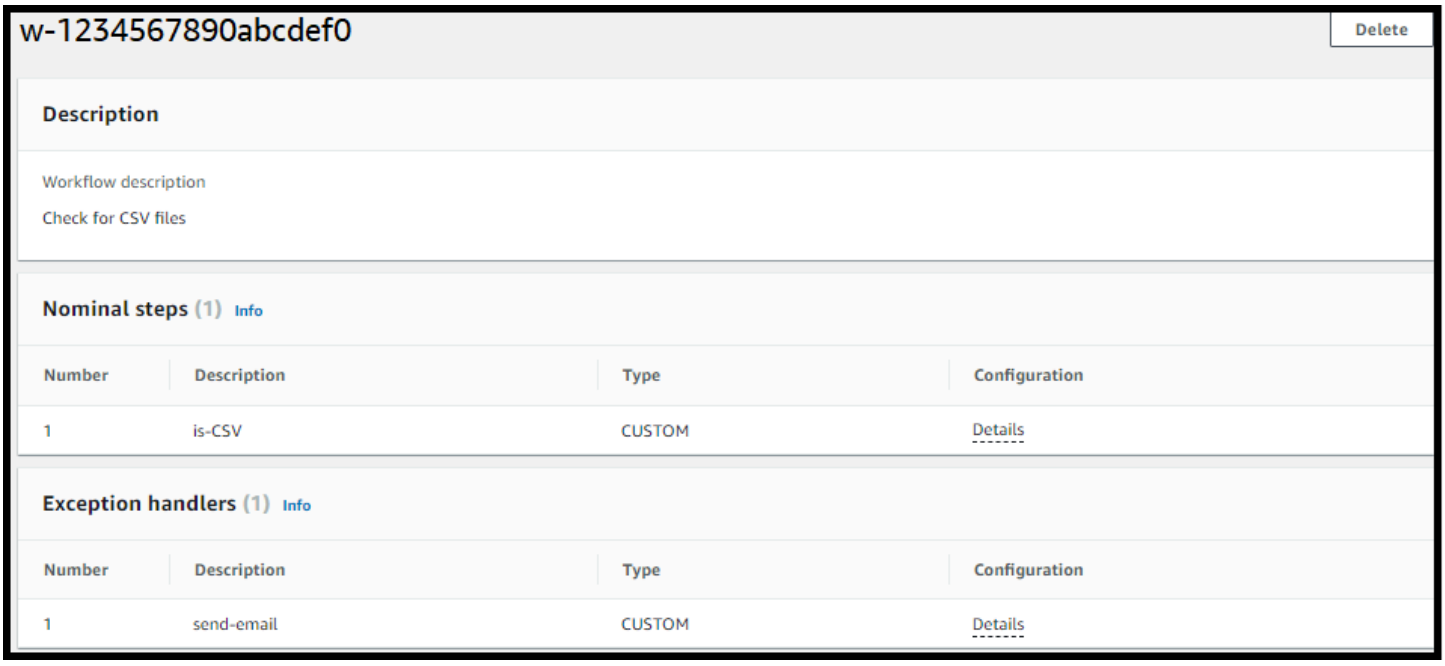
工作流程的異常處理

如果工作流程執行期間發生任何錯誤，則會執行您指定的例外狀況處理步驟。您可以使用與指定工作流程標稱步驟相同的方式來指定工作流程的錯誤處理步驟。例如，假設您已在標稱步驟中設定自訂處理來驗證傳入檔案。如果檔案驗證失敗，例外狀況處理步驟可以傳送電子郵件給系統管理員。

下列工作流程範例包含兩個步驟：

- 檢查上傳的文件是否為 CSV 格式的標稱步驟
- 例外狀況處理步驟，可在上傳的檔案不是 CSV 格式且標稱步驟失敗時傳送電子郵件

若要啟動例外狀況處理步驟，標稱步驟中的 AWS Lambda 函數必須以回應。`Status="FAILURE"`如需有關工作流程中錯誤處理的詳細資訊，請參閱the section called “使用自訂檔案處理步驟”。



監控工作流執行

Amazon 會即時 CloudWatch 監控您的 AWS 資源和執行 AWS 雲端 的應用程式。您可以使用 Amazon CloudWatch 收集和追蹤指標，這些指標是您可以為工作流程測量的變數。您可以使用 Amazon 檢視工作流程指標和整合日誌 CloudWatch。

CloudWatch 工作流程的記錄

CloudWatch 為工作流程進度和結果提供合併的稽核和記錄。

檢視工作流程的 Amazon CloudWatch 日誌

1. 在以下位置打開 Amazon CloudWatch 控制台 https://console.aws.amazon.com/cloudwatch/。
2. 在左側導覽窗格中，選擇「記錄檔」，然後選擇「記錄群組」。
3. 在 [記錄群組] 頁面的導覽列上，為您的 AWS Transfer Family 伺服器選擇正確的 [區域]。
4. 選擇與您的伺服器對應的記錄群組。

   例如，如果您的伺服器 ID 是`s-1234567890abcdef0`，則您的記錄群組為`/aws/transfer/s-1234567890abcdef0`。
5. 在伺服器的日誌群組詳細資料頁面上，會顯示最新的記錄資料流。您正在探索的使用者有兩個記錄資料流：

   - 每個安全殼層 (SSH) 檔案傳輸通訊協定 (SFTP) 工作階段各一個。
   - 一個用於為您的伺服器執行的工作流程。工作流程的記錄資料流格式為*`username`*`.`*`workflowID`*`.`*`uniqueStreamSuffix`*。

   例如，如果您的使用者是`mary-major`，則會有下列記錄資料流：

```
mary-major-east.1234567890abcdef0
mary.w-abcdef01234567890.021345abcdef6789
```

> **Note**
>
> 此範例中列出的 16 位數字英數識別碼是虛構的。您在 Amazon 看到的值 CloudWatch 是不同的。

的 [記錄事件] 頁面會mary-major-usa-east.1234567890abcdef0顯示每個使用者階段作業的詳細資訊，而mary.w-abcdef01234567890.021345abcdef6789記錄資料流則包含工作流程的詳細資訊。

以下是以包含複製步驟的工作流程 (w-abcdef01234567890) 為mary.w-abcdef01234567890.021345abcdef6789基礎的範例記錄資料流。

```
{
    "type": "ExecutionStarted",
    "details": {
        "input": {
            "initialFileLocation": {
                "bucket": "DOC-EXAMPLE-BUCKET",
                "key": "mary/workflowSteps2.json",
                "versionId": "version-id",
                "etag": "etag-id"
            }
        }
    },
    "workflowId":"w-abcdef01234567890",
    "executionId":"execution-id",
    "transferDetails": {
        "serverId":"s-server-id",
        "username":"mary",
        "sessionId":"session-id"
    }
},
{
    "type":"StepStarted",
    "details": {
        "input": {
            "fileLocation": {
                "backingStore":"S3",
                "bucket":"DOC-EXAMPLE-BUCKET",
                "key":"mary/workflowSteps2.json",
                "versionId":"version-id",
                "etag":"etag-id"
            }
        },
        "stepType":"COPY",
        "stepName":"copyToShared"
    },
    "workflowId":"w-abcdef01234567890",
```

```
    "executionId":"execution-id",
    "transferDetails": {
        "serverId":"s-server-id",
        "username":"mary",
        "sessionId":"session-id"
    }
},
{
    "type":"StepCompleted",
    "details":{
        "output":{},
        "stepType":"COPY",
        "stepName":"copyToShared"
    },
    "workflowId":"w-abcdef01234567890",
    "executionId":"execution-id",
    "transferDetails":{
        "serverId":"server-id",
        "username":"mary",
        "sessionId":"session-id"
    }
},
{
    "type":"ExecutionCompleted",
    "details": {},
    "workflowId":"w-abcdef01234567890",
    "executionId":"execution-id",
    "transferDetails":{
        "serverId":"s-server-id",
        "username":"mary",
        "sessionId":"session-id"
    }
}
```

CloudWatch 工作流程的指標

AWS Transfer Family 提供工作流程的數個指標。您可以檢視前一分鐘開始、成功完成和失敗的工作流程執行數目的度量。「Transfer Family」的所有 CloudWatch 量度均在中說明使用 Transfer Family 的 CloudWatch 量度。

從範本建立工作流程

您可以部署從範本建立工作流程和伺服器的 AWS CloudFormation 堆疊。此程序包含可用來快速部署工作流程的範例。

若要建立建立 AWS Transfer Family 工作流程和伺服器的 AWS CloudFormation 堆疊

1. 請在以下位置開啟 AWS CloudFormation 主控台。 https://console.aws.amazon.com/cloudformation
2. 將以下代碼保存到文件中。

   YAML

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  SFTPServer:
    Type: 'AWS::Transfer::Server'
    Properties:
      WorkflowDetails:
        OnUpload:
          - ExecutionRole: workflow-execution-role-arn
            WorkflowId: !GetAtt
              - TransferWorkflow
              - WorkflowId
  TransferWorkflow:
    Type: AWS::Transfer::Workflow
    Properties:
      Description: Transfer Family Workflows Blog
      Steps:
        - Type: COPY
          CopyStepDetails:
            Name: copyToUserKey
            DestinationFileLocation:
              S3FileLocation:
                Bucket: archived-records
                Key: ${transfer:UserName}/
            OverwriteExisting: 'TRUE'
        - Type: TAG
          TagStepDetails:
            Name: tagFileForArchive
            Tags:
              - Key: Archive
```

```
                Value: yes
        - Type: CUSTOM
          CustomStepDetails:
            Name: transferExtract
            Target: arn:aws:lambda:region:account-id:function:function-name
            TimeoutSeconds: 60
        - Type: DELETE
          DeleteStepDetails:
            Name: DeleteInputFile
            SourceFileLocation: '${original.file}'
      Tags:
        - Key: Name
          Value: TransferFamilyWorkflows
```

JSON

```
{
    "AWSTemplateFormatVersion": "2010-09-09",
    "Resources": {
        "SFTPServer": {
            "Type": "AWS::Transfer::Server",
            "Properties": {
                "WorkflowDetails": {
                    "OnUpload": [
                        {
                            "ExecutionRole": "workflow-execution-role-arn",
                            "WorkflowId": {
                                "Fn::GetAtt": [
                                    "TransferWorkflow",
                                    "WorkflowId"
                                ]
                            }
                        }
                    ]
                }
            }
        },
        "TransferWorkflow": {
            "Type": "AWS::Transfer::Workflow",
            "Properties": {
                "Description": "Transfer Family Workflows Blog",
                "Steps": [
                    {
```

```
                        "Type": "COPY",
                        "CopyStepDetails": {
                            "Name": "copyToUserKey",
                            "DestinationFileLocation": {
                                "S3FileLocation": {
                                    "Bucket": "archived-records",
                                    "Key": "${transfer:UserName}/"
                                }
                            },
                            "OverwriteExisting": "TRUE"
                        }
                    },
                    {
                        "Type": "TAG",
                        "TagStepDetails": {
                            "Name": "tagFileForArchive",
                            "Tags": [
                                {
                                    "Key": "Archive",
                                    "Value": "yes"
                                }
                            ]
                        }
                    },
                    {
                        "Type": "CUSTOM",
                        "CustomStepDetails": {
                            "Name": "transferExtract",
                            "Target": "arn:aws:lambda:region:account-
id:function:function-name",
                            "TimeoutSeconds": 60
                        }
                    },
                    {
                        "Type": "DELETE",
                        "DeleteStepDetails": {
                            "Name": "DeleteInputFile",
                            "SourceFileLocation": "${original.file}"
                        }
                    }
                ],
                "Tags": [
                    {
                        "Key": "Name",
```

```
                        "Value": "TransferFamilyWorkflows"
                    }
                ]
            }
        }
    }
}
```

3. 以您的實際值取代下列項目。

   - 將 *workflow-execution-role-arn* 取代為具有實際工作流程執行角色的 ARN。例如：`arn:aws:transfer:us-east-2:111122223333:workflow/w-1234567890abcdef0`
   - `arn:aws:lambda:`*region*`:`*account-id*`:function:`*function-name*以您的 Lambda 函數的 ARN 取代。例如 `arn:aws:lambda:us-east-2:123456789012:function:example-lambda-idp`。

4. 請遵循《使用指南》中的「選取 AWS CloudFormation 堆疊範本」中，從現有範本部署堆疊的AWS CloudFormation 指示。

部署堆疊之後，您可以在 CloudFormation 主控台的 [輸出] 索引標籤中檢視堆疊的詳細資料。範本會建立使用服務管理使用者的新 AWS Transfer Family SFTP 伺服器，以及新的工作流程，並將工作流程與新伺服器相關聯。

從轉移系列伺服器移除工作流程

如果您已將工作流程與 Transfer Family 伺服器產生關聯，而您現在想要移除該關聯，則可以使用主控台或以程式設計方式執行此操作。

Console

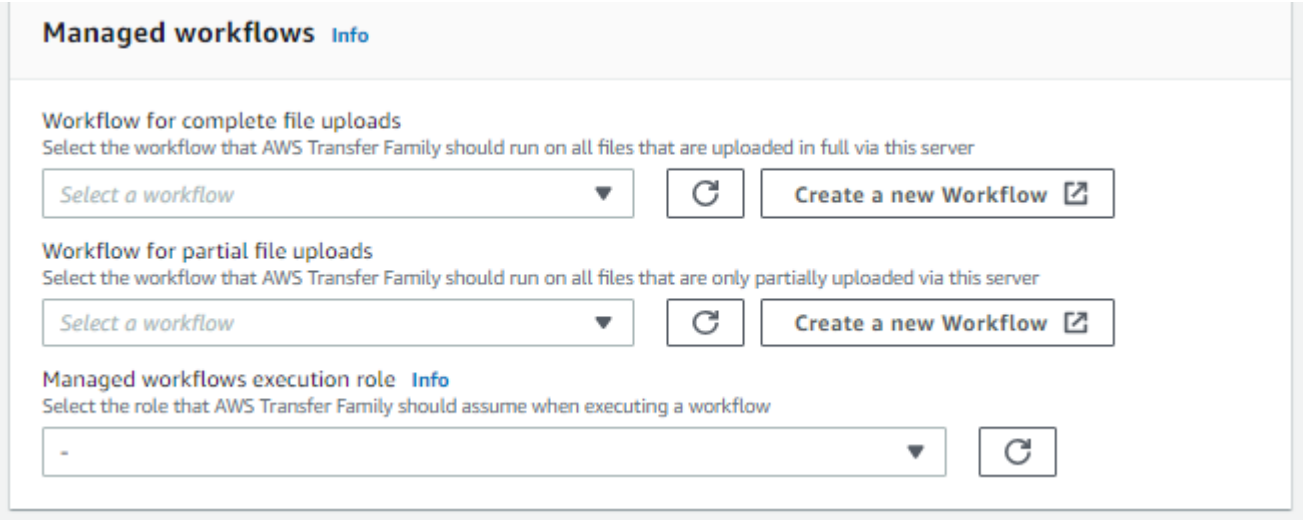
從轉移族群伺服器移除工作流程的步驟

1. 開啟主 AWS Transfer Family 控台，網址為 https://console.aws.amazon.com/transfer/。
2. 在左側導覽窗格中，選擇 [伺服器]。
3. 在「伺服器 ID」欄中選擇伺服器的識別碼。
4. 在伺服器的詳細資訊頁面上，向下捲動至 [其他詳細資料] 區段，然後選擇 [編輯]。
5. 在 [編輯其他詳細資料] 頁面的 [受管理的工作流程] 區段中，清除所有設定的資訊：

- 從工作流程的工作流程清單中選取破折號 (-)，以進行完整的檔案上傳。
- 如果尚未清除，請從用於部分檔案上載的工作流程清單中選取破折號 (-)。
- 從「受管理的工作流程」執行角色的角色清單中選取破折號 (-)。

如果看不到破折號，請向上捲動直到看到它，因為它是每個選單中的第一個值。

螢幕應如下所示。



6. 向下捲動並選擇 [儲存] 以儲存變更。

CLI

您可以使用 `update-server` (或 `UpdateServer` API) 呼叫，並為`OnUpload`和參數提供空白引`OnPartialUpload`數。

從中執 AWS CLI行下列命令：

```
aws transfer update-server --server-id your-server-id --workflow-details
 '{"OnPartialUpload":[],"OnUpload":[]}'
```

*`your-server-id`*以伺服器的 ID 取代。例如，如果您的伺服器 ID 為`s-01234567890abcdef`、，則指令如下：

```
aws transfer update-server --server-id s-01234567890abcdef --workflow-details
 '{"OnPartialUpload":[],"OnUpload":[]}'
```

受管理的工作流程限制和

限制

下列限制目前適用於的上載後處理工作流程 AWS Transfer Family。

- 不支援跨帳戶和跨區域 AWS Lambda 功能。不過，只要您的 AWS Identity and Access Management (IAM) 政策設定正確，您就可以跨帳戶進行複製。
- 對於所有工作流程步驟，工作流程存取的任何 Amazon S3 儲存貯體必須與工作流程本身位於相同的區域。
- 對於解密步驟，解密目的地必須與區域和支援存放區的來源相符 (例如，如果要解密的檔案存放在 Amazon S3 中，則指定的目標也必須位於 Amazon S3 中)。
- 僅支援非同步自訂步驟。
- 自定義步驟超時是近似值。也就是說，超時可能需要比指定的時間稍長。此外，工作流程取決於 Lambda 函數。因此，如果函數在執行期間延遲，則工作流程不會意識到延遲。
- 如果您超過節流限制，「Transfer Family」不會將工作流程作業新增至佇列。
- 不會針對大小為 0 的檔案啟動工作流程。大小大於 0 的檔案會起始關聯的工作流程。

限制

此外，下列功能限制適用於「Transfer Family」的工作流程：

- 每個區域每個帳戶的工作流程數量上限為 10。
- 自訂步驟的逾時時間上限為 30 分鐘。
- 工作流程中的最大步驟數為 8。
- 每個工作流程的標籤數目上限為 50。
- 包含解密步驟的並行執行數目上限為每個工作流程 250 個。
- 每個 Transfer Family 伺服器每個使用者最多可以儲存 3 個 PGP 私密金鑰。
- 解密檔案的大小上限為 10 GB。
- 我們使用突發容量為 100 且補充率為 1 的令牌桶系統來調節新的執行速率。
- 每當您從伺服器中移除工作流程並以新工作流程取代，或更新伺服器組態 (這會影響工作流程的執行角色) 時，您必須等待大約 10 分鐘，才能執行新的工作流程。Transfer Family 伺服器會快取工作流程詳細資料，伺服器需要 10 分鐘才能重新整理其快取。

此外，您必須登出任何作用中的 SFTP 工作階段，然後在 10 分鐘的等待期後重新登入，以查看變更。

管理伺服器

在本節中，您可以找到有關如何檢視伺服器清單、如何檢視伺服器詳細資訊、如何編輯伺服器詳細資訊，以及如何變更已啟用 SFTP 之伺服器之主機金鑰的資訊。

主題

- 檢視伺服器清單
- 刪除伺服器
- 檢視 SFTP、FTP 伺服器和 FTP 伺服器的詳細資訊
- 檢視 AS2 伺服器詳細資訊
- 編輯伺服器詳情
- 管理啟用 SFTP 的伺服器的主機金鑰
- 在主控台中監控使用情況

檢視伺服器清單

在 AWS Transfer Family 主控台上，您可以找到所選 AWS 區域中所有伺服器的清單。

尋找某個 AWS 區域中存在的伺服器清單

- 請在以下位置開啟 AWS Transfer Family 主控台。 https://console.aws.amazon.com/transfer/

  如果您目前的 AWS 區域中有一或多部伺服器，主控台會開啟並顯示您的伺服器清單。如果您沒有看到伺服器清單，請確定您位於正確的地區。您也可以從導覽窗格選擇 Servers (伺服器)。

  如需檢視伺服器詳細資訊的詳細資訊，請參閱檢視 SFTP、FTP 伺服器和 FTP 伺服器的詳細資訊。

刪除伺服器

此程序說明如何使用 AWS Transfer Family 主控台或刪除 Transfer Family 伺服器 AWS CLI。

> **Important**
>
> 在您刪除伺服器之前，會針對每個啟用存取端點的通訊協定向您收費。

> **Warning**
>
> 刪除伺服器會導致其所有使用者遭到刪除。使用伺服器存取的儲存貯體中的資料不會被刪除，而且擁有這些 Amazon S3 儲存貯體權限的使用 AWS 者仍可存取。

Console

使用控制台刪除伺服器

1. 請在以下位置開啟 AWS Transfer Family 主控台。 https://console.aws.amazon.com/transfer/
2. 在左側導覽窗格中，選擇 [伺服器]。
3. 選取要刪除之伺服器的核取方塊。
4. 對於 Actions (動作)，請選擇 Delete (刪除)。
5. 在出現的確認對話方塊中，輸入文字**delete**，然後選擇 [刪除] 以確認您要刪除伺服器。

伺服器會從「伺服器」頁面中刪除，而且不會再向您收取費用。

AWS CLI

使用 CLI 刪除伺服器

1. (選擇性) 執行下列命令，以檢視您要永久刪除之伺服器的詳細資料。

   ```
   aws transfer describe-server --server-id your-server-id
   ```

   此`describe-server`命令返回您的服務器的所有詳細信息。
2. 執行下列命令以刪除伺服器。

   ```
   aws transfer delete-server --server-id your-server-id
   ```

如果成功，該命令將刪除服務器，並且不返回任何信息。

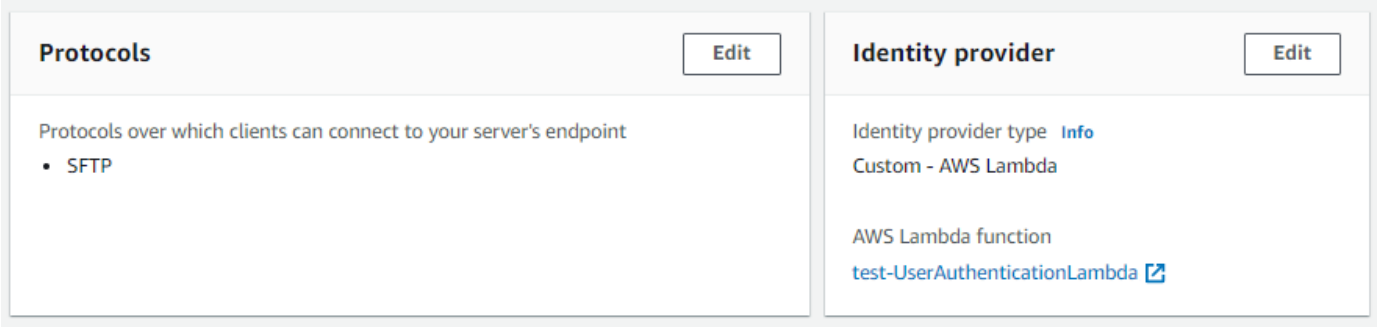
檢視 SFTP、FTP 伺服器和 FTP 伺服器的詳細資訊

您可以找到個別 AWS Transfer Family 伺服器的詳細資料和屬性清單。伺服器內容包括通訊協定、身分識別提供者、狀態、端點類型、自訂主機名稱、端點、使用者、記錄角色、伺服器主機金鑰和標籤。

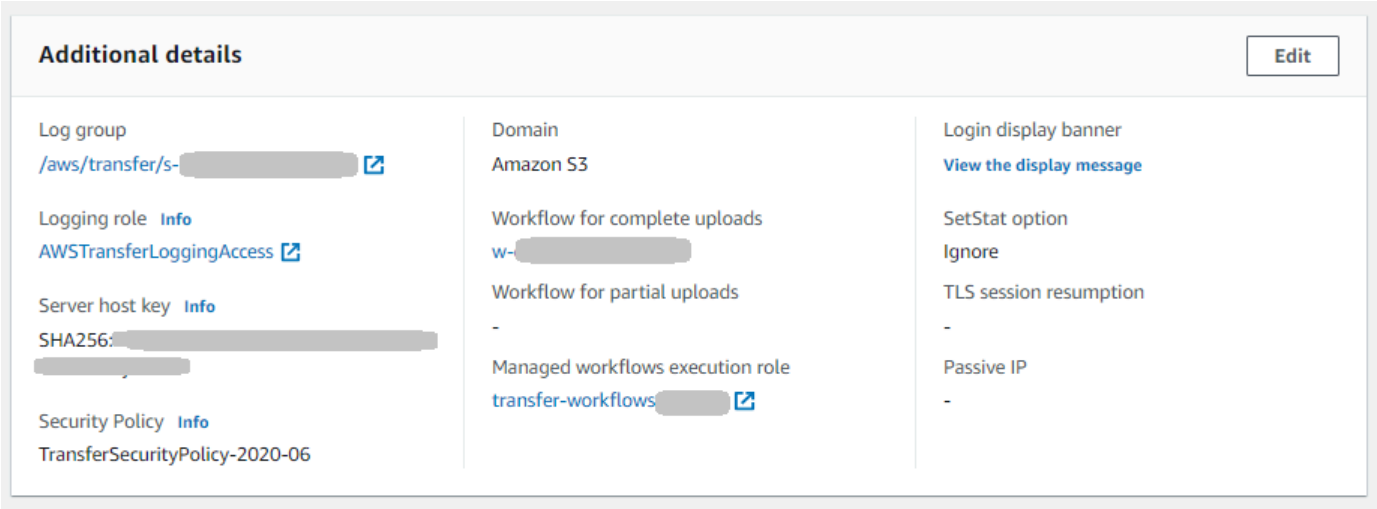
檢視伺服器詳細資訊

1. 請在以下位置開啟 AWS Transfer Family 主控台。 https://console.aws.amazon.com/transfer/
2. 在導覽窗格中，選擇 Servers (伺服器)。
3. 在「伺服器 ID」欄中選擇識別碼，以查看「伺服器詳細資訊」頁面，如下所示。

   您可以選擇編輯，在此頁面上變更伺服器的特性。如需編輯伺服器詳細資訊的詳細資訊，請參閱編輯伺服器詳情。AS2 伺服器的詳細資訊頁面略有不同。如需 AS2 伺服器，請參閱檢視 AS2 伺服器詳細資訊。

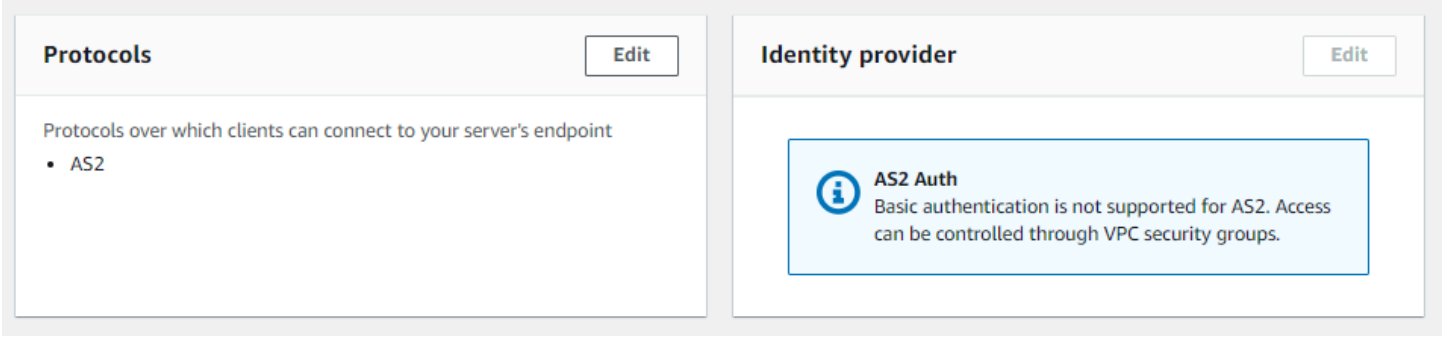


> **Note**
>
> 從 2022 年 9 月起，伺服器主機金鑰描述和匯入日期值是新的。這些值是為了支援多個主機金鑰功能而引入的。此功能需要在引入多個主機金鑰之前移轉使用中的任何單一主機金鑰。
>
> 已移轉伺服器主機金鑰的匯入日期值會設定為伺服器的上次修改日期。也就是說，您所看到的已移轉主機金鑰的日期與伺服器主機金鑰移轉之前，您上次以任何方式修改伺服器的日期相對應。
>
> 唯一移轉的金鑰是您最舊的或唯一的伺服器主機金鑰。任何其他金鑰都有其匯入金鑰的實際日期。此外，移轉的金鑰還有一個描述，可讓您輕鬆將其識別為已移轉。
>
> 遷移發生在 9 月 2 日至 9 月 13 日之間。此範圍內的實際遷移日期取決於伺服器的區域。

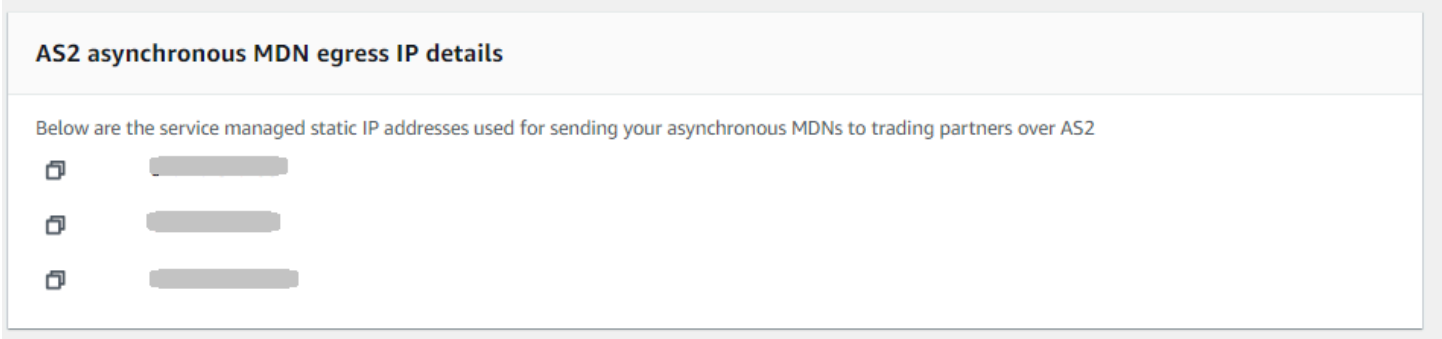


檢視 AS2 伺服器詳細資訊

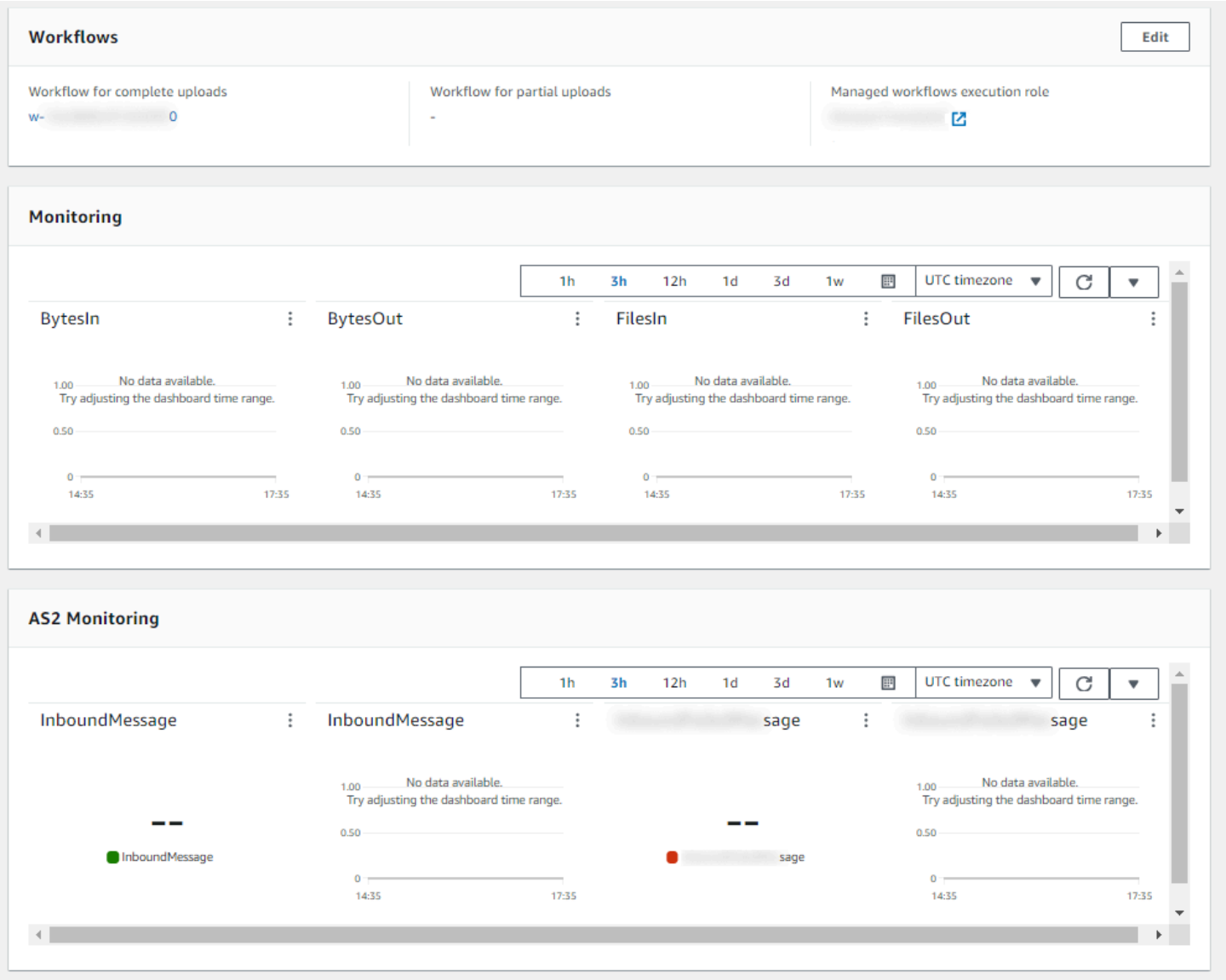
您可以找到個別 AWS Transfer Family 伺服器的詳細資料和屬性清單。伺服器屬性包括通訊協定、狀態等。對於 AS2 伺服器，您也可以檢視 AS2 非同步 MDN 輸出 IP 位址。



每個 AS2 伺服器都會指派三個靜態 IP 位址。使用這些 IP 位址透過 AS2 傳送非同步 MDN 給您的交易夥伴。



AS2 伺服器詳細資料頁面的底部包含任何附加工作流程的詳細資料，以及監視和標記資訊。



編輯伺服器詳情

建立 AWS Transfer Family 伺服器之後，您可以編輯伺服器組態。

主題

- 編輯檔案傳輸通訊協定
- 編輯自訂身分提供者參數
- 編輯伺服器端點
- 編輯您的記錄設定
- 編輯安全性原則

- 變更伺服器的受管理工作流程
- 變更伺服器的顯示橫幅
- 讓伺服器連線或離線

編輯伺服器的組態

1. 請在以下位置開啟 AWS Transfer Family 主控台。 https://console.aws.amazon.com/transfer/
2. 在左側導覽窗格中，選擇 [伺服器]。
3. 在「伺服器 ID」欄中選擇識別碼，以查看「伺服器詳細資訊」頁面，如下所示。

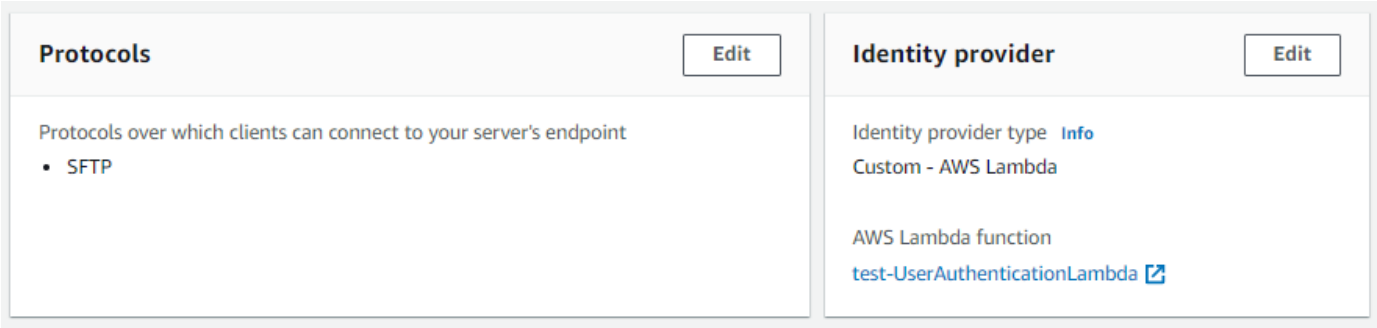
   您可以選擇編輯，在此頁面變更伺服器的特性：

   - 若要變更通訊協定，請參閱編輯檔案傳輸通訊協定。
   - 對於身分識別提供者，請注意，您無法在建立伺服器之後變更伺服器的身分識別提供者類型。若要變更身分提供者，請刪除伺服器然後使用您希望的身分提供者建立新的伺服器。

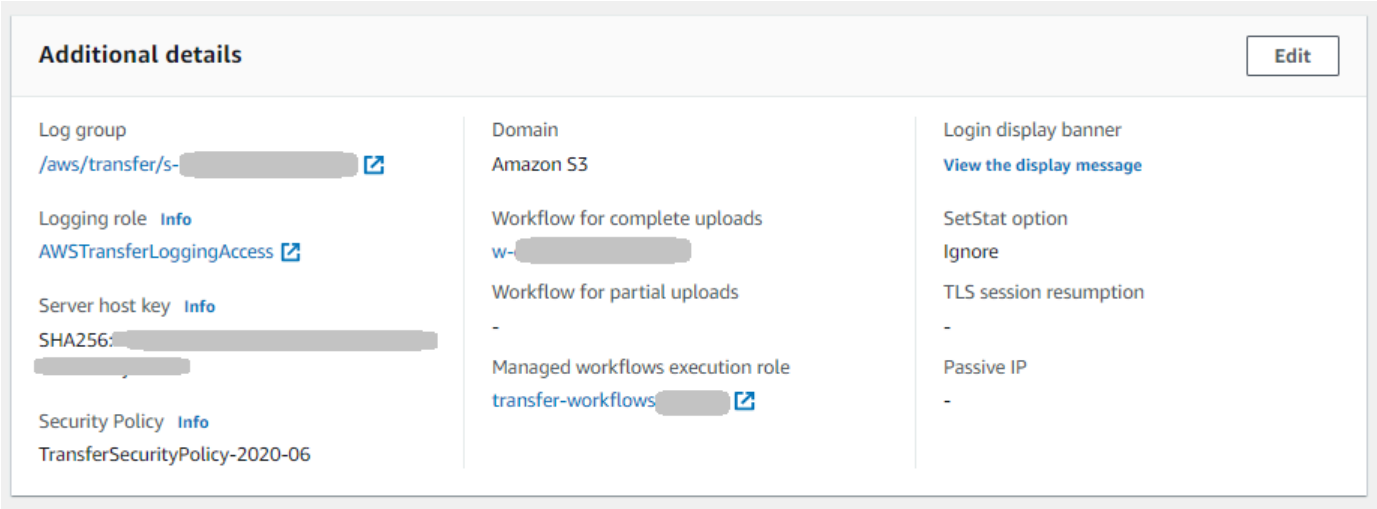
     > **Note**
     >
     > 如果您的伺服器使用自訂身分識別提供者，您可以編輯某些屬性。如需詳細資訊，請參閱 編輯自訂身分提供者參數。

   - 若要變更端點類型或自訂主機名稱，請參閱編輯伺服器端點。
   - 若要新增合約，您必須先將 AS2 作為通訊協定新增至伺服器。如需詳細資訊，請參閱 編輯檔案傳輸通訊協定。
   - 若要管理伺服器的主機金鑰，請參閱管理啟用 SFTP 的伺服器的主機金鑰。
   - 在「其他詳細資訊」下，您可以編輯下列資訊：
     - 若要變更記錄角色，請參閱編輯您的記錄設定。
     - 若要變更安全性原則，請參閱編輯安全性原則。
     - 若要變更伺服器主機金鑰，請參閱管理啟用 SFTP 的伺服器的主機金鑰。
     - 若要變更伺服器的受管理工作流程，請參閱變更伺服器的受管理工作流程。
     - 若要編輯伺服器的顯示橫幅，請參閱變更伺服器的顯示橫幅。
   - 在其他模型組態下，您可以編輯下列資訊：
     - SetStat 選項：啟用此選項可忽略用戶端嘗試在您上傳至 Amazon S3 儲存貯體的檔案SETSTAT上使用時產生的錯誤。如需其他詳細資訊，請參SetStatOption閱ProtocolDetails主題中的文件。

  - TLS 工作階段重新開始：提供一種機制，可在 FTPS 工作階段的控制項和資料連線之間繼續或共用協商的密鑰。如需其他詳細資訊，請參閱`TlsSessionResumptionMode`ProtocolDetails主題中的文件。
  - 被動 IP：表示被動模式，用於 FTP 和 FTPS 協議。輸入單一 IPv4 地址，例如防火牆、路由器或負載平衡器的公有 IP 地址。如需其他詳細資訊，請參閱`PassiveIp`ProtocolDetails主題中的文件。
- 若要啟動或停止伺服器，請參閱讓伺服器連線或離線。
- 若要刪除伺服器，請參閱刪除伺服器。
- 若要編輯使用者的屬性，請參閱管理存取控制。



> **Note**
>
> 從 2022 年 9 月起，伺服器主機金鑰描述和匯入日期值是新的。這些值是為了支援多個主機金鑰功能而引入的。此功能需要在引入多個主機金鑰之前移轉使用中的任何單一主機金鑰。
>
> 已移轉伺服器主機金鑰的匯入日期值會設定為伺服器的上次修改日期。也就是說，您所看到的已移轉主機金鑰的日期與伺服器主機金鑰移轉之前，您上次以任何方式修改伺服器的日期相對應。
>
> 唯一移轉的金鑰是您最舊的或唯一的伺服器主機金鑰。任何其他金鑰都有其匯入金鑰的實際日期。此外，移轉的金鑰還有一個描述，可讓您輕鬆將其識別為已移轉。
>
> 遷移發生在 9 月 2 日至 9 月 13 日之間。此範圍內的實際遷移日期取決於伺服器的區域。



編輯檔案傳輸通訊協定

在 AWS Transfer Family 主控台上，您可以編輯檔案傳輸通訊協定。檔案傳輸通訊協定會將用戶端連線到伺服器的端點。

若要編輯通訊協定

1. 在 [伺服器詳細資料] 頁面上，選擇 [通訊協定] 旁的 [
2. 在 [編輯通訊協定] 頁面上，選取或清除通訊協定核取方塊或核取方塊，以新增或移除下列檔案傳輸通訊協定：

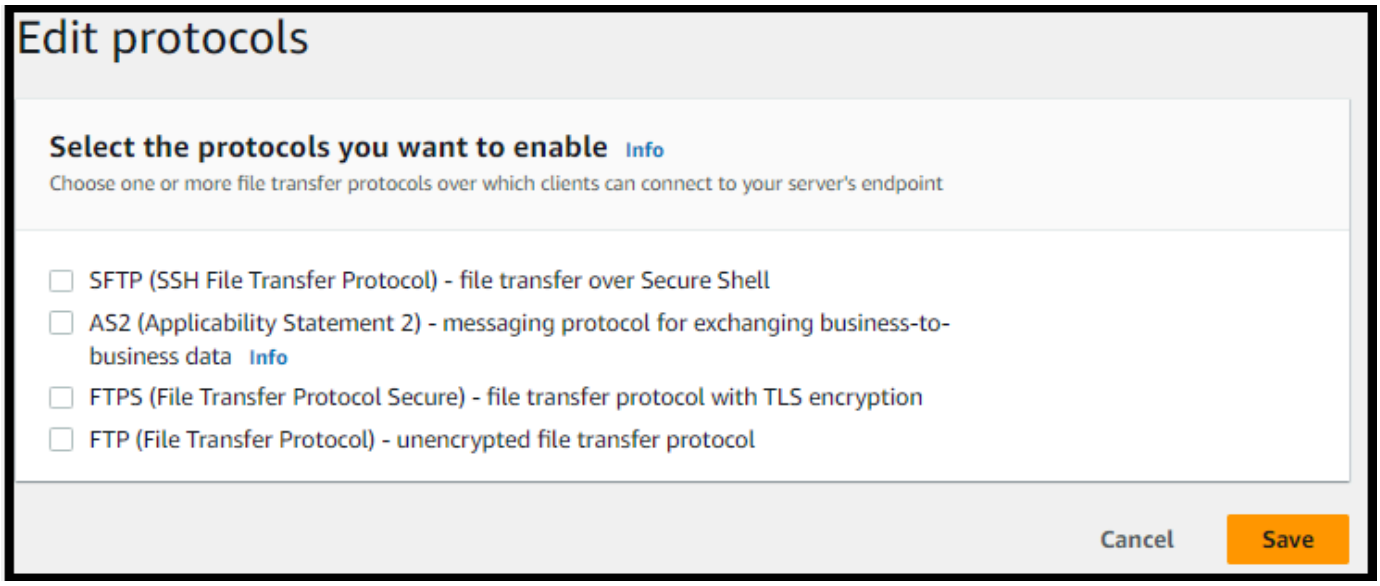
   - 安全殼層 (SSH) 檔案傳輸通訊協定 (SFTP) — 透過 SSH 進行檔案傳輸

     若要取得有關 SFTP 的更多資訊，請參閱建立啟用 SFTP 的伺服器。
   - 文件傳輸協議安全（FTPS）-使用 TLS 加密進行文件傳輸

     若要取得有關 FTP 的更多資訊，請參閱建立啟用 FTP 的伺服器。
   - 檔案傳輸通訊協定 (FTP) — 未加密的檔案傳輸

     如需 FTPS 的詳細資訊，請參閱建立啟用 FTP 的伺服器。

> **Note**
>
> 如果您只為 SFTP 啟用了現有伺服器，並且想要新增 FTPS 和 FTP，則必須確定您擁有與 FTPS 和 FTP 相容的正確身分識別提供者和端點類型設定。



如果您選取 FTPS，則必須選擇儲存在 AWS Certificate Manager (ACM) 中的憑證，當用戶端透過 FTPS 連線到伺服器時，該憑證將用來識別您的伺服器。

若要要求新的公用憑證，請參閱AWS Certificate Manager 使用者指南中的要求公用憑證。

若要將現有憑證匯入 ACM，請參閱《AWS Certificate Manager 使用指南》中的〈將憑證匯入 ACM〉。

若要要求私有憑證以透過私有 IP 位址使用 FTPS，請參閱使用AWS Certificate Manager 者指南中的要求私人憑證。

支援具有下列密碼編譯演算法和金鑰大小的憑證：

- 2048 位元 RSA (RSA_2048)
- 4096 位元 RSA (RSA_4096)
- 橢圓定焦曲線 256 位元 (EC_prime256v1)
- 橢圓定焦曲線 384 位元 (EC_secp384r1)

- 橢圓定焦曲線 521 位元 (EC_secp521r1)

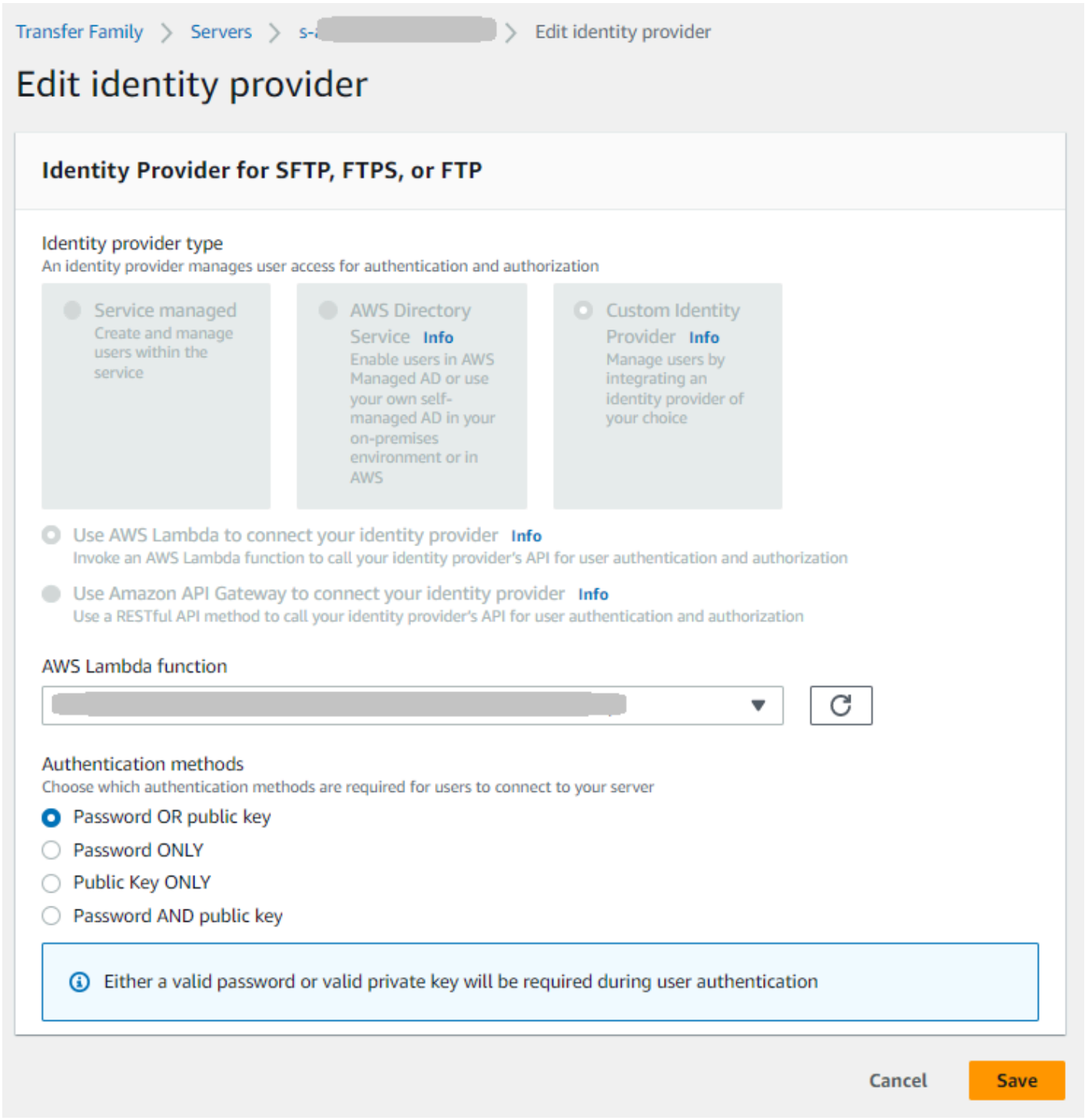
> **Note**
>
> 憑證必須是有效的 SSL/TLS X.509 第 3 版憑證，且其中指定了 FQDN 或 IP 位址，並包含發行者的相關資訊。

3. 選擇儲存。您會返回「伺服器詳細資訊」頁面。

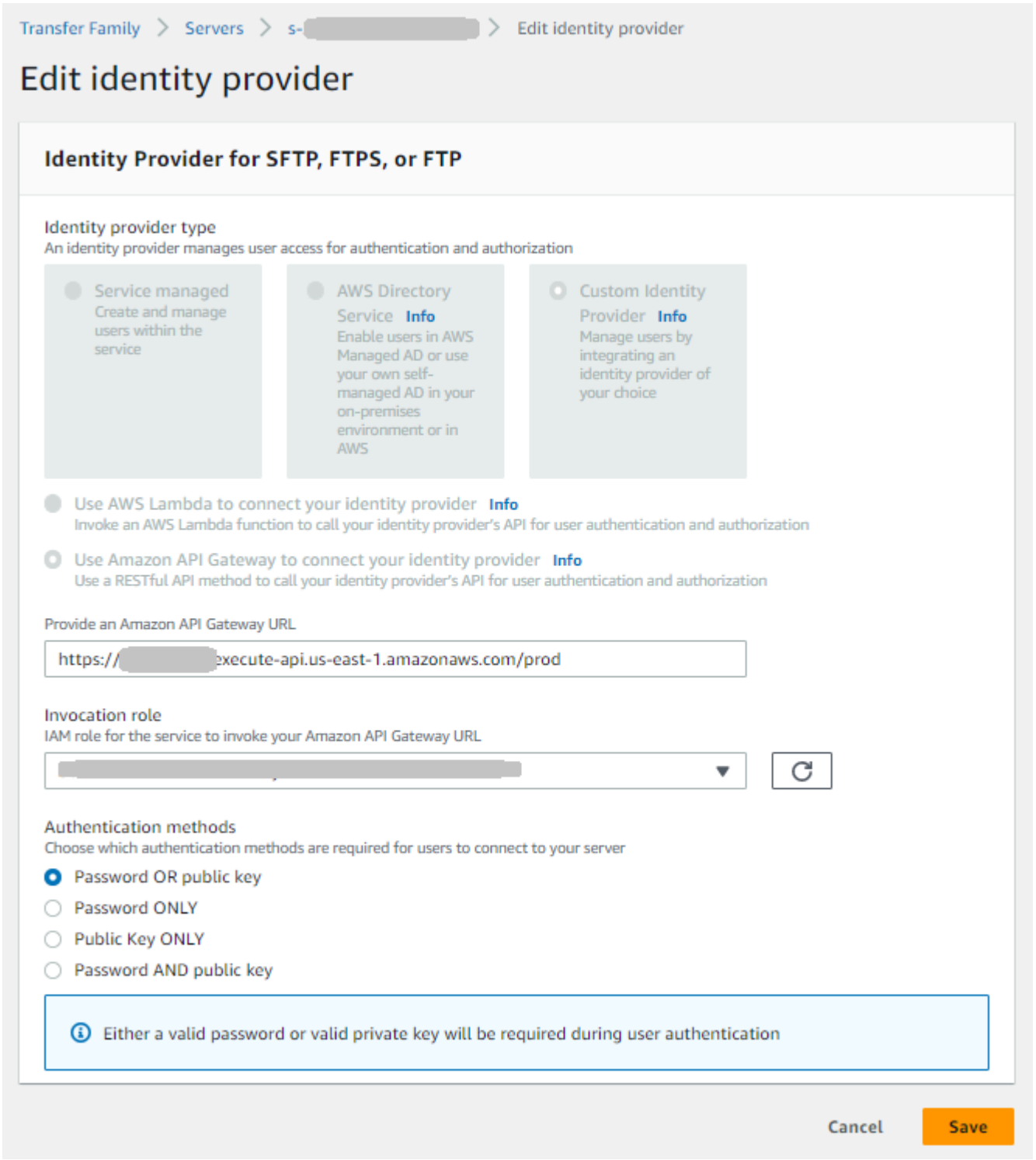
編輯自訂身分提供者參數

在 AWS Transfer Family 主控台上，對於自訂身分識別提供者，您可以根據您使用的是 Lambda 函數還是 API Gateway 來變更某些設定。在任何一種情況下，如果您的伺服器使用 SFTP 通訊協定，您都可以編輯驗證方法。

- 如果您使用 Lambda 做為身分識別提供者，您可以變更基礎 Lambda 函數。



- 如果您使用 API Gateway 做為身分識別提供者，則可以更新閘道 URL 或叫用角色，或兩者都更新。



編輯伺服器端點

在主 AWS Transfer Family 控台上，您可以修改伺服器端點類型和自訂主機名稱。此外，對於 VPC 端點，您可以編輯可用區域資訊。

編輯伺服器端點詳細資訊

1. 在伺服器詳細資料頁面上，選擇端點詳細資料旁邊的編輯。
2. 您必須先停止伺服器，才能編輯端點類型。然後，在 [編輯端點組態] 頁面上，對於 [端點類型]，您可以選擇下列其中一個值：

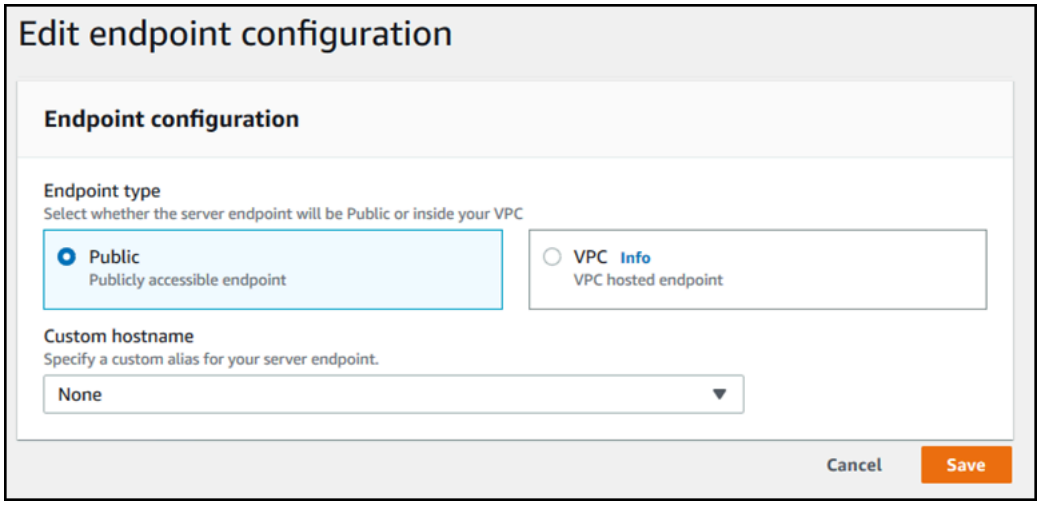
   - 公開 — 此選項可讓您的伺服器透過網際網路存取。
   - VPC — 此選項使您的服務器可以在虛擬私有雲（VPC）中訪問。如需 VPC 的詳細資訊，請參閱在虛擬私有雲中建立伺服器。
3. 在「自訂主機名稱」中，選擇下列其中一項：

   - 無 — 如果您不想使用自訂網域，請選擇 [無]。

     您會取得由提供的伺服器主機名稱 AWS Transfer Family。伺服器主機名稱的格式為 *serverId*.server.transfer.*regionId*.amazonaws.com。
   - Amazon 路線 53 DNS 別名 — 若要使用在路由 53 中為您自動建立的 DNS 別名，請選擇此選項。
   - 其他 DNS — 若要使用您已在外部 DNS 服務中擁有的主機名稱，請選擇 [其他 DNS]。

   選擇 Amazon Route 53 DNS 別名或其他 DNS 會指定要與伺服器端點建立關聯的名稱解析方法。

   例如，您的自訂網域可能是 sftp.inbox.example.com。自訂主機名稱會使用您提供且 DNS 服務可解析的 DNS 名稱。您可以使用 Route 53 作為 DNS 解析程式，或使用您自己的 DNS 服務供應商。若要瞭解如何 AWS Transfer Family 使用 Route 53 將流量從您的自訂網域路由到伺服器端點，請參閱使用自訂主機名稱。



4. 對於 VPC 端點，您可以變更 [可用區域] 窗格中的資訊。

5. 選擇儲存。您會返回「伺服器詳細資訊」頁面。

編輯您的記錄設定

在主 AWS Transfer Family 控台上，您可以變更記錄設定。

> **Note**
>
> 如果 Transfer Family 在您建立伺服器時為您建立 CloudWatch 記錄 IAM 角色，則會呼叫 IAM 角色`AWSTransferLoggingAccess`。您可以將其用於所有轉移系列服務器。

若要編輯您的記錄設定

1. 在 [伺服器詳細資料] 頁面上，選擇 [其他詳細資料] 旁邊的
2. 根據您的組態，在記錄角色、結構化 JSON 記錄或兩者之間進行選擇。如需詳細資訊，請參閱 更新伺服器的記錄。

編輯安全性原則

此程序說明如何使用 AWS Transfer Family 主控台或變更 Transfer Family 伺服器的安全性原則 AWS CLI。

> **Note**
>
> 如果您的端點已啟用 FIPS，則無法將 FIPS 安全性原則變更為非 FIPS 安全性原則。

Console

使用主控台編輯安全性原則

1. 在 [伺服器詳細資料] 頁面上，選擇 [其他詳細資料] 旁邊的
2. 在 [密碼編譯演算法選項] 區段中，選擇包含伺服器啟用的加密演算法的安全性原則。

   如需關於安全政策的詳細資訊，請參閱AWS Transfer Family 伺服器的安全性原則。
3. 選擇儲存。

您會返回 [伺服器詳細資料] 頁面，您可以在其中查看更新的安全性原則。

AWS CLI

使用 CLI 編輯安全性原則

1. 執行下列命令以檢視附加至伺服器的目前安全性原則。

```
aws transfer describe-server --server-id your-server-id
```

此describe-server命令會傳回伺服器的所有詳細資訊，包括下列行：

```
"SecurityPolicyName": "TransferSecurityPolicy-2018-11"
```

在此情況下，伺服器的安全性原則為TransferSecurityPolicy-2018-11。

2. 請務必將安全性原則的確切名稱提供給命令。例如，執行下列命令將伺服器更新為TransferSecurityPolicy-2023-05。

```
aws transfer update-server --server-id your-server-id --security-policy-name
 "TransferSecurityPolicy-2023-05"
```

> **Note**
>
> 中列出了可用安全策略的名稱AWS Transfer Family 伺服器的安全性原則。

如果成功，命令會傳回下列程式碼，並更新伺服器的安全性原則。

```
{
    "ServerId": "your-server-id"
}
```

變更伺服器的受管理工作流程

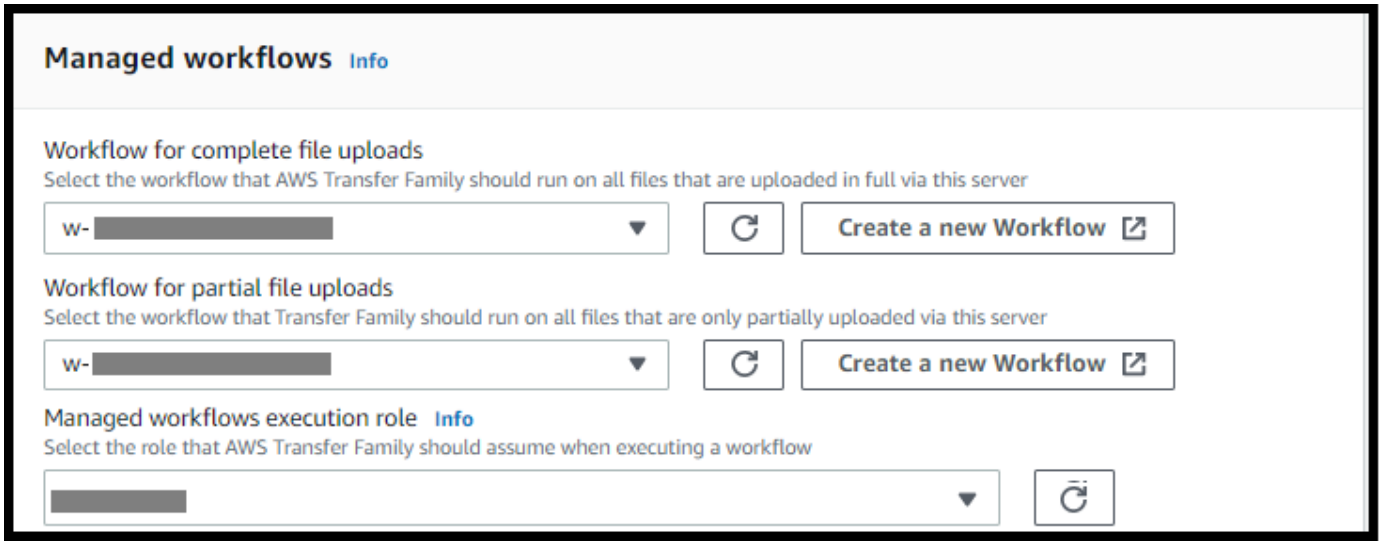
在 AWS Transfer Family 主控台上，您可以變更與伺服器相關聯的受管理工作流程。

變更受管理的工作流程

1. 在 [伺服器詳細資料] 頁面上，選擇 [其他詳細資料] 旁邊的
2. 在 [編輯其他詳細資料] 頁面的 [受管理的工作流程] 區段中，選取要在所有上傳上執行的工作流程。

> **Note**
>
> 如果您還沒有工作流程，請選擇「創建一個新的工作流程」以創建一個工作流程。

   a. 選取要使用的工作流程 ID。
   b. 選擇執行角色。這是「Transfer Family」在執行工作流程步驟時所承擔的角色。如需詳細資訊，請參閱 工作流程的 IAM 政策。選擇 Save (儲存)。



3. 選擇儲存。您會返回「伺服器詳細資訊」頁面。

變更伺服器的顯示橫幅

在 AWS Transfer Family 主控台上，您可以變更與伺服器相關聯的顯示橫幅。

變更顯示橫幅

1. 在 [伺服器詳細資料] 頁面上，選擇 [其他詳細資料] 旁邊的
2. 在 [編輯其他詳細資料] 頁面的 [顯示橫幅] 區段中，輸入可用顯示橫幅的文字。

3. 選擇儲存。您會返回「伺服器詳細資訊」頁面。

讓伺服器連線或離線

在 AWS Transfer Family 主機上，您可以讓伺服器上線或離線。

使您的伺服器上線

1. 請在以下位置開啟 AWS Transfer Family 主控台。 https://console.aws.amazon.com/transfer/
2. 在導覽窗格中，選擇 Servers (伺服器)。
3. 選取離線伺服器的核取方塊。
4. 針對 Actions (動作)，選擇 Start (啟動)。

伺服器可能需要幾分鐘的時間才能從離線切換到線上。

> **Note**
>
> 當您停止伺服器使其離線時，您目前仍在累積該伺服器的服務費用。若要免除額外的伺服器費用，請刪除該伺服器。

使伺服器離線

1. 請在以下位置開啟 AWS Transfer Family 主控台。 https://console.aws.amazon.com/transfer/
2. 在導覽窗格中，選擇 Servers (伺服器)。
3. 選取連線伺服器的核取方塊。
4. 針對 Actions (動作)，選擇 Stop (停止)。

伺服器啟動或關閉時，伺服器無法用於檔案作業。主控台不會顯示啟動中和停止中狀態。

如果您發現錯誤狀況`STOP_FAILED`，`START_FAILED`或聯絡 AWS Support 以協助解決您的問題。

管理啟用 SFTP 的伺服器的主機金鑰

> **Important**
>
> 如果您不打算將現有使用者從現有啟用 SFTP 的伺服器遷移到新啟用 SFTP 的伺服器，請忽略本節。
>
> 意外變更伺服器的主機金鑰可能造成破壞。視 SFTP 用戶端的設定方式而定，它可能會立即失敗，並顯示信任主機金鑰不存在或出現威脅性提示的訊息。如果有用於自動連接的腳本，它們很可能也會失敗。

依預設，會為已啟用 SFTP 的伺服器 AWS Transfer Family 提供主機金鑰。您可以將預設的主機金鑰以來自其他伺服器的主機金鑰取代。只有當您計劃將現有使用者從現有啟用 SFTP 的伺服器移至新啟用 SFTP 的伺服器時，才這樣做。

若要避免提示使用者再次驗證已啟用 SFTP 的伺服器的真實性，請將內部部署伺服器的主機金鑰匯入啟用 SFTP 的伺服器。這樣做也可以防止您的使用者收到有關潛在 man-in-the-middle 攻擊的警告。

您也可以定期輪換主機金鑰，作為額外的安全措施。

> **Note**
>
> 雖然 Transfer Family 主控台可讓您為所有伺服器指定和新增伺服器主機金鑰，但這些金鑰僅適用於使用 SFTP 通訊協定的伺服器。

主題

- 新增其他伺服器主機金鑰
- 刪除伺服器主機金鑰
- 旋轉伺服器主機金鑰
- 其他伺服器主機金鑰資訊

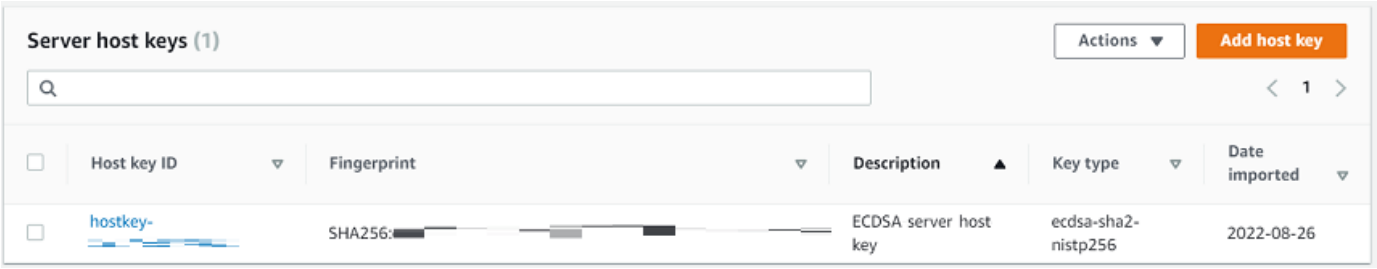
新增其他伺服器主機金鑰

在主 AWS Transfer Family 控台上，您可以新增其他伺服器主機金鑰。新增不同格式的其他主機金鑰對於在用戶端連線到伺服器時識別伺服器，以及改善您的安全性設定檔非常有用。例如，如果您的原始金鑰是 RSA 金鑰，您可以新增額外的 ECDSA 金鑰。

> **Note**
>
> SFTP 用戶端會使用可與其中一個使用中伺服器金鑰相符的第一個公開金鑰進行連線。

新增其他伺服器主機金鑰

1. 開啟主 AWS Transfer Family 控台，網址為 https://console.aws.amazon.com/transfer/。
2. 在左側導覽窗格中，選擇 [伺服器]，然後選擇使用 SFTP 通訊協定的伺服器。
3. 在伺服器詳細資料頁面上，向下捲動至 [伺服器主機金鑰] 區段。



4. 選擇新增主機金鑰。

   新增伺服器主機金鑰頁面隨即顯示。

5. 在「伺服器主機金鑰」區段中，輸入 RSA、ECDSA 或 ED25519 私密金鑰，當用戶端透過啟用了 SFTP 的伺服器連線至伺服器時，用來識別伺服器。

   > **Note**
   >
   > 當您建立伺服器主機金鑰時，請務必指定 `-N ""` (無複雜密碼)。如需如何產生金鑰配對在 macOS、Linux 或 Unix 上建立安全殼層金鑰的詳細資訊，請參閱。

6. (選擇性) 新增說明以區分多個伺服器主機金鑰。您也可以為金鑰新增標籤。
7. 選擇 Add key (新增金鑰)。您將返回伺服器詳細資訊頁面。

若要使用 AWS Command Line Interface (AWS CLI) 新增主機金鑰，請使用 the section called "ImportHostKey" API 作業並提供新的主機金鑰。如果您建立新的啟用了 SFTP 的伺服器，請在 API 作業中提供主機金鑰做為參數。the section called "CreateServer"您也可以使用 AWS CLI 來更新現有主機金鑰的描述。

下列範例`import-host-key` AWS CLI 命令會匯入指定啟用 SFTP 之伺服器的主機金鑰。

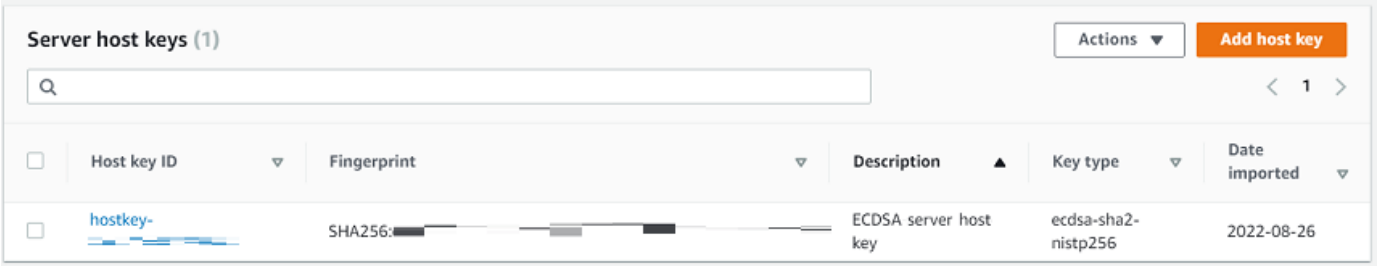
```
aws transfer import-host-key --description key-description --server-id your-server-id
 --host-key-body file://my-host-key
```

刪除伺服器主機金鑰

在主 AWS Transfer Family 控台上，您可以刪除伺服器主機金鑰。

刪除伺服器主機金鑰

1. 開啟主 AWS Transfer Family 控台，網址為 https://console.aws.amazon.com/transfer/。
2. 在左側導覽窗格中，選擇 [伺服器]，然後選擇使用 SFTP 通訊協定的伺服器。
3. 在伺服器詳細資料頁面上，向下捲動至 [伺服器主機金鑰] 區段。



4. 在 [伺服器主機金鑰] 區段中，選取金鑰，然後在 [動作] 下選擇 [刪除]。
5. 在出現的確認對話方塊中，輸入文字**delete**，然後選擇 [刪除] 以確認您要刪除主機金鑰。

主機金鑰會從 [伺服器] 頁面刪除。

若要使用刪除主機金鑰 AWS CLI，請使用 the section called “DeleteHostKey” API 作業並提供伺服器 ID 和主機金鑰識別碼。

下列範例`delete-host-key` AWS CLI 命令會刪除指定啟用 SFTP 之伺服器的主機金鑰。

```
aws transfer delete-host-key --server-id your-server-id --host-key-id your-host-key-id
```

旋轉伺服器主機金鑰

您可以定期輪換伺服器主機金鑰。

用戶端如何選擇伺服器主機金鑰

Transfer Family 選擇要套用哪個伺服器金鑰的方式取決於 SFTP 用戶端的條件，如此處所述。假設有一個較舊的金鑰和一個較新的金鑰。

- SFTP 用戶端沒有伺服器的先前公開主機金鑰。用戶端第一次連線到伺服器時，會發生下列其中一種情況：
  - 如果用戶端設定為連線失敗。
  - 或者，用戶端會選擇符合可用演算法的第一個金鑰，並詢問使用者是否可以信任該金鑰。如果是這樣，用戶端會自動更新known_hosts檔案 (或用戶端用來記錄信任決策的任何本機設定檔或資源) 並輸入該金鑰。
- SFTP 用戶端的known_hosts檔案中有較舊的金鑰。用戶端偏好使用此金鑰，即使存在較新的金鑰，無論是針對此金鑰的演算法或其他演算法。這是因為客戶端對其known_hosts文件中的密鑰具有更高的信任級別。
- SFTP 客戶端在其密鑰文件中具有新密known_hosts鑰（在任何可用算法中）。用戶端會忽略較舊的金鑰，因為它們不受信任且使用新金鑰。
- SFTP 用戶端的known_hosts檔案中有兩個金鑰。客戶端通過與服務器提供的可用密鑰列表匹配的索引選擇第一個密鑰。

Transfer Family 更喜歡 SFTP 客戶端在其known_hosts文件中具有所有密鑰，因為這樣可以在連接到 Transfer Family 服務器時具有最大的靈活性。金鑰輪換是以同一個 Transfer Family 伺服器的known_hosts檔案中可能存在多個項目為基礎。

輪替伺服器主機金鑰程序

舉例來說，假設您已將下列伺服器主機金鑰集新增至 Transfer Family 伺服器。

伺服器主機金鑰

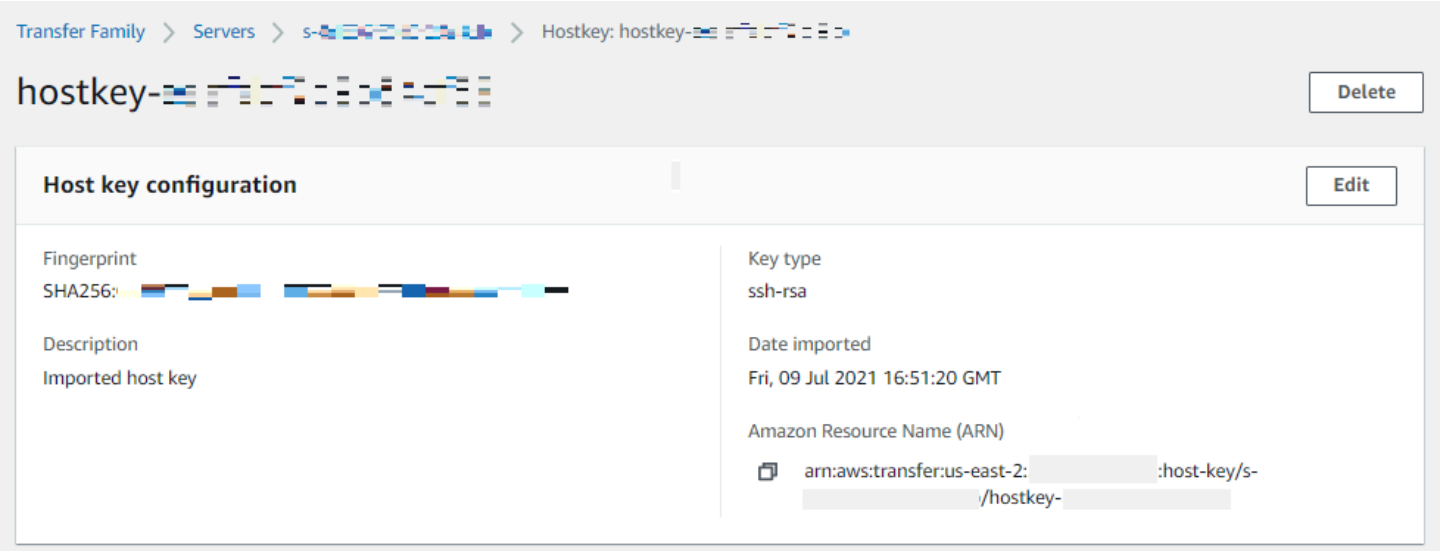
主機金鑰類型	添加到服務器的日期
RSA	2020 年 4 月 1 日
ECDSA	二零二零年二月一日
ED25519	2019 年 12 月 1 日
RSA	2019 年 10 月 1 日
ECDSA	二 ○ 一九年六月一日
ED25519	2019 年 3 月 1 日

旋轉伺服器主機金鑰

1. 新增伺服器主機金鑰。有關此程序的說明，請參閱新增其他伺服器主機金鑰。
2. 刪除之前新增的相同類型的一或多個主機金鑰。有關此程序的說明，請參閱刪除伺服器主機金鑰。
3. 所有按鍵都是可見的，並且可以處於作用中狀態，視先前所述的行為而定用戶端如何選擇伺服器主機金鑰。

其他伺服器主機金鑰資訊

您可以選取主機金鑰來顯示該金鑰的詳細資訊。



您可以刪除主機金鑰，或從「伺服器詳細資訊」畫面上的「動作」功能表編輯其說明。選取主機金鑰，然後從功能表中選擇適當的動作。

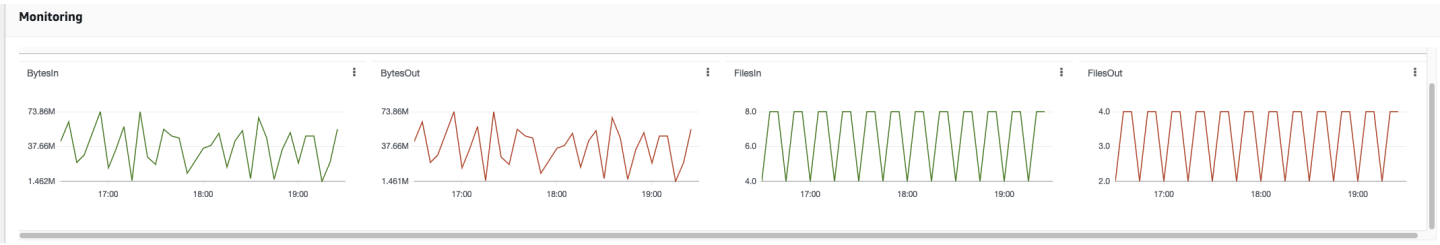
在主控台中監控使用情況

您可以在伺服器詳細資訊頁面上取得伺服器指標的相關資訊。這可讓您在單一位置監控檔案傳輸工作負載。您可以追蹤已與合作夥伴交換的檔案數量，並使用集中式儀表板密切追蹤其使用情況。如需詳細資訊，請參閱 檢視 SFTP、FTP 伺服器和 FTP 伺服器的詳細資訊。下表說明「Transfer Family」可用的測量結果。

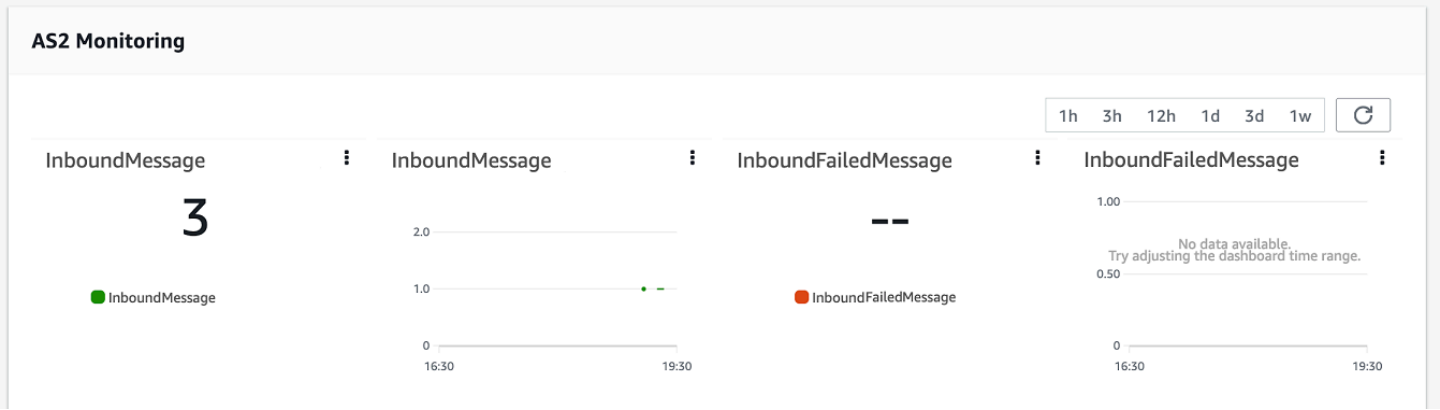
命名空間	指標	描述
AWS/Transfer	BytesIn	傳輸到伺服器的位元組總數。 單位：計數 期間：5 分鐘
	BytesOut	從伺服器傳出的位元組總數。 單位：計數 期間：5 分鐘
	FilesIn	傳輸到伺服器的檔案總數。 對於使用 AS2 通訊協定的伺服器，此測量結果代表接收的訊息數目。 單位：計數 期間：5 分鐘
	FilesOut	從伺服器傳出的檔案總數。 單位：計數 期間：5 分鐘
	InboundMessage	成功從交易夥伴收到的 AS2 訊息總數。 單位：計數 期間：5 分鐘

命名空間	指標	描述
	InboundFailedMessage	從交易夥伴收到未成功的 AS2 訊息總數。也就是說，交易夥伴發送了一條消息，但 Transfer Family 服務器無法成功處理它。 單位：計數 期間：5 分鐘
	OnUploadExecutionsStarted	在伺服器上啟動的工作流程執行總數。 單位：計數 時間：1 分鐘
	OnUploadExecutionsSuccess	伺服器上成功的工作流程執行總數。 單位：計數 時間：1 分鐘
	OnUploadExecutionsFailed	伺服器上失敗的工作流程執行總數。 單位：計數 時間：1 分鐘

「監控」區段包含四個個別的圖表。這些圖表顯示位元組、位元組輸出、檔案輸入和檔案輸出。



對於已啟用 AS2 通訊協定的伺服器，[監視] 資訊下方會有 [AS2 監視] 區段。本節包含輸入訊息數目 (成功與失敗) 的詳細資訊。



若要在自己的視窗中開啟所選圖形，請選擇展開圖示
(⛶)。
您也可以按一下圖表的垂直省略符號圖示
(⋮)，
開啟包含下列項目的下拉式功能表：

- 放大 — 在所選圖形自己的視窗中開啟所選圖形。
- 重新整理 — 使用最新資料重新載入圖形。
- 在指標中檢視 — 在 Amazon 中開啟對應的指標詳細資訊 CloudWatch。
- 檢視防護記錄 — 在中開啟對應的防護記錄群組 CloudWatch。

管理存取控制

您可以使用 AWS Identity and Access Management (IAM) 政策來控制使用者對 AWS Transfer Family 資源的存取。IAM 政策是一種語句，通常是 JSON 格式，允許特定級別的資源訪問權限。您可以使用 IAM 政策來定義要允許使用者執行而不執行的檔案操作。您也可以使用 IAM 政策來定義要讓使用者存取的 Amazon S3 儲存貯體或儲存貯體。若要為使用者指定這些政策，您可以為其建立 IAM 角色，AWS Transfer Family 該角色具有 IAM 政策和信任關聯性。

每個使用者都會獲指派一個 IAM 角色。 AWS Transfer Family 使用的 IAM 角色類型稱為服務角色。當使用者登入您的伺服器時， AWS Transfer Family 會假設對應至該使用者的 IAM 角色。若要了解如何建立可讓使用者存取 Amazon S3 儲存貯體的 IAM 角色，請參閱 IAM 使用者指南中的建立角色以委派許可給 AWS 服務。

您可以使用 IAM 政策中的特定許可，授予 Amazon S3 物件的唯寫存取權。如需詳細資訊，請參閱 授予僅寫入和列出檔案的能力。

AWS 儲存區部落格包含一篇文章，詳細說明如何設定最低權限存取權限。如需詳細資訊，請參閱在AWS Transfer Family 工作流程中實作最低權限存取。

> **Note**
>
> 如果您的 Amazon S3 儲存貯體使用 AWS Key Management Service (AWS KMS) 加密，則必須在政策中指定其他許可。如需詳細資訊，請參閱 Amazon S3 中的資料加密。此外，您可以在 IAM 使用者指南中查看有關工作階段政策的詳細資訊。

主題

- 允許讀取和寫入訪問 Amazon S3 存儲桶
- 為 Amazon S3 儲存貯體建立工作階段政策
- 防止使用者mkdir在 S3 儲存貯體中執行

允許讀取和寫入訪問 Amazon S3 存儲桶

本節說明如何建立 IAM 政策，以允許對特定 Amazon S3 儲存貯體進行讀取和寫入存取。將具有此 IAM 政策的 IAM 角色指派給您的使用者，可讓該使用者讀取/寫入指定 Amazon S3 儲存貯體的存取權。

下列政策提供對 Amazon S3 儲存貯體的程式設計讀取、寫入和標記存取。只有在您需要啟用「跨帳戶存取」時，才需要GetObjectACL和對帳PutObjectACL單。也就是說，您的 Transfer Family 服務器需要訪問不同帳戶中的存儲桶。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid":"ReadWriteS3",
      "Action": [
            "s3:ListBucket"
                ],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::DOC-EXAMPLE-BUCKET"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
      ],
      "Resource": ["arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"]
    }
  ]
}
```

ListBucket 動作需要對儲存貯體本身的許可。PUT、GET 和 DELETE 動作需要物件許可。因為這些是不同的資源，所以使用不同的 Amazon 資源名稱 (ARN) 來指定它們。

若要進一步限制使用者只能存取指定 Amazon S3 儲存貯體的home前置詞，請參閱為 Amazon S3 儲存貯體建立工作階段政策。

為 Amazon S3 儲存貯體建立工作階段政策

工作階段政策是一種 AWS Identity and Access Management (IAM) 政策，可將使用者限制在 Amazon S3 儲存貯體的某些部分。它會透過即時評估存取來執行此作業。

> **Note**
>
> 工作階段政策僅適用於 Amazon S3。對於 Amazon EFS，您可以使用 POSIX 檔案許可來限制存取。

當您需要授予一組使用者對 Amazon S3 儲存貯體特定部分的相同存取權時，可以使用工作階段政策。例如，使用者群組可能只需要存取 home 目錄。該使用者群組共用相同的 IAM 角色。

> **Note**
>
> 工作階段原則的最大長度為 2048 個字元。如需詳細資訊，請參閱 API 參考資料中CreateUser動作的原則要求參數。

若要建立工作階段政策，請在 IAM 政策中使用下列政策變數：

- `${transfer:HomeBucket}`
- `${transfer:HomeDirectory}`
- `${transfer:HomeFolder}`
- `${transfer:UserName}`

> **Important**
>
> 您無法在受管策略中使用上述變數。您也不能在 IAM 角色定義中將它們用作政策變數。您可以在 IAM 政策中建立這些變數，並在設定使用者時直接提供這些變數。此外，您無法在此工作階段原則中使用`${aws:Username}`變數。此變數參照 IAM 使用者名稱，而不是所需的使用者名稱 AWS Transfer Family。

下面的代碼顯示了一個示例會話策略。

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Sid": "AllowListingOfUserFolder",
          "Action": [
              "s3:ListBucket"
          ],
          "Effect": "Allow",
          "Resource": [
              "arn:aws:s3:::${transfer:HomeBucket}"
          ],
          "Condition": {
              "StringLike": {
                  "s3:prefix": [
                      "${transfer:HomeFolder}/*",
                      "${transfer:HomeFolder}"
                  ]
              }
          }
      },
      {
          "Sid": "HomeDirObjectAccess",
          "Effect": "Allow",
          "Action": [
              "s3:PutObject",
              "s3:GetObject",
              "s3:DeleteObjectVersion",
              "s3:DeleteObject",
              "s3:GetObjectVersion",
              "s3:GetObjectACL",
              "s3:PutObjectACL"
          ],
          "Resource": "arn:aws:s3:::${transfer:HomeDirectory}/*"
       }
  ]
}
```

> **Note**
>
> 上述原則範例假設使用者的主目錄設定為包含尾隨斜線，表示該目錄為目錄。另一方面，如果您在沒有尾部斜杠的HomeDirectory情況下設置了用戶，那麼您應該將其作為策略的一部分包括在內。

在上一個範例原則中，請注意transfer:HomeFoldertransfer:HomeBucket、和transfer:HomeDirectory原則參數的使用。這些參數是針對HomeDirectory為使用者設定的設定，如HomeDirectory和中所述實作您的 API Gateway 方法。這些參數具有下列定義：

- transfer:HomeBucket參數會取代為的第一個元件HomeDirectory。
- transfer:HomeFolder參數會被參數的剩餘部分取HomeDirectory代。
- 該transfer:HomeDirectory參數已移除前導正斜線 (/)，以便在Resource陳述式中用作 S3 Amazon 資源名稱 (ARN) 的一部分。

> **Note**
>
> 如果您使用的是邏輯目錄 (也就是使用者homeDirectoryType是)，則不支援LOGICAL這些原則參數 (HomeBucketHomeDirectory、和HomeFolder)。

例如，假設為「Transfer Family」使用者設定的HomeDirectory參數為/home/bob/amazon/stuff/。

- transfer:HomeBucket設定為/home。
- transfer:HomeFolder設定為/bob/amazon/stuff/。
- transfer:HomeDirectory變成home/bob/amazon/stuff/。

第一個"Sid"允許用戶列出從開始的所有目錄/home/bob/amazon/stuff/。

第二個"Sid"限制了用戶put和get訪問相同的路徑，/home/bob/amazon/stuff/.

有了先前的策略後，當使用者登入時，他們只能存取其主目錄中的物件。在連線時， AWS Transfer Family 會以適當的使用者值取代這些變數。這樣做可讓將相同政策文件套用到多名使用者的過程變得更為容易。這種方法可減少 IAM 角色和政策管理的開銷，以管理使用者對 Amazon S3 儲存貯體的存取權。

您也可以使用工作階段原則，根據您的業務需求自訂每個使用者的存取權限。如需詳細資訊，請參閱《IAM 使用者指南》 AssumeRoleWithWebIdentity中的「 AssumeRoleWithSAML」和「的許可」。AssumeRole

> **Note**
>
> AWS Transfer Family 儲存政策 JSON，而不是政策的 Amazon 資源名稱 (ARN)。因此，當您在 IAM 主控台中變更政策時，您需要返回 AWS Transfer Family 主控台，並使用最新的政策內容更新使用者。您可以在 [使用者設定] 區段的 [原則資訊] 索引標籤上更新使用者。
> 如果您使用的是 AWS CLI，您可以使用下列命令來更新原則。
>
> ```
> aws transfer update-user --server-id server --user-name user --policy \
>    "$(aws iam get-policy-version --policy-arn policy --version-id version --
> output json)"
> ```

防止使用者mkdir在 S3 儲存貯體中執行

您可以限制使用者在 Amazon S3 儲存貯體中建立目錄的能力。若要這麼做，您可以建立允許s3:PutObject動作的 IAM 政策，但在金鑰以「/」(正斜線) 結尾時也會拒絕該動作。下列範例政策允許使用者將檔案上傳到 Amazon S3 儲存貯體，但拒絕 Amazon S3 儲存貯體中的mkdir命令。

```
{
   "Sid":"DenyMkdir",
   "Action":[
      "s3:PutObject"
   ],
   "Effect":"Deny",
   "Resource":[
      "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*/",
      "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*/*"
    ]
}
```

> **Note**
>
> 第二個資源行使得用戶無法通過運行命令來創建子文件夾，例如put my-file DOC-EXAMPLE-BUCKET/new-folder/my-file。

為 AWS Transfer Family 記錄日誌。

AWS Transfer Family與 Amazon AWS CloudTrail 和整合 CloudWatch。 CloudTrail 並 CloudWatch 服務於不同但互補的目的：

- CloudTrail 是一項AWS服務，用於創建在您的AWS 帳戶. 它會持續監視和記錄 API 呼叫，例如主控台登入、AWS Command Line Interface命令和 SDK/API 呼叫等活動。這使您可以保留誰採取了什麼行動，何時以及從何處進行的日誌。 CloudTrail 提供AWS環境中所有活動的歷史記錄，協助稽核、存取管理和法規遵循。如需詳細資訊，請參閱AWS CloudTrail使用者指南。
- CloudWatch 是AWS資源和應用程式的監視服務。它收集指標和日誌，以提供資源使用率，應用程序性能和整體系統健康狀況的可見性。 CloudWatch 協助進行操作工作，例如疑難排解問題、設定警示和自動調度資源 如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南。

主題

- AWS CloudTrail記錄 AWS Transfer Family
- Amazon CloudWatch 日誌記錄 AWS Transfer Family

AWS CloudTrail記錄 AWS Transfer Family

AWS Transfer Family與 (提供中的使用者AWS CloudTrail、角色或服務所採取的動作記錄) 的AWS服務整合AWS Transfer Family。 CloudTrail 擷取AWS Transfer Family作為事件的所有 API 呼叫。擷取的呼叫包括從 AWS Transfer Family 主控台進行的呼叫，以及針對 AWS Transfer Family API 操作的程式碼呼叫。

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。

如需您 AWS 帳戶中正在進行事件的記錄 (包含 AWS Transfer Family 的事件)，請建立線索。追蹤可 CloudTrail 將日誌檔交付到 Amazon S3 儲存貯體。根據預設，當您在主控台建立線索時，線索會套用到所有 AWS 區域。該追蹤會記錄來自 AWS 分割區中所有區域的事件，並將日誌檔案交付到您指定的 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，請參閱下列內容：

- 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 日誌文件並從多個帳戶接收 CloudTrail 日誌文件

所有AWS Transfer Family動作均由記錄， CloudTrail 並將記錄在中ActionsAPI reference。例如，呼叫`ListUsers`和`StopServer`動作會`CreateServer`在 CloudTrail 記錄檔中產生項目。

每一筆事件或日誌項目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：

- 該請求是否使用根或 AWS Identity and Access Management 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。
- 該請求是否由另一項 AWS 服務提出。

如需詳細資訊，請參閱 CloudTrail userIdentity 元素。

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AWS Transfer Family. 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，您可以判斷提出的要求AWS Transfer Family、提出要求的 IP 位址、提出要求的人員、提出要求的時間，以及其他詳細資訊。

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

主題

- 啟用AWS CloudTrail記錄
- 建立伺服器的範例記錄項目

啟用AWS CloudTrail記錄

您可以使用 AWS CloudTrail 監控 AWS Transfer Family API 呼叫。透過監控 API 呼叫，您可以取得有用的安全及操作資訊。如果您已啟用 Amazon S3 物件層級日誌記錄`RoleSessionName`，請求者欄位中會包含為`[AWS:Role Unique Identifier]/username.sessionid@server-id`。如需有關 AWS Identity and Access Management (IAM) 角色唯一識別碼的詳細資訊，請參閱AWS Identity and Access Management使用者指南中的唯一識別碼。

> **Important**
>
> 的最大長度RoleSessionName為 64 個字元。如果RoleSessionName較長，則會server-id被截斷。

建立伺服器的範例記錄項目

下列範例顯示示範CreateServer動作的 CloudTrail 記錄項目 (JSON 格式)。

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AAAA4FFF5HHHHH6NNWWWW:user1",
        "arn": "arn:aws:sts::123456789102:assumed-role/Admin/user1",
        "accountId": "123456789102",
        "accessKeyId": "AAAA52C2WWWWWW3BB4Z",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-12-18T20:03:57Z"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AAAA4FFF5HHHHH6NNWWWW",
                "arn": "arn:aws:iam::123456789102:role/Admin",
                "accountId": "123456789102",
                "userName": "Admin"
            }
        }
    },
    "eventTime": "2024-02-05T19:18:53Z",
    "eventSource": "transfer.amazonaws.com",
    "eventName": "CreateServer",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "11.22.1.2",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/121.0.0.0 Safari/537.36",
    "requestParameters": {
        "domain": "S3",
        "hostKey": "HIDDEN_DUE_TO_SECURITY_REASONS",
```

```
        "protocols": [
            "SFTP"
        ],
        "protocolDetails": {
            "passiveIp": "AUTO",
            "tlsSessionResumptionMode": "ENFORCED",
            "setStatOption": "DEFAULT"
        },
        "securityPolicyName": "TransferSecurityPolicy-2020-06",
        "s3StorageOptions": {
            "directoryListingOptimization": "ENABLED"
        }
    },
    "responseElements": {
        "serverId": "s-1234abcd5678efghi"
    },
    "requestID": "6fe7e9b1-72fc-45b0-a7f9-5840268aeadf",
    "eventID": "4781364f-7c1e-464e-9598-52d06aa9e63a",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789102",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "transfer.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}
```

Amazon CloudWatch 日誌記錄 AWS Transfer Family

Amazon 會即時 CloudWatch 監控您的 AWS Transfer Family 資源和執行 AWS 的應用程式。您可以用 CloudWatch 來收集和追蹤指標，這些指標是您可以針對資源和應用程式測量的變數。

CloudWatch 首頁會自動顯示有關「Transfer Family」和您使用的所有其他 AWS 服務的量度。您還可以建立自訂儀表板，以顯示自訂應用程式的相關指標，以及顯示您選擇的自訂指標集合。

您可以建立警示來監控指標，並於超過閾值時傳送通知，或自動變更您所監控的資源。例如，您可以監視傳輸到 Transfer Family 伺服器的檔案，並使用該資料來決定是否需要部署其他伺服器來處理增加的負載。您也可以使用這些資料來停止或刪除未充分使用的執行個體，以節省成本。

Transfer Family 的 CloudWatch 日誌記錄類型

「Transfer Family」提供兩種方式來記錄事件 CloudWatch：

- JSON 結構化記錄
- 透過記錄角色進行記錄

對於 Transfer Family 伺服器，您可以選擇您偏好的記錄機制。對於連接器和工作流程，僅支援記錄角色。

JSON 結構化記錄

對於記錄伺服器事件，我們建議使用 JSON 結構化記錄。這會提供更全面的記錄格式，以啟用記 CloudWatch 錄查詢。對於這種類型的記錄，建立伺服器 (或編輯伺服器的記錄設定) 之使用者的 IAM 政策必須包含下列權限：

- `logs:CreateLogDelivery`
- `logs:DeleteLogDelivery`
- `logs:DescribeLogGroups`
- `logs:DescribeResourcePolicies`
- `logs:GetLogDelivery`
- `logs:ListLogDeliveries`
- `logs:PutResourcePolicy`
- `logs:UpdateLogDelivery`

政策範例如下。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogDelivery",
                "logs:GetLogDelivery",
                "logs:UpdateLogDelivery",
```

```
                "logs:DeleteLogDelivery",
                "logs:ListLogDeliveries",
                "logs:PutResourcePolicy",
                "logs:DescribeResourcePolicies",
                "logs:DescribeLogGroups"
            ],
            "Resource": "arn:aws:logs:region-id:AWS ##:log-group:/aws/transfer/*"
        }
    ]
}
```

如需設定 JSON 結構化記錄的詳細資訊，請參閱建立、更新及檢視伺服器的記錄。

記錄角色

若要記錄附加至伺服器的受管理工作流程以及連接器的事件，您需要指定記錄角色。若要設定存取權，您可以建立以資源為基礎的 IAM 政策和提供該存取資訊的 IAM 角色。以下是可以記錄伺服器事件的範例原則。 AWS 帳戶

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:DescribeLogStreams",
                "logs:CreateLogGroup",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/transfer/*"
        }
    ]
}
```

如需配置記錄角色以記錄工作流程事件的詳細資訊，請參閱管理工作流程的記錄。

主題

- 建立、更新及檢視伺服器的記錄
- 管理工作流程的記錄

- 設定 CloudWatch 記錄角色
- 檢視 Transfer Family 日誌串流
- 創建 Amazon CloudWatch 警報
- 將 Amazon S3 API 呼叫記錄到 S3 存取日誌
- 限制混淆副問題的例子
- CloudWatch 轉移系列的記錄結構
- 範例 CloudWatch 記錄項目
- 使用 Transfer Family 的 CloudWatch 量度
- AWS 使用者通知 搭配使用 AWS Transfer Family
- 使用查詢篩選記錄項目

建立、更新及檢視伺服器的記錄

對於所有 AWS Transfer Family 伺服器，您可以選擇兩個記錄選項：`LoggingRole`(用於記錄附加到伺服器的工作流程) 或`StructuredLogDestinations`. 使用 `StructuredLogDestinations` 的優點包括：

- 接收結構化 JSON 格式的記錄檔。
- 使用 Amazon 日誌洞見查詢您的 CloudWatch 日誌，這會自動探索 JSON 格式的欄位。
- 跨 AWS Transfer Family 資源共用記錄群組可讓您將來自多部伺服器的記錄串流合併為單一記錄群組，讓您更輕鬆地管理監控組態和記錄保留設定。
- 建立可新增至 CloudWatch儀表板的彙總量度和視覺效果。
- 使用記錄群組建立合併的記錄指標、視覺效果和儀表板，以追蹤使用情況和效能資料。

`LoggingRole`或的選項`StructuredLogDestinations`會分別設定及控制。對於每個服務器，您可以設置一種或兩種日誌記錄方法，或將服務器配置為沒有任何日誌記錄（儘管不建議這樣做）。

如果您使用 Transfer Family 主控台建立新伺服器，則預設會啟用記錄功能。建立伺服器之後，您可以使用 `UpdateServer` API 呼叫來變更記錄設定。有關詳情，請參閱StructuredLog目的地。

目前，對於工作流程，如果您要啟用記錄，則必須指定記錄角色：

- 如果您使用`CreateServer`或 `UpdateServer` API 呼叫將工作流程與伺服器產生關聯，則系統不會自動建立記錄角色。如果您想要記錄工作流程事件，則需要將記錄角色明確附加到伺服器。

- 如果您使用 Transfer Family 主控台建立伺服器，並附加工作流程，則會將記錄傳送到名稱中包含伺服器 ID 的記錄群組。例如/aws/transfer/*server-id*，格式為/aws/transfer/s-1111aaaa2222bbbb3。伺服器記錄檔可以傳送到這個相同的記錄群組或不同的記錄群組。

在主控台中建立及編輯伺服器的記錄考量

- 透過主控台建立的新伺服器僅支援結構化 JSON 記錄，除非工作流程已附加至伺服器。
- 沒有記錄不是您在控制台中創建的新服務器的選項。
- 現有伺服器可以隨時透過主控台啟用結構化 JSON 記錄。
- 透過主控台啟用結構化 JSON 記錄會停用現有的記錄方法，以免向客戶收取雙倍費用。如果工作流程已附加至伺服器，則例外。
- 如果您啟用結構化 JSON 記錄，則稍後無法透過主控台停用它。
- 如果啟用結構化 JSON 記錄，您可以隨時透過主控台變更記錄群組目的地。
- 如果啟用結構化 JSON 記錄，則無法透過 API 啟用這兩種記錄類型，則無法透過主控台編輯記錄角色。如果您的伺服器已附加工作流程，則例外。不過，記錄角色會繼續出現在其他詳細資料中。

使用 API 或 SDK 建立和編輯伺服器的記錄考量

- 如果您透過 API 建立新伺服器，您可以設定其中一種或兩種類型的記錄，或選擇不記錄。
- 對於現有伺服器，隨時啟用和停用結構化 JSON 記錄。
- 您可以隨時透過 API 變更記錄群組。
- 您可以隨時透過 API 變更記錄角色。

若要啟用結構化記錄，您必須使用下列權限登入帳戶

- `logs:CreateLogDelivery`
- `logs:DeleteLogDelivery`
- `logs:DescribeLogGroups`
- `logs:DescribeResourcePolicies`
- `logs:GetLogDelivery`
- `logs:ListLogDeliveries`
- `logs:PutResourcePolicy`
- `logs:UpdateLogDelivery`

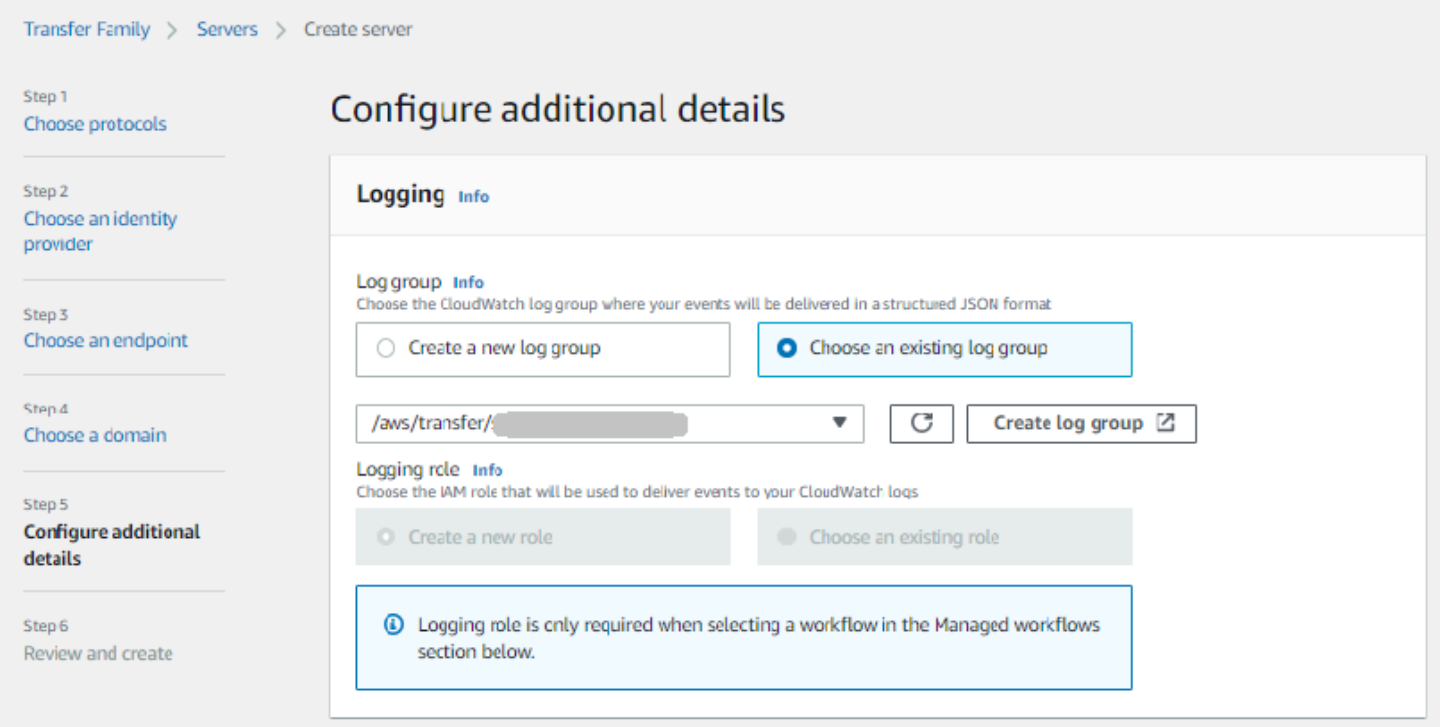
此區段提供範例原則設定 CloudWatch 記錄角色。

主題

- 建立伺服器的記錄
- 更新伺服器的記錄
- 檢視伺服器組態

建立伺服器的記錄

建立新伺服器時，您可以在 [設定其他詳細資料] 頁面上指定現有的記錄群組，或建立新的記錄群組。



如果您選擇 [建立記錄群組]， CloudWatch 主控台 (https://console.aws.amazon.com/cloudwatch/) 會開啟 [建立記錄群組] 頁面。如需詳細資訊，請參閱在 CloudWatch 記錄檔中建立記錄群組。

更新伺服器的記錄

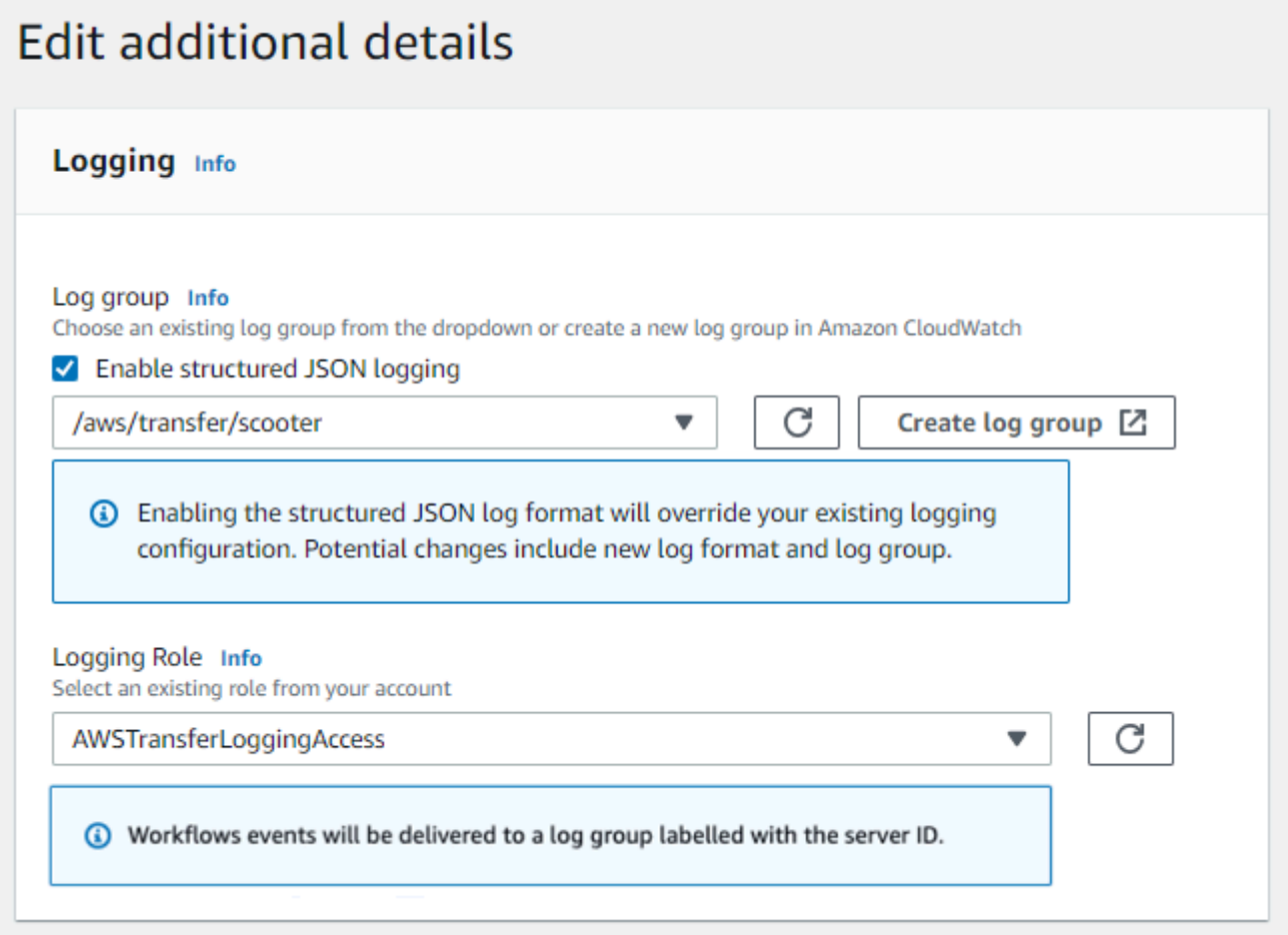
記錄的詳細資料取決於您更新的案例。

> **Note**
>
> 當您選擇使用結構化 JSON 記錄時，在極少數情況下，Transfer Family 會停止以舊格式記錄，但需要一些時間才能開始以新的 JSON 格式登錄。這可能會導致無法記錄的事件。不會有任何

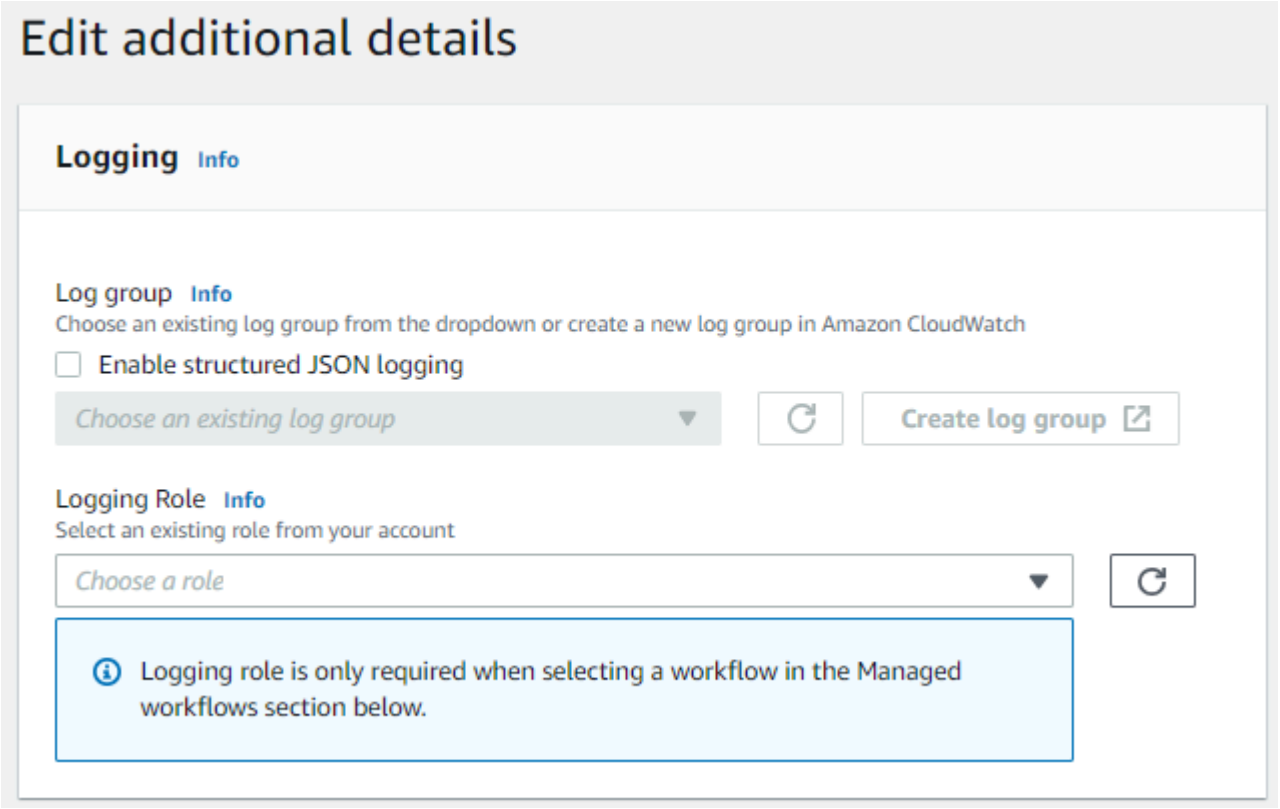
服務中斷，但在變更記錄方法之後的第一個小時內，您應該小心傳輸檔案，因為記錄檔可能會遭到捨棄。

如果您正在編輯現有伺服器，您的選項取決於伺服器的狀態。

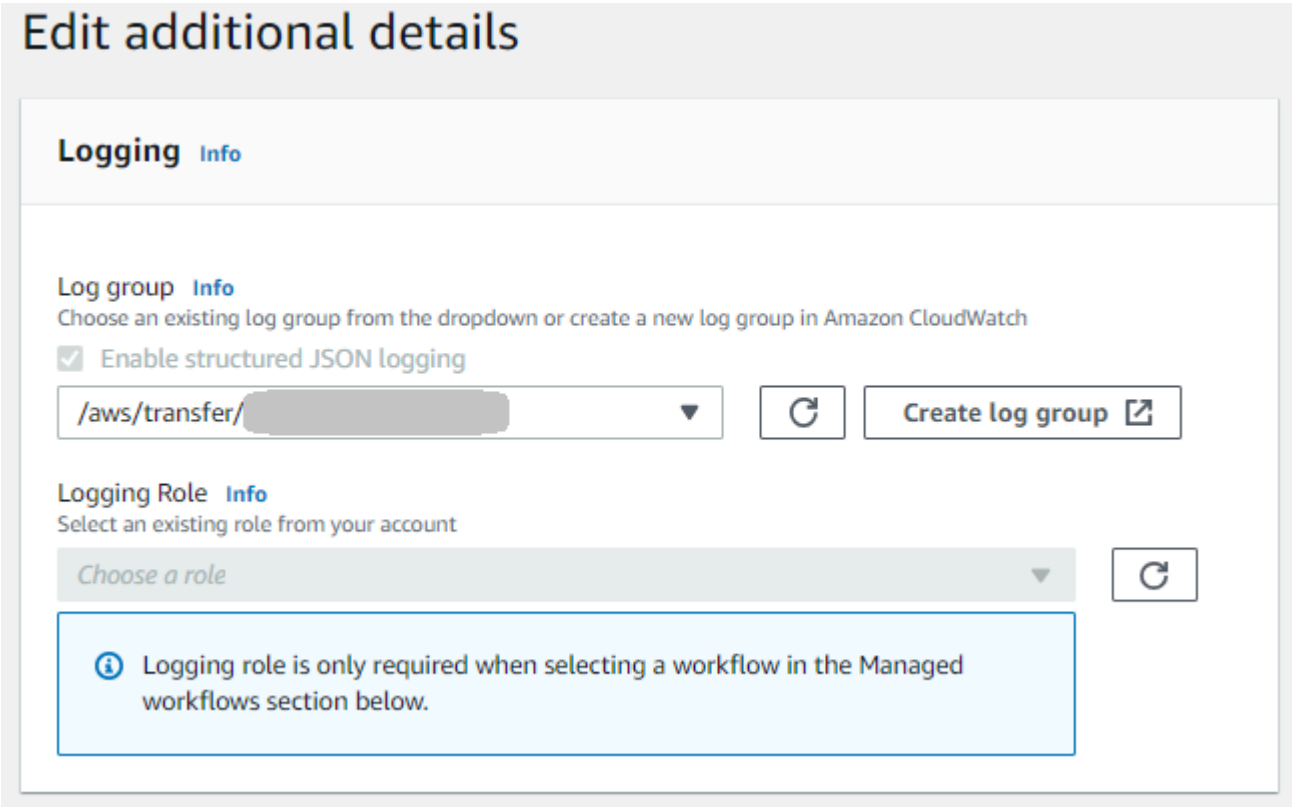
- 伺服器已啟用記錄角色，但未啟用結構化 JSON 記錄。



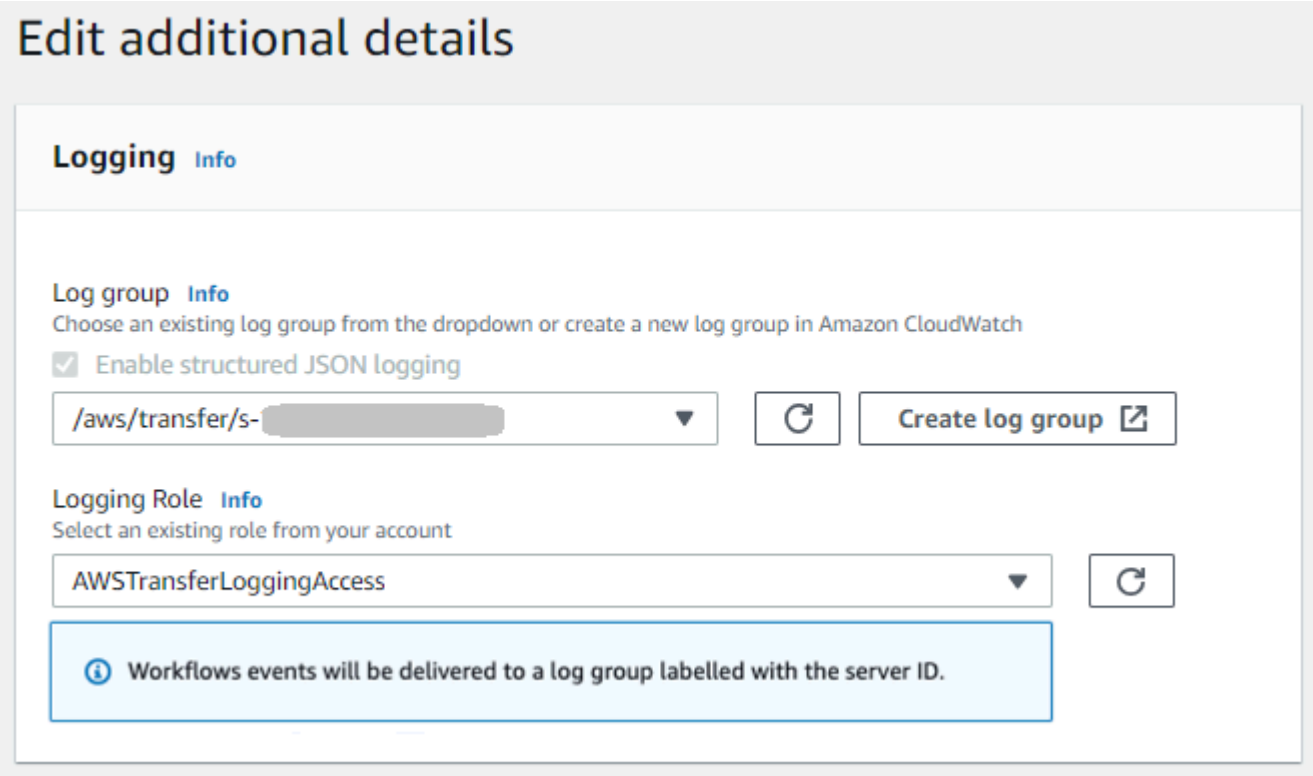
- 伺服器未啟用任何記錄。



- 伺服器已啟用結構化 JSON 記錄，但未指定記錄角色。



- 伺服器已啟用結構化 JSON 記錄，並且還具有指定的記錄角色。

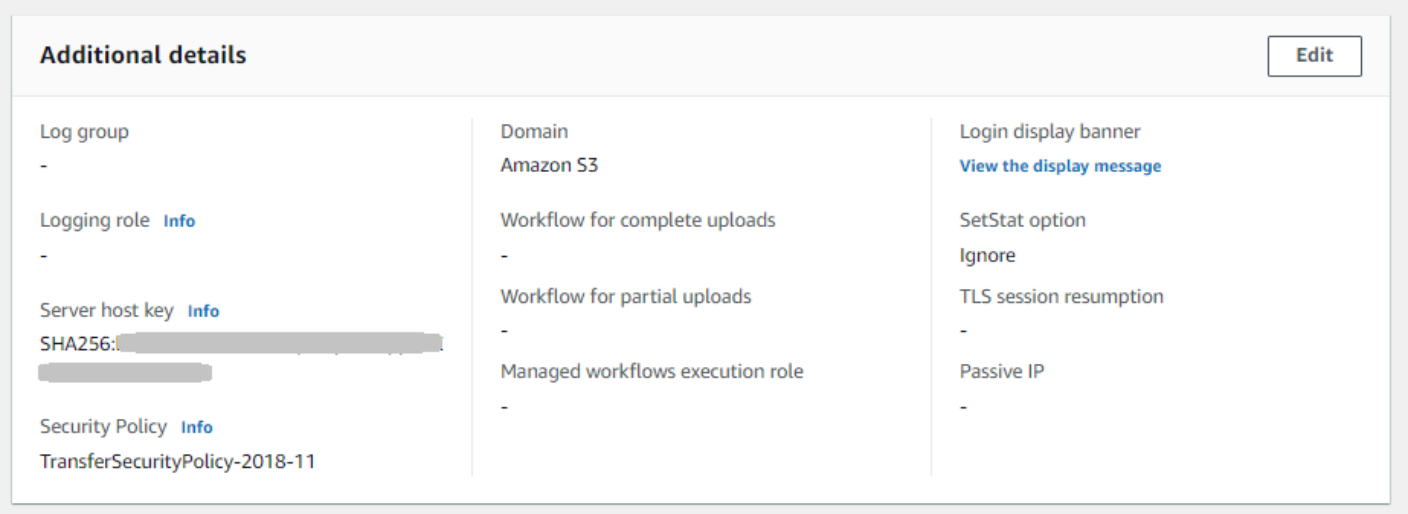


檢視伺服器組態

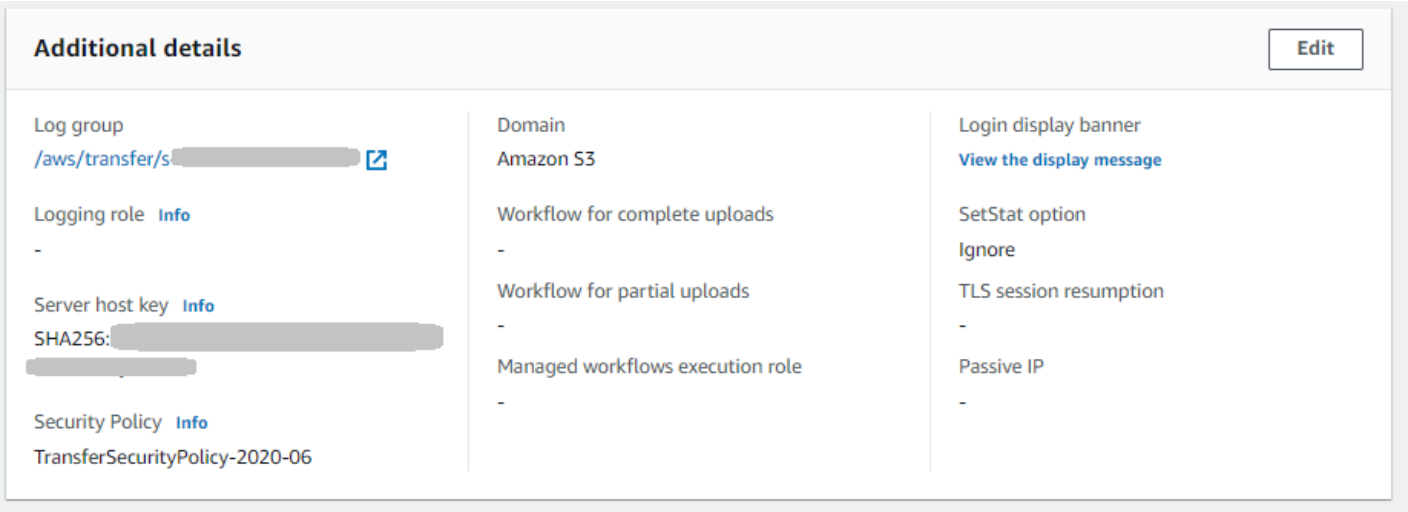
伺服器設定頁面的詳細資訊取決於您的案例：

視您的案例而定，伺服器組態頁面可能看起來像下列其中一個範例：

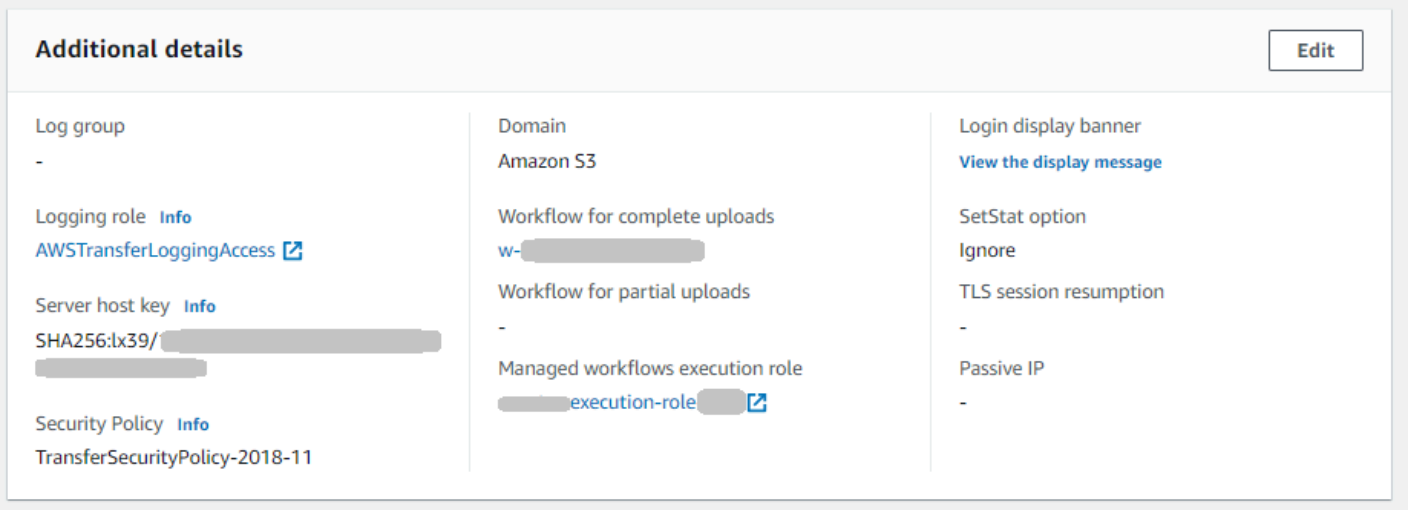
- 未啟用記錄。



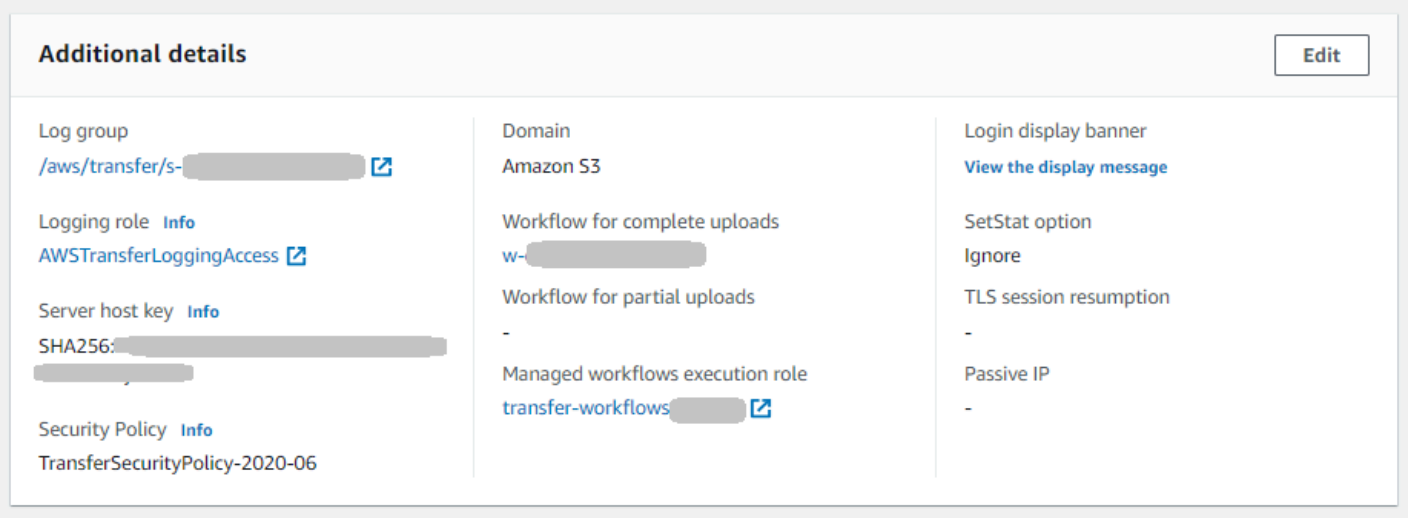
- 已啟用結構化 JSON 記錄。



- 已啟用記錄角色，但未啟用結構化 JSON 記錄。



- 這兩種類型的記錄 (記錄角色和結構化 JSON 記錄) 都會啟用。



管理工作流程的記錄

CloudWatch 為工作流程進度和結果提供合併的稽核和記錄。此外，還 AWS Transfer Family 提供工作流程的數個指標。您可以檢視前一分鐘開始、成功完成和失敗的工作流程執行數目的度量。「Transfer Family」的所有 CloudWatch 量度均在中說明使用 Transfer Family 的 CloudWatch 量度。

檢視工作流程的 Amazon CloudWatch 日誌

1. 在以下位置打開 Amazon CloudWatch 控制台 https://console.aws.amazon.com/cloudwatch/。
2. 在左側導覽窗格中，選擇「記錄檔」，然後選擇「記錄群組」。
3. 在 [記錄群組] 頁面的導覽列上，為您的 AWS Transfer Family 伺服器選擇正確的 [區域]。
4. 選擇與您的伺服器對應的記錄群組。

   例如，如果您的伺服器 ID 是`s-1234567890abcdef0`，則您的記錄群組為`/aws/transfer/s-1234567890abcdef0`。
5. 在伺服器的日誌群組詳細資料頁面上，會顯示最新的記錄資料流。您正在探索的使用者有兩個記錄資料流：

   - 每個安全殼層 (SSH) 檔案傳輸通訊協定 (SFTP) 工作階段各一個。
   - 一個用於為您的伺服器執行的工作流程。工作流程的記錄資料流格式為*`username`*`.`*`workflowID`*`.`*`uniqueStreamSuffix`*。

   例如，如果您的使用者是`mary-major`，則會有下列記錄資料流：

```
mary-major-east.1234567890abcdef0
mary.w-abcdef01234567890.021345abcdef6789
```

> **Note**
>
> 此範例中列出的 16 位數字英數識別碼是虛構的。您在 Amazon 看到的值 CloudWatch 是不同的。

的 [記錄事件] 頁面會mary-major-usa-east.1234567890abcdef0顯示每個使用者階段作業的詳細資訊，而mary.w-abcdef01234567890.021345abcdef6789記錄資料流則包含工作流程的詳細資訊。

以下是以包含複製步驟的工作流程 (w-abcdef01234567890) 為mary.w-abcdef01234567890.021345abcdef6789基礎的範例記錄資料流。

```
{
    "type": "ExecutionStarted",
    "details": {
        "input": {
            "initialFileLocation": {
                "bucket": "DOC-EXAMPLE-BUCKET",
                "key": "mary/workflowSteps2.json",
                "versionId": "version-id",
                "etag": "etag-id"
            }
        }
    },
    "workflowId":"w-abcdef01234567890",
    "executionId":"execution-id",
    "transferDetails": {
        "serverId":"s-server-id",
        "username":"mary",
        "sessionId":"session-id"
    }
},
{
    "type":"StepStarted",
    "details": {
        "input": {
```

```
            "fileLocation": {
                "backingStore":"S3",
                "bucket":"DOC-EXAMPLE-BUCKET",
                "key":"mary/workflowSteps2.json",
                "versionId":"version-id",
                "etag":"etag-id"
            }
        },
        "stepType":"COPY",
        "stepName":"copyToShared"
    },
    "workflowId":"w-abcdef01234567890",
    "executionId":"execution-id",
    "transferDetails": {
        "serverId":"s-server-id",
        "username":"mary",
        "sessionId":"session-id"
    }
},
{
    "type":"StepCompleted",
    "details":{
        "output":{},
        "stepType":"COPY",
        "stepName":"copyToShared"
    },
    "workflowId":"w-abcdef01234567890",
    "executionId":"execution-id",
    "transferDetails":{
        "serverId":"server-id",
        "username":"mary",
        "sessionId":"session-id"
    }
},
{
    "type":"ExecutionCompleted",
    "details": {},
    "workflowId":"w-abcdef01234567890",
    "executionId":"execution-id",
    "transferDetails":{
        "serverId":"s-server-id",
        "username":"mary",
        "sessionId":"session-id"
    }
```

```
}
```

設定 CloudWatch 記錄角色

若要設定存取權，您可以建立以資源為基礎的 IAM 政策和提供該存取資訊的 IAM 角色。

若要啟用 Amazon CloudWatch 記錄，請先建立啟用 CloudWatch記錄功能的 IAM 政策。然後，您可以建立 IAM 角色並將政策附加到該角色。您可以在建立伺服器或編輯現有伺服器時執行此操作。如需詳細資訊 CloudWatch，請參閱什麼是 Amazon CloudWatch？ 什麼是 Amazon CloudWatch 日誌？ 在 Amazon 用 CloudWatch 戶指南。

使用下列 IAM 政策範例允許 CloudWatch 記錄。

Use a logging role

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:DescribeLogStreams",
                "logs:CreateLogGroup",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/transfer/*"
        }
    ]
}
```

Use structured logging

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogDelivery",
                "logs:GetLogDelivery",
```

```
                "logs:UpdateLogDelivery",
                "logs:DeleteLogDelivery",
                "logs:ListLogDeliveries",
                "logs:PutResourcePolicy",
                "logs:DescribeResourcePolicies",
                "logs:DescribeLogGroups"
            ],
            "Resource": "arn:aws:logs:region-id:AWS ##:log-group:/aws/transfer/*"
        }
    ]
}
```

在上述範例政策中，針對**Resource**，取代*#####AWS ##*與您的值。例如：**"Resource": "arn:aws::logs:us-east-1:111122223333:log-group:/aws/transfer/*"**

然後，您可以建立角色並附加您建立的 CloudWatch 記錄檔原則。

建立 IAM 角色並連接政策

1. 在導覽窗格中，選擇 Roles (角色)，然後選擇 Create role (建立角色)。

   在 [建立角色] 頁面上，確定已選取AWS 服務。
2. 從服務清單選擇 Transfer (傳輸)，然後選擇 Next: Permissions (下一步：許可)。這會在 AWS Transfer Family 和 IAM 角色之間建立信任關係。此外，添加`aws:SourceAccount`和`aws:SourceArn`調節鍵以保護自己免受混淆的副問題。如需詳細資訊，請參閱下列文件：

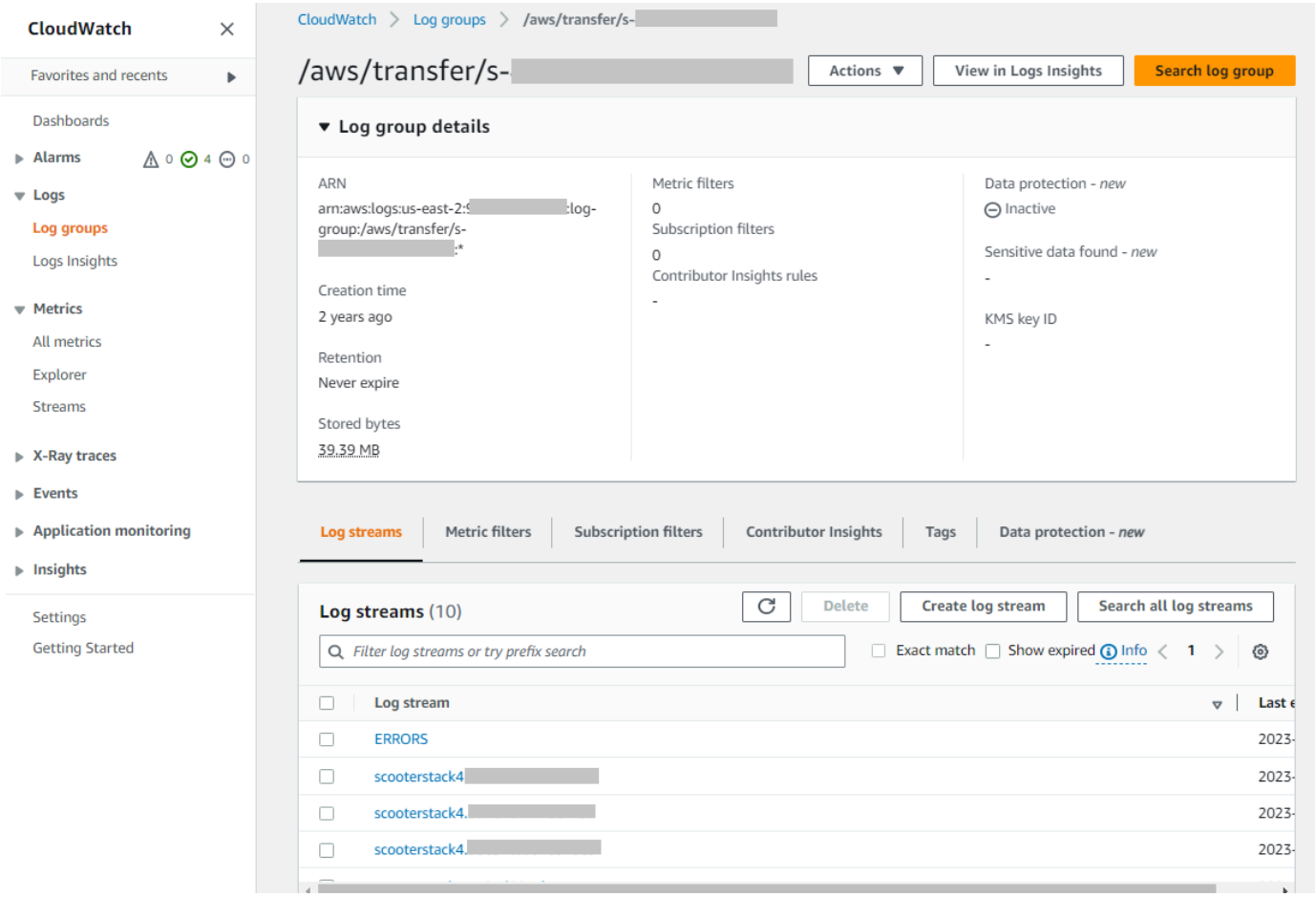
   - 建立信任關係的程序 AWS Transfer Family：建立信任關係
   - 混淆副問題描述：混淆的副問題
3. 在 [附加權限原則] 區段中，找出並選擇您剛建立的 CloudWatch 記錄檔原則，然後選擇 [下一步：標籤]。
4. (選用) 輸入標籤的金鑰和值，然後選擇 Next: Review (下一步：檢閱)。
5. 在 Review (檢閱) 頁面上，輸入您新角色的名稱和描述，然後選擇 Create role (建立角色)。
6. 若要檢視記錄檔，請選擇 [伺服器 ID] 以開啟伺服器組態頁面，然後選擇 [檢視記錄檔]。您將被重定向到 CloudWatch 控制台，您可以在其中查看日誌流。

在伺服器的 CloudWatch 頁面上，您可以看到使用者驗證 (成功與失敗)、資料上傳 (PUT作業) 和資料下載 (GET作業) 的記錄。

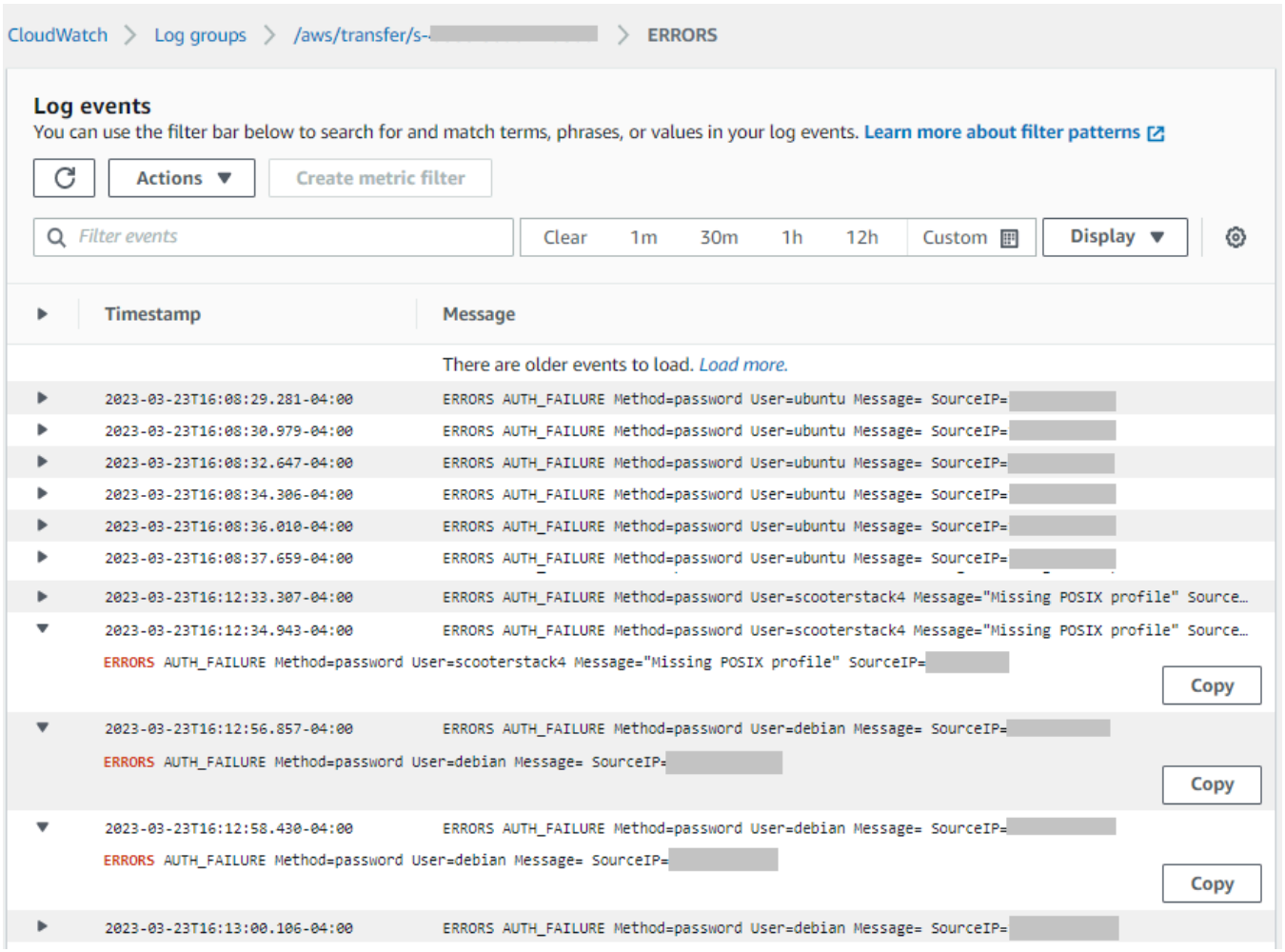
檢視 Transfer Family 日誌串流

若要檢視轉移系列伺服器記錄

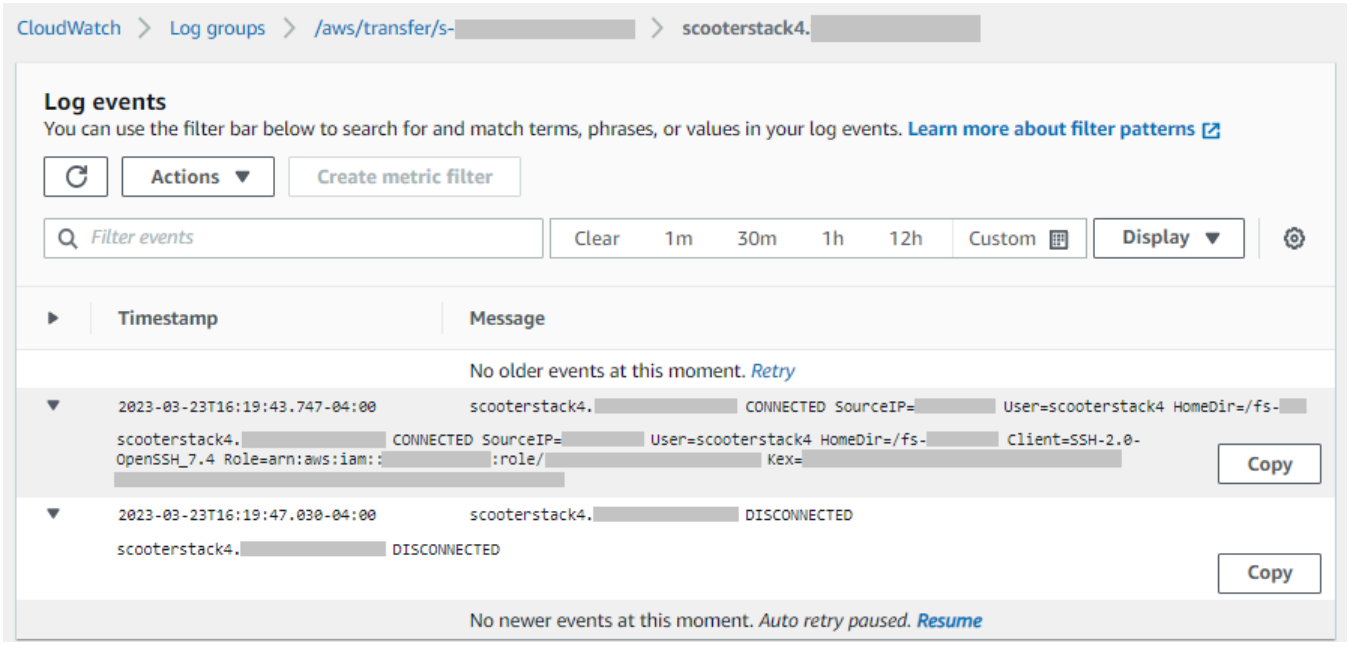
1. 導覽至伺服器的詳細資訊頁面。
2. 選擇 [檢視記錄]。這將打開 Amazon CloudWatch。
3. 此時會顯示所選伺服器的記錄群組。



4. 您可以選取記錄串流，以顯示串流的詳細資料和個別項目。
   - 如果有 ERRO RS 清單，您可以選擇此清單來檢視伺服器最新錯誤的詳細資訊。

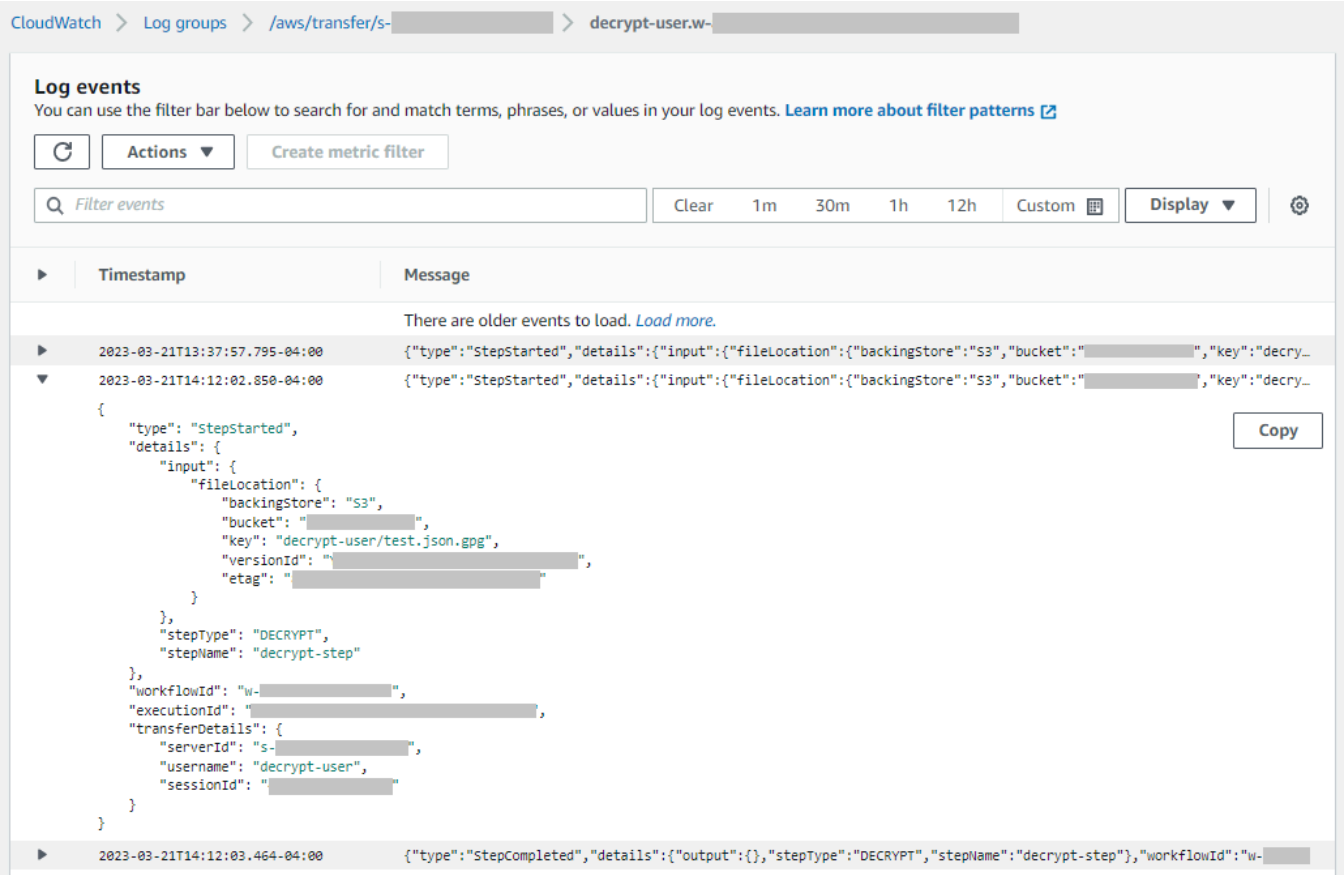


- 選擇任何其他項目以查看範例記錄資料流。



- 如果您的伺服器具有與其關聯的受管理工作流程，您可以檢視工作流程執行的記錄。

> **Note**
>
> 工作流程的記錄資料流格式為*username*.*workflowId*.*uniqueStreamSuffix*。例如，解密使用者 .w-a1111222233334444.aa1111bbbb2222 可以是使用者和工作流程的記錄資料流的名稱。**decrypt-user w-a1111222233334444**



> **Note**
>
> 對於任何展開的記錄項目，您可以選擇 [複製] 將項目複製到剪貼簿。如需有關 CloudWatch 記錄檔的詳細資訊，請參閱檢視記錄資料。

創建 Amazon CloudWatch 警報

下列範例顯示如何使用 AWS Transfer Family 指標建立 Amazon CloudWatch 警示`FilesIn`。

CDK

```
new cloudwatch.Metric({
  namespace: "AWS/Transfer",
  metricName: "FilesIn",
  dimensionsMap: { ServerId: "s-00000000000000000" },
  statistic: "Average",
  period: cdk.Duration.minutes(1),
}).createAlarm(this, "AWS/Transfer FilesIn", {
  threshold: 1000,
  evaluationPeriods: 10,
  datapointsToAlarm: 5,
  comparisonOperator:
 cloudwatch.ComparisonOperator.GREATER_THAN_OR_EQUAL_TO_THRESHOLD,
});
```

AWS CloudFormation

```
Type: AWS::CloudWatch::Alarm
Properties:
  Namespace: AWS/Transfer
  MetricName: FilesIn
  Dimensions:
    - Name: ServerId
      Value: s-00000000000000000
  Statistic: Average
  Period: 60
  Threshold: 1000
  EvaluationPeriods: 10
  DatapointsToAlarm: 5
  ComparisonOperator: GreaterThanOrEqualToThreshold
```

將 Amazon S3 API 呼叫記錄到 S3 存取日誌

如果您使用 Amazon S3 存取日誌來識別代表檔案傳輸使用者發出的 S3 請求，則會使用`RoleSessionName`哪個 IAM 角色來顯示為檔案傳輸服務的 IAM 角色。它還顯示其他信息，例如用於傳輸的用戶名，會話 ID 和服務器 ID。格式包含在「請求者」欄位中。`[AWS:Role Unique`

Identifier]/username.sessionid@server-id例如，以下是複製到 S3 儲存貯體之檔案的 S3 存取日誌中範例請求者欄位的內容。

arn:aws:sts::AWS-Account-ID:assumed-role/*IamRoleName*/username.sessionid@server-id

在上面的「請求者」欄位中，它會顯示呼叫IamRoleName的 IAM 角色。如需 IAM 角色唯一識別碼的詳細資訊，請參閱AWS Identity and Access Management 使用者指南中的唯一識別碼。

限制混淆副問題的例子

混淆代理人問題屬於安全性議題，其中沒有執行動作許可的實體可以強制具有更多許可的實體執行該動作。在中 AWS，跨服務模擬可能會導致混淆的副問題。如需詳細資訊，請參閱預防跨服務混淆代理人。

> **Note**
>
> 在下列範例中，將每個*#########*取代為您自己的資訊。
> 在這些範例中，如果伺服器沒有附加任何工作流程，您可以移除工作流程的 ARN 詳細資料。

下列範例記錄/叫用策略允許帳戶中的任何伺服器 (和工作流程) 擔任該角色。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAllServersWithWorkflowAttached",
            "Effect": "Allow",
            "Principal": {
                "Service": "transfer.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "account-id"
                },
                "ArnLike": {
                   "aws:SourceArn": [
                     "arn:aws:transfer:region:account-id:server/*",
                     "arn:aws:transfer:region:account-id:workflow/*"
```

```
                    ]
                }
            }
        }
    ]
}
```

下列範例記錄/呼叫原則可讓特定伺服器 (和工作流程) 擔任該角色。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSpecificServerWithWorkflowAttached",
            "Effect": "Allow",
            "Principal": {
                "Service": "transfer.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "account-id"
                },
                "ArnEquals": {
                   "aws:SourceArn": [
                       "arn:aws:transfer:region:account-id:server/server-id",
                       "arn:aws:transfer:region:account-id:workflow/workflow-id"
                   ]
                }
            }
        }
    ]
}
```

CloudWatch 轉移系列的記錄結構

本主題說明 Transfer Family 記錄中填入的欄位：JSON 結構化記錄項目和舊版記錄項目。

主題

- Transfer Family 列的 JSON 結構化記錄
- Transfer Family 列的舊版記錄

Transfer Family 列的 JSON 結構化記錄

下表包含「Transfer Family SFTP/FTPS」動作的記錄項目欄位詳細資料，採用新的 JSON 結構化記錄格式。

欄位	描述	項目範例
activity-type	The action by the user	打開 | 關閉 | 部分 _ 關閉 | 斷開連接 | 已連接
bytes-in	Number of bytes uploaded by the user	29238420042
bytes-out	Number of bytes downloaded by the user	23094032490328
ciphers	Specifies the SSH cipher negotiated for the connection (available ciphers are listed in 加密算法)	aes256-gcm@openssh.com
client	The user's client software	SSH-2.0-OpenSSH_7.4
home-dir	The directory that the end user lands on when they connect to the endpoint if their home directory type is PATH: if they have a logical home directory, this value is always /	/user-home-bucket/test
kex	Specifies the negotiated SSH key exchange (KEX) for the connection (available KEX are listed in 加密算法)	diffie-hellman-group14-sha256
message	Provides more information related to the error	*<string>*
method	The authentication method	publickey

欄位	描述	項目範例
mode	Specifies how a client opens a file	CREATE | TRUNCATE | WRITE
operation	The client operation on a file	OPEN | CLOSE
path	Actual file path affected	/user-test-bucket/test-file-1.pdf
resource-arn	A system-assigned, unique identifier for a specific resource (for example, a server)	射線:AWN: 轉移:A-東北-1 :12346789012: 伺服器
role	The IAM role of the user	ARN: AW: IAM:: 0293883675: 角色/測試用戶角色
session-id	A system-assigned, unique identifier for a single session	9 CA9A0E1 电子 6AD9
source-ip	Client IP address	18.323.0.129
user	The end user's username	myname192
user-policy	The permissions specified for the end user: this field is populated if the user's policy is a session policy.	The JSON code for the session policy that is being used

Transfer Family 列的舊版記錄

下表包含各種「Transfer Family 列」動作的記錄項目詳細資訊。

> **Note**
>
> 這些項目不是新的 JSON 結構化記錄格式。

下表包含各種「Transfer Family」動作的記錄項目詳細資料，採用新的 JSON 結構化記錄格式。

動作	Amazon 日誌中的對應 CloudWatch 日誌
Authentication failures (身分驗證失敗)	驗證失敗的錯誤方法 = 公開金鑰使用者 = LHR 訊息 = "RSA SHA256: LFZ3 R2 解碼器 +B7RB1RSV 資料夾 + 加上 HX0C7L1JIZ0 SourceIP =3.8.172.211
複製/標籤/刪除/解密工作流程	{「類型」：「，」詳細信息」：{StepStarted「輸入」：{「文件位置」：{「備份存儲」：「EFS」，「文件系統」：「FS-12345678」，「路徑」：「/lhr/regex.py」}，「步驟類型」：「標籤」，「stepName」：「成功標籤」「執行識別碼」: "執行識別碼": "-1234-效果 -5678 字串", "傳輸詳細資料": {"serverId": "-1234 固定檔 5678ghi」, "使用者名稱」: "lhr」, "會 sessionId」：
自訂步驟工作流	{"類型」: CustomStepInvoked「," 詳細資訊」：{"輸出」: {"令牌」: "MZM4MG5」下EzMy午 00 YjIz LWI3OG MtYz U4OGI2 ZjQyMz E5"}, "步驟類型」: "自定義」, "stepName」: "EFS-s3_copy_2"},「workflowId 動」: "w-9283e49" 執行" "傳輸詳細資料": {"伺服器識別碼」: "serverId」: "-" 使用者名稱 "," 使用者名稱」: "超級」, "工作 sessionId」: "1234567890abcdef0"}}
刪除	刪除路徑 =/儲存貯體/使用者
下載	開放路徑 =/儲存貯體/使用者 /123.JPG 模式 = 已讀取 封閉路徑 =/儲存貯體/使用者 BytesOut
登入/登出	連線 SourceIP = 邏輯用戶端 = 邏輯用戶端 = SS-7.4 角色 = 角色 HomeDir 中斷連線的使用者

動作	Amazon 日誌中的對應 CloudWatch 日誌
重新命名	重新命名路徑 =/儲存貯體/使用者/花瓶 .png = /儲存組/使用者/法拉利 NewPath
工作流程錯誤記錄檔	{"類型」: StepErrored「」, "詳細資料」: {"errorType」: "錯誤請求」, "errorMessage」: "無法標記檔案", "步驟類型」: "標籤」, "stepName」: "成功 _ 標籤」步驟 "}," workflowId 標籤」: "w -1234abcd5678efi」4-方法 -5678 輸入 "," 傳輸詳細資料」: {"serverId」: "-1234B」, "使用者名稱": "lhr」, "工作 sessionId」: "1234567890abcdef0"}}
符號鏈接	創建符號鏈接 = /fs-12445678/lhr/pqr.jpg = LinkPath TargetPath
上傳	開放路徑 =/儲存貯體/使用者 /123.JPG 模式 = 建立 | 主幹 | 寫入 封閉路徑 =/儲存貯體/使用者 BytesIn
工作流程	{"類型」: ExecutionStarted「," 詳細資料」: {"輸入」: {」 「備份存儲」: "檔案系統": "檔案系統": "FS-12345678」, "路徑」:」/lhr/regex.py initialFileLocation「}}," workflowId 標 ":" W-1111AAA22bb3", "「傳輸詳細資料」: {"serverId」: "-" 使用者名稱」: "使用者名稱」: "lhr」, "工作 sessionId": "1234567890」 {「類型」:「」, StepStarted「詳細資訊」: {"輸入」: {"檔案位置」: {"備份存儲」: "EFS", "檔案系統」: "fs-12345678」, "路徑」:」/lhr/regex.py「}," 步驟類型」: "自訂」, "stepName」: "「執行識別碼」: "執行識別碼」: "-1834-效果 -5678," 傳輸詳細資料」: {"serverId": "-18ca49dce5d842e0b」, "使用者名稱」: "lhr」, 0"}}

範例 CloudWatch 記錄項目

本主題介紹範例記錄項目。

主題

- 傳輸工作階段記錄項目範
- SFTP 連接器的記錄項目範例
- 金鑰交換演算法失敗的範例記錄項目

傳輸工作階段記錄項目範

在此範例中，SFTP 使用者連線至 Transfer Family 伺服器、上傳檔案，然後中斷與工作階段的連線。

下列記錄項目會反映連線至 Transfer Family 伺服器的 SFTP 使用者。

```
{
   "role": "arn:aws:iam::500655546075:role/scooter-transfer-s3",
   "activity-type": "CONNECTED",
   "ciphers": "chacha20-poly1305@openssh.com,chacha20-poly1305@openssh.com",
   "client": "SSH-2.0-OpenSSH_7.4",
   "source-ip": "52.94.133.133",
   "resource-arn": "arn:aws:transfer:us-east-1:500655546075:server/
s-3fe215d89f074ed2a",
   "home-dir": "/scooter-test/log-me",
   "user": "log-me",
   "kex": "ecdh-sha2-nistp256",
   "session-id": "9ca9a0e1cec6ad9d"
}
```

下列日誌項目反映了將檔案上傳到其 Amazon S3 儲存貯體的 SFTP 使用者。

```
{
   "mode": "CREATE|TRUNCATE|WRITE",
   "path": "/scooter-test/log-me/config-file",
   "activity-type": "OPEN",
   "resource-arn": "arn:aws:transfer:us-east-1:500655546075:server/
s-3fe215d89f074ed2a",
   "session-id": "9ca9a0e1cec6ad9d"
}
```

下列記錄項目反映 SFTP 使用者中斷其 SFTP 工作階段的連線。首先，用戶端會關閉與值區的連線，然後用戶端中斷 SFTP 工作階段的連線。

```
{
   "path": "/scooter-test/log-me/config-file",
   "activity-type": "CLOSE",
   "resource-arn": "arn:aws:transfer:us-east-1:500655546075:server/
s-3fe215d89f074ed2a",
   "bytes-in": "121",
   "session-id": "9ca9a0e1cec6ad9d"
}

{
   "activity-type": "DISCONNECTED",
   "resource-arn": "arn:aws:transfer:us-east-1:500655546075:server/
s-3fe215d89f074ed2a",
   "session-id": "9ca9a0e1cec6ad9d"
}
```

SFTP 連接器的記錄項目範例

本節包含傳輸成功和失敗傳輸的範例記錄檔。記錄會產生至名為的記錄群組`/aws/transfer/`*`connector-id`*，其中*`####`*別碼是 SFTP 連接器的識別碼。

> **Note**
>
> SFTP 連接器的記錄項目只會在您執行`StartFileTransfer`指令時產生。

此記錄項目適用於成功完成的移轉作業。

```
{
    "operation": "RETRIEVE",
    "timestamp": "2023-10-25T16:33:27.373720Z",
    "connector-id": "connector-id",
    "transfer-id": "transfer-id",
    "file-transfer-id": "transfer-id/file-transfer-id",
    "url": "sftp://192.0.2.0",
    "file-path": "/remotebucket/remotefilepath",
    "status-code": "COMPLETED",
    "start-time": "2023-10-25T16:33:26.945481Z",
    "end-time": "2023-10-25T16:33:27.159823Z",
```

```
    "account-id": "480351544584",
    "connector-arn": "arn:aws:transfer:us-east-1:480351544584:connector/connector-id",
    "local-directory-path": "/connectors-localbucket"
    "bytes": 514
}
```

此記錄項目適用於逾時的傳輸，因此未順利完成。

```
{
    "operation": "RETRIEVE",
    "timestamp": "2023-10-25T22:33:47.625703Z",
    "connector-id": "connector-id",
    "transfer-id": "transfer-id",
    "file-transfer-id": "transfer-id/file-transfer-id",
    "url": "sftp://192.0.2.0",
    "file-path": "/remotebucket/remotefilepath",
    "status-code": "FAILED",
    "failure-code": "TIMEOUT_ERROR",
    "failure-message": "Transfer request timeout.",
    "account-id": "480351544584",
    "connector-arn": "arn:aws:transfer:us-east-1:480351544584:connector/connector-id",
    "local-directory-path": "/connectors-localbucket"
}
```

此記錄項目適用於成功的 SEND 作業。

```
{
    "operation": "SEND",
    "timestamp": "2024-04-24T18:16:12.513207284Z",
    "connector-id": "connector-id",
    "transfer-id": "transfer-id",
    "file-transfer-id": "transfer-id/file-transfer-id",
    "url": "sftp://server-id.server.transfer.us-east-1.amazonaws.com",
    "file-path": "/DOC-EXAMPLE-BUCKET/my-test-folder/connector-metrics-us-
east-1-2024-01-02.csv",
    "status-code": "COMPLETED",
    "start-time": "2024-04-24T18:16:12.295235884Z",
    "end-time": "2024-04-24T18:16:12.461840732Z",
    "account-id": "255443218509",
    "connector-arn": "arn:aws:transfer:us-east-1:255443218509:connector/connector-id",
    "bytes": 275
}
```

上一個記錄範例中某些主鍵欄位的描述。

- timestamp表示記錄新增至的時間 CloudWatch。 start-time並end-time對應於連接器實際啟動和完成傳輸的時間。
- transfer-id是針對每個start-file-transfer要求指派的唯一識別碼。如果用戶在單個 start-file-transfer API 調用中傳遞多個文件路徑，則所有文件共享相同的路徑transfer-id。
- file-transfer-id是針對每個傳輸的檔案產生的唯一值。請注意，的file-transfer-id初始部分與transfer-id。

金鑰交換演算法失敗的範例記錄項目

本節包含金鑰交換演算法 (KEX) 失敗的範例記錄。這些是結構化記錄檔的 ERRO RS 記錄資料流中的範例。

此記錄項目是發生主機金鑰類型錯誤的範例。

```
{
    "activity-type": "KEX_FAILURE",
    "source-ip": "999.999.999.999",
    "resource-arn": "arn:aws:transfer:us-east-1:999999999999:server/
s-999999999999999999",
    "message": "no matching host key type found",
    "kex": "ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,ecdsa-sha2-
nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-
nistp521-cert-v01@openssh.com,ssh-ed25519,ssh-rsa,ssh-dss"
}
```

此記錄項目是 KEX 不相符的範例。

```
{
    "activity-type": "KEX_FAILURE",
    "source-ip": "999.999.999.999",
    "resource-arn": "arn:aws:transfer:us-east-1:999999999999:server/
s-999999999999999999",
    "message": "no matching key exchange method found",
    "kex": "diffie-hellman-group1-sha1,diffie-hellman-group14-sha1,diffie-hellman-
group14-sha256"
}
```

使用 Transfer Family 的 CloudWatch 量度

> **Note**
>
> 您也可以從「Transfer Family」主控台本身取得「Transfer Family」的指標。如需詳細資訊，請參閱 在主控台中監控使用情況

您可以使用 CloudWatch 指標獲取有關服務器的信息。量度代表發佈至 CloudWatch的一組時間順序的資料點。使用量度時，您必須指定「Transfer Family」命名空間、量度名稱和維度。如需有關指標的詳細資訊，請參閱 Amazon CloudWatch 使用者指南中的指標。

下表說明「Transfer Family」的 CloudWatch 測量結果。

命名空間	指標	描述
AWS/Transfer	BytesIn	傳輸到伺服器的位元組總數。 單位：計數 期間：5 分鐘
	BytesOut	從伺服器傳出的位元組總數。 單位：計數 期間：5 分鐘
	FilesIn	傳輸到伺服器的檔案總數。 對於使用 AS2 通訊協定的伺服器，此測量結果代表接收的訊息數目。 單位：計數 期間：5 分鐘
	FilesOut	從伺服器傳出的檔案總數。 單位：計數

命名空間	指標	描述
		期間：5 分鐘
	InboundMessage	成功從交易夥伴收到的 AS2 訊息總數。 單位：計數 期間：5 分鐘
	InboundFailedMessage	從交易夥伴收到未成功的 AS2 訊息總數。也就是說，交易夥伴發送了一條消息，但 Transfer Family 服務器無法成功處理它。 單位：計數 期間：5 分鐘
	OnUploadExecutionsStarted	在伺服器上啟動的工作流程執行總數。 單位：計數 時間：1 分鐘
	OnUploadExecutionsSuccess	伺服器上成功的工作流程執行總數。 單位：計數 時間：1 分鐘
	OnUploadExecutionsFailed	伺服器上失敗的工作流程執行總數。 單位：計數 時間：1 分鐘

Transfer Family 維度

維度是一組名稱值對，是指標身分的一部分。如需維度的詳細資訊，請參閱 Amazon CloudWatch 使用者指南中的維度。

下表說明「Transfer Family」的 CloudWatch 維度。

維度	描述
ServerId	伺服器的唯一識別碼。

AWS 使用者通知 搭配使用 AWS Transfer Family

若要收到有關 AWS Transfer Family 事件的通知，您可AWS 使用者通知以使用設定各種傳送管道。當事件符合您指定的規則時，您會收到通知。

您可以透過多個管道接收事件通知，包括電子郵件、AWS Chatbot 聊天通知或 AWS Console Mobile Application 推送通知。您也可以在「主控台通知中心」中查看通知。 使用者通知 支援彙總，可減少您在特定事件期間收到的通知數量。

如需詳細資訊，請參閱使用 AWS Transfer Family 受管理的工作流程自訂檔案傳遞通知部落格文章和什麼是 AWS 使用者通知？ 在《AWS 使用者通知 使用者指南》中。

使用查詢篩選記錄項目

您可以使用 CloudWatch 查詢來篩選和識別「Transfer Family」的記錄項目。本節包含一些範例。

1. 請登入 AWS Management Console 並開啟 CloudWatch 主控台，網址為 https://console.aws.amazon.com/cloudwatch/。
2. 您可以建立查詢或規則。
   - 若要建立 Logs Insights 查詢，請從左側導覽面板中選擇「記錄深入解析」，然後輸入查詢的詳細資料。
   - 若要建立參與者見解規則，請從左側導覽面板中選擇「深入解析」>「參與者見解」，然後輸入規則的詳細資料。
3. 執行您建立的查詢或規則。

檢視主要的驗證失敗因素

在您的結構化記錄檔中，驗證失敗記錄項目看起來類似下列內容：

```
{
  "method":"password",
  "activity-type":"AUTH_FAILURE",
  "source-ip":"999.999.999.999",
```

```
  "resource-arn":"arn:aws:transfer:us-east-1:999999999999:server/s-0123456789abcdef",
  "message":"Invalid user name or password",
  "user":"exampleUser"
}
```

執行下列查詢，檢視驗證失敗的主要貢獻者。

```
filter @logStream = 'ERRORS'
| filter `activity-type` = 'AUTH_FAILURE'
| stats count() as AuthFailures by user, method
| sort by AuthFailures desc
| limit 10
```

您可以建立CloudWatch 貢獻CloudWatch 者見解規則來檢視驗證失敗，而不是使用記錄深入解析。建立類似下列內容的規則。

```
{
    "AggregateOn": "Count",
    "Contribution": {
        "Filters": [
            {
                "Match": "$.activity-type",
                "In": [
                    "AUTH_FAILURE"
                ]
            }
        ],
        "Keys": [
            "$.user"
        ]
    },
    "LogFormat": "JSON",
    "Schema": {
        "Name": "CloudWatchLogRule",
        "Version": 1
    },
    "LogGroupARNs": [
        "arn:aws:logs:us-east-1:999999999999:log-group:/customer/structured_logs"
    ]
}
```

檢視開啟檔案的記錄項目

在結構化記錄檔中，檔案讀取記錄項目看起來類似下列內容：

```
{
  "mode":"READ",
  "path":"/fs-0df669c89d9bf7f45/avtester/example",
  "activity-type":"OPEN",
  "resource-arn":"arn:aws:transfer:us-east-1:999999999999:server/s-0123456789abcdef",
  "session-id":"0049cd844c7536c06a89"
}
```

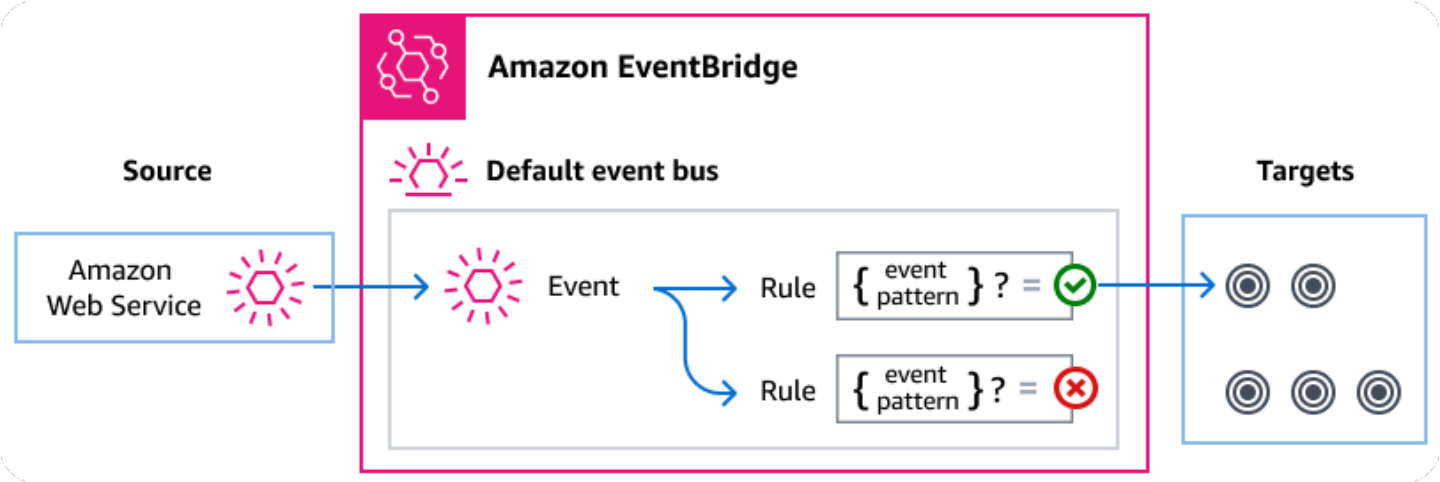
執行下列查詢以檢視指出檔案已開啟的記錄項目。

```
filter `activity-type` = 'OPEN'
| display @timestamp, @logStream, `session-id`, mode, path
```

使用管理 Transfer Family 事件 Amazon EventBridge

Amazon EventBridge 是一種使用事件將應用程式元件連接在一起的無伺服器服務，可讓您更輕鬆地建置可擴充的事件驅動應用程式。事件驅動架構是一種構建鬆散耦合的軟件系統的風格，該軟件系統通過發出和響應事件來協同工作。事件代表資源或環境中的變化。

與許多 AWS 服務一樣， Transfer Family 會產生事件並將其傳送至 EventBridge 預設事件匯流排。請注意，預設事件匯流排會在每個 AWS 帳戶中自動佈建。事件匯流排是接收事件，並將事件傳遞至零個或多個目的地或目標的路由器。您可以為事件匯流排指定規則，以便在事件到達時評估事件。每個規則都會檢查事件是否符合規則的事件模式。如果事件相符，則事件匯流排會將事件傳送至一或多個指定的目標。



主題

- Transfer Family 事件
- 使用 EventBridge 規則傳送 Transfer Family 事件
- Amazon EventBridge 權限
- 其他 EventBridge 資源
- Transfer Family 事件詳細參考

Transfer Family 事件

Transfer Family 會自動將事件傳送至預設 EventBridge 事件匯流排。您可以在事件匯流排上建立規則，其中每個規則都包含事件模式和一或多個目標。符合規則事件模式的事件會以最佳方式傳遞至指定目標，但是某些事件可能會按順序傳送。

下列事件由產生 Transfer Family。若要取得更多資訊，請參閱《Amazon EventBridge 使用指南》中的EventBridge 事件。

SFTP、FTP 伺服器和 FTP 伺服器事件

事件明細類型	描述
FTP 檔案伺服器下載完成	已成功下載 FTP 通訊協定的檔案。
FTP 檔案伺服器下載失敗	FTP 通訊協定的嘗試下載檔案失敗。
FTP 檔案伺服器上傳完成	FTP 通訊協定的檔案已成功上傳。
FTP 檔案伺服器上傳失敗	FTP 通訊協定的嘗試上傳檔案失敗。
FTPS 檔案伺服器下載完成	已成功下載 FTPS 通訊協定的檔案。
FTPS 檔案伺服器下載失敗	FTPS 通訊協定的嘗試下載檔案失敗。
FTPS 檔案伺服器上傳完成	已成功上傳 FTPS 通訊協定的檔案。
FTPS 檔案伺服器上傳失敗	FTPS 通訊協定的嘗試上傳檔案失敗。
SFTP 伺服器檔案下載完成	SFTP 通訊協定的檔案已成功下載。
SFTP 伺服器檔案下載失敗	SFTP 通訊協定的嘗試下載檔案失敗。
SFTP 伺服器檔案上傳完成	SFTP 通訊協定的檔案已成功上傳。
SFTP 伺服器檔案上傳失敗	SFTP 通訊協定的嘗試上傳檔案失敗。

SFTP 連接器事件

事件明細類型	描述
SFTP 連接器檔案傳送完成	從連接器到遠端 SFTP 伺服器的檔案傳輸已成功完成。
SFTP 連接器檔案傳送失敗	從連接器到遠端 SFTP 伺服器的檔案傳輸失敗。
SFTP 連接器檔案擷取完成	從遠端 SFTP 伺服器到連接器的檔案傳輸已成功完成。

事件明細類型	描述
SFTP 連接器檔案擷取失敗	從遠端 SFTP 伺服器到連接器的檔案傳輸失敗。
SFTP 連接器目錄清單已完成	已成功完成的開始檔案目錄列出呼叫。
SFTP 連接器目錄清單失敗	失敗的起始檔案目錄清單。

A2S 活動

事件明細類型	描述
AS2 承載接收已完成	已收到 AS2 訊息的裝載。
AS2 裝載接收失敗	尚未收到 AS2 訊息的裝載。
AS2 承載傳送完成	AS2 訊息的裝載已成功傳送。
AS2 裝載傳送失敗	AS2 訊息的裝載無法傳送。
AS2 MDN 接收完成	已收到 AS2 訊息的訊息配置通知。
AS2 MDN 接收失敗	尚未收到 AS2 訊息的郵件配置通知。
MDN 傳送完成	AS2 訊息的郵件配置通知已成功傳送。
AS2 MDN 傳送失敗	AS2 郵件的郵件配置通知無法傳送。

使用 EventBridge 規則傳送 Transfer Family 事件

如果您希望 EventBridge 預設事件匯流排將 Transfer Family 事件傳送至目標，則必須建立包含與所需 Transfer Family 事件中資料相符的事件模式的規則。

您可以依照下列一般步驟建立規則：

1. 為指定下列項目的規則建立事件模式：
   - Transfer Family 是規則評估的事件來源。
   - (選擇性) 任何其他要比對的事件資料。

如需詳細資訊，請參閱 ???。

2. (選擇性) 建立輸入轉換器，在將資訊 EventBridge 傳送至規則目標之前自訂事件中的資料。

   如需詳細資訊，請參閱《EventBridge 使用指南》中的〈輸入轉換〉。

3. 指定您要 EventBridge 傳遞符合事件模式之事件的目標。

   目標可以是其他 AWS 服務、軟體即服務 (SaaS) 應用程式、API 目標或其他自訂端點。如需詳細資訊，請參閱《EventBridge 使用者指南》中的目標。

如需建立事件匯流排規則的完整指示，請參閱《使用指南》中的〈建立對事件做出反應的規則EventBridge 〉。

建立事件的 Transfer Family 事件模式

將事件傳 Transfer Family 遞至預設事件匯流排時， EventBridge 會使用為每個規則定義的事件模式來決定是否應將事件傳遞至規則的目標。事件模式匹配所需 Transfer Family 事件中的數據。每個事件模式都是包含下列項目的 JSON 物件：

- 識別傳送事件之服務的 `source` 屬性。對於 Transfer Family 事件，來源是`aws.transfer`。
- (選擇`detail-type`性) 包含要比對之事件類型陣列的屬性。
- (選擇`detail`性) 包含要比對的任何其他事件資料的屬性。

例如，下列事件模式會比對來自下列所有事件 Transfer Family：

```
{
  "source": ["aws.transfer"]
}
```

下列事件模式範例符合所有 SFTP 連接器事件：

```
{
  "source": ["aws.transfer"],
  "detail-type": ["SFTP Connector File Send Completed", "SFTP Connector File Retrieve
 Completed",
                  "SFTP Connector File Retrieve Failed", "SFTP Connector File Send
 Failed"]
}
```

下列事件模式範例符合所有「Transfer Family」失敗事件：

```
{
  "source": ["aws.transfer"],
  "detail-type": [{"wildcard", "*Failed"}]
}
```

下列事件模式範例與使用者使用者##的 SFTP 下載成功相符：

```
{
  "source": ["aws.transfer"],
  "detail-type": ["SFTP Server File Download Completed"],
  "detail": {
    "username": [username]
  }
}
```

如需撰寫事件模式的詳細資訊，請參閱EventBridge 使用指南中的事件模式。

測試 Transfer Family 事件模式 EventBridge

您可以使用 S EventBridge andbox 快速定義和測試事件模式，而無需完成更廣泛的建立或編輯規則程序。您可以使用 Sandbox 定義事件模式，並使用範例事件來確認模式是否符合所需的事件。EventBridge 提供您直接從沙箱中使用該事件模式來建立新規則的選項。

如需詳細資訊，請參閱使用指南中的使用 EventBridge 沙箱測試事件模式。EventBridge

Amazon EventBridge 權限

Transfer Family 不需要任何其他權限即可將事件傳遞給 Amazon EventBridge。

您指定的目標可能需要特定的權限或組態。如需有關針對目標使用特定服務的詳細資訊，請參閱《使Amazon EventBridge 用指南》中的Amazon EventBridge 目標。

其他 EventBridge 資源

如需有關如何使Amazon EventBridge 用處理和管理事件的詳細資訊，請參閱《使 EventBridge 用指南》中的下列主題。

- 如需事件匯流排如何運作的詳細資訊，請參閱Amazon EventBridge 事件匯流排。

- 如需有關事件結構的資訊，請參閱事件。
- 如需建構事件模式以便在符合規則時 EventBridge 使用的相關資訊，請參閱事件模式。
- 如需建立規則以指定 EventBridge 處理哪些事件的相關資訊，請參閱規則。
- 如需如何指定 EventBridge 將相符事件傳送至哪些服務或其他目的地的資訊，請參閱目標。

Transfer Family 事件詳細參考

來自 AWS 服務的所有事件都有一組共同的欄位，其中包含有關事件的中繼資料。這些中繼資料可以包含做為事件來源的 AWS 服務、產生事件的時間、事件發生的帳戶和地區，以及其他服務。如需這些一般欄位的定義，請參閱《Amazon EventBridge 使用指南》中的「事件結構參考」。

此外，每個事件都有一個 `detail` 欄位，其中包含該特定事件的特定資料。下面的參考定義了各種 Transfer Family 事件的詳細信息字段。

當您使用 EventBridge 來選取和管理 Transfer Family 事件時，請考慮下列事項：

- 所有來源事件的`source`欄位 Transfer Family 都設定為`aws.transfer`。
- `detail-type` 欄位指定事件類型。

  例如 `FTP File Server Download Completed`。
- `detail` 欄位包含該特定事件的特定資料。

如需有關建構啟用規則以符合 Transfer Family 事件的事件模式的資訊，請參閱《Amazon EventBridge 使用指南》中的事件模式。

如需有關事件及其 EventBridge 處理方式的詳細資訊，請參閱《Amazon EventBridge 使用指南》中的Amazon EventBridge 事件。

主題

- SFTP、FTP 伺服器和 FTP 伺服器事件
- SFTP 連接器事件
- 澳大事件

SFTP、FTP 伺服器和 FTP 伺服器事件

以下是 SFTP、FTPS 和 FTP 伺服器事件的詳細資料欄位：

- FTP 檔案伺服器下載完成
- FTP 檔案伺服器下載失敗
- FTP 檔案伺服器上傳完成
- FTP 檔案伺服器上傳失敗
- FTPS 檔案伺服器下載完成
- FTPS 檔案伺服器下載失敗
- FTPS 檔案伺服器上傳完成
- FTPS 檔案伺服器上傳失敗
- SFTP 伺服器檔案下載完成
- SFTP 伺服器檔案下載失敗
- SFTP 伺服器檔案上傳完成
- SFTP 伺服器檔案上傳失敗

`source`和`detail-type`欄位包含在下方，因為它們包含 Transfer Family 事件的特定值。如需所有事件中包含的其他中繼資料欄位的定義，請參閱《Amazon EventBridge 使用指南》中的「事件結構參考」。

```
{
  . . .,
  "detail-type": "string",
  "source": "aws.transfer",
  . . .,
  "detail": {
    "failure-code" : "string",
    "status-code" : "string",
    "protocol" : "string",
    "bytes" : "number",
    "client-ip" : "string",
    "failure-message" : "string",
    "end-timestamp" : "string",
    "etag" : "string",
    "file-path" : "string",
    "server-id" : "string",
    "username" : "string",
    "session-id" : "string",
    "start-timestamp" : "string"
  }
```

```
}
```

`detail-type`

識別事件的類型。

對於此事件，值是先前列出的其中一個 SFTP、FTPS 或 FTP 伺服器事件名稱。

`source`

識別產生事件的服務。對於「Transfer Family」事件，此值為`aws.transfer`。

`detail`

包含事件相關資訊的 JSON 物件。產生事件的服務會決定此欄位的內容。

對於此事件，資料包括下列項目：

`failure-code`

轉移失敗原因的類別。數值: `PARTIAL_UPLOAD` | `PARTIAL_DOWNLOAD` | `UNKNOWN_ERROR`

`status-code`

轉移是否成功。價值觀：`COMPLETED` | `FAILED`。

`protocol`

用於傳輸的通訊協定。數值: `SFTP` | `FTPS` | `FTP`

`bytes`

已傳輸的位元組數目。

`client-ip`

轉移所涉及之用戶端的 IP 位址

`failure-message`

如果是轉移失敗，請參閱轉移失敗原因的詳細資料。

`end-timestamp`

對於成功的傳輸，檔案處理完成時的時間戳記。

`etag`

實體標籤 (僅用於 Amazon S3 檔案)。

`file-path`

要傳輸之檔案的路徑。

`server-id`

Transfer Family 伺服器的唯一 ID。

`username`

正在執行移轉的使用者。

`session-id`

移轉工作階段的唯一識別碼。

`start-timestamp`

對於成功的傳輸，檔案處理開始時的時間戳記。

Example SFTP 伺服器檔案下載失敗範例事件

下列範例顯示 SFTP 伺服器上下載失敗的事件 (即使Amazon EFS 用的儲存空間)。

```
{
    "version": "0",
    "id": "event-ID",
    "detail-type": "SFTP Server File Download Failed",
    "source": "aws.transfer",
    "account": "958412138249",
    "time": "2024-01-29T17:20:27Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:transfer:us-east-1:958412138249:server/s-1234abcd5678efghi"
    ],
    "detail": {
        "failure-code": "PARTIAL_DOWNLOAD",
        "status-code": "FAILED",
        "protocol": "SFTP",
        "bytes": 4100,
        "client-ip": "IP-address",
        "failure-message": "File was partially downloaded.",
        "end-timestamp": "2024-01-29T17:20:27.749749117Z",
        "file-path": "/fs-1234abcd5678efghi/user0/test-file",
        "server-id": "s-1234abcd5678efghi",
```

```
        "username": "test",
        "session-id": "session-ID",
        "start-timestamp": "2024-01-29T17:20:16.706282454Z"
    }
}
```

Example FTP 檔案伺服器上傳完成範例事件

下列範例顯示在 FTP 伺服器上成功完成上載的事件 (Amazon S3 即使用的儲存空間)。

```
{
    "version": "0",
    "id": "event-ID",
    "detail-type": "FTP Server File Upload Completed",
    "source": "aws.transfer",
    "account": "958412138249",
    "time": "2024-01-29T16:31:43Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:transfer:us-east-1:958412138249:server/s-1111aaaa2222bbbb3"
    ],
    "detail": {
        "status-code": "COMPLETED",
        "protocol": "FTP",
        "bytes": 1048576,
        "client-ip": "10.0.0.141",
        "end-timestamp": "2024-01-29T16:31:43.311866408Z",
        "etag": "b6d81b360a5672d80c27430f39153e2c",
        "file-path": "/DOC-EXAMPLE-BUCKET/test/1mb_file",
        "server-id": "s-1111aaaa2222bbbb3",
        "username": "test",
        "session-id": "event-ID",
        "start-timestamp": "2024-01-29T16:31:42.462088327Z"
    }
}
```

SFTP 連接器事件

以下是 SFTP 連接器事件的詳細資料欄位：

- SFTP 連接器檔案傳送完成
- SFTP 連接器檔案傳送失敗

- SFTP 連接器檔案擷取完成
- SFTP 連接器檔案擷取失敗
- SFTP 連接器目錄清單已完成
- SFTP 連接器目錄清單失敗

`source`和`detail-type`欄位包含在下方，因為它們包含 Transfer Family 事件的特定值。如需所有事件中包含的其他中繼資料欄位的定義，請參閱《Amazon EventBridge 使用指南》中的「事件結構參考」。

```
{
  . . .,
  "detail-type": "string",
  "source": "aws.transfer",
  . . .,
  "detail": {
    "operation" : "string",
    "max-items" : "number",
    "connector-id" : "string",
    "output-directory-path" : "string",
    "listing-id" : "string",
    "transfer-id" : "string",
    "file-transfer-id" : "string",
    "url" : "string",
    "file-path" : "string",
    "status-code" : "string",
    "failure-code" : "string",
    "failure-message" : "string",
    "start-timestamp" : "string",
    "end-timestamp" : "string",
    "local-directory-path" : "string",
    "remote-directory-path" : "string"
    "item-count" : "number"
    "truncated" : "boolean"
    "bytes" : "number",
    "local-file-location" : {
      "domain" : "string",
      "bucket" : "string",
      "key" : "string"
    },
    "output-file-location" : {
      "domain" : "string",
```

```
      "bucket" : "string",
      "key" : "string"
    }
  }
}
```

`detail-type`

識別事件的類型。

對於此事件，值是先前列出的其中一個 SFTP 連接器事件名稱。

`source`

識別產生事件的服務。對於 Transfer Family 事件，此值為`aws.transfer`。

`detail`

包含事件相關資訊的 JSON 物件。產生事件的服務會決定此欄位的內容。

對於此事件，資料包括下列項目：

`max-items`

要返回的目錄/文件名的最大數量。

`operation`

`StartFileTransfer`請求是否正在發送或檢索文件。價值觀：`SEND|RETRIEVE`。

`connector-id`

所使用之 SFTP 連接器的唯一識別碼。

`output-directory-path`

Amazon S3 中用來存放檔案/目錄清單結果的路徑 (儲存貯體和前置詞)。

`listing-id`

`StartDirectoryListing`API 呼叫的唯一識別碼。此識別碼可用於檢查 CloudWatch 記錄，以查看刊登要求的狀態。

`transfer-id`

移轉事件的唯一識別碼 (`StartFileTransfer`要求)。

`file-transfer-id`

要傳輸之檔案的唯一識別碼。

`url`

合作夥伴的 AS2 或 SFTP 端點的網址。

`file-path`

要傳送或擷取的位置和檔案。

`status-code`

轉移是否成功。價值觀：`FAILED | COMPLETED`。

`failure-code`

如果是轉移失敗，轉移失敗的原因代碼。

`failure-message`

如果是轉移失敗，請參閱轉移失敗原因的詳細資料。

`start-timestamp`

對於成功的傳輸，檔案處理開始時的時間戳記。

`end-timestamp`

如果是成功傳輸，則為檔案處理完成時的時間戳記。

`local-directory-path`

若為RETRIEVE請求，則為放置擷取檔案的位置。

`remote-directory-path`

若為SEND要求，則為將檔案放置在夥伴 SFTP 伺服器上的檔案目錄。這是傳遞給請StartFileTransfer求RemoteDirectoryPath的用戶的值。您可以在夥伴的 SFTP 伺服器上指定預設目錄。如果是這樣，則此字段為空。

`item-count`

針對刊登要求傳回的項目 (目錄和檔案) 數目。

`truncated`

列表輸出是否包含遠程目錄中包含的所有項目。

bytes

正在傳輸的字節數。傳輸失敗的值為 0。

local-file-location

此參數包含 AWS 儲存檔案位置的詳細資訊。

domain

正在使用的存儲。目前，唯一的值是S3。

bucket

Amazon S3 中對象的容器。

key

在 Amazon S3 中指派給物件的名稱。

output-file-location

此參數包含在 AWS 儲存體中儲存目錄清單結果的位置詳細資訊。

domain

正在使用的存儲。目前，唯一的值是S3。

bucket

Amazon S3 中對象的容器。

key

在 Amazon S3 中指派給物件的名稱。

Example SFTP 連接器檔案傳送失敗範例事件

下列範例顯示 SFTP 連接器在嘗試傳送檔案至遠端 SFTP 伺服器時失敗的事件。

```
{
    "version": "0",
    "id": "event-ID",
    "detail-type": "SFTP Connector File Send Failed",
    "source": "aws.transfer",
    "account": "123456789012",
    "time": "2024-01-24T19:30:45Z",
```

```
    "region": "us-east-1",
    "resources": [
        "arn:aws:transfer:us-east-1:123456789012:connector/c-f1111aaaa2222bbbb3"
    ],
    "detail": {
        "operation": "SEND",
        "connector-id": "c-f1111aaaa2222bbbb3",
        "transfer-id": "transfer-ID",
        "file-transfer-id": "file-transfer-ID",
        "url": "sftp://s-21a23456789012a.server.transfer.us-east-1.amazonaws.com",
        "file-path": "/DOC-EXAMPLE-BUCKET/testfile.txt",
        "status-code": "FAILED",
        "failure-code": "CONNECTION_ERROR",
        "failure-message": "Unknown Host",
        "remote-directory-path": "",
        "bytes": 0,
        "start-timestamp": "2024-01-24T18:29:33.658729Z",
        "end-timestamp": "2024-01-24T18:29:33.993196Z",
        "local-file-location": {
            "domain": "S3",
            "bucket": "DOC-EXAMPLE-BUCKET",
            "key": "testfile.txt"
        }
    }
}
```

Example SFTP 連接器檔案擷取已完成範例事件

下列範例顯示 SFTP 連接器成功擷取從遠端 SFTP 伺服器傳送之檔案的事件。

```
{
    "version": "0",
    "id": "event-ID",
    "detail-type": "SFTP Connector File Retrieve Completed",
    "source": "aws.transfer",
    "account": "123456789012",
    "time": "2024-01-24T18:28:08Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:transfer:us-east-1:123456789012:connector/c-f1111aaaa2222bbbb3"
    ],
    "detail": {
        "operation": "RETRIEVE",
        "connector-id": "c-fc68000012345aa18",
```

```
        "transfer-id": "file-transfer-ID",
        "file-transfer-id": "file-transfer-ID",
        "url": "sftp://s-21a23456789012a.server.transfer.us-east-1.amazonaws.com",
        "file-path": "testfile.txt",
        "status-code": "COMPLETED",
        "local-directory-path": "/DOC-EXAMPLE-BUCKET",
        "bytes": 63533,
        "start-timestamp": "2024-01-24T18:28:07.632388Z",
        "end-timestamp": "2024-01-24T18:28:07.774898Z",
        "local-file-location": {
            "domain": "S3",
            "bucket": "DOC-EXAMPLE-BUCKET",
            "key": "testfile.txt"
        }
    }
}
```

Example SFTP 連接器目錄清單已完成範例事件

下列範例顯示一個事件，其中開始目錄清單呼叫從遠端 SFTP 伺服器擷取清單檔案。

```
{
    "version": "0",
    "id": "event-ID",
    "detail-type": "SFTP Connector Directory Listing Completed",
    "source": "aws.transfer",
    "account": "123456789012",
    "time": "2024-01-24T18:28:08Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:transfer:us-east-1:123456789012:connector/c-f1111aaaa2222bbbb3"
    ],
    "detail": {
        "max-items": 10000,
        "connector-id": "c-fc68000012345aa18",
        "output-directory-path": "/DOC-EXAMPLE-BUCKET/example/file-listing-output",
        "listing-id": "123456-23aa-7980-abc1-1a2b3c4d5e",
        "url": "sftp://s-21a23456789012a.server.transfer.us-east-1.amazonaws.com",

        "status-code": "COMPLETED",
        "remote-directory-path": "/home",
        "item-count": 10000,
        "truncated": true,
        "start-timestamp": "2024-01-24T18:28:07.632388Z",
```

```
        "end-timestamp": "2024-01-24T18:28:07.774898Z",
        "output-file-location": {
            "domain": "S3",
            "bucket": "DOC-EXAMPLE-BUCKET",
            "key": "c-fc1ab90fd0d047e7a-70987273-49nn-4006-bab1-1a7290cc412ba.json"
        }
    }
}
```

澳大事件

以下是 AS2 事件的詳細資訊欄位：

- AS2 承載接收已完成
- AS2 裝載接收失敗
- AS2 承載傳送完成
- AS2 裝載傳送失敗
- AS2 MDN 接收完成
- AS2 MDN 接收失敗
- MDN 傳送完成
- AS2 MDN 傳送失敗

`source`和`detail-type`欄位包含在下方，因為它們包含 Transfer Family 事件的特定值。如需所有事件中包含的其他中繼資料欄位的定義，請參閱《Amazon EventBridge 使用指南》中的「事件結構參考」。

```
{
   . . .,
  "detail-type": "string",
  "source": "aws.transfer",
  . . .,
  "detail": {
    "s3-attributes" : {
      "file-bucket" : "string",
      "file-key" : "string",
      "json-bucket" : "string",
      "json-key" : "string",
      "mdn-bucket" : "string",
      "mdn-key" : "string"
```

```
      }
    "mdn-subject" : "string",
    "mdn-message-id" : "string",
    "disposition" : "string",
    "bytes" : "number",
    "as2-from" : "string",
    "as2-message-id" : "string",
    "as2-to" : "string",
    "connector-id" : "string",
    "client-ip" : "string",
    "agreement-id" : "string",
    "server-id" : "string",
    "requester-file-name" : "string",
    "message-subject" : "string",
    "start-timestamp" : "string",
    "end-timestamp" : "string",
    "status-code" : "string",
    "failure-code" : "string",
    "failure-message" : "string",
    "transfer-id" : "string"
  }
}
```

`detail-type`

識別事件的類型。

對於此事件，值是先前列出的其中一個 AS2 事件。

`source`

識別產生事件的服務。對於 Transfer Family 事件，此值為`aws.transfer`。

`detail`

包含事件相關資訊的 JSON 物件。產生事件的服務會決定此欄位的內容。

`s3-attributes`

識別要傳輸之檔案的 Amazon S3 儲存貯體和金鑰。對於 MDN 事件，它還可以識別 MDN 文件的存儲桶和密鑰。

`file-bucket`

Amazon S3 中對象的容器。

`file-key`

在 Amazon S3 中指派給物件的名稱。

`json-bucket`

對於「已完成」或「失敗」傳輸，則為 JSON 檔案的容器。

`json-key`

對於已完成或失敗的傳輸，指派給 Amazon S3 中 JSON 檔案的名稱。

`mdn-bucket`

MDN 事件是 MDN 檔案的容器。

`mdn-key`

對於 MDN 事件，指派給 Amazon S3 中 MDN 檔案的名稱。

`mdn-subject`

對於 MDN 事件，郵件配置的文字說明。

`mdn-message-id`

MDN 事件是 MDN 訊息的唯一識別碼。

`disposition`

針對 MDN 事件，則為處理方式的類別。

`bytes`

訊息中的位元組數。

`as2-from`

傳送訊息的 AS2 交易夥伴。

`as2-message-id`

要傳輸之 AS2 訊息的唯一識別碼。

`as2-to`

接收訊息的 AS2 交易夥伴。

`connector-id`

對於從轉移系列伺服器傳送至交易夥伴的 AS2 訊息，則為所使用 AS2 連接器的唯一識別碼。

`client-ip`

對於伺服器事件 (從交易夥伴轉移到「Transfer Family」伺服器)，轉移過程中涉及的用戶端 IP 位址。

`agreement-id`

對於伺服器事件，AS2 合約的唯一識別碼。

`server-id`

對於伺服器事件，僅適用於「Transfer Family」伺服器的唯一 ID。

`requester-file-name`

對於有效負載事件，則為傳輸期間接收到的檔案的原始名稱。

`message-subject`

郵件主旨的文字說明。

`start-timestamp`

對於成功的傳輸，檔案處理開始時的時間戳記。

`end-timestamp`

如果是成功傳輸，則為檔案處理完成時的時間戳記。

`status-code`

對應至 AS2 郵件傳輸程序狀態的程式碼。有效值：`COMPLETED | FAILED | PROCESSING`。

`failure-code`

對於失敗的轉移，為什麼轉移失敗的類別。

`failure-message`

如果是轉移失敗，請參閱轉移失敗原因的詳細資料。

`transfer-id`

移轉事件的唯一識別碼。

Example AS2 裝載接收已完成範例事件

```
{
    "version": "0",
     "id": "event-ID",
    "detail-type": "AS2 Payload Receive Completed",
    "source": "aws.transfer",
    "account": "076722215406",
    "time": "2024-02-07T06:47:05Z",
    "region": "us-east-1",
    "resources": ["arn:aws:transfer:us-east-1:076722215406:connector/
c-1111aaaa2222bbbb3"],
    "detail": {
        "s3-attributes": {
            "file-key": "/inbound/processed/testAs2Message.dat",
            "file-bucket": "DOC-EXAMPLE-BUCKET"
        },
        "client-ip": "client-IP-address",
        "requester-file-name": "testAs2MessageVerifyFile.dat",
        "end-timestamp": "2024-02-07T06:47:06.040031Z",
        "as2-from": "as2-from-ID",
        "as2-message-id": "as2-message-ID",
        "message-subject": "Message from AS2 tests",
        "start-timestamp": "2024-02-07T06:47:05.410Z",
        "status-code": "PROCESSING",
        "bytes": 63,
        "as2-to": "as2-to-ID",
        "agreement-id": "a-1111aaaa2222bbbb3",
        "server-id": "s-1234abcd5678efghi"
    }
}
```

Example AS2 MDN 接收失敗的範例事件

```
{
  "version": "0",
  "id": "event-ID",
  "detail-type": "AS2 MDN Receive Failed",
  "source": "aws.transfer",
  "account": "889901007463",
  "time": "2024-02-06T22:05:09Z",
  "region": "us-east-1",
  "resources": ["arn:aws:transfer:us-east-1:076722215406:server/s-1111aaaa2222bbbb3"],
```

```
  "detail": {
      "mdn-subject": "Your Requested MDN Response re: Test run from Id 123456789abcde
 to partner ijklmnop987654",
      "s3-attributes": {
          "json-bucket": "DOC-EXAMPLE-BUCKET1",
          "file-key": "/as2Integ/TestOutboundWrongCert.dat",
          "file-bucket": "DOC-EXAMPLE-BUCKET2",
          "json-key": "/as2Integ/failed/TestOutboundWrongCert.dat.json"
      },
      "mdn-message-id": "MDN-message-ID",
      "end-timestamp": "2024-02-06T22:05:09.479878Z",
      "as2-from": "PartnerA",
      "as2-message-id": "as2-message-ID",
      "connector-id": "c-1234abcd5678efghj",
      "message-subject": "Test run from Id 123456789abcde to partner ijklmnop987654",
      "start-timestamp": "2024-02-06T22:05:03Z",
      "failure-code": "VERIFICATION_FAILED_NO_MATCHING_KEY_FOUND",
      "status-code": "FAILED",
      "as2-to": "MyCompany",
      "failure-message": "No public certificate matching message signature could be
 found in profile: p-1234abcd5678efghj",
      "transfer-id": "transfer-ID"
  }
}
```

中的安全性 AWS Transfer Family

雲安全 AWS 是最高的優先級。身為 AWS 客戶，您可以從資料中心和網路架構中獲益，該架構專為滿足對安全性最敏感的組織的需求而打造。

安全是 AWS 與您之間共同的責任。共同責任模型 將此描述為雲端的安全和雲端內的安全：

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。

本文件可協助您瞭解如何在使用時套用共同責任模型 AWS Transfer Family。下列主題說明如何設定 AWS Transfer Family 以符合安全性與合規性目標。您還將學習如何使用其他 AWS 服務來幫助您監控和保護您的 AWS Transfer Family 資源。

我們提供了一個研討會，提供規範指導，並提供實驗室，讓您無需修改現有應用程式或管理伺服器基礎架構 AWS 即可建置可擴充且安全的檔案傳輸架構。您可以在此處查看此工作坊的詳細信息。

主題

- AWS Transfer Family 伺服器的安全性原則
- AWS Transfer Family SFTP 連接器的安全性原則
- 使用混合式後量子金鑰交換 AWS Transfer Family
- 資料保護 AWS Transfer Family
- 的身分識別與存取管理 AWS Transfer Family
- 符合性驗證 AWS Transfer Family
- 韌性在 AWS Transfer Family
- 基礎結構安全 AWS Transfer Family
- 新增 Web 應用程式防火牆
- 預防跨服務混淆代理人
- AWSAWS Transfer Family 的受管理政策

AWS Transfer Family 伺服器的安全性原則

中的伺服器安全性原則可 AWS Transfer Family 讓您限制與伺服器相關聯的一組加密演算法 (訊息驗證碼 (MAC)、金鑰交換 (KEX) 和密碼套件)。如需支援的加密演算法清單，請參閱加密算法。如需與伺服器主機金鑰和服務管理的使用者金鑰搭配使用的支援金鑰演算法清單，請參閱支援的使用者和伺服器金鑰演算法。

> **Note**
>
> 我們強烈建議您將伺服器更新為我們最新的安全政策。我們最新的安全性原則為預設值。任何使用 CloudFormation並接受預設安全性原則建立 Transfer Family 伺服器的客戶，都會自動指

派最新策略。如果您擔心客戶端的兼容性，請確認說明您在創建或更新服務器時希望使用哪種安全策略，而不是使用默認策略，這可能會更改。
若要變更伺服器的安全性原則，請參閱編輯安全性原則。

如需 Transfer Family 中安全性的詳細資訊，請參閱部落格文章：Transfer Family 如何協助您建置安全、合規的受管理檔案傳輸解決方案。

主題

- 加密算法
- TransferSecurity政策
- TransferSecurity政策
- TransferSecurity政策
- TransferSecurity政策
- TransferSecurity政策
- TransferSecurity政策-通信 -2024-01 /政策-FIPS-2024-05 TransferSecurity
- TransferSecurity政策-火災
- TransferSecurity政策-五
- 後量子安全性原則

Note

TransferSecurityPolicy-2024-01是使用主控台、API 或 CLI 建立伺服器時，附加到伺服器的預設安全性原則。

加密算法

對於主機金鑰，我們支援下列演算法：

- rsa-sha2-256
- rsa-sha2-512
- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384

- ecdsa-sha2-nistp521
- ssh-ed25519

此外，下列安全性原則允許ssh-rsa：

- TransferSecurity政策
- TransferSecurity政策
- TransferSecurity政策-五
- TransferSecurity政策-火災
- TransferSecurity政策-FIPS-2024-01
- TransferSecurity政策-SSH-菲普斯-實驗 -2023-04

> **Note**
>
> 請務必瞭解 RSA 金鑰類型 (永遠ssh-rsa是) 和 RSA 主機金鑰演算法 (可以是任何支援的演算法) 之間的區別。

以下是每個安全性原則所支援的密碼編譯演算法清單。

> **Note**
>
> 在下表和原則中，請注意下列演算法類型的使用方式。
>
> - SFTP 伺服器僅使用、和SshMacs區段SshCiphers中SshKexs的演算法。
> - FTPS 伺服器僅使用TlsCiphers本節中的演算法。
> - FTP 伺服器不使用加密，因此請勿使用任何這些演算法。
> - FIPS-2024-05 和 FIPS-2024-01 安全性原則是相同的，不同的是 FIPS-2024-05 不支援ssh-rsa演算法。

安全政策	2024-01	2023-05	2022-03	2020-06	FIPS-2024-05 FIPS-2024-01	菲的同位	飛行器	2018-11
SshCiphers								
中心	♦			♦	♦		♦	♦
aes128-gcm@openssh.com	♦	♦	♦	♦	♦	♦	♦	♦
中心	♦	♦	♦	♦	♦	♦	♦	♦
中心	♦	♦	♦	♦	♦	♦	♦	♦
aes256-gcm@openssh.com	♦	♦	♦	♦	♦	♦	♦	♦
chacha20-poly1305@openssh.com				♦				♦
SshKexs								
曲線	♦	♦	♦					♦
curve25519-sha256@libssh.org	♦	♦	♦					♦

安全政策	2024-01	2023-05	2022-03	2020-06	FIPS-2024-05 FIPS-2024-01	菲的同位	飛行器	2018-11
迪菲-赫尔曼集团								♦
迪菲-赫尔曼集团				♦			♦	♦
迪菲-赫尔曼集团	♦	♦	♦	♦	♦	♦	♦	♦
迪菲-赫尔曼集团	♦	♦	♦	♦	♦	♦	♦	♦
迪菲-赫爾曼組-交換-sha256		♦	♦	♦		♦	♦	♦
ecdh-nist p256-kyber-512r3-sha256-d00 @openquantumsafe.org	♦				♦			

安全政策	2024-01	2023-05	2022-03	2020-06	FIPS-2024-05 FIPS-2024-01	菲的同位	飛行器	2018-11
ecdh-nist p384-kyber-768r3-sha384-d00 @openquantumsafe.org	♦				♦			
ecdh-nist p521-kyber-1024r3-sha512-d00@openquantumsafe.org	♦				♦			
埃克德什-沙 2-尼斯特 P256	♦			♦	♦		♦	♦
埃克德什-沙 2-尼斯特 P384	♦			♦	♦		♦	♦

安全政策	2024-01	2023-05	2022-03	2020-06	FIPS-2024-05 FIPS-2024-01	菲的同位	飛行器	2018-11
埃克德什-沙 2-尼斯特 P521	♦			♦	♦		♦	♦
x25519-kyber-512r3-sha256-d00@amazon.com	♦							
SshMacs								
哈馬克沙 1								♦
hmac-sha1-etm@openssh.com								♦
哈馬克沙 2-256			♦	♦			♦	♦

安全政策	2024-01	2023-05	2022-03	2020-06	FIPS-2024-05 FIPS-2024-01	菲的同位	飛行器	2018-11
hmac-sha2-256-etm@openssh.com	♦	♦	♦	♦	♦	♦	♦	♦
哈馬克沙2-512			♦	♦			♦	♦
hmac-sha2-512-etm@openssh.com	♦	♦	♦	♦	♦	♦	♦	♦
umac-128-etm@openssh.com				♦				♦
umac-128@openssh.com				♦				♦
umac-64-etm@openssh.com								♦

安全政策	2024-01	2023-05	2022-03	2020-06	FIPS-2024-05 FIPS-2024-01	菲的同位	飛行器	2018-11
umac-64@openssh.com								♦
TlsCiphers								
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256		♦	♦	♦	♦	♦	♦	♦
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256		♦	♦	♦	♦	♦	♦	♦
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384		♦	♦	♦	♦	♦	♦	♦
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384		♦	♦	♦	♦	♦	♦	♦

安全政策	2024-01	2023-05	2022-03	2020-06	FIPS-2024-05 FIPS-2024-01	菲的同位	飛行器	2018-11
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256		♦	♦	♦	♦	♦	♦	♦
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256		♦	♦	♦	♦	♦	♦	♦
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384		♦	♦	♦	♦	♦	♦	♦
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384		♦	♦	♦	♦	♦	♦	♦
TLS_RSA_WITH_AES_128_CBC_SHA256								♦

安全政策	2024-01	2023-05	2022-03	2020-06	FIPS-2024-05 FIPS-2024-01	菲的同位	飛行器	2018-11
TLS_RSA_WITH_AES_256_CBC_SHA256								◆

TransferSecurity政策

以下顯示了 TransferSecurityPolicy -2024-01 安全性原則。

```
{
    "SecurityPolicy": {
        "Fips": false,
        "SecurityPolicyName": "TransferSecurityPolicy-2024-01",
        "SshCiphers": [
            "aes128-gcm@openssh.com",
            "aes256-gcm@openssh.com",
            "aes128-ctr",
            "aes256-ctr",
            "aes192-ctr"
        ],
        "SshKexs": [
            "ecdh-nistp384-kyber-768r3-sha384-d00@openquantumsafe.org",
            "x25519-kyber-512r3-sha256-d00@amazon.com",
            "ecdh-nistp256-kyber-512r3-sha256-d00@openquantumsafe.org",
            "ecdh-nistp521-kyber-1024r3-sha512-d00@openquantumsafe.org",
            "ecdh-sha2-nistp256",
            "ecdh-sha2-nistp384",
            "ecdh-sha2-nistp521",
            "curve25519-sha256",
            "curve25519-sha256@libssh.org",
            "diffie-hellman-group18-sha512",
            "diffie-hellman-group16-sha512",
            "diffie-hellman-group-exchange-sha256"
        ],
        "SshMacs": [
```

```
            "hmac-sha2-256-etm@openssh.com",
            "hmac-sha2-512-etm@openssh.com"
        ],
        "TlsCiphers": [
            "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
            "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
            "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
            "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
            "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
            "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
            "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
            "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
        ]
    }
}
```

TransferSecurity政策

以下顯示了 TransferSecurityPolicy -2023-05 安全性原則。

```
{
    "SecurityPolicy": {
        "Fips": false,
        "SecurityPolicyName": "TransferSecurityPolicy-2023-05",
        "SshCiphers": [
            "aes256-gcm@openssh.com",
            "aes128-gcm@openssh.com",
            "aes256-ctr",
            "aes192-ctr"
        ],
        "SshKexs": [
            "curve25519-sha256",
            "curve25519-sha256@libssh.org",
            "diffie-hellman-group16-sha512",
            "diffie-hellman-group18-sha512",
            "diffie-hellman-group-exchange-sha256"
        ],
        "SshMacs": [
            "hmac-sha2-512-etm@openssh.com",
            "hmac-sha2-256-etm@openssh.com"
        ],
        "TlsCiphers": [
            "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
```

```
            "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
            "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
            "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
            "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
            "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
            "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
            "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
        ]
    }
}
```

TransferSecurity政策

以下顯示了 TransferSecurityPolicy -2022-03 安全性原則。

```
{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2022-03",
    "SshCiphers": [
      "aes256-gcm@openssh.com",
      "aes128-gcm@openssh.com",
      "aes256-ctr",
      "aes192-ctr"
    ],
    "SshKexs": [
      "curve25519-sha256",
      "curve25519-sha256@libssh.org",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group-exchange-sha256"
    ],
    "SshMacs": [
      "hmac-sha2-512-etm@openssh.com",
      "hmac-sha2-256-etm@openssh.com",
      "hmac-sha2-512",
      "hmac-sha2-256"
    ],
    "TlsCiphers": [
      "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
```

```
      "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
      "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
      "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
      "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ]
  }
}
```

TransferSecurity政策

下面顯示了 TransferSecurityPolicy -2020 年 06 月的安全性原則。

```
{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2020-06",
    "SshCiphers": [
      "chacha20-poly1305@openssh.com",
      "aes128-ctr",
      "aes192-ctr",
      "aes256-ctr",
      "aes128-gcm@openssh.com",
      "aes256-gcm@openssh.com"
    ],
    "SshKexs": [
      "ecdh-sha2-nistp256",
      "ecdh-sha2-nistp384",
      "ecdh-sha2-nistp521",
      "diffie-hellman-group-exchange-sha256",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group14-sha256"
    ],
    "SshMacs": [
      "umac-128-etm@openssh.com",
      "hmac-sha2-256-etm@openssh.com",
      "hmac-sha2-512-etm@openssh.com",
      "umac-128@openssh.com",
      "hmac-sha2-256",
      "hmac-sha2-512"
    ],
    "TlsCiphers": [
      "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
```

```
      "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
      "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
      "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
      "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
      "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ]
  }
}
```

TransferSecurity政策

下面顯示了 TransferSecurityPolicy -2018-11 安全性原則。

```
{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2018-11",
    "SshCiphers": [
      "chacha20-poly1305@openssh.com",
      "aes128-ctr",
      "aes192-ctr",
      "aes256-ctr",
      "aes128-gcm@openssh.com",
      "aes256-gcm@openssh.com"
    ],
    "SshKexs": [
      "curve25519-sha256",
      "curve25519-sha256@libssh.org",
      "ecdh-sha2-nistp256",
      "ecdh-sha2-nistp384",
      "ecdh-sha2-nistp521",
      "diffie-hellman-group-exchange-sha256",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group14-sha256",
      "diffie-hellman-group14-sha1"
    ],
    "SshMacs": [
      "umac-64-etm@openssh.com",
      "umac-128-etm@openssh.com",
      "hmac-sha2-256-etm@openssh.com",
```

```
      "hmac-sha2-512-etm@openssh.com",
      "hmac-sha1-etm@openssh.com",
      "umac-64@openssh.com",
      "umac-128@openssh.com",
      "hmac-sha2-256",
      "hmac-sha2-512",
      "hmac-sha1"
    ],
    "TlsCiphers": [
      "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
      "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
      "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
      "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
      "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384",
      "TLS_RSA_WITH_AES_128_CBC_SHA256",
      "TLS_RSA_WITH_AES_256_CBC_SHA256"
    ]
  }
}
```

TransferSecurity政策-通信 -2024-01 /政策-FIPS-2024-05 TransferSecurity

下面顯示了 TransferSecurityPolicy安全性原則。 TransferSecurityPolicy

> **Note**
>
> FIPS 服務端點以及 TransferSecurityPolicy安全性原則僅在某些 TransferSecurityPolicy地區提供。 AWS 如需詳細資訊，請參閱 AWS 一般參考 中的 AWS Transfer Family 端點和配額。這兩個安全策略之間的唯一區別是 TransferSecurityPolicy-FIPS-2024-01 支持該`ssh-rsa`算法，而-FIPS-2024-05 不支持。 TransferSecurityPolicy

```
{
    "SecurityPolicy": {
        "Fips": true,
        "SecurityPolicyName": "TransferSecurityPolicy-FIPS-2024-01",
        "SshCiphers": [
            "aes128-gcm@openssh.com",
```

```
            "aes256-gcm@openssh.com",
            "aes128-ctr",
            "aes256-ctr",
            "aes192-ctr"
        ],
        "SshKexs": [
            "ecdh-nistp384-kyber-768r3-sha384-d00@openquantumsafe.org",
            "ecdh-nistp256-kyber-512r3-sha256-d00@openquantumsafe.org",
            "ecdh-nistp521-kyber-1024r3-sha512-d00@openquantumsafe.org",
            "ecdh-sha2-nistp256",
            "ecdh-sha2-nistp384",
            "ecdh-sha2-nistp521",
            "diffie-hellman-group18-sha512",
            "diffie-hellman-group16-sha512",
            "diffie-hellman-group-exchange-sha256"
        ],
        "SshMacs": [
            "hmac-sha2-256-etm@openssh.com",
            "hmac-sha2-512-etm@openssh.com"
        ],
        "TlsCiphers": [
            "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
            "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
            "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
            "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
            "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
            "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
            "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
            "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
        ]
    }
}
```

TransferSecurity政策-火災

的 FIPS 認證詳細資訊可在 AWS Transfer Family 以下位置找到：https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search/all

下面顯示了 TransferSecurityPolicy安全性原則。

> **Note**
>
> FIPS 服務端點和 TransferSecurityPolicy-FIPS-2023-05 安全性原則僅適用於某些地區。 AWS 如需詳細資訊，請參閱 AWS 一般參考 中的 AWS Transfer Family 端點和配額。

```
{
    "SecurityPolicy": {
        "Fips": true,
        "SecurityPolicyName": "TransferSecurityPolicy-FIPS-2023-05",
        "SshCiphers": [
            "aes256-gcm@openssh.com",
            "aes128-gcm@openssh.com",
            "aes256-ctr",
            "aes192-ctr"
        ],
        "SshKexs": [
            "diffie-hellman-group16-sha512",
            "diffie-hellman-group18-sha512",
            "diffie-hellman-group-exchange-sha256"
        ],
        "SshMacs": [
            "hmac-sha2-256-etm@openssh.com",
            "hmac-sha2-512-etm@openssh.com"
        ],
        "TlsCiphers": [
            "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
            "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
            "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
            "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
            "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
            "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
            "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
            "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
        ]
    }
}
```

TransferSecurity政策-五

的 FIPS 認證詳細資訊可在 AWS Transfer Family 以下位置找到：https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search/all

以下顯示了 TransferSecurityPolicy安全性原則。

> **Note**
>
> FIPS 服務端點和 TransferSecurityPolicy-FIPS-2020-06 安全性原則僅適用於部分地區。 AWS 如需詳細資訊，請參閱 AWS 一般參考 中的 AWS Transfer Family 端點和配額。

```
{
  "SecurityPolicy": {
    "Fips": true,
    "SecurityPolicyName": "TransferSecurityPolicy-FIPS-2020-06",
    "SshCiphers": [
      "aes128-ctr",
      "aes192-ctr",
      "aes256-ctr",
      "aes128-gcm@openssh.com",
      "aes256-gcm@openssh.com"
    ],
    "SshKexs": [
      "ecdh-sha2-nistp256",
      "ecdh-sha2-nistp384",
      "ecdh-sha2-nistp521",
      "diffie-hellman-group-exchange-sha256",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group14-sha256"
    ],
    "SshMacs": [
      "hmac-sha2-256-etm@openssh.com",
      "hmac-sha2-512-etm@openssh.com",
      "hmac-sha2-256",
      "hmac-sha2-512"
    ],
    "TlsCiphers": [
      "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
```

```
      "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
      "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
      "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
      "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
      "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ]
  }
}
```

後量子安全性原則

下表列出 Transfer Family 列後量子安全性原則的演算法。這些政策在中詳細描述。使用混合式後量子金鑰交換 AWS Transfer Family

政策清單會跟隨下表格。

安全政策	TransferSecurity政策-普 Q-SS-實驗的 -2023-04	TransferSecurity政策-SSH-菲普斯-實驗 -2023-04
SSH ciphers		
中心		♦
aes128-gcm@openssh.com	♦	♦
中心	♦	♦
中心	♦	♦
aes256-gcm@openssh.com	♦	♦
KEXs		
ecdh-nistp256-kyber-512r3-sha256-d00@openquantumsafe.org	♦	♦
ecdh-nistp384-kyber-768r3-sha384-d00@openquantumsafe.org	♦	♦

安全政策	TransferSecurity政策-普 Q-SS-實驗的 -2023-04	TransferSecurity政策-SSH-菲普斯-實驗 -2023-04
ecdh-nistp521-kyber-1024r3-sha512-d00@openquantumsafe.org	♦	♦
x25519-kyber-512r3-sha256-d00@amazon.com	♦	
迪菲-赫尔曼集团		♦
迪菲-赫尔曼集团	♦	♦
迪菲-赫尔曼集团	♦	♦
埃克德什-沙 2-尼斯特 P384		♦
埃克德什-沙 2-尼斯特 P521		♦
迪菲-赫爾曼組-交換-sha256	♦	♦
埃克德什-沙 2-尼斯特 P256		♦
curve25519-sha256@libssh.org	♦	
曲線	♦	
MACs		
hmac-sha2-256-etm@openssh.com	♦	♦
哈馬克沙 2-256	♦	♦
hmac-sha2-512-etm@openssh.com	♦	♦
哈馬克沙 2-512	♦	♦

安全政策	TransferSecurity政策-普 Q-SS-實驗的 -2023-04	TransferSecurity政策-SSH-菲普斯-實驗 -2023-04
TLS ciphers		
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	♦	♦
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	♦	♦
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	♦	♦
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	♦	♦
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	♦	♦
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	♦	♦
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	♦	♦
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	♦	♦

TransferSecurity政策-普 Q-SS-實驗的 -2023-04

下面顯示了 TransferSecurityPolicy-PQ-SSH 實驗 -2023-04 安全性原則。

```
{
    "SecurityPolicy": {
        "Fips": false,
        "SecurityPolicyName": "TransferSecurityPolicy-PQ-SSH-Experimental-2023-04",
        "SshCiphers": [
            "aes256-gcm@openssh.com",
            "aes128-gcm@openssh.com",
```

```
            "aes256-ctr",
            "aes192-ctr"
        ],
        "SshKexs": [
            "ecdh-nistp384-kyber-768r3-sha384-d00@openquantumsafe.org",
            "x25519-kyber-512r3-sha256-d00@amazon.com",
            "ecdh-nistp256-kyber-512r3-sha256-d00@openquantumsafe.org",
            "ecdh-nistp521-kyber-1024r3-sha512-d00@openquantumsafe.org",
            "curve25519-sha256",
            "curve25519-sha256@libssh.org",
            "diffie-hellman-group16-sha512",
            "diffie-hellman-group18-sha512",
            "diffie-hellman-group-exchange-sha256"
        ],
        "SshMacs": [
            "hmac-sha2-512-etm@openssh.com",
            "hmac-sha2-256-etm@openssh.com",
            "hmac-sha2-512",
            "hmac-sha2-256"
        ],
        "TlsCiphers": [
            "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
            "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
            "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
            "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
            "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
            "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
            "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
            "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
        ]
    }
}
```

TransferSecurity政策-SSH-菲普斯-實驗 -2023-04

下面顯示了-PQ-SSH-菲 TransferSecurityPolicy普斯實驗 -2023-04 安全策略。

```
{
    "SecurityPolicy": {
        "Fips": true,
        "SecurityPolicyName": "TransferSecurityPolicy-PQ-SSH-FIPS-
Experimental-2023-04",
        "SshCiphers": [
```

```
            "aes256-gcm@openssh.com",
            "aes128-gcm@openssh.com",
            "aes256-ctr",
            "aes192-ctr",
            "aes128-ctr"
        ],
        "SshKexs": [
            "ecdh-nistp384-kyber-768r3-sha384-d00@openquantumsafe.org",
            "ecdh-nistp256-kyber-512r3-sha256-d00@openquantumsafe.org",
            "ecdh-nistp521-kyber-1024r3-sha512-d00@openquantumsafe.org",
            "ecdh-sha2-nistp256",
            "ecdh-sha2-nistp384",
            "ecdh-sha2-nistp521",
            "diffie-hellman-group-exchange-sha256",
            "diffie-hellman-group16-sha512",
            "diffie-hellman-group18-sha512",
            "diffie-hellman-group14-sha256"
        ],
        "SshMacs": [
            "hmac-sha2-512-etm@openssh.com",
            "hmac-sha2-256-etm@openssh.com",
            "hmac-sha2-512",
            "hmac-sha2-256"
        ],
        "TlsCiphers": [
            "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
            "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
            "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
            "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
            "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
            "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
            "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
            "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
        ]
    }
}
```

AWS Transfer Family SFTP 連接器的安全性原則

中的 SFTP 連接器安全性原則可 AWS Transfer Family 讓您限制與 SFTP 連接器相關聯的一組加密演算法 (訊息驗證碼 (MAC)、金鑰交換 (KEXS) 和加密套件)。以下是每個 SFTP 連接器安全性原則所支援的密碼編譯演算法清單。

> **Note**
>
> TransferSFTPConnectorSecurityPolicy-2024-03是套用至 SFTP 連接器的預設安全性原則。

您可以變更連接器的安全性原則。從「Transfer Family」左側導覽窗格中選取「連接器」，然後選取連接器。然後在 Sftp 配置部分中選擇編輯。在 [密碼編譯演算法選項] 區段中，從 [安全性原則] 欄位的下拉式清單中選擇任何可用的安全性原則。

安全政策	傳輸 FTP 政策 Connector Security	傳輸 FTP 政策 Connector Security
Ciphers		
中心		♦
aes128-gcm@openssh.com	♦	♦
中心	♦	♦
中心	♦	♦
aes256-gcm@openssh.com	♦	♦
Kexs		
曲線	♦	♦
curve25519-sha256@libssh.org	♦	♦
迪菲-赫尔曼集团		♦
迪菲-赫尔曼集团	♦	♦
迪菲-赫尔曼集团	♦	♦
迪菲-赫爾曼組-交換-sha256	♦	♦
Macs		

安全政策	傳輸 FTP 政策 Connector Security	傳輸 FTP 政策 Connector Security
hmac-sha2-512-etm@openssh.com	♦	♦
hmac-sha2-256-etm@openssh.com	♦	♦
哈馬克沙 2-512	♦	♦
哈馬克沙 2-256	♦	♦
哈馬克沙 1		♦
hmac-沙 1-96		♦
Host Key Algorithms		
RSA-沙	♦	♦
RSA-沙	♦	♦
埃克薩·沙 2-尼斯特 P256	♦	♦
埃克薩·沙 2-尼斯特 P384	♦	♦
埃克萨·沙 2-尼斯特 P521	♦	♦
瑞士呼吸系統		♦

使用混合式後量子金鑰交換 AWS Transfer Family

AWS Transfer Family 支援安全殼層 (SSH) 通訊協定的混合式後量子金鑰建立選項。需要建立後量子密鑰，因為它已經可以記錄網絡流量並將其保存以供 future 通過量子計算機進行解密，該計算機稱為現在-現在收穫-以後的攻擊。

當您連線到傳輸系列，以安全傳入和傳出 Amazon 簡單儲存服務 (Amazon S3) 儲存或 Amazon 彈性檔案系統 (Amazon EFS) 的檔案傳輸時，您可以使用此選項。SSH 中的後量子混合密鑰建立引入後量子

密鑰建立機制，它與傳統密鑰交換算法一起使用。使用經典密碼套件創建的 SSH 密鑰可以使用當前技術免受暴力攻擊。但是，在 future 大規模量子計算出現之後，傳統加密不會保持安全。

如果您的組織仰賴透過 Transfer Family 連線傳遞的資料的長期機密性，您應該考慮在大規模量子電腦可供使用之前移轉至後量子密碼編譯的計畫。

為了保護今天加密的數據免受 future 潛在的攻擊， AWS 正與加密社區參與開發量子抗性或後量子算法。我們已經在 Transfer Family 中實施了混合式後量子密鑰交換密碼套件，該套件結合了經典和後量子元素。

這些混合式加密套件可用於大部分 AWS 區域的生產工作負載。但是，由於混合式加密套件的效能特性和頻寬需求與傳統金鑰交換機制不同，因此建議您在 Transfer Family 連線上進行測試。

在後量子密碼學安全部落格文章中深入瞭解後量子密碼學。

內容

- 關於 SSH 中的後量子混合金鑰交換
- 後量子混合密鑰建立如何在 Transfer Family 中工作
  - 為什麼是凱伯？
  - 後量子混合式 SSH 金鑰交換與加密需求 (FIPS 140)
- 在 Transfer Family 列中測試後量子混合金鑰交換
  - 在 SFTP 端點上啟用後量子混合式金鑰交換
  - 設定支援後量子混合式金鑰交換的 SFTP 用戶端
  - 確認 SFTP 中的後量子混合金鑰交換

關於 SSH 中的後量子混合金鑰交換

Transfer Family 支持後量子混合密鑰交換密鑰套件，它同時使用經典的橢圓曲線迪菲-赫爾曼（ECDH）密鑰交換算法和晶體 Kyber。Kyber 是一種後量子公鑰加密和金鑰建立演算法，美國國家標準與技術研究院 (NIST) 已指定為其第一個標準後量子金鑰協定演算法。

客戶端和服務器仍然進行 ECDH 密鑰交換。此外，伺服器會將後量子共用密碼封裝至用戶端的後量子 KEM 公開金鑰，該公開金鑰會在用戶端的 SSH 金鑰交換訊息中公告。這種策略結合了經典密鑰交換的高度保證和提議的後量子密鑰交換的安全性，有助於確保只要 ECDH 或後量子共享密鑰不能被破壞，就可以保護握手。

後量子混合密鑰建立如何在 Transfer Family 中工作

AWS 最近宣布支持 SFTP 文件傳輸中的後量子密鑰交換。 AWS Transfer Family Transfer Family 使用 SFTP 和其他通訊協定，安全地將 business-to-business 檔案傳輸擴展到 AWS 儲存服務。SFTP 是透過 SSH 執行的檔案傳輸通訊協定 (FTP) 更安全的版本。傳輸系列的後量子金鑰交換支援提高了透過 SFTP 傳輸資料的安全性標準。

Transfer Family 中的後量子混合式金鑰交換 SFTP 支援包括結合後量子演算法 Kyber-512、凱伯 -768 和凱伯 -1024，以及 ECDH 超過 P256、P384、P521 或曲線 25519 曲線。下列對應的 SSH 金鑰交換方法在後量子混合式 SSH 金鑰交換草案中指定。

- `ecdh-nistp256-kyber-512r3-sha256-d00@openquantumsafe.org`
- `ecdh-nistp384-kyber-768r3-sha384-d00@openquantumsafe.org`
- `ecdh-nistp521-kyber-1024r3-sha512-d00@openquantumsafe.org`
- `x25519-kyber-512r3-sha256-d00@amazon.com`

> **Note**
>
> 這些新的金鑰交換方法可能會隨著草案向標準化的發展或 NIST 批准 Kyber 演算法而改變。

為什麼是凱伯？

AWS 致力於支援標準化、可互操作的演算法。Kyber 是 NIST 後量子密碼學專案選定用於標準化的第一個後量子加密演算法。一些標準機構已經將 Kyber 集成到協議中。 AWS 在某些 AWS API 端點中已經支持 TLS 中的凱伯。

作為這項承諾的一部分， AWS 已向 IETF 提交了一份關於後量子密碼學的提案草案，該建議將 Kyber 與 NIST 批准的曲線（例如 SSH 的 P256）結合在一起。為了協助提升客戶的安全性，SFTP 和 SSH 中的後量子金鑰交換 AWS 實作遵循該草案。我們計劃支持 future 的更新，直到我們的建議被 IETF 採用並成為標準。

隨著草案向標準化發展或 NIST 批准 Kyber 算法，新的密鑰交換方法（在部分中列出後量子混合密鑰建立如何在 Transfer Family 中工作）可能會發生變化。

> **Note**
>
> 後量子演算法支援目前可用於 TLS 中的後量子混合金鑰交換 AWS KMS (請參閱使用混合後量子 TLS 搭配 AWS KMS) 和 AWS Secrets Manager API 端點。AWS Certificate Manager

後量子混合式 SSH 金鑰交換與加密需求 (FIPS 140)

對於需要 FIPS 合規性的客戶，Transfer Family 使用 FIPS 140 認證的開放原始碼編譯程式庫-LC，以 SSH 提供 AWS FIPS 核准的加密技術。 AWS根據 NIST 的 SP 800-56Cr2（第 2 節），Transfer Family 中支持的 TransferSecurityPolicy-PQ-SSH-FIPS 實驗 -2023-04 支持的後量子混合密鑰交換方法。德國聯邦信息安全局（BSI）和法國國家信息系統（AN SSI）也推薦這種後量子混合密鑰交換方法。

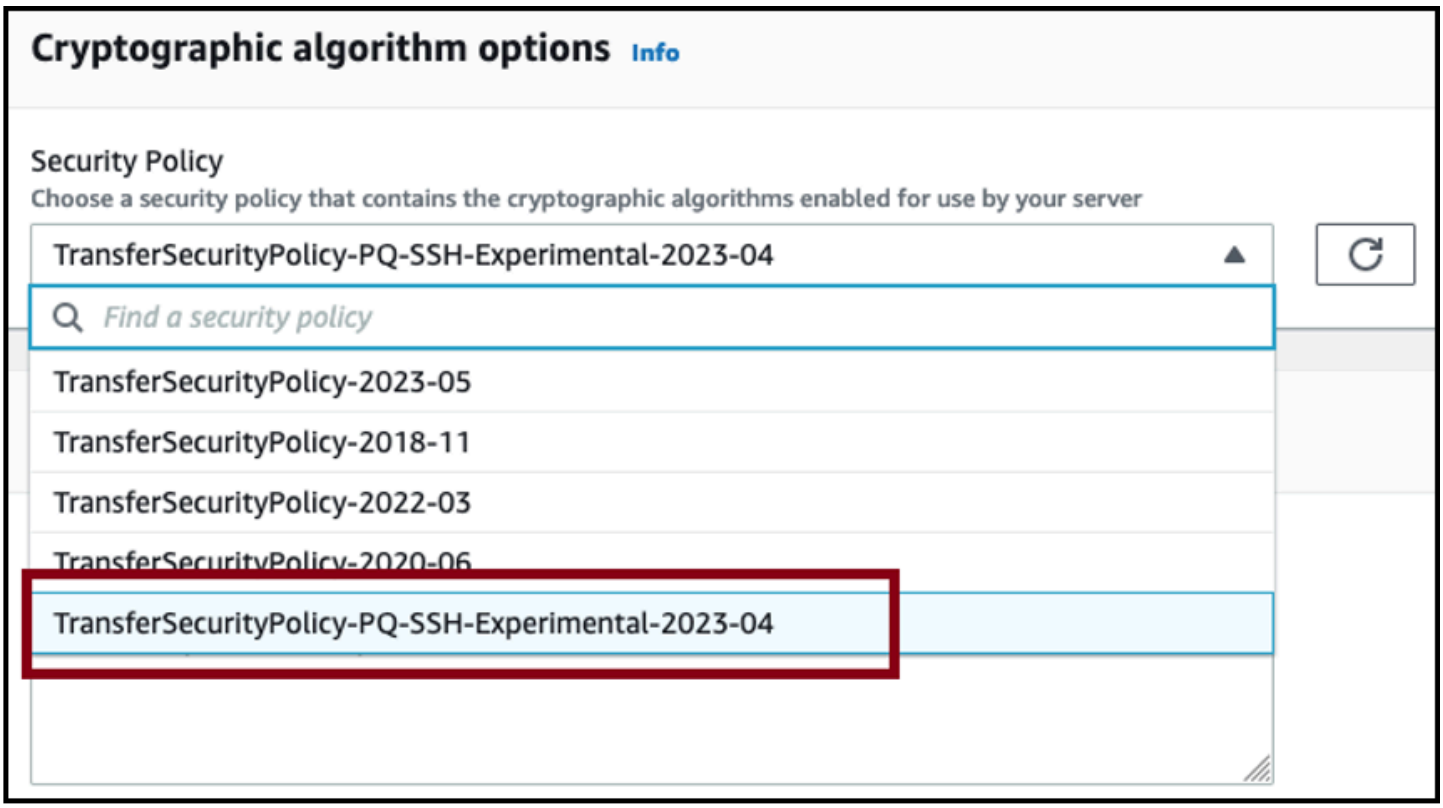
在 Transfer Family 列中測試後量子混合金鑰交換

本節說明測試後量子混合金鑰交換所採取的步驟。

1. 在 SFTP 端點上啟用後量子混合式金鑰交換.
2. 遵循上述草案規格中的指引，使用支援後量子混合式金鑰交換的 SFTP 用戶端 (例如設定支援後量子混合式金鑰交換的 SFTP 用戶端)。
3. 使用轉移系列伺服器傳輸檔案。
4. 確認 SFTP 中的後量子混合金鑰交換.

在 SFTP 端點上啟用後量子混合式金鑰交換

您可以在 Transfer Family 列中建立新的 SFTP 伺服器端點時，或編輯現有 SFTP 端點中的密碼編譯演算法選項，來選擇 SSH 政策。以下快照顯示了 AWS Management Console 更新 SSH 策略的範例。



支援後量子金鑰交換的 SSH 原則名稱為政策-PQ-SSH 實驗 -2023-04 和政TransferSecurity策-PQ-SS-FIP 實驗- 2023-04。TransferSecurity如需 Transfer Family 政策的詳細資訊，請參閱AWS Transfer Family 伺服器的安全性原則。

設定支援後量子混合式金鑰交換的 SFTP 用戶端

在 SFTP Transfer Family 端點中選取正確的量子後 SSH 原則之後，您可以在 Transfer Family 中嘗試量子後 SFTP。您可以使用支援後量子混合金鑰交換的 SFTP 用戶端 (例如 OQS OpenSSH)，方法是遵循上述草案規格草案中的指引。

OQS OpenSSH 是 OpenSSH 的一個開源分支，它通過使用將量子安全加密技術添加到 SSH。`liboqs` `liboqs`是一個開源的 C 庫，實現了抗量子加密算法。OQS OpenSSH 並且`liboqs`是開放量子安全（OQS）項目的一部分。

若要使用 OQS OpenSSH 在 Transfer Family SFTP 中測試後量子混合式金鑰交換，您需要建置 OQS OpenSSH，如專案的讀我檔案所述。建立 OQS OpenSSH 之後，您可以執行範例 SFTP 用戶端，透過使用後量子混合式金鑰交換方法來連線到 SFTP 端點 (例如`s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com`)，如下列命令所示。

```
./sftp -S ./ssh -v -o \
```

```
    KexAlgorithms=ecdh-nistp384-kyber-768r3-sha384-d00@openquantumsafe.org \
    -i username_private_key_PEM_file \
    username@server-id.server.transfer.region-id.amazonaws.com
```

在上一個命令中，用您自己的資訊取代下列項目：

- 以 SFTP *######## PEM ################*
- 以 SFTP 使用者*##*取代使用者名稱
- 以 Transfer Family *### ID* 取代伺服器 ID
- 將區*# ID* 替換為 Transfer Family 服務器所在的實際區域

確認 SFTP 中的後量子混合金鑰交換

若要確認 SFTP Transfer Family 列的 SSH 連線期間使用量子後混合金鑰交換，請檢查用戶端輸出。或者，您可以使用封包擷取程式。如果您使用開放量子安全 OpenSSH 用戶端，輸出應類似下列內容 (為簡潔起見省略不相關的資訊)：

```
$./sftp -S ./ssh -v -o KexAlgorithms=ecdh-nistp384-kyber-768r3-sha384-
d00@openquantumsafe.org -
i username_private_key_PEM_file username@s-1111aaaa2222bbbb3.server.transfer.us-
west-2.amazonaws.com
OpenSSH_8.9-2022-01_p1, Open Quantum Safe 2022-08, OpenSSL 3.0.2 15 Mar 2022
debug1: Reading configuration data /home/lab/openssh/oqs-test/tmp/ssh_config
debug1: Authenticator provider $SSH_SK_PROVIDER did not resolve; disabling
debug1: Connecting to s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com
 [xx.yy.zz..12] port 22.
debug1: Connection established.
[...]
debug1: Local version string SSH-2.0-OpenSSH_8.9-2022-01_
debug1: Remote protocol version 2.0, remote software version AWS_SFTP_1.1
debug1: compat_banner: no match: AWS_SFTP_1.1
debug1: Authenticating to s-1111aaaa2222bbbb3.server.transfer.us-
west-2.amazonaws.com:22 as 'username'
debug1: load_hostkeys: fopen /home/lab/.ssh/known_hosts2: No such file or directory
[...]
debug1: SSH2_MSG_KEXINIT sent
debug1: SSH2_MSG_KEXINIT received
debug1: kex: algorithm: ecdh-nistp384-kyber-768r3-sha384-d00@openquantumsafe.org
debug1: kex: host key algorithm: ssh-ed25519
debug1: kex: server->client cipher: aes192-ctr MAC: hmac-sha2-256-etm@openssh.com
 compression: none
```

```
debug1: kex: client->server cipher: aes192-ctr MAC: hmac-sha2-256-etm@openssh.com
 compression: none
debug1: expecting SSH2_MSG_KEX_ECDH_REPLY
debug1: SSH2_MSG_KEX_ECDH_REPLY received
debug1: Server host key: ssh-ed25519 SHA256:e3b0c44298fc1c149afbf4c8996fb92427ae41e4649
[...]
debug1: rekey out after 4294967296 blocks
debug1: SSH2_MSG_NEWKEYS sent
debug1: expecting SSH2_MSG_NEWKEYS
debug1: SSH2_MSG_NEWKEYS received
debug1: rekey in after 4294967296 blocks
[...]
Authenticated to AWS.Tranfer.PQ.SFTP.test-endpoint.aws.com ([xx.yy.zz..12]:22) using
 "publickey".s
debug1: channel 0: new [client-session]
[...]
Connected to s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com.
sftp>
```

輸出顯示用戶端交涉是使用後量子混合`ecdh-nistp384-kyber-768r3-sha384-d00@openquantumsafe.org`方法發生的，並成功建立 SFTP 工作階段。

資料保護 AWS Transfer Family

AWS 共同責任模型適用於 AWS Transfer Family (Transfer Family) 中的資料保護。如此模型所述，AWS 負責保護執行所有 AWS 雲端的全域基礎結構。您負責維護在此基礎設施上託管內容的控制權。此內容包括您使用之 AWS 服務的安全性設定和管理工作。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。如需歐洲資料保護的相關資訊，請參閱AWS 安全部落格上的AWS 共同責任模型和 GDPR 部落格文章。

基於資料保護目的，我們建議您使用 AWS Identity and Access Management (IAM) 保護 AWS 帳戶登入資料，並設定個別使用者帳戶。如此一來，每個使用者都只會獲得授予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。我們支援 TLS 1.2。
- 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 AWS 服務中的所有預設安全性控制。
- 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 Simple Storage Service (Amazon Simple Storage Service (Amazon S3)) 的個人資料。

- 如果您在透過命令列介面或 API 存取 AWS 時，需要 FIPS 140-2 驗證的加密模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的詳細資訊，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帳戶號碼等敏感的識別資訊，放在自由格式的欄位中，例如名稱欄位。這包括當您使用主控台、API 或 AWS SDK 使用 Transfer Family 或其他 AWS 服務時。 AWS CLI您在 Transfer Family 服務組態或其他服務的組態中輸入的任何組態資料都可能會被拾取以包含在診斷記錄中。當您提供外部伺服器的 URL 時，請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

相反地，傳入和下載作業進出 Transfer Family 伺服器的資料會被視為完全私有，絕不會存在於加密通道之外，例如 SFTP 或 FTPS 連線。此數據僅供授權人員訪問。

主題

- Amazon S3 中的資料加密
- 在 Transfer Family 中管理安全殼層和 PGP 金鑰

Amazon S3 中的資料加密

AWS Transfer Family 使用您為 Amazon S3 儲存貯體設定的預設加密選項來加密資料。當您在儲存貯體上啟用加密時，存放於儲存貯體中的所有物件都會加密。使用伺服器端加密與 Amazon S3 受管金鑰 (SSE-S3) 或 () 受管金鑰 AWS Key Management Service (SSE-KMS AWS KMS) 來加密物件。有關伺服器端加密的資訊，請參閱 Amazon 簡單儲存服務使用者指南中的使用伺服器端加密保護資料。

下列步驟說明如何在中加密資料 AWS Transfer Family。

允許加密 AWS Transfer Family

1. 為您的 Amazon S3 儲存貯體啟用預設加密。如需指示，請參閱 Amazon 簡單儲存服務使用者指南中的 Amazon S3 儲存貯體預設加密。
2. 更新附加至使用者的 AWS Identity and Access Management (IAM) 角色政策，以授予所需的 AWS Key Management Service (AWS KMS) 權限。
3. 如果您為使用者使用工作階段原則，工作階段原則必須授與所需的 AWS KMS 權限。

以下範例顯示 IAM 政策，該政策授予與已啟用 AWS KMS 加密的 Amazon S3 儲存貯體 AWS Transfer Family 搭配使用時所需的最低許可。如果您使用的是，請在使用者 IAM 角色政策和工作階段政策中包含此範例政策。

```
{
```

```
 "Sid": "Stmt1544140969635",
 "Action": [
  "kms:Decrypt",
  "kms:Encrypt",
  "kms:GenerateDataKey"
 ],
 "Effect": "Allow",
 "Resource": "arn:aws:kms:region:account-id:key/kms-key-id"
}
```

> **Note**
>
> 您在此原則中指定的 KMS 金鑰識別碼必須與步驟 1 中為預設加密指定的 KMS 金鑰識別碼相同。
>
> AWS KMS 金鑰政策中必須允許根或用於使用者的 IAM 角色。如需金 AWS KMS 鑰原則的相關資訊，請參閱AWS Key Management Service 開發人員指南中的使用 AWS KMS 中的金鑰原則。

在 Transfer Family 中管理安全殼層和 PGP 金鑰

在本節中，您可以找到有關安全殼層金鑰的資訊，包括如何產生這些金鑰以及如何旋轉這些金鑰。如需使用 Transfer Family 搭配管理金鑰的詳細資訊，請參閱 AWS Lambda 以 A AWS Transfer Family 和啟用使用者自助式金鑰管理的部落格文章 AWS Lambda。

> **Note**
>
> AWS Transfer Family 接受 RSA、ECDSA 和 ED25519 金鑰。

本節還介紹瞭如何生成和管理良好的隱私（PGP）密鑰。

主題

- 支援的使用者和伺服器金鑰演算法
- 為服務管理的使用者產生 SSH 金鑰
- 旋轉 SSH 金鑰
- 產生和管理 PGP 金鑰
- 支援的 PGP 用戶端

支援的使用者和伺服器金鑰演算法

使用者和伺服器金鑰組支援下列金鑰演算法。 AWS Transfer Family

> **Note**
>
> 如需在工作流程中搭配 PGP 解密使用的演算法，請參閱 PGP 金鑰配對支援的演算法。

- 對於 ED25519：`ssh-ed25519`
- 對於 RSA：
  - `rsa-sha2-256`
  - `rsa-sha2-512`
- 對於 ECDSA：
  - `ecdsa-sha2-nistp256`
  - `ecdsa-sha2-nistp384`
  - `ecdsa-sha2-nistp521`

> **Note**
>
> 我們為`ssh-rsa`舊版安全性原則提供 SHA1 支援。如需詳細資訊，請參閱 加密算法。

為服務管理的使用者產生 SSH 金鑰

您可以將伺服器設定為使用服務管理驗證方法來驗證使用者，其中使用者名稱和 SSH 金鑰會儲存在服務中。使用者的公開安全殼層金鑰會作為使用者的屬性上傳至伺服器。伺服器會使用此金鑰做為標準金鑰型驗證程序的一部分。每個使用者都可以針對個別伺服器上的檔案擁有多個公有 SSH 金鑰。如需每位使用者可儲存的金鑰數目限制，請參閱AWS Transfer Family Amazon Web Services 一般參考.

作為服務管理驗證方法的替代方法，您可以使用自訂身分識別提供者或來驗證使用者 AWS Directory Service for Microsoft Active Directory。如需詳細資訊，請參閱 使用自訂身分識別提供者 或 使用 AWS Directory Service 身分識別提供者 。

伺服器只能使用一種方法 (服務管理、目錄服務或自訂身分識別提供者) 來驗證使用者，而且在建立伺服器之後無法變更該方法。

主題

- 在 macOS、Linux 或 Unix 上建立安全殼層金鑰
- 在 Microsoft 視窗上建立 SSH 金鑰
- 將 SSH2 公開金鑰轉換為 PEM 格式

在 macOS、Linux 或 Unix 上建立安全殼層金鑰

在 macOS、Linux 或 Unix 作業系統上，您可以使用`ssh-keygen`指令來建立安全殼層公開金鑰和 SSH 私密金鑰 (也稱為 key pair)。

在 macOS、Linux 或 Unix 作業系統上建立安全殼層金鑰

1. 在 macOS、Linux 或 Unix 作業系統上，開啟指令終端機。
2. AWS Transfer Family 接受 RSA、ECDSA 和格式化的金鑰。根據您要產生的金鑰配對類型選擇適當的指令。

> **Note**
>
> 在下面的例子中，我們不指定密碼：在這種情況下，該工具會要求您輸入密碼，然後重複以驗證。建立密碼片語可為您的私密金鑰提供更好的保護，也可能改善整體系統安全性。您無法復原密碼片語：如果忘記密碼，就必須建立新的金鑰。
> 但是，如果您要產生伺服器主機金鑰，則必須指定指令中的`-N ""`選項 (或在出現提示時按**Enter**兩次) 來指定空的複雜密碼，因為 Transfer Family Server 無法在啟動時要求密碼。

- 若要產生 RSA 4096 位元 key pair，請執行下列動作：

```
ssh-keygen -t rsa -b 4096 -f key_name
```

- 若要產生一組 521 位元金鑰配對 (ECDSA 的位元大小為 256、384 和 521)，請執行下列動作：

```
ssh-keygen -t ecdsa -b 521 -f key_name
```

- 若要產生 ED25519 key pair：

```
ssh-keygen -t ed25519 -f key_name
```

> **Note**
>
> *key_name*是 SSH key pair 檔案名稱。

以下顯示ssh-keygen輸出的範例。

```
ssh-keygen -t rsa -b 4096 -f key_name
Generating public/private rsa key pair.

Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in key_name.
Your public key has been saved in key_name.pub.
The key fingerprint is:
SHA256:8tDDwPmanTFcEzjTwPGETVWOGW1nVz+gtCCE8hL7PrQ bob.amazon.com
The key's randomart image is:
+---[RSA 4096]----+
|    . ....E      |
| .   = ...       |
|. . . = ..o      |
| . o +  oo =     |
|  + =  .S.= *    |
| . o o ..B + o   |
|     .o.+.* .    |
|     =o*+*.      |
|    ..*o*+.      |
+----[SHA256]-----+
```

> **Note**
>
> 當您如上所述執行 ssh-keygen 命令時，它會在目前的目錄內以檔案的型式建立公有和私有金鑰。

您的 SSH key pair 現在已準備好可供使用。依照步驟 3 和 4 為您的服務管理使用者儲存 SSH 公開金鑰。這些使用者在傳輸系列伺服器端點上傳輸檔案時會使用這些金鑰。

3. 導航到該*key_name*.pub文件並打開它。

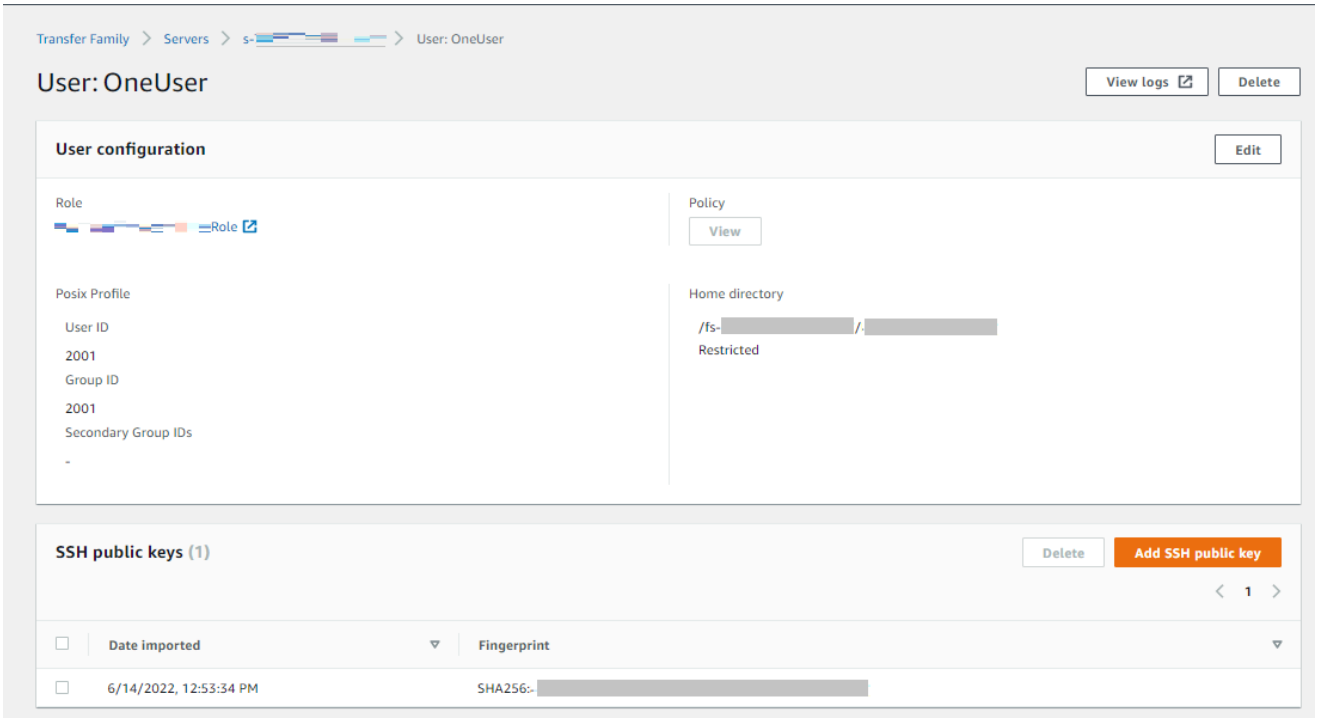
4. 複製文字並將其貼到服務管理使用者的 SSH 公開金鑰中。

   a. 在 https://console.aws.amazon.com/transfer/ 開啟 AWS Transfer Family 主控台，然後從導覽窗格中選取 [伺服器]。

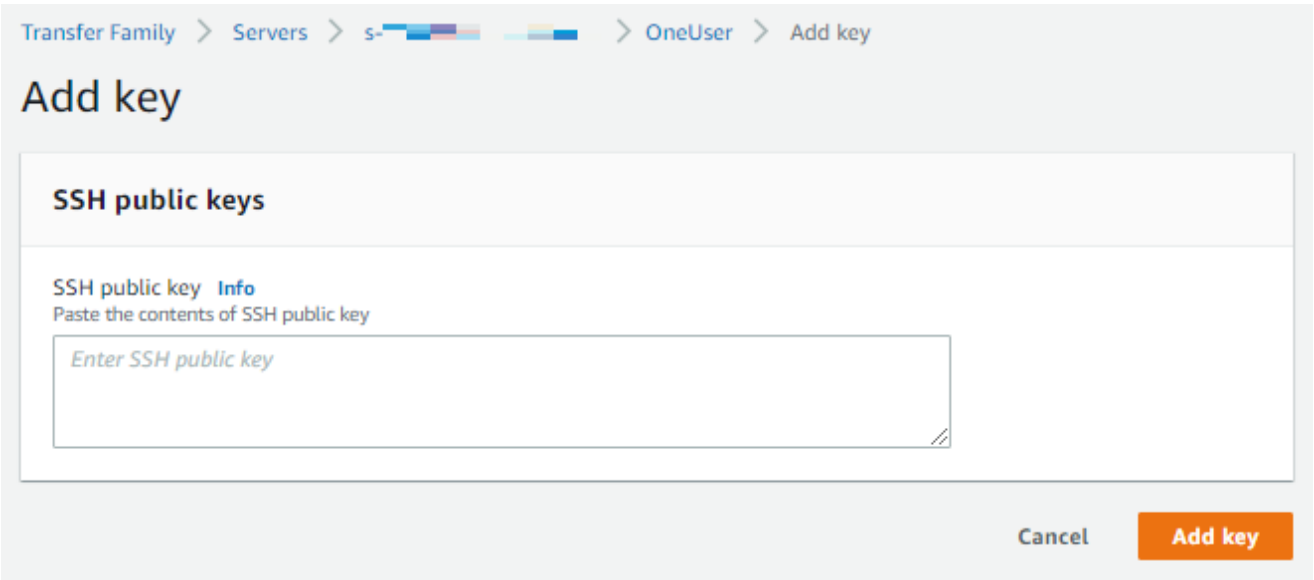
   b. 在 [伺服器] 頁面上，選取包含您要更新之使用者之伺服器的伺服器 ID。

   c. 選取要為其新增公開金鑰的使用者。

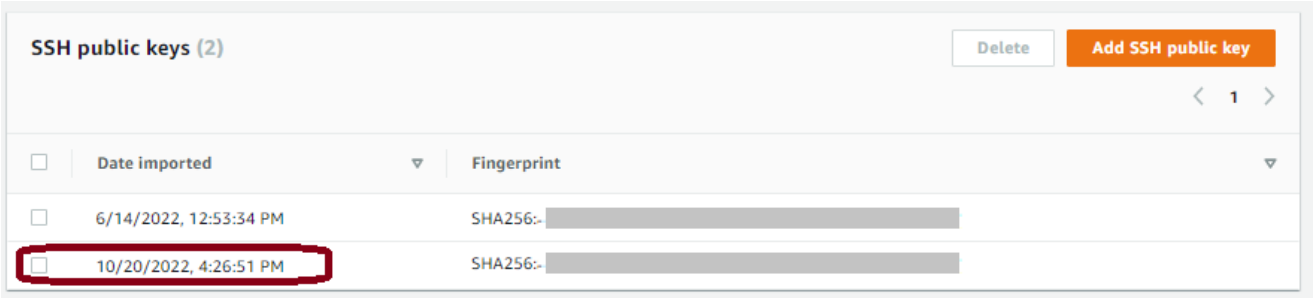
   d. 在 [SSH 公開金鑰] 窗格中，選擇 [新增安全殼層公開金鑰]。



   e. 將您產生的公開金鑰文字貼到 SSH 公開金鑰文字方塊中，然後選擇 [新增金鑰]。



新金鑰會列在 SSH 公開金鑰窗格中。



在 Microsoft 視窗上建立 SSH 金鑰

Windows 會使用稍微不同的 SSH 金鑰對格式。公有金鑰的格式必須是 PUB 格式，私有金鑰的格式則必須是 PPK 格式。在 Windows 上，您可以使用 PuTTYgen 以適當的格式建立 SSH 金鑰對。您也可以使用 PuTTYgen，將使用 ssh-keygen 產生的私有金鑰轉換成 .ppk 檔案。

> **Note**
>
> 如果您以非.ppk格式的私密金鑰檔案呈現 WinSCP，則該用戶端會提供將金鑰轉換為您的.ppk格式。

如需在 Windows 上使用 Puttygen 建立安全殼層金鑰的教學課程，請參閱 SSH.com 網站。

將 SSH2 公開金鑰轉換為 PEM 格式

AWS Transfer Family 僅接受 PEM 格式的公鑰。如果您有 SSH2 公鑰，則需要將其轉換。SSH2 公開金鑰的格式如下：

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-20160402"
AAAAB3NzaC1yc2EAAAABJQAAAgEAiL0jjDdFqK/kYThqKt7THrjABTPWvXmB3URI
:
:
---- END SSH2 PUBLIC KEY ----
```

PEM 公開金鑰的格式如下：

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAA...
```

執行下列命令，將 SSH2 格式的公開金鑰轉換為 PEM 格式的公開金鑰。將 *ssh2 ##*替換為 SSH2 密鑰的名稱，將 PEM 密鑰替換為您的 *PEM ##*的名稱。

```
ssh-keygen -i -f ssh2-key.pub > PEM-key.pub
```

旋轉 SSH 金鑰

為了安全起見，我們建議您使用輪換安全殼層金鑰的最佳作法。通常，此輪替被指定為安全策略的一部分，並以某種自動化方式實施。視安全性等級而定，對於高度敏感的通訊，SSH key pair 可能只會使用一次。這樣做可消除任何因存放金鑰所帶來的風險。但是，存儲 SSH 憑據一段時間並設置不會給用戶造成不必要負擔的間隔更為常見。常見的間隔是三個月。

執行 SSH 金鑰輪換的方法有兩種：

- 在主控台上，您可以上傳新的安全殼層公開金鑰，並刪除現有的安全殼層公開金鑰。
- 使用 API，您可以使用 DeleteSshPublicKeyAPI 刪除使用者的安全殼層 (SSH) 公開金鑰，以及將新的安全殼層 (SSH) 公開金鑰新增至使用者帳戶的 ImportSshPublicKeyAPI 來更新現有使用者。

Console

在主控台中執行按鍵旋轉

1. 請在以下位置開啟 AWS Transfer Family 主控台。 https://console.aws.amazon.com/transfer/
2. 瀏覽至「伺服器」頁面。
3. 在「伺服器 ID」欄中選擇識別碼，以查看「伺服器詳細資訊」頁面。
4. 在 [使用者] 底下，選取您要輪換其安全殼層公開金鑰之使用者的核取方塊，然後選擇 [動作]，然後選擇 [新增金鑰] 以查看 [新增金鑰] 頁面。

   或

   選擇使用者名稱以查看 [使用者詳細資料] 頁面，然後選擇 [新增安全殼層公開金鑰] 查看 [新增金鑰] 頁面。
5. 輸入新的 SSH 公開金鑰，然後選擇 [新增金鑰]。

   > **Important**
   >
   > SSH 公開金鑰的格式取決於您產生的金鑰類型。
   >
   > - 對於 RSA 金鑰，格式為`ssh-rsa` *`string`*。

- 對於 ED25519 金鑰，格式為ssh-ed25519 *string*。
- 對於 ECDSA 金鑰，金鑰會以ecdsa-sha2-nistp256、或開頭 ecdsa-sha2-nistp384ecdsa-sha2-nistp521，視您產生的金鑰大小而定。然後，開始字符串後跟*string*，類似於其他鍵類型。

您會返回 [使用者詳細資料] 頁面，而您剛才輸入的新安全殼層公開金鑰會出現在 SSH 公開金鑰區段中。

6. 選取您要刪除之舊金鑰的核取方塊，然後選擇 [刪除]。
7. 輸入文字以確認刪除作業delete，然後選擇 [刪除]。

API

使用 API 執行金鑰輪換

1. 在 macOS、Linux 或 Unix 作業系統上，開啟指令終端機。
2. 輸入下列命令，擷取您要刪除的 SSH 金鑰。若要使用此命令，請以您*serverID*的 Transfer Family 伺服器的伺服器 ID 取代，並以您的使*username*用者名稱取代。

```
aws transfer describe-user --server-id='serverID' --user-name='username'
```

該命令返回有關用戶的詳細信息。複製"SshPublicKeyId":欄位的內容。您稍後需要在此程序中輸入此值。

```
"SshPublicKeys": [ { "SshPublicKeyBody": "public-key", "SshPublicKeyId":
 "keyID",
   "DateImported": 1621969331.072 } ],
```

3. 接下來，為您的使用者匯入新的 SSH 金鑰。在 提示中輸入下列命令。要使用此命令，請替換*serverID*為 Transfer Family 服務器的服務器 ID，*username*替換為您的用戶名，然後*public-key*用新的公鑰的指紋替換。

```
aws transfer import-ssh-public-key --server-id='serverID' --user-name='username'
   --ssh-public-key-body='public-key'
```

如果命令成功，則不會返回任何輸出。

4. 最後，通過運行以下命令刪除舊密鑰。若要使用此命令，請以您*serverID*的 Transfer Family 伺服器的伺服器 ID 取代，取代*username*為您的使*keyID-from-step-2*用者名稱，並以您在此程序的步驟 2 中複製的金鑰 ID 值取代

```
aws transfer delete-ssh-public-key --server-id='serverID' --user-name='username'
   --ssh-public-key-id='keyID-from-step-2'
```

5. (選擇性) 若要確認舊金鑰不再存在，請重複步驟 2。

產生和管理 PGP 金鑰

您可以搭配 Transfer Family 使用工作流程處理的檔案，使用 Pretty Good Privacy (PGP) 解密。若要在工作流程步驟中使用解密，請提供 PGP 金鑰。

AWS 存儲博客有一篇文章，描述瞭如何簡單地解密文件而不使用 Transfer Family 託管工作流程編寫任何代碼，使用 PGP 和 AWS Transfer Family.

產生 PGP 金鑰

您用來產生 PGP 金鑰的操作員，取決於您的作業系統和您使用的金鑰產生軟體版本。

如果您使用的是 Linux 或 Unix，請使用套件安裝程式進行安裝gpg。根據您的 Linux 發行版本，下列其中一個指令應適用於您。

```
sudo yum install gnupg
```

```
sudo apt-get install gnupg
```

對於視窗或 macOS，您可以從以下位置下載所需的內容 https://gnupg.org/download/。

安裝 PGP 金鑰產生器軟體之後，您可以執行`gpg --full-gen-key`或`gpg --gen-key`指令來產生 key pair。

> **Note**
>
> 如果您使用的是 2.3.0 或更高GnuPG版本，則必須運行`gpg --full-gen-key`。當系統提示您輸入要建立的金鑰類型時，請選擇 RSA 或 ECC。但是，如果您選擇 ECC，請務必BrainPool為橢圓曲線選擇NIST或。不要選擇Curve 25519。

PGP 金鑰配對支援的演算法

我們支援 PGP 金鑰配對的下列演算法：

- RSA
- 妖精
- ECC：
  - NIST
  - BrainPool

> **Note**
>
> 我們不支援金鑰。

有用的**gpg**子命令

以下是一些有用的子命令：gpg

- `gpg --help`— 此指令會列出可用的選項，並可能包含一些範例。
- `gpg --list-keys`— 此指令會列出您已建立之所有金鑰配對的詳細資訊。
- `gpg --fingerprint`— 此命令列出了所有密鑰對的詳細信息，包括每個密鑰的指紋。
- `gpg --export -a` *`user-name`*— 此命令會匯出產生金鑰時所使用之金鑰的公開金鑰部分。*`user-name`*

管理 PGP 金鑰

若要管理您的 PGP 金鑰，請使用 AWS Secrets Manager。

> **Note**
>
> 您的密碼名稱包括您的 Transfer Family 服務器 ID。這意味著您應該已經識別或創建了一台服務器，然後才能將 PGP 密鑰信息存儲在中 AWS Secrets Manager。

如果您要為所有使用者使用一個金鑰和密碼，您可以將 PGP 金鑰區塊資訊儲存在密碼名稱下`aws/transfer/`*`server-id`*`/@pgp-default`，其中*`server-id`*是您的 Transfer Family 伺服器的 ID。如果沒有與執行工作流程的使用者*`user-name`*相符的金鑰，則 Transfer Family 會使用此預設金鑰。

您可以為特定使用者建立金鑰。在此情況下，密碼名稱的格式為`aws/transfer/`*`server-id`*`/`*`user-name`*，其中*`user-name`*與執行 Transfer Family 伺服器工作流程的使用者相符。

> **Note**
>
> 每個 Transfer Family 伺服器每個使用者最多可以儲存 3 個 PGP 私密金鑰。

設定要與解密搭配使用的 PGP 金鑰

1. 視您使用的 GPG 版本而定，執行下列其中一個指令來產生不使用 Curve 25519 加密演算法的 PGP key pair。

   - 如果您使用的是 2.3.0 或更新**GnuPG**版本，請執行下列命令：

     ```
     gpg --full-gen-key
     ```

     您可以選擇**RSA**，或者，如果您選擇**ECC**，您可以**BrainPool**為橢圓曲線選擇**NIST**或。如果您`gpg --gen-key`改為執行，則建立使用 ECC 曲線 25519 加密演算法的 key pair，我們目前不支援 PGP 金鑰。

   - 對於 2.3.0 之**GnuPG**前的版本，您可以使用下列命令，因為 RSA 是預設的加密類型。

     ```
     gpg --gen-key
     ```

   > **Important**
   >
   > 在金鑰產生過程中，您必須提供密碼片語和電子郵件地址。請務必注意這些值。當您在本程序 AWS Secrets Manager 稍後輸入金鑰的詳細資訊時，必須提供複雜密碼。在下一步中，您必須提供相同的電子郵件地址才能導出私鑰。

2. 執行下列命令以匯出私密金鑰。若要使*`private.pgp`*用此命令，請取代為儲存私密金鑰區塊的檔案名稱，以及*`marymajor@example.com`*您在產生金 key pair 時使用的電子郵件地址。

```
gpg --output private.pgp --armor --export-secret-key marymajor@example.com
```

3. 用 AWS Secrets Manager 於儲存您的 PGP 金鑰。

   a. 請登入 AWS Management Console 並開啟 AWS Secrets Manager 主控台，網址為 https://console.aws.amazon.com/secretsmanager/。

   b. 在左側導覽窗格中，選擇秘密。

   c. 在「密碼」頁面上，選擇「儲存新密碼」。

   d. 在 [選擇密碼類型] 頁面上，對於 [密碼類型]，選取 [其他密碼類型]。

   e. 在「鍵/值對」區段中，選擇「鍵/值」標籤。

   - 鍵-輸入**PGPPrivateKey**。

     > **Note**
     > 您必須完全輸入**PGPPrivateKey**字串：請勿在字元之前或之間加入任何空格。

   - value — 將私鑰的文本粘貼到值字段中。您可以在先前在此程序中匯出金鑰時所指定的檔案 (例如`private.pgp`) 中找到私密金鑰的文字。金鑰的開頭`-----BEGIN PGP PRIVATE KEY BLOCK-----`與結尾為`-----END PGP PRIVATE KEY BLOCK-----`。

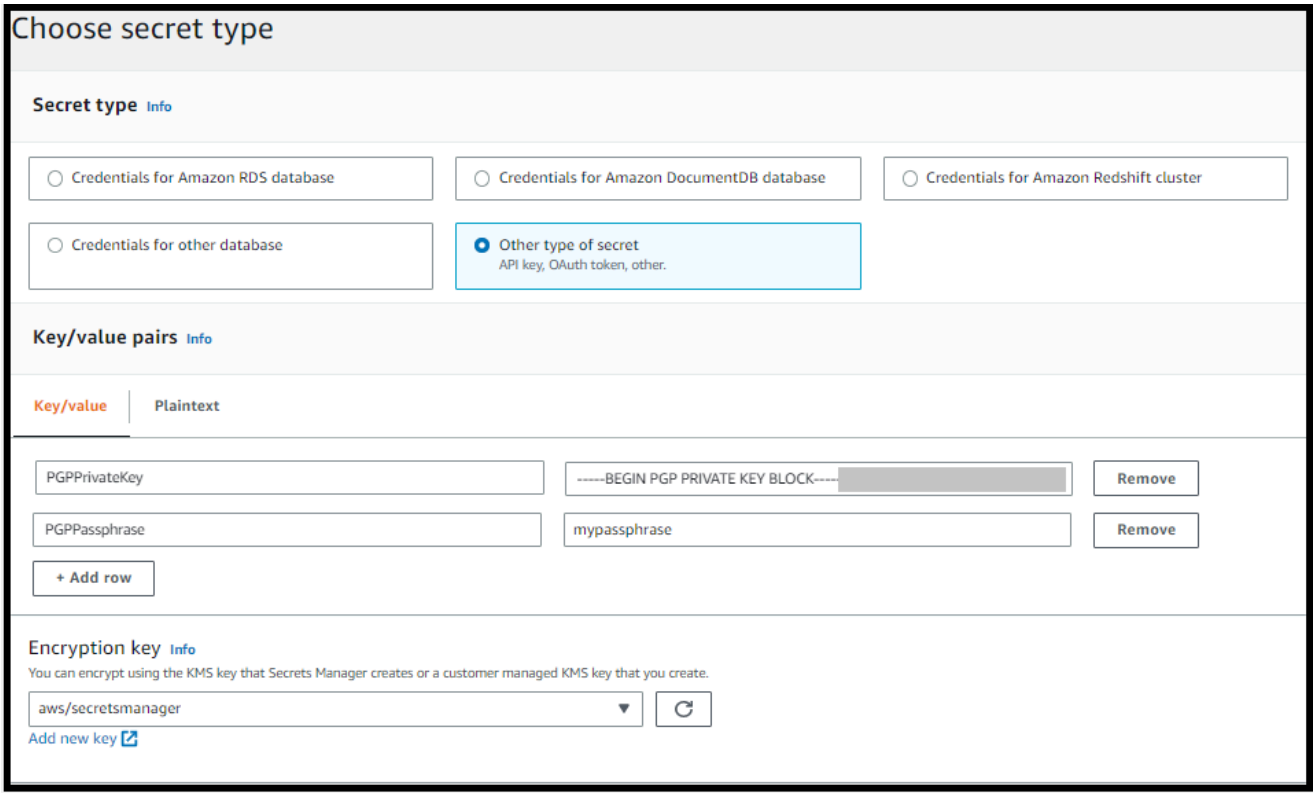
     > **Note**
     > 請確定文字區塊只包含私密金鑰，而且不包含公開金鑰。

   f. 選擇添加行，然後在鍵/值對部分中，選擇鍵/值選項卡。

   - 鍵-輸入**PGPPassphrase**。

     > **Note**
     > 您必須完全輸入**PGPPassphrase**字串：請勿在字元之前或之間加入任何空格。

   - value — 輸入您在產生 PGP key pair 時使用的複雜密碼。



> **Note**
>
> 您最多可以新增 3 組金鑰和密碼。若要新增第二個集合，請新增兩個新資料列，然後**PGPPassphrase2**為金鑰輸入**PGPPrivateKey2**和，然後貼上另一個私密金鑰和複雜密碼。要添加第三個集合，鍵值必須是**PGPPrivateKey3**和**PGPPassphrase3**。

g. 選擇下一步。

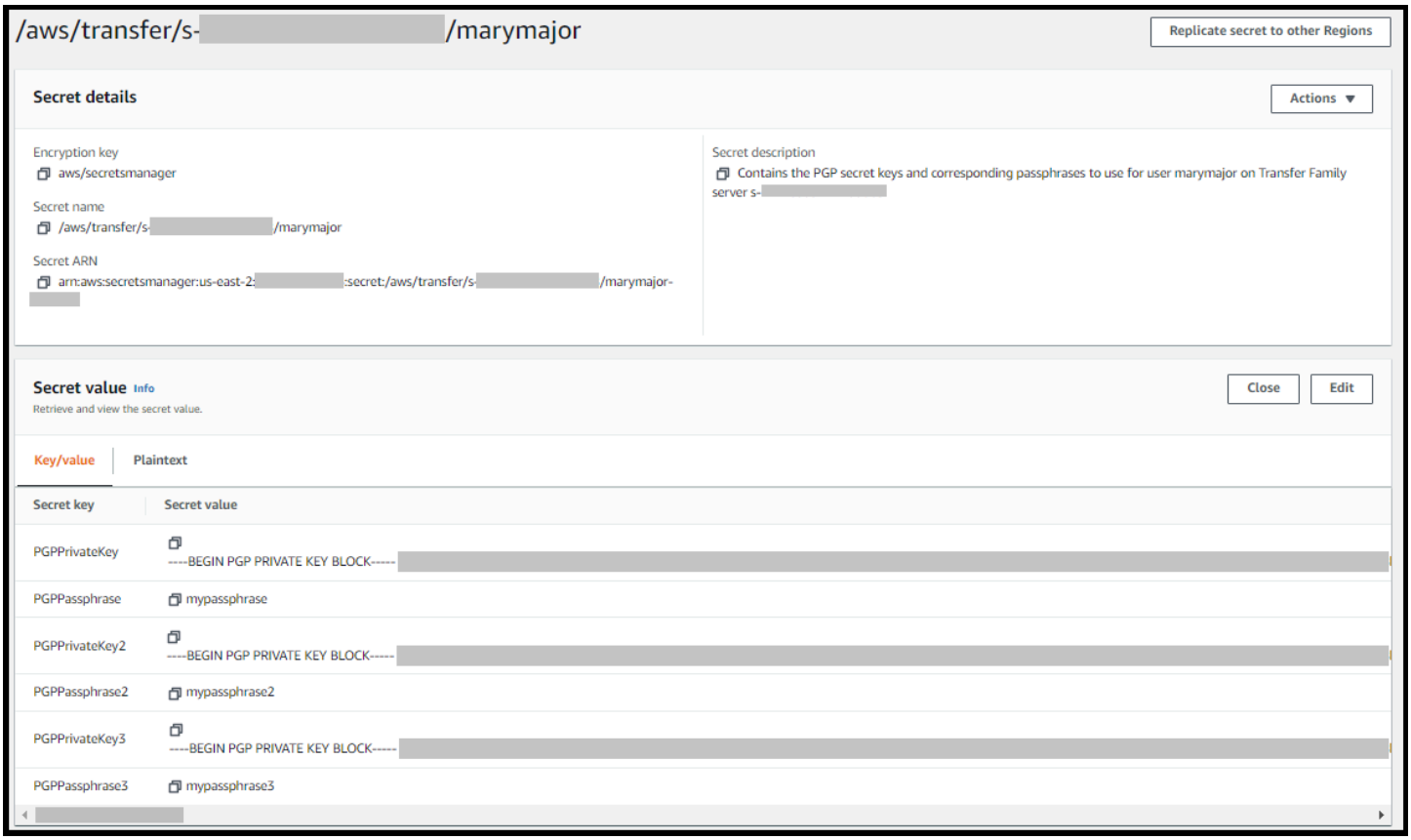
h. 在 [設定密碼] 頁面上，輸入密碼的名稱和說明。

- 如果您要建立預設金鑰，也就是任何「Transfer Family」使用者都可以使用的金鑰，請輸入**aws/transfer/*server-id*/@pgp-default**。取代*server-id*為包含具有解密步驟之工作流程之伺服器的 ID。
- 如果您正在建立供特定 Transfer Family 使用者使用的金鑰，請輸入**aws/transfer/*server-id*/*user-name***。取代*server-id*為包含具有解密步驟之工作流程的伺服器 ID，並取代*user-name*為執行工作流程的使用者名稱。會儲存*user-name*在「Transfer Family」伺服器正在使用的身分識別提供者中。

i. 選擇 [下一步] 並接受 [設定輪替] 頁面上的預設值。然後選擇下一步。

j. 在「檢閱」頁面上，選擇「儲存」以建立並儲存密碼。

下列螢幕擷取畫面顯示特定「Transfer Family」伺服器的使用者**marymajor**詳細資料。此範例顯示三個金鑰及其對應的密碼。

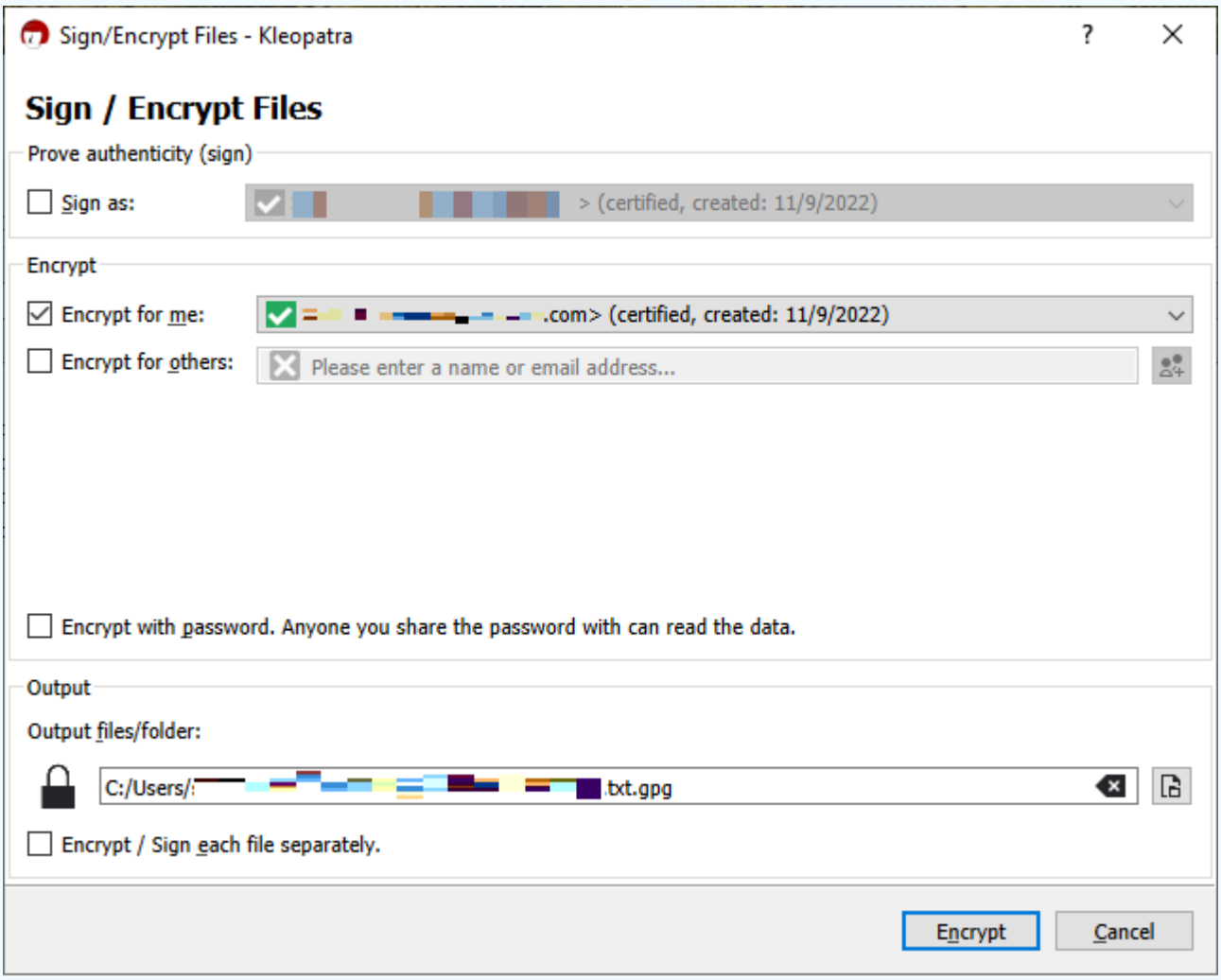


支援的 PGP 用戶端

下列用戶端已通過 Transfer Family 的測試，可用來產生 PGP 金鑰，以及加密您要透過工作流程解密的檔案。

- GPG4 贏 + 克列奧帕特拉。

> **Note**
>
> 當您選取「簽署/加密檔案」時，請務必清除「簽署為：我們目前不支援簽署加密檔案」的選項。



如果您簽署加密檔案，並嘗試使用解密工作流程將其上傳到 Transfer Family 伺服器，您會收到下列錯誤：

```
Encrypted file with signed message unsupported
```

- 主要的 GnuPG 版本：2.4、2.3、2.2、2.0 和 1.4。

請注意，其他 PGP 客戶端可能也可以正常工作，但只有此處提到的客戶端已通過 Transfer Family 進行了測試。

的身分識別與存取管理 AWS Transfer Family

AWS Identity and Access Management (IAM) 可協助系統管理員安全地控制 AWS 資源存取權。 AWS 服務 IAM 管理員控制哪些人可以通過身份驗證 (登入) 和授權 (具有權限) 來使用 AWS Transfer Family 資源。您可以使用 IAM AWS 服務 ，無需額外付費。

主題

- 物件
- 使用身分驗證
- 使用政策管理存取權
- 如何與 IAM AWS Transfer Family 搭配使用
- AWS Transfer Family 以識別為基礎的原則範例
- AWS Transfer Family 基於標籤的策略範例
- 疑難排解 AWS Transfer Family 身分和存取

物件

您使用 AWS Identity and Access Management (IAM) 的方式會有所不同，具體取決於您在進行的工作 AWS Transfer Family。

服務使用者 — 如果您使用 AWS Transfer Family 服務執行工作，則管理員會為您提供所需的認證和權限。當您使用更多 AWS Transfer Family 功能來完成工作時，您可能需要其他權限。了解存取的管理方式可協助您向管理員請求正確的許可。若您無法存取 AWS Transfer Family中的某項功能，請參閱疑難排解 AWS Transfer Family 身分和存取。

服務管理員 — 如果您負責公司的 AWS Transfer Family 資源，您可能擁有完整的存取權 AWS Transfer Family。決定您的服務使用者應該存取哪些 AWS Transfer Family 功能和資源是您的工作。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。若要進一步瞭解貴公司如何搭配使用 IAM AWS Transfer Family，請參閱如何與 IAM AWS Transfer Family 搭配使用。

IAM 管理員：如果您是 IAM 管理員，建議您掌握如何撰寫政策以管理 AWS Transfer Family存取權的詳細資訊。若要檢視可在 IAM 中使用的 AWS Transfer Family 基於身分的政策範例，請參閱。AWS Transfer Family 以識別為基礎的原則範例

使用身分驗證

驗證是您 AWS 使用身分認證登入的方式。您必須以 IAM 使用者身分或假設 IAM 角色進行驗證 (登入 AWS)。 AWS 帳戶根使用者

您可以使用透過 AWS 身分識別來源提供的認證，以聯合身分識別身分登入。 AWS IAM Identity Center (IAM 身分中心) 使用者、貴公司的單一登入身分驗證，以及您的 Google 或 Facebook 登入資料都是聯合身分識別的範例。您以聯合身分登入時，您的管理員先前已設定使用 IAM 角色的聯合身分。當您使 AWS 用同盟存取時，您會間接擔任角色。

根據您的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需登入的詳細資訊 AWS，請參閱AWS 登入 使用者指南中的如何登入您 AWS 帳戶的。

如果您 AWS 以程式設計方式存取，請 AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以使用您的認證以加密方式簽署要求。如果您不使用 AWS 工具，則必須自行簽署要求。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) 來增加帳戶的安全性。如需更多資訊，請參閱 AWS IAM Identity Center 使用者指南中的多重要素驗證和 IAM 使用者指南中的在 AWS中使用多重要素驗證 (MFA)。

AWS 帳戶根使用者

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

聯合身分

最佳作法是要求人類使用者 (包括需要系統管理員存取權的使用者) 使用與身分識別提供者的同盟，才能使用臨時認證 AWS 服務 來存取。

聯合身分識別是來自企業使用者目錄的使用者、Web 身分識別提供者、Identi ty Center 目錄，或使用透過身分識別來源提供的認證進行存取 AWS 服務 的任何使用者。 AWS Directory Service同盟身分存取時 AWS 帳戶，他們會假設角色，而角色則提供臨時認證。

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識別來源中的一組使用者和群組，以便在所有應用

程式 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 使用者是您內部的身分，具 AWS 帳戶 有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。如需更多資訊，請參閱 IAM 使用者指南中的為需要長期憑證的使用案例定期輪換存取金鑰。

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

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供暫時憑證。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 內部具有特定許可的身分。它類似 IAM 使用者，但不與特定的人員相關聯。您可以切換角色，在中暫時擔任 IAM 角色。 AWS Management Console 您可以透過呼叫 AWS CLI 或 AWS API 作業或使用自訂 URL 來擔任角色。如需使用角色的方法更多相關資訊，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 – 若要向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需有關聯合角色的相關資訊，請參閱 IAM 使用者指南中的為第三方身分提供者建立角色。如果您使用 IAM Identity Center，則需要設定許可集。為控制身分驗證後可以存取的內容，IAM Identity Center 將許可集與 IAM 中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的許可集。
- 暫時 IAM 使用者許可 – IAM 使用者或角色可以擔任 IAM 角色來暫時針對特定任務採用不同的許可。
- 跨帳戶存取權 – 您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的委託人) 存取您帳戶中的資源。角色是授予跨帳戶存取權的主要方式。但是，對於某些策略 AWS 服務，您可以將策略直接附加到資源（而不是使用角色作為代理）。若要了解跨帳戶存取權角色和資源型政策間的差異，請參閱 IAM 使用者指南中的 IAM 角色與資源類型政策的差異。

- 跨服務訪問 — 有些 AWS 服務 使用其他 AWS 服務功能。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。
  - 轉寄存取工作階段 (FAS) — 當您使用 IAM 使用者或角色在中執行動作時 AWS，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 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱《轉發存取工作階段》。
  - 服務角色 – 服務角色是服務擔任的 IAM 角色，可代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需更多資訊，請參閱 IAM 使用者指南中的建立角色以委派許可給 AWS 服務。
  - 服務連結角色 — 服務連結角色是連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。
- 在 Amazon EC2 上執行的應用程式 — 您可以使用 IAM 角色管理在 EC2 執行個體上執行的應用程式以及發出 AWS CLI 或 AWS API 請求的臨時登入資料。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體並提供給其所有應用程式，請建立連接至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。如需更多資訊，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。

若要了解是否要使用 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 AWS 過建立原則並將其附加至 AWS 身分識別或資源來控制中的存取。原則是一個物件 AWS ，當與身分識別或資源相關聯時，會定義其權限。 AWS 當主參與者 (使用者、root 使用者或角色工作階段) 提出要求時，評估這些原則。政策中的許可決定是否允許或拒絕請求。大多數原則會 AWS 以 JSON 文件的形式儲存在中。如需 JSON 政策文件結構和內容的更多相關資訊，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。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

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

身分型政策

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。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。受管理的策略是獨立策略，您可以將其附加到您的 AWS 帳戶. 受管政策包括 AWS 受管政策和客戶管理的策略。若要了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限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

資源型政策是位於該服務中的內嵌政策。您無法在以資源為基礎的政策中使用 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 S3 和 Amazon VPC 是支援 ACL 的服務範例。 AWS WAF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 支援其他較不常見的原則類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- 許可界限 – 許可範圍是一種進階功能，可供您設定身分型政策能授予 IAM 實體 (IAM 使用者或角色) 的最大許可。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交

集。會在 Principal 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需許可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。

- 服務控制策略（SCP）— SCP 是 JSON 策略，用於指定中組織或組織單位（OU）的最大權限。AWS Organizations AWS Organizations 是一種用於分組和集中管理您企業擁 AWS 帳戶 有的多個服務。若您啟用組織中的所有功能，您可以將服務控制政策 (SCP) 套用到任何或所有帳戶。SCP 限制成員帳戶中實體的權限，包括每個 AWS 帳戶根使用者帳戶。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。要了解如何在涉及多個政策類型時 AWS 確定是否允許請求，請參閱《IAM 使用者指南》中的政策評估邏輯。

如何與 IAM AWS Transfer Family 搭配使用

在使用 AWS Identity and Access Management (IAM) 管理存取權之前 AWS Transfer Family，您應該瞭解哪些 IAM 功能可搭配使用 AWS Transfer Family。若要深入瞭解如何以 AWS Transfer Family 及其他 AWS 服務如何與 IAM 搭配使用，請參閱 IAM 使用者指南中的與 IAM 搭配使用的AWS 服務。

主題

- AWS Transfer Family 身分型政策
- AWS Transfer Family 資源型政策
- 以 AWS Transfer Family 標籤為基礎的授權
- AWS Transfer Family IAM 角色

AWS Transfer Family 身分型政策

使用 IAM 身分類型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下會允許或拒絕動作。 AWS Transfer Family 支援特定動作、資源及條件索引鍵。若要了解您在 JSON 政策中使用的所有元素，請參閱使用AWS Identity and Access Management 者指南中的 IAM JSON 政策元素參考資料。

動作

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，哪個主體在什麼条件下可以對什麼資源執行哪些動作。

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

政策會使用動作來授予執行相關聯動作的許可。

中的策略動作在動作之前 AWS Transfer Family 使用下列前置詞：`transfer:`例如，若要授與某人建立伺服器的權限，請使用「Transfer Family `CreateServer` API」作業，您可以將`transfer:CreateServer`動作納入他們的政策中。政策陳述式必須包含 `Action` 或 `NotAction` 元素。 AWS Transfer Family 會定義一組自己的動作，來描述您可以使用此服務執行的任務。

若要在單一陳述式中指定多個 動作，請用逗號分隔，如下所示。

```
"Action": [
      "transfer:action1",
      "transfer:action2"
```

您也可以使用萬用字元 (*) 來指定多個動作。例如，如需指定開頭是 `Describe` 文字的所有動作，請包含以下動作：

```
"Action": "transfer:Describe*"
```

若要查看 AWS Transfer Family 動作清單，請參閱服務授權參考 AWS Transfer Family中所定義的動作。

資源

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 (例如列出操作)，請使用萬用字元 (*) 來表示陳述式適用於所有資源。

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

轉移系列伺服器資源具有以下 ARN。

```
arn:aws:transfer:${Region}:${Account}:server/${ServerId}
```

例如，若要在陳述式中指定 s-01234567890abcdef Transfer Family 列伺服器，請使用下列 ARN。

```
"Resource": "arn:aws:transfer:us-east-1:123456789012:server/s-01234567890abcdef"
```

如需 ARN 格式的詳細資訊，請參閱服務授權參考中的 Amazon 資源名稱 (ARN) 或 IAM 使用者指南中的 IAM ARN。

如需指定屬於特定帳戶的所有執行個體，請使用萬用字元 (*)。

```
"Resource": "arn:aws:transfer:us-east-1:123456789012:server/*"
```

某些 AWS Transfer Family 動作會在多個資源上執行，例如 IAM 政策中使用的動作。在這些情況下，您必須使用萬用字元 (*)。

```
"Resource": "arn:aws:transfer:*:123456789012:server/*"
```

在某些情況下，您需要指定一種以上的資源類型，例如，如果您建立允許存取 Transfer Family 伺服器和使用者的策略。若要在單一陳述式中指定多項資源，請使用逗號分隔 ARN。

```
"Resource": [
      "resource1",
      "resource2"
            ]
```

若要查看 AWS Transfer Family 資源清單，請參閱服務授權參考 AWS Transfer Family中所定義的資源類型。

條件索引鍵

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。如果您為單一條件索引鍵指定多個值，請使用邏輯OR運算來 AWS 評估條件。必須符合所有條件，才會授與陳述式的許可。

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

AWS 支援全域條件金鑰和服務特定條件金鑰。若要查看所有 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。

AWS Transfer Family 定義了它自己的一組條件鍵，並且還支持使用一些全局條件鍵。若要查看 AWS Transfer Family 條件索引鍵清單，請參閱服務授權參考 AWS Transfer Family中的條件金鑰。

範例

若要檢視以 AWS Transfer Family 身分為基礎的原則範例，請參閱。AWS Transfer Family 以識別為基礎的原則範例

AWS Transfer Family 資源型政策

以資源為基礎的策略是 JSON 政策文件，指定指定的主體可以在 AWS Transfer Family 資源上以及在何種情況下執行的動作。Amazon S3 支援 Amazon S3 儲存#體的資源型許可政策。資源型政策可讓您依資源將使用許可授予至其他帳戶。您也可以使用以資源為基礎的政策來允許 AWS 服務存取 Amazon S3 儲存#體。

若要啟用跨帳戶存取，您可以指定在其他帳戶內的所有帳戶或 IAM 實體，作為資源型政策的委託人。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當主參與者和資源位於不同的 AWS 帳號中時，您也必須授與主參與者實體存取資源的權限。透過將身分型政策連接到實體來授予許可。不過，如果資源型政策會為相同帳戶中的委託人授予存取，這時就不需要額外的身分型政策。如需詳細資訊，請參閱AWS Identity and Access Management 使用者指南中的 IAM 角色與以資源為基礎的政策有何不同。

Amazon S3 服務僅支援一種類型的資源型政策，稱為儲存#體政策，該政策附加至儲存#體。此原則定義哪些主參與者實體 (帳戶、使用者、角色和同盟使用者) 可以對物件執行動作。

範例

若要檢視 AWS Transfer Family 以資源為基礎的政策範例，請參閱AWS Transfer Family 基於標籤的策略範例。

以 AWS Transfer Family 標籤為基礎的授權

您可以將標籤附加至 AWS Transfer Family 資源，或將要求中的標籤傳遞給 AWS Transfer Family。若要根據標籤控制存取，請使用 `transfer: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。如需如何使用標籤控制資源存取權的相關 AWS Transfer Family 資訊，請參閱AWS Transfer Family 基於標籤的策略範例。

AWS Transfer Family IAM 角色

IAM 角色是您 AWS 帳戶中具有特定許可的實體。

使用臨時登入資料 AWS Transfer Family

您可以搭配聯合使用暫時憑證、擔任 IAM 角色，或是擔任跨帳戶角色。您可以透過呼叫AssumeRole或GetFederation權杖等 AWS STS API 作業來取得臨時安全登入資料。

AWS Transfer Family 支援使用臨時認證。

AWS Transfer Family 以識別為基礎的原則範例

根據預設，IAM 使用者和角色不具備建立或修改 AWS Transfer Family 資源的許可。他們也無法使用 AWS Management Console AWS CLI、或 AWS API 執行工作。IAM 管理員必須建立 IAM 政策，授予使用者和角色在指定資源上執行特定 API 作業的所需許可。管理員接著必須將這些政策連接至需要這些許可的 IAM 使用者或群組。

若要了解如何使用這些 JSON 政策文件範例建立 IAM 身分型政策，請參閱使用AWS Identity and Access Management 者指南中的 JSON 索引標籤上建立政策。

主題

- 政策最佳實務
- 使用 AWS Transfer Family 主控台
- 允許使用者檢視他們自己的許可

政策最佳實務

以身分識別為基礎的政策會決定某人是否可以建立、存取或刪除您帳戶中的 AWS Transfer Family 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 受管原則並邁向最低權限權限 — 若要開始將權限授與使用者和工作負載，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們在您的 AWS 帳戶. 建議您透過定義特定於您使用案例的 AWS 客戶管理政策，進一步降低使用權限。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與對服務動作的存取權 (如透過特定 AWS 服務) 使用 AWS CloudFormation。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。
- 需要多因素身份驗證 (MFA) — 如果您的案例需要 IAM 使用者或根使用者 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。若要在呼叫 API 作業時請求 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。

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

使用 AWS Transfer Family 主控台

若要存取 AWS Transfer Family 主控台，您必須擁有最少一組權限。這些權限必須允許您列出並檢視您 AWS 帳戶中 AWS Transfer Family 資源的詳細資料。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 (IAM 使用者或角色) 而言，主控台就無法如預期運作。如需詳細資訊，請參閱《使用指南》中的〈將權限新增至AWS Identity and Access Management使用者〉。

您不需要為僅對 AWS CLI 或 AWS API 進行呼叫的使用者允許最低主控台權限。反之，只需允許存取符合您嘗試執行之 API 操作的動作就可以了。

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。此原則包含在主控台上或以程式設計方式使用 AWS CLI 或 AWS API 完成此動作的權限。

```
{
    "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": "*"
        }
    ]
}
```

AWS Transfer Family 基於標籤的策略範例

以下是如何根據標籤控制資 AWS Transfer Family 源存取的範例。

使用標籤來控制對 AWS Transfer Family 資源的存取

IAM 政策中的條件是您用來指定 AWS Transfer Family 資源許可的語法的一部分。您可以根據這些 AWS Transfer Family 資源的標籤來控制對資源 (例如使用者、伺服器、角色和其他實體) 的存取。標籤均為金鑰值對。如需有關標記資源的詳細AWS 資訊，請參閱在 AWS 一般參考.

在中 AWS Transfer Family，資源可以有標籤，而某些動作可以包含標籤。建立 IAM 政策時，可使用標籤條件索引鍵來控制以下項目：

- 哪些使用者可以根據資 AWS Transfer Family 源具有的標籤對資源執行動作。
- 可在動作請求中傳遞的標記。
- 請求中是否可使用特定的標籤鍵。

透過使用以標籤為基礎的存取控制，您可以套用比 API 層級更精細的控制。與使用以資源為基礎的存取控制相比，您也可以套用更多的動態控制。您可以根據請求中提供的標籤 (請求標記) 建立允許或拒絕作業的 IAM 政策。您也可以根據正在操作的資源（資源標籤）的標籤建立 IAM 政策。一般來說，資源標籤適用於已在資源上的標籤，請求標籤適用於向資源添加標籤或從資源中刪除標籤時使用。

如需標籤條件金鑰的完整語法和語意，請參閱 IAM 使用者指南中的使用資源標籤控制資源的存取。AWS 如需使用 API Gateway 指定 IAM 政策的詳細資訊，請參閱《API Gateway 開發人員指南》中的使用 IAM 許可控制 API 的存取。

範例 1：根據資源標籤拒絕動作

您可以拒絕要根據標籤對資源執行的動作。下列範例原則會拒絕`TagResource`、`UntagResource`、`StartServer`、`StopServer`、`DescribeServer`和`DescribeUser`作業，如果使用者或伺服器資源標記為索引鍵`stage`和值`prod`。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "transfer:TagResource",
                "transfer:UntagResource",
                "transfer:StartServer",
                "transfer:StopServer",
                "transfer:DescribeServer",
                "transfer:DescribeUser
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/stage": "prod"
                }
            }
        }
    ]
```

```
}
```

範例 2：允許根據資源標籤執行動作

您可以允許根據標籤對資源執行動作。如果使用者或伺服器資源使用索引鍵和值標記DescribeServer，則下列範例原則允TagResource許、、、stage和DescribeUser作業prod。UntagResource StartServer StopServer

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "transfer:TagResource",
                "transfer:UntagResource",
                "transfer:StartServer",
                "transfer:StopServer",
                "transfer:DescribeServer",
                "transfer:DescribeUser
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/stage": "prod"
                }
            }
        }
    ]
}
```

範例 3：拒絕根據要求標記建立使用者或伺服器

下列範例原則包含兩個陳述式。如果標籤的成本中心金鑰沒有值，則第一個陳述式會拒絕所有資源的CreateServer作業。

如果標籤的成本中心索引鍵包含 1、2 或 3 以外的任何其他值，則第二個陳述式會拒絕該CreateServer作業。

> **Note**
>
> 此原則確實允許建立或刪除包含名為costcenter1、2或值的索引鍵的資源3。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "transfer:CreateServer"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "Null":  {
                    "aws:RequestTag/costcenter": "true"
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": "transfer:CreateServer",
            "Resource": [
                "*"
            ],
            "Condition": {
                "ForAnyValue:StringNotEquals": {
                    "aws:RequestTag/costcenter": [
                        "1",
                        "2",
                        "3"
                    ]
                }
            }
        }
    ]
}
```

疑難排解 AWS Transfer Family 身分和存取

使用下列資訊可協助您診斷和修正使用和 IAM 時可能會遇到的 AWS Transfer Family 常見問題。

主題

- 我沒有執行操作的授權 AWS Transfer Family

- 我沒有授權執行 iam：PassRole
- 我想允許 AWS 帳戶以外的人員存取我的 AWS Transfer Family 資源

我沒有執行操作的授權 AWS Transfer Family

如果 AWS Management Console 告訴您您沒有執行動作的授權，則您必須聯絡管理員以尋求協助。您的管理員是為您提供簽署憑證的人員。

以下範例錯誤會在 `mateojackson` IAM 使用者嘗試使用主控台檢視 *`widget`* 的詳細資訊，但卻沒有 `transfer:`*`GetWidget`* 許可時發生。

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

在此情況下，Mateo 會請求管理員更新他的政策，允許他使用 *`my-example-widget`* 動作存取 `transfer;:`*`GetWidget`* 資源。

我沒有授權執行 iam：PassRole

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

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

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

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

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

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

下列範例原則包含將角色傳遞給的權限 AWS Transfer Family。

```
{
   "Version": "2012-10-17",
   "Statement": [
```

```
      { "Action": "iam:PassRole",
        "Resource": "arn:aws::iam::123456789012:role/*",
        "Effect": "Allow"
      }
   ]
}
```

我想允許 AWS 帳戶以外的人員存取我的 AWS Transfer Family 資源

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

如需進一步了解，請參閱以下內容：

- 若要瞭解是否 AWS Transfer Family 支援這些功能，請參閱如何與 IAM AWS Transfer Family 搭配使用。
- 若要了解如何提供對您所擁有資源 AWS 帳戶 的存取權，請參閱《IAM 使用者指南》中您擁有的另一 AWS 帳戶 個 IAM 使用者提供存取權限。
- 若要了解如何將資源存取權提供給第三方 AWS 帳戶，請參閱 IAM 使用者指南中的提供第三方 AWS 帳戶 擁有的存取權。
- 若要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。

符合性驗證 AWS Transfer Family

協力廠商稽核員會評估其安全性與合規性， AWS Transfer Family 做為多個 AWS 合規計畫的一部分。這些包括 SOC、PCI、HIPAA 等。如需完整清單，請參閱合規計劃範圍內的AWS 服務。

如需特定法規遵循計劃範圍內的 AWS 服務清單，請參閱合規計劃範圍內的服務。如需一般資訊，請參閱 AWS 合規計劃。

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

您在使用時的合規責任取決 AWS Transfer Family 於資料的敏感性、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，並提供在上部署以安全性和法規遵循為重點的基準環境的步驟。 AWS
- 建構 HIPAA 安全性與合規性白皮書 — 本白皮書說明公司如何使用建立符合 HIPAA 標準的應用 AWS 程式。
- AWS 合規資源 – 這組手冊和指南可能適用於您的產業和位置。
- AWS Config— 此 AWS 服務評估您的資源配置是否符合內部實踐，行業準則和法規。
- AWS Security Hub— 此 AWS 服務提供安全狀態的全面檢視，協助您檢查您 AWS 是否符合安全性產業標準和最佳做法。

韌性在 AWS Transfer Family

AWS 全球基礎架構是圍繞區 AWS 域和可用區域建立的。 AWS 區域提供多個實體分離和隔離的可用區域，這些區域透過低延遲、高輸送量和高度備援的網路連線。透過可用區域，您所設計與操作的應用程式和資料庫，就能夠在可用區域之間自動容錯移轉，而不會發生中斷。可用區域的可用性、容錯能力和擴充能力，均較單一或多個資料中心的傳統基礎設施還高。

AWS Transfer Family 最多支援 3 個可用區域，並由 auto 擴展的備援叢集支援，適用於您的連線和傳輸要求。

注意下列事項：

- 對於公用端點：
  - 服務內建可用性區域層級備援
  - 每個 AZ 都有備援叢集。
  - 此備援會自動提供
- 如需 Virtual Private Cloud (VPC) 端 (VPC) 中的端點，請參閱在虛擬私有雲中建立伺服器。

另請參閱

- 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。
- 如需如何透過使用延遲型路由來建置更高冗餘並將網路延遲降至最低的範例，請參閱部落格文章將伺服器的網路延遲降至最低。 AWS Transfer Family

基礎結構安全 AWS Transfer Family

作為託管服務， AWS Transfer Family 受到 AWS 全球網絡安全的保護。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 AWS Transfer Family 過網路進行存取。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。

新增 Web 應用程式防火牆

AWS WAF 是一種網絡應用程序防火牆，可幫助保護 Web 應用程序和 API 免受攻擊。您可以使用它來設定一組稱為 Web 存取控制清單 (Web ACL) 的規則，以根據您定義的可自訂 Web 安全規則和條件允許、封鎖或計數 Web 要求。如需詳細資訊，請參閱使用 AWS WAF 來保護您的 API。

若要新增 AWS WAF

1. 在以下網址開啟 API Gateway 主控台：https://console.aws.amazon.com/apigateway/。
2. 在 API 瀏覽窗格中，然後選擇您的自訂身分識別提供者範本。
3. 選擇 Stages (階段)。
4. 在 Stages (階段) 窗格中，選擇階段的名稱。
5. 在 Stage Editor (階段編輯器) 窗格中，選擇 Settings (設定) 標籤。
6. 執行以下任意一項：

   - 在 Web 應用程式防火牆 (WAF) 下，針對 Web ACL，選擇您要與此階段產生關聯的 Web ACL。
   - 如果您需要的 Web ACL 不存在，則需要執行以下操作來建立一個 ACL：

     1. 選擇「建立網頁 ACL」。
     2. 在 AWS WAF 服務首頁上，選擇建立網路 ACL。

3. 在 Web ACL 詳細資料中，對於「名稱」，輸入 Web ACL 的名稱。
4. 在「規則」中選擇「新增規則」，然後選擇「新增我自己的規則和規則群組」。
5. 針對「規則類型」，選擇「IP 集」以識別特定 IP 位址清單。
6. 在「規則」中，輸入規則的名稱。
7. 對於 IP 集，請選擇現有的 IP 集。若要建立 IP 集，請參閱建立 IP 集。
8. 若要將 IP 位址用作原始位址，請在標頭中選擇 IP 位址。
9. 針對 「表頭欄位名稱」，輸入SourceIP。
10. 針對標頭內的位置，選擇 [第一個 IP 位址]。
11. 對於遺失 IP 位址的後援，請根據您要在標頭中處理無效 (或遺失) IP 位址的方式，選擇「符合」或「不相符」。
12. 在「動作」中，選擇 IP 集的處理行動。
13. 對於不符合任何規則的要求的預設 Web ACL 動作，請選擇 [允許] 或 [封鎖]，然後按 [下一步]。
14. 對於步驟 4 和 5，請選擇「下一步」。
15. 在 [檢閱並建立] 中檢閱您的選擇，然後選擇 [建立 Web ACL]。

7. 選擇 Save Changes (儲存變更)。
8. 選擇資源。
9. 針對「動作」，選擇「部署 API」。

如需 AWS Web 應用程式防火牆安全性 AWS Transfer Family 的相關資訊，請參閱 AWS 儲存部落格中AWS Transfer Family 的使 AWS 用應用程式防火牆和 Amazon API Gateway 進行保護。

預防跨服務混淆代理人

混淆代理人問題屬於安全性議題，其中沒有執行動作許可的實體可以強制具有更多許可的實體執行該動作。在中 AWS，跨服務模擬可能會導致混淆的副問題。在某個服務 (呼叫服務) 呼叫另一個服務 (被呼叫服務) 時，可能會發生跨服務模擬。呼叫服務可以被操縱，使用其權限對其他客戶的資源採取行動，以其他方式不應該有其他訪問權限。為了預防這種情況， AWS 提供的工具可協助您保護所有服務的資料，而這些服務主體已獲得您帳戶中資源的存取權。如需此問題的詳細說明，請參閱 IAM 使用者指南中混淆的副問題。

建議您在資源策略中使用aws:SourceArn和aws:SourceAccount全域條件前後關聯索引鍵，以限制 Tran AWS sfer Family 對資源所具有的權限。如果同時使用全域條件內容索引鍵，則在相同政策陳述式中使用 aws:SourceAccount 值和 aws:SourceArn 值中的帳戶時，必須使用相同的帳戶 ID。

防範混淆代理人問題的最有效方法是精確使用您允許的資源 Amazon Resource Name (ARN) 資源。如果您要指定多個資源，請針對 ARN 的未知部分使用萬用字元 (*) 的`aws:SourceArn`全域內容條件索引鍵。例如 `arn:aws:transfer::region::account-id:server/*`。

AWS 「Transfer Family 列」會使用下列類型的角色：

- 使用者角色 — 允許服務管理的使用者存取必要的「Transfer Family」資源。 AWS 「Transfer Family」在「Transfer Family」使用者 ARN 的內容中擔任此角色。
- 存取角色 — 僅提供對正在傳輸的 Amazon S3 檔案的存取權。對於輸入 AS2 傳輸，存取角色使用 Amazon 資源名稱 (ARN) 作為協議。對於輸出 AS2 傳輸，存取角色會使用 ARN 作為連接器。
- 叫用角色 — 可搭配 Amazon API Gateway 作為伺服器的自訂身分提供者使用。「Transfer Family」會在「轉 Transfer Family」伺服器 ARN 的內容中擔任此角色。
- 記錄角色 — 用於將項目記錄到 Amazon CloudWatch。Transfer Family 會使用此角色記錄成功和失敗詳細資料，以及檔案傳輸的相關資訊。「Transfer Family」會在「轉 Transfer Family」伺服器 ARN 的內容中擔任此角色。對於輸出 AS2 傳輸，記錄角色會使用連接器 ARN。
- 執行角色 — 允許「Transfer Family」使用者呼叫和啟動工作流程。「Transfer Family」會在「Transfer Family」工作流程 ARN 的內容中擔任此角色。

如需詳細資訊，請參閱《 IAM 使用者指南》中的 IAM 中的政策和許可。

> **Note**
>
> 在下列範例中，將每個`#########`取代為您自己的資訊。

> **Note**
>
> 在我們的範例中，我們同時使用`ArnLike`和`ArnEquals`。它們在功能上是相同的，因此您可以在構建策略時使用任何一種。「Transfer Family」文件會在條件包含萬用字元`ArnLike`時使用，並`ArnEquals`指出完全相符的條件。

AWS Transfer Family 用戶角色跨服務混淆副預防

下列範例原則允許帳戶中任何伺服器的任何使用者擔任該角色。

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Service": "transfer.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "account-id"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:transfer:region:account-id:user/*"
                }
            }
        }
    ]
}
```

下列範例原則可讓特定伺服器的任何使用者擔任該角色。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Service": "transfer.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "account-id"
                },
                "ArnEquals": {
                    "aws:SourceArn": "arn:aws:transfer:region:account-id:user/server-
id/*"
                }
            }
        }
```

```
    ]
}
```

下列範例原則可讓特定伺服器的特定使用者擔任該角色。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Service": "transfer.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:transfer:region:account-id:user/server-
id/user-name"
                }
            }
        }
    ]
}
```

AWS Transfer Family 工作流程角色跨服務混淆副預防

下列範例原則允許帳戶中的任何工作流程擔任該角色。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Service": "transfer.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "account-id"
                },
```

```
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:transfer:region:account-id:workflow/*"
                }
            }
        }
    ]
}
```

下列範例原則允許特定工作流程擔任該角色。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Service": "transfer.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:transfer:region:account-
id:workflow/workflow-id"
                }
            }
        }
    ]
}
```

AWS Transfer Family 記錄和調用角色跨服務混淆副預防

> **Note**
>
> 下列範例可用於記錄和叫用角色。
> 在這些範例中，如果伺服器沒有附加任何工作流程，您可以移除工作流程的 ARN 詳細資料。

下列範例記錄/叫用策略允許帳戶中的任何伺服器 (和工作流程) 擔任該角色。

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAllServersWithWorkflowAttached",
            "Effect": "Allow",
            "Principal": {
                "Service": "transfer.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "account-id"
                },
                "ArnLike": {
                   "aws:SourceArn": [
                     "arn:aws:transfer:region:account-id:server/*",
                     "arn:aws:transfer:region:account-id:workflow/*"
                   ]
                }
            }
        }
    ]
}
```

下列範例記錄/呼叫原則可讓特定伺服器 (和工作流程) 擔任該角色。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSpecificServerWithWorkflowAttached",
            "Effect": "Allow",
            "Principal": {
                "Service": "transfer.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "account-id"
                },
                "ArnEquals": {
                   "aws:SourceArn": [
                       "arn:aws:transfer:region:account-id:server/server-id",
```

```
                    "arn:aws:transfer:region:account-id:workflow/workflow-id"
                ]
            }
        }
    }
  ]
}
```

AWSAWS Transfer Family 的受管理政策

若要新增使用者、群組和角色的權限，使用 AWS 受管理的原則比自己撰寫原則更容易。建立 AWS Identity and Access Management (IAM) 客戶受管政策需要時間和專業知識，這些政策僅為您的團隊提供所需的許可。若要快速開始使用，您可以使用我們的 AWS 受管政策。這些政策涵蓋常見的使用案例，並可在您的 AWS 帳戶中使用。如需 AWS 受管政策的更多相關資訊，請參閱 IAM 使用者指南中的 AWS 受管政策。如需所有 AWS 受管理策略的詳細清單，請參閱受AWS 管政策參考指南。

AWS 服務會維護和更新 AWS 受管理的策略。您無法變更 AWS 受管理原則中的權限。服務偶爾會在 AWS 受管政策中新增其他許可以支援新功能。此類型的更新會影響已連接政策的所有身分識別 (使用者、群組和角色)。當新功能啟動或新操作可用時，服務很可能會更新 AWS 受管政策。服務不會從 AWS 受管理的政策移除權限，因此政策更新不會破壞您現有的權限。

此外，還 AWS 支援跨多個服務之工作職能的受管理原則。例如，`ReadOnlyAccess` AWS 受管理的策略提供對所有 AWS 服務和資源的唯讀存取。當服務啟動新功能時，會為新作業和資源新 AWS 增唯讀權限。如需任務職能政策的清單和說明，請參閱 IAM 使用者指南中有關任務職能的AWS 受管政策。

AWS 受管理的策略： AWSTransferConsoleFullAccess

此`AWSTransferConsoleFullAccess`原則可透過 AWS 管理主控台提供「Transfer Family」的完整存取權。

許可詳細資訊

此政策包含以下許可。

- `acm:ListCertificates`— 授予擷取憑證 Amazon 資源名稱 (ARN) 清單和每個 ARN 網域名稱的權限。
- `ec2:DescribeAddresses`— 授予描述一或多個彈性 IP 位址的權限。
- `ec2:DescribeAvailabilityZones`— 授予描述您可用之一或多個可用區域的權限。
- `ec2:DescribeNetworkInterfaces`— 授予描述一或多個彈性網路介面的權限。

- ec2:DescribeSecurityGroups— 授予描述一或多個安全群組的權限。
- ec2:DescribeSubnets— 授予描述一或多個子網路的權限。
- ec2:DescribeVpcs— 授予描述一或多個虛擬私有雲 (VPC) 的權限。
- ec2:DescribeVpcEndpoints— 授與描述一或多個 VPC 端點的權限。
- health:DescribeEventAggregates— 傳回每個事件類型 (問題、排程變更和帳戶通知) 的事件數目。
- iam:GetPolicyVersion— 授與擷取指定受管理策略版本 (包括策略文件) 相關資訊的權限。
- iam:ListPolicies— 授與列出所有受管理策略的權限。
- iam:ListRoles— 授予列出具有指定路徑前置詞的 IAM 角色的權限。
- iam:PassRole— 授予將 IAM 角色傳遞給「Transfer Family」的權限。如需詳細資訊，請參閱授與使用者將角色傳遞給 AWS 服務.
- route53:ListHostedZones— 授予取得與目前相關聯之公用和私有託管區域清單的權限 AWS 帳戶。
- s3:ListAllMyBuckets— 授予列出要求已驗證寄件者所擁有之所有值區的權限。
- transfer:*— 授予 Transfer Family 資源的訪問權限。星號 (*) 會授予對所有資源的存取權。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "transfer.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "acm:ListCertificates",
                "ec2:DescribeAddresses",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeSecurityGroups",
```

```
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeVpcEndpoints",
                "health:DescribeEventAggregates",
                "iam:GetPolicyVersion",
                "iam:ListPolicies",
                "iam:ListRoles",
                "route53:ListHostedZones",
                "s3:ListAllMyBuckets",
                "transfer:*"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS 受管理的策略： AWSTransferFullAccess

該AWSTransferFullAccess政策提供對 Transfer Family 服務的完全訪問權限。

許可詳細資訊

此政策包含以下許可。

- transfer:*— 授予訪問 Transfer Family 資源的權限。星號 (*) 會授予對所有資源的存取權。
- iam:PassRole— 授予將 IAM 角色傳遞給「Transfer Family」的權限。如需詳細資訊，請參閱授與使用者將角色傳遞給 AWS 服務.
- ec2:DescribeAddresses— 授予描述一或多個彈性 IP 位址的權限。
- ec2:DescribeNetworkInterfaces— 授予描述一個或多個網絡接口的權限。
- ec2:DescribeVpcEndpoints— 授與描述一或多個 VPC 端點的權限。

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

```
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "transfer.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeAddresses"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS 受管理的策略： AWSTransferLoggingAccess

此AWSTransferLoggingAccess政策會授予 AWS Transfer Family 完整存取權，以建立記錄串流和群組，並將記錄事件放入您的帳戶。

許可詳細資訊

此原則包含的下列權限 Amazon CloudWatch Logs。

- CreateLogStream— 授與主體建立記錄資料流的權限。
- DescribeLogStreams— 授與主參與者列出記錄群組之記錄資料流的權限。
- CreateLogGroup— 授與主參與者建立記錄群組的權限。
- PutLogEvents— 授與主參與者將記錄事件批次上載至記錄串流的權限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
```

```
                "logs:CreateLogStream",
                "logs:DescribeLogStreams",
                "logs:CreateLogGroup",
                "logs:PutLogEvents"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS 受管理的策略： AWSTransferReadOnlyAccess

此原AWSTransferReadOnlyAccess則提供 Transfer Family 服務的唯讀存取權。

許可詳細資訊

此原則包含「Transfer Family 列」的下列權限。

- DescribeUser— 授與主參與者檢視使用者描述的權限。
- DescribeServer— 授與主參與者檢視伺服器描述的權限。
- ListUsers— 授與主參與者列出伺服器使用者的權限。
- ListServers— 授與主參與者列出帳戶伺服器的權限。
- TestIdentityProvider— 授與主體的權限，以測試已配置的身分識別提供者是否正確設定。
- ListTagsForResource— 授與主參與者列出資源標籤的權限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "transfer:DescribeUser",
                "transfer:DescribeServer",
                "transfer:ListUsers",
                "transfer:ListServers",
                "transfer:TestIdentityProvider",
                "transfer:ListTagsForResource"
            ],
```

```
            "Resource": "*"
        }
    ]
}
```

AWS 將 Family 更新轉移至 AWS 受管理的

檢視有關 AWS Transfer Family AWS 受管理政策更新的詳細資料，因為此服務開始追蹤這些變更。如需有關此頁面變更的自動提醒，請訂閱 的文件歷史記錄 AWS Transfer Family 頁面的 RSS 摘要。

變更	描述	日期
文件更新	新增每個「Transfer Family」管理政策的區段。	2022 年 1 月 27 日
AWSTransferReadOnlyAccess – 更新現有政策	AWS Transfer Family 已新增權限以允許讀取原則 AWS Managed Microsoft AD。	2021 年 9 月 30 日
AWS Transfer Family 開始追蹤變更	AWS Transfer Family 已開始追蹤其 AWS 受管理政策的變更。	2021 年 6 月 15 日

疑難排 AWS Transfer Family

使用下列資訊可協助您診斷及修正使用時可能會遇到的常見問題 AWS Transfer Family。

如需 Transfer Family 中 IAM 的相關問題，請參閱疑難排解 AWS Transfer Family 身分和存取。

主題

- 服務管理使用者疑難
- Amazon API Gateway 問題的疑難
- 疑難排解加密 Amazon S3 儲存貯體的政策
- 排解驗證問題
- 排解受管理工作流程
- 疑難排解工作流程解
- 解決 Amazon EFS 問題
- 疑難排解測試身分提供者
- 疑難排解為 SFTP 連接器新增受信任的主機金鑰
- 排解檔案上傳問題
- ResourceNotFound例外疑難排
- SFTP 連接器問題疑難排解
- 疑難排解 AS2 問題

服務管理使用者疑難

本節說明下列問題的可能解決方案。

主題

- 疑難排解 Amazon EFS 服務受管使用
- 公開金鑰主體太長的疑難排解
- 疑難排解無法新增 SSH 公開金鑰

疑難排解 Amazon EFS 服務受管使用

Description

您執行命sftp令，但不會出現提示，而是會看到下列訊息：

```
Couldn't canonicalize: Permission denied
           Need cwd
```

原因

您的 AWS Identity and Access Management (IAM) 使用者角色沒有存取 Amazon Elastic File System (Amazon EFS) 的權限。

解決方案

增加使用者角色的原則權限。您可以新增受 AWS 管理的策略，例如AmazonElasticFileSystemClientFullAccess。

公開金鑰主體太長的疑難排解

Description

當您嘗試建立服務管理的使用者時，您會收到下列錯誤：

```
Failed to create user (1 validation error detected:
'sshPublicKeyBody' failed to satisfy constraint: Member must have length less than or
 equal to 2048)
```

原因

您可能正在為公開金鑰內文輸入 PGP 金鑰，而且 AWS Transfer Family 不支援服務管理使用者的 PGP 金鑰。

解決方案

如果 PGP 金鑰是基於 RSA 的，您可以將其轉換為 PEM 格式。例如，Ubuntu 在這裡提供了一個轉換工具：https://manpages.ubuntu.com/manpages/xenial/man1/openpgp2ssh.1.html

疑難排解無法新增 SSH 公開金鑰

Description

當您嘗試為服務管理的使用者新增公開金鑰時，您會收到下列錯誤：

```
Failed to add SSH public key (Unsupported or invalid SSH public key format)
```

原因

您可能嘗試匯入 SSH2 格式的公開金鑰， AWS Transfer Family 但不支援服務管理使用者使用 SSH2 格式的公開金鑰。

解決方案

您需要將密鑰轉換為 OpenSSH 格式。此程序會在中描述將 SSH2 公開金鑰轉換為 PEM 格式。

Amazon API Gateway 問題的疑難

本節說明下列 API Gateway 問題的可能解決方案。

主題

- 驗證失敗次數太多
- 連接已關閉

驗證失敗次數太多

Description

當您嘗試使用安全殼層 (SSH) 檔案傳輸通訊協定 (SFTP) 連線到伺服器時，您會收到下列錯誤：

```
Received disconnect from 3.15.127.197 port 22:2: Too many authentication failures
Authentication failed.
Couldn't read packet: Connection reset by peer
```

原因

您可能輸入的使用者密碼不正確。請再試一次，輸入正確的密碼。

如果密碼正確，則問題可能是因為無效的 Amazon 資源名稱 (ARN) 角色所造成。若要確認這是問題所在，請測試伺服器的身分識別提供者。如果您看到類似下列內容的回應，則角色 ARN 僅為預留位置，如所有零的角色 ID 值所指出：

```
{
    "Response": "{\"Role\": \"arn:aws:iam::000000000000:role/MyUserS3AccessRole\",
\"HomeDirectory\": \"/\"}",
    "StatusCode": 200,
```

```
    "Message": "",
    "Url": "https://api-gateway-ID.execute-api.us-east-1.amazonaws.com/prod/
servers/transfer-server-ID/users/myuser/config"
}
```

解決方案

將預留位置角色 ARN 取代為具有存取伺服器權限的實際角色。

更新角色

1. 開啟主 AWS CloudFormation 控台，網址為 https://console.aws.amazon.com/cloudformation。
2. 在左側導覽窗格中，選擇 Stacks (堆疊)。
3. 在「堆疊」清單中，選擇您的堆疊，然後選擇「參數」標籤。
4. 選擇更新。在 [更新堆疊] 頁面上，選擇 [使用目前的範本]，然後選擇 [下一步]。
5. 請以具有足夠權限存取您的 Transfer Family 伺服器的角色 ARN 取代UserRoleArn。

   > **Note**
   >
   > 若要授與必要的權限，您可以將AmazonAPIGatewayAdministrator和受AmazonS3FullAccess管理的政策新增至您的角色。

6. 選擇 [下一步]，然後再選擇 [下一步]。在 [檢閱##] 頁面上，選取 [我確認 AWS CloudFormation 可能會建立 IAM 資源]，然後選擇 [更新堆疊]。

連接已關閉

Description

當您嘗試使用安全殼層 (SSH) 檔案傳輸通訊協定 (SFTP) 連線到伺服器時，您會收到下列錯誤：

```
Connection closed
```

原因

造成此問題的一個可能原因是您的 Amazon CloudWatch 記錄角色與 Transfer Family 沒有信任關係。

解決方案

請確定伺服器的記錄角色與「Transfer Family」具有信任關係。如需詳細資訊，請參閱 建立信任關係。

疑難排解加密 Amazon S3 儲存貯體的政策

Description

您有一個加密的 Amazon S3 儲存貯體，用作 Transfer Family 伺服器的儲存體。如果您嘗試將檔案上傳到伺服器，則會收到錯誤訊息`Couldn't close file: Permission denied`。

如果您檢視伺服器記錄檔，您會看到下列錯誤：

```
ERROR Message="Access denied" Operation=CLOSE Path=/bucket/user/test.txt BytesIn=13
ERROR Message="Access denied"
```

原因

IAM 使用者的政策沒有存取加密儲存貯體的權限。

解決方案

您必須在原則中指定其他權限，才能授與所需的 AWS Key Management Service (AWS KMS) 權限。如需詳細資訊，請參閱 Amazon S3 中的資料加密。

排解驗證問題

本節說明下列驗證問題的可能解決方案。

主題

- 驗證失敗 — SS/sFTP
- 受管理 AD 不相符範圍問題
- 其他驗證問題

驗證失敗 — SS/sFTP

Description

當您嘗試使用安全殼層 (SSH) 檔案傳輸通訊協定 (SFTP) 連線到伺服器時，您會收到類似下列內容的訊息：

```
Received disconnect from 3.130.115.105 port 22:2: Too many authentication failures
  Authentication failed.
```

> **Note**
>
> 如果您正在使用 API Gateway 並收到此錯誤訊息，請參閱驗證失敗次數太多。

原因

您尚未為使用者新增 RSA key pair，因此您必須改為使用密碼進行驗證。

解決方案

當您執行命sftp令時，請指定-o PubkeyAuthentication=no選項。此選項會強制系統要求您的密碼。例如：

```
sftp -o PubkeyAuthentication=no sftp-user@server-id.server.transfer.region-
id.amazonaws.com
```

受管理 AD 不相符範圍問題

Description

使用者的範圍及其群組範圍必須相符。它們必須同時位於預設範圍中，否則兩者都必須位於受信任的範圍中。

原因

如果使用者及其群組不相符，則無法透過 Transfer Family 驗證該使用者。如果您測試使用者的身分識別提供者，您會收到錯誤訊息：找不到使用者群組的相關存取權。

解決方案

參照使用者範圍中符合群組範圍 (預設或信任) 的群組。

其他驗證問題

Description

您收到身份驗證錯誤，其他故障排除都不起作用

原因

您可能已經為包含前置或結尾斜線 (/) 的邏輯目錄指定了目標。

解決方案

更新您的邏輯目錄目標，以確保它以斜線開頭，並且不包含尾隨斜線。例如，/DOC-EXAMPLE-BUCKET/images是可以接受的DOC-EXAMPLE-BUCKET/images，但不/DOC-EXAMPLE-BUCKET/images/是。

排解受管理工作流程

本節說明下列工作流程問題的可能解決方案。

主題

- 使用 Amazon 疑難排解工作流程相關錯誤 CloudWatch
- 排解工作流程複製錯

使用 Amazon 疑難排解工作流程相關錯誤 CloudWatch

Description

如果您的工作流程發生問題，可以使 CloudWatch 用 Amazon 調查原因。

原因

可能有幾個原因。使用 Amazon CloudWatch 日誌進行調查。

解決方案

「Transfer Family」會將工作流程執行狀態發出至 CloudWatch 記錄 CloudWatch 記錄檔中可能會出現下列類型的工作流程錯誤：

- `"type": "StepErrored"`
- `"type": "ExecutionErrored"`
- `"type": "ExecutionThrottled"`
- `"Service failure on starting workflow"`

您可以使用不同的篩選器和模式語法來篩選工作流程的執行記錄。例如，您可以在記錄檔中建立 CloudWatch 記錄篩選器，以擷取包含ExecutionErrored訊息的工作流程執行記錄。如需詳細資訊，請參閱 Amazon CloudWatch 日誌使用者指南中的使用訂閱即時處理日誌資料和篩選器和模式語法。

StepErrored

```
2021-10-29T12:57:26.272-05:00
            {"type":"StepErrored","details":
{"errorType":"BAD_REQUEST","errorMessage":"Cannot
            tag Efs file","stepType":"TAG","stepName":"successful_tag_step"},
            "workflowId":"w-
abcdef01234567890","executionId":"1234abcd-56ef-78gh-90ij-1234klmno567",
            "transferDetails":
{"serverId":"s-1234567890abcdef0","username":"lhr","sessionId":"1234567890abcdef0"}
```

此處StepErrored指出工作流程中的某個步驟已產生錯誤。在單一工作流程中，您可以設定多個步驟。此錯誤會告訴您發生錯誤的步驟，並提供錯誤訊息。在此特定範例中，步驟設定為標記檔案；不過，不支援在 Amazon EFS 檔案系統中標記檔案，因此步驟產生錯誤。

ExecutionErrored

```
2021-10-29T12:57:26.618-05:00
            {"type":"ExecutionErrored","details":{},"workflowId":"w-w-
abcdef01234567890",
            "executionId":"1234abcd-56ef-78gh-90ij-1234klmno567","transferDetails":
{"serverId":"s-1234567890abcdef0",
            "username":"lhr","sessionId":"1234567890abcdef0"}}
```

當工作流程無法執行任何步驟時，會產生ExecutionErrored訊息。例如，如果您已在指定的工作流程中設定單一步驟，而且該步驟無法執行，則整體工作流程會失敗。

執行限制

如果工作流程的觸發速度超過系統所能支援的速度，則會限制執行。此記錄訊息指出您必須降低工作流程的執行速率。如果您無法縮小工作流程執行率，請通過 Contact 聯繫 AWS Support 。 AWS

啟動工作流程時服務失敗

每當您從伺服器中移除工作流程並以新工作流程取代，或更新伺服器組態 (這會影響工作流程的執行角色) 時，您必須等待大約 10 分鐘，才能執行新的工作流程。Transfer Family 伺服器會快取工作流程詳細資料，伺服器需要 10 分鐘才能重新整理其快取。

此外，您必須登出任何作用中的 SFTP 工作階段，然後在 10 分鐘的等待期後重新登入，以查看變更。

排解工作流程複製錯

Description

如果您執行的工作流程包含複製上傳檔案的步驟，可能會遇到下列錯誤：

```
{
  "type": "StepErrored", "details": {
    "errorType": "BAD_REQUEST", "errorMessage": "Bad Request (Service: Amazon S3;
 Status Code: 400; Error Code: 400 Bad Request;
    Request ID: request-ID; S3 Extended Request ID: request-ID Proxy: null)",
 "stepType": "COPY", "stepName": "copy-step-name" },
  "workflowId": "workflow-ID",
  "executionId": "execution-ID",
  "transferDetails": {
     "serverId": "server-ID",
     "username": "user-name",
     "sessionId": "session-ID"
  }
}
```

原因

來源檔案位於與目標儲存貯體 AWS 區域 不同的 Amazon S3 儲存貯體中。

解決方案

如果您要執行的工作流程包含複製步驟，請確定來源值區和目的地值區位於相同的值區中 AWS 區域。

疑難排解工作流程解

本節說明下列加密工作流程問題的可能解決方案。

主題

- 疑難排解簽署加密檔案的錯誤
- 疑難排解 FIPS 演算法的錯誤

疑難排解簽署加密檔案的錯誤

Description

您的解密工作流程失敗，您收到下列錯誤：

```
"Encrypted file with signed message unsupported"
```

原因

Transfer Family 目前不支援簽署加密檔案。

解決方案

在您的 PGP 客戶端中，如果有簽署加密文件的選項，請確保清除選擇，因為 Transfer Family 目前不支持對加密文件進行簽名。

疑難排解 FIPS 演算法的錯誤

Description

您的解密工作流程失敗，且記錄訊息類似下列：

```
{
   "type": "StepErrored",
   "details": {
      "errorType": "BAD_REQUEST",
      "errorMessage": "File encryption algorithm not supported with FIPS mode
 enabled.",
      "stepType": "DECRYPT",
      "stepName": "step-name"
   },
   "workflowId": "workflow-ID",
   "executionId": "execution-ID",
   "transferDetails": {
      "serverId": "server-ID",
      "username": "user-name",
      "sessionId": "session-ID"
   }
}
```

原因

您的 Transfer Family 伺服器已啟用 FIPS 模式和關聯的「解密」工作流程步驟。在上傳到 Transfer Family 伺服器之前加密檔案時，加密用戶端可能會產生使用非 FIP 核准的對稱加密演算法的加密檔案。在這種情況下，工作流程無法解密檔案。在下列範例中，GnuPG 2.4.0 版使用 OCB (非 FIPS 區塊加密模式) 來加密檔案：這會導致工作流程失敗。

解決方案

您必須編輯用來加密檔案的 GPG 金鑰，然後再重新加密這些金鑰。下列程序說明您必須採取的步驟。

若要編輯您的 PGP 金鑰

1. 透過執行識別您必須編輯的金鑰 `gpg --list-keys`

   這將返回鍵的列表。每個金鑰都有類似下列內容的詳細資訊：

   ```
   pub   ed25519 2022-07-07 [SC]
         wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
   uid           [ultimate] Mary Major <marymajor@example.com>
   sub   cv25519 2022-07-07 [E]
   ```

2. 識別您要編輯的金鑰。在上一個步驟中顯示的範例中，ID 為`wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`。
3. 執行 `gpg --edit-key wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`。

   系統會回應 GnuPG 程式和指定金鑰的詳細資訊。
4. 出現提`gpg>`示時，輸入`showpref`。會傳回下列詳細資訊：

   ```
   [ultimate] (1). Mary Major <marymajor@example.com>
      Cipher: AES256, AES192, AES, 3DES
      AEAD: OCB
      Digest: SHA512, SHA384, SHA256, SHA224, SHA1
      Compression: ZLIB, BZIP2, ZIP, Uncompressed
      Features: MDC, AEAD, Keyserver no-modify
   ```

   請注意，會列出儲存在金鑰上的慣用演算法。
5. 我們希望編輯密鑰以保留除 OCB 以外的所有算法。執行命`setpref`令，指定要保留的所有演算法：

   ```
   gpg> setpref AES256, AES192,AES,3DES,SHA512, SHA384, SHA256, SHA224, SHA1,ZLIB,
    BZIP2, ZIP, Uncompressed
   ```

這將返回以下詳細信息：

```
Set preference list to:
     Cipher: AES256, AES192, AES, 3DES
     AEAD:
     Digest: SHA512, SHA384, SHA256, SHA224, SHA1
     Compression: ZLIB, BZIP2, ZIP, Uncompressed
     Features: MDC, Keyserver no-modify
Really update the preferences? (y/N)
```

6. 輸入y以更新，然後在提示確認變更時輸入密碼。
7. 儲存變更。

```
gpg> save
```

在重新執行解密工作流程之前，您必須使用已編輯的金鑰重新加密檔案。

解決 Amazon EFS 問題

本節說明下列 Amazon EFS 問題的可能解決方案。

主題

- 排解遺失的 POSIX 設定檔
- 使用 Amazon EFS 疑難排解邏輯目錄

排解遺失的 POSIX 設定檔

Description

如果您正在為伺服器使用 Amazon EFS 儲存，並且使用自訂身分供應商，則必須為您的 AWS Lambda 函數提供 POSIX 設定檔。

原因

一個可能的原因是，我們為建立 AWS Lambda支援的 Amazon API Gateway 方法所提供的範本目前不包含 POSIX 資訊。

如果您確實提供了 POSIX 信息，則轉移系列可能無法正確解析您用於提供 POSIX 信息的格式。

解決方案

請確定您提供 JSON 元素以轉移`PosixProfile`參數的族群。

例如，如果您使用的是 Python，則可以在解析`PosixProfile`參數的位置添加以下行：

```
if PosixProfile:
        response_data["PosixProfile"] = json.loads(PosixProfile)
```

或者，在中 JavaScript，您可以添加以下行，其中*`uid-value`*和*`gid-value`*是 0 或更大的整數，分別代表用戶 ID（UID）和組 ID（GID）：

```
PosixProfile: {"Uid": uid-value, "Gid": gid-value},
```

這些程式碼範例會將`PosixProfile`參數以 JSON 物件的形式傳送至「轉移系列」，而不是以字串形式傳送。

此外，在中 AWS Secrets Manager，您必須儲存`PosixProfile`參數，如下所示。將您*`your-gid`*的 GID *`your-uid`* 和 UID 的實際值替換為和。

```
{"Uid": your-uid, "Gid": your-gid, "SecondaryGids": []}
```

使用 Amazon EFS 疑難排解邏輯目錄

Description

如果使用者的主目錄不存在，且他們執行`ls`命令，則系統回應如下：

```
sftp> ls
remote readdir ("/"): No such file or directory
```

原因

如果您的 Transfer Family 伺服器使用 Amazon EFS，則必須使用讀取和寫入存取權建立使用者的主目錄，使用者才能在其邏輯主目錄中工作。使用者無法自行建立此目錄，因為他們缺乏邏輯主目錄的權限。`mkdir`

解決方案

具有父目錄管理存取權的使用者需要建立使用者的邏輯主目錄。

疑難排解測試身分提供者

Description

如果您使用主控台或 TestIdentityProvider API 呼叫來測試身分識別提供者，則Response欄位為空白。例如：

```
{
    "Response": "{}",
    "StatusCode": 200,
    "Message": ""
}
```

原因

最有可能的原因是驗證失敗，因為使用者名稱或密碼不正確。

解決方案

請確定您使用的是正確的使用者認證，並在必要時更新使用者名稱或密碼。

疑難排解為 SFTP 連接器新增受信任的主機金鑰

Description

當您建立或編輯 SFTP 連接器，並新增受信任的主機金鑰時，您會收到下列錯誤：`Failed to edit connector details (Invalid host key format.)`

原因

如果您貼上正確的公開金鑰，問題可能是您已包含金鑰的comment部分。 AWS Transfer Family 目前不接受密鑰的註釋部分。

解決方案

當您將金鑰貼入文字欄位時，請刪除金鑰的註解部分。例如，假設您的金鑰看起來類似下列內容：

```
ssh-rsa AAAA...== marymajor@dev-dsk-marymajor-1d-c1234567.us-east-1.amazon.com
```

移除字元後面的文==字，並且只貼到金鑰的部分，直到並包含在內==。

```
ssh-rsa AAAA...==
```

排解檔案上傳問題

本節說明下列檔案上傳問題的可能解決方案。

主題

- 疑難排解 Amazon S3 檔案上傳錯誤
- 疑難排解無法讀取的檔名

疑難排解 Amazon S3 檔案上傳錯誤

Description

當您嘗試使用 Transfer Family 列將檔案上傳到 Amazon S3 儲存時，您會收到下列錯誤訊息：AWS 傳輸不支援 S3 物件的隨機存取寫入。

原因

當您將 Amazon S3 用於伺服器儲存時，Transfer Family 不支援單一傳輸的多個連線。

解決方案

如果您的 Transfer Family 伺服器使用 Amazon S3 進行儲存，請停用用戶端軟體的任何選項，這些選項提及使用多個連線進行單次傳輸。

疑難排解無法讀取的檔名

Description

您在某些上傳的文件中看到損壞的文件名。使用者有時會遇到 FTP 和 SFTP 傳輸問題，這些檔案名稱中的某些字元會造成混亂，例如變音符號、重音字母或某些指令碼，例如中文或阿拉伯文。

原因

雖然 FTP 和 SFTP 通訊協定可以允許用戶端協商檔案名稱的字元編碼，但 Amazon S3 和 Amazon EFS 卻無法交涉。相反地，它們需要 UTF-8 字元編碼。因此，某些字元無法正確呈現。

解決方案

若要解決這個問題，請檢閱用戶端應用程式的檔案名稱字元編碼，並確定其設定為 UTF-8。

ResourceNotFound例外疑難排

Description

您會收到無法找到資源的錯誤訊息。例如，如果您執行UpdateServer，您可能會收到下列錯誤：

```
An error occurred (ResourceNotFoundException) when calling the UpdateServer operation:
 Unknown server
```

原因

收到ResourceNotFoundException訊息的原因有幾個。在大多數情況下，您在 API 命令中指定的資源不存在。如果您確實指定了現有資源，則最可能的原因是您的預設區域與資源的區域不同。例如，如果您的預設區域是 us-east-1，而您的 Transfer Family 伺服器位於 us-east-2 中，您將會收到一個未知的資源例外狀況。

有關設定預設區域的詳細資訊，請參閱使用快速設定aws configure。

解決方案

在 API 命令中添加一個區域參數，以明確指定在哪裡可以找到特定資源。

```
aws transfer -describe-server --server-id server-id --region us-east-2
```

SFTP 連接器問題疑難排解

本節說明下列 SFTP 連接器問題的可能解決方案。

主題

- 金鑰交涉失敗
- 其他 SFTP 連接器問題

金鑰交涉失敗

Description

您會收到金鑰交換交涉失敗的錯誤。例如：

```
Key exchange negotiation failed due to incompatible host key algorithms.
Client offered: [ecdsa-sha2-nistp256, ecdsa-sha2-nistp384,
ecdsa-sha2-nistp521, rsa-sha2-512, rsa-sha2-256] Server offered: [ssh-rsa]
```

原因

此錯誤是因為伺服器支援的主機金鑰演算法與連接器支援的主機金鑰演算法之間沒有重疊。

解決方案

請確定遠端伺服器支援錯誤訊息中列出的至少一個 Client 主機金鑰演算法。如需支援演算法的清單，請參閱AWS Transfer Family SFTP 連接器的安全性原則。

其他 SFTP 連接器問題

Description

您在執行後收到錯誤訊息`StartFileTransfer`，但不知道問題的原因，而且只會在 API 呼叫後傳回連接器識別碼。

原因

此錯誤可能有多種原因。若要進行疑難排解，建議您測試連接器並搜尋記 CloudWatch 錄。

解決方案

- 測試您的連接器：請參閱測試 SFTP 連接器。如果測試失敗，系統會根據測試失敗的原因提供錯誤訊息。本節說明如何從主控台或使用 TestConnectionAPI 命令來測試連接器。
- 檢視連接器的 CloudWatch 記錄：請參閱SFTP 連接器的記錄項目範例。本主題提供 SFTP 連接器記錄項目的範例，以及可協助您尋找適當記錄檔的命名慣例。

疑難排解 AS2 問題

已啟用適用性陳述式 2 (AS2) 之伺服器的錯誤訊息和疑難排解提示說明如下：AS2 錯誤代碼

API 參考

以下各節說明 AWS Transfer Family API 服務呼叫、資料類型、參數和錯誤。

主題

- 歡迎使用 AWS Transfer Family API
- 動作
- 資料類型
- 提出 API 要求
- 常見參數
- 常見錯誤

歡迎使用 AWS Transfer Family API

AWS Transfer Family 這是一種安全傳輸服務，可透過下列協定將檔案傳入和傳出 Amazon 簡單儲存服務 (Amazon S3) 儲存：

- 安全殼層 (SSH) 檔案傳輸通訊協定 (SFTP)
- 安全檔案傳輸通訊協定 (FTPS)
- 檔案傳輸通訊協定 (FTP)
- 適用性聲明 2 (AS2)

檔案傳輸通訊協定用於不同產業的資料交換工作流程，例如金融服務、醫療保健、廣告和零售等。AWS Transfer Family 簡化了將檔案傳輸工作流程移轉至 AWS.

要使用該 AWS Transfer Family 服務，請在您選擇的 AWS 區域中實例化服務器。您可以建立伺服器、列出可用的伺服器，以及更新和刪除伺服器。伺服器是要求檔案作業的實體 AWS Transfer Family。伺服器有多項重要屬性。伺服器是具名的執行個體，由系統指派的 `ServerId` 識別符來識別。您可以選擇將主機名稱，甚至自訂主機名稱指派給伺服器。任何具現化伺服器 (甚至是伺服器`OFFLINE`) 的服務帳單，以及傳輸的資料量。

請求文件操作的服務器必須知道用戶。使用者會由使用者名稱來識別，
並指派給伺服器。使用者名稱可用來驗證要求。伺服器只能有一種驗證方
法：`AWS_DIRECTORY_SERVICE`、`SERVICE_MANAGED`、`AWS_LAMBDA`、或`API_GATEWAY`。

您可以使用下列任何身分識別提供者類型來驗證使用者：

- 對於SERVICE_MANAGED，SSH 公鑰與用戶的屬性一起存儲在服務器上。使用者可以擁有一個或多個 SSH 公開金鑰，以供SERVICE_MANAGED驗證方法使用。當客戶端請求SERVICE_MANAGED方法的文件操作時，客戶端提供用戶名和 SSH 私鑰，這是經過身份驗證，並提供訪問。
- 您可以透過選取驗證方法來管理使用者驗AWS_DIRECTORY_SERVICE證和存取您的 Microsoft 活動目錄群組。
- 您可以使用連線至自訂身分識別提供者 AWS Lambda。選擇AWS_LAMBDA驗證方法。
- 您也可以使用自訂的身分驗證方法來驗證使用者請求，以同時提供使用者身分驗證和存取權。此方法依賴 Amazon API Gateway 來使用身分供應商提供的 API 呼叫來驗證使用者請求。此方法在 API 呼叫API_GATEWAY中稱為，在主控台中稱為「自訂」。您可以使用自訂方法，藉由目錄服務、資料庫名稱/密碼對，或一些其他機制來驗證使用者。

將指派給使用者與 Amazon S3 儲存貯體之間具有信任關係的政策。他們可以存取部分或所有儲存貯體。伺服器必須繼承使用者的信任關係，伺服器必須繼承來自使用者的信任關係。系統會建立包含信任關係的 AWS Identity and Access Management (IAM) 角色，並為該角色指派AssumeRole動作。然後，服務器可以像用戶一樣執行文件操作。

已設定home目錄屬性的使用者將使該目錄 (或資料夾) 充當檔案作業的目標和來源。如果未設定任何 home 目錄，儲存貯體的 `root` 目錄就會變成登陸目錄。

伺服器、使用者和角色均以其 Amazon 資源名稱 (ARN) 識別。您可以將標籤 (鍵值配對) 指派給具有 ARN 的實體。標記是可用來分組或搜尋這些實體的中繼資料。舉例來說，標籤在會計用途方面就非常有用。

以下是 AWS Transfer Family ID 格式的慣例：

- `ServerId` 值採用 `s-01234567890abcdef` 的形式。
- `SshPublicKeyId` 值採用 `key-01234567890abcdef` 的形式。

Amazon 資源名稱 (ARN) 格式採用以下形式：

- 對於伺服器，ARN 會採用這種形式arn:aws:transfer:*region*:*account-id*:server/*server-id*。

  伺服器 ARN 的範例為 `arn:aws:transfer:us-east-1:123456789012:server/s-01234567890abcdef`。

- 針對使用者，ARN 採用 `arn:aws:transfer:region:account-id:user/server-id/username` 的形式。

  例如，`arn:aws:transfer:us-east-1:123456789012:user/s-01234567890abcdef/user1`。

使用中的 DNS 項目 (端點) 如下：

- API 端點採用 `transfer.region.amazonaws.com` 的形式。
- 伺服器端點採用 `server.transfer.region.amazonaws.com` 的形式。

如需依 AWS 區域 Transfer Family 列AWS Transfer Family 端點的清單，請參閱 AWS 一般參考.

此 API 介面參考 AWS Transfer Family 包含可用來管理之程式設計介面的文件 AWS Transfer Family。參考結構如下：

- 如需依字母順序排列的 API 動作清單，請參閱Actions。
- 如需按字母順序排列的資料類型清單，請參閱Data Types。
- 如需常用查詢參數的清單，請參閱常用參數。
- 如需錯誤碼的說明，請參閱常見錯誤。

> **Tip**
>
> 您可以在任何 API 呼叫中使用參數來產生並顯示`--generate-cli-skeleton`參數範本，而不是實際執行命令。然後，您可以使用產生的範本來自訂並用作稍後指令的輸入。如需詳細資訊，請參閱產生並使用參數骨架檔案。

動作

支援以下動作：

- CreateAccess
- CreateAgreement
- CreateConnector
- CreateProfile

- CreateServer
- CreateUser
- CreateWorkflow
- DeleteAccess
- DeleteAgreement
- DeleteCertificate
- DeleteConnector
- DeleteHostKey
- DeleteProfile
- DeleteServer
- DeleteSshPublicKey
- DeleteUser
- DeleteWorkflow
- DescribeAccess
- DescribeAgreement
- DescribeCertificate
- DescribeConnector
- DescribeExecution
- DescribeHostKey
- DescribeProfile
- DescribeSecurityPolicy
- DescribeServer
- DescribeUser
- DescribeWorkflow
- ImportCertificate
- ImportHostKey
- ImportSshPublicKey
- ListAccesses
- ListAgreements
- ListCertificates

- ListConnectors
- ListExecutions
- ListHostKeys
- ListProfiles
- ListSecurityPolicies
- ListServers
- ListTagsForResource
- ListUsers
- ListWorkflows
- SendWorkflowStepState
- StartDirectoryListing
- StartFileTransfer
- StartServer
- StopServer
- TagResource
- TestConnection
- TestIdentityProvider
- UntagResource
- UpdateAccess
- UpdateAgreement
- UpdateCertificate
- UpdateConnector
- UpdateHostKey
- UpdateProfile
- UpdateServer
- UpdateUser

CreateAccess

系統管理員用來選擇目錄中的哪些群組應該有權透過已啟用的通訊協定上傳和下載檔案 AWS Transfer Family。例如，Microsoft 活動目錄可能包含 50,000 個用戶，但只有一小部分可能需要將文件傳輸到服務器的能力。管理員可以用CreateAccess來限制對需要此功能的正確使用者集的存取權。

請求語法

```
{
   "ExternalId": "string",
   "HomeDirectory": "string",
   "HomeDirectoryMappings": [
      {
         "Entry": "string",
         "Target": "string",
         "Type": "string"
      }
   ],
   "HomeDirectoryType": "string",
   "Policy": "string",
   "PosixProfile": {
      "Gid": number,
      "SecondaryGids": [ number ],
      "Uid": number
   },
   "Role": "string",
   "ServerId": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

ExternalId

識別目錄中特定群組所需的唯一識別碼。您關聯之群組的使用者可以透過已啟用的協定存取 Amazon S3 或 Amazon EFS 資源 AWS Transfer Family。如果您知道群組名稱，您可以使用 Windows 執行下列命令來檢視 SID 值 PowerShell。

```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties
* | Select SamAccountName,ObjectSid
```

在該命令中，YourGroupName用您的活動目錄組的名稱替換。

用來驗證此參數的規則運算式是由不含空格的大寫和小寫英數字元所組成的字元字串。您也可以包含底線或下列任何字元：=, 。 @：/-

類型：字串

長度限制：長度下限為 1。長度上限為 256。

模式：S-1-[\d-]+

必要：是

HomeDirectory

使用者使用其用戶端登入伺服器時的登陸目錄 (資料夾)。

HomeDirectory 範例為 /bucket_name/home/mydirectory。

> **Note**
>
> 只有在 HomeDirectoryType 設為 PATH 時才會使用 HomeDirectory 參數。

類型：字串

長度限制：長度下限為 0。長度上限為 1024。

模式：(|/.*)

必要：否

HomeDirectoryMappings

邏輯目錄對應，指定您的使用者可以看到哪些 Amazon S3 或 Amazon EFS 路徑和金鑰，以及您希望如何顯示這些路徑和金鑰。您必須指定Entry和Target配對，其中Entry顯示路徑的顯示方式，以及Target實際的 Amazon S3 或 Amazon EFS 路徑。如果您僅指定目標，則會依原樣顯示該目標。您還必須確保您的 AWS Identity and Access Management (IAM) 角色可提供中路徑的存取權Target。只有當設定為邏輯時HomeDirectoryType，才能設定此值。

以下是Entry和配Target對範例。

```
[ { "Entry": "/directory1", "Target": "/bucket_name/home/
mydirectory" } ]
```

在大多數情況下，您可以使用此值而不是工作階段原則，將使用者鎖定到指定的主目錄 (」chroot「)。若要執行此操作，您可以設Entry定為/並Target將其設定為HomeDirectory參數值。

以下是的Entry和Target配對範例chroot。

```
[ { "Entry": "/", "Target": "/bucket_name/home/mydirectory" } ]
```

類型：HomeDirectoryMapEntry 物件陣列

陣列成員：項目數下限為 1。5 萬個物品的最大數量。

必要：否

HomeDirectoryType

使用者登入伺服器時，您希望的使用者主目錄之登陸目錄 (資料夾) 類型。如果將其設定為PATH，使用者將在其檔案傳輸協定用戶端中看到絕對的 Amazon S3 儲存貯體或 Amazon EFS 路徑。如果將其設定為LOGICAL，則需要在中提供對應，以便讓使用者看到 Amazon S3 或 Amazon EFS 路徑的方式。HomeDirectoryMappings

> **Note**
>
> 如果HomeDirectoryType是LOGICAL，則必須使用HomeDirectoryMappings參數提供對映。另一方面，HomeDirectoryType如果您使用HomeDirectory參數提供絕對路徑。PATH您的範本HomeDirectoryMappings中不HomeDirectory能同時擁有和。

類型：字串

有效值:PATH | LOGICAL

必要：否

Policy

適用於您的使用者的工作階段政策，以便您可以在多個使用者間使用相同的 AWS Identity and Access Management (IAM) 角色。此政策限制了使用者對 Amazon S3 儲存貯體部分的存取權限。

您可以在此政策內使用的變數包括 `${Transfer:UserName}`、`${Transfer:HomeDirectory}` 和 `${Transfer:HomeBucket}`。

> **Note**
>
> 只有在的網域`ServerId`是 Amazon S3 時，才適用此政策。Amazon EFS 不使用工作階段政策。
> 對於工作階段政策，請將政策 AWS Transfer Family 儲存為 JSON Blob，而不是政策的 Amazon 資源名稱 (ARN)。您會將政策作為 JSON blob 儲存，並在 `Policy` 引數中傳遞它。
> 如需工作階段政策的範例，請參閱 Example session policy (工作階段政策範例)。
> 如需詳細資訊，請參閱 AWS Security Token Service API 參考AssumeRole中的。

類型：字串

長度限制：長度下限為 0。長度上限為 2048。

必要：否

PosixProfile

控制使用者存取 Amazon EFS 檔案系統的完整 POSIX 身分，包括使用者 ID (`Uid`)、群組 ID (`Gid`) 和任何次要群組 ID (`SecondaryGids`)。對檔案系統中的檔案和目錄設定的 POSIX 許可，會決定使用者在 Amazon EFS 檔案系統中傳入和傳出檔案時所取得的存取等級。

類型：PosixProfile 物件

必要：否

Role

(IAM) 角色的亞馬遜資源名稱 AWS Identity and Access Management (ARN)，用於控制使用者對 Amazon S3 儲存貯體或 Amazon EFS 檔案系統的存取。連接到此角色的政策會決定在將檔案傳入和傳出您的 Amazon S3 儲存貯體或 Amazon EFS 檔案系統時，您希望提供給使用者的存取層級。IAM 角色也應包含信任關係，允許伺服器在處理您使用者的傳輸請求時，存取您的資源。

類型：字串

長度限制：長度下限為 20。長度上限為 2048。

模式：`arn:.*role/\S+`

必要：是

ServerId

伺服器執行個體的系統指派唯一識別碼。這是您新增使用者的特定目標伺服器。

類型：字串

長度約束：固定長度為 19。

模式：`s-([0-9a-f]{17})`

必要：是

回應語法

```
{
   "ExternalId": "string",
   "ServerId": "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。

ExternalId

群組的外部識別碼，其使用者可以透過已啟用的協定存取您的 Amazon S3 或 Amazon EFS 資源 AWS Transfer Family。

類型：字串

長度限制：長度下限為 1。長度上限為 256。

模式：`S-1-[\d-]+`

ServerId

使用者所附加之伺服器的識別碼。

類型：字串

長度約束：固定長度為 19。

模式：`s-([0-9a-f]{17})`

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceExistsException

請求的資源不存在，或者存在於為命令指定的區域以外的區域中。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

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

CreateAgreement

建立協議。協議是一個 AWS Transfer Family 服務器和 AS2 進程之間的雙邊貿易夥伴協議或合作夥伴關係。此協議可定義伺服器與 AS2 程序之間的檔案和訊息傳輸關係。為定義協議，Transfer Family 結合伺服器、本機設定檔、合作夥伴設定檔、憑證和其他屬性。

使用 `PartnerProfileId` 識別合作夥伴，並使用 `LocalProfileId` 識別 AS2 程序。

請求語法

```
{
   "AccessRole": "string",
   "BaseDirectory": "string",
   "Description": "string",
   "LocalProfileId": "string",
   "PartnerProfileId": "string",
   "ServerId": "string",
   "Status": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

AccessRole

連接器可用來使用 AS2 或 SFTP 通訊協定來傳送檔案。對於存取角色，請提供要使用之 AWS Identity and Access Management 角色的 Amazon 資源名稱 (ARN)。

適用於 AS2 連接器

使用 AS2，即可透過呼叫 `StartFileTransfer`，並在請求參數 `SendFilePaths` 中指定檔案路徑的方式傳送檔案。使用該檔案的父目錄 (例如，`--send-file-paths /bucket/dir/file.txt` 的父目錄為 `/bucket/dir/`) 暫時儲存已處理的 AS2 訊息檔案、於接收到合作夥伴的

MDN 時進行儲存，並寫入包含傳輸相關中繼資料的最終 JSON 檔案。因此，AccessRole 需要針對 StartFileTransfer 請求中使用之檔案位置的父目錄提供讀寫權限。此外，還需要針對欲透過 StartFileTransfer 傳送之檔案的父目錄提供讀寫權限。

如果您使用 AS2 連接器的基本驗證，則存取角色需要密碼的secretsmanager:GetSecretValue權限。如果密碼是使用客戶管理的金鑰而非 Secrets Manager 中的 AWS 受管理金鑰加密，則該角色也需要該金鑰的kms:Decrypt權限。

適用於 SFTP 連接器

StartFileTransfer請確定存取角色提供對要求中所使用之檔案位置之父目錄的讀取和寫入存取權。此外，請確定角色提供的secretsmanager:GetSecretValue權限 AWS Secrets Manager。

類型：字串

長度限制：長度下限為 20。長度上限為 2048。

模式：arn:.*role/\S+

必要：是

BaseDirectory

使用 AS2 通訊協定傳輸之檔案的登陸目錄 (資料夾)。

BaseDirectory 範例為 /DOC-EXAMPLE-BUCKET/home/mydirectory。

類型：字串

長度限制：長度下限為 0。長度上限為 1024。

模式：(|/.*)

必要：是

Description

用來識別合約的名稱或簡短描述。

類型：字串

長度限制：長度下限為 1。長度上限為 200。

模式：[\p{Graph}]+

必要：否

LocalProfileId

AS2 本機設定檔的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：p-([0-9a-f]{17})

必要：是

PartnerProfileId

協議中使用之合作夥伴設定檔的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：p-([0-9a-f]{17})

必要：是

ServerId

伺服器執行個體的系統指派唯一識別碼。這是合約使用的特定伺服器。

類型：字串

長度約束：固定長度為 19。

模式：s-([0-9a-f]{17})

必要：是

Status

協議的狀態。協定可以是ACTIVE或INACTIVE。

類型：字串

有效值:ACTIVE | INACTIVE

必要：否

Tags

可用於進行協議分組和搜尋的金鑰/值對。

類型：Tag 物件陣列

陣列成員：項目數下限為 1。項目數上限為 50。

必要：否

回應語法

```
{
   "AgreementId": "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。

AgreementId

協定的唯一識別元。使用此 ID 來刪除或更新合約，以及在需要您指定合約 ID 的任何其他 API 呼叫中使用。

類型：字串

長度約束：固定長度為 19。

模式：a-([0-9a-f]{17})

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceExistsException

請求的資源不存在，或者存在於為命令指定的區域以外的區域中。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

HTTP 狀態碼：500

ThrottlingException

由於請求調節，因此請求遭到拒絕。

HTTP 狀態碼：400

範例

範例

下列範例會建立協定，並傳回協定 ID。

```
aws transfer create-agreement --server-id s-021345abcdef6789 --local-profile-
id p-1234567890abcdef0 --partner-profile-id p-abcdef01234567890 --base-folder /DOC-
EXAMPLE-BUCKET/AS2-files --access-role arn:aws:iam::111122223333:role/AS2-role
```

回應範例

API 呼叫會傳回新合約的合約 ID。

```
{
    "AgreementId": "a-11112222333344444"
}
```

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

CreateConnector

建立連接器，以擷取 AS2 或 SFTP 通訊協定連線的參數。對於 AS2，將檔案傳送到外部託管的 AS2 伺服器時，需要連接器。對於 SFTP，將檔案傳送至 SFTP 伺服器或從 SFTP 伺服器接收檔案時需要連接器。如需有關連接器的詳細資訊，請參閱設定 AS2 連接器和建立 SFTP 連接器。

> **Note**
>
> 您必須只指定一個配置物件：用於 AS2 (`As2Config`) 或 SFTP (`SftpConfig`)。

請求語法

```
{
   "AccessRole": "string",
   "As2Config": {
      "BasicAuthSecretId": "string",
      "Compression": "string",
      "EncryptionAlgorithm": "string",
      "LocalProfileId": "string",
      "MdnResponse": "string",
      "MdnSigningAlgorithm": "string",
      "MessageSubject": "string",
      "PartnerProfileId": "string",
      "SigningAlgorithm": "string"
   },
   "LoggingRole": "string",
   "SecurityPolicyName": "string",
   "SftpConfig": {
      "TrustedHostKeys": [ "string" ],
      "UserSecretId": "string"
   },
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ],
   "Url": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

AccessRole

連接器可用來使用 AS2 或 SFTP 通訊協定來傳送檔案。對於存取角色，請提供要使用之 AWS Identity and Access Management 角色的 Amazon 資源名稱 (ARN)。

適用於 AS2 連接器

使用 AS2，即可透過呼叫 `StartFileTransfer`，並在請求參數 `SendFilePaths` 中指定檔案路徑的方式傳送檔案。使用該檔案的父目錄 (例如，`--send-file-paths /bucket/dir/file.txt` 的父目錄為 `/bucket/dir/`) 暫時儲存已處理的 AS2 訊息檔案、於接收到合作夥伴的 MDN 時進行儲存，並寫入包含傳輸相關中繼資料的最終 JSON 檔案。因此，`AccessRole` 需要針對 `StartFileTransfer` 請求中使用之檔案位置的父目錄提供讀寫權限。此外，還需要針對欲透過 `StartFileTransfer` 傳送之檔案的父目錄提供讀寫權限。

如果您使用 AS2 連接器的基本驗證，則存取角色需要密碼的`secretsmanager:GetSecretValue`權限。如果密碼是使用客戶管理的金鑰而非 Secrets Manager 中的 AWS 受管理金鑰加密，則該角色也需要該金鑰的`kms:Decrypt`權限。

適用於 SFTP 連接器

`StartFileTransfer`請確定存取角色提供對要求中所使用之檔案位置之父目錄的讀取和寫入存取權。此外，請確定角色提供的`secretsmanager:GetSecretValue`權限 AWS Secrets Manager。

類型：字串

長度限制：長度下限為 20。長度上限為 2048。

模式：`arn:.*role/\S+`

必要：是

As2Config

包含 AS2 連接器物件參數的結構。

類型：As2ConnectorConfig 物件

必要：否

LoggingRole

(IAM) 角色的亞馬遜資源名稱 AWS Identity and Access Management (ARN)，可讓連接器開啟 Amazon S3 事件的 CloudWatch 記錄功能。設定後，您可以在 CloudWatch 記錄檔中檢視連接器活動。

類型：字串

長度限制：長度下限為 20。長度上限為 2048。

模式：`arn:.*role/\S+`

必要：否

SecurityPolicyName

指定連接器的安全性原則名稱。

類型：字串

長度限制：長度下限為 0。長度上限為 100。

模式：`TransferSFTPConnectorSecurityPolicy-[A-Za-z0-9-]+`

必要：否

SftpConfig

包含 SFTP 連接器物件參數的結構。

類型：SftpConnectorConfig 物件

必要：否

Tags

金鑰/值對，可用來分組和搜尋連接器。標籤是基於任何目的附加至連接器的中繼資料。

類型：Tag 物件陣列

陣列成員：項目數下限為 1。項目數上限為 50。

必要：否

Url

合作夥伴的 AS2 或 SFTP 端點的網址。

類型：字串

長度限制：長度下限為 0。長度上限為 255。

必要：是

回應語法

```
{
   "ConnectorId": "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。

ConnectorId

連接器的唯一識別碼，在 API 呼叫成功後傳回。

類型：字串

長度約束：固定長度為 19。

模式：`c-([0-9a-f]{17})`

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceExistsException

請求的資源不存在，或者存在於為命令指定的區域以外的區域中。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

HTTP 狀態碼：500

ThrottlingException

由於請求調節，因此請求遭到拒絕。

HTTP 狀態碼：400

範例

範例

下列範例會建立 AS2 連接器。在命令中，取代項目，如下所示：

- `url`：提供交易夥伴 AS2 伺服器的 URL。
- `your-IAM-role-for-bucket-access`：一種 IAM 角色，可存取您用來存放檔案的 Amazon S3 儲存貯體。
- 使用 ARN 作為您的記錄角色，其中包括您的 AWS 帳戶 ID。
- 提供包含 AS2 連接器組態參數之檔案的路徑。AS2 連接器配置物件的說明如 As ConnectorConfig 2。

```
// Listing for testAs2Config.json
{
  "LocalProfileId": "your-profile-id",
  "PartnerProfileId": "partner-profile-id",
  "MdnResponse": "SYNC",
  "Compression": "ZLIB",
  "EncryptionAlgorithm": "AES256_CBC",
  "SigningAlgorithm": "SHA256",
  "MdnSigningAlgorithm": "DEFAULT",
  "MessageSubject": "Your Message Subject"
}
```

```
aws transfer create-connector --url "http://partner-as2-server-url" \
          --access-role your-IAM-role-for-bucket-access \
          --logging-role arn:aws:iam::your-account-id:role/service-role/
AWSTransferLoggingAccess \
          --as2-config file://path/to/testAS2Config.json
```

範例

下列範例會建立 SFTP 連接器。在命令中，取代項目，如下所示：

- `sftp-server-url`：提供您要交換檔案之 SFTP 伺服器的 URL。
- `your-IAM-role-for-bucket-access`：一種 IAM 角色，可存取您用來存放檔案的 Amazon S3 儲存貯體。
- 使用 ARN 作為您的記錄角色，其中包括您的 AWS 帳戶 ID。
- 提供包含 SFTP 連接器組態參數之檔案的路徑。SFTP 連接器 SftpConnectorConfig 物件在設定中說明。

```
// Listing for testSFTPConfig.json
{
   "UserSecretId": "arn:aws:secretsmanager:us-east-2:123456789012:secret:aws/transfer/
example-username-key",
   "TrustedHostKeys": [
      "sftp.example.com ssh-rsa AAAAbbbb...EEEE="
   ]
}
```

```
aws transfer create-connector --url "sftp://sftp-server-url" \
--access-role your-IAM-role-for-bucket-access \
--logging-role arn:aws:iam::your-account-id:role/service-role/AWSTransferLoggingAccess
 \
--sftp-config file://path/to/testSFTPConfig.json
```

範例

API 呼叫會傳回新連接器的連接器識別碼。

回應範例

```
{
    "ConnectorId": "a-11112222333344444"
}
```

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

CreateProfile

建立要用於 AS2 傳輸的本機或合作夥伴設定檔。

請求語法

```
{
   "As2Id": "string",
   "CertificateIds": [ "string" ],
   "ProfileType": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

As2Id

As2Id 是 AS2 名稱，如 RFC 4130 中所定義。若為對內傳輸，這是合作夥伴傳送的 AS2 訊息 AS2-From 標頭。若為對外連接器，這是使用 StartFileTransfer API 操作傳送給合作夥伴的 AS2 訊息 AS2-To 標頭。此 ID 不可包含空格。

類型：字串

長度限制：長度下限為 1。長度上限為 128。

模式：[\p{Print}\s]*

必要：是

CertificateIds

已匯入憑證的識別碼陣列。您可以使用此識別碼處理設定檔和合作夥伴設定檔。

類型：字串陣列

長度約束：固定長度為 22。

模式：`cert-([0-9a-f]{17})`

必要：否

ProfileType

決定要建立的設定檔類型：

- 指定LOCAL此選項可建立本機設定檔。本機設定檔代表已啟用 AS2 的「Transfer Family」伺服器組織或對象。
- 指定PARTNER以建立合作夥伴設定檔。合作夥伴設定檔代表「Transfer Family」外部的遠端組織。

類型：字串

有效值:`LOCAL | PARTNER`

必要：是

Tags

可用於分組和搜尋 AS2 設定檔的索引鍵值配對。

類型：Tag 物件陣列

陣列成員：項目數下限為 1。項目數上限為 50。

必要：否

回應語法

```
{
   "ProfileId": "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。

ProfileId

AS2 設定檔的唯一識別碼，在 API 呼叫成功後傳回。

類型：字串

長度約束：固定長度為 19。

模式：`p-([0-9a-f]{17})`

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

HTTP 狀態碼：500

ThrottlingException

由於請求調節，因此請求遭到拒絕。

HTTP 狀態碼：400

範例

範例

下列範例會建立描述檔，並傳回描述檔 ID。

憑證 ID 會在您執行時建立import-certificate，一個用於簽署憑證，另一個用於加密憑證。

```
aws transfer create-profile --as2-id MYCORP --certificate-ids c-abcdefg123456hijk
               c-987654aaaa321bbbb
```

回應範例

API 呼叫會傳回新設定檔的描述檔 ID。

```
{
    "ProfileId": "p-11112222333344444"
}
```

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

CreateServer

在 AWS中根據所選檔案傳輸通訊協定，將自動擴展虛擬伺服器執行個體化。當您更新啟用檔案傳輸通訊協定的伺服器，或使用使用者時，請使用指派給新建立伺服器的由服務產生的 ServerId 屬性。

請求語法

```
{
   "Certificate": "string",
   "Domain": "string",
   "EndpointDetails": {
      "AddressAllocationIds": [ "string" ],
      "SecurityGroupIds": [ "string" ],
      "SubnetIds": [ "string" ],
      "VpcEndpointId": "string",
      "VpcId": "string"
   },
   "EndpointType": "string",
   "HostKey": "string",
   "IdentityProviderDetails": {
      "DirectoryId": "string",
      "Function": "string",
      "InvocationRole": "string",
      "SftpAuthenticationMethods": "string",
      "Url": "string"
   },
   "IdentityProviderType": "string",
   "LoggingRole": "string",
   "PostAuthenticationLoginBanner": "string",
   "PreAuthenticationLoginBanner": "string",
   "ProtocolDetails": {
      "As2Transports": [ "string" ],
      "PassiveIp": "string",
      "SetStatOption": "string",
      "TlsSessionResumptionMode": "string"
   },
   "Protocols": [ "string" ],
   "S3StorageOptions": {
      "DirectoryListingOptimization": "string"
   },
   "SecurityPolicyName": "string",
   "StructuredLogDestinations": [ "string" ],
   "Tags": [
```

```
      {
         "Key": "string",
         "Value": "string"
      }
   ],
   "WorkflowDetails": {
      "OnPartialUpload": [
         {
            "ExecutionRole": "string",
            "WorkflowId": "string"
         }
      ],
      "OnUpload": [
         {
            "ExecutionRole": "string",
            "WorkflowId": "string"
         }
      ]
   }
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

Certificate

AWS Certificate Manager (ACM) 憑證的 Amazon Resource Name (ARN)。當 `Protocols` 設定為 FTPS 時，此為必要項目。

若要要求新的公用憑證，請參閱 AWS Certificate Manager 使用者指南中的要求公用憑證。

若要將現有憑證匯入 ACM，請參閱《 AWS Certificate Manager 使用指南》中的〈將憑證匯入 ACM〉。

若要要求私有憑證以透過私有 IP 位址使用 FTPS，請參閱使用 AWS Certificate Manager 者指南中的要求私人憑證。

支援具有下列密碼編譯演算法和金鑰大小的憑證：

- 2048 位元 RSA (RSA_2048)

- 4096 位元 RSA (RSA_4096)
- 橢圓定焦曲線 256 位元 (EC_prime256v1)
- 橢圓定焦曲線 384 位元 (EC_secp384r1)
- 橢圓定焦曲線 521 位元 (EC_secp521r1)

> **Note**
>
> 憑證必須是有效的 SSL/TLS X.509 版本 3 憑證，並具備 FQDN 或 IP 位址，以及簽發者的相關資訊。

類型：字串

長度限制：長度下限為 0。長度上限為 1600。

必要：否

Domain

用於檔案傳輸的儲存系統網域。有兩個域可用：Amazon Simple Storage Service (Amazon S3) 和 Amazon Elastic File System（Amazon EFS）。預設值為 S3。

> **Note**
>
> 建立伺服器之後，就無法變更網域。

類型：字串

有效值:`S3 | EFS`

必要：否

EndpointDetails

為伺服器設定的 Virtual Private Cloud (VPC) 端點設定。當您將端點託管於 VPC 時，您可以限定只有 VPC 內的資源才可存取端點，或連接彈性 IP 地址以開放給網際網路上的用戶端存取端點。VPC 的預設安全群組會自動指派給端點。

類型：EndpointDetails 物件

必要：否

EndpointType

您希望您伺服器使用的端點類型。您可以選擇將伺服器的端點設為可公開存取 (PUBLIC)，或在 VPC 中託管。若為 VPC 中託管的端點，您可以限制只能存取 VPC 中的伺服器和資源，或直接連接彈性 IP 地址，讓其面向網際網路。

> **Note**
>
> 2021 年 5 月 19 日之後， AWS 帳戶 如果您的帳戶EndpointType=VPC_ENDPOINT在 2021 年 5 月 19 日之前尚未使用，您將無法使用中的伺服器來建立伺服器。如果您已EndpointType=VPC_ENDPOINT在 2021 年 5 月 19 AWS 帳戶 日或之前建立伺服器，則不會受到影響。在此日期之後，使用 EndpointType = VPC。
> 如需詳細資訊，請參閱 停止使用 VPC_ 端點。
> 建議使用 VPC 作為 EndpointType。使用此端點類型時，您可以選擇直接將最多三個彈性 IPv4 地址 (包括 BYO IP) 與伺服器的端點建立關聯，並使用 VPC 安全群組依用戶端的公用 IP 地址來限制流量。當 EndpointType 設為 VPC_ENDPOINT 時就無法如此。

類型：字串

有效值:PUBLIC | VPC | VPC_ENDPOINT

必要：否

HostKey

RSA、ECDSA 或 ED25519 私密金鑰，以用於啟用了 SFTP 的伺服器。如果您想要旋轉金鑰，或有一組使用不同演算法的作用中金鑰，您可以新增多個主機金鑰。

使用下列指令產生不含密碼的 RSA 2048 位元金鑰：

```
ssh-keygen -t rsa -b 2048 -N "" -m PEM -f my-new-server-key.
```

-b選項使用最小值 2048。您可以使用 3072 或 4096 來建立更強大的金鑰。

使用下列指令產生不含複雜密碼的 ECDSA 256 位元金鑰：

```
ssh-keygen -t ecdsa -b 256 -N "" -m PEM -f my-new-server-key.
```

ECDSA 的選-b項的有效值為 256、384 和 521。

使用下列指令來產生不含密碼的 ED25519 金鑰：

```
ssh-keygen -t ed25519 -N "" -f my-new-server-key.
```

對於所有這些命令，您可以my-new-server-key用您選擇的字符串替換。

> **Important**
>
> 如果您不打算將現有使用者從現有啟用 SFTP 的伺服器遷移到新伺服器，請不要更新主機金鑰。意外變更伺服器的主機金鑰可能造成破壞。

如需詳細資訊，請參閱《 AWS Transfer Family 使用指南》中的更新已啟用 SFTP 之伺服器的主機金鑰。

類型：字串

長度限制：長度下限為 0。長度上限為 4096。

必要：否

IdentityProviderDetails

設定IdentityProviderType為AWS_DIRECTORY_SERVICE、 AWS_LAMBDA或時需要API_GATEWAY。接受包含在 AWS_DIRECTORY_SERVICE 中使用目錄或叫用客戶所提供驗證 API 所需全部資訊的陣列，包括 API Gateway URL。當 IdentityProviderType 設定為 SERVICE_MANAGED 時，此為非必要項目。

類型：IdentityProviderDetails 物件

必要：否

IdentityProviderType

伺服器的身分驗證模式。預設值為SERVICE_MANAGED，可讓您在 AWS Transfer Family 服務中儲存和存取使用者認證。

用AWS_DIRECTORY_SERVICE於在內部部署環境 AWS Directory Service for Microsoft Active Directory 或 AWS 使用 AD Connector 中，提供存取作用中目錄群組或 Microsoft Active Directory。此選項也要求您使用 IdentityProviderDetails 參數提供 Directory ID。

使用 API_GATEWAY 值來和您選擇的身分提供者整合。API_GATEWAY 設定要求您提供 Amazon API Gateway 端點 URL，以使用 IdentityProviderDetails 參數呼叫驗證。

使用該AWS_LAMBDA值直接使用 AWS Lambda 函數作為您的身份提供者。如果選擇此值，則必須在IdentityProviderDetails資料類型的參數中指定 Lambda 函Function數的 ARN。

類型：字串

有效值:SERVICE_MANAGED | API_GATEWAY | AWS_DIRECTORY_SERVICE | AWS_LAMBDA

必要：否

LoggingRole

(IAM) 角色的 Amazon 資源名稱 AWS Identity and Access Management (ARN)，可讓伺服器為 Amazon Amazon S3 或 Amazon EFSENTS 開啟亞馬遜 CloudWatch 日誌記錄。設定後，您可以檢視 CloudWatch 記錄中的使用者活動。

類型：字串

長度限制：長度下限為 0。長度上限為 2048。

模式：(|arn:.*role/\S+)

必要：否

PostAuthenticationLoginBanner

指定使用者連線到伺服器時要顯示的字串。此字串會在使用者驗證後顯示。

> **Note**
>
> SFTP 通訊協定不支援驗證後顯示橫幅。

類型：字串

長度限制：長度下限為 0。長度上限為 4096。

模式：[\x09-\x0D\x20-\x7E]*

必要：否

PreAuthenticationLoginBanner

指定使用者連線到伺服器時要顯示的字串。此字串會在使用者驗證之前顯示。例如，下列橫幅會顯示有關使用系統的詳細資訊：

```
This system is for the use of authorized users only. Individuals using
this computer system without authority, or in excess of their authority,
are subject to having all of their activities on this system monitored
and recorded by system personnel.
```

類型：字串

長度限制：長度下限為 0。長度上限為 4096。

模式：`[\x09-\x0D\x20-\x7E]*`

必要：否

ProtocolDetails

為伺服器設定的通訊協定設定。

- 若要指出被動模式 (用於 FTP 和 FTPS 通訊協定)，請使用 `PassiveIp` 參數。輸入單一點分四進制 IPv4 位址，例如防火牆、路由器或負載平衡器的外部 IP 地址。
- 若要忽略在用戶端嘗試對您上傳至 Amazon S3 儲存貯體的檔案使用 SETSTAT 命令時所產生的錯誤，請使用 `SetStatOption` 參數。若要讓 AWS Transfer Family 伺服器忽略指SETSTAT令並上傳檔案而不需對 SFTP 用戶端進行任何變更，請將值設定為`ENABLE_NO_OP`。如果將`SetStatOption`參數設定為`ENABLE_NO_OP`，Transfer Family 會產生 Amazon CloudWatch 日誌的日誌項目，以便您可以判斷用戶端何時SETSTAT撥打電話。
- 若要判斷 AWS Transfer Family 伺服器是否透過唯一的工作階段 ID 繼續最近交涉的工作階段，請使用參數`TlsSessionResumptionMode`。
- `As2Transports` 指出 AS2 訊息的傳輸方法。目前僅支援 HTTP。

類型：ProtocolDetails 物件

必要：否

Protocols

在您的檔案傳輸通訊協定用戶端可以連線到伺服器的端點上，指定檔案傳輸通訊協定或通訊協定。可用的通訊協定包括：

- SFTP (安全殼層 (SSH) 檔案傳輸通訊協定)：透過 SSH 傳輸檔案
- FTPS (檔案傳輸通訊協定安全)：使用 TLS 加密的檔案傳輸
- FTP (檔案傳輸通訊協定)：未加密的檔案傳輸
- AS2 (適用性聲明 2) ：用於傳輸結構化數據 business-to-business

> **Note**
>
> - 如果您選取FTPS，您必須選擇儲存在 AWS Certificate Manager (ACM) 中的憑證，當用戶端透過 FTPS 連線至伺服器時，此憑證可用來識別您的伺服器。
> - 如果 Protocol 包含 FTP 或 FTPS，則 EndpointType 必須是 VPC 且 IdentityProviderType 必須是 AWS_DIRECTORY_SERVICE、AWS_LAMBDA 或 API_GATEWAY。
> - 如果 Protocol 包含 FTP，則無法與 AddressAllocationIds 建立關聯。
> - 如果 Protocol 僅設定為 SFTP，則 EndpointType 可以設定為 PUBLIC，且 IdentityProviderType 可以設定任何支援的識別類型：SERVICE_MANAGED、AWS_DIRECTORY_SERVICE、AWS_LAMBDA 或 API_GATEWAY。
> - 如果 Protocol 包括 AS2，則 EndpointType 必須為 VPC，且網域必須為 Amazon S3。

類型：字串陣列

陣列成員：項目數下限為 1。最多 4 個項目數。

有效值:SFTP | FTP | FTPS | AS2

必要：否

S3StorageOptions

指定您的 Amazon S3 目錄的效能是否已最佳化。此選項根據預設為停用。

依預設，主目錄對應具有TYPE的DIRECTORY. 如果啟用此選項，如FILE果您希望對應具有檔案目標，則需要明確地將設定為。HomeDirectoryMapEntry Type

類型：S3StorageOptions 物件

必要：否

SecurityPolicyName

指定伺服器的安全性原則名稱。

類型：字串

長度限制：長度下限為 0。長度上限為 100。

模式：Transfer[A-Za-z0-9]*SecurityPolicy-[A-Za-z0-9-]+

必要：否

StructuredLogDestinations

指定要將伺服器記錄檔傳送至的記錄群組。

若要指定記錄群組，您必須提供現有記錄群組的 ARN。在此情況下，記錄群組的格式如下：

arn:aws:logs:region-name:amazon-account-id:log-group:log-group-name:*

例如：arn:aws:logs:us-east-1:111122223333:log-group:mytestgroup:*

如果您先前已為伺服器指定記錄群組，則可以在update-server呼叫中為此參數提供空白值，將其清除，並實際關閉結構化記錄。例如：

update-server --server-id s-1234567890abcdef0 --structured-log-destinations

類型：字串陣列

陣列成員：項目數下限為 0。項目數上限為 1。

長度限制：長度下限為 20。長度上限為 1600。

模式：arn:\S+

必要：否

Tags

鍵/值對，可用來分組和搜尋伺服器。

類型：Tag 物件陣列

陣列成員：項目數下限為 1。項目數上限為 50。

必要：否

WorkflowDetails

指定要指派之工作流程的工作流程 ID，以及用於執行工作流程的執行角色。

除了完全上傳檔案時要執行的工作流程外，WorkflowDetails 亦可包含要在部分上傳時執行之工作流程的工作流程 ID (和執行角色)。當伺服器工作階段中斷連線，而檔案仍在上載時，就會發生部分上傳。

類型：WorkflowDetails 物件

必要：否

回應語法

```
{
   "ServerId": "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。

ServerId

所建立之伺服器的服務指派識別碼。

類型：字串

長度約束：固定長度為 19。

模式：s-([0-9a-f]{17})

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：400

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceExistsException

請求的資源不存在，或者存在於為命令指定的區域以外的區域中。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

HTTP 狀態碼：500

ThrottlingException

由於請求調節，因此請求遭到拒絕。

HTTP 狀態碼：400

範例

範例

下列範例會使用VPC_ENDPOINT.

請求範例

```
{
   "EndpointType": "VPC",
   "EndpointDetails":...,
   "HostKey": "Your RSA private key",
   "IdentityProviderDetails": "IdentityProvider",
   "IdentityProviderType": "SERVICE_MANAGED",
```

```
   "LoggingRole": "CloudWatchLoggingRole",
   "Tags": [
      {
         "Key": "Name",
         "Value": "MyServer"
      }
   ]
}
```

範例

這是此 API 呼叫的範例回應。

回應範例

```
{
   "ServerId": "s-01234567890abcdef"
}
```

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

CreateUser

建立使用者，並將其與現有已啟用檔案傳輸通訊協定的伺服器建立關聯。您只能建立並將使用者與將 IdentityProviderType 設為 SERVICE_MANAGED 的伺服器建立關聯。使用的參數CreateUser，您可以指定使用者名稱、設定主目錄、儲存使用者的公開金鑰，以及指派使用者的 AWS Identity and Access Management (IAM) 角色。您也可以選用地新增工作階段政策，並使用可用來分組和搜尋使用者的標籤指派中繼資料。

請求語法

```
{
   "HomeDirectory": "string",
   "HomeDirectoryMappings": [
      {
         "Entry": "string",
         "Target": "string",
         "Type": "string"
      }
   ],
   "HomeDirectoryType": "string",
   "Policy": "string",
   "PosixProfile": {
      "Gid": number,
      "SecondaryGids": [ number ],
      "Uid": number
   },
   "Role": "string",
   "ServerId": "string",
   "SshPublicKeyBody": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ],
   "UserName": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

HomeDirectory

使用者使用其用戶端登入伺服器時的登陸目錄 (資料夾)。

HomeDirectory 範例為 /bucket_name/home/mydirectory。

> **Note**
>
> 只有在 HomeDirectoryType 設為 PATH 時才會使用 HomeDirectory 參數。

類型：字串

長度限制：長度下限為 0。長度上限為 1024。

模式：(|/.*)

必要：否

HomeDirectoryMappings

邏輯目錄對應，指定您的使用者可以看到哪些 Amazon S3 或 Amazon EFS 路徑和金鑰，以及您希望如何顯示這些路徑和金鑰。您必須指定Entry和Target配對，其中Entry顯示路徑的顯示方式，以及Target實際的 Amazon S3 或 Amazon EFS 路徑。如果您僅指定目標，則會依原樣顯示該目標。您還必須確保您的 AWS Identity and Access Management (IAM) 角色可提供中路徑的存取權Target。只有當設定為 LO GIC 時HomeDirectoryType，才能設定此值。

以下是Entry和配Target對範例。

```
[ { "Entry": "/directory1", "Target": "/bucket_name/home/
mydirectory" } ]
```

在大多數情況下，您可以使用此值而不是工作階段原則，將使用者鎖定到指定的主目錄 (」chroot「)。若要這麼做，您可Entry以設定/並設Target定為使用者在登入時應該看到的主目錄的值。

以下是的Entry和Target配對範例chroot。

```
[ { "Entry": "/", "Target": "/bucket_name/home/mydirectory" } ]
```

類型：HomeDirectoryMapEntry 物件陣列

陣列成員：項目數下限為 1。5 萬個物品的最大數量。

必要：否

HomeDirectoryType

使用者登入伺服器時，您希望的使用者主目錄之登陸目錄 (資料夾) 類型。如果將其設定為PATH，使用者將在其檔案傳輸協定用戶端中看到絕對的 Amazon S3 儲存貯體或 Amazon EFS 路徑。如果將其設定為LOGICAL，則需要在中提供對應，以便讓使用者看到 Amazon S3 或 Amazon EFS 路徑的方式。HomeDirectoryMappings

> **Note**
>
> 如果HomeDirectoryType是LOGICAL，則必須使用HomeDirectoryMappings參數提供對映。另一方面，HomeDirectoryType如果您使用HomeDirectory參數提供絕對路徑。PATH您的範本HomeDirectoryMappings中不HomeDirectory能同時擁有和。

類型：字串

有效值:PATH | LOGICAL

必要：否

Policy

適用於您的使用者的工作階段政策，以便您可以在多個使用者間使用相同的 AWS Identity and Access Management (IAM) 角色。此政策限制了使用者對 Amazon S3 儲存貯體部分的存取權限。您可以在此政策內使用的變數包括 ${Transfer:UserName}、${Transfer:HomeDirectory} 和 ${Transfer:HomeBucket}。

> **Note**
>
> 只有在的網域ServerId是 Amazon S3 時，才適用此政策。Amazon EFS 不使用工作階段政策。
> 對於工作階段政策，請將政策 AWS Transfer Family 儲存為 JSON Blob，而不是政策的 Amazon 資源名稱 (ARN)。您會將政策作為 JSON blob 儲存，並在 Policy 引數中傳遞它。
> 如需工作階段政策的範例，請參閱 Example session policy (工作階段政策範例)。
> 如需詳細資訊，請參閱 AWS 安全性權杖服務 API 參考AssumeRole中的。

類型：字串

長度限制：長度下限為 0。長度上限為 2048。

必要：否

PosixProfile

指定完整的 POSIX 身分，包括使用者 ID (Uid)、群組 ID (Gid) 和任何次要群組 ID (SecondaryGids)，以控制使用者對 Amazon EFS 檔案系統的存取。Amazon EFS 中檔案和目錄上設定的 POSIX 許可決定使用者在將檔案傳入和傳出 Amazon EFS 檔案系統時獲得的存取層級。

類型：PosixProfile 物件

必要：否

Role

(IAM) 角色的亞馬遜資源名稱 AWS Identity and Access Management (ARN)，用於控制使用者對 Amazon S3 儲存貯體或 Amazon EFS 檔案系統的存取。連接到此角色的政策會決定在將檔案傳入和傳出您的 Amazon S3 儲存貯體或 Amazon EFS 檔案系統時，您希望提供給使用者的存取層級。IAM 角色也應包含信任關係，允許伺服器在處理您使用者的傳輸請求時，存取您的資源。

類型：字串

長度限制：長度下限為 20。長度上限為 2048。

模式：`arn:.*role/\S+`

必要：是

ServerId

伺服器執行個體的系統指派唯一識別碼。這是您新增使用者的特定目標伺服器。

類型：字串

長度約束：固定長度為 19。

模式：`s-([0-9a-f]{17})`

必要：是

SshPublicKeyBody

用於向伺服器驗證使用者的安全殼層 (SSH) 金鑰的公開部分。

三個標準安全殼層公開金鑰格式元素是<key type><body base64>、和選用的<comment>，每個元素之間都有空格。

AWS Transfer Family 接受 RSA、ECDSA 和 ED25519 金鑰。

- 對於 RSA 金鑰，金鑰類型為ssh-rsa。
- 對於 ED25519 金鑰，金鑰類型為ssh-ed25519。
- 對於 ECDSA 金鑰，金鑰類型為ecdsa-sha2-nistp256、或 ecdsa-sha2-nistp384ecdsa-sha2-nistp521，視您產生的金鑰大小而定。

類型：字串

長度限制：長度下限為 0。長度上限為 2048。

必要：否

Tags

鍵/值對，可用來分組和搜尋使用者。標籤是基於任何用途連接到使用者的中繼資料。

類型：Tag 物件陣列

陣列成員：項目數下限為 1。項目數上限為 50。

必要：否

UserName

識別使用者並且和 ServerId 建立關聯的唯一字串。此使用者名稱的長度必須最少為 3 個字元，最多為 100 個字元。以下是有效字元：a-z、A-Z、0-9、底線 '_'、連字號 '-'、句號 '.'，以及位置符號 '@'。使用者名稱不能以連字號、句號或符號開頭。

類型：字串

長度限制：長度下限為 3。長度上限為 100。

模式：[\w][\w@.-]{2,99}

必要：是

回應語法

```
{
```

```
    "ServerId": "string",
    "UserName": "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。

ServerId

使用者所附加之伺服器的識別碼。

類型：字串

長度約束：固定長度為 19。

模式：`s-([0-9a-f]{17})`

UserName

識別 Transfer Family 使用者的唯一字串。

類型：字串

長度限制：長度下限為 3。長度上限為 100。

模式：`[\w][\w@.-]{2,99}`

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceExistsException

請求的資源不存在，或者存在於為命令指定的區域以外的區域中。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

HTTP 狀態碼：500

範例

範例

若要建立使用者，您可以先將參數儲存到 JSON 檔案中`createUserParameters`，然後執行建立使用者 API 命令。

```
{
    "HomeDirectory": "/DOC-EXAMPLE-BUCKET",
    "HomeDirectoryType": "PATH",
    "Role": "arn:aws:iam::111122223333:role/bob-role",
    "ServerId": "s-1111aaaa2222bbbb3",
    "SshPublicKeyBody": "ecdsa-sha2-nistp521 AAAAE2VjZHNhLXNoYTItbmlzdHA...
 bobusa@mycomputer.us-east-1.amazon.com",
    "UserName": "bobusa-API"
}
```

請求範例

```
aws transfer create-user --cli-input-json file://createUserParameters
```

回應範例

```
{
```

```
    "ServerId": ""s-1111aaaa2222bbbb3",
    "UserName": "bobusa-API"
}
```

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

CreateWorkflow

可讓您建立工作流程，其中包含檔案傳輸完成後工作流程叫用的指定步驟和步驟詳細資訊。建立工作流程之後，您可以在 CreateServer 和 UpdateServer 操作中指定 workflow-details 欄位，將建立的工作流程與任何傳輸伺服器建立關聯。

請求語法

```
{
   "Description": "string",
   "OnExceptionSteps": [
      {
         "CopyStepDetails": {
            "DestinationFileLocation": {
               "EfsFileLocation": {
                  "FileSystemId": "string",
                  "Path": "string"
               },
               "S3FileLocation": {
                  "Bucket": "string",
                  "Key": "string"
               }
            },
            "Name": "string",
            "OverwriteExisting": "string",
            "SourceFileLocation": "string"
         },
         "CustomStepDetails": {
            "Name": "string",
            "SourceFileLocation": "string",
            "Target": "string",
            "TimeoutSeconds": number
         },
         "DecryptStepDetails": {
            "DestinationFileLocation": {
               "EfsFileLocation": {
                  "FileSystemId": "string",
                  "Path": "string"
               },
               "S3FileLocation": {
                  "Bucket": "string",
                  "Key": "string"
               }
```

```
            },
            "Name": "string",
            "OverwriteExisting": "string",
            "SourceFileLocation": "string",
            "Type": "string"
         },
         "DeleteStepDetails": {
            "Name": "string",
            "SourceFileLocation": "string"
         },
         "TagStepDetails": {
            "Name": "string",
            "SourceFileLocation": "string",
            "Tags": [
               {
                  "Key": "string",
                  "Value": "string"
               }
            ]
         },
         "Type": "string"
      }
   ],
   "Steps": [
      {
         "CopyStepDetails": {
            "DestinationFileLocation": {
               "EfsFileLocation": {
                  "FileSystemId": "string",
                  "Path": "string"
               },
               "S3FileLocation": {
                  "Bucket": "string",
                  "Key": "string"
               }
            },
            "Name": "string",
            "OverwriteExisting": "string",
            "SourceFileLocation": "string"
         },
         "CustomStepDetails": {
            "Name": "string",
            "SourceFileLocation": "string",
            "Target": "string",
```

```
            "TimeoutSeconds": number
         },
         "DecryptStepDetails": {
            "DestinationFileLocation": {
               "EfsFileLocation": {
                  "FileSystemId": "string",
                  "Path": "string"
               },
               "S3FileLocation": {
                  "Bucket": "string",
                  "Key": "string"
               }
            },
            "Name": "string",
            "OverwriteExisting": "string",
            "SourceFileLocation": "string",
            "Type": "string"
         },
         "DeleteStepDetails": {
            "Name": "string",
            "SourceFileLocation": "string"
         },
         "TagStepDetails": {
            "Name": "string",
            "SourceFileLocation": "string",
            "Tags": [
               {
                  "Key": "string",
                  "Value": "string"
               }
            ]
         },
         "Type": "string"
      }
   ],
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

Description

工作流程的文字描述。

類型：字串

長度限制：長度下限為 0。長度上限為 256。

模式：`[\w- ]*`

必要：否

OnExceptionSteps

指定工作流程執行期間遇到錯誤時要採取的步驟 (動作)。

> **Note**
>
> 對於自訂步驟，Lambda 函數需要傳送`FAILURE`至回呼 API 以啟動例外狀況步驟。此外，如果 Lambda 未在逾時`SUCCESS`之前傳送，則會執行例外步驟。

類型：WorkflowStep 物件陣列

陣列成員：項目數下限為 0。最多 8 個項目數。

必要：否

Steps

指定在指定工作流程中步驟的詳細資訊。

`TYPE`指定要針對此步驟採取下列哪些動作。

- **`COPY`** - 將檔案複製到另一個位置。
- **`CUSTOM`**-使用 AWS Lambda 函數目標執行自訂步驟。
- **`DECRYPT`** - 解密上傳前已加密的檔案。

- **DELETE** - 刪除檔案。
- **TAG** - 在檔案中新增標籤。

> **Note**
>
> 目前，僅 S3 支援複製和標記。

對於檔案位置，您可以指定 Amazon S3 儲存貯體和金鑰，或指定 Amazon EFS 檔案系統識別碼和路徑。

類型：WorkflowStep 物件陣列

陣列成員：項目數下限為 0。最多 8 個項目數。

必要：是

Tags

鍵/值對，可用來分組和搜尋工作流程。標籤是基於任何用途連接到工作流程的中繼資料。

類型：Tag 物件陣列

陣列成員：項目數下限為 1。項目數上限為 50。

必要：否

回應語法

```
{
   "WorkflowId": "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。

WorkflowId

工作流程的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：`w-([a-z0-9]{17})`

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：400

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceExistsException

請求的資源不存在，或存在於為命令指定的區域以外的區域中。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

HTTP 狀態碼：500

ThrottlingException

由於請求調節，因此請求遭到拒絕。

HTTP 狀態碼：400

範例

範例

您可以將工作流程步驟資訊儲存到文字檔案中，然後使用該檔案來建立工作流程，如下列範例所示。下列範例假設您已將工作流程步驟儲存至 *example-file.json* (與您執行命令的相同資料夾中)，且您想要在維吉尼亞北部 (us-east-1) 區域建立工作流程。

```
aws transfer create-workflow --description "example workflow from a file" --steps
 file://example-file.json --region us-east-1
```

```
// Example file containing workflow steps
[
   {
     "Type": "TAG",
     "TagStepDetails": {
        "Name": "TagStep",
        "Tags": [
          {
            "Key": "name",
            "Value": "testTag"
          }
        ]
     }
   },
   {
     "Type": "COPY",
     "CopyStepDetails": {
        "Name": "CopyStep",
        "DestinationFileLocation": {
        "S3FileLocation": {
           "Bucket": "DOC-EXAMPLE-BUCKET",
           "Key": "DOC-EXAMPLE-KEY/"
                  }
        },
        "OverwriteExisting": "TRUE",
        "SourceFileLocation": "${original.file}"
     }
   },
   {
     "Type": "DELETE",
     "DeleteStepDetails":{
```

```
      "Name":"DeleteStep",
      "SourceFileLocation": "${original.file}"
      }
   }
]
```

範例

`CreateWorkflow`呼叫會傳回新工作流程的工作流程 ID。

回應範例

```
{
    "WorkflowId": "w-1234abcd5678efghi"
}
```

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

DeleteAccess

可讓您刪除ServerID和ExternalID參數中指定的存取權。

請求語法

```
{
   "ExternalId": "string",
   "ServerId": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

ExternalId

識別目錄中特定群組所需的唯一識別碼。您關聯之群組的使用者可以透過已啟用的協定存取 Amazon S3 或 Amazon EFS 資源 AWS Transfer Family。如果您知道群組名稱，您可以使用 Windows 執行下列命令來檢視 SID 值 PowerShell。

```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties
* | Select SamAccountName,ObjectSid
```

在該命令中，YourGroupName用您的活動目錄組的名稱替換。

用來驗證此參數的規則運算式是由不含空格的大寫和小寫英數字元所組成的字元字串。您也可以包含底線或下列任何字元：=, 。 @：/-

類型：字串

長度限制：長度下限為 1。長度上限為 256。

模式：S-1-[\d-]+

必要：是

ServerId

系統指派給已指派此使用者之伺服器的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：`s-([0-9a-f]{17})`

必要：是

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

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

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 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

DeleteAgreement

刪除提供的中指定的合約AgreementId。

請求語法

```
{
   "AgreementId": "string",
   "ServerId": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

AgreementId

合約的唯一識別碼。建立協定時會傳回此識別元。

類型：字串

長度約束：固定長度為 19。

模式：a-([0-9a-f]{17})

必要：是

ServerId

與您要刪除之合約相關聯的伺服器識別碼。

類型：字串

長度約束：固定長度為 19。

模式：s-([0-9a-f]{17})

必要：是

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

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

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 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

DeleteCertificate

刪除CertificateId參數中指定的憑證。

請求語法

```
{
   "CertificateId": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

CertificateId

您要刪除之憑證物件的識別碼。

類型：字串

長度約束：固定長度為 22。

模式：cert-([0-9a-f]{17})

必要：是

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

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

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

DeleteConnector

刪除提供的中指定的連接器ConnectorId。

請求語法

```
{
   "ConnectorId": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

ConnectorId

連接器的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：c-([0-9a-f]{17})

必要：是

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

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

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

DeleteHostKey

刪除HostKeyId參數中指定的主機金鑰。

請求語法

```
{
   "HostKeyId": "string",
   "ServerId": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

HostKeyId

您要刪除之主機金鑰的識別碼。

類型：字串

長度約束：固定長度為 25。

模式：hostkey-[0-9a-f]{17}

必要：是

ServerId

包含要刪除之主機金鑰之伺服器的識別碼。

類型：字串

長度約束：固定長度為 19。

模式：s-([0-9a-f]{17})

必要：是

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

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

HTTP 狀態碼：500

ThrottlingException

由於請求調節，因此請求遭到拒絕。

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

DeleteProfile

刪除ProfileId參數中指定的設定檔。

請求語法

```
{
   "ProfileId": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

ProfileId

您要刪除之設定檔的識別碼。

類型：字串

長度約束：固定長度為 19。

模式：p-([0-9a-f]{17})

必要：是

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

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

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

DeleteServer

刪除您指定的已啟用檔案傳輸通訊協定的伺服器。

此作業未傳回任何回應。

請求語法

```
{
   "ServerId": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

ServerId

系統指派給伺服器執行個體的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：`s-([0-9a-f]{17})`

必要：是

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

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：400

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

HTTP 狀態碼：500

範例

範例

下列範例會刪除伺服器。

請求範例

```
{
   "ServerId": "s-01234567890abcdef"
}
```

範例

如果成功，則不會返回任何內容。

回應範例

```
{
```

```
}
```

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

DeleteSshPublicKey

刪除使用者的安全殼層 (SSH) 公開金鑰。

請求語法

```
{
   "ServerId": "string",
   "SshPublicKeyId": "string",
   "UserName": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

ServerId

系統指派給已啟用檔案傳輸通訊協定的伺服器執行個體的唯一識別碼，其使用者已指派給該執行個體。

類型：字串

長度約束：固定長度為 19。

模式：`s-([0-9a-f]{17})`

必要：是

SshPublicKeyId

用來參照使用者特定安全殼層金鑰的唯一識別碼。

類型：字串

長度限制：固定長度為 21。

模式：`key-[0-9a-f]{17}`

必要：是

UserName

識別要刪除其公開金鑰之使用者的唯一字串。

類型：字串

長度限制：長度下限為 3。長度上限為 100。

模式：`[\w][\w@.-]{2,99}`

必要：是

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

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

HTTP 狀態碼：500

ThrottlingException

由於請求調節，因此請求遭到拒絕。

HTTP 狀態碼：400

範例

範例

下列範例會刪除使用者的安全殼層公開金鑰。

請求範例

```
{
   "ServerId": "s-01234567890abcdef",
   "SshPublicKeyId": "MyPublicKey",
   "UserName": "my_user"
}
```

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

DeleteUser

刪除屬於您指定之已啟用檔案傳輸通訊協定之伺服器的使用者。

此作業未傳回任何回應。

> **Note**
>
> 當您從伺服器刪除使用者時，該使用者的資訊會遺失。

請求語法

```
{
   "ServerId": "string",
   "UserName": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

ServerId

系統指派給伺服器執行個體的唯一識別碼，其中已指派使用者。

類型：字串

長度約束：固定長度為 19。

模式：`s-([0-9a-f]{17})`

必要：是

UserName

識別從伺服器刪除之使用者的唯一字串。

類型：字串

長度限制：長度下限為 3。長度上限為 100。

模式：[\w][\w@.-]{2,99}

必要：是

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

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

HTTP 狀態碼：500

範例

範例

下列範例會刪除「Transfer Family」使用者。

請求範例

```
{
   "ServerId": "s-01234567890abcdef",
   "UserNames": "my_user"
}
```

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

DeleteWorkflow

刪除指定的工作流程。

請求語法

```
{
   "WorkflowId": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

WorkflowId

工作流程的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：`w-([a-z0-9]{17})`

必要：是

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

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：400

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

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 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

DescribeAccess

描述指派給已啟用特定檔案傳輸通訊協定之伺服器的存取權，如其ServerId內容及其識別。ExternalId

此呼叫的回應會傳回與指定ServerId值相關聯的存取屬性。

請求語法

```
{
   "ExternalId": "string",
   "ServerId": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

ExternalId

識別目錄中特定群組所需的唯一識別碼。您關聯之群組的使用者可以透過已啟用的協定存取 Amazon S3 或 Amazon EFS 資源 AWS Transfer Family。如果您知道群組名稱，您可以使用 Windows 執行下列命令來檢視 SID 值 PowerShell。

```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties
* | Select SamAccountName,ObjectSid
```

在該命令中，YourGroupName用您的活動目錄組的名稱替換。

用來驗證此參數的規則運算式是由不含空格的大寫和小寫英數字元所組成的字元字串。您也可以包含底線或下列任何字元：=, 。 @：/-

類型：字串

長度限制：長度下限為 1。長度上限為 256。

模式：S-1-[\d-]+

必要：是

ServerId

系統指派給已指派此存取權之伺服器的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：s-([0-9a-f]{17})

必要：是

回應語法

```
{
   "Access": {
      "ExternalId": "string",
      "HomeDirectory": "string",
      "HomeDirectoryMappings": [
         {
            "Entry": "string",
            "Target": "string",
            "Type": "string"
         }
      ],
      "HomeDirectoryType": "string",
      "Policy": "string",
      "PosixProfile": {
         "Gid": number,
         "SecondaryGids": [ number ],
         "Uid": number
      },
      "Role": "string"
   },
   "ServerId": "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。

Access

存取所附加之伺服器的外部識別碼。

類型：DescribedAccess 物件

ServerId

系統指派給已指派此存取權之伺服器的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：`s-([0-9a-f]{17})`

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

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

DescribeAgreement

描述由識別的合約AgreementId。

請求語法

```
{
   "AgreementId": "string",
   "ServerId": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

AgreementId

合約的唯一識別碼。建立協定時會傳回此識別元。

類型：字串

長度約束：固定長度為 19。

模式：a-([0-9a-f]{17})

必要：是

ServerId

與合約相關聯的伺服器識別碼。

類型：字串

長度約束：固定長度為 19。

模式：s-([0-9a-f]{17})

必要：是

回應語法

```
{
```

```
   "Agreement": {
      "AccessRole": "string",
      "AgreementId": "string",
      "Arn": "string",
      "BaseDirectory": "string",
      "Description": "string",
      "LocalProfileId": "string",
      "PartnerProfileId": "string",
      "ServerId": "string",
      "Status": "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。

Agreement

指定協定的詳細資訊，以DescribedAgreement物件形式傳回。

類型：DescribedAgreement 物件

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

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

DescribeCertificate

描述由識別的憑證CertificateId。

請求語法

```
{
   "CertificateId": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

CertificateId

已匯入憑證的識別碼陣列。您可以使用此識別碼處理設定檔和合作夥伴設定檔。

類型：字串

長度約束：固定長度為 22。

模式：cert-([0-9a-f]{17})

必要：是

回應語法

```
{
   "Certificate": {
      "ActiveDate": number,
      "Arn": "string",
      "Certificate": "string",
      "CertificateChain": "string",
      "CertificateId": "string",
      "Description": "string",
      "InactiveDate": number,
      "NotAfterDate": number,
      "NotBeforeDate": number,
```

```
      "Serial": "string",
      "Status": "string",
      "Tags": [
         {
            "Key": "string",
            "Value": "string"
         }
      ],
      "Type": "string",
      "Usage": "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。

Certificate

指定憑證的詳細資料，以物件傳回。

類型：DescribedCertificate 物件

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

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

DescribeConnector

描述由以下項目識別的連接器 ConnectorId.

請求語法

```
{
   "ConnectorId": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

ConnectorId

連接器的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：c-([0-9a-f]{17})

必要：是

回應語法

```
{
   "Connector": {
      "AccessRole": "string",
      "Arn": "string",
      "As2Config": {
         "BasicAuthSecretId": "string",
         "Compression": "string",
         "EncryptionAlgorithm": "string",
         "LocalProfileId": "string",
         "MdnResponse": "string",
         "MdnSigningAlgorithm": "string",
```

```
         "MessageSubject": "string",
         "PartnerProfileId": "string",
         "SigningAlgorithm": "string"
      },
      "ConnectorId": "string",
      "LoggingRole": "string",
      "SecurityPolicyName": "string",
      "ServiceManagedEgressIpAddresses": [ "string" ],
      "SftpConfig": {
         "TrustedHostKeys": [ "string" ],
         "UserSecretId": "string"
      },
      "Tags": [
         {
            "Key": "string",
            "Value": "string"
         }
      ],
      "Url": "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。

Connector

包含連接器詳細資訊的結構。

類型：DescribedConnector 物件

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

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 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

DescribeExecution

您可以使DescribeExecution用檢查指定工作流程執行的詳細資訊。

> **Note**
>
> 此 API 呼叫只會傳回進行中工作流程的詳細資料。
> 如果您為未進行中的執行提供 ID，或者執行與指定的工作流程 ID 不符，則會收到ResourceNotFound例外狀況。

請求語法

```
{
   "ExecutionId": "string",
   "WorkflowId": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

ExecutionId

用於執行工作流程的唯一識別元。

類型：字串

長度約束：固定長度為 36。

模式：[0-9a-fA-F]{8}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{12}

必要：是

WorkflowId

工作流程的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：w-([a-z0-9]{17})

必要：是

回應語法

```
{
   "Execution": {
      "ExecutionId": "string",
      "ExecutionRole": "string",
      "InitialFileLocation": {
         "EfsFileLocation": {
            "FileSystemId": "string",
            "Path": "string"
         },
         "S3FileLocation": {
            "Bucket": "string",
            "Etag": "string",
            "Key": "string",
            "VersionId": "string"
         }
      },
      "LoggingConfiguration": {
         "LoggingRole": "string",
         "LogGroupName": "string"
      },
      "PosixProfile": {
         "Gid": number,
         "SecondaryGids": [ number ],
         "Uid": number
      },
      "Results": {
         "OnExceptionSteps": [
            {
               "Error": {
                  "Message": "string",
                  "Type": "string"
               },
               "Outputs": "string",
               "StepType": "string"
            }
```

```
         ],
         "Steps": [
            {
               "Error": {
                  "Message": "string",
                  "Type": "string"
               },
               "Outputs": "string",
               "StepType": "string"
            }
         ]
      },
      "ServiceMetadata": {
         "UserDetails": {
            "ServerId": "string",
            "SessionId": "string",
            "UserName": "string"
         }
      },
      "Status": "string"
   },
   "WorkflowId": "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。

Execution

包含工作流程執行詳細資訊的結構。

類型：DescribedExecution 物件

WorkflowId

工作流程的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：`w-([a-z0-9]{17})`

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

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

DescribeHostKey

傳回與所指定之主機金鑰的詳細資HostKeyId料ServerId。

請求語法

```
{
   "HostKeyId": "string",
   "ServerId": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

HostKeyId

您要描述之主機金鑰的識別碼。

類型：字串

長度約束：固定長度為 25。

模式：hostkey-[0-9a-f]{17}

必要：是

ServerId

包含您要描述之主機金鑰之伺服器的識別碼。

類型：字串

長度約束：固定長度為 19。

模式：s-([0-9a-f]{17})

必要：是

回應語法

```
{
```

```
   "HostKey": {
      "Arn": "string",
      "DateImported": number,
      "Description": "string",
      "HostKeyFingerprint": "string",
      "HostKeyId": "string",
      "Tags": [
         {
            "Key": "string",
            "Value": "string"
         }
      ],
      "Type": "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。

HostKey

返回指定主機密鑰的詳細信息。

類型：DescribedHostKey 物件

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

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

DescribeProfile

傳回由指定之設定檔的詳細資訊ProfileId。

請求語法

```
{
   "ProfileId": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

ProfileId

您要描述之設定檔的識別碼。

類型：字串

長度約束：固定長度為 19。

模式：p-([0-9a-f]{17})

必要：是

回應語法

```
{
   "Profile": {
      "Arn": "string",
      "As2Id": "string",
      "CertificateIds": [ "string" ],
      "ProfileId": "string",
      "ProfileType": "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。

Profile

指定配置文件的詳細信息，作為對象返回。

類型：DescribedProfile 物件

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

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

DescribeSecurityPolicy

說明附加至伺服器或 SFTP 連接器的安全性原則。回應包含安全性原則屬性的說明。如需有關安全性原則的詳細資訊，請參閱使用伺服器的安全性原則或使用 SFTP 連接器的安全性原則。

請求語法

```
{
   "SecurityPolicyName": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

SecurityPolicyName

指定您要取得詳細資料之安全原則的文字名稱。

類型：字串

長度限制：長度下限為 0。長度上限為 100。

模式：Transfer[A-Za-z0-9]*SecurityPolicy-[A-Za-z0-9-]+

必要：是

回應語法

```
{
   "SecurityPolicy": {
      "Fips": boolean,
      "Protocols": [ "string" ],
      "SecurityPolicyName": "string",
      "SshCiphers": [ "string" ],
      "SshHostKeyAlgorithms": [ "string" ],
      "SshKexs": [ "string" ],
      "SshMacs": [ "string" ],
      "TlsCiphers": [ "string" ],
```

```
        "Type": "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。

SecurityPolicy

包含安全性原則內容的陣列。

類型：DescribedSecurityPolicy 物件

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

HTTP 狀態碼：500

範例

範例

下列範例命令會使用安全性原則名稱做為引數，並傳回指定安全性原則的演算法。

請求範例

```
aws transfer describe-security-policy --security-policy-name "TransferSecurityPolicy-
FIPS-2023-05"
```

回應範例

```
{
    "SecurityPolicy": {
        "Fips": true,
        "SecurityPolicyName": "TransferSecurityPolicy-FIPS-2023-05",
        "SshCiphers": [
            "aes256-gcm@openssh.com",
            "aes128-gcm@openssh.com",
            "aes256-ctr",
            "aes192-ctr"
        ],
        "SshKexs": [
            "diffie-hellman-group16-sha512",
            "diffie-hellman-group18-sha512",
            "diffie-hellman-group-exchange-sha256"
        ],
        "SshMacs": [
            "hmac-sha2-256-etm@openssh.com",
            "hmac-sha2-512-etm@openssh.com"
        ],
        "TlsCiphers": [
            "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
            "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
            "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
            "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
            "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
            "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
            "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
            "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
        ]
    }
```

```
}
```

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

DescribeServer

說明您透過傳遞參ServerId數來指定的已啟用檔案傳輸通訊協定的伺服器。

響應包含服務器屬性的描述。當您設定EndpointType為 VPC 時，回應將包含. EndpointDetails

請求語法

```
{
   "ServerId": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

ServerId

系統指派給伺服器的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：s-([0-9a-f]{17})

必要：是

回應語法

```
{
   "Server": {
      "Arn": "string",
      "As2ServiceManagedEgressIpAddresses": [ "string" ],
      "Certificate": "string",
      "Domain": "string",
      "EndpointDetails": {
         "AddressAllocationIds": [ "string" ],
         "SecurityGroupIds": [ "string" ],
         "SubnetIds": [ "string" ],
         "VpcEndpointId": "string",
```

```
      "VpcId": "string"
   },
   "EndpointType": "string",
   "HostKeyFingerprint": "string",
   "IdentityProviderDetails": {
      "DirectoryId": "string",
      "Function": "string",
      "InvocationRole": "string",
      "SftpAuthenticationMethods": "string",
      "Url": "string"
   },
   "IdentityProviderType": "string",
   "LoggingRole": "string",
   "PostAuthenticationLoginBanner": "string",
   "PreAuthenticationLoginBanner": "string",
   "ProtocolDetails": {
      "As2Transports": [ "string" ],
      "PassiveIp": "string",
      "SetStatOption": "string",
      "TlsSessionResumptionMode": "string"
   },
   "Protocols": [ "string" ],
   "S3StorageOptions": {
      "DirectoryListingOptimization": "string"
   },
   "SecurityPolicyName": "string",
   "ServerId": "string",
   "State": "string",
   "StructuredLogDestinations": [ "string" ],
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ],
   "UserCount": number,
   "WorkflowDetails": {
      "OnPartialUpload": [
         {
            "ExecutionRole": "string",
            "WorkflowId": "string"
         }
      ],
      "OnUpload": [
```

```
            {
               "ExecutionRole": "string",
               "WorkflowId": "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。

Server

包含具有ServerID您指定之伺服器屬性的陣列。

類型：DescribedServer 物件

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

HTTP 狀態碼：500

範例

範例

下列範例會傳回指派給伺服器的屬性。

請求範例

```
{
   "ServerId": "s-01234567890abcdef"
}
```

範例

此範例說明的一種用法 DescribeServer。

回應範例

```
{
    "Server": {
        "Arn": "arn:aws:transfer:us-east-1:176354371281:server/s-01234567890abcdef",
        "EndpointDetails": {
            "AddressAllocationIds": [
                "eipalloc-01a2eabe3c04d5678",
                "eipalloc-102345be"
            ],
            "SubnetIds": [
                "subnet-047eaa7f0187a7cde",
                "subnet-0a2d0f474daffde18"
            ],
            "VpcEndpointId": "vpce-03fe0080e7cb008b8",
            "VpcId": "vpc-09047a51f1c8e1634"
        },
        "EndpointType": "VPC",
```

```
        "HostKeyFingerprint": "your host key,
        "IdentityProviderType": "SERVICE_MANAGED",
        "ServerId": "s-01234567890abcdef",
        "State": "ONLINE",
        "Tags": [],
        "UserCount": 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 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

DescribeUser

描述指派給已啟用檔案傳輸通訊協定之特定伺服器的使用者，如其ServerId內容所識別。

此呼叫的回應會傳回與指定ServerId值相關聯的使用者屬性。

請求語法

```
{
   "ServerId": "string",
   "UserName": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

ServerId

系統指派給已指派此使用者之伺服器的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：s-([0-9a-f]{17})

必要：是

UserName

指派給一或多部伺服器的使用者名稱。使用者名稱是使用 AWS Transfer Family 服務和執行檔案傳輸工作的登入認證的一部分。

類型：字串

長度限制：長度下限為 3。長度上限為 100。

模式：[\w][\w@.-]{2,99}

必要：是

回應語法

```
{
   "ServerId": "string",
   "User": {
      "Arn": "string",
      "HomeDirectory": "string",
      "HomeDirectoryMappings": [
         {
            "Entry": "string",
            "Target": "string",
            "Type": "string"
         }
      ],
      "HomeDirectoryType": "string",
      "Policy": "string",
      "PosixProfile": {
         "Gid": number,
         "SecondaryGids": [ number ],
         "Uid": number
      },
      "Role": "string",
      "SshPublicKeys": [
         {
            "DateImported": number,
            "SshPublicKeyBody": "string",
            "SshPublicKeyId": "string"
         }
      ],
      "Tags": [
         {
            "Key": "string",
            "Value": "string"
         }
      ],
      "UserName": "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。

ServerId

系統指派給已指派此使用者之伺服器的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：`s-([0-9a-f]{17})`

User

陣列，其中包含您指定`ServerID`值的「Transfer Family」使用者性質。

類型：DescribedUser 物件

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

HTTP 狀態碼：500

範例

範例

下列範例顯示現有使用者的詳細資訊。

請求範例

```
aws transfer describe-user --server-id s-1111aaaa2222bbbb3 --user-name bob-test
```

回應範例

```
{
    "ServerId": "s-1111aaaa2222bbbb3",
    "User": {
        "Arn": "arn:aws:transfer:us-east-1:111122223333:user/s-1111aaaa2222bbbb3/bob-
test",
        "HomeDirectory": "/DOC-EXAMPLE-BUCKET",
        "HomeDirectoryType": "PATH",
        "Role": "arn:aws:iam::111122223333:role/bob-role",
        "SshPublicKeys": [
            {
                "DateImported": "2022-03-31T12:27:52.614000-04:00",
                "SshPublicKeyBody": "ssh-rsa AAAAB3NzaC1yc..... bobusa@mycomputer.us-
east-1.amaazon.com",
                "SshPublicKeyId": "key-abcde12345fghik67"
            }
        ],
        "Tags": [],
        "UserName": "bob-test"
    }
}
```

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

DescribeWorkflow

描述指定的工作流程。

請求語法

```
{
   "WorkflowId": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

WorkflowId

工作流程的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：w-([a-z0-9]{17})

必要：是

回應語法

```
{
   "Workflow": {
      "Arn": "string",
      "Description": "string",
      "OnExceptionSteps": [
         {
            "CopyStepDetails": {
               "DestinationFileLocation": {
                  "EfsFileLocation": {
                     "FileSystemId": "string",
                     "Path": "string"
                  },
                  "S3FileLocation": {
```

```
                "Bucket": "string",
                "Key": "string"
            }
        },
        "Name": "string",
        "OverwriteExisting": "string",
        "SourceFileLocation": "string"
    },
    "CustomStepDetails": {
        "Name": "string",
        "SourceFileLocation": "string",
        "Target": "string",
        "TimeoutSeconds": number
    },
    "DecryptStepDetails": {
        "DestinationFileLocation": {
            "EfsFileLocation": {
                "FileSystemId": "string",
                "Path": "string"
            },
            "S3FileLocation": {
                "Bucket": "string",
                "Key": "string"
            }
        },
        "Name": "string",
        "OverwriteExisting": "string",
        "SourceFileLocation": "string",
        "Type": "string"
    },
    "DeleteStepDetails": {
        "Name": "string",
        "SourceFileLocation": "string"
    },
    "TagStepDetails": {
        "Name": "string",
        "SourceFileLocation": "string",
        "Tags": [
            {
                "Key": "string",
                "Value": "string"
            }
        ]
    },
```

```
            "Type": "string"
         }
      ],
      "Steps": [
         {
            "CopyStepDetails": {
               "DestinationFileLocation": {
                  "EfsFileLocation": {
                     "FileSystemId": "string",
                     "Path": "string"
                  },
                  "S3FileLocation": {
                     "Bucket": "string",
                     "Key": "string"
                  }
               },
               "Name": "string",
               "OverwriteExisting": "string",
               "SourceFileLocation": "string"
            },
            "CustomStepDetails": {
               "Name": "string",
               "SourceFileLocation": "string",
               "Target": "string",
               "TimeoutSeconds": number
            },
            "DecryptStepDetails": {
               "DestinationFileLocation": {
                  "EfsFileLocation": {
                     "FileSystemId": "string",
                     "Path": "string"
                  },
                  "S3FileLocation": {
                     "Bucket": "string",
                     "Key": "string"
                  }
               },
               "Name": "string",
               "OverwriteExisting": "string",
               "SourceFileLocation": "string",
               "Type": "string"
            },
            "DeleteStepDetails": {
               "Name": "string",
```

```
                "SourceFileLocation": "string"
            },
            "TagStepDetails": {
                "Name": "string",
                "SourceFileLocation": "string",
                "Tags": [
                    {
                        "Key": "string",
                        "Value": "string"
                    }
                ]
            },
            "Type": "string"
        }
    ],
    "Tags": [
        {
            "Key": "string",
            "Value": "string"
        }
    ],
    "WorkflowId": "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。

Workflow

包含工作流程詳細資訊的結構。

類型：DescribedWorkflow 物件

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

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

ImportCertificate

匯入建立本機 (AS2) 設定檔和合作夥伴設定檔所需的簽署和加密憑證。

請求語法

```
{
   "ActiveDate": number,
   "Certificate": "string",
   "CertificateChain": "string",
   "Description": "string",
   "InactiveDate": number,
   "PrivateKey": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ],
   "Usage": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

ActiveDate

選擇性日期，指定憑證變為作用的時間。

類型：Timestamp

必要：否

Certificate

- 針對 CLI，請以 URI 格式提供憑證的檔案路徑。例如 `--certificate file://encryption-cert.pem`。或者，您可以提供原始內容。
- 針對 SDK，指定憑證檔案的原始內容。例如 `--certificate "`cat encryption-cert.pem`"`。

類型：字串

長度限制：長度下限為 1。長度上限為 16384。

模式：`[\u0009\u000A\u000D\u0020-\u00FF]*`

必要：是

CertificateChain

組成要匯入之憑證鏈結的選擇性憑證清單。

類型：字串

長度限制：長度下限為 1。最大長度

模式：`[\u0009\u000A\u000D\u0020-\u00FF]*`

必要：否

Description

有助於識別憑證的簡短說明。

類型：字串

長度限制：長度下限為 1。長度上限為 200。

模式：`[\p{Graph}]+`

必要：否

InactiveDate

選擇性日期，指定憑證變為停用的時間。

類型：Timestamp

必要：否

PrivateKey

- 針對 CLI，請以 URI 格式提供私密金鑰的檔案路徑。例如，。`--private-key file://encryption-key.pem`或者，您可以提供私密金鑰檔案的原始內容。
- 針對 SDK，指定私密金鑰檔案的原始內容。例如：`--private-key "`cat encryption-key.pem`"`

類型：字串

長度限制：長度下限為 1。長度上限為 16384。

模式：[\u0009\u000A\u000D\u0020-\u00FF]*

必要：否

Tags

金鑰/值對，可用來分組和搜尋憑證。

類型：Tag 物件陣列

陣列成員：項目數下限為 1。項目數上限為 50。

必要：否

Usage

指定如何使用此憑證。它可以通過以下方式使用：

- SIGNING：用於簽署 AS2 訊息
- ENCRYPTION：用於加密 AS2 訊息
- TLS：用於保護透過 HTTPS 傳送的 AS2 通訊安全

類型：字串

有效值:SIGNING | ENCRYPTION

必要：是

回應語法

```
{
   "CertificateId": "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。

CertificateId

已匯入憑證的識別碼陣列。您可以使用此識別碼處理設定檔和合作夥伴設定檔。

類型：字串

長度約束：固定長度為 22。

模式：`cert-([0-9a-f]{17})`

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

HTTP 狀態碼：500

範例

範例

下列範例會匯入要用於加密的憑證。在第一個命令中，我們提供了證書和證書鏈文件的內容。此格式用於 SDK 命令。

```
aws transfer import-certificate --usage ENCRYPTION --certificate "`cat encryption-
cert.pem`" \
    --private-key "`cat encryption-key.pem`" --certificate-chain "`cat root-ca.pem`"
```

範例

下列範例與上述命令相同，不同之處在於我們提供私密金鑰、憑證和憑證鏈結檔案的檔案位置。如果您使用的是 SDK，則此版本的命令不起作用。

```
aws transfer import-certificate --usage ENCRYPTION --certificate file://encryption-
cert.pem \
    --private-key file://encryption-key.pem --certificate-chain file://root-ca.pem
```

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

ImportHostKey

將主機金鑰新增至ServerId參數所指定的伺服器。

請求語法

```
{
   "Description": "string",
   "HostKeyBody": "string",
   "ServerId": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

Description

識別此主機金鑰的文字描述。

類型：字串

長度限制：長度下限為 0。長度上限為 200。

模式：[\p{Print}]*

必要：否

HostKeyBody

SSH key pair 的私密金鑰部分。

AWS Transfer Family 接受 RSA、ECDSA 和 ED25519 金鑰。

類型：字串

長度限制：長度下限為 0。長度上限為 4096。

必要：是

ServerId

包含要匯入之主機金鑰之伺服器的識別碼。

類型：字串

長度約束：固定長度為 19。

模式：`s-([0-9a-f]{17})`

必要：是

Tags

可用於分組和搜尋主機金鑰的索引鍵值配對。

類型：Tag 物件陣列

陣列成員：項目數下限為 1。項目數上限為 50。

必要：否

回應語法

```
{
   "HostKeyId": "string",
   "ServerId": "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。

HostKeyId

返回導入密鑰的主機密鑰標識符。

類型：字串

長度約束：固定長度為 25。

模式：`hostkey-[0-9a-f]{17}`

ServerId

返回包含導入密鑰的服務器標識符。

類型：字串

長度約束：固定長度為 19。

模式：`s-([0-9a-f]{17})`

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceExistsException

請求的資源不存在，或者存在於為命令指定的區域以外的區域中。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

HTTP 狀態碼：500

ThrottlingException

由於請求調節，因此請求遭到拒絕。

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

ImportSshPublicKey

將安全殼層 (SSH) 公開金鑰新增至 Transfer Family 使用者，該使用者可透過指派給已啟用特定檔案傳輸通訊協定的伺服器 (以識別) 來識別。`UserName` `ServerId`

回應會`UserName`傳回的`ServerId`值、值和名稱`SshPublicKeyId`。

請求語法

```
{
   "ServerId": "string",
   "SshPublicKeyBody": "string",
   "UserName": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

ServerId

系統指派給伺服器的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：`s-([0-9a-f]{17})`

必要：是

SshPublicKeyBody

SSH key pair 的公開金鑰部分。

AWS Transfer Family 接受 RSA、ECDSA 和 ED25519 金鑰。

類型：字串

長度限制：長度下限為 0。長度上限為 2048。

必要：是

UserName

指派給一或多部伺服器的「Transfer Family」使用者名稱。

類型：字串

長度限制：長度下限為 3。長度上限為 100。

模式：[\w][\w@.-]{2,99}

必要：是

回應語法

```
{
   "ServerId": "string",
   "SshPublicKeyId": "string",
   "UserName": "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。

ServerId

系統指派給伺服器的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：s-([0-9a-f]{17})

SshPublicKeyId

由匯入的系統指定給公開金鑰的名稱。

類型：字串

長度限制：固定長度為 21。

模式：`key-[0-9a-f]{17}`

UserName

指派給您指定`ServerID`值的使用者名稱。

類型：字串

長度限制：長度下限為 3。長度上限為 100。

模式：`[\w][\w@.-]{2,99}`

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceExistsException

請求的資源不存在，或者存在於為命令指定的區域以外的區域中。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

HTTP 狀態碼：500

ThrottlingException

由於請求調節，因此請求遭到拒絕。

HTTP 狀態碼：400

範例

範例

此指令會id_ecdsa.pub匯入儲存在檔案中的 ECDSA 金鑰。

```
aws transfer import-ssh-public-key --server-id s-021345abcdef6789 --ssh-public-key-body
 file://id_ecdsa.pub --user-name jane-doe
```

範例

如果您執行上一個指令，系統會傳回下列資訊。

```
{
    "ServerId": "s-021345abcdef6789",
   "SshPublicKeyId": "key-1234567890abcdef0",
   "UserName": "jane-doe"
}
```

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

ListAccesses

列出伺服器上所有存取的詳細資料。

請求語法

```
{
   "MaxResults": number,
   "NextToken": "string",
   "ServerId": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

MaxResults

指定要傳回的存取 SID 數目上限。

類型：整數

有效範圍：最小值為 1。最大值為 1000。

必要：否

NextToken

當您可以從`ListAccesses`呼叫中取得其他結果時，會在輸出中傳回`NextToken`參數。然後，您可以將後續命令傳遞給`NextToken`參數，以繼續列出其他存取權限。

類型：字串

長度限制：長度下限為 1。長度上限為 6144。

必要：否

ServerId

系統指派給伺服器的唯一識別碼，其中已指派使用者。

類型：字串

長度約束：固定長度為 19。

模式：`s-([0-9a-f]{17})`

必要：是

回應語法

```
{
   "Accesses": [
      {
         "ExternalId": "string",
         "HomeDirectory": "string",
         "HomeDirectoryType": "string",
         "Role": "string"
      }
   ],
   "NextToken": "string",
   "ServerId": "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。

Accesses

傳回您指定`ServerId`值的存取及其屬性。

類型：ListedAccess 物件陣列

NextToken

當您可以從`ListAccesses`呼叫中取得其他結果時，會在輸出中傳回`NextToken`參數。然後，您可以將後續命令傳遞給`NextToken`參數，以繼續列出其他存取權限。

類型：字串

長度限制：長度下限為 1。長度上限為 6144。

ServerId

系統指派給伺服器的唯一識別碼，其中已指派使用者。

類型：字串

長度約束：固定長度為 19。

模式：`s-([0-9a-f]{17})`

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidNextTokenException

傳遞的`NextToken`參數無效。

HTTP 狀態碼：400

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

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

ListAgreements

傳回您所提供之伺服器所識別之合約的ServerId清單。如果要將結果限制為特定數目，請為MaxResults參數提供一個值。如果您先前已執行指令，並收到的值NextToken，您可以提供該值，以繼續列出您中斷之處的合約。

請求語法

```
{
   "MaxResults": number,
   "NextToken": "string",
   "ServerId": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

MaxResults

要傳回的合約數目上限。

類型：整數

有效範圍：最小值為 1。最大值為 1000。

必要：否

NextToken

當您可以從ListAgreements呼叫中取得其他結果時，會在輸出中傳回NextToken參數。然後，您可以將後續指令傳遞至NextToken參數，以繼續列出其他協定。

類型：字串

長度限制：長度下限為 1。長度上限為 6144。

必要：否

ServerId

您想要合約清單之伺服器的識別碼。

類型：字串

長度約束：固定長度為 19。

模式：s-([0-9a-f]{17})

必要：是

回應語法

```
{
   "Agreements": [
      {
         "AgreementId": "string",
         "Arn": "string",
         "Description": "string",
         "LocalProfileId": "string",
         "PartnerProfileId": "string",
         "ServerId": "string",
         "Status": "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。

Agreements

傳回陣列，其中每個項目都包含合約的詳細資訊。

類型：ListedAgreement 物件陣列

NextToken

返回一個令牌，您可以用它ListAgreements再次調用並接收其他結果（如果有的話）。

類型：字串

長度限制：長度下限為 1。長度上限為 6144。

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidNextTokenException

傳遞的NextToken參數無效。

HTTP 狀態碼：400

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

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

ListCertificates

傳回已匯入至的目前憑證清單 AWS Transfer Family。如果要將結果限制為特定數目，請為MaxResults參數提供一個值。如果您先前執行命令並收到NextToken參數的值，您可以提供該值以繼續列出您中斷之處的憑證。

請求語法

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

MaxResults

要傳回的憑證數目上限。

類型：整數

有效範圍：最小值為 1。最大值為 1000。

必要：否

NextToken

當您可以從ListCertificates呼叫中取得其他結果時，會在輸出中傳回NextToken參數。然後，您可以將後續命令傳遞給NextToken參數，以繼續列出其他憑證。

類型：字串

長度限制：長度下限為 1。長度上限為 6144。

必要：否

回應語法

```
{
```

```
   "Certificates": [
      {
         "ActiveDate": number,
         "Arn": "string",
         "CertificateId": "string",
         "Description": "string",
         "InactiveDate": number,
         "Status": "string",
         "Type": "string",
         "Usage": "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。

Certificates

傳回ListCertificates呼叫中指定的憑證陣列。

類型：ListedCertificate 物件陣列

NextToken

傳回下一個 Token，您可以使用它列出下一個憑證。

類型：字串

長度限制：長度下限為 1。長度上限為 6144。

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidNextTokenException

傳遞的NextToken參數無效。

HTTP 狀態碼：400

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

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

ListConnectors

列出指定區域的連接器。

請求語法

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

MaxResults

要傳回的連接器數目上限。

類型：整數

有效範圍：最小值為 1。最大值為 1000。

必要：否

NextToken

當您可以從ListConnectors呼叫中取得其他結果時，會在輸出中傳回NextToken參數。然後，您可以將後續指令傳遞至NextToken參數，以繼續列出其他連接器。

類型：字串

長度限制：長度下限為 1。長度上限為 6144。

必要：否

回應語法

```
{
   "Connectors": [
```

```
      {
         "Arn": "string",
         "ConnectorId": "string",
         "Url": "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。

Connectors

傳回陣列，其中每個項目都包含連接器的詳細資訊。

類型：ListedConnector 物件陣列

NextToken

返回一個令牌，您可以用它ListConnectors再次調用並接收其他結果（如果有的話）。

類型：字串

長度限制：長度下限為 1。長度上限為 6144。

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidNextTokenException

傳遞的NextToken參數無效。

HTTP 狀態碼：400

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

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

ListExecutions

列出指定工作流程的所有進行中執行。

> **Note**
>
> 如果找不到指定的工作流程 ID，則會`ListExecutions`傳回`ResourceNotFound`例外狀況。

請求語法

```
{
   "MaxResults": number,
   "NextToken": "string",
   "WorkflowId": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

MaxResults

指定要傳回的最大執行次數。

類型：整數

有效範圍：最小值為 1。最大值為 1000。

必要：否

NextToken

`ListExecutions`返回輸出中的`NextToken`參數。然後，您可以在後續命令中傳遞`NextToken`參數，以繼續列出其他執行項目。

例如，這對於分頁很有用。如果您有 100 個工作流程的執行，您可能只想列出前 10 個。如果是這樣，請指定以下內容來呼叫 API`max-results`：

```
aws transfer list-executions --max-results 10
```

這將返回前 10 個執行的詳細信息，以及指向第 11 個執行的指針（NextToken）。您現在可以再次呼叫 API，提供您收到的NextToken值：

```
aws transfer list-executions --max-results 10 --next-token
$somePointerReturnedFromPreviousListResult
```

此呼叫會傳回接下來的 10 個執行，即第 11 至 20 次。然後，您可以重複呼叫，直到傳回所有 100 個執行的詳細資料為止。

類型：字串

長度限制：長度下限為 1。長度上限為 6144。

必要：否

WorkflowId

工作流程的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：w-([a-z0-9]{17})

必要：是

回應語法

```
{
   "Executions": [
      {
         "ExecutionId": "string",
         "InitialFileLocation": {
            "EfsFileLocation": {
               "FileSystemId": "string",
               "Path": "string"
            },
            "S3FileLocation": {
               "Bucket": "string",
               "Etag": "string",
               "Key": "string",
               "VersionId": "string"
```

```
            }
         },
         "ServiceMetadata": {
            "UserDetails": {
               "ServerId": "string",
               "SessionId": "string",
               "UserName": "string"
            }
         },
         "Status": "string"
      }
   ],
   "NextToken": "string",
   "WorkflowId": "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。

Executions

返回每個執行的詳細信息，在一個ListedExecution數組。

類型：ListedExecution 物件陣列

NextToken

ListExecutions返回輸出中的NextToken參數。然後，您可以在後續命令中傳遞NextToken參數，以繼續列出其他執行項目。

類型：字串

長度限制：長度下限為 1。長度上限為 6144。

WorkflowId

工作流程的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：`w-([a-z0-9]{17})`

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidNextTokenException

傳遞的`NextToken`參數無效。

HTTP 狀態碼：400

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

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 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

ListHostKeys

傳回ServerId參數所指定之伺服器的主機金鑰清單。

請求語法

```
{
   "MaxResults": number,
   "NextToken": "string",
   "ServerId": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

MaxResults

要傳回的主機金鑰數目上限。

類型：整數

有效範圍：最小值為 1。最大值為 1000。

必要：否

NextToken

如果有其他未傳回的結果，則會傳回NextToken參數。您可以將該值用於後續呼叫，以ListHostKeys繼續列出結果。

類型：字串

長度限制：長度下限為 1。長度上限為 6144。

必要：否

ServerId

包含您要檢視之主機金鑰之伺服器的識別碼。

類型：字串

長度約束：固定長度為 19。

模式：s-([0-9a-f]{17})

必要：是

回應語法

```
{
   "HostKeys": [
      {
         "Arn": "string",
         "DateImported": number,
         "Description": "string",
         "Fingerprint": "string",
         "HostKeyId": "string",
         "Type": "string"
      }
   ],
   "NextToken": "string",
   "ServerId": "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。

HostKeys

返回一個數組，其中每個項目包含主機密鑰的詳細信息。

類型：ListedHostKey 物件陣列

NextToken

返回一個令牌，您可以用它ListHostKeys再次調用並接收其他結果（如果有的話）。

類型：字串

長度限制：長度下限為 1。長度上限為 6144。

ServerId

返回包含列出的主機密鑰的服務器標識符。

類型：字串

長度約束：固定長度為 19。

模式：`s-([0-9a-f]{17})`

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidNextTokenException

傳遞的`NextToken`參數無效。

HTTP 狀態碼：400

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

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

ListProfiles

傳回系統的設定檔清單。如果要將結果限制為特定數目，請為MaxResults參數提供一個值。如果您先前執行了指令並收到的值NextToken，您可以提供該值以繼續列出您中斷之處的設定檔。

請求語法

```
{
   "MaxResults": number,
   "NextToken": "string",
   "ProfileType": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

MaxResults

要傳回的設定檔數目上限。

類型：整數

有效範圍：最小值為 1。最大值為 1000。

必要：否

NextToken

如果有其他未傳回的結果，則會傳回NextToken參數。您可以將該值用於後續呼叫，以ListProfiles繼續列出結果。

類型：字串

長度限制：長度下限為 1。長度上限為 6144。

必要：否

ProfileType

指示是否僅列出 LOCAL 類型設定檔，或僅列出 PARTNER 類型設定檔。如果請求中未提供，命令會將所有類型的設定檔列出。

類型：字串

有效值:LOCAL | PARTNER

必要：否

回應語法

```
{
   "NextToken": "string",
   "Profiles": [
      {
         "Arn": "string",
         "As2Id": "string",
         "ProfileId": "string",
         "ProfileType": "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

返回一個令牌，您可以用它ListProfiles再次調用並接收其他結果（如果有的話）。

類型：字串

長度限制：長度下限為 1。長度上限為 6144。

Profiles

返回一個數組，其中每個項目包含配置文件的詳細信息。

類型：ListedProfile 物件陣列

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidNextTokenException

傳遞的NextToken參數無效。

HTTP 狀態碼：400

InvalidRequestException

當客戶端提交格式錯誤的請求拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

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 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

ListSecurityPolicies

列出附加至伺服器和 SFTP 連接器的安全性原則。如需有關安全性原則的詳細資訊，請參閱使用伺服器的安全性原則或使用 SFTP 連接器的安全性原則。

請求語法

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

MaxResults

指定要傳回作為ListSecurityPolicies查詢回應的安全性原則數目。

類型：整數

有效範圍：最小值為 1。最大值為 1000。

必要：否

NextToken

從ListSecurityPolicies指令取得其他結果時，會在輸出中傳回NextToken參數。然後，您可以在後續命令中傳遞NextToken參數，以繼續列出其他安全策略。

類型：字串

長度限制：長度下限為 1。長度上限為 6144。

必要：否

回應語法

```
{
```

```
    "NextToken": "string",
    "SecurityPolicyNames": [ "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

當您可以從ListSecurityPolicies作業取得其他結果時，會在輸出中傳回NextToken參數。在下列命令中，您可以傳入NextToken參數以繼續列出安全性原則。

類型：字串

長度限制：長度下限為 1。長度上限為 6144。

SecurityPolicyNames

列出的安全性原則陣列。

類型：字串陣列

長度限制：長度下限為 0。長度上限為 100。

模式：Transfer[A-Za-z0-9]*SecurityPolicy-[A-Za-z0-9-]+

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidNextTokenException

傳遞的NextToken參數無效。

HTTP 狀態碼：400

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

HTTP 狀態碼：500

範例

範例

下列範例會列出所有可用安全性原則的名稱。

請求範例

```
aws transfer list-security-policies
```

回應範例

```
{
    "SecurityPolicyNames": [
        "TransferSecurityPolicy-2023-05",
        "TransferSecurityPolicy-2022-03",
        "TransferSecurityPolicy-FIPS-2024-01",
        "TransferSecurityPolicy-2024-01",
        "TransferSecurityPolicy-PQ-SSH-FIPS-Experimental-2023-04",
        "TransferSecurityPolicy-PQ-SSH-Experimental-2023-04",
        "TransferSecurityPolicy-FIPS-2020-06",
        "TransferSecurityPolicy-2020-06",
        "TransferSecurityPolicy-2018-11",
        "TransferSecurityPolicy-FIPS-2023-05"
    ]
}
```

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

ListServers

列出與您帳戶相關聯的已啟用檔案傳輸通訊協定的 AWS 伺服器。

請求語法

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

MaxResults

指定要傳回作為ListServers查詢回應的伺服器數目。

類型：整數

有效範圍：最小值為 1。最大值為 1000。

必要：否

NextToken

從ListServers指令取得其他結果時，會在輸出中傳回NextToken參數。然後，您可以在後續命令中傳遞NextToken參數，以繼續列出其他伺服器。

類型：字串

長度限制：長度下限為 1。長度上限為 6144。

必要：否

回應語法

```
{
```

```
   "NextToken": "string",
   "Servers": [
      {
         "Arn": "string",
         "Domain": "string",
         "EndpointType": "string",
         "IdentityProviderType": "string",
         "LoggingRole": "string",
         "ServerId": "string",
         "State": "string",
         "UserCount": number
      }
   ]
}
```

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

當您可以從ListServers作業取得其他結果時，會在輸出中傳回NextToken參數。在下列命令中，您可以傳入NextToken參數以繼續列出其他伺服器。

類型：字串

長度限制：長度下限為 1。長度上限為 6144。

Servers

列出的伺服器陣列。

類型：ListedServer 物件陣列

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidNextTokenException

傳遞的NextToken參數無效。

HTTP 狀態碼：400

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

HTTP 狀態碼：500

範例

範例

下列範例會列出您的 AWS 帳戶.

請注意，示例NextToken值不是真實的：它們旨在指示如何使用該參數。

請求範例

```
{
   "MaxResults": 1,
   "NextToken": "token-from-previous-API-call"
}
```

回應範例

```
{
   "NextToken": "another-token-to-continue-listing",
   "Servers": [
      {
         "Arn": "arn:aws:transfer:us-east-1:111112222222:server/s-01234567890abcdef",
         "Domain": "S3",
         "IdentityProviderType": "SERVICE_MANAGED",
```

```
            "EndpointType": "PUBLIC",
            "LoggingRole": "arn:aws:iam::111112222222:role/my-role",
            "ServerId": "s-01234567890abcdef",
            "State": "ONLINE",
            "UserCount": 3
        }
    ]
}
```

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

ListTagsForResource

列出與您指定的 Amazon 資源名稱 (ARN) 相關聯的所有標籤。資源可以是使用者、伺服器或角色。

請求語法

```
{
   "Arn": "string",
   "MaxResults": number,
   "NextToken": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

Arn

請求與特定 Amazon 資源名稱 (ARN) 相關聯的標籤。ARN 是特定 AWS 資源 (例如伺服器、使用者或角色) 的識別碼。

類型：字串

長度限制：長度下限為 20。長度上限為 1600。

模式：`arn:\S+`

必要：是

MaxResults

指定要傳回作為`ListTagsForResource`要求回應的標籤數目。

類型：整數

有效範圍：最小值為 1。最大值為 1000。

必要：否

NextToken

當您從`ListTagsForResource`作業要求其他結果時，會在輸入中傳回`NextToken`參數。然後，您可以將後續指令傳遞至`NextToken`參數，以繼續列出其他標籤。

類型：字串

長度限制：長度下限為 1。長度上限為 6144。

必要：否

回應語法

```
{
   "Arn": "string",
   "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。

Arn

您指定要列出標籤的 ARN。

類型：字串

長度限制：長度下限為 20。長度上限為 1600。

模式：arn:\S+

NextToken

當您可以從ListTagsForResource呼叫中取得其他結果時，會在輸出中傳回NextToken參數。然後，您可以將後續指令傳遞至NextToken參數，以繼續列出其他標籤。

類型：字串

長度限制：長度下限為 1。長度上限為 6144。

Tags

指定給資源的鍵值配對，通常用於分組和搜尋項目。標籤是您定義的中繼資料。

類型：Tag 物件陣列

陣列成員：項目數下限為 1。項目數上限為 50。

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidNextTokenException

傳遞的NextToken參數無效。

HTTP 狀態碼：400

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

HTTP 狀態碼：500

範例

範例

下列範例會列出具有您指定 ARN 之資源的標籤。

請求範例

```
{
   "Arn": "arn:aws:transfer:us-east-1:176354371281:server/s-01234567890abcdef"
}
```

範例

此範例說明的一種用法 ListTagsForResource。

回應範例

```
{
   "Tags": [
      {
         "Key": "Name",
         "Value": "MyServer"
      }
   ]
}
```

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

ListUsers

列出您透過傳遞參數所指定之已啟用檔案傳輸通訊協定之ServerId伺服器的使用者。

請求語法

```
{
   "MaxResults": number,
   "NextToken": "string",
   "ServerId": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

MaxResults

指定要傳回作為ListUsers要求回應的使用者數目。

類型：整數

有效範圍：最小值為 1。最大值為 1000。

必要：否

NextToken

如果ListUsers呼叫有其他結果，則會在輸出中傳回NextToken參數。然後，您可以將指令傳遞NextToken給後續ListUsers指令，以繼續列出其他使用者。

類型：字串

長度限制：長度下限為 1。長度上限為 6144。

必要：否

ServerId

系統指派給伺服器的唯一識別碼，其中已指派使用者。

類型：字串

長度約束：固定長度為 19。

模式：s-([0-9a-f]{17})

必要：是

回應語法

```
{
   "NextToken": "string",
   "ServerId": "string",
   "Users": [
      {
         "Arn": "string",
         "HomeDirectory": "string",
         "HomeDirectoryType": "string",
         "Role": "string",
         "SshPublicKeyCount": number,
         "UserName": "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

當您可以從ListUsers呼叫中取得其他結果時，會在輸出中傳回NextToken參數。然後，您可以將後續命令傳遞給NextToken參數，以繼續列出其他使用者。

類型：字串

長度限制：長度下限為 1。長度上限為 6144。

ServerId

系統指派給使用者之伺服器的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：s-([0-9a-f]{17})

Users

傳回您指定ServerId值的「轉移族群」使用者及其性質。

類型：ListedUser 物件陣列

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidNextTokenException

傳遞的NextToken參數無效。

HTTP 狀態碼：400

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

HTTP 狀態碼：500

範例

範例

ListUsersAPI 呼叫會傳回與您指定之伺服器相關聯的使用者清單。

請求範例

```
        {
         "MaxResults": 100,
         "NextToken": "eyJNYXJrZXIiOiBudWxsLCAiYm90b1X0cnVuU2F0ZV9hbW91bnQiOiAyfQ==",
         "ServerId": "s-01234567890abcdef"
         }
```

範例

這是此 API 呼叫的範例回應。

回應範例

```
{
   "NextToken": "eyJNYXJrZXIiOiBudWxsLCAiYm90b1X0cnVuU2F0ZV9hbW91bnQiOiAyfQ==",
   "ServerId": "s-01234567890abcdef",
   "Users": [
      {
         "Arn": "arn:aws:transfer:us-east-1:176354371281:user/s-01234567890abcdef/
charlie",
         "HomeDirectory": "/tests/home/charlie",
         "SshPublicKeyCount": 1,
         "Role": "arn:aws:iam::176354371281:role/transfer-role1",
         "Tags": [
            {
               "Key": "Name",
               "Value": "user1"
            }
         ],
         "UserName": "my_user"
      }
   ]
}
```

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

ListWorkflows

列出與您目前區域相關聯 AWS 帳戶 的所有工作流程。

請求語法

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

MaxResults

指定要傳回的最大工作流程數目。

類型：整數

有效範圍：最小值為 1。最大值為 1000。

必要：否

NextToken

ListWorkflows返回輸出中的NextToken參數。然後，您可以在後續指令中傳遞NextToken參數，以繼續列出其他工作流程。

類型：字串

長度限制：長度下限為 1。長度上限為 6144。

必要：否

回應語法

```
{
   "NextToken": "string",
```

```
   "Workflows": [
      {
         "Arn": "string",
         "Description": "string",
         "WorkflowId": "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

ListWorkflows返回輸出中的NextToken參數。然後，您可以在後續指令中傳遞NextToken參數，以繼續列出其他工作流程。

類型：字串

長度限制：長度下限為 1。長度上限為 6144。

Workflows

Description針對每個工作流程傳回WorkflowId、和。Arn

類型：ListedWorkflow 物件陣列

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidNextTokenException

傳遞的NextToken參數無效。

HTTP 狀態碼：400

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

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

SendWorkflowStepState

傳送非同步自訂步驟的回呼。

在ExecutionId工作流程的自訂步驟執行期間WorkflowId，會將、和Token傳遞至目標資源。您必須在回調中包含那些內容並提供狀態。

請求語法

```
{
   "ExecutionId": "string",
   "Status": "string",
   "Token": "string",
   "WorkflowId": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

ExecutionId

用於執行工作流程的唯一識別元。

類型：字串

長度約束：固定長度為 36。

模式：[0-9a-fA-F]{8}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{12}

必要：是

Status

指出指定的步驟是成功還是失敗。

類型：字串

有效值:SUCCESS | FAILURE

必要：是

Token

用於區分相同執行中多個 Lambda 步驟的多個回呼。

類型：字串

長度限制：長度下限為 1。長度上限為 64。

模式：\w+

必要：是

WorkflowId

工作流程的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：w-([a-z0-9]{17})

必要：是

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

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：400

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

HTTP 狀態碼：500

ThrottlingException

由於請求調節，因此請求遭到拒絕。

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

StartDirectoryListing

從遠端 SFTP 伺服器擷取目錄內容的清單。您可以指定連接器 ID、輸出路徑和遠端目錄路徑。您也可以指定選用MaxItems值，以控制從遠端目錄列出的項目數目上限。此 API 返回遠程目錄中所有文件和目錄的列表（最大值），但不返回子目錄中的文件或文件夾。也就是說，它只返回一層深的文件和目錄的列表。

收到清單檔案後，您可以提供要傳輸至 StartFileTransfer API 呼叫RetrieveFilePaths參數的檔案。

輸出檔案的命名慣例為 *connector-ID-listing-ID*.json。輸出檔案包含下列資訊：

- filePath: 遠端檔案的完整路徑，相對於遠端伺服器上 SFTP 連接器的清單要求目錄。
- modifiedTimestamp: 上次修改檔案的時間，採用 UTC 時間格式。此欄位為選用欄位。如果遠端檔案屬性不包含時間戳記，則會在檔案清單中省略該時間戳記。
- size：文件的大小，以字節為單位。此欄位為選用欄位。如果遠端檔案屬性不包含檔案大小，則會從檔案清單中省略該檔案大小。
- path: 遠端目錄的完整路徑，相對於遠端伺服器上 SFTP 連接器的清單要求目錄。
- truncated：一個標誌，指示列表輸出是否包含遠程目錄中包含的所有項目。如果您的Truncated輸出值為 true，則可以增加可選 max-items input 屬性中提供的值，以便能夠列出更多項目（最多允許列表大小為 10,000 個項目）。

請求語法

```
{
   "ConnectorId": "string",
   "MaxItems": number,
   "OutputDirectoryPath": "string",
   "RemoteDirectoryPath": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

ConnectorId

連接器的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：`c-([0-9a-f]{17})`

必要：是

MaxItems

選用參數，您可以在其中指定要擷取的檔案/目錄名稱數目上限。預設值為 1,000。

類型：整數

有效範圍：最小值為 1。最大值為 10000。

必要：否

OutputDirectoryPath

指定 Amazon S3 儲存中用於存放目錄清單結果的路徑 (儲存貯體和前置詞)。

類型：字串

長度限制：長度下限為 1。長度上限為 1024。

模式：`(.)+`

必要：是

RemoteDirectoryPath

指定遠端 SFTP 伺服器上要列出其內容的目錄。

類型：字串

長度限制：長度下限為 1。長度上限為 1024。

模式：`(.)+`

必要：是

回應語法

```
{
   "ListingId": "string",
   "OutputFileName": "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。

ListingId

返回目錄列表調用的唯一標識符。

類型：字串

長度限制：長度下限為 1。長度上限為 512。

模式：`[0-9a-zA-Z./-]+`

OutputFileName

返回存儲結果的文件名。這是連接器識別碼和清單識別碼的組合：`<connector-id>-<listing-id>.json`。

類型：字串

長度限制：長度下限為 26。最大長度為 537。

模式：`c-([0-9a-f]{17})-[0-9a-zA-Z./-]+.json`

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

HTTP 狀態碼：500

ThrottlingException

由於請求調節，因此請求遭到拒絕。

HTTP 狀態碼：400

範例

範例

下列範例會列出遠端 SFTP 伺服器上的home資料夾內容，此內容由指定的連接器識別。結果會放置在 Amazon S3 位置/DOC-EXAMPLE-BUCKET/connector-files，並放入名為的檔案中c-AAAA1111BBBB2222C-6666abcd-11aa-22bb-cc33-0000aaaa3333.json。

請求範例

```
{
    "ConnectorId": "c-AAAA1111BBBB2222C",
    "MaxItems": "10",
    "OutputDirectoryPath": "/DOC-EXAMPLE-BUCKET/connector-files",
    "RemoteDirectoryPath": "/home"
}
```

回應範例

```
{
```

```
    "ListingId": "6666abcd-11aa-22bb-cc33-0000aaaa3333",
    "OutputFileName": "c-AAAA1111BBBB2222C-6666abcd-11aa-22bb-cc33-0000aaaa3333.json"
}
```

```
// under bucket "DOC-EXAMPLE-BUCKET"
connector-files/c-AAAA1111BBBB2222C-6666abcd-11aa-22bb-cc33-0000aaaa3333.json
{
    "files": [
        {
            "filePath": "/home/what.txt",
            "modifiedTimestamp": "2024-01-30T20:34:54Z",
            "size" : 2323
        },
        {
            "filePath": "/home/how.pgp",
            "modifiedTimestamp": "2024-01-30T20:34:54Z",
            "size" : 51238
        }
    ],
    "paths": [
        {
            "path": "/home/magic"
        },
        {
            "path": "/home/aws"
        },
    ],
    "truncated": false
}
```

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

StartFileTransfer

開始本機 AWS 儲存與遠端 AS2 或 SFTP 伺服器之間的檔案傳輸。

- 對於 AS2 連接器，您可以指定`ConnectorId`和一個或多個`SendFilePaths`以識別要傳輸的檔案。
- 對於 SFTP 連接器，檔案傳輸可以是輸出或輸入。在這兩種情況下，您都可以指定`ConnectorId`. 根據轉移方向，您也可以指定下列項目：
  - 如果要將檔案從合作夥伴的 SFTP 伺服器傳輸到 Amazon Web Services 儲存體，請指定一個或多個用於識別`RetrieveFilePaths`要傳輸的檔案，並指`LocalDirectoryPath`定目標資料夾。
  - 如果您要從 AWS 儲存裝置傳輸檔案至協力廠商的 SFTP 伺服器，您可以指定一或多個`SendFilePaths`來識別您要傳輸的檔案，並指`RemoteDirectoryPath`定目的地資料夾。

請求語法

```
{
   "ConnectorId": "string",
   "LocalDirectoryPath": "string",
   "RemoteDirectoryPath": "string",
   "RetrieveFilePaths": [ "string" ],
   "SendFilePaths": [ "string" ]
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

ConnectorId

連接器的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：`c-([0-9a-f]{17})`

必要：是

LocalDirectoryPath

對於輸入傳輸，LocaDirectoryPath指定從合作夥伴 SFTP 伺服器傳輸的一或多個檔案的目的地。

類型：字串

長度限制：長度下限為 1。長度上限為 1024。

模式：(.)+

必要：否

RemoteDirectoryPath

對於輸出傳輸，RemoteDirectoryPath指定傳輸至夥伴 SFTP 伺服器之一或多個檔案的目的地。如果未指定RemoteDirectoryPath，傳輸檔案的目的地就是 SFTP 使用者的主目錄。

類型：字串

長度限制：長度下限為 1。長度上限為 1024。

模式：(.)+

必要：否

RetrieveFilePaths

合作夥伴 SFTP 伺服器的一或多個來源路徑。每個字串代表一個輸入檔案傳輸的來源檔案路徑。

類型：字串陣列

陣列成員：項目數下限為 1。項目數上限為 10。

長度限制：長度下限為 1。長度上限為 1024。

模式：(.)+

必要：否

SendFilePaths

Amazon S3 儲存的一或多個來源路徑。每個字串代表一個輸出檔案傳輸的來源檔案路徑。例如 *DOC-EXAMPLE-BUCKET/myfile.txt* 。

> **Note**
>
> 更換為您 *DOC-EXAMPLE-BUCKET* 的實際存儲桶之一。

類型：字串陣列

陣列成員：項目數下限為 1。項目數上限為 10。

長度限制：長度下限為 1。長度上限為 1024。

模式：`(.)+`

必要：否

回應語法

```
{
   "TransferId": "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。

TransferId

返回文件傳輸的唯一標識符。

類型：字串

長度限制：長度下限為 1。長度上限為 512。

模式：`[0-9a-zA-Z./-]+`

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

HTTP 狀態碼：500

ThrottlingException

由於請求調節，因此請求遭到拒絕。

HTTP 狀態碼：400

範例

範例

下列範例會啟動從 Transfer Family 伺服器到遠端交易夥伴端點的 AS2 檔案傳輸。更換為您 *DOC-EXAMPLE-BUCKET* 的實際存儲桶之一。

請求範例

```
{
    "ConnectorId": "c-AAAA1111BBBB2222C",
    "SendFilePaths": [
        "/DOC-EXAMPLE-BUCKET/myfile-1.txt",
        "/DOC-EXAMPLE-BUCKET/myfile-2.txt",
        "/DOC-EXAMPLE-BUCKET/myfile-3.txt"
```

```
    ]
}
```

回應範例

```
{
   "TransferId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

範例

下列範例會啟動從本機 AWS 儲存至遠端 SFTP 伺服器的檔案傳輸。

請求範例

```
{
    "ConnectorId": "c-01234567890abcdef",
    "SendFilePaths": [
        "/DOC-EXAMPLE-BUCKET/myfile-1.txt",
        "/DOC-EXAMPLE-BUCKET/myfile-2.txt",
        "/DOC-EXAMPLE-BUCKET/myfile-3.txt"
    ],
    "RemoteDirectoryPath": "/MySFTPRootFolder/fromTranferFamilyServer"
}
```

回應範例

```
{
   "TransferId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222"
}
```

範例

下列範例會啟動從遠端 SFTP 伺服器到本機 AWS 儲存的檔案傳輸。

請求範例

```
{
    "ConnectorId": "c-111122223333AAAAA",
    "RetrieveFilePaths": [
        "/MySFTPFolder/toTranferFamily/myfile-1.txt",
```

```
        "/MySFTPFolder/toTranferFamily/myfile-2.txt",
        "/MySFTPFolder/toTranferFamily/myfile-3.txt"
    ],
    "LocalDirectoryPath": "/DOC-EXAMPLE-BUCKET/mySourceFiles"
}
```

回應範例

```
{
   "TransferId": "a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa"
}
```

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

StartServer

將已啟用檔案傳輸通訊協定之伺服器的狀態從OFFLINE變更為。ONLINE它對已經存在的服務器沒有影響ONLINE。ONLINE伺服器可以接受和處理檔案傳輸工作。

的狀態STARTING表示伺服器處於中繼狀態，可能無法完全回應，或未完全連線。的值START_FAILED可以指示錯誤狀況。

此呼叫不會傳回任何回應。

請求語法

```
{
   "ServerId": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

ServerId

系統為您啟動的伺服器指派的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：s-([0-9a-f]{17})

必要：是

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

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

HTTP 狀態碼：500

ThrottlingException

由於請求調節，因此請求遭到拒絕。

HTTP 狀態碼：400

範例

範例

下列範例會啟動伺服器。

請求範例

```
{
   "ServerId": "s-01234567890abcdef"
}
```

範例

這是此 API 呼叫的範例回應。

回應範例

```
{
   "ServerId": "s-01234567890abcdef"
}
```

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

StopServer

將已啟用檔案傳輸通訊協定之伺服器的狀態從ONLINE變更為。OFFLINEOFFLINE伺服器無法接受和處理檔案傳輸工作。與伺服器相關的資訊 (例如伺服器和使用者屬性) 不會受到停止伺服器的影響。

> **Note**
>
> 停止伺服器不會減少或影響您的檔案傳輸通訊協定端點計費；您必須刪除伺服器才能停止計費。

的狀態STOPPING表示伺服器處於中繼狀態，可能無法完全回應或無法完全離線。的值STOP_FAILED可以指示錯誤狀況。

此呼叫不會傳回任何回應。

請求語法

```
{
   "ServerId": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

ServerId

系統為您停止的伺服器指派的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：s-([0-9a-f]{17})

必要：是

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

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

HTTP 狀態碼：500

ThrottlingException

由於請求調節，因此請求遭到拒絕。

HTTP 狀態碼：400

範例

範例

下列範例會停止伺服器。

請求範例

```
{
   "ServerId": "s-01234567890abcdef"
}
```

範例

這是此 API 呼叫的範例回應。

回應範例

```
{
   "ServerId": "s-01234567890abcdef"
}
```

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

TagResource

將索引鍵值對附加至資源，如其 Amazon 資源名稱 (ARN) 所識別。資源是使用者、伺服器、角色和其他實體。

此呼叫未傳回任何回應。

請求語法

```
{
   "Arn": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

Arn

特定資源 (例如伺服器、使用者或角色) 的 Amazon AWS 資源名稱 (ARN)。

類型：字串

長度限制：長度下限為 20。長度上限為 1600。

模式：`arn:\S+`

必要：是

Tags

指派給 ARN 的索引鍵值配對，可用來依類型分組和搜尋資源。您可以為任何目的將此中繼資料附加至資源 (伺服器、使用者、工作流程等)。

類型：Tag 物件陣列

陣列成員：項目數下限為 1。項目數上限為 50。

必要：是

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

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

HTTP 狀態碼：500

範例

範例

下列範例會將標籤新增至已啟用檔案傳輸通訊協定的伺服器。

請求範例

```
{
   "Arn": "arn:aws:transfer:us-east-1:176354371281:server/s-01234567890abcdef",
   "Tags": [
      {
         "Key": "Group",
         "Value": "Europe"
      }
   ]
}
```

範例

此範例說明的一種用法 TagResource。

回應範例

```
        HTTP 200 response with an empty HTTP body.
```

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

TestConnection

測試您的 SFTP 連接器是否已成功設定。我們強烈建議您呼叫此作業，以測試您在本機 AWS 儲存空間與交易夥伴的 SFTP 伺服器之間傳輸檔案的能力。

請求語法

```
{
   "ConnectorId": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

ConnectorId

連接器的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：`c-([0-9a-f]{17})`

必要：是

回應語法

```
{
   "ConnectorId": "string",
   "Status": "string",
   "StatusMessage": "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。

ConnectorId

傳回您正在測試之連接器物件的識別碼。

類型：字串

長度約束：固定長度為 19。

模式：`c-([0-9a-f]{17})`

Status

返回OK測試成功，或者ERROR如果測試失敗。

類型：字串

StatusMessage

`Connection succeeded`如果測試成功返回。或者，如果測試失敗，則傳回描述性錯誤訊息。下列清單提供疑難排解詳細資料，視您收到的錯誤訊息而定。

- 確認您的密碼名稱與「轉移角色」權限中的名稱一致。
- 驗證連接器組態中的伺服器 URL，並確認登入認證在連接器外部成功運作。
- 確認密碼存在且格式正確。
- 確認連接器組態中的受信任主機金鑰與`ssh-keyscan`輸出相符。

類型：字串

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

HTTP 狀態碼：500

範例

範例

下列範例會測試與遠端伺服器的連線。

```
aws transfer test-connection --connector-id c-abcd1234567890fff
```

回應範例

如果成功，API 呼叫會傳回下列詳細資訊。

```
{
    "Status": "OK",
    "StatusMessage": "Connection succeeded"
}
```

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

TestIdentityProvider

如果已啟用檔案傳輸通訊協定IdentityProviderType的伺服器是AWS_DIRECTORY_SERVICE或API_Gateway，請測試您的身分識別提供者是否已成功設定。我們強烈建議您在建立伺服器後立即呼叫此作業來測試驗證方法。如此一來，您就可以疑難排解身分識別提供者整合的問題，以確保您的使用者可以成功使用服務。

ServerId 和 UserName 是必要參數。ServerProtocolSourceIp、和UserPassword都是選擇性的。

注意下列事項：

- TestIdentityProvider如果您IdentityProviderType的服務器是，則無法使用SERVICE_MANAGED。
- TestIdentityProvider不適用於密鑰：它只接受密碼。
- TestIdentityProvider可以測試處理金鑰和密碼的自訂身分識別提供者的密碼作業。
- 如果您為任何參數提供任何不正確的值，則Response欄位為空白。
- 如果您為使用服務管理使用者的伺服器提供伺服器 ID，您會收到錯誤訊息：

  ```
  An error occurred (InvalidRequestException) when calling the
  TestIdentityProvider operation: s-server-ID not configured for external
  auth
  ```
- 如果您輸入的伺服器 ID 無法識別實際傳送伺服器的--server-id參數，您會收到下列錯誤：

  ```
  An error occurred (ResourceNotFoundException) when calling the
  TestIdentityProvider operation: Unknown server.
  ```

  您的服務器可能位於不同的地區。您可以通過添加以下內容來指定一個區域：--region region-code，例--region us-east-2如在美國東部（俄亥俄州）指定服務器。

請求語法

```
{
   "ServerId": "string",
   "ServerProtocol": "string",
   "SourceIp": "string",
   "UserName": "string",
   "UserPassword": "string"
```

```
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

ServerId

系統指派給特定伺服器的識別碼。該伺服器的使用者驗證方法會使用使用者名稱和密碼進行測試。

類型：字串

長度約束：固定長度為 19。

模式：`s-([0-9a-f]{17})`

必要：是

ServerProtocol

要測試的檔案傳輸通訊協定類型。

可用的通訊協定包括：

- 安全殼層 (SSH) 檔案傳輸通訊協定 (SFTP)
- 安全檔案傳輸通訊協定 (FTPS)
- 檔案傳輸通訊協定 (FTP)
- 適用性聲明 2 (AS2)

類型：字串

有效值:`SFTP | FTP | FTPS | AS2`

必要：否

SourceIp

要測試帳戶的來源 IP 位址。

類型：字串

長度限制：長度下限為 0。長度上限為 32。

模式：\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}

必要：否

UserName

要測試的帳戶名稱。

類型：字串

長度限制：長度下限為 3。長度上限為 100。

模式：[\w][\w@.-]{2,99}

必要：是

UserPassword

要測試的帳戶密碼。

類型：字串

長度限制：長度下限為 0。長度上限為 1024。

必要：否

回應語法

```
{
   "Message": "string",
   "Response": "string",
   "StatusCode": number,
   "Url": "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。

Message

指出測試是否成功的訊息。

> **Note**
> 如果傳回空字串，最有可能的原因是驗證因為使用者名稱或密碼不正確而失敗。

類型：字串

Response

從您的 API Gateway 或 Lambda 函數傳回的回應。

類型：字串

StatusCode

HTTP 狀態碼，是來自 API Gateway 或 Lambda 函數的回應。

類型：整數

Url

用來驗證使用者的服務端點。

類型：字串

長度限制：長度下限為 0。長度上限為 255。

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

HTTP 狀態碼：500

範例

範例

下列要求會傳回來自身分識別提供者的訊息，告知使用者名稱和密碼組合為可搭配使用的有效身分識別 AWS Transfer Family。

請求範例

```
{
   "ServerID": "s-01234567890abcdef",
   "UserName": "my_user",
   "UserPassword": "MyPassword-1"
}
```

範例

下列回應顯示測試成功的範例回應。

回應範例

```
      "Response":"
      {\"homeDirectory\":\"/mybucket001\",\"homeDirectoryDetails\":null,
\"homeDirectoryType\":\"PATH\",\"posixProfile\":null,
      \"publicKeys\":\"[ssh-rsa-key]\",\"role\":\"arn:aws:iam::123456789012:role/
my_role\",\"policy\":null,\"username\":\"transferuser002\",
```

```
      \"identityProviderType\":null,\"userConfigMessage\":null)"}
      "StatusCode": "200",
      "Message": ""
```

範例

下列回應表示指定的使用者屬於一個以上具有存取權的群組。

```
        "Response":"",
        "StatusCode":200,
        "Message":"More than one associated access found for user's groups."
```

範例

如果您已使用 API Gateway 建立並設定自訂身分識別提供者，則可以輸入下列命令來測試使用者：

`aws transfer test-identity-provider --server-id s-0123456789abcdefg --user-name myuser`

其中 s-012345678989abcdefg 是您的傳輸服務器，我的用戶是您自定義用戶的用戶名。

如果命令成功，則您的響應類似於以下內容，其中：

- AWS 帳戶 識別碼是 012345678901
- 使用者角色是使用者角色 API 閘道
- 主目錄是我的用戶桶
- 公開金鑰是公開金鑰
- 調用網址是調用網址

```
{
    "Response": "{\"Role\": \"arn:aws:iam::012345678901:role/user-role-api-gateway\",
\"HomeDirectory\": \"/myuser-bucket\",\"PublicKeys\": \"[public-key]\"}",
    "StatusCode": 200,
    "Message": "",
    "Url": "https://invocation-URL/servers/s-0123456789abcdefg/users/myuser/config"
}
```

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

UntagResource

從資源中分離鍵值對，如其 Amazon 資源名稱 (ARN) 所識別。資源是使用者、伺服器、角色和其他實體。

此呼叫不會傳回任何回應。

請求語法

```
{
   "Arn": "string",
   "TagKeys": [ "string" ]
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

Arn

將移除標籤的資源值。Amazon 資源名稱 (ARN) 是特定 AWS 資源 (例如伺服器、使用者或角色) 的識別碼。

類型：字串

長度限制：長度下限為 20。長度上限為 1600。

模式：`arn:\S+`

必要：是

TagKeys

TagKeys 是指派給 ARN 的索引鍵值配對，可用來依類型分組和搜尋資源。此中繼資料可以基於任何目的附加至資源。

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 0。長度上限為 128。

必要：是

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

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

HTTP 狀態碼：500

範例

範例

下列範例會移除已啟用檔案傳輸通訊協定之伺服器的標籤。

請求範例

```
{
   "Arn": "arn:aws:transfer:us-east-1:176354371281:server/s-01234567890abcdef",
   "TagKeys": "Europe" ]
}
```

範例

此範例說明的一種用法 UntagResource。

回應範例

```
        HTTP 200 response with an empty HTTP body.
```

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

UpdateAccess

可讓您更新和參數中指定之存取權ServerID的ExternalID參數。

請求語法

```
{
   "ExternalId": "string",
   "HomeDirectory": "string",
   "HomeDirectoryMappings": [
      {
         "Entry": "string",
         "Target": "string",
         "Type": "string"
      }
   ],
   "HomeDirectoryType": "string",
   "Policy": "string",
   "PosixProfile": {
      "Gid": number,
      "SecondaryGids": [ number ],
      "Uid": number
   },
   "Role": "string",
   "ServerId": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

ExternalId

識別目錄中特定群組所需的唯一識別碼。您關聯之群組的使用者可以透過已啟用的協定存取 Amazon S3 或 Amazon EFS 資源 AWS Transfer Family。如果您知道群組名稱，您可以使用 Windows 執行下列命令來檢視 SID 值 PowerShell。

```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties
* | Select SamAccountName,ObjectSid
```

在該命令中，YourGroupName用活動目錄組的名稱替換。

用來驗證此參數的規則運算式是由不含空格的大寫和小寫英數字元組成的字元字串。您也可以包含底線或下列任何字元：=, 。 @：/-

類型：字串

長度限制：長度下限為 1。長度上限為 256。

模式：S-1-[\d-]+

必要：是

HomeDirectory

使用者使用其用戶端登入伺服器時的登陸目錄 (資料夾)。

HomeDirectory 範例為 /bucket_name/home/mydirectory。

> **Note**
>
> 只有在 HomeDirectoryType 設為 PATH 時才會使用 HomeDirectory 參數。

類型：字串

長度限制：長度下限為 0。長度上限為 1024。

模式：(|/.*)

必要：否

HomeDirectoryMappings

邏輯目錄對應，指定您的使用者可以看到哪些 Amazon S3 或 Amazon EFS 路徑和金鑰，以及您希望如何顯示這些路徑和金鑰。您必須指定Entry和Target配對，其中Entry顯示路徑的顯示方式，以及Target實際的 Amazon S3 或 Amazon EFS 路徑。如果您僅指定目標，則會依原樣顯示該目標。您還必須確保您的 AWS Identity and Access Management (IAM) 角色可提供中路徑的存取權Target。只有當設定為邏輯時HomeDirectoryType，才能設定此值。

以下是Entry和配Target對範例。

```
[ { "Entry": "/directory1", "Target": "/bucket_name/home/
mydirectory" } ]
```

在大多數情況下，您可以使用此值而非工作階段原則，將使用者鎖定到指定的主目錄 (」chroot「)。若要執行此操作，您可以設Entry定為/並Target將其設定為HomeDirectory參數值。

以下是的Entry和Target配對範例chroot。

```
[ { "Entry": "/", "Target": "/bucket_name/home/mydirectory" } ]
```

類型：HomeDirectoryMapEntry 物件陣列

陣列成員：項目數下限為 1。5 萬個物品的最大數量。

必要：否

HomeDirectoryType

使用者登入伺服器時，您希望的使用者主目錄之登陸目錄 (資料夾) 類型。如果將其設定為PATH，使用者將在其檔案傳輸協定用戶端中看到絕對的 Amazon S3 儲存貯體或 Amazon EFS 路徑。如果將其設定為LOGICAL，則需要在中提供對應，以便讓使用者看到 Amazon S3 或 Amazon EFS 路徑的方式。HomeDirectoryMappings

> **Note**
>
> 如果HomeDirectoryType是LOGICAL，則必須使用HomeDirectoryMappings參數提供對映。另一方面，HomeDirectoryType如果您使用HomeDirectory參數提供絕對路徑。PATH您的範本HomeDirectoryMappings中不HomeDirectory能同時擁有和。

類型：字串

有效值:PATH | LOGICAL

必要：否

Policy

用戶的會話策略，以便您可以在多個用戶之間使用相同的 AWS Identity and Access Management （IAM）角色。此政策限制了使用者對 Amazon S3 儲存貯體部分的存取權限。您可以在此政策內使用的變數包括 ${Transfer:UserName}、${Transfer:HomeDirectory} 和 ${Transfer:HomeBucket}。

> **Note**
>
> 只有在的網域`ServerId`是 Amazon S3 時，才適用此政策。Amazon EFS 不使用工作階段政策。
> 對於工作階段政策，請將政策 AWS Transfer Family 儲存為 JSON Blob，而不是政策的 Amazon 資源名稱 (ARN)。您會將政策作為 JSON blob 儲存，並在 `Policy` 引數中傳遞它。
> 如需工作階段政策的範例，請參閱 Example session policy (工作階段政策範例)。
> 如需詳細資訊，請參閱 AWS安全性權杖服務 API 參考AssumeRole中的。

類型：字串

長度限制：長度下限為 0。長度上限為 2048。

必要：否

PosixProfile

控制使用者存取 Amazon EFS 檔案系統的完整 POSIX 身分，包括使用者 ID (`Uid`)、群組 ID (`Gid`) 和任何次要群組 ID (`SecondaryGids`)。對檔案系統中的檔案和目錄設定的 POSIX 許可，會決定使用者在 Amazon EFS 檔案系統中傳入和傳出檔案時所取得的存取等級。

類型：PosixProfile 物件

必要：否

Role

(IAM) 角色的亞馬遜資源名稱 AWS Identity and Access Management (ARN)，用於控制使用者對 Amazon S3 儲存貯體或 Amazon EFS 檔案系統的存取。連接到此角色的政策會決定在將檔案傳入和傳出您的 Amazon S3 儲存貯體或 Amazon EFS 檔案系統時，您希望提供給使用者的存取層級。IAM 角色也應包含信任關係，允許伺服器在處理您使用者的傳輸請求時，存取您的資源。

類型：字串

長度限制：長度下限為 20。長度上限為 2048。

模式：`arn:.*role/\S+`

必要：否

ServerId

伺服器執行個體的系統指派唯一識別碼。這是您新增使用者的特定目標伺服器。

類型：字串

長度約束：固定長度為 19。

模式：`s-([0-9a-f]{17})`

必要：是

回應語法

```
{
   "ExternalId": "string",
   "ServerId": "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。

ExternalId

群組的外部識別碼，其使用者可以使用 AWS Transfer Family 列透過已啟用的協定存取您的 Amazon S3 或 Amazon EFS 資源。

類型：字串

長度限制：長度下限為 1。長度上限為 256。

模式：`S-1-[\d-]+`

ServerId

使用者所附加之伺服器的識別碼。

類型：字串

長度約束：固定長度為 19。

模式：`s-([0-9a-f]{17})`

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求拋出此異常。

HTTP 狀態碼：400

ResourceExistsException

請求的資源不存在，或存在於為命令指定的區域以外的區域中。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

HTTP 狀態碼：500

ThrottlingException

由於請求調節，因此請求遭到拒絕。

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

UpdateAgreement

更新現有協定的部分參數。提供您要ServerId更新之協定的AgreementId和，以及要更新之參數的新值。

請求語法

```
{
   "AccessRole": "string",
   "AgreementId": "string",
   "BaseDirectory": "string",
   "Description": "string",
   "LocalProfileId": "string",
   "PartnerProfileId": "string",
   "ServerId": "string",
   "Status": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

AccessRole

連接器可用來使用 AS2 或 SFTP 通訊協定來傳送檔案。對於存取角色，請提供要使用之 AWS Identity and Access Management 角色的 Amazon 資源名稱 (ARN)。

適用於 AS2 連接器

使用 AS2，即可透過呼叫 StartFileTransfer，並在請求參數 SendFilePaths 中指定檔案路徑的方式傳送檔案。使用該檔案的父目錄 (例如，--send-file-paths /bucket/dir/file.txt 的父目錄為 /bucket/dir/) 暫時儲存已處理的 AS2 訊息檔案、於接收到合作夥伴的 MDN 時進行儲存，並寫入包含傳輸相關中繼資料的最終 JSON 檔案。因此，AccessRole 需要針對 StartFileTransfer 請求中使用之檔案位置的父目錄提供讀寫權限。此外，還需要針對欲透過 StartFileTransfer 傳送之檔案的父目錄提供讀寫權限。

如果您使用 AS2 連接器的基本驗證，則存取角色需要密碼的secretsmanager:GetSecretValue權限。如果密碼是使用客戶管理的金鑰而非 Secrets Manager 中的 AWS 受管理金鑰加密，則該角色也需要該金鑰的kms:Decrypt權限。

適用於 SFTP 連接器

StartFileTransfer請確定存取角色提供對要求中所使用之檔案位置之父目錄的讀取和寫入存取權。此外，請確定角色提供的secretsmanager:GetSecretValue權限 AWS Secrets Manager。

類型：字串

長度限制：長度下限為 20。長度上限為 2048。

模式：arn:.*role/\S+

必要：否

AgreementId

合約的唯一識別碼。建立協定時會傳回此識別元。

類型：字串

長度約束：固定長度為 19。

模式：a-([0-9a-f]{17})

必要：是

BaseDirectory

若要變更傳輸檔案的登陸目錄 (資料夾)，請提供您要使用的值區資料夾，例如*/DOC-EXAMPLE-BUCKET/home/mydirectory* 。

類型：字串

長度限制：長度下限為 0。長度上限為 1024。

模式：(|/.*)

必要：否

Description

若要取代現有描述，請提供協定的簡短描述。

類型：字串

長度限制：長度下限為 1。長度上限為 200。

模式：[\p{Graph}]+

必要：否

LocalProfileId

AS2 本機設定檔的唯一識別碼。

若要變更本機設定檔識別碼，請在此提供新值。

類型：字串

長度約束：固定長度為 19。

模式：p-([0-9a-f]{17})

必要：否

PartnerProfileId

合作夥伴設定檔的唯一識別碼。若要變更合作夥伴設定檔識別碼，請在此提供新值。

類型：字串

長度約束：固定長度為 19。

模式：p-([0-9a-f]{17})

必要：否

ServerId

伺服器執行個體的系統指派唯一識別碼。這是合約使用的特定伺服器。

類型：字串

長度約束：固定長度為 19。

模式：s-([0-9a-f]{17})

必要：是

Status

您可以更新協定的狀況，啟動非使用中協定或反向協定。

類型：字串

有效值:ACTIVE | INACTIVE

必要：否

回應語法

```
{
   "AgreementId": "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。

AgreementId

合約的唯一識別碼。建立協定時會傳回此識別元。

類型：字串

長度約束：固定長度為 19。

模式：a-([0-9a-f]{17})

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceExistsException

請求的資源不存在，或者存在於為命令指定的區域以外的區域中。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

HTTP 狀態碼：500

ThrottlingException

由於請求調節，因此請求遭到拒絕。

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

UpdateCertificate

更新憑證的使用中和非作用中日期。

請求語法

```
{
   "ActiveDate": number,
   "CertificateId": "string",
   "Description": "string",
   "InactiveDate": number
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

ActiveDate

選擇性日期，指定憑證變為作用的時間。

類型：Timestamp

必要：否

CertificateId

您正在更新之憑證物件的識別碼。

類型：字串

長度約束：固定長度為 22。

模式：`cert-([0-9a-f]{17})`

必要：是

Description

協助識別憑證的簡短說明。

類型：字串

長度限制：長度下限為 1。長度上限為 200。

模式：`[\p{Graph}]+`

必要：否

InactiveDate

選擇性日期，指定憑證變為停用的時間。

類型：Timestamp

必要：否

回應語法

```
{
   "CertificateId": "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。

CertificateId

傳回您正在更新之憑證物件的識別碼。

類型：字串

長度約束：固定長度為 22。

模式：`cert-([0-9a-f]{17})`

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

HTTP 狀態碼：500

ThrottlingException

由於請求調節，因此請求遭到拒絕。

HTTP 狀態碼：400

範例

範例

下列範例會更新憑證的使用中日期，將有效日期設定為 2022 年 1 月 16 日下午 16 時 12:07 世界標準時間 -5 小時。

請求範例

```
aws transfer update-certificate --certificate-id c-abcdefg123456hijk --active-date
 2022-01-16T16:12:07-05:00
```

範例

以下是此 API 呼叫的範例回應。

回應範例

```
"CertificateId": "c-abcdefg123456hijk"
```

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

UpdateConnector

更新現有連接器的某些參數。ConnectorId為您要更新的連接器提供，以及要更新之參數的新值。

請求語法

```
{
   "AccessRole": "string",
   "As2Config": {
      "BasicAuthSecretId": "string",
      "Compression": "string",
      "EncryptionAlgorithm": "string",
      "LocalProfileId": "string",
      "MdnResponse": "string",
      "MdnSigningAlgorithm": "string",
      "MessageSubject": "string",
      "PartnerProfileId": "string",
      "SigningAlgorithm": "string"
   },
   "ConnectorId": "string",
   "LoggingRole": "string",
   "SecurityPolicyName": "string",
   "SftpConfig": {
      "TrustedHostKeys": [ "string" ],
      "UserSecretId": "string"
   },
   "Url": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

AccessRole

連接器可用來使用 AS2 或 SFTP 通訊協定來傳送檔案。對於存取角色，請提供要使用之 AWS Identity and Access Management 角色的 Amazon 資源名稱 (ARN)。

適用於 AS2 連接器

使用 AS2，即可透過呼叫 StartFileTransfer，並在請求參數 SendFilePaths 中指定檔案路徑的方式傳送檔案。使用該檔案的父目錄 (例如，--send-file-paths /bucket/dir/file.txt 的父目錄為 /bucket/dir/) 暫時儲存已處理的 AS2 訊息檔案、於接收到合作夥伴的 MDN 時進行儲存，並寫入包含傳輸相關中繼資料的最終 JSON 檔案。因此，AccessRole 需要針對 StartFileTransfer 請求中使用之檔案位置的父目錄提供讀寫權限。此外，還需要針對欲透過 StartFileTransfer 傳送之檔案的父目錄提供讀寫權限。

如果您使用 AS2 連接器的基本驗證，則存取角色需要密碼的secretsmanager:GetSecretValue權限。如果密碼是使用客戶管理的金鑰而非 Secrets Manager 中的 AWS 受管理金鑰加密，則該角色也需要該金鑰的kms:Decrypt權限。

適用於 SFTP 連接器

StartFileTransfer請確定存取角色提供對要求中所使用之檔案位置之父目錄的讀取和寫入存取權。此外，請確定角色提供的secretsmanager:GetSecretValue權限 AWS Secrets Manager。

類型：字串

長度限制：長度下限為 20。長度上限為 2048。

模式：arn:.*role/\S+

必要：否

As2Config

包含 AS2 連接器物件參數的結構。

類型：As2ConnectorConfig 物件

必要：否

ConnectorId

連接器的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：c-([0-9a-f]{17})

必要：是

LoggingRole

(IAM) 角色的亞馬遜資源名稱 AWS Identity and Access Management (ARN)，可讓連接器開啟 Amazon S3 事件的 CloudWatch 記錄功能。設定後，您可以在 CloudWatch 記錄檔中檢視連接器活動。

類型：字串

長度限制：長度下限為 20。長度上限為 2048。

模式：`arn:.*role/\S+`

必要：否

SecurityPolicyName

指定連接器的安全性原則名稱。

類型：字串

長度限制：長度下限為 0。長度上限為 100。

模式：`TransferSFTPConnectorSecurityPolicy-[A-Za-z0-9-]+`

必要：否

SftpConfig

包含 SFTP 連接器物件參數的結構。

類型：SftpConnectorConfig 物件

必要：否

Url

合作夥伴的 AS2 或 SFTP 端點的網址。

類型：字串

長度限制：長度下限為 0。長度上限為 255。

必要：否

回應語法

```
{
   "ConnectorId": "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。

ConnectorId

傳回您正在更新之連接器物件的識別碼。

類型：字串

長度約束：固定長度為 19。

模式：`c-([0-9a-f]{17})`

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceExistsException

請求的資源不存在，或者存在於為命令指定的區域以外的區域中。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

HTTP 狀態碼：500

ThrottlingException

由於請求調節，因此請求遭到拒絕。

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

UpdateHostKey

更新ServerId和參數所指定之主機金鑰的描HostKeyId述。

請求語法

```
{
   "Description": "string",
   "HostKeyId": "string",
   "ServerId": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

Description

主機金鑰的更新描述。

類型：字串

長度限制：長度下限為 0。長度上限為 200。

模式：[\p{Print}]*

必要：是

HostKeyId

您正在更新之主機金鑰的識別碼。

類型：字串

長度約束：固定長度為 25。

模式：hostkey-[0-9a-f]{17}

必要：是

ServerId

包含您正在更新之主機金鑰之伺服器的識別碼。

類型：字串

長度約束：固定長度為 19。

模式：s-([0-9a-f]{17})

必要：是

回應語法

```
{
   "HostKeyId": "string",
   "ServerId": "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。

HostKeyId

傳回已更新主機金鑰的主機金鑰識別碼。

類型：字串

長度約束：固定長度為 25。

模式：hostkey-[0-9a-f]{17}

ServerId

返回包含更新主機密鑰的服務器的服務器標識符。

類型：字串

長度約束：固定長度為 19。

模式：`s-([0-9a-f]{17})`

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

HTTP 狀態碼：500

ThrottlingException

由於請求調節，因此請求遭到拒絕。

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

UpdateProfile

更新現有設定檔的某些參數。ProfileId為您要更新的設定檔提供，以及要更新之參數的新值。

請求語法

```
{
   "CertificateIds": [ "string" ],
   "ProfileId": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

CertificateIds

已匯入憑證的識別碼陣列。您可以使用此識別碼處理設定檔和合作夥伴設定檔。

類型：字串陣列

長度約束：固定長度為 22。

模式：cert-([0-9a-f]{17})

必要：否

ProfileId

您正在更新之設定檔物件的識別元。

類型：字串

長度約束：固定長度為 19。

模式：p-([0-9a-f]{17})

必要：是

回應語法

```
{
```

```
    "ProfileId": "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。

ProfileId

返回正在更新的配置文件的標識符。

類型：字串

長度約束：固定長度為 19。

模式：`p-([0-9a-f]{17})`

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

HTTP 狀態碼：500

ThrottlingException

由於請求調節，因此請求遭到拒絕。

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

UpdateServer

在建立伺服器之後，更新已啟用檔案傳輸通訊協定的伺服器內容。

呼UpdateServer叫會傳回您更新ServerId的伺服器。

請求語法

```
{
   "Certificate": "string",
   "EndpointDetails": {
      "AddressAllocationIds": [ "string" ],
      "SecurityGroupIds": [ "string" ],
      "SubnetIds": [ "string" ],
      "VpcEndpointId": "string",
      "VpcId": "string"
   },
   "EndpointType": "string",
   "HostKey": "string",
   "IdentityProviderDetails": {
      "DirectoryId": "string",
      "Function": "string",
      "InvocationRole": "string",
      "SftpAuthenticationMethods": "string",
      "Url": "string"
   },
   "LoggingRole": "string",
   "PostAuthenticationLoginBanner": "string",
   "PreAuthenticationLoginBanner": "string",
   "ProtocolDetails": {
      "As2Transports": [ "string" ],
      "PassiveIp": "string",
      "SetStatOption": "string",
      "TlsSessionResumptionMode": "string"
   },
   "Protocols": [ "string" ],
   "S3StorageOptions": {
      "DirectoryListingOptimization": "string"
   },
   "SecurityPolicyName": "string",
   "ServerId": "string",
   "StructuredLogDestinations": [ "string" ],
   "WorkflowDetails": {
```

```
      "OnPartialUpload": [
         {
            "ExecutionRole": "string",
            "WorkflowId": "string"
         }
      ],
      "OnUpload": [
         {
            "ExecutionRole": "string",
            "WorkflowId": "string"
         }
      ]
   }
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

Certificate

Certificate Manager (ACM) AWS憑證的 Amazon 資源名稱 (ARN)。當 `Protocols` 設定為 FTPS 時，此為必要項目。

若要要求新的公用憑證，請參閱 Certificate Manager 使用指南中的要求公用 AWS憑證。

若要將現有憑證匯入 ACM，請參閱《Certificate Manager 使用指南》中的〈將憑 AWS證匯入 ACM〉。

若要要求私有憑證以透過私有 IP 位址使用 FTPS，請參閱 Certificate Manager 使用者指南中的要求私有 AWS憑證。

支援具有下列密碼編譯演算法和金鑰大小的憑證：

- 2048 位元 RSA (RSA_2048)
- 4096 位元 RSA (RSA_4096)
- 橢圓定焦曲線 256 位元 (EC_prime256v1)
- 橢圓定焦曲線 384 位元 (EC_secp384r1)
- 橢圓定焦曲線 521 位元 (EC_secp521r1)

> **Note**
>
> 憑證必須是有效的 SSL/TLS X.509 版本 3 憑證，並具備 FQDN 或 IP 位址，以及簽發者的相關資訊。

類型：字串

長度限制：長度下限為 0。長度上限為 1600。

必要：否

EndpointDetails

為伺服器設定的 Virtual Private Cloud (VPC) 端點設定。當您將端點託管於 VPC 時，您可以限定只有 VPC 內的資源才可存取端點，或連接彈性 IP 地址以開放給網際網路上的用戶端存取端點。VPC 的預設安全群組會自動指派給端點。

類型：EndpointDetails 物件

必要：否

EndpointType

您希望您伺服器使用的端點類型。您可以選擇將伺服器的端點設為可公開存取 (PUBLIC)，或在 VPC 中託管。若為 VPC 中託管的端點，您可以限制只能存取 VPC 中的伺服器和資源，或直接連接彈性 IP 地址，讓其面向網際網路。

> **Note**
>
> 2021 年 5 月 19 日之後，如果您的 AWS帳戶EndpointType=VPC_ENDPOINT在 2021 年 5 月 19 日之前尚未使用，您將無法使用您的帳戶建立伺服器。如果您在 2021 年 5 月 19 日或之前已經EndpointType=VPC_ENDPOINT在您的 AWS帳戶中創建了服務器，則不會受到影響。在此日期之後，使用 EndpointType = VPC。
> 如需詳細資訊，請參閱 停止使用 VPC_ 端點。
> 建議使用 VPC 作為 EndpointType。使用此端點類型時，您可以選擇直接將最多三個彈性 IPv4 地址 (包括 BYO IP) 與伺服器的端點建立關聯，並使用 VPC 安全群組依用戶端的公用 IP 地址來限制流量。當 EndpointType 設為 VPC_ENDPOINT 時就無法如此。

類型：字串

有效值:PUBLIC | VPC | VPC_ENDPOINT

必要：否

HostKey

RSA、ECDSA 或 ED25519 私密金鑰，以用於啟用了 SFTP 的伺服器。如果您想要旋轉金鑰，或有一組使用不同演算法的作用中金鑰，您可以新增多個主機金鑰。

使用下列指令產生不含密碼的 RSA 2048 位元金鑰：

```
ssh-keygen -t rsa -b 2048 -N "" -m PEM -f my-new-server-key.
```

-b選項使用最小值 2048。您可以使用 3072 或 4096 來建立更強大的金鑰。

使用下列指令產生不含複雜密碼的 ECDSA 256 位元金鑰：

```
ssh-keygen -t ecdsa -b 256 -N "" -m PEM -f my-new-server-key.
```

ECDSA -b 選項的有效值為 256、384 和 521。

使用下列指令來產生不含密碼的 ED25519 金鑰：

```
ssh-keygen -t ed25519 -N "" -f my-new-server-key.
```

對於所有這些命令，您可以my-new-server-key用您選擇的字符串替換。

> **Important**
>
> 如果您不打算將現有使用者從現有啟用 SFTP 的伺服器遷移到新伺服器，請不要更新主機金鑰。意外變更伺服器的主機金鑰可能造成破壞。

如需詳細資訊，請參閱《 AWS Transfer Family 使用指南》中的更新已啟用 SFTP 之伺服器的主機金鑰。

類型：字串

長度限制：長度下限為 0。長度上限為 4096。

必要：否

IdentityProviderDetails

陣列，其中包含呼叫客戶驗證 API 方法所需的所有資訊。

類型：IdentityProviderDetails 物件

必要：否

LoggingRole

(IAM) 角色的 Amazon 資源名稱 AWS Identity and Access Management (ARN)，可讓伺服器為 Amazon Amazon S3 或 Amazon EFSevts 開啟亞馬遜 CloudWatch 日誌記錄。設定後，您可以檢視 CloudWatch 記錄中的使用者活動。

類型：字串

長度限制：長度下限為 0。長度上限為 2048。

模式：`(|arn:.*role/\S+)`

必要：否

PostAuthenticationLoginBanner

指定使用者連線到伺服器時要顯示的字串。此字串會在使用者驗證後顯示。

> **Note**
>
> SFTP 通訊協定不支援驗證後顯示橫幅。

類型：字串

長度限制：長度下限為 0。長度上限為 4096。

模式：`[\x09-\x0D\x20-\x7E]*`

必要：否

PreAuthenticationLoginBanner

指定使用者連線到伺服器時要顯示的字串。此字串會在使用者驗證之前顯示。例如，下列橫幅會顯示有關使用系統的詳細資訊：

```
This system is for the use of authorized users only. Individuals using
this computer system without authority, or in excess of their authority,
are subject to having all of their activities on this system monitored
and recorded by system personnel.
```

類型：字串

長度限制：長度下限為 0。長度上限為 4096。

模式：[\x09-\x0D\x20-\x7E]*

必要：否

ProtocolDetails

為伺服器設定的通訊協定設定。

- 若要指出被動模式 (用於 FTP 和 FTPS 通訊協定)，請使用 PassiveIp 參數。輸入單一點分四進制 IPv4 位址，例如防火牆、路由器或負載平衡器的外部 IP 地址。
- 若要忽略在用戶端嘗試對您上傳至 Amazon S3 儲存貯體的檔案使用 SETSTAT 命令時所產生的錯誤，請使用 SetStatOption 參數。若要讓 AWS Transfer Family 伺服器忽略指SETSTAT令並上傳檔案而不需對 SFTP 用戶端進行任何變更，請將值設定為ENABLE_NO_OP。如果將SetStatOption參數設定為ENABLE_NO_OP，Transfer Family 會產生 Amazon CloudWatch 日誌的日誌項目，以便您可以判斷用戶端何時SETSTAT撥打電話。
- 若要判斷 AWS Transfer Family 伺服器是否透過唯一的工作階段 ID 繼續最近交涉的工作階段，請使用參數TlsSessionResumptionMode。
- As2Transports 指出 AS2 訊息的傳輸方法。目前僅支援 HTTP。

類型：ProtocolDetails 物件

必要：否

Protocols

在您的檔案傳輸通訊協定用戶端可以連線到伺服器的端點上，指定檔案傳輸通訊協定或通訊協定。可用的通訊協定包括：

- SFTP (安全殼層 (SSH) 檔案傳輸通訊協定)：透過 SSH 傳輸檔案
- FTPS (檔案傳輸通訊協定安全)：使用 TLS 加密的檔案傳輸
- FTP (檔案傳輸通訊協定)：未加密的檔案傳輸
- AS2 (適用性聲明 2) ：用於傳輸結構化數據 business-to-business

> **Note**
>
> - 如果您選取FTPS，您必須選擇儲存在 AWS Certificate Manager (ACM) 中的憑證，當用戶端透過 FTPS 連線至伺服器時，用來識別您的伺服器。

- 如果 Protocol 包含 FTP 或 FTPS，則 EndpointType 必須是 VPC 且 IdentityProviderType 必須是 AWS_DIRECTORY_SERVICE、AWS_LAMBDA 或 API_GATEWAY。
- 如果 Protocol 包含 FTP，則無法與 AddressAllocationIds 建立關聯。
- 如果 Protocol 僅設定為 SFTP，則 EndpointType 可以設定為 PUBLIC，且 IdentityProviderType 可以設定任何支援的識別類型：SERVICE_MANAGED、AWS_DIRECTORY_SERVICE、AWS_LAMBDA 或 API_GATEWAY。
- 如果 Protocol 包括 AS2，則 EndpointType 必須為 VPC，且網域必須為 Amazon S3。

類型：字串陣列

陣列成員：項目數下限為 1。最多 4 個項目數。

有效值:SFTP | FTP | FTPS | AS2

必要：否

S3StorageOptions

指定 Amazon S3 目錄的效能是否已最佳化。此選項根據預設為停用。

依預設，主目錄對應具有TYPE的DIRECTORY. 如果啟用此選項，如FILE果您希望對應具有檔案目標，則需要明確地將設定為。HomeDirectoryMapEntry Type

類型：S3StorageOptions 物件

必要：否

SecurityPolicyName

指定伺服器的安全性原則名稱。

類型：字串

長度限制：長度下限為 0。長度上限為 100。

模式：Transfer[A-Za-z0-9]*SecurityPolicy-[A-Za-z0-9-]+

必要：否

ServerId

系統指派給「Transfer Family」使用者所指派之伺服器執行個體的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：s-([0-9a-f]{17})

必要：是

StructuredLogDestinations

指定要將伺服器記錄檔傳送至的記錄群組。

若要指定記錄群組，您必須提供現有記錄群組的 ARN。在此情況下，記錄群組的格式如下：

arn:aws:logs:region-name:amazon-account-id:log-group:log-group-name:*

例如：arn:aws:logs:us-east-1:111122223333:log-group:mytestgroup:*

如果您先前已為伺服器指定記錄群組，則可以在update-server呼叫中為此參數提供空白值，將其清除，並實際關閉結構化記錄。例如：

```
update-server --server-id s-1234567890abcdef0 --structured-log-
destinations
```

類型：字串陣列

陣列成員：項目數下限為 0。項目數上限為 1。

長度限制：長度下限為 20。長度上限為 1600。

模式：arn:\S+

必要：否

WorkflowDetails

指定要指派之工作流程的工作流程 ID，以及用於執行工作流程的執行角色。

除了完全上傳檔案時要執行的工作流程外，WorkflowDetails 亦可包含要在部分上傳時執行之工作流程的工作流程 ID (和執行角色)。當伺服器工作階段中斷連線，而檔案仍在上載時，就會發生部分上傳。

若要從伺服器中移除相關聯的工作流程，您可以提供空白 OnUpload 物件 (如以下範例所示)。

```
aws transfer update-server --server-id s-01234567890abcdef --workflow-details '{"OnUpload":[]}'
```

類型：WorkflowDetails 物件

必要：否

回應語法

```
{
   "ServerId": "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。

ServerId

系統指派給「Transfer Family」使用者所指定之伺服器的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：s-([0-9a-f]{17})

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：400

ConflictException

當針對已啟用 VPC 作UpdateServer為端點類型的檔案傳輸通訊協定的伺服器呼叫，且伺服器不處於可用狀態時，會擲回此例外狀況。VpcEndpointID

HTTP 狀態碼：400

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceExistsException

請求的資源不存在，或存在於為命令指定的區域以外的區域中。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

HTTP 狀態碼：500

ThrottlingException

由於請求調節，因此請求遭到拒絕。

HTTP 狀態碼：400

範例

範例

下列範例會更新伺服器的角色。

請求範例

```
{
   "EndpointDetails": {
   "VpcEndpointId": "vpce-01234f056f3g13",
   "LoggingRole": "CloudWatchS3Events",
   "ServerId": "s-01234567890abcdef"
   }
}
```

範例

下列範例會從伺服器移除任何關聯的工作流程。

請求範例

```
aws transfer update-server --server-id s-01234567890abcdef --workflow-details
 '{"OnUpload":[]}'
```

範例

這是此 API 呼叫的範例回應。

回應範例

```
{
   "ServerId": "s-01234567890abcdef"
}
```

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

UpdateUser

將新屬性指派給使用者。您傳遞的參數會修改下列任一或全部項目：ServerId您指定的和的主目錄、角色UserName和原則。

回應會傳回已更新使用者的ServerId和。UserName

在主控台中，您可以在建立或更新使用者時選取「受限制」。這可確保使用者無法存取其主目錄以外的任何內容。設定此行為的程式設計方式是更新使用者。HomeDirectoryType將它們設定為LOGICAL，並指定HomeDirectoryMappingsEntry為 root (/) 並Target做為其主目錄。

例如，如果使用者的主目錄是/test/admin-user，則下列命令會更新使用者，讓他們在主控台中的組態將「受限制」旗標顯示為已選取。

```
aws transfer update-user --server-id <server-id> --user-name admin-user --
home-directory-type LOGICAL --home-directory-mappings "[{\"Entry\":\"/\",
\"Target\":\"/test/admin-user\"}]"
```

請求語法

```
{
   "HomeDirectory": "string",
   "HomeDirectoryMappings": [
      {
         "Entry": "string",
         "Target": "string",
         "Type": "string"
      }
   ],
   "HomeDirectoryType": "string",
   "Policy": "string",
   "PosixProfile": {
      "Gid": number,
      "SecondaryGids": [ number ],
      "Uid": number
   },
   "Role": "string",
   "ServerId": "string",
   "UserName": "string"
}
```

請求參數

如需所有動作的一般參數資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

HomeDirectory

使用者使用其用戶端登入伺服器時的登陸目錄 (資料夾)。

HomeDirectory 範例為 /bucket_name/home/mydirectory。

> **Note**
>
> 只有在 HomeDirectoryType 設為 PATH 時才會使用 HomeDirectory 參數。

類型：字串

長度限制：長度下限為 0。長度上限為 1024。

模式：(|/.*)

必要：否

HomeDirectoryMappings

邏輯目錄對應，指定您的使用者可以看到哪些 Amazon S3 或 Amazon EFS 路徑和金鑰，以及您希望如何顯示這些路徑和金鑰。您必須指定Entry和Target配對，其中Entry顯示路徑的顯示方式，以及Target實際的 Amazon S3 或 Amazon EFS 路徑。如果您僅指定目標，則會依原樣顯示該目標。您還必須確保您的 AWS Identity and Access Management (IAM) 角色可提供中路徑的存取權Target。只有當設定為 LO GIC 時HomeDirectoryType，才能設定此值。

以下是Entry和配Target對範例。

```
[ { "Entry": "/directory1", "Target": "/bucket_name/home/
mydirectory" } ]
```

在大多數情況下，您可以使用此值而不是工作階段原則，將使用者鎖定到指定的主目錄 (」chroot「)。要做到這一點，你可Entry以設置為 '/' 並設置Target為 HomeDirectory參數值。

以下是的Entry和Target配對範例chroot。

```
[ { "Entry": "/", "Target": "/bucket_name/home/mydirectory" } ]
```

類型：HomeDirectoryMapEntry 物件陣列

陣列成員：項目數下限為 1。5 萬個物品的最大數量。

必要：否

HomeDirectoryType

使用者登入伺服器時，您希望的使用者主目錄之登陸目錄 (資料夾) 類型。如果將其設定為PATH，使用者將在其檔案傳輸協定用戶端中看到絕對的 Amazon S3 儲存貯體或 Amazon EFS 路徑。如果將其設定為LOGICAL，則需要在中提供對應，以便讓使用者看到 Amazon S3 或 Amazon EFS 路徑的方式。HomeDirectoryMappings

> **Note**
>
> 如果HomeDirectoryType是LOGICAL，則必須使用HomeDirectoryMappings參數提供對映。另一方面，HomeDirectoryType如果您使用HomeDirectory參數提供絕對路徑。PATH您的範本HomeDirectoryMappings中不HomeDirectory能同時擁有和。

類型：字串

有效值:PATH | LOGICAL

必要：否

Policy

適用於您的使用者的工作階段政策，以便您可以在多個使用者間使用相同的 AWS Identity and Access Management (IAM) 角色。此政策限制了使用者對 Amazon S3 儲存貯體部分的存取權限。您可以在此政策內使用的變數包括 ${Transfer:UserName}、${Transfer:HomeDirectory} 和 ${Transfer:HomeBucket}。

> **Note**
>
> 只有在的網域ServerId是 Amazon S3 時，才適用此政策。Amazon EFS 不使用工作階段政策。
> 對於工作階段政策，請將政策 AWS Transfer Family 儲存為 JSON Blob，而不是政策的 Amazon 資源名稱 (ARN)。您會將政策作為 JSON blob 儲存，並在 Policy 引數中傳遞它。

如需工作階段政策的範例，請參閱 Example session policy (工作階段政策範例)。
如需詳細資訊，請參閱 AWS 安全性權杖服務 API 參考AssumeRole中的。

類型：字串

長度限制：長度下限為 0。長度上限為 2048。

必要：否

PosixProfile

指定完整的 POSIX 身分識別，包括使用者 ID (Uid)、群組 ID (Gid) 和任何次要群組 ID (SecondaryGids)，以控制使用者對 Amazon 彈性檔案系統 (Amazon EFS) 的存取。在檔案系統中的檔案和目錄上設定的 POSIX 許可決定使用者在將檔案傳入和傳出 Amazon EFS 檔案系統時獲得的存取層級。

類型：PosixProfile 物件

必要：否

Role

(IAM) 角色的亞馬遜資源名稱 AWS Identity and Access Management (ARN)，用於控制使用者對 Amazon S3 儲存貯體或 Amazon EFS 檔案系統的存取。連接到此角色的政策會決定在將檔案傳入和傳出您的 Amazon S3 儲存貯體或 Amazon EFS 檔案系統時，您希望提供給使用者的存取層級。IAM 角色也應包含信任關係，允許伺服器在處理您使用者的傳輸請求時，存取您的資源。

類型：字串

長度限制：長度下限為 20。長度上限為 2048。

模式：`arn:.*role/\S+`

必要：否

ServerId

系統指派給使用者之「Transfer Family」伺服器執行個體的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：s-([0-9a-f]{17})

必要：是

UserName

識別使用者並且和 ServerId 所指定伺服器建立關聯的唯一字串。此使用者名稱的長度必須最少為 3 個字元，最多為 100 個字元。以下是有效字元：a-z、A-Z、0-9、底線 '_'、連字號 '-'、句號 '。' ，以及位置符號 '@'。使用者名稱不能以連字號、句號或符號開頭。

類型：字串

長度限制：長度下限為 3。長度上限為 100。

模式：[\w][\w@.-]{2,99}

必要：是

回應語法

```
{
   "ServerId": "string",
   "UserName": "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。

ServerId

系統指派給帳戶之「Transfer Family」伺服器執行個體的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：s-([0-9a-f]{17})

UserName

指派給要求中所指定之伺服器執行個體之使用者的唯一識別碼。

類型：字串

長度限制：長度下限為 3。長度上限為 100。

模式：`[\w][\w@.-]{2,99}`

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InternalServiceError

當在 AWS Transfer Family 服務中發生錯誤時，拋出此異常。

HTTP 狀態碼：500

InvalidRequestException

當客戶端提交格式錯誤的請求時，拋出此異常。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

申請失敗，因為 AWS Transfer Family 服務不可用。

HTTP 狀態碼：500

ThrottlingException

由於請求調節，因此請求遭到拒絕。

HTTP 狀態碼：400

範例

範例

下列範例會更新「Transfer Family」使用者。

請求範例

```
{
   "HomeDirectory": "/bucket2/documentation",
   "HomeDirectoryMappings": [
      {
         "Entry": "/directory1",
         "Target": "/bucket_name/home/mydirectory"
      }
   ],
   "HomeDirectoryType:" "PATH",
   "Role": "AssumeRole",
   "ServerId": "s-01234567890abcdef",
   "UserName": "my_user"
}
```

範例

這是此 API 呼叫的範例回應。

回應範例

```
{
   "ServerId": "s-01234567890abcdef",
   "UserName": "my_user"
}
```

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

資料類型

目前支援下列資料類型：

- As2ConnectorConfig
- CopyStepDetails
- CustomStepDetails
- DecryptStepDetails
- DeleteStepDetails
- DescribedAccess
- DescribedAgreement
- DescribedCertificate
- DescribedConnector
- DescribedExecution
- DescribedHostKey
- DescribedProfile
- DescribedSecurityPolicy
- DescribedServer
- DescribedUser
- DescribedWorkflow
- EfsFileLocation
- EndpointDetails
- ExecutionError
- ExecutionResults
- ExecutionStepResult
- FileLocation
- HomeDirectoryMapEntry
- IdentityProviderDetails
- InputFileLocation

- ListedAccess
- ListedAgreement
- ListedCertificate
- ListedConnector
- ListedExecution
- ListedHostKey
- ListedProfile
- ListedServer
- ListedUser
- ListedWorkflow
- LoggingConfiguration
- PosixProfile
- ProtocolDetails
- S3FileLocation
- S3InputFileLocation
- S3StorageOptions
- S3Tag
- ServiceMetadata
- SftpConnectorConfig
- SshPublicKey
- Tag
- TagStepDetails
- UserDetails
- WorkflowDetail
- WorkflowDetails
- WorkflowStep

As2ConnectorConfig

包含 AS2 連接器物件的詳細資訊。連接器物件用於 AS2 輸出程序，用來連接 AWS Transfer Family 客戶與協力廠商。

目錄

BasicAuthSecretId

為 AS2 連接器 API 提供基本驗證支援。若要使用基本身份驗證，您必須在 AWS Secrets Manager 中提供密碼的名稱或 Amazon 資源名稱 (ARN)。

此參數的預設值為null，表示連接器未啟用基本驗證。

如果連接器應使用基本驗證，密碼必須採用下列格式：

```
{ "Username": "user-name", "Password": "user-password" }
```

將user-name和user-password取代為正在驗證之實際使用者的認證。

注意下列事項：

- 您將這些認證存儲在 Secrets Manager 中，而不是將它們直接傳遞到此 API 中。
- 如果您使用 API、SDK 或 CloudFormation 設定連接器，則必須先建立密碼，才能啟用基本驗證。不過，如果您使用的是 AWS 管理主控台，則可以讓系統為您建立密碼。

如果您先前已為連接器啟用基本驗證，則可以使用 UpdateConnector API 呼叫來停用它。例如，如果您使用 CLI，可以執行下列命令來移除基本驗證：

```
update-connector --connector-id my-connector-id --as2-config
'BasicAuthSecretId=""'
```

類型：字串

長度限制：長度下限為 0。長度上限為 2048。

必要：否

Compression

指定是否壓縮 AS2 檔案。

類型：字串

有效值:ZLIB | DISABLED

必要：否

EncryptionAlgorithm

用來加密檔案的演算法。

注意下列事項：

- 除非您必須支援需要此DES_EDE3_CBC演算法的舊版用戶端，否則請勿使用演算法，因為這是弱式加密演算法。
- 您只能指定連接器的 URL 是NONE否使用 HTTPS。使用 HTTPS 可確保不會以純文字傳送流量。

類型：字串

有效值:AES128_CBC | AES192_CBC | AES256_CBC | DES_EDE3_CBC | NONE

必要：否

LocalProfileId

AS2 本機設定檔的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：p-([0-9a-f]{17})

必要：否

MdnResponse

用於輸出請求（從 AWS Transfer Family 服務器到合作夥伴 AS2 服務器），以確定傳輸的合作夥伴響應是同步還是非同步。指定下列其中一個值：

- SYNC：系統需要同步 MDN 回應，確認檔案是否已成功傳輸。
- NONE：指定不需要 MDN 回應。

類型：字串

有效值:SYNC | NONE

必要：否

MdnSigningAlgorithm

MDN 回應的簽署演算法。

> **Note**
>
> 如果設定為 DEFAULT (或完全未設定)，則會使SigningAlgorithm用的值。

類型：字串

有效值:SHA256 | SHA384 | SHA512 | SHA1 | NONE | DEFAULT

必要：否

MessageSubject

用作隨連接器一起傳送之 AS2 郵件中的 Subject HTTP 標頭屬性。

類型：字串

長度限制：長度下限為 1。長度上限為 1024。

模式：[\p{Print}\p{Blank}]+

必要：否

PartnerProfileId

連接器之合作夥伴設定檔的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：p-([0-9a-f]{17})

必要：否

SigningAlgorithm

用來簽署隨連接器一起傳送的 AS2 訊息的演算法。

類型：字串

有效值:SHA256 | SHA384 | SHA512 | SHA1 | NONE

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

CopyStepDetails

每個步驟類型都有自己的StepDetails結構。

目錄

DestinationFileLocation

指定要複製的檔案的位置。${Transfer:UploadDate}在此欄位中使用${Transfer:UserName}或，可依使用者名稱或上傳日期參數化目的地前置詞。

- 將的值設定DestinationFileLocation為，可將上傳的檔案複製${Transfer:UserName}到 Amazon S3 儲存貯體，該儲存貯體以上傳檔案的傳 Transfer Family 使用者名稱為前綴。
- 將的值設定DestinationFileLocation為，${Transfer:UploadDate}將上傳的檔案複製到以上傳日期為前綴的 Amazon S3 儲存貯體。

> **Note**
>
> 系統會根據UploadDate以 UTC 上傳檔案的日期，解析為 YYYY-MM-DD 的日期格式。

類型：InputFileLocation 物件

必要：否

Name

作為識別碼使用的步驟名稱。

類型：字串

長度限制：長度下限為 0。最大長度為 30。

模式：[\w-]*

必要：否

OverwriteExisting

指示是否覆寫現有相同名稱檔案的標記。預設值為 FALSE。

如果工作流程正在處理與現有檔案名稱相同的檔案，則行為如下：

- 如果OverwriteExisting是TRUE，則會將現有檔案取代為正在處理的檔案。
- 如果OverwriteExisting是FALSE，則不會發生任何事情，且工作流程處理會停止。

類型：字串

有效值:TRUE | FALSE

必要：否

SourceFileLocation

指定要用作工作流程步驟輸入的檔案：上一個步驟的輸出，或工作流程的原始上載檔案。

- 若要使用上一個檔案做為輸入，請輸入${previous.file}。在此情況下，此工作流程步驟會使用上一個工作流程步驟的輸出檔案作為輸入。這是預設值。
- 若要使用原始上載的檔案位置做為此步驟的輸入，請輸入${original.file}。

類型：字串

長度限制：長度下限為 0。長度上限為 256。

模式：\$\{(\w+.)+\w+\}

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

CustomStepDetails

每個步驟類型都有自己的StepDetails結構。

目錄

Name

作為識別碼使用的步驟名稱。

類型：字串

長度限制：長度下限為 0。最大長度為 30。

模式：[\w-]*

必要：否

SourceFileLocation

指定要用作工作流程步驟輸入的檔案：上一個步驟的輸出，或工作流程的原始上載檔案。

- 若要使用上一個檔案做為輸入，請輸入${previous.file}。在此情況下，此工作流程步驟會使用上一個工作流程步驟的輸出檔案作為輸入。這是預設值。
- 若要使用原始上載的檔案位置做為此步驟的輸入，請輸入${original.file}。

類型：字串

長度限制：長度下限為 0。長度上限為 256。

模式：\$\{(\w+.)+\w+\}

必要：否

Target

正在呼叫的 Lambda 函數的 ARN。

類型：字串

長度限制：長度下限為 0。長度上限為 170。

模式：arn:[a-z-]+:lambda:.*

必要：否

TimeoutSeconds

步驟的逾時時間 (以秒為單位)。

類型：整數

有效範圍：最小值為 1。最大值為 1800。

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

DecryptStepDetails

每個步驟類型都有自己的StepDetails結構。

目錄

DestinationFileLocation

指定要解密之檔案的位置。${Transfer:UploadDate}在此欄位中使用${Transfer:UserName}或，可依使用者名稱或上傳日期參數化目的地前置詞。

- DestinationFileLocation將的值設定為，可將上傳的檔案解密${Transfer:UserName}至 Amazon S3 儲存貯體，該儲存貯體以上傳檔案的傳 Transfer Family 使用者名稱為前綴。
- DestinationFileLocation將的值設定為，${Transfer:UploadDate}將上傳的檔案解密到以上傳日期為前綴的 Amazon S3 儲存貯體。

> **Note**
>
> 系統會根據UploadDate以 UTC 上傳檔案的日期，解析為 YYYY-MM-DD 的日期格式。

類型：InputFileLocation 物件

必要：是

Type

使用的加密類型。目前，這個值必須是PGP。

類型：字串

有效值:PGP

必要：是

Name

作為識別碼使用的步驟名稱。

類型：字串

長度限制：長度下限為 0。最大長度為 30。

模式：[\w-]*

必要：否

OverwriteExisting

指示是否覆寫現有相同名稱檔案的標記。預設值為 FALSE。

如果工作流程正在處理與現有檔案名稱相同的檔案，則行為如下：

- 如果OverwriteExisting是TRUE，則會將現有檔案取代為正在處理的檔案。
- 如果OverwriteExisting是FALSE，則不會發生任何事情，且工作流程處理會停止。

類型：字串

有效值:TRUE | FALSE

必要：否

SourceFileLocation

指定要用作工作流程步驟輸入的檔案：上一個步驟的輸出，或工作流程的原始上載檔案。

- 若要使用上一個檔案做為輸入，請輸入${previous.file}。在此情況下，此工作流程步驟會使用上一個工作流程步驟的輸出檔案作為輸入。這是預設值。
- 若要使用原始上載的檔案位置做為此步驟的輸入，請輸入${original.file}。

類型：字串

長度限制：長度下限為 0。長度上限為 256。

模式：\$\{(\w+.)+\w+\}

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

DeleteStepDetails

用來識別刪除步驟的步驟名稱。

目錄

Name

作為識別碼使用的步驟名稱。

類型：字串

長度限制：長度下限為 0。最大長度為 30。

模式：`[\w-]*`

必要：否

SourceFileLocation

指定要用作工作流程步驟輸入的檔案：上一個步驟的輸出，或工作流程的原始上載檔案。

- 若要使用上一個檔案做為輸入，請輸入`${previous.file}`。在此情況下，此工作流程步驟會使用上一個工作流程步驟的輸出檔案作為輸入。這是預設值。
- 若要使用原始上載的檔案位置做為此步驟的輸入，請輸入`${original.file}`。

類型：字串

長度限制：長度下限為 0。長度上限為 256。

模式：`\$\{(\w+.)+\w+\}`

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

DescribedAccess

描述指定之存取權的屬性。

目錄

ExternalId

識別目錄中特定群組所需的唯一識別碼。您關聯之群組的使用者可以透過已啟用的協定存取 Amazon S3 或 Amazon EFS 資源 AWS Transfer Family。如果您知道群組名稱，您可以使用 Windows 執行下列命令來檢視 SID 值 PowerShell。

```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties
* | Select SamAccountName,ObjectSid
```

在該命令中，YourGroupName用活動目錄組的名稱替換。

用來驗證此參數的規則運算式是由不含空格的大寫和小寫英數字元組成的字元字串。您也可以包含底線或下列任何字元：=, 。 @：/-

類型：字串

長度限制：長度下限為 1。長度上限為 256。

模式：`S-1-[\d-]+`

必要：否

HomeDirectory

使用者使用其用戶端登入伺服器時的登陸目錄 (資料夾)。

`HomeDirectory` 範例為 `/bucket_name/home/mydirectory`。

> **Note**
>
> 只有在 `HomeDirectoryType` 設為 `PATH` 時才會使用 `HomeDirectory` 參數。

類型：字串

長度限制：長度下限為 0。長度上限為 1024。

模式：`(|/.*)`

必要：否

HomeDirectoryMappings

邏輯目錄對應，指定您的使用者可以看到哪些 Amazon S3 或 Amazon EFS 路徑和金鑰，以及您希望如何顯示這些路徑和金鑰。您必須指定`Entry`和`Target`配對，其中`Entry`顯示路徑的顯示方式，以及`Target`實際的 Amazon S3 或 Amazon EFS 路徑。如果您僅指定目標，則會依原樣顯示該目標。您還必須確保您的 AWS Identity and Access Management (IAM) 角色可提供中路徑的存取權`Target`。只有當設定為邏輯時`HomeDirectoryType`，才能設定此值。

在大多數情況下，您可以使用此值而非工作階段原則來鎖定對指定主目錄 (」`chroot`「) 的關聯存取。要做到這一點，你可`Entry`以設置為 '/' 並設置`Target`為`HomeDirectory`參數值。

類型：HomeDirectoryMapEntry 物件陣列

陣列成員：項目數下限為 1。5 萬個物品的最大數量。

必要：否

HomeDirectoryType

使用者登入伺服器時，您希望的使用者主目錄之登陸目錄 (資料夾) 類型。如果將其設定為`PATH`，使用者將在其檔案傳輸協定用戶端中看到絕對的 Amazon S3 儲存貯體或 Amazon EFS 路徑。如果將其設定為`LOGICAL`，則需要在中提供對應，以便讓使用者看到 Amazon S3 或 Amazon EFS 路徑的方式。`HomeDirectoryMappings`

> **Note**
>
> 如果`HomeDirectoryType`是`LOGICAL`，則必須使用`HomeDirectoryMappings`參數提供對映。另一方面，`HomeDirectoryType`如果您使用`HomeDirectory`參數提供絕對路徑。`PATH`您的範本`HomeDirectoryMappings`中不`HomeDirectory`能同時擁有和。

類型：字串

有效值:`PATH | LOGICAL`

必要：否

Policy

用戶的會話策略，以便您可以在多個用戶之間使用相同的 AWS Identity and Access Management（IAM）角色。此政策限制了使用者對 Amazon S3 儲存貯體部分的存取權限。您可以在此

政策內使用的變數包括 `${Transfer:UserName}`、`${Transfer:HomeDirectory}` 和 `${Transfer:HomeBucket}`。

類型：字串

長度限制：長度下限為 0。長度上限為 2048。

必要：否

PosixProfile

控制使用者存取 Amazon EFS 檔案系統的完整 POSIX 身分，包括使用者 ID (`Uid`)、群組 ID (`Gid`) 和任何次要群組 ID (`SecondaryGids`)。對檔案系統中的檔案和目錄設定的 POSIX 許可，會決定使用者在 Amazon EFS 檔案系統中傳入和傳出檔案時所取得的存取等級。

類型：PosixProfile 物件

必要：否

Role

(IAM) 角色的亞馬遜資源名稱 AWS Identity and Access Management (ARN)，用於控制使用者對 Amazon S3 儲存貯體或 Amazon EFS 檔案系統的存取。連接到此角色的政策會決定在將檔案傳入和傳出您的 Amazon S3 儲存貯體或 Amazon EFS 檔案系統時，您希望提供給使用者的存取層級。IAM 角色也應包含信任關係，允許伺服器在處理您使用者的傳輸請求時，存取您的資源。

類型：字串

長度限制：長度下限為 20。長度上限為 2048。

模式：`arn:.*role/\S+`

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

DescribedAgreement

描述合約的屬性。

目錄

Arn

協議的唯一 Amazon 資源名稱 (ARN)。

類型：字串

長度限制：長度下限為 20。長度上限為 1600。

模式：`arn:\S+`

必要：是

AccessRole

連接器可用來使用 AS2 或 SFTP 通訊協定來傳送檔案。對於存取角色，請提供要使用之 AWS Identity and Access Management 角色的 Amazon 資源名稱 (ARN)。

適用於 AS2 連接器

使用 AS2，即可透過呼叫 `StartFileTransfer`，並在請求參數 `SendFilePaths` 中指定檔案路徑的方式傳送檔案。使用該檔案的父目錄 (例如，`--send-file-paths /bucket/dir/file.txt` 的父目錄為 `/bucket/dir/`) 暫時儲存已處理的 AS2 訊息檔案、於接收到合作夥伴的 MDN 時進行儲存，並寫入包含傳輸相關中繼資料的最終 JSON 檔案。因此，`AccessRole` 需要針對 `StartFileTransfer` 請求中使用之檔案位置的父目錄提供讀寫權限。此外，還需要針對欲透過 `StartFileTransfer` 傳送之檔案的父目錄提供讀寫權限。

如果您使用 AS2 連接器的基本驗證，則存取角色需要密碼的`secretsmanager:GetSecretValue`權限。如果密碼是使用客戶管理的金鑰而非 Secrets Manager 中的 AWS 受管理金鑰加密，則該角色也需要該金鑰的`kms:Decrypt`權限。

適用於 SFTP 連接器

`StartFileTransfer`請確定存取角色提供對要求中所使用之檔案位置之父目錄的讀取和寫入存取權。此外，請確定角色提供的`secretsmanager:GetSecretValue`權限 AWS Secrets Manager。

類型：字串

長度限制：長度下限為 20。長度上限為 2048。

模式：arn:.*role/\S+

必要：否

AgreementId

合約的唯一識別碼。建立協定時會傳回此識別元。

類型：字串

長度約束：固定長度為 19。

模式：a-([0-9a-f]{17})

必要：否

BaseDirectory

使用 AS2 通訊協定所傳送之檔案的登陸目錄 (資料夾)。

類型：字串

長度限制：長度下限為 0。長度上限為 1024。

模式：(|/.*)

必要：否

Description

用於識別協議的名稱或簡短描述。

類型：字串

長度限制：長度下限為 1。長度上限為 200。

模式：[\p{Graph}]+

必要：否

LocalProfileId

AS2 本機設定檔的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：`p-([0-9a-f]{17})`

必要：否

PartnerProfileId

協議中使用之合作夥伴設定檔的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：`p-([0-9a-f]{17})`

必要：否

ServerId

伺服器執行個體的系統指派唯一識別碼。此識別碼可指示協議使用的特定伺服器。

類型：字串

長度約束：固定長度為 19。

模式：`s-([0-9a-f]{17})`

必要：否

Status

協議的目前狀態，`ACTIVE` 或 `INACTIVE`。

類型：字串

有效值:`ACTIVE | INACTIVE`

必要：否

Tags

可用於進行協議分組和搜尋的金鑰/值對。

類型：Tag 物件陣列

陣列成員：項目數下限為 1。項目數上限為 50。

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

DescribedCertificate

說明憑證的特性。

目錄

Arn

憑證的唯一 Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 20。長度上限為 1600。

模式：`arn:\S+`

必要：是

ActiveDate

選擇性日期，指定憑證變為作用的時間。

類型：Timestamp

必要：否

Certificate

憑證的檔案名稱。

類型：字串

長度限制：長度下限為 1。長度上限為 16384。

模式：`[\u0009\u000A\u000D\u0020-\u00FF]*`

必要：否

CertificateChain

構成憑證鏈的憑證清單。

類型：字串

長度限制：長度下限為 1。最大長度

模式：[\u0009\u000A\u000D\u0020-\u00FF]*

必要：否

CertificateId

已匯入憑證的識別碼陣列。您可以使用此識別碼處理設定檔和合作夥伴設定檔。

類型：字串

長度約束：固定長度為 22。

模式：cert-([0-9a-f]{17})

必要：否

Description

用於識別憑證的名稱或描述。

類型：字串

長度限制：長度下限為 1。長度上限為 200。

模式：[\p{Graph}]+

必要：否

InactiveDate

選擇性日期，指定憑證變為停用的時間。

類型：Timestamp

必要：否

NotAfterDate

憑證有效的最終日期。

類型：Timestamp

必要：否

NotBeforeDate

憑證有效的最早日期。

類型：Timestamp

必要：否

Serial

憑證的序號。

類型：字串

長度限制：長度下限為 0。最大長度為 48。

模式：[\p{XDigit}{2}:?]*

必要：否

Status

憑證可以是 ACTIVE、PENDING_ROTATION 或 INACTIVE。PENDING_ROTATION 代表此憑證將在過期時取代目前憑證。

類型：字串

有效值:ACTIVE | PENDING_ROTATION | INACTIVE

必要：否

Tags

金鑰/值對，可用來分組和搜尋憑證。

類型：Tag 物件陣列

陣列成員：項目數下限為 1。項目數上限為 50。

必要：否

Type

如果已為憑證指定私有金鑰，則其類型為 CERTIFICATE_WITH_PRIVATE_KEY。如果沒有私有金鑰，則類型為 CERTIFICATE。

類型：字串

有效值:CERTIFICATE | CERTIFICATE_WITH_PRIVATE_KEY

必要：否

Usage

指定如何使用此憑證。它可以通過以下方式使用：

- SIGNING：用於簽署 AS2 訊息
- ENCRYPTION：用於加密 AS2 訊息
- TLS：用於保護透過 HTTPS 傳送的 AS2 通訊安全

類型：字串

有效值:SIGNING | ENCRYPTION

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

DescribedConnector

描述連接器的參數 (由識別) ConnectorId。

目錄

Arn

連接器的唯一 Amazon 資源名稱 (ARN)。

類型：字串

長度限制：長度下限為 20。長度上限為 1600。

模式：arn:\S+

必要：是

AccessRole

連接器可用來使用 AS2 或 SFTP 通訊協定來傳送檔案。對於存取角色，請提供要使用之 AWS Identity and Access Management 角色的 Amazon 資源名稱 (ARN)。

適用於 AS2 連接器

使用 AS2，即可透過呼叫 StartFileTransfer，並在請求參數 SendFilePaths 中指定檔案路徑的方式傳送檔案。使用該檔案的父目錄 (例如，--send-file-paths /bucket/dir/file.txt 的父目錄為 /bucket/dir/) 暫時儲存已處理的 AS2 訊息檔案、於接收到合作夥伴的 MDN 時進行儲存，並寫入包含傳輸相關中繼資料的最終 JSON 檔案。因此，AccessRole 需要針對 StartFileTransfer 請求中使用之檔案位置的父目錄提供讀寫權限。此外，還需要針對欲透過 StartFileTransfer 傳送之檔案的父目錄提供讀寫權限。

如果您使用 AS2 連接器的基本驗證，則存取角色需要密碼的secretsmanager:GetSecretValue權限。如果密碼是使用客戶管理的金鑰而非 Secrets Manager 中的 AWS 受管理金鑰加密，則該角色也需要該金鑰的kms:Decrypt權限。

適用於 SFTP 連接器

StartFileTransfer請確定存取角色提供對要求中所使用之檔案位置之父目錄的讀取和寫入存取權。此外，請確定角色提供的secretsmanager:GetSecretValue權限 AWS Secrets Manager。

類型：字串

長度限制：長度下限為 20。長度上限為 2048。

模式：`arn:.*role/\S+`

必要：否

As2Config

包含 AS2 連接器物件參數的結構。

類型：As2ConnectorConfig 物件

必要：否

ConnectorId

連接器的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：`c-([0-9a-f]{17})`

必要：否

LoggingRole

(IAM) 角色的亞馬遜資源名稱 AWS Identity and Access Management (ARN)，可讓連接器開啟 Amazon S3 事件的 CloudWatch 記錄功能。設定後，您可以在 CloudWatch 記錄檔中檢視連接器活動。

類型：字串

長度限制：長度下限為 20。長度上限為 2048。

模式：`arn:.*role/\S+`

必要：否

SecurityPolicyName

指定之連接器之安全性原則的文字名稱。

類型：字串

長度限制：長度下限為 0。長度上限為 100。

模式：`TransferSFTPConnectorSecurityPolicy-[A-Za-z0-9-]+`

必要：否

ServiceManagedEgressIpAddresses

此連接器的出口 IP 位址清單。當您建立連接器時，會自動指派這些 IP 位址。

類型：字串陣列

模式：`\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}`

必要：否

SftpConfig

包含 SFTP 連接器物件參數的結構。

類型：SftpConnectorConfig 物件

必要：否

Tags

金鑰/值對，可用來分組和搜尋連接器。

類型：Tag 物件陣列

陣列成員：項目數下限為 1。項目數上限為 50。

必要：否

Url

合作夥伴的 AS2 或 SFTP 端點的網址。

類型：字串

長度限制：長度下限為 0。長度上限為 255。

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

DescribedExecution

執行物件的詳細資訊。

目錄

ExecutionId

用於執行工作流程的唯一識別元。

類型：字串

長度約束：固定長度為 36。

模式：`[0-9a-fA-F]{8}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{12}`

必要：否

ExecutionRole

與執行相關聯的 IAM 角色。

類型：字串

長度限制：長度下限為 20。長度上限為 2048。

模式：`arn:.*role/\S+`

必要：否

InitialFileLocation

描述 Amazon S3 或 EFS 檔案位置的結構。這是執行開始時的檔案位置：如果要複製檔案，這是初始檔案位置 (相對於目的地) 檔案位置。

類型：FileLocation 物件

必要：否

LoggingConfiguration

與執行相關聯的 IAM 記錄角色。

類型：LoggingConfiguration 物件

必要：否

PosixProfile

控制使用者存取 Amazon EFS 檔案系統的完整 POSIX 身分，包括使用者 ID (Uid)、群組 ID (Gid) 和任何次要群組 ID (SecondaryGids)。對檔案系統中的檔案和目錄設定的 POSIX 許可，會決定使用者在 Amazon EFS 檔案系統中傳入和傳出檔案時所取得的存取等級。

類型：PosixProfile 物件

必要：否

Results

描述執行結果的結構。這包括步驟清單，以及每個步驟的詳細資訊、錯誤類型和訊息 (如果有的話)，以及結OnExceptionSteps構。

類型：ExecutionResults 物件

必要：否

ServiceMetadata

與工作流程相關聯之工作階段詳細資訊的容器物件。

類型：ServiceMetadata 物件

必要：否

Status

狀態是其中一個執行。可以在進行中、已完成、遇到異常或處理異常。

類型：字串

有效值:IN_PROGRESS | COMPLETED | EXCEPTION | HANDLING_EXCEPTION

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

DescribedHostKey

伺服器主機金鑰的詳細資料。

目錄

Arn

主機金鑰的唯一 Amazon 資源名稱 (ARN)。

類型：字串

長度限制：長度下限為 20。長度上限為 1600。

模式：`arn:\S+`

必要：是

DateImported

將主機金鑰新增至伺服器的日期。

類型：Timestamp

必要：否

Description

此主機金鑰的文字描述。

類型：字串

長度限制：長度下限為 0。長度上限為 200。

模式：`[\p{Print}]*`

必要：否

HostKeyFingerprint

公開金鑰指紋，是用來識別較長公開金鑰的簡短位元組序列。

類型：字串

必要：否

HostKeyId

主機金鑰的唯一識別碼。

類型：字串

長度約束：固定長度為 25。

模式：`hostkey-[0-9a-f]{17}`

必要：否

Tags

可用於分組和搜尋主機金鑰的索引鍵值配對。

類型：Tag 物件陣列

陣列成員：項目數下限為 1。項目數上限為 50。

必要：否

Type

用於主機金鑰的加密演算法。使用下列其中一個值來指定Type參數：

- `ssh-rsa`
- `ssh-ed25519`
- `ecdsa-sha2-nistp256`
- `ecdsa-sha2-nistp384`
- `ecdsa-sha2-nistp521`

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

DescribedProfile

本機或合作夥伴 AS2 設定檔的詳細資訊。

目錄

Arn

設定檔的唯一 Amazon 資源名稱 (ARN)。

類型：字串

長度限制：長度下限為 20。長度上限為 1600。

模式：`arn:\S+`

必要：是

As2Id

As2Id 是 AS2 名稱，如 RFC 4130 中所定義。若為對內傳輸，這是合作夥伴傳送的 AS2 訊息 AS2-From 標頭。若為對外連接器，這是使用 StartFileTransfer API 操作傳送給合作夥伴的 AS2 訊息 AS2-To 標頭。此 ID 不可包含空格。

類型：字串

長度限制：長度下限為 1。長度上限為 128。

模式：`[\p{Print}\s]*`

必要：否

CertificateIds

已匯入憑證的識別碼陣列。您可以使用此識別碼處理設定檔和合作夥伴設定檔。

類型：字串陣列

長度約束：固定長度為 22。

模式：`cert-([0-9a-f]{17})`

必要：否

ProfileId

本機或合作夥伴 AS2 設定檔的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：`p-([0-9a-f]{17})`

必要：否

ProfileType

指示是否僅列出 LOCAL 類型設定檔，或僅列出 PARTNER 類型設定檔。如果請求中未提供，命令會將所有類型的設定檔列出。

類型：字串

有效值:`LOCAL | PARTNER`

必要：否

Tags

金鑰/值對，可用來分組和搜尋設定檔。

類型：Tag 物件陣列

陣列成員：項目數下限為 1。項目數上限為 50。

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

DescribedSecurityPolicy

說明您所指定之安全原則的特性。如需有關安全性原則的詳細資訊，請參閱使用伺服器的安全性原則或使用 SFTP 連接器的安全性原則。

目錄

SecurityPolicyName

指定安全性原則的文字名稱。

類型：字串

長度限制：長度下限為 0。長度上限為 100。

模式：`Transfer[A-Za-z0-9]*SecurityPolicy-[A-Za-z0-9-]+`

必要：是

Fips

指定此原則是否啟用聯邦資訊處理標準 (FIPS)。此參數同時適用於伺服器和連接器安全性原則。

類型：布林值

必要：否

Protocols

列出安全性原則所套用的檔案傳輸通訊協定。

類型：字串陣列

陣列成員：項目數下限為 1。項目數上限為 5。

有效值:`SFTP | FTPS`

必要：否

SshCiphers

列出連接至伺服器或連接器的安全性原則中已啟用的安全殼層 (SSH) 加密演算法。此參數同時適用於伺服器和連接器安全性原則。

類型：字串陣列

長度限制：長度下限為 0。長度上限為 50。

必要：否

SshHostKeyAlgorithms

列出安全性原則的主機金鑰演算法。

> **Note**
>
> 此參數僅適用於連接器的安全性原則。

類型：字串陣列

長度限制：長度下限為 0。長度上限為 50。

必要：否

SshKexs

列出連接至伺服器或連接器的安全性原則中已啟用的 SSH 金鑰交換 (KEX) 加密演算法。此參數同時適用於伺服器和連接器安全性原則。

類型：字串陣列

長度限制：長度下限為 0。長度上限為 50。

必要：否

SshMacs

列出連接至伺服器或連接器之安全性原則中已啟用的 SSH 訊息驗證碼 (MAC) 加密演算法。此參數同時適用於伺服器和連接器安全性原則。

類型：字串陣列

長度限制：長度下限為 0。長度上限為 50。

必要：否

TlsCiphers

列出連接至伺服器之安全性原則中已啟用的傳輸層安全性 (TLS) 加密演算法。

> **Note**
>
> 此參數僅適用於伺服器的安全性原則。

類型：字串陣列

長度限制：長度下限為 0。長度上限為 50。

必要：否

Type

安全策略套用的資源類型，可以是伺服器或連接器。

類型：字串

有效值:`SERVER | CONNECTOR`

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

DescribedServer

說明已指定之已啟用檔案傳輸通訊協定之伺服器的內容。

目錄

Arn

指定伺服器的唯一 Amazon 資源名稱 (ARN)。

類型：字串

長度限制：長度下限為 20。長度上限為 1600。

模式：`arn:\S+`

必要：是

As2ServiceManagedEgressIpAddresses

此伺服器的出口 IP 位址清單。這些 IP 位址僅與使用 AS2 通訊協定的伺服器相關。它們用於發送異步 MDN。

當您建立 AS2 伺服器時，會自動指派這些 IP 位址。此外，如果您更新現有伺服器並新增 AS2 通訊協定，也會指派靜態 IP 位址。

類型：字串陣列

模式：`\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}`

必要：否

Certificate

指定 Certificate Manager (ACM) AWS憑證的 ARN。當 `Protocols` 設定為 FTPS 時，此為必要項目。

類型：字串

長度限制：長度下限為 0。長度上限為 1600。

必要：否

Domain

指定用於檔案傳輸的儲存系統網域。有兩個域可用：Amazon Simple Storage Service (Amazon S3) 和 Amazon Elastic File System（Amazon EFS）。預設值為 S3。

類型：字串

有效值:`S3 | EFS`

必要：否

EndpointDetails

為伺服器設定的 Virtual Private Cloud (VPC) 端點設定。當您將端點託管於 VPC 時，您可以限定只有 VPC 內的資源才可存取端點，或連接彈性 IP 地址以開放給網際網路上的用戶端存取端點。VPC 的預設安全群組會自動指派給端點。

類型：EndpointDetails 物件

必要：否

EndpointType

定義伺服器所連線的端點類型。如果您的伺服器已連接到 VPC 端點，則無法透過公用網際網路存取您的伺服器。

類型：字串

有效值:`PUBLIC | VPC | VPC_ENDPOINT`

必要：否

HostKeyFingerprint

指定伺服器主機金鑰的 Base64 編碼 SHA256 指紋。這個值相當於命`ssh-keygen -l -f my-new-server-key`令的輸出。

類型：字串

必要：否

IdentityProviderDetails

指定要呼叫客戶提供的驗證 API 的資訊。當伺服器為`AWS_DIRECTORY_SERVICE`或時，不會填入此欄位`SERVICE_MANAGED`。`IdentityProviderType`

類型：IdentityProviderDetails 物件

必要：否

IdentityProviderType

伺服器的身分驗證模式。預設值為SERVICE_MANAGED，可讓您在 AWS Transfer Family 服務中儲存和存取使用者認證。

用AWS_DIRECTORY_SERVICE於在內部部署環境 AWS Directory Service for Microsoft Active Directory 或 AWS 使用 AD Connector 中，提供存取作用中目錄群組或 Microsoft Active Directory。此選項也要求您使用 IdentityProviderDetails 參數提供 Directory ID。

使用 API_GATEWAY 值來和您選擇的身分提供者整合。API_GATEWAY 設定要求您提供 Amazon API Gateway 端點 URL，以使用 IdentityProviderDetails 參數呼叫驗證。

使用該AWS_LAMBDA值直接使用 AWS Lambda 函數作為您的身份提供者。如果選擇此值，則必須在IdentityProviderDetails資料類型的參數中指定 Lambda 函Function數的 ARN。

類型：字串

有效值:SERVICE_MANAGED | API_GATEWAY | AWS_DIRECTORY_SERVICE | AWS_LAMBDA

必要：否

LoggingRole

(IAM) 角色的 Amazon 資源名稱 AWS Identity and Access Management (ARN)，可讓伺服器為 Amazon Amazon S3 或 Amazon EFSevts 開啟亞馬遜 CloudWatch 日誌記錄。設定後，您可以檢視 CloudWatch 記錄中的使用者活動。

類型：字串

長度限制：長度下限為 0。長度上限為 2048。

模式：(|arn:.*role/\S+)

必要：否

PostAuthenticationLoginBanner

指定使用者連線到伺服器時要顯示的字串。此字串會在使用者驗證後顯示。

> **Note**
>
> SFTP 通訊協定不支援驗證後顯示橫幅。

類型：字串

長度限制：長度下限為 0。長度上限為 4096。

模式：`[\x09-\x0D\x20-\x7E]*`

必要：否

PreAuthenticationLoginBanner

指定使用者連線到伺服器時要顯示的字串。此字串會在使用者驗證之前顯示。例如，下列橫幅會顯示有關使用系統的詳細資訊：

```
This system is for the use of authorized users only. Individuals using
this computer system without authority, or in excess of their authority,
are subject to having all of their activities on this system monitored
and recorded by system personnel.
```

類型：字串

長度限制：長度下限為 0。長度上限為 4096。

模式：`[\x09-\x0D\x20-\x7E]*`

必要：否

ProtocolDetails

為伺服器設定的通訊協定設定。

- 若要指出被動模式 (用於 FTP 和 FTPS 通訊協定)，請使用 `PassiveIp` 參數。輸入單一點分四進制 IPv4 位址，例如防火牆、路由器或負載平衡器的外部 IP 地址。
- 若要忽略在用戶端嘗試對您上傳至 Amazon S3 儲存貯體的檔案使用 SETSTAT 命令時所產生的錯誤，請使用 `SetStatOption` 參數。若要讓 AWS Transfer Family 伺服器忽略指SETSTAT令並上傳檔案而不需對 SFTP 用戶端進行任何變更，請將值設定為`ENABLE_NO_OP`。如果將`SetStatOption`參數設定為`ENABLE_NO_OP`，Transfer Family 會產生 Amazon CloudWatch 日誌的日誌項目，以便您可以判斷用戶端何時SETSTAT撥打電話。
- 若要判斷 AWS Transfer Family 伺服器是否透過唯一的工作階段 ID 繼續最近交涉的工作階段，請使用參數`TlsSessionResumptionMode`。
- `As2Transports` 指出 AS2 訊息的傳輸方法。目前僅支援 HTTP。

類型：ProtocolDetails 物件

必要：否

Protocols

在您的檔案傳輸通訊協定用戶端可以連線到伺服器的端點上，指定檔案傳輸通訊協定或通訊協定。可用的通訊協定包括：

- SFTP (安全殼層 (SSH) 檔案傳輸通訊協定)：透過 SSH 傳輸檔案
- FTPS (檔案傳輸通訊協定安全)：使用 TLS 加密的檔案傳輸
- FTP (檔案傳輸通訊協定)：未加密的檔案傳輸
- AS2（適用性聲明 2）：用於傳輸結構化數據 business-to-business

> **Note**
>
> - 如果您選取FTPS，您必須選擇儲存在 AWS Certificate Manager (ACM) 中的憑證，當用戶端透過 FTPS 連線至伺服器時，此憑證可用來識別您的伺服器。
> - 如果 Protocol 包含 FTP 或 FTPS，則 EndpointType 必須是 VPC 且 IdentityProviderType 必須是 AWS_DIRECTORY_SERVICE、AWS_LAMBDA 或 API_GATEWAY。
> - 如果 Protocol 包含 FTP，則無法與 AddressAllocationIds 建立關聯。
> - 如果 Protocol 僅設定為 SFTP，則 EndpointType 可以設定為 PUBLIC，且 IdentityProviderType 可以設定任何支援的識別類型：SERVICE_MANAGED、AWS_DIRECTORY_SERVICE、AWS_LAMBDA 或 API_GATEWAY。
> - 如果 Protocol 包括 AS2，則 EndpointType 必須為 VPC，且網域必須為 Amazon S3。

類型：字串陣列

陣列成員：項目數下限為 1。最多 4 個項目數。

有效值:SFTP | FTP | FTPS | AS2

必要：否

S3StorageOptions

指定您的 Amazon S3 目錄的效能是否已最佳化。此選項根據預設為停用。

依預設，主目錄對應具有TYPE的DIRECTORY. 如果啟用此選項，如FILE果您希望對應具有檔案目標，則需要明確地將設定為。HomeDirectoryMapEntry Type

類型：S3StorageOptions 物件

必要：否

SecurityPolicyName

指定伺服器的安全性原則名稱。

類型：字串

長度限制：長度下限為 0。長度上限為 100。

模式：Transfer[A-Za-z0-9]*SecurityPolicy-[A-Za-z0-9-]+

必要：否

ServerId

為您具現化的伺服器指定唯一的系統指定識別碼。

類型：字串

長度約束：固定長度為 19。

模式：s-([0-9a-f]{17})

必要：否

State

所描述的伺服器狀況。的值ONLINE表示伺服器可以接受工作和傳輸檔案。State值表OFFLINE示伺服器無法執行檔案傳輸作業。

的狀態STARTING並STOPPING指出伺服器處於中繼狀態，可能無法完全回應，或無法完全離線。START_FAILED或的值STOP_FAILED可以表示錯誤狀況。

類型：字串

有效值:OFFLINE | ONLINE | STARTING | STOPPING | START_FAILED | STOP_FAILED

必要：否

StructuredLogDestinations

指定要將伺服器記錄檔傳送至的記錄群組。

若要指定記錄群組，您必須提供現有記錄群組的 ARN。在此情況下，記錄群組的格式如下：

`arn:aws:logs:region-name:amazon-account-id:log-group:log-group-name:*`

例如：`arn:aws:logs:us-east-1:111122223333:log-group:mytestgroup:*`

如果您先前已為伺服器指定記錄群組，則可以在`update-server`呼叫中為此參數提供空白值，將其清除，並實際關閉結構化記錄。例如：

```
update-server --server-id s-1234567890abcdef0 --structured-log-
destinations
```

類型：字串陣列

陣列成員：項目數下限為 0。項目數上限為 1。

長度限制：長度下限為 20。長度上限為 1600。

模式：`arn:\S+`

必要：否

Tags

指定可用來搜尋指派給所描述之伺服器的伺服器和群組的索引鍵值配對。

類型：Tag 物件陣列

陣列成員：項目數下限為 1。項目數上限為 50。

必要：否

UserCount

指定指派給您使用指定之伺服器的使用者數目`ServerId`。

類型：整數

必要：否

WorkflowDetails

指定要指派之工作流程的工作流程 ID，以及用於執行工作流程的執行角色。

除了完全上傳檔案時要執行的工作流程外，`WorkflowDetails` 亦可包含要在部分上傳時執行之工作流程的工作流程 ID (和執行角色)。當伺服器工作階段中斷連線，而檔案仍在上載時，就會發生部分上傳。

類型：WorkflowDetails 物件

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

DescribedUser

說明指定之使用者的特性。

目錄

Arn

為要求描述的使用者指定唯一的 Amazon 資源名稱 (ARN)。

類型：字串

長度限制：長度下限為 20。長度上限為 1600。

模式：`arn:\S+`

必要：是

HomeDirectory

使用者使用其用戶端登入伺服器時的登陸目錄 (資料夾)。

`HomeDirectory` 範例為 `/bucket_name/home/mydirectory`。

> **Note**
> 只有在 `HomeDirectoryType` 設為 `PATH` 時才會使用 `HomeDirectory` 參數。

類型：字串

長度限制：長度下限為 0。長度上限為 1024。

模式：`(|/.*)`

必要：否

HomeDirectoryMappings

邏輯目錄對應，指定您的使用者可以看到哪些 Amazon S3 或 Amazon EFS 路徑和金鑰，以及您希望如何顯示這些路徑和金鑰。您必須指定`Entry`和`Target`配對，其中`Entry`顯示路徑的顯示方式，以及`Target`實際的 Amazon S3 或 Amazon EFS 路徑。如果您僅指定目標，則會依原樣顯示

該目標。您還必須確保您的 AWS Identity and Access Management (IAM) 角色可提供中路徑的存取權Target。只有當設定為邏輯時HomeDirectoryType，才能設定此值。

在大多數情況下，您可以使用此值而不是工作階段原則，將使用者鎖定到指定的主目錄 (」chroot「)。要做到這一點，你可Entry以設置為 '/' 並設置Target為 HomeDirectory參數值。

類型：HomeDirectoryMapEntry 物件陣列

陣列成員：項目數下限為 1。5 萬個物品的最大數量。

必要：否

HomeDirectoryType

使用者登入伺服器時，您希望的使用者主目錄之登陸目錄 (資料夾) 類型。如果將其設定為PATH，使用者將在其檔案傳輸協定用戶端中看到絕對的 Amazon S3 儲存貯體或 Amazon EFS 路徑。如果將其設定為LOGICAL，則需要在中提供對應，以便讓使用者看到 Amazon S3 或 Amazon EFS 路徑的方式。HomeDirectoryMappings

> **Note**
>
> 如果HomeDirectoryType是LOGICAL，則必須使用HomeDirectoryMappings參數提供對映。另一方面，HomeDirectoryType如果您使用HomeDirectory參數提供絕對路徑。PATH您的範本HomeDirectoryMappings中不HomeDirectory能同時擁有和。

類型：字串

有效值:PATH | LOGICAL

必要：否

Policy

適用於您的使用者的工作階段政策，以便您可以在多個使用者間使用相同的 AWS Identity and Access Management (IAM) 角色。此政策限制了使用者對 Amazon S3 儲存貯體部分的存取權限。您可以在此政策內使用的變數包括 ${Transfer:UserName}、${Transfer:HomeDirectory} 和 ${Transfer:HomeBucket}。

類型：字串

長度限制：長度下限為 0。長度上限為 2048。

必要：否

PosixProfile

指定完整的 POSIX 身分識別，包括使用者 ID (Uid)、群組 ID (Gid) 和任何次要群組識別碼 (SecondaryGids)，以控制使用者對 Amazon Elastic File System (Amazon EFS) 檔案系統的存取權限。對檔案系統中的檔案和目錄設定的 POSIX 許可，會決定使用者在 Amazon EFS 檔案系統中傳入和傳出檔案時所取得的存取等級。

類型：PosixProfile 物件

必要：否

Role

(IAM) 角色的亞馬遜資源名稱 AWS Identity and Access Management (ARN)，用於控制使用者對 Amazon S3 儲存貯體或 Amazon EFS 檔案系統的存取。連接到此角色的政策會決定在將檔案傳入和傳出您的 Amazon S3 儲存貯體或 Amazon EFS 檔案系統時，您希望提供給使用者的存取層級。IAM 角色也應包含信任關係，允許伺服器在處理您使用者的傳輸請求時，存取您的資源。

類型：字串

長度限制：長度下限為 20。長度上限為 2048。

模式：arn:.*role/\S+

必要：否

SshPublicKeys

指定為所描述使用者存放安全通訊殼層 (SSH) 金鑰的公有金鑰部分。

類型：SshPublicKey 物件陣列

陣列成員：項目數下限為 0。項目數上限為 5。

必要：否

Tags

為請求的用戶指定鍵值對。標籤可用於搜尋使用者並將使用者分組，以達到各種目的。

類型：Tag 物件陣列

陣列成員：項目數下限為 1。項目數上限為 50。

必要：否

UserName

指定要求描述的使用者名稱。使用者名稱用於驗證目的。這是您的用戶登錄到服務器時將使用的字符串。

類型：字串

長度限制：長度下限為 3。長度上限為 100。

模式：`[\w][\w@.-]{2,99}`

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

DescribedWorkflow

描述指定工作流程的屬性

目錄

Arn

指定工作流程的唯一 Amazon 資源名稱 (ARN)。

類型：字串

長度限制：長度下限為 20。長度上限為 1600。

模式：`arn:\S+`

必要：是

Description

指定工作流程的文字描述。

類型：字串

長度限制：長度下限為 0。長度上限為 256。

模式：`[\w- ]*`

必要：否

OnExceptionSteps

指定工作流程執行期間遇到錯誤時要採取的步驟 (動作)。

類型：WorkflowStep 物件陣列

陣列成員：項目數下限為 0。最多 8 個項目數。

必要：否

Steps

指定在指定工作流程中步驟的詳細資訊。

類型：WorkflowStep 物件陣列

陣列成員：項目數下限為 0。最多 8 個項目數。

必要：否

Tags

鍵/值對，可用來分組和搜尋工作流程。標籤是基於任何用途連接到工作流程的中繼資料。

類型：Tag 物件陣列

陣列成員：項目數下限為 1。項目數上限為 50。

必要：否

WorkflowId

工作流程的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：`w-([a-z0-9]{17})`

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

EfsFileLocation

指定工作流程中正在使用的檔案之檔案位置的詳細資料。只有在您使用 Amazon 彈性檔案系統 (Amazon EFS) 進行儲存時才適用。

目錄

FileSystemId

由 Amazon EFS 指派的檔案系統識別碼。

類型：字串

長度限制：長度下限為 0。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：否

Path

工作流程所使用之資料夾的路徑名稱。

類型：字串

長度限制：長度下限為 1。最大長度為 65536。

模式：`[^\x00]+`

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

EndpointDetails

針對已啟用檔案傳輸通訊協定的伺服器所設定的虛擬私有雲端 (VPC) 端點設定。使用 VPC 端點時，您可以限制只能存取 VPC 中的伺服器和資源。要控制傳入的互聯網流量，請調用 `UpdateServer` API 並將彈性 IP 地址附加到服務器的端點。

> **Note**
>
> 2021 年 5 月 19 日之後，如果您的 AWS帳戶`EndpointType=VPC_ENDPOINT`在 2021 年 5 月 19 日之前尚未使用，您將無法使用您的帳戶建立伺服器。如果您在 2021 年 5 月 19 日或之前已經`EndpointType=VPC_ENDPOINT`在您的 AWS帳戶中創建了服務器，則不會受到影響。在此日期之後，使用 `EndpointType = VPC`。
> 如需詳細資訊，請參閱 停止使用 VPC_ 端點。

目錄

AddressAllocationIds

將彈性 IP 地址連接至伺服器的端點時，需要的地址配置 ID 清單。

位址配置 ID 對應於彈性 IP 位址的配置識別碼。您可以從 Amazon EC2 地址資料類型的`allocationId`欄位擷取此值。擷取此值的一種方法是呼叫 EC2 DescribeAddressesAPI。

此為選用參數。如果要將 VPC 端點設定為公開，請設定此參數。如需詳細資訊，請參閱為您的伺服器建立網際網路對向端點。

> **Note**
>
> 此屬性只能設定如下：
>
> - `EndpointType`必須設定為 VPC
> - 轉移系列伺服器必須離線。
> - 您無法為使用 FTP 通訊協定的 Transfer Family 伺服器設定此參數。
> - 伺服器必須已`SubnetIds`填入 (`SubnetIds`且`AddressAllocationIds`無法同時更新)。
> - `AddressAllocationIds`不能包含重複項目，且長度必須等於`SubnetIds`。例如，如果您有三個子網路 ID，您也必須指定三個位址配置 ID。

- 呼叫 UpdateServer API 以設定或變更此參數。

類型：字串陣列

必要：否

SecurityGroupIds

可連接至伺服器端點的安全群組 ID 清單。

> **Note**
>
> 只有當 EndpointType 設為 VPC 時，才能設定此屬性。
> 只有在VPC_ENDPOINT將「EndpointType從」PUBLIC 或「變更為」時，才能在UpdateServerAPI 中編輯SecurityGroupIds屬性VPC。若要在建立之後變更與伺服器虛擬私人雲端端點相關聯的安全群組，請使用 Amazon EC2 ModifyVpcEndpointAPI。

類型：字串陣列

長度限制：長度下限為 11。長度上限為 20。

模式：sg-[0-9a-f]{8,17}

必要：否

SubnetIds

在 VPC 中託管伺服器端點時，需要的子網路 ID 清單。

> **Note**
>
> 只有當 EndpointType 設為 VPC 時，才能設定此屬性。

類型：字串陣列

必要：否

VpcEndpointId

VPC 端點的識別碼。

> **Note**
>
> 只有當 EndpointType 設為 VPC_ENDPOINT 時，才能設定此屬性。
> 如需詳細資訊，請參閱 停止使用 VPC_ 端點。

類型：字串

長度約束：固定長度為 22。

模式：vpce-[0-9a-f]{17}

必要：否

VpcId

將託管伺服器端點之 VPC 的 VPC 識別碼。

> **Note**
>
> 只有當 EndpointType 設為 VPC 時，才能設定此屬性。

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

ExecutionError

指定工作流程執行期間發生的錯誤訊息和類型。

目錄

Message

指定對應於的描述性訊息ErrorType。

類型：字串

必要：是

Type

指定錯誤類型。

- ALREADY_EXISTS：如果未選取覆寫選項，且目標位置中已存在具有相同名稱的檔案，則會發生複製步驟。
- BAD_REQUEST：一般錯誤請求：例如，嘗試標記 EFS 檔案的步驟會傳回BAD_REQUEST，因為只能標記 S3 檔案。
- CUSTOM_STEP_FAILED: 當自訂步驟提供指示失敗的回呼時發生。
- INTERNAL_SERVER_ERROR：由於各種原因可能發生的全部錯誤。
- NOT_FOUND：當請求的實體（例如複製步驟的源文件）不存在時發生。
- PERMISSION_DENIED：如果您的原則不包含完成工作流程中一或多個步驟的正確權限，就會發生。
- TIMEOUT：當執行超時時發生。

  > **Note**
  >
  > 您可以將自訂步驟設定TimeoutSeconds為 1 秒到 1800 秒 (30 分鐘) 的任何位置。

- THROTTLED：如果您超過每秒一個工作流程的新執行重新填充率，則會發生此問題。

類型：字串

有效值:PERMISSION_DENIED | CUSTOM_STEP_FAILED | THROTTLED | ALREADY_EXISTS | NOT_FOUND | BAD_REQUEST | TIMEOUT | INTERNAL_SERVER_ERROR

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 的开发
- AWS 適用於紅寶石 V3 的 SDK

ExecutionResults

指定工作流程中的步驟，以及在工作流程執行期間發生任何錯誤時要執行的步驟。

目錄

OnExceptionSteps

指定工作流程執行期間遇到錯誤時要採取的步驟 (動作)。

類型：ExecutionStepResult 物件陣列

陣列成員：項目數下限為 1。項目數上限為 50。

必要：否

Steps

指定在指定工作流程中步驟的詳細資訊。

類型：ExecutionStepResult 物件陣列

陣列成員：項目數下限為 1。項目數上限為 50。

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

ExecutionStepResult

指定步驟的下列詳細資訊：error (如果有的話)、輸出 (如果有的話) 和步驟類型。

目錄

Error

指定錯誤的詳細資訊 (如果錯誤在執行指定的工作流程步驟期間發生)。

類型：ExecutionError 物件

必要：否

Outputs

套用作為標籤至檔案的索引鍵/值組的值。只有在步驟類型為時才適用TAG。

類型：字串

長度限制：長度下限為 0。最大長度為 65536。

必要：否

StepType

其中一個可用的步驟類型。

- **COPY** - 將檔案複製到另一個位置。
- **CUSTOM**-使用 AWS Lambda 函數目標執行自訂步驟。
- **DECRYPT** - 解密上傳前已加密的檔案。
- **DELETE** - 刪除檔案。
- **TAG** - 在檔案中新增標籤。

類型：字串

有效值:COPY | CUSTOM | TAG | DELETE | DECRYPT

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

FileLocation

指定要在步驟中使用的 Amazon S3 或 EFS 檔案詳細資訊。

目錄

EfsFileLocation

指定 Amazon EFS 識別碼和所使用檔案的路徑。

類型：EfsFileLocation 物件

必要：否

S3FileLocation

指定所使用檔案的 S3 詳細資料，例如儲存貯體、ETag 等。

類型：S3FileLocation 物件

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

HomeDirectoryMapEntry

代表物件，包含 HomeDirectoryMappings 的項目和目標。

以下是的Entry和Target配對範例chroot。

```
[ { "Entry": "/", "Target": "/bucket_name/home/mydirectory" } ]
```

目錄

Entry

代表 HomeDirectoryMappings 的一個項目。

類型：字串

長度限制：長度下限為 0。長度上限為 1024。

模式：/.*

必要：是

Target

代表 HomeDirectoryMapEntry 中使用的映射目標。

類型：字串

長度限制：長度下限為 0。長度上限為 1024。

模式：/.*

必要：是

Type

指定對映的類型。FILE如果您希望對映指向檔案，或讓目錄指向目錄，請將類型設定DIRECTORY為。

> **Note**
>
> 根據預設，當您建立「Transfer Family」伺服器DIRECTORY時，主目錄對應會有一個. Type FILE如果您希望映射具有文件目標，則需要明確設Type置為。

類型：字串

有效值:`FILE | DIRECTORY`

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

IdentityProviderDetails

傳回與啟用檔案傳輸通訊協定之伺服器使用者所使用之使用者驗證類型相關的資訊。伺服器只能有一種驗證方法。

目錄

DirectoryId

您要用作身分識別提供者之 AWS Directory Service 目錄的識別碼。

類型：字串

長度約束：固定長度為 12。

模式：`d-[0-9a-f]{10}`

必要：否

Function

用於身分識別提供者之 Lambda 函數的 ARN。

類型：字串

長度限制：長度下限為 1。長度上限為 170。

模式：`arn:[a-z-]+:lambda:.*`

必要：否

InvocationRole

此參數僅適用於您`IdentityProviderType`的`API_GATEWAY`。提供驗證使用者帳戶的 `InvocationRole` 類型。

類型：字串

長度限制：長度下限為 20。長度上限為 2048。

模式：`arn:.*role/\S+`

必要：否

SftpAuthenticationMethods

對於啟用 SFTP 的伺服器，以及僅針對自訂身分識別提供者，您可以指定是使用密碼、SSH key pair 或兩者進行驗證。

- PASSWORD-使用者必須提供密碼才能連線。
- PUBLIC_KEY-使用者必須提供私密金鑰才能連線。
- PUBLIC_KEY_OR_PASSWORD-用戶可以使用其密碼或密鑰進行身份驗證。這是預設值。
- PUBLIC_KEY_AND_PASSWORD-用戶必須同時提供私鑰和密碼才能連接。伺服器會先檢查金鑰，然後如果金鑰有效，系統會提示輸入密碼。如果提供的私密金鑰與儲存的公開金鑰不符，驗證就會失敗。

類型：字串

有效值:PASSWORD | PUBLIC_KEY | PUBLIC_KEY_OR_PASSWORD | PUBLIC_KEY_AND_PASSWORD

必要：否

Url

包含用於驗證使用者身分的服務端點位置。

類型：字串

長度限制：長度下限為 0。長度上限為 255。

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

InputFileLocation

指定正在處理的檔案的位置。

目錄

EfsFileLocation

指定要解密之 Amazon Elastic File System (Amazon EFS) 檔案的詳細資料。

類型：EfsFileLocation 物件

必要：否

S3FileLocation

指定要複製或解密之 Amazon S3 檔案的詳細資訊。

類型：S3InputFileLocation 物件

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

ListedAccess

列出一或多個指定關聯存取的屬性。

目錄

ExternalId

識別目錄中特定群組所需的唯一識別碼。您關聯之群組的使用者可以透過已啟用的協定存取 Amazon S3 或 Amazon EFS 資源 AWS Transfer Family。如果您知道群組名稱，您可以使用 Windows 執行下列命令來檢視 SID 值 PowerShell。

```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties
* | Select SamAccountName,ObjectSid
```

在該命令中，YourGroupName用您的活動目錄組的名稱替換。

用來驗證此參數的規則運算式是由不含空格的大寫和小寫英數字元所組成的字元字串。您也可以包含底線或下列任何字元：=, 。 @：/-

類型：字串

長度限制：長度下限為 1。長度上限為 256。

模式：`S-1-[\d-]+`

必要：否

HomeDirectory

使用者使用其用戶端登入伺服器時的登陸目錄 (資料夾)。

`HomeDirectory` 範例為 `/bucket_name/home/mydirectory`。

> **Note**
>
> 只有在 `HomeDirectoryType` 設為 `PATH` 時才會使用 `HomeDirectory` 參數。

類型：字串

長度限制：長度下限為 0。長度上限為 1024。

模式：(|/.*)

必要：否

HomeDirectoryType

使用者登入伺服器時，您希望的使用者主目錄之登陸目錄 (資料夾) 類型。如果將其設定為PATH，使用者將在其檔案傳輸協定用戶端中看到絕對的 Amazon S3 儲存貯體或 Amazon EFS 路徑。如果將其設定為LOGICAL，則需要在中提供對應，以便讓使用者看到 Amazon S3 或 Amazon EFS 路徑的方式。HomeDirectoryMappings

> **Note**
>
> 如果HomeDirectoryType是LOGICAL，則必須使用HomeDirectoryMappings參數提供對映。另一方面，HomeDirectoryType如果您使用HomeDirectory參數提供絕對路徑。PATH您的範本HomeDirectoryMappings中不HomeDirectory能同時擁有和。

類型：字串

有效值:PATH | LOGICAL

必要：否

Role

(IAM) 角色的亞馬遜資源名稱 AWS Identity and Access Management (ARN)，用於控制使用者對 Amazon S3 儲存貯體或 Amazon EFS 檔案系統的存取。連接到此角色的政策會決定在將檔案傳入和傳出您的 Amazon S3 儲存貯體或 Amazon EFS 檔案系統時，您希望提供給使用者的存取層級。IAM 角色也應包含信任關係，允許伺服器在處理您使用者的傳輸請求時，存取您的資源。

類型：字串

長度限制：長度下限為 20。長度上限為 2048。

模式：arn:.*role/\S+

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

ListedAgreement

描述合約的屬性。

目錄

AgreementId

合約的唯一識別碼。建立協定時會傳回此識別元。

類型：字串

長度約束：固定長度為 19。

模式：`a-([0-9a-f]{17})`

必要：否

Arn

指定協議的 Amazon 資源名稱 (ARN)。

類型：字串

長度限制：長度下限為 20。長度上限為 1600。

模式：`arn:\S+`

必要：否

Description

協定的目前描述。您可以透過呼叫`UpdateAgreement`作業並提供新描述來變更它。

類型：字串

長度限制：長度下限為 1。長度上限為 200。

模式：`[\p{Graph}]+`

必要：否

LocalProfileId

AS2 本機設定檔的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：p-([0-9a-f]{17})

必要：否

PartnerProfileId

合作夥伴設定檔的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：p-([0-9a-f]{17})

必要：否

ServerId

協定的唯一識別元。

類型：字串

長度約束：固定長度為 19。

模式：s-([0-9a-f]{17})

必要：否

Status

協定可以是ACTIVE或INACTIVE。

類型：字串

有效值:ACTIVE | INACTIVE

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

ListedCertificate

說明憑證的特性。

目錄

ActiveDate

選擇性日期，指定憑證變為作用的時間。

類型：Timestamp

必要：否

Arn

指定憑證的 Amazon 資源名稱 (ARN)。

類型：字串

長度限制：長度下限為 20。長度上限為 1600。

模式：`arn:\S+`

必要：否

CertificateId

已匯入憑證的識別碼陣列。您可以使用此識別碼處理設定檔和合作夥伴設定檔。

類型：字串

長度約束：固定長度為 22。

模式：`cert-([0-9a-f]{17})`

必要：否

Description

用來識別憑證的名稱或簡短說明。

類型：字串

長度限制：長度下限為 1。長度上限為 200。

模式：[\p{Graph}]+

必要：否

InactiveDate

選擇性日期，指定憑證變為停用的時間。

類型：Timestamp

必要：否

Status

憑證可以是 ACTIVE、PENDING_ROTATION 或 INACTIVE。PENDING_ROTATION 代表此憑證將在過期時取代目前憑證。

類型：字串

有效值:ACTIVE | PENDING_ROTATION | INACTIVE

必要：否

Type

憑證的類型。如果已為憑證指定私有金鑰，則其類型為 CERTIFICATE_WITH_PRIVATE_KEY。如果沒有私有金鑰，則類型為 CERTIFICATE。

類型：字串

有效值:CERTIFICATE | CERTIFICATE_WITH_PRIVATE_KEY

必要：否

Usage

指定如何使用此憑證。它可以通過以下方式使用：

- SIGNING：用於簽署 AS2 訊息
- ENCRYPTION：用於加密 AS2 訊息
- TLS：用於保護透過 HTTPS 傳送的 AS2 通訊安全

類型：字串

有效值:SIGNING | ENCRYPTION

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

ListedConnector

傳回指定之連接器的詳細資訊。

目錄

Arn

指定連接器的 Amazon 資源名稱 (ARN)。

類型：字串

長度限制：長度下限為 20。長度上限為 1600。

模式：`arn:\S+`

必要：否

ConnectorId

連接器的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：`c-([0-9a-f]{17})`

必要：否

Url

合作夥伴的 AS2 或 SFTP 端點的網址。

類型：字串

長度限制：長度下限為 0。長度上限為 255。

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 的開發
- AWS 適用於紅寶石 V3 的 SDK

ListedExecution

傳回指定之執行的屬性。

目錄

ExecutionId

執行工作流程的唯一識別元。

類型：字串

長度約束：固定長度為 36。

模式：`[0-9a-fA-F]{8}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{12}`

必要：否

InitialFileLocation

描述 Amazon S3 或 EFS 檔案位置的結構。這是執行開始時的檔案位置：如果要複製檔案，這是初始檔案位置 (相對於目的地) 檔案位置。

類型：FileLocation 物件

必要：否

ServiceMetadata

與工作流程相關聯之工作階段詳細資訊的容器物件。

類型：ServiceMetadata 物件

必要：否

Status

狀態是其中一個執行。可以在進行中、已完成、遇到異常或處理異常。

類型：字串

有效值:`IN_PROGRESS | COMPLETED | EXCEPTION | HANDLING_EXCEPTION`

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

ListedHostKey

返回指定的主機密鑰的屬性。

目錄

Arn

主機金鑰的唯一 Amazon 資源名稱 (ARN)。

類型：字串

長度限制：長度下限為 20。長度上限為 1600。

模式：`arn:\S+`

必要：是

DateImported

將主機金鑰新增至伺服器的日期。

類型：Timestamp

必要：否

Description

主機金鑰的目前描述。您可以透過呼叫UpdateHostKey作業並提供新描述來變更它。

類型：字串

長度限制：長度下限為 0。長度上限為 200。

模式：`[\p{Print}]*`

必要：否

Fingerprint

公開金鑰指紋，是用來識別較長公開金鑰的簡短位元組序列。

類型：字串

必要：否

HostKeyId

主機金鑰的唯一識別碼。

類型：字串

長度約束：固定長度為 25。

模式：`hostkey-[0-9a-f]{17}`

必要：否

Type

用於主機金鑰的加密演算法。Type參數是使用下列其中一個值來指定：

- `ssh-rsa`
- `ssh-ed25519`
- `ecdsa-sha2-nistp256`
- `ecdsa-sha2-nistp384`
- `ecdsa-sha2-nistp521`

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

ListedProfile

傳回指定之設定檔的屬性。

目錄

Arn

指定設定檔的 Amazon 資源名稱 (ARN)。

類型：字串

長度限制：長度下限為 20。長度上限為 1600。

模式：`arn:\S+`

必要：否

As2Id

`As2Id` 是 AS2 名稱，如 RFC 4130 中所定義。若為對內傳輸，這是合作夥伴傳送的 AS2 訊息 `AS2-From` 標頭。若為對外連接器，這是使用 `StartFileTransfer` API 操作傳送給合作夥伴的 AS2 訊息 `AS2-To` 標頭。此 ID 不可包含空格。

類型：字串

長度限制：長度下限為 1。長度上限為 128。

模式：`[\p{Print}\s]*`

必要：否

ProfileId

本機或合作夥伴 AS2 設定檔的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：`p-([0-9a-f]{17})`

必要：否

ProfileType

指示是否僅列出 LOCAL 類型設定檔，或僅列出 PARTNER 類型設定檔。如果請求中未提供，命令會將所有類型的設定檔列出。

類型：字串

有效值:LOCAL | PARTNER

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

ListedServer

傳回指定之已啟用檔案傳輸通訊協定之伺服器的屬性。

目錄

Arn

為要列出的伺服器指定唯一的 Amazon 資源名稱 (ARN)。

類型：字串

長度限制：長度下限為 20。長度上限為 1600。

模式：`arn:\S+`

必要：是

Domain

指定用於檔案傳輸的儲存系統網域。有兩個域可用：Amazon Simple Storage Service (Amazon S3) 和 Amazon Elastic File System（Amazon EFS）。預設值為 S3。

類型：字串

有效值:`S3 | EFS`

必要：否

EndpointType

指定伺服器所連線的 VPC 端點類型。如果您的伺服器已連接到 VPC 端點，則無法透過公用網際網路存取您的伺服器。

類型：字串

有效值:`PUBLIC | VPC | VPC_ENDPOINT`

必要：否

IdentityProviderType

伺服器的身分驗證模式。預設值為`SERVICE_MANAGED`，可讓您在 AWS Transfer Family 服務中儲存和存取使用者認證。

用AWS_DIRECTORY_SERVICE於在內部部署環境 AWS Directory Service for Microsoft Active Directory 或 AWS 使用 AD Connector 中，提供存取作用中目錄群組或 Microsoft Active Directory。此選項也要求您使用 IdentityProviderDetails 參數提供 Directory ID。

使用 API_GATEWAY 值來和您選擇的身分提供者整合。API_GATEWAY 設定要求您提供 Amazon API Gateway 端點 URL，以使用 IdentityProviderDetails 參數呼叫驗證。

使用該AWS_LAMBDA值直接使用 AWS Lambda 函數作為您的身份提供者。如果選擇此值，則必須在IdentityProviderDetails資料類型的參數中指定 Lambda 函Function數的 ARN。

類型：字串

有效值:SERVICE_MANAGED | API_GATEWAY | AWS_DIRECTORY_SERVICE | AWS_LAMBDA

必要：否

LoggingRole

(IAM) 角色的 Amazon 資源名稱 AWS Identity and Access Management (ARN)，可讓伺服器為 Amazon Amazon S3 或 Amazon EFSevts 開啟亞馬遜 CloudWatch 日誌記錄。設定後，您可以檢視 CloudWatch 記錄中的使用者活動。

類型：字串

長度限制：長度下限為 20。長度上限為 2048。

模式：arn:.*role/\S+

必要：否

ServerId

為列出的伺服器指定唯一的系統指派識別碼。

類型：字串

長度約束：固定長度為 19。

模式：s-([0-9a-f]{17})

必要：否

State

所描述的伺服器狀況。的值ONLINE表示伺服器可以接受工作和傳輸檔案。State值表OFFLINE示伺服器無法執行檔案傳輸作業。

的狀態STARTING並STOPPING指出伺服器處於中繼狀態，可能無法完全回應，或無法完全離線。START_FAILED或的值STOP_FAILED可以表示錯誤狀況。

類型：字串

有效值:OFFLINE | ONLINE | STARTING | STOPPING | START_FAILED | STOP_FAILED

必要：否

UserCount

指定指派給您使用指定之伺服器的使用者數目ServerId。

類型：整數

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

ListedUser

傳回您指定之使用者的屬性。

目錄

Arn

為您想要了解的使用者提供唯一的 Amazon 資源名稱 (ARN)。

類型：字串

長度限制：長度下限為 20。長度上限為 1600。

模式：`arn:\S+`

必要：是

HomeDirectory

使用者使用其用戶端登入伺服器時的登陸目錄 (資料夾)。

`HomeDirectory` 範例為 `/bucket_name/home/mydirectory`。

> **Note**
> 只有在 `HomeDirectoryType` 設為 `PATH` 時才會使用 `HomeDirectory` 參數。

類型：字串

長度限制：長度下限為 0。長度上限為 1024。

模式：`(|/.*)`

必要：否

HomeDirectoryType

使用者登入伺服器時，您希望的使用者主目錄之登陸目錄 (資料夾) 類型。如果將其設定為`PATH`，使用者將在其檔案傳輸協定用戶端中看到絕對的 Amazon S3 儲存貯體或 Amazon EFS 路徑。如果將其設定為`LOGICAL`，則需要在中提供對應，以便讓使用者看到 Amazon S3 或 Amazon EFS 路徑的方式。`HomeDirectoryMappings`

> **Note**
>
> 如果HomeDirectoryType是LOGICAL，則必須使用HomeDirectoryMappings參數提供對映。另一方面，HomeDirectoryType如果您使用HomeDirectory參數提供絕對路徑。PATH您的範本HomeDirectoryMappings中不HomeDirectory能同時擁有和。

類型：字串

有效值:PATH | LOGICAL

必要：否

Role

(IAM) 角色的亞馬遜資源名稱 AWS Identity and Access Management (ARN)，用於控制使用者對 Amazon S3 儲存貯體或 Amazon EFS 檔案系統的存取。連接到此角色的政策會決定在將檔案傳入和傳出您的 Amazon S3 儲存貯體或 Amazon EFS 檔案系統時，您希望提供給使用者的存取層級。IAM 角色也應包含信任關係，允許伺服器在處理您使用者的傳輸請求時，存取您的資源。

> **Note**
>
> IAM 角色可控制使用者存取 Amazon S3 儲存貯體的伺服器Domain=S3，或控制伺服器的 EFS 檔案系統Domain=EFS。
> 附加到此角色的政策決定了在將檔案傳入和傳出 S3 儲存貯體或 EFS 檔案系統時，您希望為使用者提供的存取層級。

類型：字串

長度限制：長度下限為 20。長度上限為 2048。

模式：arn:.*role/\S+

必要：否

SshPublicKeyCount

指定為您指定的使用者儲存的 SSH 公開金鑰數目。

類型：整數

必要：否

UserName

指定已指定 ARN 的使用者名稱。使用者名稱用於驗證目的。

類型：字串

長度限制：長度下限為 3。長度上限為 100。

模式：`[\w][\w@.-]{2,99}`

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

ListedWorkflow

包含工作流程的識別碼、文字說明和 Amazon 資源名稱 (ARN)。

目錄

Arn

指定工作流程的唯一 Amazon 資源名稱 (ARN)。

類型：字串

長度限制：長度下限為 20。長度上限為 1600。

模式：`arn:\S+`

必要：否

Description

指定工作流程的文字描述。

類型：字串

長度限制：長度下限為 0。長度上限為 256。

模式：`[\w- ]*`

必要：否

WorkflowId

工作流程的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：`w-([a-z0-9]{17})`

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

LoggingConfiguration

由記錄角色和記錄群組名稱組成。

目錄

LoggingRole

(IAM) 角色的 Amazon 資源名稱 AWS Identity and Access Management (ARN)，可讓伺服器為 Amazon Amazon S3 或 Amazon EFSENTS 開啟亞馬遜 CloudWatch 日誌記錄。設定後，您可以檢視 CloudWatch 記錄中的使用者活動。

類型：字串

長度限制：長度下限為 20。長度上限為 2048。

模式：`arn:.*role/\S+`

必要：否

LogGroupName

此工作流程所屬 AWS Transfer Family 伺服器的 CloudWatch 記錄群組名稱。

類型：字串

長度限制：長度下限為 1。長度上限為 512。

模式：`[\.\-_/#A-Za-z0-9]*`

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

PosixProfile

控制使用者存取 Amazon EFS 檔案系統的完整 POSIX 身分，包括使用者 ID (Uid)、群組 ID (Gid) 和任何次要群組 ID (SecondaryGids)。對檔案系統中的檔案和目錄設定的 POSIX 許可，會決定使用者在 Amazon EFS 檔案系統中傳入和傳出檔案時所取得的存取等級。

目錄

Gid

此使用者所使用的所有 EFS 操作的 POSIX 群組 ID。

類型：Long

有效範圍：最小值為 0。最大值為 4294967295。

必要：是

Uid

此使用者所使用的所有 EFS 操作的 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

此使用者所使用的所有 EFS 操作的次要 POSIX 群組 ID。

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

ProtocolDetails

為伺服器設定的通訊協定設定。

目錄

As2Transports

指出 AS2 訊息的傳輸方法。目前僅支援 HTTP。

類型：字串陣列

陣列成員：固定項目數為 1。

有效值:HTTP

必要：否

PassiveIp

指示用於 FTP 和 FTPS 通訊協定的被動模式。輸入單一 IPv4 地址，例如防火牆、路由器或負載平衡器的公有 IP 地址。例如：

```
aws transfer update-server --protocol-details PassiveIp=0.0.0.0
```

將上述範例中的 `0.0.0.0` 取代為您要使用的實際 IP 地址。

> **Note**
>
> 如果變更 `PassiveIp` 值，為了讓變更生效，您必須停止 Transfer Family 伺服器，然後重新啟動該伺服器。如需在 NAT 環境中使用被動模式 (PASV) 的詳細資訊，請參閱在防火牆或 NAT 後方設定 FTPS 伺服器。 AWS Transfer Family

特殊值

`AUTO` 和 `0.0.0.0` 是 `PassiveIp` 參數的特殊值。在預設情況下，值 `PassiveIp=AUTO` 會被指派至 FTP 和 FTPS 類型的伺服器。在此情況下，伺服器會自動在 PASV 回應中回應一個端點 IP。`PassiveIp=0.0.0.0` 對於其使用情況具有更加獨特的應用程式。例如，如果您具有高可用性 (HA) Network Load Balancer (NLB) 環境，且您在該環境中有 3 個子網路，則只能使用 `PassiveIp` 參數指定一個 IP 地址。這會降低高可用性的有效性。在此情況下，您可以指定

PassiveIp=0.0.0.0。這會讓用戶端使用與控制連線相同的 IP 地址，並將所有可用區域用於其連線。但請注意，並非所有 FTP 用戶端都支援PassiveIp=0.0.0.0回應。 FileZilla 和 WinSCP 確實支持它。如果您使用的是其他用戶端，請檢查您的用戶端是否支援 PassiveIp=0.0.0.0 回應。

類型：字串

長度限制：長度下限為 0。長度上限為 15。

必要：否

SetStatOption

使用 SetStatOption 來忽略在用戶端嘗試對您上傳至 S3 儲存貯體的檔案使用 SETSTAT 時所產生的錯誤。

某些 SFTP 檔案傳輸用戶端可以在上傳檔案時，使用 SETSTAT 等命令來嘗試變更遠端檔案的屬性(包括時間戳記和許可)。不過，這些命令與 Amazon S3 等物件儲存系統並不相容。由於這種不相容性，即使已成功上傳檔案，從這些用戶端上傳檔案也可能導致錯誤。

將值設為 ENABLE_NO_OP，讓 Transfer Family 伺服器忽略 SETSTAT 命令，然後在不需要對 SFTP 用戶端進行任何變更的情況下上傳檔案。雖然SetStatOptionENABLE_NO_OP設定會忽略錯誤，但會在 Amazon CloudWatch Logs 中產生日誌項目，因此您可以判斷用戶端何時SETSTAT撥打電話。

> **Note**
>
> 如果要保留檔案的原始時間戳記，並使用 SETSTAT 修改其他檔案屬性，您可以將 Amazon EFS 用作採用 Transfer Family 的後端儲存。

類型：字串

有效值:DEFAULT | ENABLE_NO_OP

必要：否

TlsSessionResumptionMode

與使用 FTPS 通訊協定的 Transfer Family 伺服器搭配使用的屬性。TLS 工作階段恢復提供了一種機制，可在 FTPS 工作階段的控制和資料連線之間恢復或共用交涉的私密金鑰。TlsSessionResumptionMode 決定伺服器是否透過唯一的工作階段 ID 恢復最近交涉的工作

階段。此屬性可在 CreateServer 和 UpdateServer 呼叫期間使用。如果未在 CreateServer 期間指定 TlsSessionResumptionMode 值，則預設會設定為 ENFORCED。

- DISABLED：伺服器不會處理 TLS 工作階段恢復用戶端請求，但會為每個請求建立新的 TLS 工作階段。
- ENABLED：伺服器處理並接受正在執行 TLS 工作階段恢復的用戶端。伺服器不會拒絕未執行 TLS 工作階段恢復用戶端處理的用戶端資料連線。
- ENFORCED：伺服器處理並接受正在執行 TLS 工作階段恢復的用戶端。伺服器拒絕未執行 TLS 工作階段恢復用戶端處理的用戶端資料連線。先測試用戶端，再將值設定為 ENFORCED。

> **Note**
>
> 並非所有 FTPS 用戶端都會執行 TLS 工作階段恢復。因此，如果選擇強制執行 TLS 工作階段恢復，您可以防止任何來自不執行通訊協定交涉之 FTPS 用戶端的連線。為了判斷是否可以使用 ENFORCED 值，您需要測試用戶端。

類型：字串

有效值:DISABLED | ENABLED | ENFORCED

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

S3FileLocation

為工作流程中使用的檔案指定檔案位置的詳細資料。僅適用於使用 S3 儲存。

目錄

Bucket

指定包含正在使用之檔案的 S3 儲存貯體。

類型：字串

長度限制：長度下限為 3。長度上限為 63。

模式：`[a-z0-9][\.\-a-z0-9]{1,61}[a-z0-9]`

必要：否

Etag

實體標籤是物件的雜湊值。ETag 只會反映物件內容的變更，而非其中繼資料的變更。

類型：字串

長度限制：長度下限為 1。最大長度為 65536。

模式：`.+`

必要：否

Key

在 Amazon S3 中建立檔案時指派給該檔案的名稱。您可以使用物件金鑰來擷取該物件。

類型：字串

長度限制：長度下限為 0。長度上限為 1024。

模式：`[\P{M}\p{M}]*`

必要：否

VersionId

指定檔案版本。

類型：字串

長度限制：長度下限為 1。長度上限為 1024。

模式：`.+`

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

S3InputFileLocation

指定客戶輸入的 Amazon S3 檔案位置。如果在內部使用`copyStepDetails.DestinationFileLocation`，它應該是 S3 複製目標。

您需要提供存儲桶和密鑰。該鍵可以代表路徑或文件。這取決於您是否以正斜線 (/) 字元結束索引鍵值。如果最後一個字符是「/」，則您的文件將被複製到文件夾中，其名稱不會更改。如果最後一個字元是英數字元，則您上傳的檔案會重新命名為路徑值。在這種情況下，如果具有該名稱的文件已經存在，則該文件將被覆蓋。

例如，如果您的路徑是`shared-files/bob/`，則您上傳的檔案會複製到`shared-files/bob/`、資料夾。如果您的路徑是`shared-files/today`，則每個上傳的文件都會複製到文件`shared-files`夾並命名`today`：每次上傳都會覆蓋以前的 bob 文件版本。

目錄

Bucket

指定客戶輸入檔案的 S3 儲存貯體。

類型：字串

長度限制：長度下限為 3。長度上限為 63。

模式：`[a-z0-9][\.\-a-z0-9]{1,61}[a-z0-9]`

必要：否

Key

在 Amazon S3 中建立檔案時指派給該檔案的名稱。您可以使用物件金鑰來擷取該物件。

類型：字串

長度限制：長度下限為 0。長度上限為 1024。

模式：`[\P{M}\p{M}]*`

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

S3StorageOptions

為您的伺服器設定的 Amazon S3 儲存選項。

目錄

DirectoryListingOptimization

指定您的 Amazon S3 目錄的效能是否已最佳化。此選項根據預設為停用。

依預設，主目錄對應具有TYPE的DIRECTORY. 如果啟用此選項，如FILE果您希望對應具有檔案目標，則需要明確地將設定為。HomeDirectoryMapEntry Type

類型：字串

有效值:ENABLED | DISABLED

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 的開發
- AWS 適用於紅寶石 V3 的 SDK

S3Tag

指定在執行「加標籤」步驟期間指定給檔案的鍵值對。

目錄

Key

指派給您建立之標籤的名稱。

類型：字串

長度限制：長度下限為 1。長度上限為 128。

模式：`([\p{L}\p{Z}\p{N}_.:/=+\-@]*)`

必要：是

Value

對應於索引鍵的值。

類型：字串

長度限制：長度下限為 0。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

ServiceMetadata

與工作流程相關聯之工作階段詳細資訊的容器物件。

目錄

UserDetails

服務器 ID（`ServerId`），會話 ID（`SessionId`）和用戶（`UserName`）組成`UserDetails`。

類型：UserDetails 物件

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 的开发
- AWS 適用於紅寶石 V3 的 SDK

SftpConnectorConfig

包含 SFTP 連接器物件的詳細資訊。連接器物件用於在夥伴的 SFTP 伺服器之間傳輸檔案。

> **Note**
>
> 由於資SftpConnectorConfig料類型同時用於建立和更新 SFTP 連接器，因此其參數UserSecretId會標示為不需要。TrustedHostKeys這有點誤導，因為當您更新現有的 SFTP 連接器時不需要這些連接器，但是在建立新的 SFTP 連接器時需要這樣做。

目錄

TrustedHostKeys

主機金鑰的公用部分 (或稱為金鑰)，用來識別您要連線的外部伺服器。您可以對 SFTP 伺服器使用ssh-keyscan指令來擷取必要的金鑰。

三個標準的 SSH 公開金鑰格式元素是<key type><body base64>、和選用的<comment>，每個元素之間都有空格。僅指定<key type>和<body base64>：請勿輸入金鑰的<comment>部分。

對於受信任的主機金鑰，請 AWS Transfer Family 接受 RSA 和 ECDSA 金鑰。

- 對於 RSA 金鑰，字<key type>串為ssh-rsa。
- 對於 ECDSA 金鑰，字<key type>串是ecdsa-sha2-nistp256、或 ecdsa-sha2-nistp384ecdsa-sha2-nistp521，視您產生的金鑰大小而定。

執行此指令以擷取 SFTP 伺服器主機金鑰 (其中您的 SFTP 伺服器名稱所在)。ftp.host.com

```
ssh-keyscan ftp.host.com
```

這會將公共主機密鑰打印到標準輸出。

```
ftp.host.com ssh-rsa AAAAB3Nza...<long-string-for-public-key
```

將此字串複製並貼到create-connector指令的TrustedHostKeys欄位或主控台的 [受信任的主機金鑰] 欄位中。

類型：字串陣列

陣列成員：項目數下限為 1。項目數上限為 10。

長度限制：長度下限為 1。長度上限為 2048。

必要：否

UserSecretId

密碼的識別碼 (在 AWS Secrets Manager 中)，其中包含 SFTP 使用者的私密金鑰、密碼或兩者。識別碼必須是秘密的 Amazon 資源名稱 (ARN)。

類型：字串

長度限制：長度下限為 1。長度上限為 2048。

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

SshPublicKey

針對特定已啟用檔案傳輸通訊協定的伺服器 (如所ServerId識別)，提供與 Transfer Family 使用者相關聯的公用安全殼層 (SSH) 金鑰的相關資訊。傳回的資訊包含金鑰匯入的日期、公有金鑰的內容和公有金鑰 ID。使用者可以存放多個與其特定伺服器使用者名稱相關聯的 SSH 公有金鑰。

目錄

DateImported

指定將公開金鑰加入至「Transfer Family」使用者的日期。

類型：Timestamp

必要：是

SshPublicKeyBody

指定由 PublicKeyId 指定的 SSH 公有金鑰內容。

AWS Transfer Family 接受 RSA、ECDSA 和 ED25519 金鑰。

類型：字串

長度限制：長度下限為 0。長度上限為 2048。

必要：是

SshPublicKeyId

指定包含公開金鑰識別碼的SshPublicKeyId參數。

類型：字串

長度限制：固定長度為 21。

模式：key-[0-9a-f]{17}

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

Tag

為特定資源建立索引鍵值配對。標籤是中繼資料，您可以用來搜尋和分組資源以用於各種目的。您可以將標記套用至伺服器、使用者和角色。標籤鍵可以使用多個值。例如，若要基於會計目的將伺服器分組，您可以建立名為的標記，Group然後將值Research指派Accounting給該群組。

目錄

Key

指派給您建立之標籤的名稱。

類型：字串

長度限制：長度下限為 0。長度上限為 128。

必要：是

Value

包含您指定給您建立的金鑰名稱的一或多個值。

類型：字串

長度限制：長度下限為 0。長度上限為 256。

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 的开发
- AWS 適用於紅寶石 V3 的 SDK

TagStepDetails

每個步驟類型都有自己的StepDetails結構。

在執行工作流程步驟期間，用來標記檔案的索引鍵/值配對。

目錄

Name

作為識別碼使用的步驟名稱。

類型：字串

長度限制：長度下限為 0。最大長度為 30。

模式：[\w-]*

必要：否

SourceFileLocation

指定要用作工作流程步驟輸入的檔案：上一個步驟的輸出，或工作流程的原始上載檔案。

- 若要使用上一個檔案做為輸入，請輸入${previous.file}。在此情況下，此工作流程步驟會使用上一個工作流程步驟的輸出檔案作為輸入。這是預設值。
- 若要使用原始上載的檔案位置做為此步驟的輸入，請輸入${original.file}。

類型：字串

長度限制：長度下限為 0。長度上限為 256。

模式：\$\{(\w+.)+\w+\}

必要：否

Tags

包含 1 到 10 個鍵/值對的數組。

類型：S3Tag 物件陣列

陣列成員：項目數下限為 1。項目數上限為 10。

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

UserDetails

指定工作流程的使用者名稱、伺服器 ID 和工作階段 ID。

目錄

ServerId

系統指派給「傳送」伺服器執行個體的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：`s-([0-9a-f]{17})`

必要：是

UserName

識別與伺服器相關聯之 Transfer Family 使用者的唯一字串。

類型：字串

長度限制：長度下限為 3。長度上限為 100。

模式：`[\w][\w@.-]{2,99}`

必要：是

SessionId

系統為工作流程對應之工作階段指派的唯一識別元。

類型：字串

長度限制：長度下限為 3。長度上限為 32。

模式：`[\w-]*`

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

WorkflowDetail

指定要指派之工作流程的工作流程 ID，以及用於執行工作流程的執行角色。

除了完全上傳檔案時要執行的工作流程外，`WorkflowDetails` 亦可包含要在部分上傳時執行之工作流程的工作流程 ID (和執行角色)。當伺服器工作階段中斷連線，而檔案仍在上載時，就會發生部分上傳。

目錄

ExecutionRole

包含 Transfer 可以承繼的 S3、EFS 和 Lambda 操作的必要許可，以便所有工作流程步驟都可以在必要的資源上操作

類型：字串

長度限制：長度下限為 20。長度上限為 2048。

模式：`arn:.*role/\S+`

必要：是

WorkflowId

工作流程的唯一識別碼。

類型：字串

長度約束：固定長度為 19。

模式：`w-([a-z0-9]{17})`

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

WorkflowDetails

`WorkflowDetail` 資料類型的容器。它由觸發工作流程開始執行的動作所使用。

目錄

OnPartialUpload

啟動工作流程的觸發條件 (如果檔案只會部分上傳)。您可以將工作流程連接到只要有部分上傳就會執行的伺服器。

在工作階段中斷時開啟檔案，將會發生部分上傳的情況。

> **Note**
>
> `OnPartialUpload`最多可包含一個`WorkflowDetail`物件。

類型：WorkflowDetail 物件陣列

陣列成員：項目數下限為 0。項目數上限為 1。

必要：否

OnUpload

啟動工作流程的觸發條件：工作流程會在上傳檔案後開始執行。

若要從伺服器中移除相關聯的工作流程，您可以提供空白 `OnUpload` 物件 (如以下範例所示)。

```
aws transfer update-server --server-id s-01234567890abcdef --workflow-
details '{"OnUpload":[]}'
```

> **Note**
>
> `OnUpload`最多可包含一個`WorkflowDetail`物件。

類型：WorkflowDetail 物件陣列

陣列成員：項目數下限為 0。項目數上限為 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 適用於 Java V2 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

WorkflowStep

工作流程的基本建置區塊。

目錄

CopyStepDetails

執行檔案複製步驟的詳細資訊。

包含下列值：

- 一項描述
- 檔案複製目的地的 Amazon S3 位置。
- 指示是否覆寫現有相同名稱檔案的標記。預設值為 FALSE。

類型：CopyStepDetails 物件

必要：否

CustomStepDetails

呼叫 AWS Lambda 函數之步驟的詳細資訊。

包含 Lambda 函數的名稱、目標和逾時 (以秒為單位)。

類型：CustomStepDetails 物件

必要：否

DecryptStepDetails

解密加密檔案之步驟的詳細資料。

包含下列值：

- 描述性名稱
- 要解密的來源檔案的 Amazon S3 或亞馬遜彈性檔案系統 (Amazon EFS) 位置。
- 用於檔案解密目的地的 S3 或 Amazon EFS 位置。
- 指示是否覆寫現有相同名稱檔案的標記。預設值為 FALSE。
- 所使用的加密類型。目前僅支援 PGP 加密。

類型：DecryptStepDetails 物件

必要：否

DeleteStepDetails

刪除檔案的步驟詳細資訊。

類型：DeleteStepDetails 物件

必要：否

TagStepDetails

建立一或多個標籤的步驟詳細資訊。

您指定一或多個標籤。各標籤皆包含鍵值對。

類型：TagStepDetails 物件

必要：否

Type

目前不支援以下步驟類型。

- **COPY** - 將檔案複製到另一個位置。
- **CUSTOM**-使用 AWS Lambda 函數目標執行自訂步驟。
- **DECRYPT** - 解密上傳前已加密的檔案。
- **DELETE** - 刪除檔案。
- **TAG** - 在檔案中新增標籤。

類型：字串

有效值:COPY | CUSTOM | TAG | DELETE | DECRYPT

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

提出 API 要求

除了使用主控台之外，您還可以使用 AWS Transfer Family API 以程式設計方式設定和管理伺服器。本節說明 AWS Transfer Family 操作、身分驗證的請求簽章，以及錯誤處理。如需有關可用於 Transfer Family 的區域和AWS Transfer Family端點的資訊，請參閱 AWS 一般參考

> **Note**
>
> 使用 Transfer Family 開發應用程序時，您也可以使用 AWS SDK;。適用於 Java，.NET 和 PHP 的AWS開發套件包裝了基礎的 Transfer Family API，從而簡化了您的編程任務。如需下載 SDK 程式庫的詳細資訊，請參閱範例程式碼程式庫。

主題

- Transfer Family 必要的要求標頭
- Transfer Family 請求輸入和簽名
- 錯誤回應
- 可用程式庫

Transfer Family 必要的要求標頭

本節說明必須與每個 POST 要求一起傳送的必要標頭AWS Transfer Family。您會透過包含 HTTP 標頭，來識別關於請求的關鍵資訊，包含您希望呼叫的操作、請求的日期，以及表示授權您做為請求寄件者的資訊。標頭不區分大小寫，並且標頭的順序也不重要。

下列範例顯示ListServers作業中使用的標頭。

```
POST / HTTP/1.1
Host: transfer.us-east-1.amazonaws.com
x-amz-target: TransferService.ListServers
x-amz-date: 20220507T012034Z
```

```
Authorization: AWS4-HMAC-SHA256 Credential=AKIDEXAMPLE/20220507/us-east-1/transfer/
aws4_request,
    SignedHeaders=content-type;host;x-amz-date;x-amz-target,
    Signature=13550350a8681c84c861aac2e5b440161c2b33a3e4f302ac680ca5b686de48de
Content-Type: application/x-amz-json-1.1
Content-Length: 17

{"MaxResults":10}
```

以下是 Transfer Family 的 POST 請求中必須包含的標題。以下顯示以「x-amz」開頭的標題是特定的。AWS所有其他列出的標頭都是 HTTP 交易中使用的常見標頭。

標頭	描述
`Authorization`	授權標頭是必需的。該格式是標準的 Sigv4 請求簽名，其記錄在簽署 AWS API 請求中。
`Content-Type`	用`application/x-amz-json-1.1` 作 Transfer Family 的所有請求的內容類型。 `Content-Type: application/x-amz-json-1.1`
`Host`	使用主機標頭指定傳送請求的轉移系列端點。例如，`transfer.us-east-1.amazonaws.com` 是美國東部 (俄亥俄) 區域的端點。如需有關可用於 Transfer Family 之AWS Transfer Family端點的詳細資訊，請參閱 AWS 一般參考. `Host: transfer.` *`region`*`.amazonaws.com`
`x-amz-date`	您必須在 HTTP `Date` 標頭或標頭中提供時間戳記。AWS `x-amz-date` (有些 HTTP 用戶端程式庫不讓您設定 `Date` 標頭。) 當`x-amz-date` 標頭存在時，Transfer Family 會在要求驗證期間忽略任何`Date`標頭。`x-amz-date` 格式必須是 ISO8601，格式為年月月日「海里曼斯」Z。 `x-amz-date:` *`YYYYMMDD'T'HHMMSS'Z'`*

標頭	描述
x-amz-target	此標頭會指定 API 的版本，以及您請求的操作。目標標頭值是透過串連 API 版本及 API 名稱構成，且其格式如下。 `x-amz-target: TransferService.  operationName` 您可以從 API 清單中找到 operationName 值 (例如ListServers)。ListServers
x-amz-security-token	當用於簽署請求的登入資料為臨時登入資料或工作階段登入資料時，需要此標頭 (如需詳細資訊，請參閱《IAM 使用者指南》中的 < 使用臨時登入AWS資料 Amazon Web Services 一般參考如需詳細資訊，請參閱中的將簽章新增至 HTTP 要求。

Transfer Family 請求輸入和簽名

所有請求輸入都必須作為請求正文中 JSON 有效負載的一部分發送。例如，對於所有請求字段都是可選的操作ListServers，您仍然需要在請求主體中提供一個空的 JSON 對象，例如{}。例如，Transfer Family 有效負載請求/響應的結構記錄在現有的 API 參考中。DescribeServer

Transfer Family 支援使用AWS簽名版本 4 進行驗證。如需詳細資訊，請參閱簽署 AWS API 要求。

錯誤回應

當發生錯誤時，回應標頭資訊會包含：

- 內容類型：application/x-amz-json-1.1
- 適當的 4xx 或 5xx HTTP 狀態代碼

錯誤回應的內文會包含發生錯誤的資訊。以下範例錯誤回應會顯示所有錯誤回應常見的回應元素輸出語法。

```
{
    "__type": "String",
    "Message": "String", <!-- Message is lowercase in some instances -->
```

```
    "Resource": String,
    "ResourceType": String
    "RetryAfterSeconds": String
}
```

下表說明在上述語法中顯示的 JSON 錯誤回應欄位。

__type

Transfer Family API 呼叫的其中一個例外狀況。

類型：字串

訊息或訊息

的其中一項操作錯誤代碼訊息。

> **Note**
>
> 有些例外使用message，而其他例外則使用Message。您可以檢查界面的代碼以確定正確的大小寫。或者，您可以測試每個選項以查看哪些有效。

類型：字串

Resource

呼叫錯誤的資源。例如，如果您嘗試建立已存在的使用者，Resource就是現有使用者的使用者名稱。

類型：字串

ResourceType

呼叫錯誤的資源類型。例如，如果您嘗試建立一個已存在的使用者，則ResourceType為User.

類型：字串

RetryAfterSeconds

重試指令之前等待的秒數。

類型：字串

錯誤回應範例

如果您呼叫 DescribeServer API 並指定不存在的伺服器，則會傳回下列 JSON 主體。

```
{
  "__type": "ResourceNotFoundException",
  "Message": "Unknown server",
  "Resource": "s-11112222333344444",
  "ResourceType": "Server"
}
```

如果執行 API 導致節流發生，則返回以下 JSON 主體。

```
{
   "__type":"ThrottlingException",
   "RetryAfterSeconds":"1"
}
```

如果您使用 CreateServer API，且您沒有足夠的權限來建立轉移系列伺服器，則會傳回下列 JSON 主體。

```
{
  "__type": "AccessDeniedException",
  "Message": "You do not have sufficient access to perform this action."
}
```

如果您使用 CreateUser API 並指定已存在的使用者，則會傳回下列 JSON 主體。

```
{
  "__type": "ResourceExistsException",
  "Message": "User already exists",
  "Resource": "Alejandro-Rosalez",
  "ResourceType": "User"
}
```

可用程式庫

AWS提供程式庫、範例程式碼、教學課程和其他資源，讓他們偏好使用特定語言的 API 來建置應用程式，而不是命令列工具和 Query API 來建置應用程式。這些庫提供基本功能（不包括在 API 中），例如請求身份驗證，請求重試和錯誤處理，以便更容易上手。請參閱建置基礎的工具 AWS

如需所有語言的程式庫和範例程式碼，請參閱範例程式碼與程式庫。

常見參數

以下清單內含所有動作用來簽署 Signature 第 4 版請求的參數以及查詢字串。任何專屬於特定動作的參數則列於該動作的主題中。如需有關 Signature 第 4 版的詳細資訊，請參閱《IAM 使用者指南》中的簽署 AWS API 請求。

Action

要執行的動作。

類型：字串

必要：是

Version

編寫請求所憑藉的 API 版本，以 YYYY-MM-DD 格式表示。

類型：字串

必要：是

X-Amz-Algorithm

建立請求簽章時所使用的雜湊演算法。

條件：當您在查詢字串中而非 HTTP 授權標頭中納入驗證資訊時，應指定此參數。

類型：字串

有效值: AWS4-HMAC-SHA256

必要：有條件

X-Amz-Credential

憑證範圍值，此為一個字串，其中包含您的存取金鑰、日期、您的目標區域、您請求的服務，以及終止字串 (“aws4_request”)。值以下列格式表示：access_key/YYYYMMDD/region/service/aws4_request。

如需詳細資訊，請參閱《IAM 使用者指南》中的建立已簽署的 AWS API 請求。

條件：當您在查詢字串中而非 HTTP 授權標頭中納入驗證資訊時，應指定此參數。

類型：字串

必要：有條件

X-Amz-Date

用來建立簽署的日期。格式必須是 ISO 8601 基本格式 (YYYYMMDD'T'HHMMSS'Z')。例如，以下日期時間是有效的 X-Amz-Date 值：`20120325T120000Z`

條件： 對所有請求而言，X-Amz-Date 皆為選用，可用來覆寫用於簽署請求的日期。如果規定日期標頭採用 ISO 8601 基本格式，則不需要 X-Amz-Date。當使用 X-Amz-Date 時，其一律會覆寫日期標頭的值。如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS API 請求簽章的元素。

類型：字串

必要：有條件

X-Amz-Security-Token

透過呼叫 AWS Security Token Service (AWS STS) 所取得的臨時安全字符。如需支援 AWS STS 的臨時安全憑證的服務清單，請參閱《IAM 使用者指南》中的可搭配 IAM 運作的 AWS 服務。

條件：如果您使用 AWS STS 的臨時安全憑證，則必須納入安全字符。

類型：字串

必要：有條件

X-Amz-Signature

指定從要簽署的字串和衍生的簽署金鑰中計算出的十六進位編碼簽章。

條件：當您在查詢字串中而非 HTTP 授權標頭中納入驗證資訊時，應指定此參數。

類型：字串

必要：有條件

X-Amz-SignedHeaders

指定納入作為標準請求一部分的所有 HTTP 標頭。如需有關指定已簽署的標頭之詳細資訊，請參閱《IAM 使用者指南》中的建立已簽署的 AWS API 請求。

條件：當您在查詢字串中而非 HTTP 授權標頭中納入驗證資訊時，應指定此參數。

類型：字串

必要：有條件

常見錯誤

本部分列出所有 AWS 服務 API 動作的常見錯誤。如需此服務之 API 動作的特定錯誤，請參閱該 API 動作的主題。

AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：400

IncompleteSignature

請求簽署不符合 AWS 標準。

HTTP 狀態碼：400

InternalFailure

由於不明的錯誤、例外狀況或故障，處理請求失敗。

HTTP 狀態碼：500

InvalidAction

請求的動作或操作無效。確認已正確輸入動作。

HTTP 狀態碼：400

InvalidClientTokenId

提供的 X.509 憑證或 AWS 存取金鑰 ID 不存在於我們的記錄中。

HTTP 狀態碼：403

NotAuthorized

您沒有執行此動作的許可。

HTTP 狀態碼：400

OptInRequired

AWS 存取金鑰 ID 需要訂閱服務。

HTTP 狀態碼：403

RequestExpired

請求送達服務已超過戳印日期於請求上之後的 15 分鐘，或者已超過請求過期日期之後的 15 分鐘 (例如預先簽章的 URL)，或者請求上的日期戳印在未來將超過 15 分鐘。

HTTP 狀態碼：400

ServiceUnavailable

由於伺服器暫時故障，請求失敗。

HTTP 狀態碼：503

ThrottlingException

由於請求調節，因此請求遭到拒絕。

HTTP 狀態碼：400

ValidationError

輸入不符合 AWS 服務規定的限制。

HTTP 狀態碼：400

的文件歷史記錄 AWS Transfer Family

下表說明此版本的文件 AWS Transfer Family。

- API 版本：transfer-2018-11-05
- 最新文件更新：2024 年 4 月 23 日

變更	描述	日期
可讓 SFTP 連接器列出遠端檔案和目錄	Transfer Family 列增加了我們的客戶使用 SFTP 連接器列出存儲在遠程 SFTP 服務器中的文件的功能。如需詳細資訊，請參閱列出遠程目錄的內容	2024年4月23 日
能夠將交易夥伴的自我簽署 TLS 憑證與 AS2 訊息交換搭配使用	AWS Transfer Family 已新增匯入及使用交易夥伴的公開自簽署 TLS 憑證的選項，以透過 HTTPS 傳送適用性聲明 2 (AS2) 訊息至其伺服器。	2024年4月12日
新增 SFTP 連接器的安全性原則	AWS Transfer Family 已新增與 SFTP 連接器搭配使用的安全性原則。如需詳細資訊，請參閱 AWS Transfer Family SFTP 連接器的安全性原則。	2024年4月5 日
與 Amazon 集成 EventBridge	AWS Transfer Family 現在會 EventBridge 針對所有檔案傳輸操作，自動將事件發佈到 Amazon。如需詳細資訊，請參閱 使用管理 Transfer Family 事件 Amazon EventBridge。	2024年2月8日
增加新的安全政策	AWS Transfer Family 已新增 FIPS 和非 FIPS 安全性原則。此外，指派給伺服器的預設安	2024年2月5 日

變更	描述	日期
	全性原則永遠是最新的安全性原則。如需詳細資訊，請參閱 AWS Transfer Family 伺服器的安全性原則。	
Support SFTP 連接器和 AS2 的靜態 IP 位址	Transfer Family 現在可為 SFTP 連接器和 AS2 提供靜態 IP 位址。這會啟用與受 IP 允許清單控制項保護的遠端 SFTP 伺服器的連線。對於 AS2，我們為來自 AS2 伺服器的非同步 MDN 回應引入靜態 IP 位址。	2024年1月16日
使用者指南已重新整理，以便更緊密地與最新版本的 AWS Transfer Family一致。	自指南產生以來，「Transfer Family」已加入多個功能，因此需要重新架構指南。	2024 年 1 月 3 日
邏輯目錄對應的增強 Amazon S3 列表性能優化	Transfer Family 現在支援高達 2.1 MB 的邏輯目錄對應。您現在也可以宣告使用者對應是否為檔案。如需詳細資訊，請參閱 使用邏輯目錄的規則。 建立或更新使用 Amazon S3 進行儲存的伺服器時，您現在可以優化列出 S3 目錄 (或資料夾) 的效能。如需詳細資訊，請參閱 設定 SFTP、FTPS 或 FTP 伺服器端點。	2023 年 11 月 17 日
具有虛擬私有雲端 (VPC) 端點之 SFTP 伺服器的替代連接埠	您現在可以為具有 VPC 端點的 SFTP Transfer Family 伺服器啟用替代的非標準連接埠。如需詳細資訊，請參閱 在虛擬私有雲中建立伺服器。	2023 年 11 月 17 日

變更	描述	日期
Support SFTP 連接器	SFTP 連接器可擴充與雲端和內部部署中遠端伺服器通訊的 AWS Transfer Family 功能。如需詳細資訊，請參閱 使用 SFTP 連接器傳送和擷取檔案。	2023 年 7 月 25 日
Support AS2 基本驗證	Transfer Family 現在支援使用適用性聲明 2 (AS2) 通訊協定的伺服器使用基本驗證。如需詳細資訊，請參閱 AS2 連接器的基本驗證。	2023 年 6 月 30 日
Support 結構化 JSON 記錄	Transfer Family 現在支援將結構化 JSON 日誌提供給 Amazon CloudWatch、將日誌信號分組到自訂日誌群組中，以及跨協定執行常見的日誌查詢。如需詳細資訊，請參閱 Amazon CloudWatch 日誌記錄 AWS Transfer Family。	2023年6月24日
Support 多種驗證方法	Transfer Family 支援使用密碼、公開/私密 key pair 或兩者進行驗證。這適用於使用 SFTP 通訊協定和自訂身分識別提供者的伺服器。如需詳細資訊，請參閱 建立啟用 SFTP 的伺服器。	2023 年 5 月 17 日

變更	描述	日期
Support 相當好的隱私（PGP）解密與文件 Transfer Family 進程與工作流	Transfer Family 內置了對相當不錯的隱私（PGP）解密的支持。您可以對透過 SFTP、FTPS 或 FTP 上傳至亞馬遜簡單儲存服務 (Amazon S3) 或亞馬遜彈性檔案系統 (Amazon EFS) 的檔案使用 PGP 解密。如需詳細資訊，請參閱 產生和管理 PGP 金鑰 及 在工作流程中使用 PGP 解密。	2022 年 12 月 21 日
具有傳輸 Transfer Family 伺服器的適用性聲明 2 (AS2) 檔案傳輸通訊協定的全受管支援	您可以建立使用 AS2 通訊協定的伺服器，向 AWS 環境內外的交易夥伴傳送和接收資訊。如需詳細資訊，請參閱 配置 AS2。	2022 年 7 月 25 日
Support 創建服務器時顯示橫幅	您可以在建立伺服器時新增自訂訊息。您可以顯示預先驗證訊息 (所有通訊協定)，以及驗證後訊息 (適用於 FTP 和 FTPS 伺服器)。如需詳細資訊，請參閱「建立啟用 SFTP 的伺服器」、「建立啟用 FTP 的伺服器」或「建立啟用 FTP 的伺服器」。	2022 年 2 月 17 日
身分識別提供者的 AWS Lambda Support	您現在可以使 AWS Lambda 用其 Transfer Family 伺服器連線到自訂身分識別提供者。之前，您必須提供 Amazon API Gateway URL 來整合自訂身分識別提供者。如需詳細資訊，請參閱 用 AWS Lambda 於整合您的身分識別提供者。	2021 年 11 月 16 日

變更	描述	日期
Support 受管理檔案傳輸工作流程	受管理的檔案傳輸工作流程為您目前手動執行的一般工作提供上傳後處理摘要。如需詳細資訊，請參閱 AWS Transfer Family 管理工作流。	2021 年 9 月 2 日
Support AWS Directory Service for Microsoft Active Directory	除了服務受管理和自訂身分識別提供者之外，您現在還可以使用 AWS Directory Service for Microsoft Active Directory 來管理驗證和授權的使用者存取權限。如需詳細資訊，請參閱 使用 AWS Directory Service 身分識別提供者。	2021 年 5 月 24 日
新 AWS 區域	AWS Transfer Family 現已在非洲 (開普敦) 地區推出。如需有關 Transfer Family 端點的詳細資訊，請AWS Transfer Family 參閱 AWS 一般參考.	2021 年 2 月 24 日
新 AWS 區域	AWS Transfer Family 現已於亞太區域 (香港) 及中東 (巴林) 區域推出。如需有關 Transfer Family 端點的詳細資訊，請 AWS Transfer Family 參閱 AWS 一般參考.	2021 年 2 月 17 日

變更	描述	日期
以資料存放區的形式 Support Amazon EFS	Transfer Family 現在支援傳入和傳出 Amazon Elastic File System (Amazon EFS) 的檔案。Amazon EFS 是一個簡單、可擴展、全受管的彈性 NFS 檔案系統。如需詳細資訊，請參閱 設定 Amazon EFS 檔案系統。	2021年1月06 日
Support AWS WAF	Transfer Family 現在支援 AWS WAF這種 Web 應用程式防火牆，可協助保護 Web 應用程式和 API 作業免受攻擊。如需詳細資訊，請參閱 新增 Web 應用程式防火牆。	2020 年 11 月 24 日
Support 虛擬私有雲 (VPC) 中的多個安全群組	您現在可以將多個安全群組連接到 VPC 中的伺服器。如需詳細資訊，請參閱 在虛擬私有雲中建立伺服器。	2020 年 10 月 15 日
新 AWS 區域	Transfer Family 現在可在 AWS GovCloud (US) 區域中使用。如需有關移轉 AWS GovCloud (US) 區域的系列端AWS Transfer Family 點的詳細資訊，請參閱 AWS 一般參考. 若要取得有關在 AWS GovCloud (US) 區域中使用 Transfer Family 的資訊，請參閱《使AWS GovCloud (US) 用指南》AWS Transfer Family中的〈〉	2020 年 9 月 30 日

變更	描述	日期
支援加密演算法的安全性原則現在可以附加至您的伺服器	您現在可以將包含一組受支援的密碼編譯演算法的安全性原則附加至伺服器。如需詳細資訊，請參閱 AWS Transfer Family 伺服器的安全性原則。	2020 年 8 月 12 日
支援聯邦資訊處理標準 (FIPS) 端點	已啟用 FIPS 的端點現已在北美地區推出。 AWS 區域如需可用區AWS Transfer Family域，請參閱 AWS 一般參考. 若要為已啟用 SFTP 的伺服器端點啟用 FIPS，請參閱。建立啟用 SFTP 的伺服器若要為已啟用 FTP 的伺服器端點啟用 FIPS，請參閱。建立啟用 FTP 的伺服器若要為已啟用 FTP 的伺服器端點啟用 FIPS，請參閱。建立啟用 FTP 的伺服器	2020 年 8 月 12 日
用戶名字符長度增加和其他允許的字符	使用者名稱現在可以包含 at 符號 (@) 和句號 (.)，而且長度上限為 100 個字元。若要新增使用者，請參閱管理伺服器端點的使用者。	2020 年 8 月 12 日
Support 自動 Amazon CloudWatch 日誌記錄 AWS Identity and Access Management (IAM) 角色建立	Transfer Family 現在支援自動建立 CloudWatch 記錄 IAM 角色，以檢視使用者活動。如需詳細資訊，請參閱「建立啟用 SFTP 的伺服器」、「建立啟用 FTP 的伺服器」或「建立啟用 FTP 的伺服器」。	2020 年 7 月 30 日

變更	描述	日期
AWS Transfer Family 現在支援來源 IP 作為授權的因素。	Transfer Family 增加了對使用者來源 IP 位址作為授權因素的支援，讓您在授權透過安全檔案傳輸通訊協定 (SFTP)、SSL 上的檔案傳輸通訊協定 (FTPS) 或檔案傳輸通訊協定 (FTP) 進行存取時，可以額外套用一層安全性。如需詳細資訊，請參閱 使用自訂身分識別提供者。	2020 年 6 月 9 日
AWS SFTP 的傳輸現在已經開始， AWS Transfer Family 並增加了對 FTP 和 FTPS 的支援。	您現在可以使用兩個額外的通訊協定進行使用者的檔案傳輸：檔案傳輸通訊協定安全 (FTPS) 和檔案傳輸通訊協定 (FTP)。除了現有的安全檔案傳輸通訊協定 (SFTP) 支援外，使用者還可以移動、執行 AWS、保護和整合 SSL (FTPS) 的 FTP 和純文字 FTP 工作流程。	2020 年 4 月 23 日
Support 虛擬私有雲 (VPC) 安全群組和彈性 IP 位址	您現在可以使用安全性群組為內送 IP 位址建立允許清單，為伺服器提供額外的安全層。您也可以將彈性 IP 位址與伺服器端點建立關聯。這樣，您可以讓防火牆後方的使用者允許存取該端點。如需詳細資訊，請參閱 在虛擬私有雲中建立伺服器。	2020 年 1 月 10 日

變更	描述	日期
Support 在 VPC 中工作	您現在可以在 VPC 中建立伺服器。您可以使用伺服器透過用戶端在 Amazon S3 儲存貯體之間傳輸資料，而無需透過公用網際網路。如需詳細資訊，請參閱 在虛擬私有雲中建立伺服器。	2019 年 3 月 27 日
AWS Transfer Family 發行的第一個版本。	此初始版本包含設定方向，並說明開始使用的方法，亦提供用戶端組態、使用者組態和監控活動的相關資訊。	2018 年 11 月 25 日

AWS 詞彙表

如需最新的 AWS 術語，請參閱《AWS 詞彙表 參考》中的 AWS 詞彙表。

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。