



使用者指南

AWS Transfer Family



AWS Transfer Family: 使用者指南

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

什麼是 AWS Transfer Family ?	1
AWS Transfer Family 運作方式	3
與 Transfer Family 相關的部落格文章	4
必要條件	6
區域、端點和配額	6
註冊 AWS	6
設定儲存	7
設定 Amazon S3 儲存貯體	7
設定 Amazon EFS 檔案系統	11
建立IAM角色和政策	14
建立使用者角色	15
工作階段政策的運作方式	18
讀取/寫入存取政策範例	21
Transfer Family 教學課程	24
開始使用伺服器端點	24
必要條件	25
登入 主控台。	25
建立已啟用 SFTP的伺服器	26
新增服務受管使用者	27
使用用戶端傳輸檔案	28
建立解密工作流程	30
步驟 1：設定執行角色	30
步驟 2：建立受管工作流程	32
步驟 3：將工作流程新增至伺服器並建立使用者	33
步驟 4：建立PGP金鑰對	34
步驟 5：將PGP私有金鑰存放在 AWS Secrets Manager	35
步驟 6：加密檔案	36
步驟 7：執行工作流程並檢視結果	37
建立和使用SFTP連接器	38
步驟 1：建立必要的支援資源	39
步驟 2：建立和測試SFTP連接器	43
步驟 3：使用SFTP連接器傳送和擷取檔案	47
建立 Transfer Family 伺服器以用作遠端SFTP伺服器的程序	50
使用自訂身分提供者	52

必要條件	53
步驟 1：建立 CloudFormation 堆疊	53
步驟 2：檢查伺服器的API閘道方法組態	54
步驟 3：檢視 Transfer Family 伺服器詳細資訊	54
步驟 4：測試您的使用者是否可以連線至伺服器	56
步驟 5：測試SFTP連線和檔案傳輸	56
步驟 6：限制對儲存貯體的存取	57
如果使用 Amazon，請更新 Lambda EFS	59
設定AS2組態	60
步驟 1：為 建立憑證 AS2	61
步驟 2：建立使用AS2通訊協定的 Transfer Family 伺服器	64
步驟 3：將憑證匯入為 Transfer Family 憑證資源	67
步驟 4：為您和交易合作夥伴建立設定檔	68
步驟 5：建立您與合作夥伴之間的協議	69
步驟 6：在您與您的合作夥伴之間建立連接器	70
步驟 7：AS2使用 Transfer Family 測試交換檔案	71
轉移 SFTP、、 的系列 FTPS FTP	73
身分提供者選項	73
AWS Transfer Family 端點類型矩陣	75
設定 Transfer Family 伺服器端點	77
建立已啟用 SFTP的伺服器	79
建立已啟用 FTPS的伺服器	89
建立已啟用 FTP的伺服器	100
在 中建立伺服器 VPC	110
使用自訂主機名稱	128
透過伺服器端點傳輸檔案	132
可用的SFTP/FTPS/FTP命令	134
尋找您的 Amazon VPC端點	135
避免setstat錯誤	137
使用開啟SSH	29
使用 WinSCP	138
使用 Cyberduck	28
使用 FileZilla	141
使用 Perl 用戶端	143
上傳後處理	143
管理使用者	144

服務受管使用者	146
目錄服務使用者	154
自訂身分提供者使用者	170
使用邏輯目錄	196
使用邏輯目錄的規則	197
實作邏輯目錄和 chroot	198
設定邏輯目錄範例	200
設定 Amazon 的邏輯目錄 EFS	201
自訂 AWS Lambda 回應	202
SFTP 連接器	203
設定SFTP連接器	203
建立SFTP連接器	203
SFTP 連接器演算法	211
儲存要與SFTP連接器搭配使用的秘密	212
產生並格式化SFTP連接器私有金鑰	213
測試SFTP連接器	216
使用SFTP連接器傳輸檔案	218
管理SFTP連接器	219
更新SFTP連接器	220
檢視SFTP連接器詳細資訊	220
SFTP 連接器配額	222
的轉移系列 AS2	224
AS2 使用案例	225
設定 AS2	228
使用 Transfer Family 主控台建立AS2伺服器	230
使用範本建立AS2伺服器	233
AS2 組態	235
AS2 特徵和功能	240
設定AS2連接器	242
建立AS2連接器	242
AS2 連接器演算法	245
AS2 連接器的基本身分驗證	246
啟用AS2連接器的基本身分驗證	248
檢視連接器詳細資訊	251
管理AS2合作夥伴	253
匯入AS2憑證	253

AS2 憑證輪換	254
建立AS2設定檔	255
建立AS2協議	256
傳輸AS2訊息	257
AS2 傳送訊息	257
接收AS2訊息	258
設定 HTTPS的 AS2	259
使用AS2連接器傳輸檔案	262
檔案名稱和位置	263
狀態碼	266
範例JSON檔案	266
監視器	268
AS2 狀態碼	269
AS2 錯誤代碼	270
管理檔案處理工作流程	279
建立工作流程	281
設定和執行工作流程	282
檢視工作流程詳細資訊	284
使用預先定義的步驟	287
複製檔案	287
解密檔案	292
標籤檔案	297
刪除檔案	298
工作流程的命名變數	299
範例標籤和刪除工作流程	299
使用自訂檔案處理步驟	304
連續使用多個 Lambda 函數	305
在自訂處理後存取檔案	306
檔案上傳 AWS Lambda 時傳送至 的範例事件	307
自訂工作流程步驟的 Lambda 函數範例	308
IAM 自訂步驟的許可	309
IAM 工作流程的政策	309
工作流程信任關係	311
範例執行角色：解密、複製和標記	311
執行角色範例：執行函數和刪除	313
工作流程的例外處理	314

監控工作流程執行	315
CloudWatch 記錄工作流程	315
CloudWatch 工作流程的指標	317
從範本建立工作流程	318
從 Transfer Family 伺服器移除工作流程	321
限制和限制	323
管理伺服器	324
檢視伺服器清單	324
刪除伺服器	324
檢視SFTP伺服器詳細資訊	326
檢視AS2伺服器詳細資訊	327
編輯伺服器詳細資訊	328
編輯檔案傳輸通訊協定	331
編輯自訂身分提供者參數	333
編輯伺服器端點	335
編輯記錄	337
編輯安全政策	337
變更受管工作流程	339
變更伺服器的顯示橫幅	340
讓伺服器處於線上或離線狀態	340
管理伺服器主機金鑰	341
新增其他伺服器主機金鑰	342
刪除伺服器主機金鑰	343
輪換伺服器主機金鑰	344
其他伺服器主機金鑰資訊	345
在主控台中監控用量	346
管理存取控制	350
建立 S3 儲存貯體存取政策	350
建立工作階段政策	352
防止使用者在 S3 儲存貯體mkdir中執行	355
日誌	356
CloudTrail 記錄	356
啟用 CloudTrail 記錄	357
建立伺服器的範例記錄項目	358
CloudWatch 記錄	359
建立伺服器的記錄	360

管理工作流程的記錄	368
為 設定角色 CloudWatch	371
檢視 Transfer Family 日誌串流	373
建立 Amazon CloudWatch 警示	376
將 S3 API呼叫記錄到 S3 存取日誌	376
限制混淆代理問題的範例	377
CloudWatch 轉移系列的記錄結構	378
CloudWatch 日誌項目範例	383
使用 CloudWatch 指標	386
使用者通知	389
使用 管理事件 EventBridge	390
Transfer Family 事件	390
SFTP、FTPS和 FTP 伺服器事件	391
SFTP 連接器事件	391
A2S 事件	392
傳送 Transfer Family 事件	392
建立事件模式	393
測試事件的事件模式 Transfer Family	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
AS2 事件	404
安全	410
使用安全政策	411
密碼編譯演算法	412
TransferSecurityPolicy-2024 年 1 月	420
TransferSecurityPolicy-2023 年 5 月	421
TransferSecurityPolicy-2022 年 3 月	422
TransferSecurityPolicy-2020 年 6 月	422
TransferSecurityPolicy-2018 年 11 月	424
TransferSecurityPolicy-FIPS-2024 年 1 月	425
TransferSecurityPolicy-FIPS-2023 年 5 月	426
TransferSecurityPolicy-FIPS-2020 年 6 月	427
發佈 Quantum 安全政策	428

量化後安全政策	433
關於 中的量子後混合金鑰交換 SSH	434
使用方式	434
測試方式	435
資料保護	438
資料加密	439
金鑰管理	440
身分與存取管理	455
物件	456
使用身分驗證	456
使用政策管理存取權	459
AWS Transfer Family 如何使用 IAM	461
身分型政策範例	464
標籤型政策範例	467
對 身分與存取進行疑難排解	470
法規遵循驗證	472
恢復能力	472
基礎架構安全	473
Web 應用程式防火牆	473
預防跨服務混淆代理人	475
Transfer Family 使用者角色	476
轉移系列工作流程角色	478
Transfer Family 記錄/調用角色	479
AWS 受管政策	480
AWSTransferConsoleFullAccess	481
AWSTransferFullAccess	482
AWSTransferLoggingAccess	483
AWSTransferReadOnlyAccess	484
政策更新	485
對 Transfer Family 進行故障診斷	486
對服務受管使用者進行故障診斷	486
Amazon EFS服務受管使用者疑難排解	486
對公有金鑰內文太長進行故障診斷	487
新增SSH公有金鑰故障診斷失敗	487
對 Amazon API Gateway 問題進行故障診斷	488
身分驗證失敗太多	488

連線已關閉	489
對加密 Amazon S3 儲存貯體的政策進行故障診斷	490
對身分驗證問題進行故障診斷	490
驗證失敗 —SSH/SFTP	490
Managed AD 不相符領域問題	491
其他身分驗證問題	491
對受管工作流程問題進行故障診斷	492
使用 Amazon 對工作流程相關錯誤進行故障診斷 CloudWatch	492
對工作流程複製錯誤進行故障診斷	494
對工作流程解密問題進行故障診斷	494
對 Amazon EFS問題進行故障診斷	496
對遺失POSIX的設定檔進行故障診斷	497
使用 Amazon 對邏輯目錄進行故障診斷 EFS	498
對身分提供者進行測試的疑難排解	498
為您的SFTP連接器新增受信任主機金鑰的故障診斷	499
對檔案上傳問題進行故障診斷	499
對 Amazon S3 檔案上傳錯誤進行故障診斷	499
對無法讀取的檔案名稱進行故障診斷	500
對ResourceNotFound例外狀況進行疑難排解	500
連接器SFTP問題疑難排解	501
金鑰交涉失敗	501
其他SFTP連接器問題	501
針對 AS2 問題進行故障診斷	502
API 參考	503
歡迎	503
動作	505
CreateAccess	508
CreateAgreement	515
CreateConnector	521
CreateProfile	528
CreateServer	532
CreateUser	544
CreateWorkflow	552
DeleteAccess	560
DeleteAgreement	563
DeleteCertificate	566

DeleteConnector	568
DeleteHostKey	570
DeleteProfile	573
DeleteServer	575
DeleteSshPublicKey	578
DeleteUser	581
DeleteWorkflow	584
DescribeAccess	586
DescribeAgreement	590
DescribeCertificate	593
DescribeConnector	596
DescribeExecution	599
DescribeHostKey	604
DescribeProfile	607
DescribeSecurityPolicy	610
DescribeServer	614
DescribeUser	619
DescribeWorkflow	624
ImportCertificate	629
ImportHostKey	634
ImportSshPublicKey	638
ListAccesses	643
ListAgreements	647
ListCertificates	651
ListConnectors	654
ListExecutions	657
ListHostKeys	662
ListProfiles	666
ListSecurityPolicies	670
ListServers	674
ListTagsForResource	678
ListUsers	682
ListWorkflows	687
SendWorkflowStepState	690
StartFileTransfer	693
StartServer	699

StopServer	702
TagResource	705
TestConnection	708
TestIdentityProvider	712
UntagResource	719
UpdateAccess	722
UpdateAgreement	729
UpdateCertificate	734
UpdateConnector	738
UpdateHostKey	743
UpdateProfile	747
UpdateServer	750
UpdateUser	762
資料類型	769
As2ConnectorConfig	772
CopyStepDetails	776
CustomStepDetails	778
DecryptStepDetails	780
DeleteStepDetails	782
DescribedAccess	784
DescribedAgreement	788
DescribedCertificate	792
DescribedConnector	796
DescribedExecution	799
DescribedHostKey	802
DescribedProfile	805
DescribedSecurityPolicy	807
DescribedServer	809
DescribedUser	817
DescribedWorkflow	821
EfsFileLocation	823
EndpointDetails	825
ExecutionError	828
ExecutionResults	830
ExecutionStepResult	831
FileLocation	833

HomeDirectoryMapEntry	834
IdentityProviderDetails	836
InputFileLocation	838
ListedAccess	839
ListedAgreement	842
ListedCertificate	845
ListedConnector	848
ListedExecution	850
ListedHostKey	852
ListedProfile	854
ListedServer	856
ListedUser	859
ListedWorkflow	862
LoggingConfiguration	864
PosixProfile	865
ProtocolDetails	867
S3FileLocation	870
S3InputFileLocation	872
S3StorageOptions	874
S3Tag	875
ServiceMetadata	876
SftpConnectorConfig	877
SshPublicKey	879
Tag	881
TagStepDetails	882
UserDetails	884
WorkflowDetail	886
WorkflowDetails	888
WorkflowStep	890
提出 API 要求	892
Transfer Family 必要的要求標頭	892
Transfer Family 請求輸入和簽名	894
錯誤回應	894
可用程式庫	896
常見參數	897
常見錯誤	899

文件歷史紀錄	901
AWS 詞彙表	909
.....	cmx

什麼是 AWS Transfer Family ？

AWS Transfer Family 是一項安全傳輸服務，可讓您將檔案傳輸到 AWS 儲存服務中和傳出儲存服務。Transfer Family 是 AWS 雲端 platform 的一部分。AWS Transfer Family 提供完全受管的支援，以透過 SFTP、FTPS、AS2和 FTP 直接進出 Amazon S3 或 Amazon EFS。您可以透過維護現有的用戶端組態來無縫遷移、自動化和監控檔案傳輸工作流程，以進行身分驗證、存取和防火牆，因此您的客戶、合作夥伴和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 支援將資料從 或 傳輸到下列 AWS 儲存服務。

- Amazon Simple Storage Service (Amazon S3) 儲存。如需 Amazon S3 的相關資訊，請參閱[Amazon Simple Storage Service 入門](#)。
- Amazon Elastic File System (AmazonEFS) Network File System (NFS) 檔案系統。如需 Amazon 的相關資訊EFS，請參閱[什麼是 Amazon Elastic File System](#)

AWS Transfer Family 支援透過下列通訊協定傳輸資料：

- 安全殼層 (SSH) 檔案傳輸通訊協定 (SFTP)：第 3 版
- 檔案傳輸通訊協定安全 (FTPS)
- 檔案傳輸通訊協定 (FTP)
- 適用性陳述式 2 (AS2)

Note

對於 FTP和 FTPS 資料連線，Transfer Family 用來建立資料頻道的連接埠範圍為 8192–8200。

檔案傳輸通訊協定用於金融服務、醫療保健、廣告和零售等不同產業的資料交換工作流程。Transfer Family 可簡化檔案傳輸工作流程遷移至 的過程 AWS。

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

- 中的資料湖 AWS，用於從供應商和合作夥伴等第三方上傳。
- 針對您客戶的訂閱類型資料分發。

- 您組織的內部傳輸。

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

- 資料分佈
- 供應鏈
- 內容管理
- Web 服務應用程式

以下是搭配 使用 Transfer Family 的一些常見使用案例AS2：

- 具有合規要求的工作流程，這些要求依賴於將資料保護和安全性功能內建到通訊協定中
- 供應鏈物流
- 付款工作流程
- Business-to-business (B2B) 交易
- 與企業資源規劃 (ERP) 和客戶關係管理 (CRM) 系統整合

使用 Transfer Family，您可以在 中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設施。您可以使用此服務將檔案傳輸型工作流程遷移至 ，AWS 同時維持最終使用者的用戶端和組態。您首先將主機名稱與伺服器端點建立關聯，然後新增您的使用者，並為其佈建適當的存取層級。執行此操作後，使用者的傳輸請求會直接從 Transfer Family 伺服器端點服務。

Transfer Family 提供下列優點：

- 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設施。
- 將資料儲存在耐用的 Amazon S3 儲存體中，您可以使用原生 AWS 服務 來處理、分析、報告、稽核和封存函數。
- 使用 Amazon EFS作為資料存放區，您可以取得完全受管的彈性檔案系統，以搭配 AWS 雲端 服務和內部部署資源使用。Amazon EFS 專為隨需擴展至 PB 而打造，不會中斷應用程式、在您新增和移除檔案時自動成長和縮減。這有助於消除佈建和管理容量以適應成長的需求。
- 完全受管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 上傳的檔案處理 AWS Transfer Family。
- 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 不同功能的描述、入門教學課程、如何設定不同已啟用通訊協定之伺服器的詳細指示、如何使用不同類型的身分提供者，以及服務的API參考。

若要開始使用 Transfer Family，請參閱以下內容：

- [AWS Transfer Family 運作方式](#)
- [必要條件](#)
- [AWS Transfer Family 伺服器端點入門](#)

AWS Transfer Family 運作方式

AWS Transfer Family 是一項完全受管 AWS 的服務，您可以透過下列通訊協定，用來在 Amazon Simple Storage Service (Amazon S3) 儲存體或 Amazon Elastic File System (AmazonEFS) 檔案系統之間傳輸檔案：

- 安全殼層 (SSH) 檔案傳輸通訊協定 (SFTP)：第 3 版
- 檔案傳輸通訊協定安全 (FTPS)
- 檔案傳輸通訊協定 (FTP)
- 適用性陳述式 2 (AS2)

AWS Transfer Family 最多支援 3 個可用區域，並由自動擴展的備援機群支援，以滿足您的連線和傳輸請求。如需如何使用延遲型路由建置以增加備援並盡可能降低網路延遲的範例，請參閱部落格文章將[伺服器 AWS 傳輸的網路延遲降到最低SFTP](#)。

Transfer Family Managed File Transfer Workflows (MFTW) 是一項完全受管、無伺服器 File Transfer Workflow 服務，可讓您輕鬆設定、執行、自動化和監控使用上傳的檔案處理 AWS Transfer Family。客戶可以使用 MFTW 來自動化各種處理步驟，例如複製、標記、掃描、篩選，以及使用 Transfer Family 傳輸compressing/decompressing, and encrypting/decrypting的資料。這可提供追蹤和可稽核性的端對端可見性。如需詳細資訊，請參閱[AWS Transfer Family 受管工作流程](#)。

AWS Transfer Family 支援任何標準檔案傳輸通訊協定用戶端。一些常用的用戶端如下：

- [開啟SSH](#) – Macintosh 和 Linux 命令列公用程式。
- [WinSCP](#) – 僅限 Windows 的圖形用戶端。
- [Cyberduck](#) – Linux、Macintosh 和 Microsoft Windows 圖形用戶端。
- [FileZilla](#) – Linux、Macintosh 和 Windows 圖形用戶端。

與 Transfer Family 相關的部落格文章

下表列出包含 Transfer Family 客戶有用資訊的部落格文章。資料表會依反向時間順序排序，以便最新的文章位於資料表的開頭。

部落格文章標題和連結	日期
Transfer Family 如何協助您建置安全、合規的受管檔案傳輸解決方案	2024 年 1 月 3 日
使用 偵測惡意軟體威脅 AWS Transfer Family	2023 年 7 月 20 日
使用 擴展SAP工作負載 AWS Transfer Family	2023 年 7 月 13 日
使用 和 加密PGP和解密檔案 AWS Transfer Family	2023 年 6 月 21 日
AWS Transfer Family 使用 Azure Active Directory 和 向 進行驗證 AWS Lambda	2022 年 12 月 15 日
使用 AWS Transfer Family 受管工作流程自訂檔案交付通知	2022 年 10 月 14 日
使用 AWS Transfer Family 工作流程建置雲端原生檔案傳輸平台	2022 年 1 月 5 日
使用 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 增強資料存取控制	2021 年 10 月 5 日
使用 AWS Global Accelerator 和 AWS Transfer Family 服務改善面向網際網路的檔案傳輸輸送量	2021 年 6 月 7 日
AWS Transfer Family 使用 AWS Web Application Firewall 和 Amazon API Gateway 保護	2021 年 5 月 5 日

部落格文章標題和連結	日期
AWS Transfer Family 使用 AWS Web Application Firewall 和 Amazon API Gateway 保護	2021 年 1 月 15 日
AWS Transfer Family 支援 Amazon Elastic File System	2021 年 1 月 7 日
啟用密碼身分驗證以 AWS Transfer Family 使用 AWS Secrets Manager	2020 年 11 月 5 日
使用 AWS Transfer Family 和 集中資料存取 AWS Storage Gateway	2020 年 6 月 22 日
在無伺服器應用程式中 AWS Lambda 使用 Amazon EFS for	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
透過SFTP伺服器 AWS 傳輸將網路延遲降至最低	2020 年 2 月 19 日
將SFTP伺服器提升和轉移到 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 做為身分提供者搭配 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 Simple Storage Service (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。此信任關係允許 Transfer Family 擔任 IAM 角色來存取您的儲存貯體，以便服務使用者的檔案傳輸請求。

主題

- [支援 AWS 的區域、端點和配額](#)
- [註冊 AWS](#)
- [設定要與 搭配使用的儲存體 AWS Transfer Family](#)
- [建立 IAM 角色和政策](#)

支援 AWS 的區域、端點和配額

若要以程式設計方式連線至 AWS 服務，您可以使用端點。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，是的服務資源或操作數量上限 AWS 帳戶。在本指南中，您可以在 [AS2 配額](#) 和 [SFTP 連接器配額](#) 中找到配額。

如需支援 AWS 的區域、端點和服務配額的詳細資訊，請參閱中的 [AWS Transfer Family 端點和配額](#) Amazon Web Services 一般參考。

註冊 AWS

當您註冊 Amazon Web Services (AWS) 時，AWS 您的帳戶會自動註冊 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。

如果您已有 AWS 帳戶，請跳至下一個任務。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，請完成下列步驟以建立。

若要註冊 AWS 帳戶

1. 開啟<https://portal.aws.amazon.com/billing/註冊>。
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。

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

如需有關定價和的資訊 AWS 定價計算工具，用於取得使用 Transfer Family 的成本估算，請參閱[AWS Transfer Family 定價](#)。

如需 AWS 區域可用性的相關資訊，請參閱中的[AWS Transfer Family 端點和配額](#) AWS 一般參考。

設定要與 搭配使用的儲存體 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作為 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](#)
 - [導致延遲問題的大量零位元組物件](#)
- [設定 Amazon EFS 檔案系統](#)
 - [Amazon EFS 檔案擁有權](#)
 - [為 Transfer Family 設定 Amazon EFS使用者](#)
 - [在 Amazon 上設定 Transfer Family 使用者 EFS](#)
 - [建立 Amazon EFS根使用者](#)
 - [支援的 Amazon EFS命令](#)

設定 Amazon S3 儲存貯體

AWS Transfer Family 會存取您的 Amazon S3 儲存貯體來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通訊協定之伺服器的一部分。您可以使用現有的儲存貯體，或是建立新的。

Note

您不需要使用相同 AWS 區域中的伺服器 and Amazon S3 儲存貯體，但建議您將此作為最佳實務。

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

如需建立新儲存貯體的資訊，請參閱 Amazon Simple Storage Service 使用者指南 中的[如何建立 S3 儲存貯體？](#)。

Note

您可以使用 Amazon S3 物件鎖定，以防止物件在固定的時間或無限期覆寫。這與 Transfer Family 與其他服務的運作方式相同。如果物件存在且受到保護，則不允許寫入或刪除該檔案。如需 Amazon S3 物件鎖定的詳細資訊，請參閱Amazon Simple Storage Service 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](#)，Amazon S3 的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 Access Point 別名。您可以在 Amazon S3 中為具有存取 Amazon S3 儲存貯體中共用資料之不同許可的使用者建立數百個存取點。

例如，您可以使用存取點，讓三個不同的團隊能夠存取相同的共用資料集，其中一個團隊可以從 S3 讀取資料，另一個團隊可以將資料寫入 S3，而第三個團隊可以從 S3 讀取、寫入和刪除資料。若要實作上述精細存取控制，您可以建立 S3 存取點，其中包含對不同團隊提供非對稱存取的政策。您可以搭配 Transfer Family 伺服器使用 S3 存取點來實現精細存取控制，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 部落格文章增強資料存取控制](#)。

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，您可以最佳化 Amazon S3 目錄的效能，以消除 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 可以模擬階層式檔案系統，但有時行為可能會與一般檔案系統不同。例如，目錄在 Amazon S3 中不是一流的概念，而是以物件金鑰為基礎。AWS Transfer Family 會以正斜線字元 (/) 分割物件的金鑰，將最後一個元素視為檔案名稱，然後將具有相同字首的檔案名稱分組在一起。當您使用 `mkdir` 或 Amazon S3 主控台建立空目錄時，系統會建立零位元組物件來表示資料夾的路徑。這些物件的索引鍵結尾為正斜線。這些零位元組物件會在[使用 Amazon S3 使用者指南 中的資料夾整理 Amazon S3 主控台 中的物件](#)中說明。Amazon S3

當您執行 `ls` 命令時，有些結果是 Amazon S3 零位元組物件（這些物件的索引鍵結尾為正斜線字元），Transfer Family 會發出每個物件的 HeadObject 請求（如需詳細資訊，請參閱 Amazon Simple Storage Service API 參考[HeadObject](#)中的）。使用 Amazon S3 作為具有 Transfer Family 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 Amazon S3 物件的寫入存取權。例如，您可能想要提供寫入（或上傳）和列出儲存貯體中物件的存取權，但不要讀取（下載）物件。若要使用檔案傳輸用戶端執行 `ls` 和 `mkdir` 命令，您必須具有 Amazon S3 ListObjects 和 PutObject 許可。不過，當 Transfer Family 需要 HeadObject 呼叫寫入或列出檔案時，呼叫會失敗，但 Access 遭拒的錯誤，因為此呼叫需要 GetObject 許可。

Note

當您建立或更新 Transfer Family 伺服器時，您可以最佳化 Amazon S3 目錄的效能，以消除 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權，該條件只會為以斜線 (/) 結尾的物件新增 GetObject 許可。此條件可防止對檔案（因此無法讀取）進行 GetObject 呼叫，但允許使用者列出和周遊資料夾。下列範例政策僅提供對 Amazon S3 儲存貯體的寫入和列出存取權。若要使用此政策，*DOC-EXAMPLE-BUCKET* 請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

此政策不允許使用者附加檔案。換句話說，被指派此政策的使用者無法開啟檔案來將內容新增至他們，或修改這些內容。此外，如果您的使用案例在上傳檔案之前需要HeadObject呼叫，則此政策不適用於您。

導致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。

此問題的一個可能解決方案是刪除所有零位元組物件。注意下列事項：

- 空的目錄將不再存在。目錄的存在，是因為其名稱位於物件的金鑰中。
- 不會阻止某人再次呼叫 mkdir 和破壞一切。您可以透過制定防止目錄建立的政策來緩解這種情況。
- 有些案例會使用這些 0 位元組物件。例如，您有 /inboxes/customer1000 等結構，而且收件匣目錄每天都會清除。

另一個可能的解決方法是限制透過政策條件可見的物件數量，以減少 HeadObject 呼叫數量。為了成為可行的解決方案，您需要接受您可能只能檢視一組有限的所有子目錄。

設定 Amazon EFS 檔案系統

AWS Transfer Family 存取 Amazon Elastic File System (Amazon EFS) 以服務使用者的傳輸請求。因此，您必須提供 Amazon EFS 檔案系統，作為設定已啟用檔案傳輸通訊協定之伺服器的一部分。您可以使用現有的檔案系統，也可以建立新的檔案系統。

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中 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帳戶中，則檔案系統政策必須明確授予使用者角色許可。

如需有關如何設定多個帳戶的資訊，請參閱 AWS Organizations 使用者指南 中的 [管理組織中 AWS 的帳戶](#)。

- 設定使用者時，您可以為每個使用者指派 IAM 角色。此角色會決定他們對 Amazon EFS 檔案系統的存取層級。
- 如需掛載 Amazon EFS 檔案系統的詳細資訊，請參閱 [掛載 Amazon EFS 檔案系統](#)。

如需有關 AWS Transfer Family 和 Amazon 如何 EFS 搭配使用的詳細資訊，請參閱 Amazon Elastic File System 使用者指南 中的 [使用 AWS Transfer Family 存取 Amazon EFS 檔案系統中的檔案](#)。
Amazon Elastic File System

Amazon EFS 檔案擁有權

Amazon EFS使用可攜式作業系統介面（POSIX）檔案許可模型來表示檔案擁有權。

在中POSIX，系統中的使用者分為三個不同的許可類別：當您允許使用者使用存取存放在 Amazon EFS 檔案系統中的檔案時 AWS Transfer Family，您必須為其指派「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。

- 使用者（u）：檔案或目錄的擁有者。通常，檔案或目錄的建立者也是擁有者。
- 群組（g）：需要對共用的檔案和目錄進行相同存取的使用者集。
- 其他（o）：除擁有者和群組成員外，所有其他可存取系統的使用者。此許可類別也稱為「公開」。

在POSIX許可模型中，每個檔案系統物件（檔案、目錄、符號連結、命名管道和通訊端）都與上述三組許可相關聯。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 式系統上，使用者和群組會映射到數值識別符，Amazon EFS會使用這些識別符來表示檔案擁有權。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會使用映射的數值IDs來檢查許可。

為 Transfer Family 設定 Amazon EFS使用者

設定 Amazon EFS使用者之前，您可以執行下列任一動作：

- 您可以在 Amazon 中建立使用者和設定其主資料夾EFS。如需詳細資訊，請參閱 [在 Amazon 上設定 Transfer Family 使用者 EFS](#)。
- 如果您願意新增根使用者，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 使用者的POSIX設定檔（如上節所述）提供設定POSIX許可的功能。這些許可是根據、GID和次要UID，在使用者層級設定精細存取GIDs。

在 Amazon 上設定 Transfer Family 使用者 EFS

Transfer Family 會將使用者映射到 UID/GID and directories you specify. If the UID/GID/directories 中不存在的 EFS，然後您應該在轉移給使用者之前建立使用者。有關建立 Amazon EFS 使用者的詳細資訊，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](#)。

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

1. 使用 [PosixProfile](#) 欄位 GID，在 Transfer Family 中為您的使用者對應 EFS UID 和。
2. 如果您希望使用者在登入時從特定資料夾中啟動，您可以在 [HomeDirectory](#) 欄位下指定 EFS 目錄。

您可以使用 CloudWatch 規則和 Lambda 函數來自動化程序。如需與互動的範例 Lambda 函數 EFS，請參閱 [AWS Lambda 在無伺服器應用程式中使用 Amazon EFS for](#)。

此外，您可以為 Transfer Family 使用者設定邏輯目錄。如需詳細資訊，請參閱 [使用邏輯目錄來簡化 Transfer Family 目錄結構](#) 主題中的 [設定 Amazon 的邏輯目錄 EFS](#) 一節。

建立 Amazon EFS 根使用者

如果您的組織對於透過 SFTP/FTPS 啟用根使用者存取權以設定使用者感到自在，您可以建立 UID 且 GID 為 0 的使用者（根使用者），然後使用該根使用者來建立資料夾，並為其餘使用者指派 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](#)，並針對使用者 ID 和群組 ID，輸入 0（零）。

支援的 Amazon EFS 命令

Amazon EFS for 支援下列命令 AWS Transfer Family。

- cd
- ls/dir
- pwd
- put
- get
- rename
- chown：只有根（即 uid=0 的使用者）可以變更檔案和目錄的擁有權和許可。
- chmod：只有根可以變更檔案和目錄的擁有權和許可。

- `chgrp`：支援根 或檔案擁有者，只能將檔案的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

本主題描述可與 搭配使用的政策和角色類型 AWS Transfer Family，並逐步解說建立使用者角色的程序。它還描述工作階段政策的運作方式，並提供範例使用者角色。

AWS Transfer Family 使用以下類型的角色：

- 使用者角色 – 允許服務受管使用者存取必要的 Transfer Family 資源。在 Transfer Family 使用者 的背景 下 AWS Transfer Family 擔任此角色ARN。
- 存取角色 – 僅提供正在傳輸的 Amazon S3 檔案的存取權。對於傳入AS2傳輸，存取角色會使用 Amazon Resource Name (ARN) 作為協議。對於傳出AS2傳輸，存取角色會使用 ARN 連接器的 。
- 調用角色 – 與 Amazon API Gateway 搭配使用，作為伺服器的自訂身分提供者。Transfer Family 會在 Transfer Family 伺服器 的內容中擔任此角色ARN。
- 記錄角色 – 用於將項目記錄到 Amazon CloudWatch。Transfer Family 使用此角色記錄成功和失敗詳細資訊，以及檔案傳輸的相關資訊。Transfer Family 會在 Transfer Family 伺服器 的內容中擔任此角色ARN。對於傳出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 的內容中擔任此角色ARN。

除了這些角色之外，您也可以使用工作階段政策 。工作階段政策用於在必要時限制存取。請注意，這些政策是獨立的：也就是說，您不會將這些政策新增至角色。相反地，您可以將工作階段政策直接新增至 Transfer Family 使用者。

Note

當您建立服務受管 Transfer Family 使用者時，您可以根據主資料夾 選取自動產生政策。如果您想要限制使用者存取自己的資料夾，這是有用的捷徑。此外，您也可以在中檢視工作階段政

策和範例的詳細資訊[工作階段政策的運作方式](#)。您也可以[在 IAM 使用者指南 中的工作階段政策](#)中找到[工作階段政策](#)的詳細資訊。

主題

- [建立使用者角色](#)
- [工作階段政策的運作方式](#)
- [讀取/寫入存取政策範例](#)

建立使用者角色

當您建立使用者時，您會針對使用者存取做出許多決策。這些決定包括使用者可以存取的 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，以及檔案系統中可存取哪些檔案，以及使用者擁有哪些許可（例如 PUT 或 GET）。

若要設定存取權，您可以建立身分型 AWS Identity and Access Management (IAM) 政策和角色，以提供該存取資訊。作為此程序的一部分，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，這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 IAM 的政策 AWS Transfer Family。如中所述[為 建立 IAM 政策 AWS Transfer Family](#)。
2. 建立 IAM 角色並連接新 IAM 政策。如需範例，請參閱[讀取/寫入存取政策範例](#)。
3. 在 AWS Transfer Family 和 IAM 角色之間建立信任關係。如中所述[建立信任關係](#)。

下列程序說明如何建立 IAM 政策和角色。

為 建立 IAM 政策 AWS Transfer Family

1. 在開啟 IAM 主控台<https://console.aws.amazon.com/iam/>。
2. 在導覽窗格中，選擇 Policies (政策)，然後選擇 Create policy (建立政策)。
3. 在建立政策頁面上，選擇 JSON 索引標籤。
4. 在出現的編輯器中，將編輯器的內容取代為您想要連接至 IAM 角色 IAM 的政策。

您可以授予讀取/寫入存取權，或將使用者限制為其主目錄。如需詳細資訊，請參閱[讀取/寫入存取政策範例](#)。

5. 選擇檢閱政策並提供政策的名稱和描述，然後選擇建立政策。

接下來，您可以建立角色，並將新IAM政策連接至該IAM角色。

為 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，確定已選擇 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. 在連接許可政策區段中，找到並選擇您剛建立的政策，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。它們的功能相同，因此您可以在建構政策時使用。Transfer Family 文件用於條件包含萬用字元 ArnLike，並 ArnEquals 指示完全相符的條件。

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"。存取政策如下所示。

```
{
  "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/*"
  }
}

```

如果您想要限制特定伺服器，而不是使用者帳戶中的任何伺服器，您也可以使用 `ArnLike` 條件。例如：

```

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

```

Note

在上述範例中，取代每個 *user input placeholder* 使用您自己的資訊。

如需混淆代理問題的詳細資訊和更多範例，請參閱 [預防跨服務混淆代理人](#)。

4. 選擇更新信任政策以更新存取政策。

您現在已建立允許代表您 AWS Transfer Family 呼叫 AWS 服務 IAM 的角色。您已連接至您建立 IAM 的政策角色，以授予使用者存取權。在 [AWS Transfer Family 伺服器端點入門](#) 區段中，此角色和政策會指派給您的使用者。

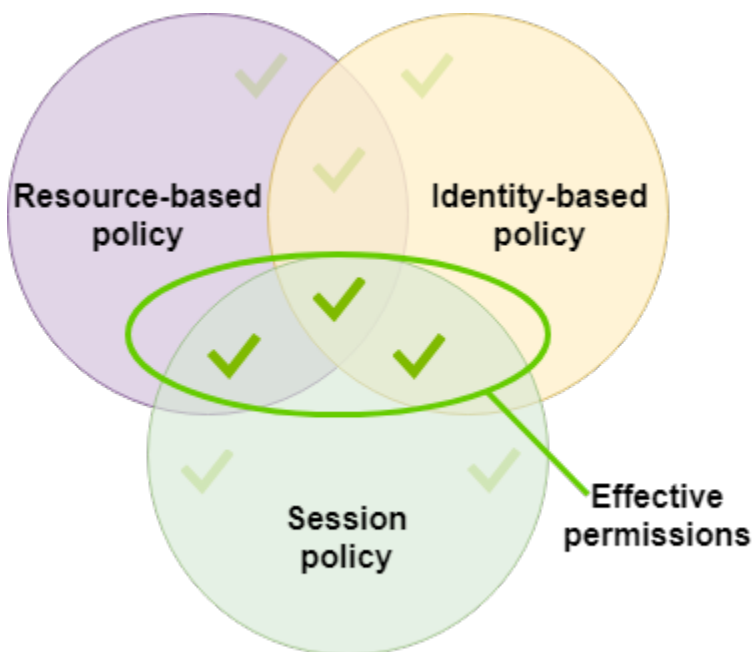
另請參閱

- 如需IAM角色的一般資訊，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 Simple Storage Service 使用者指南 中的[Amazon S3 中的身分和存取管理](#)。
- 若要進一步了解 Amazon EFS 資源的身分型政策，請參閱 Amazon Elastic [File System 使用者指南](#) 中的[使用 IAM來控制檔案系統資料存取](#)。Amazon Elastic File System

工作階段政策的運作方式

當管理員建立角色時，角色通常包含涵蓋多個使用案例或團隊成員的廣泛許可。如果管理員設定[主控台 URL](#)，則可以使用工作階段政策 來減少產生工作階段的許可。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，限制使用者僅存取其主目錄。

當您以程式設計方式為角色或使用者建立臨時工作階段時，工作階段政策是作為 參數傳遞的進階政策。工作階段政策有助於鎖定使用者，以便他們只能存取包含其使用者名稱的物件字首的儲存貯體部分。下圖顯示工作階段政策的許可是工作階段政策與資源型政策的交集，以及工作階段政策和身分型政策的交集。



如需更多詳細資訊，請參閱 IAM 使用者指南 中的[工作階段政策](#)。

在 中 AWS Transfer Family，只有在您往返 Amazon S3 傳輸時，才支援工作階段政策。下列範例政策是工作階段政策，只會限制使用者對其home目錄的存取。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 PutObjectACL 陳述式。也就是說，您的 Transfer Family 伺服器需要存取不同帳戶中的儲存貯體。
- 工作階段政策的長度上限為 2048 個字元。如需更多詳細資訊，請參閱 API 參考 中 [CreateUser 動作的政策請求參數](#)。
- 如果您的 Amazon S3 儲存貯體使用 AWS Key Management Service (AWS KMS) 加密，您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

上述政策範例假設使用者已將主目錄設定為包含尾斜線，以表示它是目錄。另一方面，如果您設定的使用者HomeDirectory沒有尾斜線，則應將其納入政策中。

在先前的範例政策中，請注意 `transfer:HomeFolder`、`transfer:HomeBucket` 和 `transfer:HomeDirectory` 政策參數的使用。這些參數是針對為使用者設定的 HomeDirectory 設定，如 [HomeDirectory](#) 和 中所述 [實作API閘道方法](#)。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。
- 參數會以`transfer:HomeFolder`參數的剩餘部分取代HomeDirectory。
- `transfer:HomeDirectory` 參數已移除正斜線 (/)，因此可在 Resource陳述式中將其用作 S3 Amazon Resource Name (ARN) 的一部分。

Note

如果您使用的是邏輯目錄，也就是使用者的 `homeDirectoryType` 是 LOGICAL，則不支援這些政策參數 (HomeBucket、HomeDirectory 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` 會變成 `home/bob/amazon/stuff/`。

第一個"Sid"允許使用者列出從 開始的所有目錄`/home/bob/amazon/stuff/`。

第二個"Sid"限制使用者對put相同路徑 的get存取`/home/bob/amazon/stuff/`。

讀取/寫入存取政策範例

授予對 Amazon S3 儲存貯體的讀取/寫入存取權

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

注意下列事項：

- Replace (取代) *DOC-EXAMPLE-BUCKET* Amazon S3 儲存貯體的名稱。
- 只有在您需要啟用跨帳戶存取時，才需要 GetObjectACL 和 PutObjectACL 陳述式。也就是說，您的 Transfer Family 伺服器需要存取不同帳戶中的儲存貯體。
- 只有在存取的 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，而不是將其完全關閉。如需詳細資訊，請參閱 [未版本、啟用版本控制和已暫停版本控制儲存貯體](#)。

```
{
  "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/*"
}
]
}

```

准許檔案系統存取 Amazon EFS 檔案系統中的檔案

Note

除了政策之外，您還必須確保POSIX檔案許可授予適當的存取權。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](#)。

下列範例政策會授予 Amazon 檔案系統中檔案的根EFS檔案系統存取權。

Note

在下列範例中，取代 *region* 您的區域 *account-id* 檔案所在的 帳戶，以及 *file-system-id* Amazon Elastic File System（Amazon EFS）的 ID。

```

{
  "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"  
      }  
    ]  
  }  
}
```

下列範例政策會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 教學課程

AWS Transfer Family 使用者指南提供數個使用案例的詳細演練。

- [AWS Transfer Family 伺服器端點入門](#)：本教學課程會逐步引導您建立 SFTP Transfer Family 伺服器和服務受管使用者，然後示範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 儲存體和 SFTP伺服器之間傳輸檔案。
- [將 Amazon API Gateway 方法設定為自訂身分提供者](#)：本教學課程說明如何設定 Amazon API Gateway 方法，並將其用作將檔案上傳至 AWS Transfer Family 伺服器的自訂身分提供者。
- [設定用於解密檔案的受管工作流程](#)：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至 Amazon S3 儲存貯體，然後檢視解密檔案。
- [設定AS2組態](#)：本教學課程會逐步解說設定 AS2 Transfer Family 伺服器所需的步驟。有匯入憑證、建立設定檔和協議、選擇性地建立AS2連接器，然後測試組態的指示。

主題

- [AWS Transfer Family 伺服器端點入門](#)
- [設定用於解密檔案的受管工作流程](#)
- [設定和使用SFTP連接器](#)
- [將 Amazon API Gateway 方法設定為自訂身分提供者](#)
- [設定AS2組態](#)

AWS Transfer Family 伺服器端點入門

使用此教學課程開始使用 AWS Transfer Family (Transfer Family)。您將了解如何使用 Amazon S3 儲存體建立具有公開存取端點的SFTP已啟用的伺服器、使用服務管理身分驗證新增使用者，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：建立已啟用 SFTP的伺服器](#)

- [步驟 3：新增服務受管使用者](#)
- [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 中的要求 [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，而設定 Transfer Family 使用的其他 AWS 服務需要許可，例如 Amazon Simple Storage Service AWS Certificate Manager、Amazon Elastic File System 和 Amazon Route 53。例如，對於 AWS 使用 Transfer Family 傳輸檔案的使用者，AmazonS3FullAccess 會授予許可來設定和使用 Amazon S3 儲存貯體。建立 Amazon S3 儲存貯體需要此政策中的一些許可。

若要使用 Transfer Family 主控台，您需要下列項目：

- AWSTransferConsoleFullAccess 會授予許可，讓您的SFTP使用者建立 Transfer Family 資源。
- IAMFullAccess (或特定而言允許建立IAM角色的政策) 只有在您希望 Transfer Family 在 Amazon CloudWatch Logs 中自動為伺服器建立記錄角色，或使用者登入伺服器的使用者角色時才需要。
- 若要建立和刪除VPC伺服器類型，您需要將動作 ec2:CreateVpcEndpoint 和 ec2:DeleteVpcEndpoints 新增至政策。

Note

AmazonS3FullAccess 和 IAMFullAccess政策本身不需要的一般使用 AWS Transfer Family。此處顯示這些項目，是確保涵蓋所有所需許可的簡單方法。此外，這些是 AWS 受管政策，這是所有 AWS 客戶都可使用的標準政策。您可以檢視這些政策中的個別許可，並判斷您為了目的所需的最小設定。

步驟 1：登入 AWS Transfer Family 主控台

若要登入 Transfer Family

1. 登入 AWS Management Console 並在 開啟 AWS Transfer Family 主控台<https://console.aws.amazon.com/transfer/>。
2. 針對帳戶 ID 或別名，輸入的 ID AWS 帳戶。

3. 針對IAM使用者名稱，輸入您為 Transfer Family 建立的使用者角色名稱。
4. 針對密碼，輸入 AWS 您的帳戶密碼。
5. 選擇 Sign In (登入)。

步驟 2：建立已啟用 SFTP的伺服器

Secure Shell (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。通訊協定支援的完整安全和身分驗證功能SSH。它廣泛用於交換資料，包括金融服務、醫療保健、零售和廣告等各種產業的業務合作夥伴之間的敏感資訊。

若要建立SFTP已啟用的伺服器

1. 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. 在選擇身分提供者中，選擇 Service 受管以將使用者身分和金鑰存放在 Transfer Family 中，然後選擇下一步。
4. 在選擇端點中，執行下列動作：
 - a. 針對端點類型，選擇可公開存取的端點類型。
 - b. 針對自訂主機名稱，選擇無。
 - c. 選擇 Next (下一步)。
5. 在選擇網域中，選擇 Amazon S3。
6. 在設定其他詳細資訊中，執行下列動作：
 - a. 針對CloudWatch 記錄，選擇建立新角色以允許 Transfer Family 自動建立IAM角色，只要您擁有建立新角色的正確許可。建立IAM的角色稱為 AWSTransferLoggingAccess。
 - b. 針對密碼編譯演算法選項，選擇包含啟用供伺服器使用之密碼編譯演算法的安全政策。預設安全政策為 TransferSecurityPolicy-2020-06。
 - c. 選擇 Next (下一步)。
7. 在檢閱和建立中，選擇建立伺服器。系統會將您導向伺服器頁面。

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操作，但您需要先建立使用者。

步驟 3：新增服務受管使用者

將使用者新增至SFTP已啟用的伺服器

1. 在伺服器頁面上，選取您要新增使用者之伺服器的核取方塊。
2. 選擇新增使用者。
3. 在使用者組態區段中，針對使用者名稱 輸入使用者名稱。此使用者名稱必須至少為 3 個字元，最多為 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 '-'、句點 '.' 和符號 '@'。使用者名稱不能以連字號、句號或符號開頭。
4. 針對存取，選擇IAM您先前建立的角色，提供對 Amazon S3 儲存貯體的存取。

您已使用 中的程序建立此IAM角色[建立IAM角色和政策](#)。該IAM角色包含提供存取 Amazon S3 儲存貯體IAM的政策。它還包括與 AWS Transfer Family 服務的信任關係，如其他IAM政策所定義。

Note

服務受管使用者IAM的角色必須包含存取所需儲存貯體的許可。S3FullAccess 涵蓋存取所需儲存貯體的許可，這會授予管理員層級許可給 S3 資源。

5. 針對政策，選擇無。
6. 對於主目錄，選擇 Amazon S3 儲存貯體以存放要使用 傳輸的資料 AWS Transfer Family。輸入使用者使用其用戶端登入時所到達的home目錄路徑。

如果您將此參數保留空白，則會使用 Amazon S3 儲存貯體的root目錄。在此情況下，請確定您的IAM角色提供此root目錄的存取權。

Note

我們建議您選擇包含使用者名稱的目錄路徑，這可讓您有效地使用工作階段政策。工作階段政策會將 Amazon S3 儲存貯體中的使用者存取權限制為該使用者的home目錄。

7. 對於受限制，選取核取方塊，您的使用者就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

為使用者指派主目錄，並將使用者限制為該主目錄時，這應足以鎖定使用者對指定資料夾的存取權。當您需要套用進一步控制項時，請使用工作階段政策。

8. 對於SSH公有金鑰，輸入SSH金鑰對的公有SSH金鑰部分。

金鑰要先經服務驗證，您才能新增新使用者。

 Important

SSH 公有金鑰的格式為 `ssh-rsa <string>`。如需如何產生SSH金鑰對的指示，請參閱[為受服務管理的使用者產生SSH金鑰](#)。

9. (選用) 針對金鑰和值，輸入一或多個標籤作為鍵值對，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。

新使用者會出現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操作，透過 AWS Transfer Family 服務傳輸檔案。AWS Transfer Family 支援多個用戶端。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 Cyberduck 和 Open 的程序SSH。

主題

- [使用 Cyberduck](#)
- [使用開啟SSH](#)

使用 Cyberduck

AWS Transfer Family 使用 Cyberduck 傳輸檔案

1. 開啟 [Cyberduck](#) 用戶端。
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. 對於伺服器，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、FTPS和 FTP 伺服器詳細資訊](#)。
5. 對於連接埠號碼，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. 針對SSH私密金鑰，選擇或輸入SSH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，然後將其拖放至 Amazon S3 目錄（目標）。
- 在 Amazon S3 目錄（來源）中，選擇要傳輸的檔案，然後將其拖放至本機目錄（目標）。

使用開啟SSH

使用下列指示，使用 Open 來從命令列傳輸檔案SSH。

Note

此用戶端僅適用於SFTP已啟用的伺服器。

AWS Transfer Family 使用開啟SSH命令列公用程式傳輸檔案

1. 在 Linux 或 Macintosh 上，開啟命令終端機。
2. 在提示中，輸入下列命令：`% sftp -i transfer-key sftp_user@service_endpoint`

在上述命令中，`sftp_user` 是使用者名稱，`transfer-key`是SSH私有金鑰。此處`service_endpoint`是伺服器端點，如所選伺服器的 AWS Transfer Family 主控台所示。

應會出現 `sftp` 提示。

3. （選用）若要檢視使用者的主目錄，請在`sftp`提示中輸入下列命令：`sftp> pwd`
4. 在下一行中，輸入下列文字：`sftp> cd /mybucket/home/sftp_user`

在此入門練習中，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`

put 命令會將檔案傳輸至 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
```

設定用於解密檔案的受管工作流程

本教學課程說明如何設定包含解密步驟的受管工作流程。教學課程也會示範如何將加密檔案上傳至 Amazon S3 儲存貯體，然後檢視相同儲存貯體中的解密檔案。

Note

AWS 儲存部落格有一個文章，說明如何使用 和 加密 [PGP和解密檔案、加密和解密檔案 AWS Transfer Family](#)。

主題

- [步驟 1：設定執行角色](#)
- [步驟 2：建立受管工作流程](#)
- [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金鑰對](#)
- [步驟 5：將PGP私有金鑰存放在 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。中說明建立執行角色的程序[IAM 工作流程的政策](#)。

Note

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](#)。

下列執行角色政策包含成功執行您將在本教學課程中建立的工作流程所需的所有必要許可。若要使用此範例政策，請以您自己的資訊取代 *user input placeholders*。DOC-EXAMPLE-BUCKET 將取代為 Amazon S3 儲存貯體的名稱，您將在其中上傳加密的檔案。

Note

並非每個工作流程都需要此範例中列出的每個許可。您可以根據特定工作流程中的步驟類型來限制許可。每個預先定義步驟類型所需的許可如 所述[使用預先定義的步驟](#)。自訂步驟所需的許可會在 中說明[IAM 自訂步驟的許可](#)。

```
{
  "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：建立受管工作流程

現在您需要建立包含解密步驟的工作流程。

建立包含解密步驟的工作流程

1. 在 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：
 - 輸入描述，例如 **Decrypt workflow example**。
 - 在額定步驟區段中，選擇 新增步驟 。
4. 對於選擇步驟類型，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**。步驟名稱中不允許空格。
 - 針對解密檔案的目的地，選擇 Amazon S3。
 - 針對目的地儲存貯體名稱，選擇您在步驟 1 中建立 IAM 的政策 *DOC-EXAMPLE-BUCKET* 中指定為的相同 Amazon S3 儲存貯體。
 - 針對目的地金鑰字首，輸入您要將解密檔案存放在目的地儲存貯體的字首（資料夾）名稱，例如 **decrypted-files/**。

 Note

請務必將尾斜線（ / ）新增至字首。

- 在此教學課程中，請清除覆寫現有的。清除此設定時，如果您嘗試解密具有相同名稱的現有檔案，工作流程處理會停止，而且不會處理新檔案。

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的工作流程。

請注意新工作流程的工作流程 ID。您需要此 ID 才能進行下一個步驟。本教學課程使用 *w-1234abcd5678efghi* 作為範例工作流程 ID。

步驟 3：將工作流程新增至伺服器並建立使用者

現在您已有一個工作流程與解密步驟，您必須將其與 Transfer Family 伺服器建立關聯。本教學課程說明如何將工作流程連接至現有的 Transfer Family 伺服器。或者，您可以建立新的伺服器以搭配工作流程使用。

將工作流程連接至伺服器後，您必須建立可 SFTP 連線至伺服器的使用者，並觸發工作流程以執行。

設定 Transfer Family 伺服器以執行工作流程

1. 在開啟 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訊區段，然後選擇編輯。
4. 在編輯其他詳細資訊頁面的受管工作流程區段中，選擇您的工作流程，然後選擇對應的執行角色。
 - 針對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：建立受管工作流程](#)，例如 *w-1234abcd5678efghi*。
 - 針對受管工作流程執行角色，選擇您在 中建立 IAM 的角色 [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。

請注意您正在使用的伺服器的 ID。您用來存放PGP金鑰的 AWS Secrets Manager 秘密名稱部分是以伺服器 ID 為基礎。

新增可觸發工作流程的使用者

1. 在 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，然後選擇您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，輸入下列詳細資訊：
 - 對於 User name (使用者名稱)，請輸入 **decrypt-user**。
 - 針對角色，選擇可存取伺服器的使用者角色。
 - 針對主目錄，選擇您先前使用的 Amazon S3 儲存貯體，例如 **DOC-EXAMPLE-BUCKET**。
 - 對於SSH公有金鑰，請將 貼到對應至您擁有之私有金鑰的公有金鑰中。如需詳細資訊，請參閱 [為受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。

請注意此伺服器的 Transfer Family 使用者名稱。秘密部分取決於使用者的名稱。為了簡化，本教學課程使用預設秘密，可供伺服器的任何使用者使用。

步驟 4：建立PGP金鑰對

使用其中一個[支援的PGP用戶端](#)來產生PGP金鑰對。此程序會在 [中](#)詳細說明[產生PGP金鑰](#)。

若要產生PGP金鑰對

1. 對於本教學課程，您可以使用 gpg (GnuPG) 2.0.22 版用戶端來產生金鑰PGP對，以RSA用作加密演算法。對於此用戶端，請執行下列命令，並提供電子郵件地址和密碼片語。您可以使用您喜歡的任何名稱或電子郵件地址。請務必記住您使用的值，因為稍後需要在教學課程中輸入這些值。

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

Note

如果您使用的是 2GnuPG.3.0 版或更新版本，則必須執行 `gpg --full-gen-key`。當系統提示要建立的金鑰類型時，請選擇 RSA 或 ECC。不過，如果您選擇 ECC，請務必選擇 NIST 或 BrainPool 橢圓曲線。請勿選擇 Curve 25519。

2. 執行下列命令來匯出私有金鑰。`user@example.com` 將取代為您產生金鑰時使用的電子郵件地址。

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

此命令會將私有金鑰匯出至 **workflow-tutorial-key.pgp** 檔案。您可以為輸出檔案命名任何您喜歡的名稱。您也可以將私有金鑰檔案新增至之後刪除該私有金鑰檔案 AWS Secrets Manager。

步驟 5：將 PGP 私有金鑰存放在 AWS Secrets Manager

您需要以非常具體的方式將私有金鑰存放在 Secrets Manager 中，以便工作流程在上傳檔案上執行解密步驟時，可以找到私有金鑰。

Note

當您將秘密存放在 Secrets Manager 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 Secrets Manager 中存放 PGP 私有金鑰

1. 登入 AWS Management Console 並在 開啟 AWS Secrets Manager 主控台 <https://console.aws.amazon.com/secretsmanager/>。
2. 在左側導覽窗格中，選擇秘密。
3. 在秘密頁面上，選擇儲存新的秘密。
4. 在選擇秘密類型頁面上，針對秘密類型，選擇其他類型的秘密。
5. 在金鑰/值對區段中，選擇金鑰/值標籤。
 - 金鑰 – 輸入 **PGPPrivateKey**。

- 值 – 將私有金鑰的文字貼到值欄位中。
6. 選擇新增列，然後在鍵/值對區段中，選擇鍵/值索引標籤。
 - 金鑰 – 輸入 **PGPPassphrase**。
 - value – 輸入您在 中產生PGP金鑰對時使用的複雜密碼 [步驟 4：建立PGP金鑰對](#)。
 7. 選擇 Next (下一步)。
 8. 在設定秘密頁面上，輸入秘密的名稱和描述。在此教學課程中，您可以建立所有使用者都可以使用的預設秘密。假設伺服器 ID 為 **s-11112222333344445**，命名秘密 **aws/transfer/s-11112222333344445/pggp-default**。**s-11112222333344445** 以 Transfer Family 伺服器的 ID 取代。輸入秘密的說明。

 Note

若要僅為您先前建立的使用者建立秘密，請命名秘密 **aws/transfer/s-11112222333344445/decrypt-user**。

9. 選擇下一個，然後在設定輪換頁面上接受預設值。然後選擇下一步。
10. 在檢閱頁面上，選擇儲存以建立和儲存秘密。

如需將PGP私有金鑰新增至 Secrets Manager 的詳細資訊，請參閱[使用 AWS Secrets Manager 來存放 PGP 金鑰](#)。

步驟 6：加密檔案

使用 gpg 程式來加密要用於工作流程的檔案。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，**marymajor@example.com** 請以您在建立 PGP 金鑰對時所使用的電子郵件地址取代。
- 此 --openpgp 旗標為選用。此旗標可讓加密的檔案符合 [OpenPGP RFC4880](#) 標準。
- 此命令會在 **testfile.txt.gpg** 與 相同的位置建立名為 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，您可以使用您在步驟 3 中建立的使用者連線到 Transfer Family 伺服器。然後，您可以查看您在步驟 2.5 中指定的 Amazon S3 儲存貯體，設定目的地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. 執行下列命令，*your-endpoint* 以實際端點取代，*transfer-key* 並以您使用者的 SSH 私有金鑰取代：

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

例如，如果私有金鑰存放在 `~/.ssh/decrypt-user`，且您的端點為 `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，此命令將傳回下列項目：

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

您的目錄反映了 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. 針對解密檔案的目的地，您在建立工作流程時指定了 `decrypted-files/` 資料夾。現在，您可以導覽至該資料夾並列出內容。

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

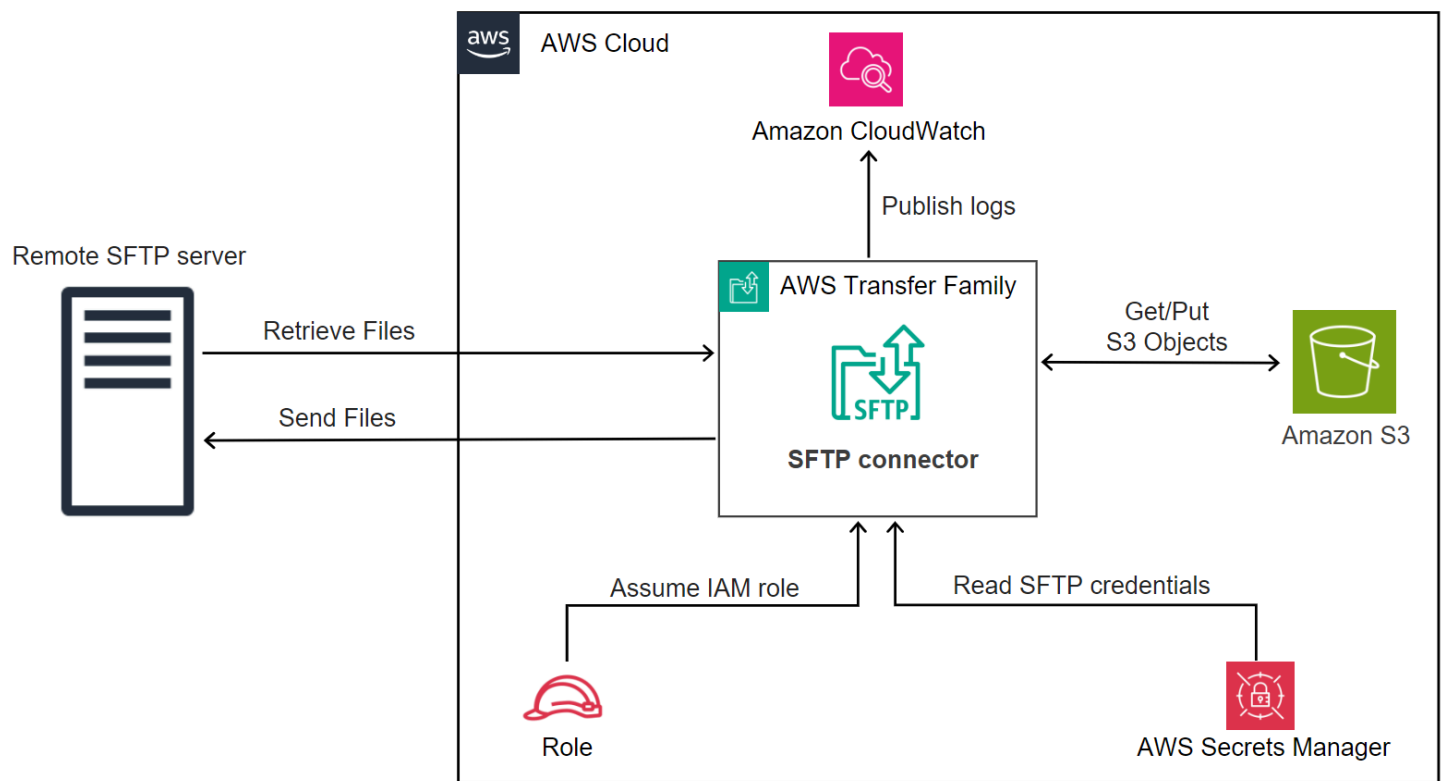
如果成功，`ls` 命令會列出 `testfile.txt` 檔案。您可以下載此檔案，並確認它與您先前加密的原始檔案相同。

設定和使用SFTP連接器

連接器的目的是在 AWS 儲存體與合作夥伴的SFTP伺服器之間建立關係。您可以將檔案從 Amazon S3 傳送至外部的合作夥伴擁有目的地。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 儲存體和SFTP伺服器之間傳輸檔案。

SFTP 連接器會從 擷取SFTP憑證 AWS Secrets Manager，以向遠端SFTP伺服器進行身分驗證並建立連線。連接器會將檔案傳送至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 角色用於允許存取 Amazon S3 儲存貯體和儲存在 Secrets Manager 中的憑證。您也可以登入 Amazon CloudWatch。



主題

- [步驟 1：建立必要的支援資源](#)
- [步驟 2：建立和測試SFTP連接器](#)
- [步驟 3：使用SFTP連接器傳送和擷取檔案](#)
- [建立 Transfer Family 伺服器以用作遠端SFTP伺服器的程序](#)

步驟 1：建立必要的支援資源

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。在此教學課程中，我們使用 AWS Transfer Family 伺服器作為遠端SFTP伺服器。我們需要建立和設定下列資源：

- 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：[建立 Amazon S3 儲存貯體](#)。
- 在 Secrets Manager 中建立存取 Amazon S3 儲存貯體和秘密 AWS Identity and Access Management 的角色：[建立具有必要許可IAM的角色](#)。
- 建立使用SFTP通訊協定的 Transfer Family 伺服器，以及使用SFTP連接器將檔案傳輸到伺服器或從SFTP伺服器傳輸的服務受管使用者：[建立 Transfer Family SFTP 伺服器和使用者的](#)。
- 建立 AWS Secrets Manager 秘密，以存放SFTP連接器用來登入遠端SFTP伺服器的憑證：[在中建立和存放秘密 AWS Secrets Manager](#)。

建立 Amazon S3 儲存貯體

建立 Amazon S3 儲存貯體

1. 在 登入 AWS Transfer Family 主控台<https://console.aws.amazon.com/s3/>。
2. 選擇區域並輸入名稱。

在此教學課程中，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，然後選擇建立儲存貯體。

如需建立 Amazon S3 儲存貯體的完整詳細資訊，請參閱 Amazon Simple Storage Service 使用者指南中的[如何建立 S3 儲存貯體？](#)。

建立具有必要許可IAM的角色

針對存取角色，建立具有下列許可的政策。

下列範例授予必要許可，以存取 **DOC-EXAMPLE-BUCKET** 在 Amazon S3 中，以及存放在 Secrets Manager 中的指定秘密。

```
{  
  "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"
  }
]
}

```

依下列方式取代項目：

- 用於 *DOC-EXAMPLE-BUCKET*，教學課程使用 **s3-storage-east**。
- 用於 *region*，教學課程使用 **us-east-1**。
- 用於 *account-id*，使用您的 AWS 帳戶 ID。

- 用於 *SecretName-6RandomCharacters*，我們 **using sftp-connector1** 是名稱（您將有自己的六個隨機字元作為秘密）。

您還必須確保此角色包含信任關係，允許連接器在服務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](#)。

 Note

若要查看我們用於教學課程的角色詳細資訊，請參閱 [合併使用者和存取角色](#)。

在 中建立和存放秘密 AWS Secrets Manager

我們需要在 Secrets Manager 中存放秘密，才能儲存SFTP連接器的使用者憑證。您可以使用密碼、SSH私有金鑰或兩者。針對教學課程，我們使用私有金鑰。

 Note

當您將秘密存放在 Secrets Manager 時，AWS 帳戶 會產生費用。如需定價的資訊，請參閱 [AWS Secrets Manager 定價](#)。

在開始儲存秘密的程序之前，請擷取並格式化您的私有金鑰。私有金鑰必須與遠端SFTP伺服器上為使用者設定的公有金鑰相對應。在我們的教學課程中，私有金鑰必須對應到為測試使用者儲存在用作遠端伺服器的 Transfer Family SFTP 伺服器上的公有金鑰。

若要執行此操作，請執行下列命令：

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

例如，如果您的私有金鑰檔案位於 `~/.ssh/sftp-testuser-privatekey`，則命令如下所示。

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

這會以正確的格式（包含內嵌的新行字元）將金鑰輸出至標準輸出。將此文字複製到某個位置，因為您需要在下列程序中貼上（步驟 6）。

在 Secrets Manager 中存放SFTP連接器的使用者憑證

1. 登入 AWS Management Console 並在 開啟 AWS Secrets Manager 主控台<https://console.aws.amazon.com/secretsmanager/>。
2. 在左側導覽窗格中，選擇秘密。
3. 在秘密頁面上，選擇儲存新的秘密。
4. 在選擇秘密類型頁面上，針對秘密類型，選擇其他類型的秘密。
5. 在金鑰/值對區段中，選擇金鑰/值標籤。
 - 金鑰 – 輸入 **Username**。
 - value – 輸入我們使用者 的名稱**sftp-testuser**。
6. 若要輸入金鑰，建議您使用純文字索引標籤。
 - a. 選擇新增列，然後輸入 **PrivateKey**。
 - b. 選擇純文字索引標籤。欄位現在包含下列文字：

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

- c. 在空白雙引號 ("") 之間貼上私有金鑰的文字 (先前儲存) 。

您的畫面應如下所示 (索引鍵資料顯示為灰色) 。



7. 選擇 Next (下一步)。

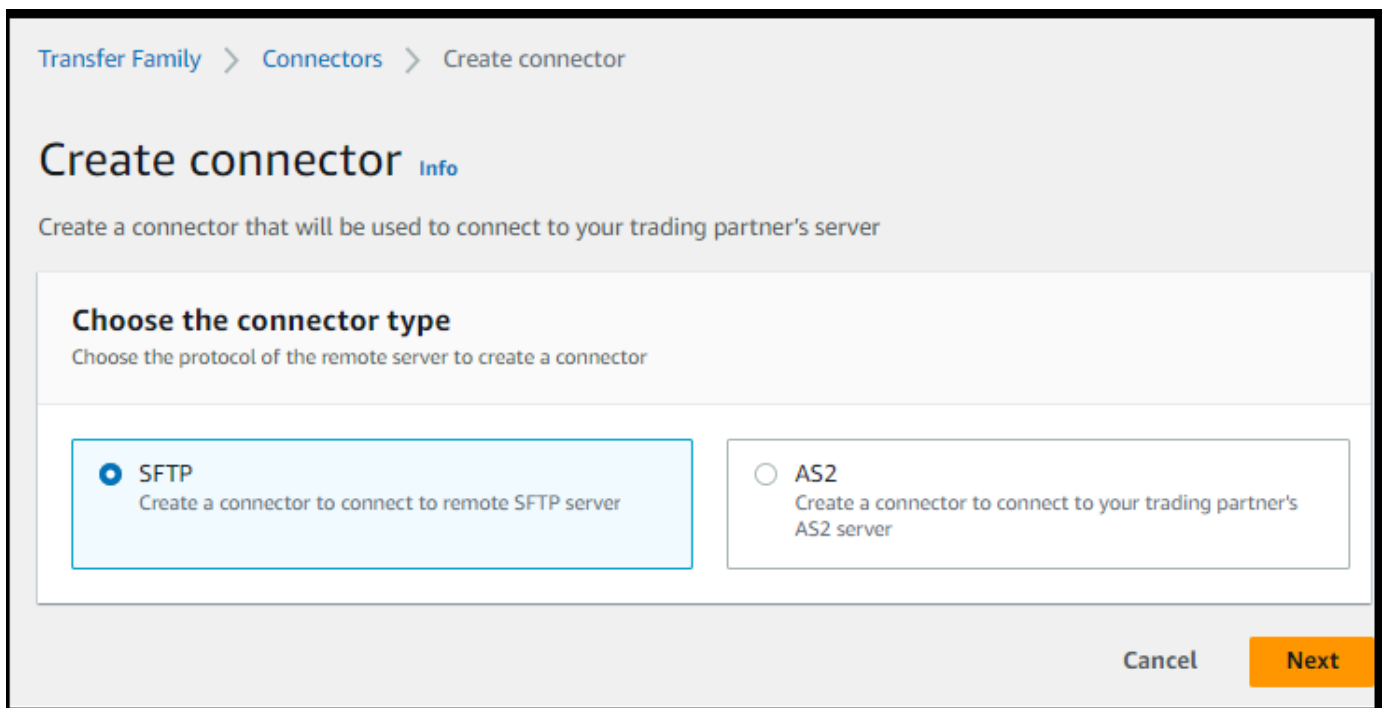
8. 在設定秘密頁面上，輸入秘密的名稱。在本教學課程中，我們會命名秘密 **aws/transfer/sftp-connector1**。
9. 選擇下一個，然後在設定輪換頁面上接受預設值。然後選擇下一步。
10. 在檢閱頁面上，選擇儲存以建立和儲存秘密。

步驟 2：建立和測試SFTP連接器

在本節中，我們會建立使用先前建立的所有資源的SFTP連接器。如需詳細資訊，請參閱[設定SFTP連接器](#)。

若要建立SFTP連接器

1. 在開啟 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. 選擇SFTP連接器類型以建立SFTP連接器，然後選擇下一步。



Transfer Family > Connectors > Create connector

Create connector Info

Create a connector that will be used to connect to your trading partner's server

Choose the connector type

Choose the protocol of the remote server to create a connector

☒ SFTP
Create a connector to connect to remote SFTP server

☐ AS2
Create a connector to connect to your trading partner's AS2 server

Cancel Next

4. 在連接器組態區段中，提供下列資訊：
 - 對於 URL，輸入URL遠端SFTP伺服器的。在教學課程中，我們會輸入用作遠端伺服器的 Transfer Family SFTP 伺服器URL。

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

Replace (取代) **1111aaaa2222bbbb3** 使用您的 Transfer Family 伺服器 ID。

- 針對存取角色，輸入我們先前建立的角色 **sftp-connector-role**。
- 針對記錄角色，選擇 **AWSTransferLoggingAccess**。

 Note

AWSTransferLoggingAccess 是 AWS 受管政策。此政策會在 [中詳細說明AWS 受管政策：AWSTransferLoggingAccess](#)。

Connector configuration

URL

Specify the URL of remote server

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

Access role

IAM Role for Amazon S3 access and AWS Secrets Manager access

sftp-connector-role

Logging role - optional [Info](#)

IAM role for the connector to push events to your CloudWatch logs

AWSTransferLoggingAccess

5. 在SFTP組態區段中，提供下列資訊：

- 針對 Connector 憑證，選擇包含SFTP憑證的 Secrets Manager 資源名稱。針對教學課程，選擇 **aws/transfer/sftp-connector1**。
- 對於信任的主機金鑰，請貼在主機金鑰的公有部分。您可以ssh-keyscan為您的SFTP伺服器執行來擷取此金鑰。如需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。

SFTP configuration Info

Connector credentials
Select the username and password / SSH private key that will be used to connect to the remote server from AWS Secret Manager

aws/transfer/sftp-connector1 [Refresh] [Store a new secret]

Trusted host keys
Connector connects to the remote server only if the SSH public key matches one of the below

ssh-rsa AAA... [Remove]

[Add trusted host key]

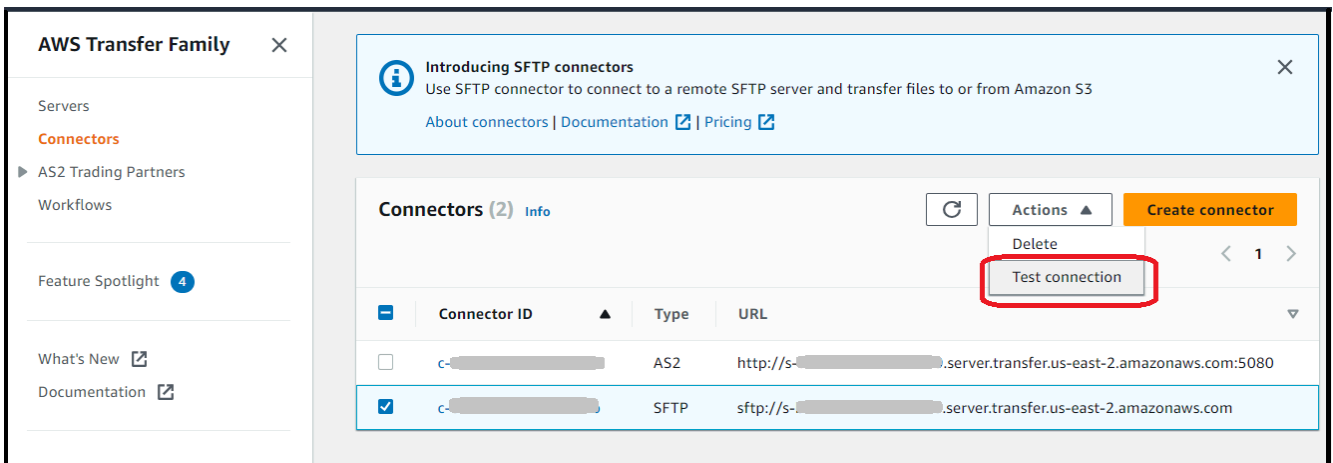
6. 確認所有設定後，請選擇建立連接器以建立SFTP連接器。

建立SFTP連接器之後，建議您先測試連接器，然後再嘗試使用新連接器傳輸任何檔案。

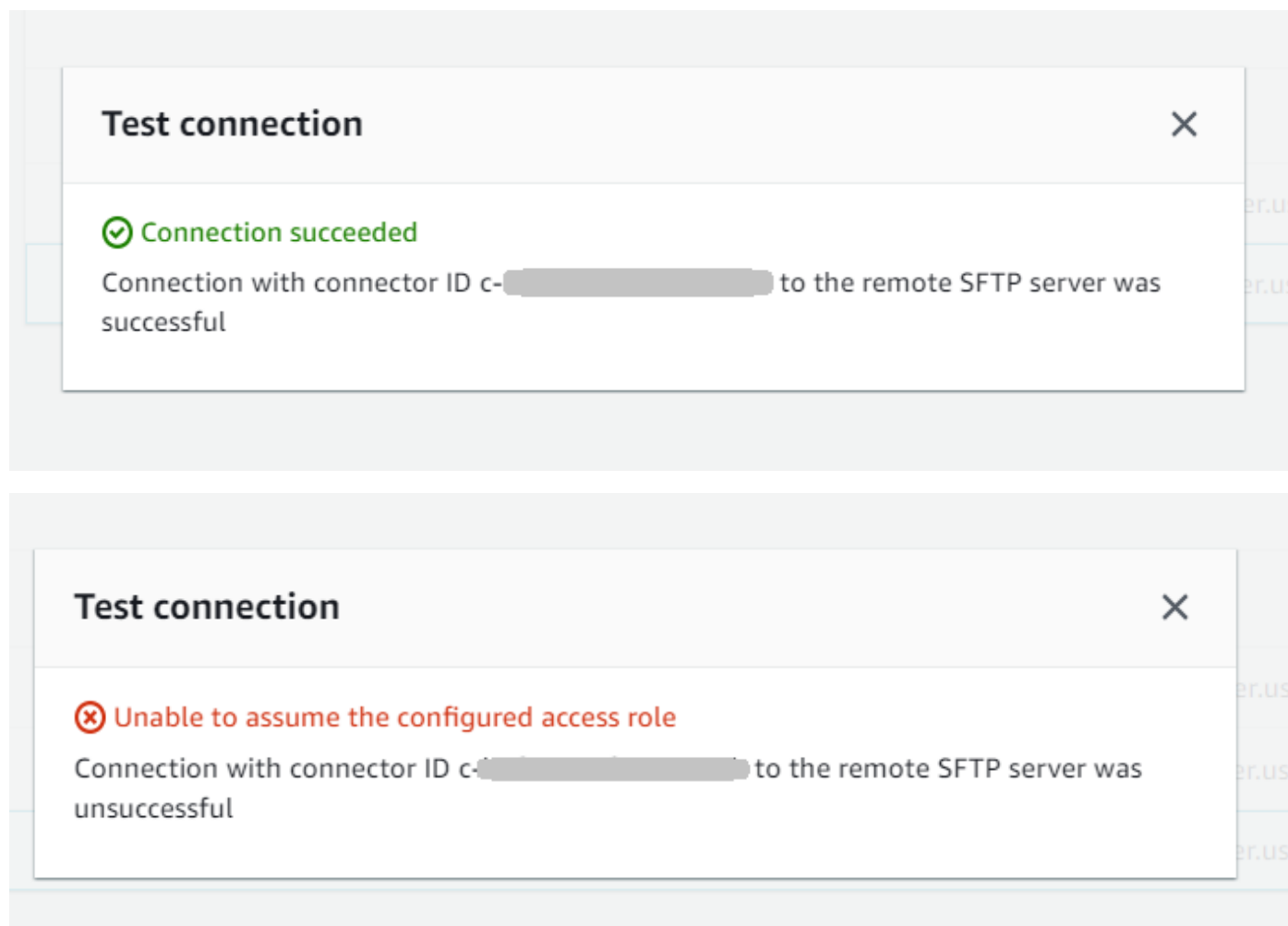
Test a connector using the console

測試SFTP連接器

1. 在開啟 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，然後選擇連接器。
3. 從動作功能表中，選擇測試連線。



系統會傳回訊息，指出測試是否通過或失敗。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（取代 *connector-id* 使用實際連接器 ID）：

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

如果測試成功，則會傳回下列行：

```
{
  "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

為了簡化，我們假設您的 Amazon S3 儲存貯體中已有檔案。

Note

本教學課程使用來源和目的地儲存位置的 Amazon S3 儲存貯體。如果您的SFTP伺服器未使用 Amazon S3 儲存體，則無論您在下列命令`sftp-server-storage-east`中看到什麼位置，都可以將路徑取代為可從SFTP伺服器存取的檔案位置路徑。

- 我們將名為 的檔案`SEND-to-SERVER.txt`從 Amazon S3 儲存傳送至SFTP伺服器。
- 我們將名為 的檔案`RETRIEVE-to-S3.txt`從SFTP伺服器擷取至 Amazon S3 儲存體。

Note

在下列命令中，取代 *connector-id* 您的連接器 ID。

首先，我們將檔案從 Amazon S3 儲存貯體傳送至遠端SFTP伺服器。從命令提示中，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`儲存貯體現在看起來應該像這樣。

Amazon S3 > Buckets > sftp-server-storage-east > incoming/

incoming/

Copy S3 URI

Objects | Properties

Objects (1) Info

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Copy S3 URI Copy URL Download Open Delete Actions Create folder

Upload

< 1 >

☐	Name	Type	Last modified	Size	Storage class
☐	SEND-to-SERVER.txt	txt	December 18, 2023, 10:36:40 (UTC-05:00)	4.1 KB	Standard

如果您未如預期看到檔案，請檢查您的 CloudWatch 日誌。

若要檢查 CloudWatch 日誌

1. 在 開啟 Amazon CloudWatch 主控台 <https://console.aws.amazon.com/cloudwatch/>
2. 從左側導覽功能表中選取日誌群組。
3. 在搜尋列中輸入連接器 ID 以尋找您的日誌。
4. 選取從搜尋傳回的日誌串流。
5. 展開最新的日誌項目。

如果成功，日誌項目如下所示：

```
{
  "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，日誌項目會包含指定問題的錯誤訊息。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。從命令提示中，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，Amazon S3 儲存貯體會包含傳輸的檔案，如下所示。

The screenshot shows the Amazon S3 console interface. At the top, the breadcrumb navigation is 'Amazon S3 > Buckets > s3-storage-east > incoming/'. Below this, the 'incoming/' folder is selected, and a 'Copy S3 URI' button is visible. The 'Objects' tab is active, showing a list of objects. The list has one object, 'RETRIEVE-to-S3.txt', which is a text file (txt) of 4.1 KB, last modified on December 18, 2023, at 10:26:58 (UTC-05:00), with a storage class of 'Standard'. Above the list, there are buttons for 'Copy S3 URI', 'Copy URL', 'Download', 'Open', 'Delete', 'Actions', and 'Create folder'. There is also an 'Upload' button and a search bar labeled 'Find objects by prefix'.

Name	Type	Last modified	Size	Storage class
RETRIEVE-to-S3.txt	txt	December 18, 2023, 10:26:58 (UTC-05:00)	4.1 KB	Standard

如果成功，日誌項目如下所示：

```

{
  "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 伺服器以用作遠端SFTP伺服器的程序

接下來，我們概述建立 Transfer Family 伺服器的步驟，該伺服器可做為本教學課程的遠端SFTP伺服器。注意下列事項：

- 我們使用 Transfer Family 伺服器來代表遠端SFTP伺服器。一般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 伺服器和使用者的程序](#)。
- 由於我們使用 Transfer Family 伺服器，因此我們也使用服務管理SFTP的使用者。此外，為了簡化起見，我們合併了此使用者存取 Transfer Family 伺服器所需的許可，以及他們使用我們的連接器所需的許可。同樣地，大多數SFTP連接器使用案例都有未與 Transfer Family 伺服器相關聯的個別SFTP使用者。請參閱 [建立 Transfer Family SFTP 伺服器和使用者的程序](#)。
- 針對教學課程，由於我們使用 Amazon S3 儲存體做為遠端SFTP伺服器，因此需要建立第二個儲存貯體 **s3-storage-east**，才能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 伺服器和使用者的程序

大多數使用者不需要建立 Transfer Family SFTP 伺服器和使用者的程序，因為您已有具有使用者的SFTP伺服器，而且您可以使用此伺服器來來回傳輸檔案。不過，為了簡化本教學課程，我們使用 Transfer Family 伺服器作為遠端SFTP伺服器。

請遵循 中所述的程序來[建立已啟用 SFTP的伺服器](#)建立伺服器，以及[步驟 3：新增服務受管使用者](#)新增使用者。以下是我們在教學課程中使用的使用者詳細資訊：

- 建立服務受管使用者 `sftp-testuser`。

- 將主目錄設定為 `/sftp-server-storage-east/sftp-testuser`
- 建立使用者時，您會存放公有金鑰。稍後，當您在 Secrets Manager 中建立秘密時，您需要提供對應的私有金鑰。
- 角色：`sftp-connector-role`。針對教學課程，我們同時為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，您可能會有單獨的使用者和存取角色。
- 伺服器主機金鑰：建立連接器時，您需要使用伺服器主機金鑰。您可以`ssh-keyscan`為您的伺服器執行來擷取此金鑰。例如，如果您的伺服器 ID 為 `s-1111aaaa2222bbbb3`，且其端點位於 `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
```

將此文字複製到某個位置，因為您需要將其貼到[步驟 2：建立和測試SFTP連接器](#)程序中。

合併使用者和存取角色

針對教學課程，我們使用單一的合併角色。我們對SFTP使用者以及連接器的存取都使用此角色。下列範例包含此角色的詳細資訊，以防您想要在教學課程中執行任務。

下列範例授予必要許可，以存取 Amazon S3 中的兩個儲存貯體，以及`aws/transfer/sftp-connector1`儲存在 Secrets Manager 中的名為 `SECRET_NAME` 的秘密。對於教學課程，此角色名為 `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"
    }
]
}

```

如需為 Transfer Family 建立角色的完整詳細資訊，請遵循 中所述的程序[建立使用者角色](#)來建立角色。

將 Amazon API Gateway 方法設定為自訂身分提供者

本教學課程說明如何設定 Amazon API Gateway 方法，並將其用作將檔案上傳至 AWS Transfer Family 伺服器的自訂身分提供者。本教學課程僅使用[基本堆疊範本](#)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閘道方法組態](#)
- [步驟 3：檢視 Transfer Family 伺服器詳細資訊](#)
- [步驟 4：測試您的使用者是否可以連線至伺服器](#)

- [步驟 5：測試SFTP連線和檔案傳輸](#)
- [步驟 6：限制對儲存貯體的存取](#)
- [如果使用 Amazon，請更新 Lambda EFS](#)

必要條件

在 中建立 Transfer Family 資源之前 AWS CloudFormation，請建立您的儲存體和使用者角色。

指定儲存體並建立使用者角色

1. 根據您使用的儲存體，請參閱下列文件：
 - 若要建立 Amazon S3 儲存貯體，請參閱 Amazon Simple Storage Service 使用者指南 中的[如何建立 S3 儲存貯體？](#)。
 - 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](#)

在下一節中建立 AWS CloudFormation 堆疊時，您可以輸入儲存體的詳細資訊和使用者角色。

步驟 1：建立 CloudFormation 堆疊

從提供的範本建立 AWS CloudFormation 堆疊

1. 在 <https://console.aws.amazon.com/cloudformation> 開啟 AWS CloudFormation 主控台。
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](#)，並將其貼到 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。請務必執行下列動作：
 - 取代 Username 和 的預設值 UserPassword。
 - 對於 UserHomeDirectory，輸入您先前建立的儲存體（Amazon S3 儲存貯體或 Amazon EFS 檔案系統）的詳細資訊。
 - 將預設值取代 UserRoleArn 為您先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 角色和儲存貯體政策的範例，請參閱 [步驟 6：限制對儲存貯體的存取](#)。

- 如果您想要使用公有金鑰而非密碼進行身分驗證，請在 UserPublicKey1 欄位中輸入公有金鑰。第一次使用連線至伺服器時SFTP，您會提供私有金鑰而非密碼。
7. 選擇下一個，然後在設定堆疊選項頁面上再次選擇下一個。
 8. 檢閱您要建立之堆疊的詳細資訊，然後選擇建立堆疊。

Note

在頁面底部，在功能下，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閘道方法組態

Note

若要提高安全性，您可以設定 Web 應用程式防火牆。AWS WAF 是 Web 應用程式防火牆，可讓您監控轉送至 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](#)。

檢查伺服器的API閘道方法組態並部署

1. 在開啟API閘道主控台<https://console.aws.amazon.com/apigateway/>。
2. 選擇 AWS CloudFormation 範本產生的 Transfer Custom Identity Provider 基本範本API。
3. 在資源窗格中，選擇 GET，然後選擇方法請求。
4. 針對動作，選擇部署 API。針對部署階段，選擇產品，然後選擇部署。

成功部署API閘道方法後，請在階段編輯器區段中檢視其效能。

Note

複製出現在頁面頂端的調用URL地址。下一步需要用到它。

步驟 3：檢視 Transfer Family 伺服器詳細資訊

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

檢視 Transfer Family 伺服器詳細資訊

1. 在 <https://console.aws.amazon.com/cloudformation> 開啟 AWS CloudFormation 主控台。
2. 選擇您建立的堆疊。
3. 選擇 Resources (資源) 標籤。

Resources (18)			
Search resources			
Logical ID ▲	Physical ID ▼	Type ▼	
ApiCloudWatchLogsRole	-ApiCloudWatchLogsRole-	AWS::IAM::Role	
ApiDeployment202008		AWS::ApiGateway::Deployment	
ApiLoggingAccount		AWS::ApiGateway::Account	
ApiStage	prod	AWS::ApiGateway::Stage	
CloudWatchLoggingRole	-CloudWatchLoggingRole-	AWS::IAM::Role	
CustomIdentityProviderApi		AWS::ApiGateway::RestApi	
GetUserConfigLambda	-GetUserConfigLambda-	AWS::Lambda::Function	
GetUserConfigLambdaPermission	GetUserConfigLambdaPermission-	AWS::Lambda::Permission	
GetUserConfigRequest		AWS::ApiGateway::Method	
GetUserConfigResource		AWS::ApiGateway::Resource	
GetUserConfigResponseModel	UserConfigResponseModel	AWS::ApiGateway::Model	
LambdaExecutionRole	-LambdaExecutionRole-	AWS::IAM::Role	
ServerIdResource		AWS::ApiGateway::Resource	
ServersResource		AWS::ApiGateway::Resource	
TransferIdentityProviderRole	-TransferIdentityProviderRole-	AWS::IAM::Role	
TransferServer	arn:aws:transfer:us-east-2: server/s-	AWS::Transfer::Server	
UserNameResource		AWS::ApiGateway::Resource	
UsersResource		AWS::ApiGateway::Resource	

伺服器ARN會顯示在TransferServer資料列的實體 ID 欄中。伺服器 ID 包含在 中ARN，例如 s-11112222333344445。

4. 在 開啟 AWS Transfer Family 主控台<https://console.aws.amazon.com/transfer/>，並在伺服器頁面上選擇新的伺服器。

伺服器 ID 與 中TransferServer資源顯示的 ID 相符 AWS CloudFormation。

步驟 4：測試您的使用者是否可以連線至伺服器

若要測試您的使用者是否可以連線至伺服器，請使用 Transfer Family 主控台

1. 在 開啟 AWS Transfer Family 主控台 <https://console.aws.amazon.com/transfer/>。
2. 在伺服器頁面上，選擇新的伺服器，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登入憑證的文字。這些是您部署 AWS CloudFormation 堆疊時設定的值。
4. 針對伺服器通訊協定 ，選取 SFTP，針對來源 IP ，輸入 **127.0.0.1**。
5. 選擇 測試。

如果使用者身分驗證成功，測試會傳回StatusCode：200HTML回應和JSON物件，其中包含使用者角色和許可的詳細資訊。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，請將閘道API AWS 受管政策之一新增至您用於 的角色API。

步驟 5：測試SFTP連線和檔案傳輸

測試SFTP連線

1. 在 Linux 或 macOS 裝置上，開啟命令終端機。
2. 輸入下列其中一個命令，取決於您使用密碼或金鑰對進行身分驗證。
 - 如果您使用密碼，請輸入此命令：

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

出現提示時，輸入您的密碼。

- 如果您使用的是金鑰對，請輸入此命令：

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

Note

對於這些sftp命令，請插入 Transfer Family 伺服器所在的 AWS 區域 程式碼。例如，如果您的伺服器位於美國東部（俄亥俄），請輸入 **us-east-2**。

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

步驟 6：限制對儲存貯體的存取

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 堆疊和您為使用者選取的政策中使用的設定。

在此範例中，我們為 AWS CloudFormation 堆疊設定下列參數：

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

Important

這是範例密碼。當您設定API閘道方法時，請確定您輸入強式密碼。

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

UserPublicKey1 是您作為公有/私有金鑰對的一部分產生的公有金鑰。

對於您建立的使用者角色而言，*role-id* 是唯一的。附加至 的政策myuser-api-gateway-role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 連線至伺服器SFTP，請在提示中輸入下列其中一個命令。

- 如果您使用密碼進行身分驗證，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。

- 如果您使用金鑰對進行身分驗證，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 命令，請使用 AWS 區域 Transfer Family 伺服器所在的 ID。例如，如果您的伺服器位於美國東部（俄亥俄），請使用 us-east-2。

出現 sftp 提示時，系統會將您導向主目錄，您可以執行 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，請更新 Lambda EFS

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

將 posix 設定檔新增至 Lambda 函數

1. 在開啟 Lambda 主控台 <https://console.aws.amazon.com/lambda/>。
2. 選取您先前建立的 Lambda 函數。Lambda 函數的格式為 **stack-name-GetUserConfigLambda-lambda-identifier**，其中 **stack-name** 是 CloudFormation 堆疊名稱和 **lambda-identifier** 是函數的識別符。
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 response，在 Policy 和 之間新增下列行 HomeDirectory：

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

其中 **uid-value** 以及 **gid-value** 是 0 或更高的整數，分別代表使用者 ID 和群組 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

本教學課程將逐步說明如何使用 設定適用性聲明 2（AS2）組態 AWS Transfer Family。完成此處所述的步驟後，您將擁有AS2啟用的伺服器，已準備好接受來自範例交易合作夥伴AS2的訊息。您也會有一個連接器，可用來傳送訊息AS2給範例交易合作夥伴。

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 使用者指南 [中的安裝或更新最新版本的 AWS CLI](#)。AWS Command Line Interface

1. 為自己和交易合作夥伴建立憑證。如果您有可使用的現有憑證，可以略過本節。

此程序會在 中說明 [步驟 1：為 建立憑證 AS2](#)。

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 地址新增至伺服器，使其面向網際網路。

此程序會在 中說明 [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 伺服器才能進行傳入傳輸。如果您只執行傳出傳輸，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 中說明 [步驟 3：將憑證匯入為 Transfer Family 憑證資源](#)。

4. 若要設定您的交易合作夥伴，請建立本機設定檔和合作夥伴設定檔。

此程序會在 [中說明步驟 4：為您和交易合作夥伴建立設定檔](#)。

5. 建立您與您的交易合作夥伴之間的協議。

此程序會在 [中說明步驟 5：建立您與合作夥伴之間的協議](#)。

 Note

您必須建立僅限傳入傳輸的協議。如果您只執行傳出傳輸，則不需要協議。

6. 在您和您的交易合作夥伴之間建立連接器。

此程序會在 [中說明步驟 6：在您與您的合作夥伴之間建立連接器](#)。

 Note

您必須建立僅限傳出傳輸的連接器。如果您只執行傳入傳輸，則不需要連接器。

7. 測試AS2檔案交換。

此程序會在 [中說明步驟 7：AS2使用 Transfer Family 測試交換檔案](#)。

完成這些步驟後，您可以執行下列動作：

- 使用 Transfer Family `start-file-transfer` AWS Command Line Interface (AWS CLI) 命令將檔案傳送至已啟用遠端 AS2 的合作夥伴伺服器。
- 透過虛擬私有雲端 (VPC) 端點，從連接埠 5080 上已啟用遠端 AS2 的合作夥伴伺服器接收檔案。

步驟 1：為 建立憑證 AS2

AS2 交換中的雙方都需要 X.509 憑證。您可以按照自己喜歡的方式建立這些憑證。本主題說明如何從命令列使用 [OpenSSL](#) 來建立根憑證，然後簽署下級憑證。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，最多為 4096 位元。

若要使用合作夥伴傳輸檔案，請注意下列事項：

- 您可以將憑證連接至設定檔。憑證包含公有或私有金鑰。
- 您的交易合作夥伴會傳送其公有金鑰給您，然後您再將公有金鑰傳送給他們。
- 您的貿易合作夥伴會使用公有金鑰加密訊息，並使用其私有金鑰簽署訊息。相反地，您可以使用合作夥伴的公有金鑰加密訊息，並使用私有金鑰簽署訊息。

 Note

如果您偏好使用 管理金鑰GUI，[Portecle](#) 是您可以使用的一個選項。

若要產生範例憑證

 Important

請勿將私有金鑰傳送給合作夥伴。在此範例中，您會為一方產生一組自我簽署的公有和私有金鑰。如果您要擔任兩個交易合作夥伴進行測試，您可以重複這些指示來產生兩組金鑰：每個交易合作夥伴一個金鑰。在此情況下，您不需要產生兩個根憑證授權機構（CAs）。

1. 執行下列命令，以產生具有 2048 位元長模數的RSA私有金鑰。

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

2. 執行下列命令，使用 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=R00TCA" \  
-key root-ca-key.pem \  
-out root-ca.pem
```

-subj 引數包含下列值。

	名稱	描述
C	國家代碼	組織所在國的雙字母代碼。
ST	狀態、區域或省份	組織所在的州、區域或省。 (在此情況下，區域不會參考您的 AWS 區域。)
L	Locality name (地區名稱)	組織所在的城市。
O	組織名稱	組織的完整法定名稱，包括字尾，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)	在此情況下，我們正在建立根憑證，因此值為 ROOTCA。在這些範例中，我們使用 CN 來描述憑證的目的。

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 Open AS2，會要求您使用相同的憑證來簽署和加密。在此情況下，您可以匯入相同的私有金鑰和憑證，以達成這兩個目的。若要執行此命令，請執行此命令，而非先前的兩個命令：

```
/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請求 (CSRs)。

```
/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，您必須建立 signing-cert.conf 檔案和 encryption-cert.conf 檔案。

- 使用文字編輯器建立具有下列內容 signing-cert.conf 的檔案：

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

- 使用文字編輯器建立具有下列內容 encryption-cert.conf 的檔案：

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

6. 最後，您可以執行下列命令來建立簽署的憑證。

```
/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 AS2 已啟用的伺服器 AWS CLI。

Note

許多範例步驟使用從檔案載入參數的命令。如需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](#)。

如果您想要改為使用 主控台，請參閱 [使用 Transfer Family 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 `create-server` AWS CLI 命令的 `--protocols AS2` 參數來建立AS2已啟用的伺服器。目前，Transfer Family 僅支援VPC端點類型和具有AS2通訊協定的 Amazon S3 儲存體。

當您使用 `create-server`命令為 Transfer Family 建立AS2已啟用的伺服器時，系統會自動為您建立VPC端點。此端點公開TCP連接埠 5080，以便接受AS2訊息。

如果您想要公開將VPC端點公開暴露至網際網路，您可以將彈性 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：

- 您的 ID VPC (例如 `vpc-abcdef01`)。
- VPC 子網路IDs的 (例如子網路 `abcdef01`、`subnet-subnet-abcdef01`、子網路 `021345ab`)。
- 一或多個IDs安全群組，允許來自交易合作夥伴的TCP連接埠 5080 傳入流量 (例如 `sg-1234567890abcdef0` 和 `sg-abcdef01234567890`)。
- (選用) 您要與VPC端點建立關聯的彈性 IP 地址。
- 如果您的交易合作夥伴未VPC透過 連線至您的 VPN，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線至網際網路](#)。

若要建立AS2已啟用的伺服器

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. (選用) 您可以公開VPC端點。您只能透過 `update-server`操作將彈性 IP 地址連接至 Transfer Family 伺服器。下列命令會停止伺服器、使用彈性 IP 地址進行更新，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有 IP 地址DNS的記錄。若要讓您的交易合作夥伴存取伺服器，您需要提供他們下列資訊。在此情況下，*your-region*會參考您的 AWS 區域。

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

URL 您提供給交易合作夥伴的完整內容如下：

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

- 若要測試AS2已啟用的伺服器是否可以存取，請使用下列命令。請確定您的伺服器可以透過VPC端點的私有DNS地址或透過公有端點存取（如果您將彈性 IP 地址與端點建立關聯）。

如果您的伺服器設定正確，連線將會成功。不過，由於您未傳送有效AS2訊息，因此會收到HTTP狀態碼 400（錯誤請求）回應。

- 對於公有端點（如果您在上一個步驟中與彈性 IP 地址相關聯），請執行下列命令，以取代您的伺服器 ID 和區域。

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

- 如果您要在中連線VPC，請執行下列命令來查詢VPC端點的私有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 ID。使用此值來執行下列命令。

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

此describe-vpc-endpoints命令會傳回具有數個DnsName參數的DNSEntries陣列。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，下列命令顯示上一個命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. (選用) 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。若要提供 Transfer Family 存取您帳戶中的 CloudWatch 日誌，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`，並連接 `AWSTransferLoggingAccess` 受管政策。如需詳細資訊，請參閱 [建立IAM角色和政策](#)。請注意您剛建立之IAM角色的 Amazon Resource Name (ARN)，並執行下列 `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，我們強烈建議進行設定，以便您可以查看訊息的狀態並對組態問題進行疑難排解。

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。如果您想要改為使用 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。如果您使用相同的憑證進行加密和簽署，請匯入相同的憑證兩次（一次使用 `SIGNING`，另一次 `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
```

此命令會傳回您的簽署 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
```

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

接下來，執行下列命令來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
```

此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
```

此命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：為您和交易合作夥伴建立設定檔

此程序說明如何使用 建立 AS2 設定檔 AWS CLI。如果您想要改為使用 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。此命令參考包含公有和私有金鑰的憑證。

```
aws transfer create-profile --as2-id MYCORP --profile-type LOCAL --certificate-ids \  
my-signing-cert-id my-encrypt-cert-id
```

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

現在執行下列命令來建立合作夥伴設定檔。此命令只會使用您合作夥伴的公有金鑰憑證。若要使用此命令，*user input placeholders* 請以您自己的資訊取代；例如，合作夥伴 AS2 的名稱和憑證 IDs。

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

此命令會傳回合作夥伴的設定檔 ID。在下一節中，此 ID 稱為 *partner-profile-id*。

Note

在先前的命令中，取代 *MYCORP* 您組織的名稱，以及 *PARTNER-COMPANY* 交易合作夥伴組織的名稱。

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協議 AWS CLI。如果您想要改為使用 Transfer Family 主控台，請參閱 [the section called “建立AS2協議”](#)。

協議將兩個設定檔（本機和合作夥伴）、其憑證和允許雙方之間傳入AS2傳輸的伺服器組態集合在一起。您可以執行下列命令來列出項目。

```
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，具有對儲存貯體的讀取/寫入存取權。建立此角色的指示與 Transfer Family SFTP、和 FTPS 通訊協定相同FTP，可在 中使用 [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（以及物件字首，如果指定的話）
- 可存取儲存貯體ARNIAM的角色的
- 您的 Transfer Family 伺服器 ID
- 您的設定檔 ID 和合作夥伴的設定檔 ID

執行下列命令來建立協議。

```
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，此命令會傳回協議的 ID。然後，您可以使用下列命令檢視協議的詳細資訊。

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

步驟 6：在您與您的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。如果您想要改為使用 Transfer Family 主控台，請參閱 [the section called “設定 AS2 連接器”](#)。

您可以使用 StartFileTransferAPI 操作，透過連接器將存放在 Amazon S3 中的檔案傳送至交易合作夥伴的 AS2 端點。您可以執行下列命令，找到先前建立的設定檔。

```
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 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，因為它是較弱的加密演算法。

然後執行下列命令來建立連接器。


```
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
```

步驟 7：AS2使用 Transfer Family 測試交換檔案

從交易合作夥伴接收檔案

如果您將公有彈性 IP 地址與VPC端點建立關聯，Transfer Family 會自動建立包含公有 IP 地址DNS的名稱。子網域是您的 AWS Transfer Family 伺服器 ID（格式為 s-1234567890abcdef0）。以下列格式將伺服器URL提供給交易合作夥伴。

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

如果您沒有將公有彈性 IP 地址與VPC端點建立關聯，請查詢端點的主機名稱，該VPC端點可以接受連接埠 5080 上HTTPPOST交易合作夥伴AS2的訊息。若要擷取VPC端點詳細資訊，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 IDvpce-1234abcd5678efghi。然後，您可以使用下列命令來擷取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的VPC端點的所有詳細資訊。

DNS 名稱會列在DnsEntries陣列中。您的交易合作夥伴必須位於 內VPC，才能存取您的VPC端點（例如透過 AWS PrivateLink 或 VPN）。以下列格式將您的VPC端點URL提供給合作夥伴。

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

例如，以下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 `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](#)。如果我們成功接收名為 `myfile1.txt` 和 `myfile2.txt` 的檔案，檔案會儲存為 `/path-defined-in-the-agreement/processed/original_filename.messageId.original_extension`。在這裡，檔案會儲存為 `/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，您也可以檢查 CloudWatch 日誌中的 AS2 訊息狀態。

將檔案傳送至您的交易合作夥伴

您可以使用 Transfer Family，參考連接器 ID 和檔案路徑來 AS2 傳送訊息，如下列 `start-file-transfer` AWS Command Line Interface (AWS CLI) 命令所示：

```
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訊，請執行下列命令：

```
aws transfer list-connectors
```

`list-connectors` 命令會傳回連接器的連接器 IDs、URLs 和 Amazon Resource Names (ARNs)。

若要傳回特定連接器的屬性，請使用您要使用的 ID 執行下列命令：

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

`describe-connector` 命令會傳回連接器的所有屬性，包括其 URL、角色、設定檔、訊息處置通知 (MDNs)、標籤和監控指標。

您可以檢視 JSON 和 檔案，確認合作夥伴已成功收到 MDN 檔案。這些檔案是根據中所述的慣例命名 [檔案名稱和位置](#)。如果您在建立連接器時設定了記錄角色，您也可以檢查 CloudWatch 日誌是否有 AS2 訊息的狀態。

設定 SFTP、FTPS或 FTP 伺服器端點

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

主題

- [身分提供者選項](#)
- [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](#)
- [使用邏輯目錄來簡化 Transfer Family 目錄結構](#)

身分提供者選項

AWS Transfer Family 提供數種驗證和管理使用者的方法。下表比較您可以與 Transfer Family 搭配使用的可用身分提供者。

動作	AWS Transfer Family 服務受管	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
金鑰型身分驗證	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
邏輯主目錄	是	是	是	是

動作	AWS Transfer Family 服務受管	AWS Managed Microsoft AD	Amazon API Gateway	AWS Lambda
參數化存取（以使用者名稱為基礎）	是	是	是	是
臨時存取結構	是	否	是	是
AWS WAF	否	否	是	否

備註：

- IAM 用於控制 Amazon S3 後端儲存體的存取，並POSIX用於 Amazon EFS。
- Ad hoc 是指在執行階段傳送使用者設定檔的功能。例如，您可以透過傳遞使用者名稱作為變數，將使用者登陸到其主目錄中。
- 如需的詳細資訊 AWS WAF，請參閱 [新增 Web 應用程式防火牆](#)。
- 有一篇部落格文章描述使用與 Microsoft Azure AD 整合的 Lambda 函數作為 Transfer Family 身分提供者。如需詳細資訊，請參閱[AWS Transfer Family 使用 Azure Active Directory 和 向 驗證 AWS Lambda](#)。
- 我們提供多個 AWS CloudFormation 範本，協助您快速部署使用自訂身分提供者的 Transfer Family 伺服器。如需詳細資訊，請參閱 [Lambda 函數範本](#)。

在下列程序中，您可以建立SFTP已啟用的伺服器、已啟用 FTPS的伺服器、已啟用 FTP的伺服器或已啟用 AS2的伺服器。

下一步驟

- [建立已啟用 SFTP的伺服器](#)
- [建立已啟用 FTPS的伺服器](#)
- [建立已啟用 FTP的伺服器](#)
- [設定 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徵。

端點類型矩陣

特性	公有	VPC - 網路	VPC - 內部	VPC_端點 (已棄用)
支援的通訊協定	SFTP	SFTP, FTPS, AS2	SFTP, FTP, FTPS, AS2	SFTP
存取	透過網際網路從。此端點類型不需要在您的中進行任何特殊組態VPC。	透過網際網路以及來自 VPC和 VPC連線環境，例如透過 AWS Direct Connect 或的內部部署資料中心VPN。	從內部 VPC 和 VPC連線的環境，例如透過 AWS Direct Connect 或的內部部署資料中心VPN。	從內部 VPC 和 VPC連線的環境，例如透過 AWS Direct Connect 或的內部部署資料中心VPN。
靜態 IP 地址	您無法連接靜態 IP 地址。AWS 提供可能變更的 IP 地址。	您可以將彈性 IP 地址連接至端點。這些可以是 AWS擁有的 IP 地址或您自己的 IP 地址 (攜帶您自己的 IP 地址)。連接至端點的彈性 IP 地址不會變更。 連接到伺服器的私有 IP 地址也不會變更。	連接至端點的私有 IP 地址不會變更。	連接至端點的私有 IP 地址不會變更。
來源 IP 允許清單	此端點類型不支援依來源 IP 地址允許清單。	若要依來源 IP 地址允許存取，您可以使用連接至伺服器端點的	若要依來源 IP 地址允許存取，您可以使用連接至伺服器端點的安	若要依來源 IP 地址允許存取，您可以使用連接至伺服器端點的

特性	公有	VPC - 網路	VPC - 內部	VPC_端點 (已棄用)
	端點可公開存取，並接聽連接埠 22 的流量。  Note 對於VPC託管的端點，SFTPTransfer Family 伺服器可以透過連接埠 22 (預設) 或連接埠 2222 操作。	安全群組，以及 ACLs連接至端點所在的子網路的安全群組。	全群組，以及連接至端點所在的子網路的網路存取控制清單 (網路 ACLs) 。	安全群組，以及 ACLs連接至端點所在的子網路的安全群組。
用戶端防火牆允許清單	您必須允許伺服器DNS的名稱。 由於 IP 地址可能會變更，請避免將 IP 地址用於用戶端防火牆允許清單。	您可以允許伺服器DNS的名稱或連接到伺服器的彈性 IP 地址。	您可以允許私有 IP 地址或端點 DNS的名稱。	您可以允許私有 IP 地址或端點 DNS的名稱。

 Note

VPC_ENDPOINT 端點類型現在已棄用，無法用來建立新的伺服器。不使用 EndpointType=VPC_ENDPOINT，請使用新的VPC端點類型 (EndpointType=VPC)，

您可以將其作用面向內部或面向網際網路，如上表所述。如需詳細資訊，請參閱 [停止使用 VPC_ENDPOINT](#)。

請考慮下列選項，以提高伺服器的安全狀態 AWS Transfer Family：

- 使用具有內部存取權的VPC端點，以便伺服器只能透過或存取您 VPC或 VPC連線環境中的用戶端，例如內部部署資料中心 AWS Direct Connect VPN。
- 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，請使用具有面向網際網路存取的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 地址的流量。
- 如果您需要以密碼為基礎的身分驗證，且搭配伺服器使用自訂身分提供者，則您的密碼政策最佳實務是防止使用者建立較弱的密碼，並限制失敗的登入嘗試次數。
- AWS Transfer Family 是受管服務，因此不提供 Shell 存取。您無法直接存取基礎SFTP伺服器，以在 Transfer Family 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 變更為不同的連接埠。這可以降低連接埠掃描器和機器人探查伺服器的風險，但不能消除，因為連接埠 22 最常用於掃描。如需詳細資訊，請參閱部落格文章 [Network Load Balancer 現在支援安全群組](#)。

Note

如果您使用 Network Load Balancer，AWS Transfer Family CloudWatch 日誌會顯示的 IP 地址NLB，而不是實際的用戶端 IP 地址。

設定 SFTP、FTPS或 FTP 伺服器端點

您可以使用 AWS Transfer Family 服務建立檔案傳輸伺服器。下列檔案傳輸通訊協定可供使用：

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

Note

我們提供建立 SFTP Transfer Family 伺服器 AWS CDK 的範例。此範例使用 TypeScript、和，可於 GitHub [此處取得](#)。

- 檔案傳輸通訊協定安全 (FTPS) – 使用TLS加密進行檔案傳輸。如需詳細資訊，請參閱 [the section called “建立已啟用 FTPS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 “建立已啟用 FTP的伺服器”](#)。
- 適用性陳述式 2 (AS2) – 用於傳輸結構化 business-to-business資料的檔案傳輸。如需詳細資訊，請參閱 [the section called “設定 AS2”](#)。對於 AS2，您可以快速建立 AWS CloudFormation 堆疊以供示範之用。此程序說明於 [使用 範本建立示範 Transfer Family AS2堆疊](#)。

您可以使用多個通訊協定建立伺服器。

 Note

如果您針對相同的伺服器端點啟用了多個通訊協定，並且想要在多個通訊協定上使用相同的使用者名稱來提供存取權，只要身分提供者已設定了通訊協定的特定憑證，您就可以這麼做。對於 FTP，我們建議您與 SFTP和 保持單獨的憑證FTPS。這是因為與 SFTP和 不同FTPS，會以純文字FTP傳輸憑證。透過從 SFTP 或 隔離FTP憑證FTPS，如果共用或公開FTP憑證，您的工作負載會使用 SFTP或 FTPS 保持安全。

建立伺服器時，您可以選擇特定 AWS 區域 來執行指派給該伺服器之使用者的檔案操作請求。除了指派伺服器一或多個通訊協定之外，您還可以指派下列其中一種身分提供者類型：

- 使用SSH金鑰 管理服務。如需詳細資訊，請參閱 [使用服務受管使用者](#)。
- AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD)。此方法可讓您整合 Microsoft Active Directory 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 身分提供者](#)。
- 自訂方法。自訂身分提供者方法使用 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 [使用自訂身分提供者](#)。Transfer Family 提供 AWS CloudFormation 範本，可用來快速部署使用自訂身分提供者的伺服器。
 - [用於身分驗證的 Lambda 函數](#) 說明使用 Lambda 函數進行身分驗證的 CloudFormation 範本。
 - [使用API閘道方法進行驗證](#) 說明 CloudFormation使用 Amazon API Gateway 方法進行身分驗證的範本。

您也可以使用預設伺服器端點，或使用 Amazon Route 53 服務，或使用您選擇的網域名稱系統（ ）服務，來指派端點類型（公開存取或VPC託管DNS）和主機名稱給伺服器。伺服器主機名稱在其建立 AWS 區域 的 中必須是唯一的。

此外，您可以指派 Amazon CloudWatch 記錄角色，將事件推送至 CloudWatch 日誌，選擇包含啟用供伺服器使用的密碼編譯演算法的安全政策，並以鍵值對的標籤形式將中繼資料新增至伺服器。

Important

您需為現代化伺服器和資料傳輸支付費用。如需有關定價和 的資訊 [AWS 定價計算工具](#)，用於取得使用 Transfer Family 的成本估算，請參閱[AWS Transfer Family 定價](#)。

建立已啟用 SFTP的伺服器

Secure Shell（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。通訊協定支援 的完整安全和身分驗證功能SSH。它廣泛用於交換資料，包括金融服務、醫療保健、零售和廣告等各種產業的業務合作夥伴之間的敏感資訊。

Note

SFTP 適用於 Transfer Family 的 伺服器透過連接埠 22 運作。對於 VPC託管的端點，SFTPTransfer Family 伺服器也可以透過連接埠 2222 操作。如需詳細資訊，請參閱 [在虛擬私有雲端中建立伺服器](#)。

另請參閱

- 我們提供建立 SFTP Transfer Family 伺服器 AWS CDK 的範例。此範例使用 TypeScript、 和 ，可於 GitHub [此處取得](#)。
- 如需如何在 內部署 Transfer Family 伺服器的詳細資訊VPC，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SFTP已啟用的伺服器

- 在 開啟 AWS Transfer Family 主控台<https://console.aws.amazon.com/transfer/>，然後從導覽窗格中選取伺服器，然後選擇建立伺服器。
- 在選擇通訊協定 中，選取 SFTP，然後選擇下一步。

Choose protocols

Select the protocols you want to enable [Info](#)

Choose one or more file transfer protocols over which clients can connect to your server's endpoint

- ☒ SFTP (SSH File Transfer Protocol) - file transfer over Secure Shell
- ☐ AS2 (Applicability Statement 2) - messaging protocol for exchanging business-to-business data [Info](#)
- ☐ FTPS (File Transfer Protocol Secure) - file transfer protocol with TLS encryption
- ☐ FTP (File Transfer Protocol) - unencrypted file transfer protocol

[Cancel](#) [Next](#)

3. 在選擇身分提供者 中，選擇您要用來管理使用者存取權的身分提供者。您有下列選項：

- 服務受管：您可以在 中存放使用者身分和金鑰 AWS Transfer Family。

Choose an identity provider

Identity provider

Identity provider type
An identity provider manages user access for authentication and authorization

☒ **Service managed**
Create and manage users within the service

☐ **AWS Directory Service** [Info](#)
Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☐ **Custom Identity Provider** [Info](#)
Manage users by integrating an identity provider of your choice

[Cancel](#) [Previous](#) [Next](#)

- AWS Directory Service for Microsoft Active Directory – 您提供一個 AWS Directory Service 目錄來存取端點。如此一來，您可以使用儲存在 Active Directory 中的憑證來驗證使用者。若要進一步了解如何使用 AWS Managed Microsoft AD 身分提供者，請參閱 [使用 AWS Directory Service 身分提供者](#)。

Note

- 不支援跨帳戶和共用目錄 AWS Managed Microsoft AD。

- 若要使用 Directory Service 作為身分提供者來設定伺服器，您需要新增一些 AWS Directory Service 許可。如需詳細資訊，請參閱 [開始使用 之前 AWS Directory Service for Microsoft Active Directory](#)。

Choose an identity provider

Identity provider

Identity provider type
An identity provider manages user access for authentication and authorization

☐ Service managed
Create and manage users within the service

☒ AWS Directory Service [Info](#)
Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☐ Custom Identity Provider [Info](#)
Manage users by integrating an identity provider of your choice

Directory

TATER3

Cancel Previous Next

- 自訂身分提供者 – 選擇下列其中一個選項：
 - 使用 AWS Lambda 來連接身分提供者 – 您可以使用現有的身分提供者，並由 Lambda 函數提供支援。您提供 Lambda 函數的名稱。如需詳細資訊，請參閱[使用 AWS Lambda 整合您的身分提供者](#)。
 - 使用 Amazon API Gateway 來連接您的身分提供者 – 您可以建立由 Lambda 函數支援的 API 閘道方法，以用作身分提供者。您提供 Amazon API Gateway URL 和調用角色。如需詳細資訊，請參閱[使用 Amazon API Gateway 整合您的身分提供者](#)。

對於任一選項，您也可以指定如何驗證。

- 密碼或金鑰 – 使用者可以使用其密碼或金鑰進行身分驗證。這是預設值。
- 密碼 ONLY – 使用者必須提供密碼才能連線。
- 金鑰 ONLY – 使用者必須提供其私有金鑰才能連線。

- 密碼AND金鑰 – 使用者必須提供其私有金鑰和密碼才能連線。伺服器會先檢查金鑰，如果金鑰有效，系統會提示輸入密碼。如果提供的私有金鑰與儲存的公有金鑰不相符，身分驗證會失敗。

Choose an identity provider

Identity Provider for SFTP, FTPS, or FTP

Identity provider type
An identity provider manages user access for authentication and authorization

- ☐ Service managed
Create and manage users within the service
- ☐ AWS Directory Service [Info](#)
Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS
- ☒ Custom Identity Provider [Info](#)
Manage users by integrating an identity provider of your choice

☒ Use AWS Lambda to connect your identity provider [Info](#)
Invoke an AWS Lambda function to call your identity provider's API for user authentication and authorization

☐ Use Amazon API Gateway to connect your identity provider [Info](#)
Use a RESTful API method to call your identity provider's API for user authentication and authorization

AWS Lambda function

Choose a Lambda function ▼

Authentication methods
Choose which authentication methods are required for users to connect to your server

- ☒ Password OR public key
- ☐ Password ONLY
- ☐ Public Key ONLY
- ☐ Password AND public key

Either a valid password or valid private key will be required during user authentication

Cancel Previous **Next**

4. 選擇 Next (下一步)。
5. 在選擇端點 中，執行下列動作：
 - a. 針對端點類型，選擇可公開存取的端點類型。如需VPC託管端點，請參閱 [在虛擬私有雲端中建立伺服器](#)。
 - b. (選用) 針對自訂主機名稱，選擇無。

您可以取得 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。若要進一步了解如何使用自訂主機名稱，請參閱 [使用自訂主機名稱](#)。

- c. （選用）針對 FIPS 已啟用，選取 FIPS 已啟用端點核取方塊，以確保端點符合聯邦資訊處理標準（FIPS）。

Note

FIPS 啟用的端點僅適用於北美 AWS 區域。如需可用區域的資訊，請參閱中的 [AWS Transfer Family 端點和配額](#) AWS 一般參考。如需的詳細資訊 FIPS，請參閱 [聯邦資訊處理標準（FIPS）140-2](#)。

- d. 選擇 Next (下一步)。

Choose an endpoint

Endpoint configuration [Info](#)

Endpoint type
Select whether the endpoint will be publicly accessible or hosted inside your VPC

☒ **Publicly accessible**
Accessible over the internet

☐ **VPC hosted** [Info](#)
Access controlled using Security Groups

Custom hostname
Specify a custom alias for your server endpoint.

None ▼

FIPS Enabled
Select whether the endpoint should comply with Federal Information Processing Standards (FIPS)

☐ FIPS Enabled endpoint

Cancel Previous Next

6. 在選擇網域頁面上，選擇您要用來透過所選通訊協定存放和存取資料的 AWS 儲存服務：

- 選擇 Amazon S3 以儲存和存取檔案作為所選通訊協定上的物件。
- 選擇 Amazon EFS，透過選取的通訊協定將檔案存放和存取到您的 Amazon EFS 檔案系統中。

選擇 Next (下一步)。

7. 在設定其他詳細資訊 中，執行下列動作：

- a. 若要記錄，請指定現有的日誌群組或建立新的日誌群組（預設選項）。

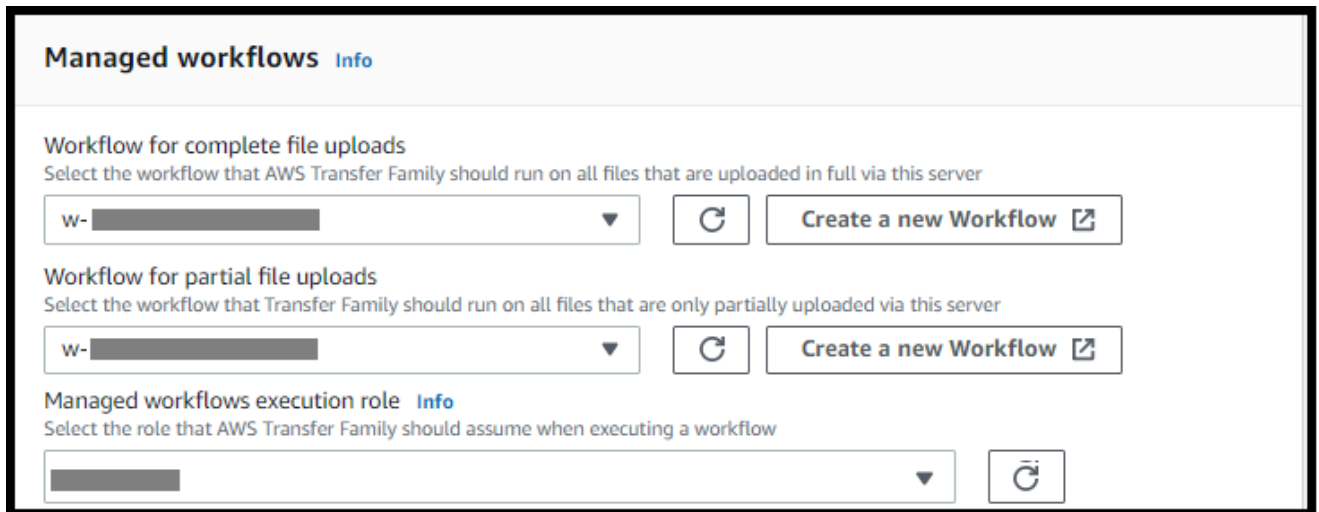
The screenshot shows the 'Configure additional details' step in the AWS Transfer Family console. The left sidebar lists steps 1 through 6, with step 5, 'Configure additional details', highlighted. The main content area is titled 'Configure additional details' and contains a 'Logging' section. Under 'Log group', the option 'Create a new log group' is selected with a radio button. Below this is a dropdown menu showing '/aws/transfer/' and a 'Create log group' button. The 'Logging role' section has 'Create a new role' selected. A note at the bottom states: 'Logging role is only required when selecting a workflow in the Managed workflows section below.'

如果您選擇現有的日誌群組，您必須選取與 相關聯的日誌群組 AWS 帳戶。

This screenshot is similar to the previous one but shows the 'Choose an existing log group' radio button selected. The dropdown menu for the log group is now populated with a specific path: '/aws/transfer/'. The 'Create log group' button is still present. The 'Logging role' section remains the same with 'Create a new role' selected. The same note about the logging role requirement is displayed at the bottom.

如果您選擇建立日誌群組，CloudWatch 主控台（<https://console.aws.amazon.com/cloudwatch/>）會開啟建立日誌群組頁面。如需詳細資訊，請參閱在 [日誌中建立 CloudWatch 日誌群組](#)。

- b. (選用) 針對受管工作流程，選擇 Transfer Family 在執行工作流程時應擔任的工作流程 IDs (和對應的角色)。您可以選擇一個工作流程在完整上傳時執行，另一個工作流程在部分上傳時執行。若要進一步了解如何使用受管工作流程處理檔案，請參閱 [AWS Transfer Family 受管工作流程](#)。



Managed workflows [Info](#)

Workflow for complete file uploads
Select the workflow that AWS Transfer Family should run on all files that are uploaded in full via this server

w- [redacted] ↗

Workflow for partial file uploads
Select the workflow that Transfer Family should run on all files that are only partially uploaded via this server

w- [redacted] ↗

Managed workflows execution role [Info](#)
Select the role that AWS Transfer Family should assume when executing a workflow

[redacted]

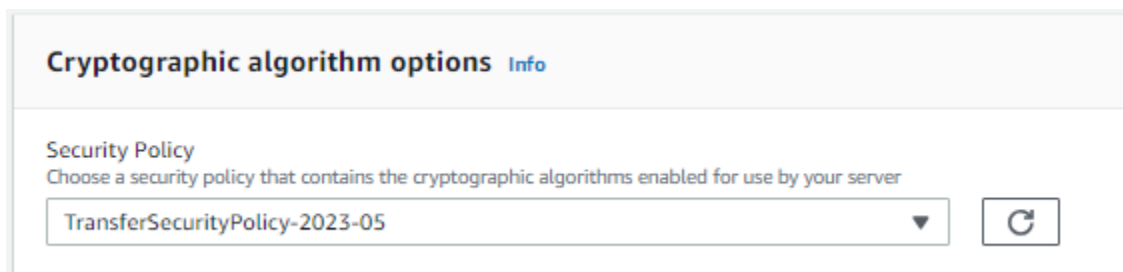
- c. 針對密碼編譯演算法選項，選擇包含啟用供伺服器使用之密碼編譯演算法的安全政策。

Note

根據預設：

- 如果未選取FIPS已啟用端點，則TransferSecurityPolicy-2020-06安全政策會連接至您的伺服器。
- 如果選取FIPS已啟用端點，則TransferSecurityPolicy-FIPS-2020-06安全政策會連接至您的伺服器。

如需關於安全政策的詳細資訊，請參閱[安全政策 AWS Transfer Family](#)。



Cryptographic algorithm options [Info](#)

Security Policy
Choose a security policy that contains the cryptographic algorithms enabled for use by your server

TransferSecurityPolicy-2023-05

- d. (選用) 對於伺服器主機金鑰，輸入 RSA、ED25519 或 ECDSA 私有金鑰，當用戶端透過連線到伺服器時，該金鑰將用於識別您的伺服器 SFTP。您也可以新增描述，以區分多個主機金鑰。

建立伺服器後，您可以新增其他主機金鑰。如果您想要輪換金鑰，或想要擁有不同類型的金鑰，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已啟用 SFTP 的現有伺服器遷移使用者。

Server Host Key [Info](#)

Private key - optional

Upload an RSA, ECDSA, or ED25519 private key that will be used to identify your SFTP server when clients connect to it. Additional keys can be added once the server is created.

Enter an optional RSA, ECDSA, or ED25519 key

Description - optional

Add a description to differentiate between multiple private keys

Enter optional description

Note You can ignore this section unless you are migrating users from an existing SFTP server.

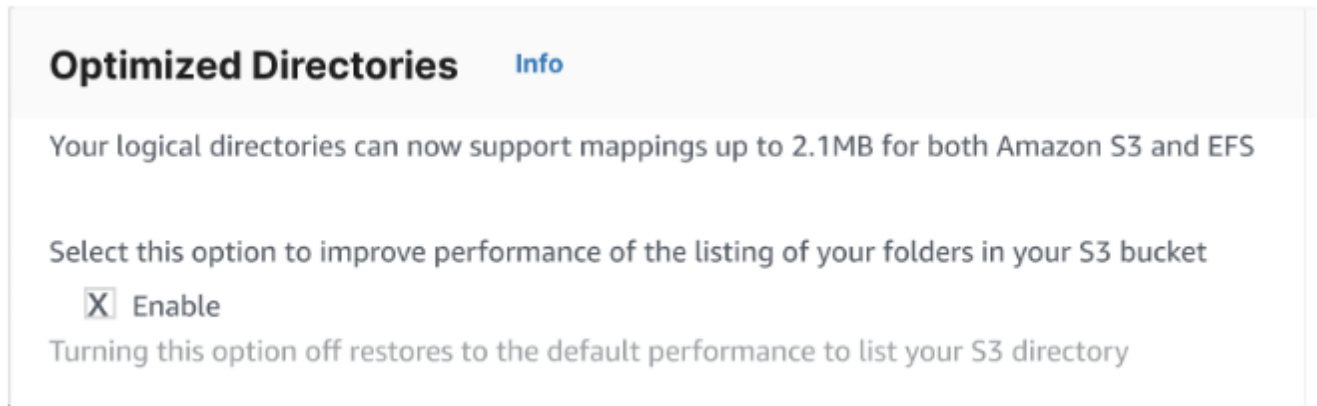
- e. (選用) 針對標籤，針對金鑰和值，輸入一或多個標籤作為鍵值對，然後選擇新增標籤。
- f. 選擇 Next (下一步)。

Tags

Key	Value	
Enter key	Enter value	<button>Remove tag</button>
<button>Add tag</button>		

CancelPreviousNext

- g. 您可以最佳化 Amazon S3 目錄的效能。例如，假設您進入主目錄，並且有 10,000 個子目錄。換句話說，S3 儲存貯體有 10,000 個資料夾。在此案例中，如果您執行 `ls` (清單) 命令，則清單操作需要 6 到 8 分鐘。不過，如果您最佳化目錄，此操作只需要幾秒鐘的時間。



Optimized Directories [Info](#)

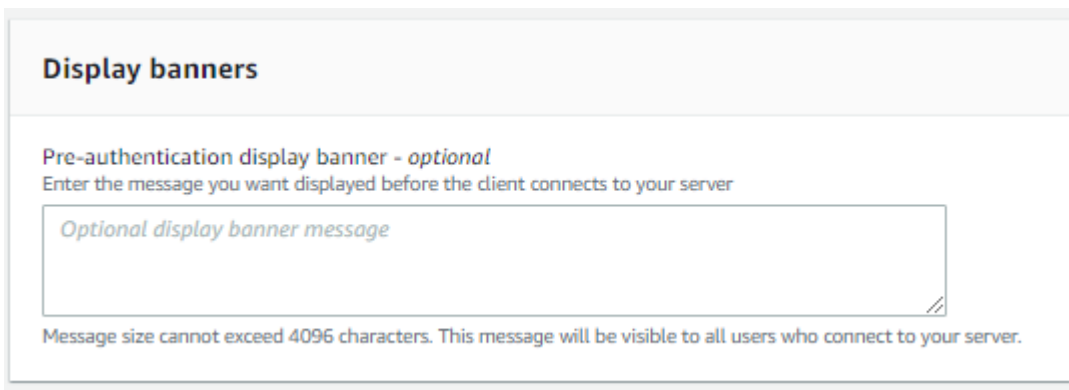
Your logical directories can now support mappings up to 2.1MB for both Amazon S3 and EFS

Select this option to improve performance of the listing of your folders in your S3 bucket

☒ Enable

Turning this option off restores to the default performance to list your S3 directory

- h. (選用) 設定 AWS Transfer Family 伺服器向最終使用者顯示自訂訊息，例如組織政策或條款與條件。對於顯示橫幅，在預先驗證顯示橫幅文字方塊中，輸入您要在使用者驗證之前顯示的文字簡訊。



Display banners

Pre-authentication display banner - *optional*
Enter the message you want displayed before the client connects to your server

Optional display banner message

Message size cannot exceed 4096 characters. This message will be visible to all users who connect to your server.

- i. (選用) 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到 Amazon S3 儲存貯體的檔案 SETSTAT 上使用時所產生的錯誤。如需其他詳細資訊，請參閱 中的 SetStatOption 文件 [ProtocolDetails](#)。
 - **TLS 工作階段恢復**：只有在您啟用 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。

Additional configuration

SetStat option - *optional* [Info](#)

Select whether you want this server to ignore SetStat command

☐ Enable

TLS session resumption - *optional* [Info](#)

Choose how you want your server to process TLS session resumption requests

☒ Enforce

☐ Enable

☐ Disable

 To enable TLS session resumption, enable FTPS as one of the protocols selected in Step 1

Passive IP - *optional* [Info](#)

Provide passive IP (PASV) that file transfer clients can use to connect this server

1.2.3.4

 To enable Passive IP, enable FTP or FTPS as one of the protocols selected in Step 1

8. 在檢閱和建立 中，檢閱您的選擇。

- 如果您想要編輯其中任何一個，請選擇步驟旁的編輯。

Note

您必須在選擇編輯的步驟之後檢閱每個步驟。

- 如果您沒有變更，請選擇建立伺服器以建立伺服器。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。

Servers (1)							
					Actions ▼	Add user	Create server
< 1 >							
☐	Hostname ▲	Server ID ▼	State ▼	users ▼	Endpoint type ▼	Domain ▼	
☐	-	s-	Starting	 No Users	Public	Amazon S3	

建立已啟用 FTPS 的伺服器

透過 SSL (FTPS) 的檔案傳輸通訊協定是 的延伸FTP。它使用 Transport Layer Security (TLS) 和 Secure Sockets Layer (SSL) 密碼編譯通訊協定來加密流量。FTPS 允許同時或獨立加密控制和資料通道連線。

若要建立已啟用 FTPS 的伺服器

1. 在 開啟 AWS Transfer Family 主控台<https://console.aws.amazon.com/transfer/>，然後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。

針對伺服器憑證，選擇儲存在 AWS Certificate Manager (ACM) 中的憑證，當用戶端透過它連線時，該憑證將用於識別您的伺服器，FTPS然後選擇下一步。

若要請求新的公有憑證，請參閱 AWS Certificate Manager 使用者指南 中的[請求公有憑證](#)。

若要將現有憑證匯入 ACM，請參閱 使用者指南 中的[將憑證匯入 ACM](#)。AWS Certificate Manager

若要FTPS透過私有 IP 地址請求私有憑證，請參閱 AWS Certificate Manager 使用者指南 中的[請求私有憑證](#)。

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

憑證必須是指定 FQDN 或 IP 地址的有效 SSL/TLS X.509 第 3 版憑證，以及發行者的相關資訊。

Choose protocols

Select the protocols you want to enable [Info](#)

Choose one or more file transfer protocols over which clients can connect to your server's endpoint

- ☐ SFTP (SSH File Transfer Protocol) - file transfer over Secure Shell
- ☐ AS2 (Applicability Statement 2) - messaging protocol for exchanging business-to-business data [Info](#)
- ☒ FTPS (File Transfer Protocol Secure) - file transfer protocol with TLS encryption
- ☐ FTP (File Transfer Protocol) - unencrypted file transfer protocol

AWS Certificate Manager (ACM) certificate [Info](#)

Server certificate

Choose a certificate stored in ACM which will be used to identify your server when clients connect to it over FTPS



[Cancel](#) [Next](#)

3. 在選擇身分提供者 中，選擇您要用來管理使用者存取權的身分提供者。您有下列選項：
- AWS Directory Service for Microsoft Active Directory – 您提供一個 AWS Directory Service 目錄來存取端點。如此一來，您可以使用儲存在 Active Directory 中的憑證來驗證使用者。若要進一步了解如何使用 AWS Managed Microsoft AD 身分提供者，請參閱 [使用 AWS Directory Service 身分提供者](#)。

 Note

- 不支援跨帳戶和共用目錄 AWS Managed Microsoft AD。
- 若要使用 Directory Service 作為身分提供者來設定伺服器，您需要新增一些 AWS Directory Service 許可。如需詳細資訊，請參閱 [開始使用 之前 AWS Directory Service for Microsoft Active Directory](#)。

Choose an identity provider

Identity provider

Identity provider type
An identity provider manages user access for authentication and authorization

☐ **Service managed**
Create and manage users within the service

☒ **AWS Directory Service** [Info](#)
Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☐ **Custom Identity Provider** [Info](#)
Manage users by integrating an identity provider of your choice

Directory

TATER3 ▼ 

Cancel Previous Next

- 自訂身分提供者 – 選擇下列其中一個選項：
- 使用 AWS Lambda 來連接您的身分提供者 – 您可以使用現有的身分提供者，並由 Lambda 函數提供支援。您提供 Lambda 函數的名稱。如需詳細資訊，請參閱[使用 AWS Lambda 整合您的身分提供者](#)。
- 使用 Amazon API Gateway 來連接您的身分提供者 – 您可以建立由 Lambda 函數支援的 API 閘道方法，以用作身分提供者。您提供 Amazon API Gateway URL 和調用角色。如需詳細資訊，請參閱[使用 Amazon API Gateway 整合您的身分提供者](#)。

Choose an identity provider

Identity Provider for SFTP, FTPS, or FTP

Identity provider type

An identity provider manages user access for authentication and authorization

☐ Service managed

Create and manage users within the service

☐ AWS Directory Service [Info](#)

Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☒ Custom Identity Provider [Info](#)

Manage users by integrating an identity provider of your choice

☒ Use AWS Lambda to connect your identity provider [Info](#)

Invoke an AWS Lambda function to call your identity provider's API for user authentication and authorization

☐ Use Amazon API Gateway to connect your identity provider [Info](#)

Use a RESTful API method to call your identity provider's API for user authentication and authorization

AWS Lambda function

Choose a Lambda function



Authentication methods

Choose which authentication methods are required for users to connect to your server

☒ Password OR public key

☐ Password ONLY

☐ Public Key ONLY

☐ Password AND public key

[i](#) To choose an authentication method, enable SFTP as one of the protocols selected in Step 1

Cancel

Previous

Next

4. 選擇 Next (下一步)。
5. 在選擇端點 中，執行下列動作：

[i](#) Note

FTPS 適用於 Transfer Family 的 伺服器透過連接埠 21（控制頻道）和連接埠範圍 8192–8200（資料頻道）運作。

- a. 對於端點類型，選擇VPC託管端點類型以託管伺服器的端點。如需有關設定VPC託管端點的資訊，請參閱 [在虛擬私有雲端中建立伺服器](#)。

 Note

不支援公開存取的端點。

- b. (選用) 針對FIPS已啟用，選取FIPS已啟用端點核取方塊，以確保端點符合聯邦資訊處理標準 (FIPS)。

 Note

FIPS啟用的端點僅適用於北美 AWS 區域。如需可用區域的資訊，請參閱中的[AWS Transfer Family 端點和配額](#) AWS 一般參考。如需的詳細資訊FIPS，請參閱[聯邦資訊處理標準 \(FIPS \) 140-2](#)。

- c. 選擇 Next (下一步)。

Choose an endpoint

Endpoint configuration [Info](#)

Endpoint type
Select whether the endpoint will be publicly accessible or hosted inside your VPC

☐ Publicly accessible
Accessible over the internet

☒ VPC hosted [Info](#)
Access controlled using Security Groups

Access [Info](#)

☒ Internal

☐ Internet Facing

VPC
Select a VPC ID

[Create a VPC](#)

FIPS Enabled
Select whether the endpoint should comply with Federal Information Processing Standards (FIPS)

☐ FIPS Enabled endpoint

[Cancel](#) [Previous](#) [Next](#)

6. 在選擇網域頁面上，選擇您要用來透過所選通訊協定存放和存取資料的 AWS 儲存服務：

- 選擇 Amazon S3，以儲存和存取檔案作為所選通訊協定上的物件。
- 選擇 Amazon EFS 以透過選取的通訊協定，將檔案存放和存取到您的 Amazon EFS 檔案系統中。

選擇 Next (下一步)。

7. 在設定其他詳細資訊 中，執行下列動作：

- a. 若要記錄，請指定現有的日誌群組或建立新的日誌群組（預設選項）。

Transfer Family > Servers > Create server

Step 1
Choose protocols

Step 2
Choose an identity provider

Step 3
Choose an endpoint

Step 4
Choose a domain

Step 5
Configure additional details

Step 6
Review and create

Configure additional details

Logging Info

Log group Info
Choose the CloudWatch log group where your events will be delivered in a structured JSON format

☒ Create a new log group ☐ Choose an existing log group

Choose an existing log group

Logging role Info
Choose the IAM role that will be used to deliver events to your CloudWatch logs

☐ Create a new role ☐ Choose an existing role

i Logging role is only required when selecting a workflow in the Managed workflows section below.

如果您選擇現有的日誌群組，您必須選取與相關聯的日誌群組 AWS 帳戶。

Transfer Family > Servers > Create server

Step 1
Choose protocols

Step 2
Choose an identity provider

Step 3
Choose an endpoint

Step 4
Choose a domain

Step 5
Configure additional details

Step 6
Review and create

Configure additional details

Logging Info

Log group Info
Choose the CloudWatch log group where your events will be delivered in a structured JSON format

☐ Create a new log group ☒ Choose an existing log group

/aws/transfer/

Logging role Info
Choose the IAM role that will be used to deliver events to your CloudWatch logs

☐ Create a new role ☐ Choose an existing role

i Logging role is only required when selecting a workflow in the Managed workflows section below.

如果您選擇建立日誌群組，CloudWatch 主控台（<https://console.aws.amazon.com/cloudwatch/>）會開啟建立日誌群組頁面。如需詳細資訊，請參閱在[日誌中建立 CloudWatch 日誌群組](#)。

- b. （選用）針對受管工作流程，選擇 Transfer Family 在執行工作流程時應擔任的工作流程 IDs（和對應的角色）。您可以選擇一個工作流程在完整上傳時執行，另一個工作流程在部分

上傳時執行。若要進一步了解如何使用受管工作流程處理檔案，請參閱 [AWS Transfer Family 受管工作流程](#)。

Managed workflows [Info](#)

Workflow for complete file uploads
Select the workflow that AWS Transfer Family should run on all files that are uploaded in full via this server

w- [dropdown] [refresh] [Create a new Workflow](#)

Workflow for partial file uploads
Select the workflow that Transfer Family should run on all files that are only partially uploaded via this server

w- [dropdown] [refresh] [Create a new Workflow](#)

Managed workflows execution role [Info](#)
Select the role that AWS Transfer Family should assume when executing a workflow

[dropdown] [refresh]

- c. 針對密碼編譯演算法選項，選擇包含啟用供伺服器使用之密碼編譯演算法的安全政策。

Note

根據預設：

- 如果未選取FIPS已啟用端點，則TransferSecurityPolicy-2020-06安全政策會連接至您的伺服器。
- 如果選取FIPS已啟用端點，則TransferSecurityPolicy-FIPS-2020-06安全政策會連接至您的伺服器。

如需關於安全政策的詳細資訊，請參閱[安全政策 AWS Transfer Family](#)。

Cryptographic algorithm options [Info](#)

Security Policy
Choose a security policy that contains the cryptographic algorithms enabled for use by your server

TransferSecurityPolicy-2023-05 [dropdown] [refresh]

- d. 對於伺服器主機金鑰，請保留空白。

Note

伺服器主機金鑰區段僅用於從已啟用 SFTP 的現有伺服器遷移使用者。

Server Host Key [Info](#)**Private key - optional**

Upload an RSA, ECDSA, or ED25519 private key that will be used to identify your SFTP server when clients connect to it. Additional keys can be added once the server is created.

Enter an optional RSA, ECDSA, or ED25519 key

Description - optional

Add a description to differentiate between multiple private keys

Enter optional description

i You can ignore this section unless you are migrating users from an existing SFTP server.

- e. (選用) 針對標籤，針對索引鍵和值，輸入一或多個標籤做為索引鍵值對，然後選擇新增標籤。
- f. 您可以最佳化 Amazon S3 目錄的效能。例如，假設您進入主目錄，並且有 10,000 個子目錄。換句話說，S3 儲存貯體有 10,000 個資料夾。在此案例中，如果您執行 `ls` (清單) 命令，則清單操作需要 6 到 8 分鐘。不過，如果您最佳化目錄，此操作只需要幾秒鐘的時間。

Optimized Directories [Info](#)

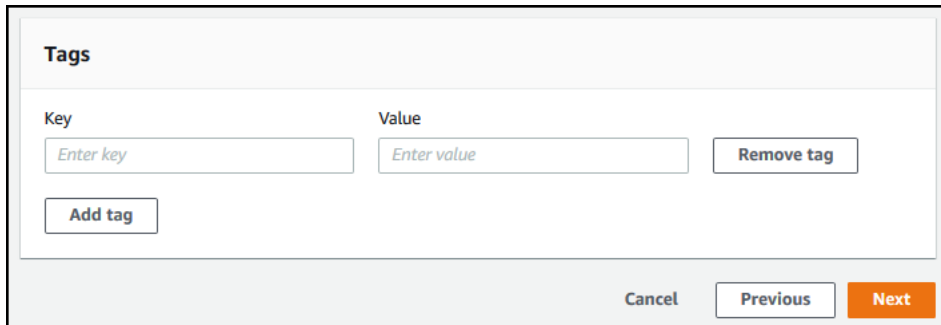
Your logical directories can now support mappings up to 2.1MB for both Amazon S3 and EFS

Select this option to improve performance of the listing of your folders in your S3 bucket

☒ Enable

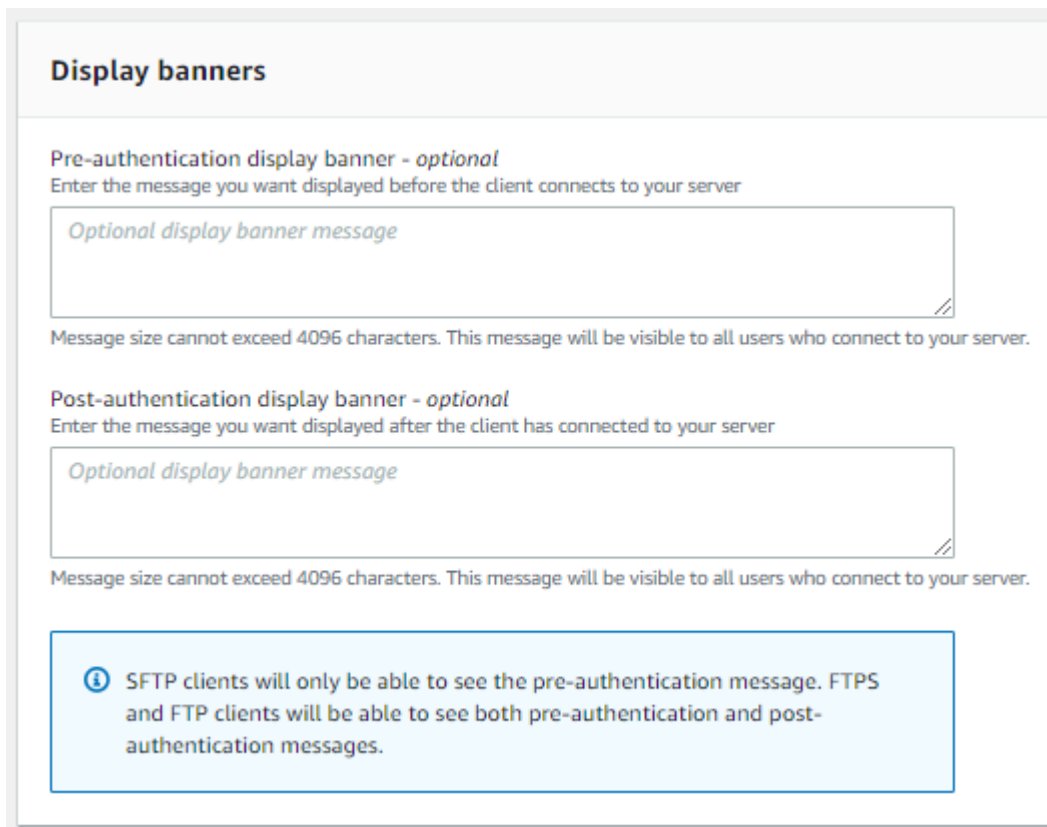
Turning this option off restores to the default performance to list your S3 directory

- g. 選擇 Next (下一步)。



- h. (選用) 您可以設定 AWS Transfer Family 伺服器向最終使用者顯示自訂訊息，例如組織政策或條款與條件。您也可以向已成功驗證的使用者顯示自訂的當天訊息 (MOTD)。

對於顯示橫幅，在驗證前顯示橫幅文字方塊中，輸入您要在使用者驗證前顯示的文字，並在驗證後顯示橫幅文字方塊中，輸入您希望在使用者成功驗證後顯示的文字。



- i. (選用) 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 上使用時所產生的錯誤。如需其他詳細資訊，請參閱 [ProtocolDetails](#) 主題中的 SetStatOption 文件。

- **TLS 工作階段恢復**：提供機制，在FTPS工作階段的控制和資料連線之間繼續或共用交涉的秘密金鑰。如需其他詳細資訊，請參閱 [ProtocolDetails](#)主題中的 `TlsSessionResumptionMode` 文件。
- **被動 IP**：表示 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。如需其他詳細資訊，請參閱 [ProtocolDetails](#)主題中的 `PassiveIp` 文件。

Additional configuration

SetStat option - optional [Info](#)
Select whether you want this server to ignore SetStat command

☐ Enable

TLS session resumption - optional [Info](#)
Choose how you want your server to process TLS session resumption requests

☒ Enforce
☐ Enable
☐ Disable

Passive IP - optional [Info](#)
Provide passive IP (PASV) that file transfer clients can use to connect this server

1.2.3.4

8. 在檢閱和建立 中，檢閱您的選擇。

- 如果您想要編輯其中任何項目，請選擇步驟旁的編輯。

Note

您必須在選擇編輯的步驟之後檢閱每個步驟。

- 如果您沒有變更，請選擇建立伺服器以建立伺服器。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。

Servers (1)							Actions	Add user	Create server
	Hostname	Server ID	State	users	Endpoint type	Domain			
☐	-	s-	Starting	No Users	Public	Amazon S3			

後續步驟：在下一個步驟中，繼續前往 [使用自訂身分提供者](#) 以設定使用者。

建立已啟用 FTP 的伺服器

檔案傳輸通訊協定（FTP）是用於資料傳輸的網路通訊協定。FTP 使用單獨的頻道進行控制和資料傳輸。控制頻道會開啟，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 使用純文字，不支援流量加密。

Note

啟用時 FTP，您必須選擇 VPC 託管端點的內部存取選項。如果您需要伺服器的資料周遊公有網路，則必須使用安全通訊協定，例如 SFTP 或 FTPS。

若要建立 FTP 已啟用的伺服器

1. 在開啟 AWS Transfer Family 主控台 <https://console.aws.amazon.com/transfer/>，然後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 FTP，然後選擇下一步。

Choose protocols

Select the protocols you want to enable [Info](#)

Choose one or more file transfer protocols over which clients can connect to your server's endpoint

- ☐ SFTP (SSH File Transfer Protocol) - file transfer over Secure Shell
- ☐ AS2 (Applicability Statement 2) - messaging protocol for exchanging business-to-business data [Info](#)
- ☐ FTPS (File Transfer Protocol Secure) - file transfer protocol with TLS encryption
- ☒ FTP (File Transfer Protocol) - unencrypted file transfer protocol

Cancel **Next**

3. 在選擇身分提供者中，選擇您要用來管理使用者存取權的身分提供者。您有下列選項：

- AWS Directory Service for Microsoft Active Directory – 您提供一個 AWS Directory Service 目錄來存取端點。如此一來，您可以使用儲存在 Active Directory 中的憑證來驗證使用者。若要進一步了解如何使用 AWS Managed Microsoft AD 身分提供者，請參閱 [使用 AWS Directory Service 身分提供者](#)。

Note

- 不支援跨帳戶和共用目錄 AWS Managed Microsoft AD。
- 若要使用 Directory Service 作為身分提供者來設定伺服器，您需要新增一些 AWS Directory Service 許可。如需詳細資訊，請參閱 [開始使用之前 AWS Directory Service for Microsoft Active Directory](#)。

Choose an identity provider

Identity provider

Identity provider type
An identity provider manages user access for authentication and authorization

☐ **Service managed**
Create and manage users within the service

☒ **AWS Directory Service** [Info](#)
Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☐ **Custom Identity Provider** [Info](#)
Manage users by integrating an identity provider of your choice

Directory
TATER3 ▼ ↺

Cancel Previous Next

- 自訂身分提供者 – 選擇下列其中一個選項：
- 使用 AWS Lambda 來連接您的身分提供者 – 您可以使用現有的身分提供者，並由 Lambda 函數提供支援。您提供 Lambda 函數的名稱。如需詳細資訊，請參閱 [使用 AWS Lambda 整合您的身分提供者](#)。
- 使用 Amazon API Gateway 來連接您的身分提供者 – 您可以建立由 Lambda 函數支援的 API 閘道方法，以用作身分提供者。您提供 Amazon API Gateway URL 和調用角色。如需詳細資訊，請參閱 [使用 Amazon API Gateway 整合您的身分提供者](#)。

Choose an identity provider

Identity Provider for SFTP, FTPS, or FTP

Identity provider type

An identity provider manages user access for authentication and authorization

☐ Service managed

Create and manage users within the service

☐ AWS Directory Service [Info](#)

Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☒ Custom Identity Provider [Info](#)

Manage users by integrating an identity provider of your choice

☒ Use AWS Lambda to connect your identity provider [Info](#)

Invoke an AWS Lambda function to call your identity provider's API for user authentication and authorization

☐ Use Amazon API Gateway to connect your identity provider [Info](#)

Use a RESTful API method to call your identity provider's API for user authentication and authorization

AWS Lambda function

Choose a Lambda function



Authentication methods

Choose which authentication methods are required for users to connect to your server

☒ Password OR public key

☐ Password ONLY

☐ Public Key ONLY

☐ Password AND public key

[i](#) To choose an authentication method, enable SFTP as one of the protocols selected in Step 1

Cancel

Previous

Next

4. 選擇 Next (下一步)。
5. 在選擇端點 中，執行下列動作：

[i](#) Note

FTP 適用於 Transfer Family 的 伺服器透過連接埠 21（控制頻道）和連接埠範圍 8192–8200（資料頻道）運作。

- a. 對於端點類型，選擇VPC託管以託管伺服器的端點。如需有關設定VPC託管端點的資訊，請參閱 [在虛擬私有雲端中建立伺服器](#)。

Note

不支援公開存取的端點。

- b. 對於FIPS已啟用，請保持清除FIPS已啟用端點核取方塊。

Note

FIPSFTP 伺服器不支援已啟用的端點。

- c. 選擇 Next (下一步)。

Choose an endpoint

Endpoint configuration [Info](#)

Endpoint type
Select whether the endpoint will be publicly accessible or hosted inside your VPC

☐ Publicly accessible
Accessible over the internet

☒ VPC hosted [Info](#)
Access controlled using Security Groups

Access [Info](#)

☒ Internal
☐ Internet Facing

VPC
Select a VPC ID

▼

FIPS Enabled
Select whether the endpoint should comply with Federal Information Processing Standards (FIPS)

☐ FIPS Enabled endpoint

Cancel

Previous

Next

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

- 選擇 Amazon S3，以儲存和存取檔案作為所選通訊協定上的物件。
- 選擇 AmazonEFS，透過選取的通訊協定將檔案存放和存取到您的 Amazon EFS 檔案系統中。

選擇 Next (下一步)。

7. 在設定其他詳細資訊 中，執行下列動作：

- a. 若要記錄，請指定現有的日誌群組或建立新的日誌群組（預設選項）。

如果您選擇現有的日誌群組，您必須選取與 相關聯的日誌群組 AWS 帳戶。

如果您選擇建立日誌群組，CloudWatch 主控台（<https://console.aws.amazon.com/cloudwatch/>）會開啟建立日誌群組頁面。如需詳細資訊，請參閱在[日誌中建立 CloudWatch 日誌群組](#)。

- b. （選用）針對受管工作流程，選擇 Transfer Family 在執行工作流程時應擔任的工作流程 IDs（和對應的角色）。您可以選擇一個工作流程在完整上傳時執行，另一個工作流程在部分上傳時執行。若要進一步了解如何使用受管工作流程處理檔案，請參閱 [AWS Transfer Family 受管工作流程](#)。

- c. 針對密碼編譯演算法選項，選擇包含已啟用供伺服器使用之密碼編譯演算法的安全政策。

Note

Transfer Family 會將最新的安全政策指派給您的FTP伺服器。不過，由於FTP通訊協定不會使用任何加密，因此FTP伺服器不會使用任何安全政策演算法。除非您的伺服器也使用 FTPS或 SFTP通訊協定，否則安全政策會保持未使用狀態。

Cryptographic algorithm options [Info](#)**Security Policy**

Choose a security policy that contains the cryptographic algorithms enabled for use by your server

TransferSecurityPolicy-2023-05



- d. 對於伺服器主機金鑰，請保留空白。

Note

伺服器主機金鑰區段僅用於從已啟用 SFTP的現有伺服器遷移使用者。

Server Host Key [Info](#)**Private key - optional**

Upload an RSA, ECDSA, or ED25519 private key that will be used to identify your SFTP server when clients connect to it. Additional keys can be added once the server is created.

Enter an optional RSA, ECDSA, or ED25519 key

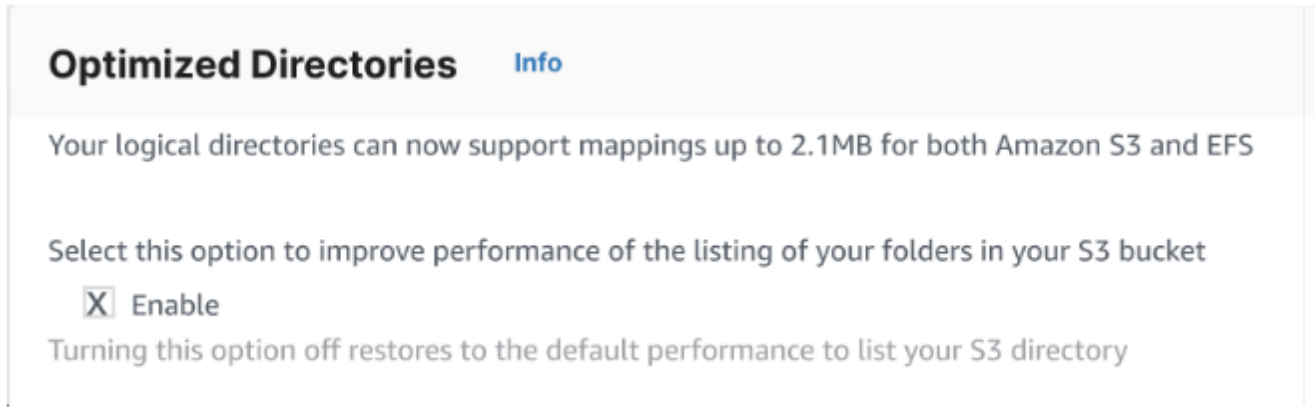
Description - optional

Add a description to differentiate between multiple private keys

Enter optional description

Note You can ignore this section unless you are migrating users from an existing SFTP server.

- e. (選用) 針對標籤，針對金鑰和值，輸入一或多個標籤作為鍵值對，然後選擇新增標籤。
- f. 您可以最佳化 Amazon S3 目錄的效能。例如，假設您進入主目錄，並且有 10,000 個子目錄。換句話說，S3 儲存貯體有 10,000 個資料夾。在此案例中，如果您執行 `ls` (清單) 命令，則清單操作需要 6 到 8 分鐘。不過，如果您最佳化目錄，此操作只需要幾秒鐘的時間。



Optimized Directories [Info](#)

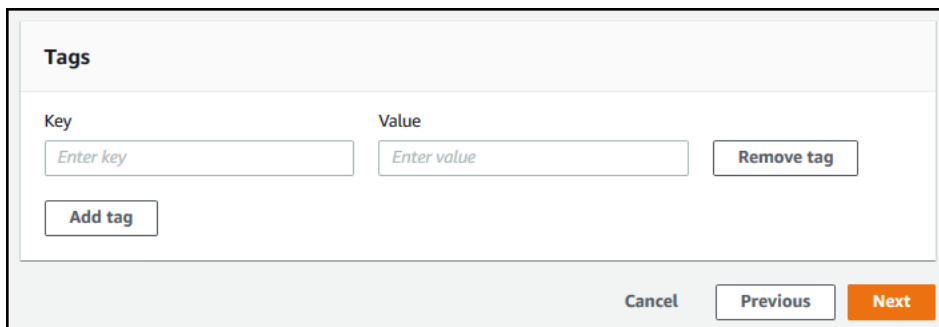
Your logical directories can now support mappings up to 2.1MB for both Amazon S3 and EFS

Select this option to improve performance of the listing of your folders in your S3 bucket

☒ Enable

Turning this option off restores to the default performance to list your S3 directory

- g. 選擇 Next (下一步)。



Tags

Key Value

- h. (選用) 您可以設定 AWS Transfer Family 伺服器向最終使用者顯示自訂訊息，例如組織政策或條款與條件。您也可以向成功驗證的使用者顯示自訂的當天訊息 (MOTD)。

對於顯示橫幅，在驗證前顯示橫幅文字方塊中，輸入您要在使用者驗證前顯示的文字簡訊，並在驗證後顯示橫幅文字方塊中，輸入您希望在使用者成功驗證後顯示的文字。

Display banners

Pre-authentication display banner - optional
Enter the message you want displayed before the client connects to your server

Optional display banner message

Message size cannot exceed 4096 characters. This message will be visible to all users who connect to your server.

Post-authentication display banner - optional
Enter the message you want displayed after the client has connected to your server

Optional display banner message

Message size cannot exceed 4096 characters. This message will be visible to all users who connect to your server.

i SFTP clients will only be able to see the pre-authentication message. FTPS and FTP clients will be able to see both pre-authentication and post-authentication messages.

i. (選用) 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上使用時所產生的錯誤。如需其他詳細資訊，請參閱 [ProtocolDetails](#)主題中的 SetStatOption 文件。
- **TLS 工作階段恢復**：提供機制，在FTPS工作階段的控制和資料連線之間繼續或共用交涉的秘密金鑰。如需其他詳細資訊，請參閱 [ProtocolDetails](#)主題中的 TlsSessionResumptionMode 文件。
- **被動 IP**：表示 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。如需其他詳細資訊，請參閱 [ProtocolDetails](#)主題中的 PassiveIp 文件。

Additional configuration

SetStat option - optional [Info](#)

Select whether you want this server to ignore SetStat command

☐ Enable

TLS session resumption - optional [Info](#)

Choose how you want your server to process TLS session resumption requests

☒ Enforce

☐ Enable

☐ Disable

Passive IP - optional [Info](#)

Provide passive IP (PASV) that file transfer clients can use to connect this server

1.2.3.4

8. 在檢閱和建立 中，檢閱您的選擇。

- 如果您想要編輯其中任何一個，請選擇步驟旁的編輯。

Note

您必須在選擇編輯的步驟之後檢閱每個步驟。

- 如果您沒有變更，請選擇建立伺服器以建立伺服器。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。

Servers (1)									Actions ▾	Add user	Create server
								< 1 >			
☐	Hostname ▲	Server ID ▼	State ▼	users ▼	Endpoint type ▼	Domain ▼					
☐	-	s-	Starting		Public	Amazon S3					

後續步驟：在後續步驟中，繼續前往 [使用自訂身分提供者](#) 以設定使用者。

在虛擬私有雲端中建立伺服器

您可以在虛擬私有雲端（VPC）中託管伺服器的端點，以用於在 Amazon S3 儲存貯體或 Amazon EFS 檔案系統中來回傳輸資料，而無需透過公有網際網路。

Note

2021 年 5 月 19 日後，如果您的帳戶未在 2021 年 5 月 19 日之前使用 建立伺服器，則無法在EndpointType=VPC_ENDPOINT AWS 帳戶中使用 建立伺服器。如果您已EndpointType=VPC_ENDPOINT在 2021 年 2 月 21 日或之前在 AWS 帳戶中使用 建立伺服器，則不會受到影響。在此日期之後，請使用 EndpointType=VPC。如需詳細資訊，請參閱[the section called “停止使用 VPC_ENDPOINT”](#)。

如果您使用 Amazon Virtual Private Cloud（Amazon VPC）託管 AWS 資源，您可以在 VPC 和 伺服器之間建立私有連線。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。

使用 Amazon VPC，您可以在自訂虛擬網路中啟動 AWS 資源。您可以使用 VPC 來控制網路設定，例如 IP 地址範圍、子網路、路由表和網路閘道。如需的詳細資訊 VPCs，請參閱 [Amazon 使用者指南 VPC 中的什麼是 Amazon？](#)。 VPC

在下一節中，尋找如何建立 並將其連線至 VPC 伺服器的指示。概觀如下：

1. 使用 VPC 端點設定伺服器。
2. 透過 VPC 端點使用 內部的用戶端連線至您的伺服器。這樣做可讓您使用 ，透過用戶端傳輸存放在 Amazon S3 儲存貯體中的資料 AWS Transfer Family。即使網路與公有網際網路中斷連線，您也可以執行此傳輸。
3. 此外，如果您選擇讓伺服器的端點面向網際網路，您可以將彈性 IP 地址與端點建立關聯。這樣做可讓 VPC 連線伺服器以外的用戶端。您可以使用 VPC 安全群組來控制對僅來自允許地址之請求的已驗證使用者的存取。

主題

- [建立只能在您的 內存取的伺服器端點 VPC](#)
- [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_ENDPOINT](#)

- [將 AWS Transfer Family 伺服器端點類型從 VPC_ENDPOINT 更新為 VPC](#)

建立只能在您的 內存取的伺服器端點 VPC

在下列程序中，您可以建立只能存取 內資源的伺服器端點VPC。

在 內建立伺服器端點 VPC

1. 在 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，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：建立已啟用 SFTP的伺服器](#)。
4. 在選擇身分提供者 中，選擇 Service 受管以將使用者身分和金鑰存放在 中 AWS Transfer Family，然後選擇下一步。

Note

此程序使用服務受管選項。如果您選擇自訂，您會提供 Amazon API Gateway 端點和 AWS Identity and Access Management (IAM) 角色來存取端點。如此一來，您就可以整合目錄服務來驗證和授權您的使用者。若要進一步了解使用自訂身分提供者，請參閱[使用自訂身分提供者](#)。

5. 在選擇端點 中，執行下列動作：

Note

FTP 和 Transfer Family 的FTPS伺服器透過連接埠 21（控制頻道）和連接埠範圍 8192-8200（資料頻道）運作。

- a. 對於端點類型，選擇VPC託管端點類型以託管伺服器的端點。
- b. 針對存取，選擇內部，讓端點只能使用端點私有 IP 地址的用戶端存取。

Note

如需網際網路面向選項的詳細資訊，請參閱 [為您的伺服器建立面向網際網路的端點](#)。在 中建立VPC僅供內部存取的伺服器不支援自訂主機名稱。

- c. 針對 VPC，選擇現有的 VPC ID 或選擇建立 VPC 以建立新的 VPC。
- d. 在可用區域區段中，選擇最多三個可用區域和相關聯的子網路。
- e. 在安全群組區段中，選擇現有的安全群組 ID，IDs 或選擇建立安全群組以建立新的安全群組。如需安全群組的詳細資訊，請參閱 Amazon Virtual Private Cloud 使用者指南 中的 [安全群組 VPC](#)。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 會自動隨附預設安全群組。如果您在啟動伺服器時未指定不同的安全群組，我們會將預設安全群組與您的伺服器建立關聯。

對於安全群組的傳入規則，您可以將 SSH 流量設定為使用連接埠 22、2222 或兩者。連接埠 22 預設為。若要使用連接埠 2222，您可以將傳入規則新增至安全群組。對於類型，請選擇自訂 TCP，然後在 2222 連接埠範圍 中輸入，然後在來源中輸入與 SSH 連接埠 22 規則相同的 CIDR 範圍。

VPC > Security Groups > sg- > default > Edit inbound rules

Edit inbound rules [info](#)

Inbound rules control the incoming traffic that's allowed to reach the instance.

Security group rule ID	Type	Protocol	Port range	Source
sg-	HTTP	TCP	80	Custom 0.0.0.0/0
sg-	RDP	TCP	3389	Custom 0.0.0.0/0
sg-	HTTPS	TCP	443	Custom 0.0.0.0/0
sg-	Custom TCP	TCP	2222	Custom 72.21.196.64/32
sg-	SSH	TCP	22	Custom 72.21.196.64/32

Add rule

- f. (選用) 針對 FIPS 已啟用，選取 FIPS 已啟用端點核取方塊，以確保端點符合聯邦資訊處理標準 (FIPS)。

Note

FIPS啟用的端點僅適用於北美 AWS 區域。如需可用區域的資訊，請參閱中的[AWS Transfer Family 端點和配額](#) AWS 一般參考。如需的詳細資訊FIPS，請參閱[聯邦資訊處理標準（FIPS）140-2](#)。

- g. 選擇 Next (下一步)。
6. 在設定其他詳細資訊 中，執行下列動作：
- a. 針對CloudWatch 記錄，請選擇下列其中一項來啟用 Amazon CloudWatch 記錄您的使用者活動：
- 建立新的角色，以允許 Transfer Family 自動建立IAM角色，只要您擁有建立新角色的正確許可。建立IAM的角色稱為 AWSTransferLoggingAccess。
 - 選擇現有角色，從您的帳戶中選擇現有IAM角色。在記錄角色 下，選擇角色。此IAM角色應包含服務設定為 的信任政策transfer.amazonaws.com。

如需 CloudWatch 記錄的詳細資訊，請參閱 [設定 CloudWatch 記錄角色](#)。

Note

- CloudWatch 如果您未指定記錄角色，則無法在 中檢視最終使用者活動。
- 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. 針對密碼編譯演算法選項，選擇包含啟用供伺服器使用之密碼編譯演算法的安全政策。

Note

根據預設，除非您選擇不同的安全政策，否則TransferSecurityPolicy-2020-06安全政策會連接至您的伺服器。

如需關於安全政策的詳細資訊，請參閱[的安全政策 AWS Transfer Family](#)。

- c. （選用）對於伺服器主機金鑰，輸入 RSA、ED25519或 ECDSA 私有金鑰，當用戶端透過連線到伺服器時，該金鑰將用於識別您的伺服器SFTP。

 Note

本節僅適用於從已啟用 SFTP 的現有伺服器遷移使用者。

- d. (選用) 對於標籤，對於索引鍵和值，輸入一或多個標籤作為索引鍵值對，然後選擇新增標籤。
 - e. 選擇 Next (下一步)。
7. 在檢閱和建立 中，檢閱您的選擇。如果您：
- 想要編輯其中任何一個，請選擇步驟旁的編輯。

 Note

您將需要在選擇編輯的步驟之後檢閱每個步驟。

- 沒有變更，請選擇建立伺服器以建立伺服器。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。

新伺服器狀態變更為線上 之前，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。

為您的伺服器建立面向網際網路的端點

在下列程序中，您可以建立伺服器端點。此端點只能透過網際網路存取，其來源 IP 地址在 VPC 的預設安全群組中為允許的用戶端。此外，透過使用彈性 IP 地址讓端點面向網際網路，您的用戶端可以使用彈性 IP 地址，允許存取其防火牆中的端點。

 Note

只有 SFTP 和 FTPS 可用於面向網際網路的 VPC 託管端點。

建立面向網際網路的端點

1. 在 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，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，然後選擇下一個。如需通訊協定的詳細資訊，請參閱 [步驟 2：建立已啟用 SFTP 的伺服器](#)。
4. 在選擇身分提供者 中，選擇 Service 受管以將使用者身分和金鑰存放在 中 AWS Transfer Family，然後選擇下一步。

 Note

此程序使用服務受管選項。如果您選擇自訂，您會提供 Amazon API Gateway 端點和 AWS Identity and Access Management (IAM) 角色來存取端點。如此一來，您就可以整合目錄服務來驗證和授權您的使用者。若要進一步了解使用自訂身分提供者，請參閱[使用自訂身分提供者](#)。

5. 在選擇端點 中，執行下列動作：
 - a. 對於端點類型，選擇 VPC 託管端點類型以託管伺服器的端點。
 - b. 針對存取，選擇網際網路面向，讓用戶端可透過網際網路存取您的端點。

 Note

當您選擇面向網際網路時，您可以選擇每個子網路或子網路中的現有彈性 IP 地址。或者，您可以前往 VPC 主控台（<https://console.aws.amazon.com/vpc/>）配置一或多個新的彈性 IP 地址。這些地址可以由您擁有 AWS 或由您擁有。您無法將已在端點上使用的彈性 IP 地址建立關聯。

- c. （選用）針對自訂主機名稱，選擇下列其中一項：

 Note

AWS GovCloud (US) 需要直接透過彈性 IP 地址連線的客戶，或在 Commercial Route 53 中建立指向其的主機名稱記錄 EIP。如需針對 GovCloud 端點使用 Route 53 的詳細資訊，請參閱 AWS GovCloud (US) [使用者指南 中的使用 AWS GovCloud \(US\) 資源設定 Amazon Route 53](#)。

- Amazon Route 53 DNS 別名 – 如果您要使用的主機名稱已向 Route 53 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提供者註冊。然後，您可以輸入主機名稱。
- 無 – 使用伺服器的端點，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)，選取無不會以此格式建立主機名稱。

若要進一步了解如何使用自訂主機名稱，請參閱 [使用自訂主機名稱](#)。

- d. 針對 VPC，選擇現有的 VPC ID 或選擇建立 VPC以建立新的 VPC。
- e. 在可用區域區段中，選擇最多三個可用區域和相關聯的子網路。針對IPv4地址，為每個子網路選擇彈性 IP 地址。這是用戶端可用來允許存取其防火牆中端點的 IP 地址。
- f. 在安全群組區段中，選擇現有的安全群組 ID，IDs或選擇建立安全群組以建立新的安全群組。如需安全群組的詳細資訊，請參閱 Amazon Virtual Private Cloud 使用者指南 中的 [安全群組 VPC](#)。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會自動隨附預設安全群組。如果您在啟動伺服器時未指定不同的安全群組，我們會將預設安全群組與您的伺服器建立關聯。

對於安全群組的傳入規則，您可以將SSH流量設定為使用連接埠 22、2222 或兩者。連接埠 22 預設為。若要使用連接埠 2222，您可以將傳入規則新增至安全群組。對於類型，請選擇自訂 TCP，然後在2222連接埠範圍 中輸入，然後在來源中輸入與SSH連接埠 22 規則相同的CIDR範圍。

VPC > Security Groups > sg-...-default > Edit inbound rules

Edit inbound rules [Info](#)

Inbound rules control the incoming traffic that's allowed to reach the instance.

Security group rule ID	Type info	Protocol info	Port range info	Source info
sg-...	HTTP	TCP	80	Custom 0.0.0.0/0 X
sg-...	RDP	TCP	3389	Custom 0.0.0.0/0 X
sg-...	HTTPS	TCP	443	Custom 0.0.0.0/0 X
sg-...	Custom TCP	TCP	2222	Custom 72.21.196.64/32 X
sg-...	SSH	TCP	22	Custom 72.21.196.64/32 X

Add rule

- g. (選用) 針對FIPS已啟用，選取FIPS已啟用端點核取方塊，以確保端點符合聯邦資訊處理標準 (FIPS)。

Note

FIPS啟用的端點僅適用於北美 AWS 區域。如需可用區域的資訊，請參閱中的[AWS Transfer Family 端點和配額](#) AWS 一般參考。如需的詳細資訊FIPS，請參閱[聯邦資訊處理標準 \(FIPS\) 140-2](#)。

- h. 選擇 Next (下一步)。

6. 在設定其他詳細資訊 中，執行下列動作：

- a. 針對CloudWatch 記錄，請選擇下列其中一項來啟用 Amazon CloudWatch 記錄您的使用者活動：
- 建立新的角色，以允許 Transfer Family 自動建立IAM角色，只要您擁有建立新角色的正確許可。建立IAM的角色稱為 `AWSTransferLoggingAccess`。
 - 選擇現有角色，從您的帳戶中選擇現有IAM角色。在記錄角色 下，選擇角色。此IAM角色應包含服務設定為 的信任政策 `transfer.amazonaws.com`。

如需 CloudWatch 記錄的詳細資訊，請參閱 [設定 CloudWatch 記錄角色](#)。

Note

- CloudWatch 如果您未指定記錄角色，則無法在 中檢視最終使用者活動。

- 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. 針對密碼編譯演算法選項，選擇包含啟用供伺服器使用之密碼編譯演算法的安全政策。

Note

根據預設，除非您選擇不同的安全政策，否則TransferSecurityPolicy-2020-06安全政策會連接至您的伺服器。

如需關於安全政策的詳細資訊，請參閱[安全政策 AWS Transfer Family](#)。

- c. (選用) 對於伺服器主機金鑰，輸入 RSA、ED25519 或 ECDSA 私有金鑰，當用戶端透過連線到伺服器時，該金鑰將用於識別您的伺服器SFTP。

Note

本節僅適用於從已啟用 SFTP的現有伺服器遷移使用者。

- d. (選用) 針對標籤，針對金鑰和值，輸入一或多個標籤作為鍵值對，然後選擇新增標籤。
- e. 選擇 Next (下一步)。
- f. (選用) 針對受管工作流程，選擇 Transfer Family 在執行工作流程時應擔任的工作流程 IDs (和對應的角色)。您可以選擇一個工作流程在完整上傳時執行，另一個工作流程在部分上傳時執行。若要進一步了解如何使用受管工作流程處理檔案，請參閱[AWS Transfer Family 受管工作流程](#)。

Managed workflows [Info](#)

Workflow for complete file uploads
Select the workflow that AWS Transfer Family should run on all files that are uploaded in full via this server

W- [dropdown] [refresh] [Create a new Workflow](#)

Workflow for partial file uploads
Select the workflow that Transfer Family should run on all files that are only partially uploaded via this server

W- [dropdown] [refresh] [Create a new Workflow](#)

Managed workflows execution role [Info](#)
Select the role that AWS Transfer Family should assume when executing a workflow

[dropdown] [refresh]

7. 在檢閱和建立 中，檢閱您的選擇。如果您：

- 想要編輯其中任何一個，請選擇步驟旁的編輯。

Note

您將需要在選擇編輯的步驟之後檢閱每個步驟。

- 沒有變更，請選擇建立伺服器以建立伺服器。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。

您可以選擇伺服器 ID，以查看您剛建立之伺服器的詳細設定。填入資料欄公有IPv4地址後，您提供的彈性 IP 地址會成功與伺服器的端點建立關聯。

Note

當您在 中的伺服器VPC上線時，只能修改子網路，且只能透過 [UpdateServer](#) 進行修改API。您必須[停止伺服器](#)，才能新增或變更伺服器端點的彈性 IP 地址。

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（即具有公有端點類型），您可以將其端點變更為VPC端點。

Note

如果您在VPC顯示為 的 中有現有伺服器VPC_ENDPOINT，建議您將其修改為新的VPC端點類型。使用此新端點類型時，您不再需要使用 Network Load Balancer（NLB）將彈性 IP 地址與伺服器的端點建立關聯。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。

下列程序假設您有一個伺服器使用目前的公有端點類型或較舊的VPC_ENDPOINT類型。

變更伺服器的端點類型

1. 在 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. 選取您要變更其端點類型的伺服器的核取方塊。

 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，選擇停止以確認您想要停止伺服器。

 Note

在繼續下一個步驟之前，在端點詳細資訊 中，等待伺服器狀態變更為離線；這可能需要幾分鐘的時間。您可能需要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. 在端點詳細資訊 中，選擇編輯。

7. 在編輯端點組態 中，執行下列動作：

- a. 對於編輯端點類型，選擇VPC託管的。
- b. 針對存取，選擇下列其中一項：
 - 內部，讓端點只能使用端點私有 IP 地址的用戶端存取。
 - 網際網路面向，讓用戶端可透過公有網際網路存取您的端點。

 Note

當您選擇面向網際網路時，您可以選擇每個子網路或子網路中現有的彈性 IP 地址。或者，您可以前往VPC主控台（<https://console.aws.amazon.com/vpc/>）配置一或多個新的彈性 IP 地址。這些地址可由您擁有或 AWS 由您擁有。您無法將已在端點上使用的彈性 IP 地址建立關聯。

c. （僅適用於網際網路面向存取的選用）對於自訂主機名稱，請選擇下列其中一項：

- Amazon Route 53 DNS 別名 – 如果您要使用的主機名稱已向 Route 53 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提供者註冊。然後，您可以輸入主機名稱。

- 無 – 使用伺服器的端點，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`。

若要進一步了解如何使用自訂主機名稱，請參閱 [使用自訂主機名稱](#)。

- d. 針對 VPC，選擇現有的 VPC ID，或選擇建立 VPC以建立新的 VPC。
- e. 在可用區域區段中，選取最多三個可用區域和相關聯的子網路。如果選擇網際網路面向，也請為每個子網路選擇彈性 IP 地址。

Note

如果您想要最多三個可用區域，但沒有足夠的可用，請在VPC主控台（ ）中建立可用區域<https://console.aws.amazon.com/vpc/>。

如果您修改子網路或彈性 IP 地址，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 Save (儲存)。

8. 對於動作，選擇開始並等待伺服器狀態變更為線上；這可能需要幾分鐘的時間。

Note

如果您將公有端點類型變更為VPC端點類型，請注意您伺服器的端點類型已變更為 VPC。

預設安全群組會連接至端點。若要變更或新增其他安全群組，請參閱[建立安全群組](#)。

停止使用 VPC_ENDPOINT

AWS Transfer Family 正在停止EndpointType=VPC_ENDPOINT為新 AWS 帳戶使用 建立伺服器的功能。自 2021 年 5 月 19 日起，不擁有端點類型為之 AWS Transfer Family 伺服器 AWS 的帳戶VPC_ENDPOINT將無法使用 建立新的伺服器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盡快開始使用。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](#)。

我們在 2020 年稍早推出新的VPC端點類型。如需詳細資訊，請參閱 [AWS Transfer Family 的 SFTP支援VPC安全群組和彈性 IP 地址](#)。這個新端點的功能更豐富且符合成本效益，而且不 PrivateLink 收取費用。如需詳細資訊，請參閱[AWS PrivateLink 定價](#)。

此端點類型在功能上相當於先前的端點類型（VPC_ENDPOINT）。您可以直接將彈性 IP 地址連接至端點，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，以保護 AWS Transfer Family 適用於SFTP伺服器的](#) 部落格文章。

您也可以在此共用環境中託管此端點VPC。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 之外SFTP，您可以使用 VPCEndpointType來啟用 FTPS和 FTP。我們不打算將這些功能和 FTPS/FTP支援新增至 EndpointType=VPC_ENDPOINT。我們也從 AWS Transfer Family 主控台中移除此端點類型作為選項。

您可以使用 Transfer Family 主控台、AWS CLI、APISDKs或 變更伺服器的端點類型 AWS CloudFormation。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_ENDPOINT 更新為 VPC](#)。

如果您有任何問題，請聯絡 AWS 支援 或您的 AWS 客戶團隊。

Note

我們不打算將這些功能和FTPS/或FTP支援新增至 EndpointType=VPC_ENDPOINT。我們不再提供它作為 AWS Transfer Family 主控台上的選項。

如果您有其他問題，可以透過 AWS 支援 或您的客戶團隊與我們聯絡。

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

您可以使用 AWS Management Console AWS CloudFormation、或 Transfer Family，API將伺服器的 EndpointType 從 更新VPC_ENDPOINT為 VPC。下列各節提供使用每種方法來更新伺服器端點類型的詳細程序和範例。如果您在多個 AWS 區域和多個 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進行修改，以使用您需要更新的VPC_ENDPOINT類型來識別伺服器。

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 更新伺服器 API](#)

使用VPC_ENDPOINT端點類型識別伺服器

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

使用主控台使用VPC_ENDPOINT端點類型識別伺服器

1. 在 開啟 AWS Transfer Family 主控台<https://console.aws.amazon.com/transfer/>。
2. 在導覽窗格中選擇伺服器，以顯示您帳戶中該區域的伺服器清單。
3. 依端點類型排序伺服器清單，以查看使用 的所有伺服器VPC_ENDPOINT。

VPC_ENDPOINT 跨多個 AWS 區域和帳戶使用 識別伺服器

如果您在多個 AWS 區域和多個 AWS 帳戶中有伺服器，您可以使用下列範例指令碼進行修改，以使用VPC_ENDPOINT端點類型識別伺服器。範例指令碼使用 Amazon EC2[DescribeRegions](#)和 Transfer Family [ListServers](#)API呼叫，以取得使用 的所有伺服器的伺服器IDs和區域的清單VPC_ENDPOINT。如果您有多個 AWS 帳戶，如果您使用工作階段設定檔向身分提供者進行身分驗證，則可以使用具有僅供讀取稽核員存取權IAM的角色來循環瀏覽您的帳戶。

1. 以下是簡單的範例。

```
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後，您可以使用下列各節所述的其中一種方法，將 更新EndpointType為 VPC。

使用 更新伺服器端點類型 AWS Management Console

1. 在 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. 選取您要變更其端點類型的伺服器的核取方塊。

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，選擇停止以確認您想要停止伺服器。

Note

在繼續下一個步驟之前，請等待伺服器狀態變更為離線；這可能需要幾分鐘的時間。您可能需要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 後，選擇要顯示伺服器詳細資訊頁面的伺服器。
7. 在端點詳細資訊區段中，選擇編輯。
8. 針對端點類型 選擇VPC託管。
9. 選擇儲存
10. 對於動作，選擇開始並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 將伺服器的 更新EndpointType為 VPC。針對您已使用 部署的 Transfer Family 伺服器，請使用此程序 AWS CloudFormation。在此範例中，用於部署 Transfer Family 伺服器的原始 AWS CloudFormation 範本如下所示：

```
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

```

範本會更新為下列變更：

- EndpointType 已變更為 VPC。
- AWS::EC2::VPCEndpoint 資源已移除。
- SecurityGroupId、SubnetIds 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
```

使用 更新部署的 Transfer Family 伺服器端點類型 AWS CloudFormation

1. 使用下列步驟停止您要更新的伺服器。
 - a. 在 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. 選取您要變更其端點類型的伺服器的核取方塊。

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，選擇停止以確認您想要停止伺服器。

Note

在繼續下一個步驟之前，請等待伺服器狀態變更為離線；這可能需要幾分鐘的時間。您可能需要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. 在 <https://console.aws.amazon.com/cloudformation> 開啟 AWS CloudFormation 主控台。
- b. 選擇用於建立 Transfer Family 伺服器的堆疊。
- c. 選擇更新。
- d. 選擇取代目前範本
- e. 上傳新範本。CloudFormation 變更集可協助您了解範本變更將如何影響執行中的資源，然後再實作它們。在此範例中，轉接伺服器資源將被修改，而VPCEndpoint資源將被移除。VPC端點類型伺服器會代表您建立VPC端點，取代原始VPCEndpoint資源。

上傳新範本後，變更集看起來會類似以下內容：

Change set preview				
Changes (2)				
Search changes				
Action	Logical ID	Physical ID	Resource type	Replacement
Modify	TransferServer	arn:aws:transfer:us-east-1:364810874344:server/s-6a7d04e12d494ec98	AWS::Transfer::Server	Conditional
Remove	VPCEndpoint	vpce-04e685f8702849573 ↗	AWS::EC2::VPCEndpoint	-

- f. 更新堆疊。
3. 堆疊更新完成後，請前往位於的 Transfer Family 管理主控台<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，然後從動作功能表中選擇開始。

EndpointType 使用 更新伺服器 API

您可以使用 [describe-server](#) AWS CLI 命令或 [UpdateServer](#) API命令。下列範例指令碼會停止 Transfer Family 伺服器、更新 EndpointType、移除 VPC_ENDPOINT並啟動伺服器。

```
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連線到伺服器時，在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，您可以使用自訂主機名稱，例如 `mysftpserver.mysubdomain.domain.com`。

若要將流量從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）供應商。Route 53 是 AWS Transfer Family 原生支援DNS的服務。

主題

- [使用 Amazon Route 53 作為您的DNS供應商](#)
- [使用其他DNS供應商](#)
- [非主控台建立伺服器的自訂主機名稱](#)

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 Route 53 DNS 別名 – 如果您要使用的主機名稱已向 Route 53 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提供者註冊。然後，您可以輸入主機名稱。
- 無 – 使用伺服器的端點，不使用自訂主機名稱。

當您建立新的伺服器或編輯現有伺服器的組態時，請設定此選項。如需建立新伺服器的詳細資訊，請參閱 [步驟 2：建立已啟用 SFTP的伺服器](#)。如需有關編輯現有伺服器組態的詳細資訊，請參閱 [編輯伺服器詳細資訊](#)。

如需將自己的網域用於伺服器主機名稱以及如何 AWS Transfer Family 使用 Route 53 的詳細資訊，請參閱下列各節。

使用 Amazon Route 53 作為您的DNS供應商

建立伺服器時，您可以使用 Amazon Route 53 作為DNS提供者。將網域與 Route 53 搭配使用之前，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 [網域註冊如何運作](#)。

當您使用 Route 53 提供DNS路由至伺服器時，AWS Transfer Family 會使用您輸入的自訂主機名稱來擷取其託管區域。當 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，但沒有託管區域，會 AWS Transfer Family 新增新的託管區域和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 中有託管區域，而沒有任何CNAME記錄，會將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。

 Note

如果此步驟是伺服器建立工作流程的一部分，您的伺服器已成功建立，並且您的自訂主機名稱設定為無。

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

建立伺服器時，您也可以使用 Amazon Route 53 以外的DNS供應商。如果您使用替代DNS提供者，請確定來自您網域的流量已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。端點主機名稱在主控台中看起來像這樣：

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，VPC請在伺服器的詳細資訊頁面上選取，然後在VPC儀表板上選取VPC端點 ID。端點是列出的端點DNS的名字。

非主控台建立伺服器的自訂主機名稱

當您使用 AWS Cloud Development Kit (AWS CDK) AWS CloudFormation、或透過 建立伺服器時 CLI，如果您想要該伺服器具有自訂主機名稱，則必須新增標籤。當您使用主控台建立 Transfer Family 伺服器時，會自動完成標記。

 Note

您也需要建立DNS記錄，將流量從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](#)。

針對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 作為DNS供應商，請新增 `transfer:route53HostedZoneId`。此標籤會將自訂主機名稱連結至 Route 53 Hosted Zone ID。

若要新增自訂主機名稱，請發出下列CLI命令。

```
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，請發出下列命令，將自訂主機名稱連結至 Route 53 Hosted Zone 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，請執行下列命令以檢視您的標籤：

```
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

您的公有、託管區域及其IDs可在 Amazon Route 53 上使用。
登入 AWS Management Console 並在 開啟 Route 53 主控台<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操作，透過 AWS Transfer Family 服務傳輸檔案。AWS Transfer Family 支援下列用戶端：

- 我們支援第 3 版的SFTP通訊協定。
- 開啟SSH（macOS 和 Linux）

Note

此用戶端僅適用於啟用 Secure Shell（SSH）檔案傳輸通訊協定（）的伺服器SFTP。

- WinSCP（僅限 Microsoft Windows）
- Cyberduck（Windows、macOS 和 Linux）
- FileZilla（Windows、macOS 和 Linux）

下列限制適用於每個用戶端：

- 每個連線的並行多工SFTP工作階段數目上限為 10。
- Amazon S3 和 Amazon EFS（由於NFSv4通訊協定）需要檔案名稱為 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（FTPS）的檔案傳輸通訊協定，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 STREAM 模式。
- 對於 FTP和 FTPS，僅支援映像/二進位模式。
- 對於 FTP和 FTPS，TLS資料連線的 TLS - PROT C（未受保護）是預設值，AWS Transfer Family FTPS但通訊協定不支援 PROT C。因此，對於 FTPS，您需要發出 PROT P 才能接受資料操作。

- 如果您將 Amazon S3 用於伺服器的儲存，且您的用戶端包含使用多個連線進行單次傳輸的選項，請務必停用此選項。否則，大型檔案上傳可能會以無法預測的方式失敗。請注意，如果您使用 Amazon EFS 作為儲存後端，EFS 會支援單一傳輸的多個連線。

以下是 FTP 和 的可用命令清單 FTPS：

可用命令					
ABOR	FEAT	MLST	PASS	RETR	STOR
AUTH	LANG	MKD	PASV	RMD	STOU
CDUP	LIST	MODE	PBSZ	RNFR	STRU
CWD	MDTM	NLST	PROT	RNTO	SYST
DELE	MFMT	NOOP	PWD	SIZE	TYPE
EPSV	MLSD	OPTS	QUIT	STAT	USER

Note

不支援 APPE。

對於 SFTP，使用 Amazon Elastic File System（Amazon）之伺服器上邏輯主目錄的使用者目前不支援下列操作 EFS。

不支援的 SFTP 命令			
SSH_FXP_R EADLINK	SSH_FXP_SYMLINK	SSH_FXP_STAT 當請 求的檔案為 symlink 時	SSH_FXP_R EALPATH 當請求的路 徑包含任何符號連結 元件時

產生公有-私有金鑰對

您必須先有公有私有金鑰對可供使用，才能傳輸檔案。如果您先前尚未產生金鑰對，請參閱 [為受服務管理的使用者產生SSH金鑰](#)。

主題

- [可用的SFTP/FTPS/FTP命令](#)
- [尋找您的 Amazon VPC端點](#)
- [避免setstat錯誤](#)
- [使用開啟SSH](#)
- [使用 WinSCP](#)
- [使用 Cyberduck](#)
- [使用 FileZilla](#)
- [使用 Perl 用戶端](#)
- [上傳後處理](#)

可用的SFTP/FTPS/FTP命令

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

Note

資料表提到 Amazon S3 的檔案和目錄，僅支援儲存貯體和物件：沒有階層。不過，您可以在物件金鑰名稱中使用字首來暗示階層，並以類似於資料夾的方式整理資料。此行為會在 Amazon Simple Storage Service 使用者指南 中的 [使用物件中繼資料](#) 中說明。

SFTP/FTPS/FTP 命令

Command	Amazon S3	Amazon EFS
cd	支援	支援
chgrp	不支援	支援（root 或 owner 專用）
chmod	不支援	支援（root僅限）
chmtime	不支援	支援

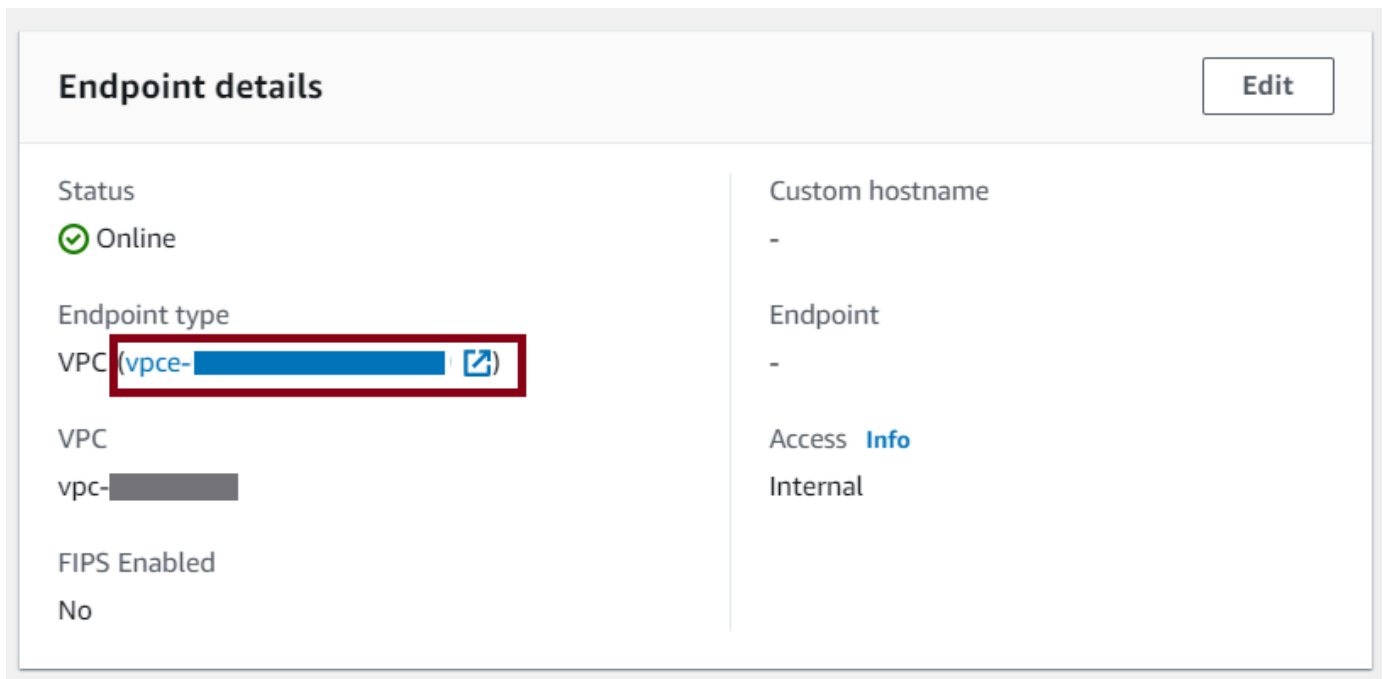
Command	Amazon S3	Amazon EFS
chown	不支援	支援 (root僅限)
get	支援	支援 (包括解析符號連結)
ln -s	不支援	支援
ls/dir	支援	支援
mkdir	支援	支援
put	支援	支援
pwd	支援	支援
rename	僅支援 檔案	支援  Note 不支援重新命名會覆寫現有檔案或目錄。
rm	支援	支援
rmdir	支援 (僅限空白目錄)	支援
version	支援	支援

尋找您的 Amazon VPC端點

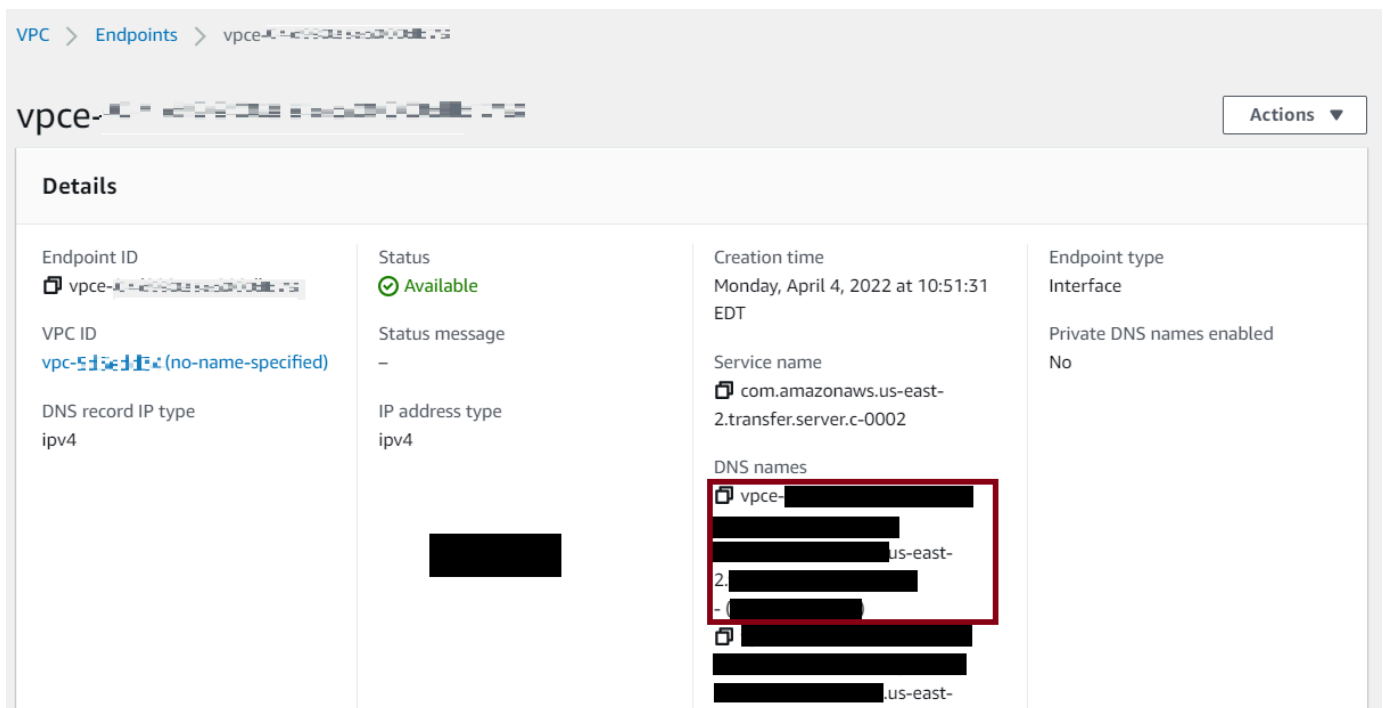
如果 Transfer Family 伺服器的端點類型為 VPC，則識別用於傳輸檔案的端點並不簡單。在此情況下，請使用下列程序尋找您的 Amazon VPC端點。

尋找您的 Amazon VPC端點

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



3. 在 Amazon VPC 儀表板中，選取 VPC 端點 ID。
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

有些SFTP檔案傳輸用戶端可能會嘗試使用 `setstat` 命令來變更遠端檔案的屬性，包括時間戳記和許可，例如上傳檔案SETSTAT時。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` 時API，請使用 `ProtocolDetails` 選項 `SetStatOption` 來忽略當用戶端嘗試在您上傳到 S3 儲存貯體的檔案SETSTAT上使用時所產生的錯誤。
- 將值設定為 `ENABLE_NO_OP`，讓 Transfer Family 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 日誌中產生日誌項目，因此您可以判斷用戶端何時SETSTAT撥打電話。

如需此選項API的詳細資訊，請參閱 [ProtocolDetails](#)。

使用開啟SSH

使用下列指示，使用 `Open` 來從命令列傳輸檔案SSH。

Note

此用戶端僅適用於SFTP已啟用的伺服器。

AWS Transfer Family 使用開啟SSH命令列公用程式傳輸檔案

- 在 Linux、macOS 或 Windows 上，開啟命令終端機。
- 在提示中，輸入下列命令：

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

在上述命令中，*sftp_user* 是使用者名稱，*transfer-key* 是SSH私有金鑰。此處 *service_endpoint* 是伺服器端點，如所選伺服器的 AWS Transfer Family 主控台所示。

Note

此命令會使用預設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。您可以新增 **-P** 旗標至命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，如果您始終要使用連接埠 2222，則可以更新ssh_config檔案中的預設連接埠。

應會出現 sftp 提示。

3. （選用）若要檢視使用者的主目錄，請在sftp提示中輸入下列命令：

```
pwd
```

4. 若要將檔案從檔案系統上傳至 Transfer Family 伺服器，請使用 put 命令。例如，若要上傳 hello.txt（假設檔案位於檔案系統上目前的目錄中），請在sftp提示中執行下列命令：

```
put hello.txt
```

出現類似下列的訊息，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

建立伺服器後，伺服器端點主機名稱可能需要幾分鐘的時間，才能由環境中DNS的服務解決。

使用 WinSCP

使用下列指示，使用 Win 傳輸命令列中的檔案SCP。

 Note

如果您使用的是 WinSCP 5.19，則可以使用 AWS 憑證直接連線至 Amazon S3，並上傳/下載檔案。如需詳細資訊，請參閱[連線至 Amazon S3 服務](#)。

AWS Transfer Family 使用 Win 傳輸檔案SCP

1. 開啟 WinSCP 用戶端。
2. 在登入對話方塊中，針對檔案通訊協定，選擇通訊協定：SFTP或FTP。

如果您選擇 FTP，請在加密 中，選擇下列其中一項：

- 無加密 FTP
 - TLS/SSL 的明確加密 FTPS
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訊頁面上。如需詳細資訊，請參閱[檢視 SFTP、FTPS和 FTP 伺服器詳細資訊](#)。

 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，輸入下列內容：
 - 適用於 SFTP 的 22
 - 21 適用於 FTP/FTPS
5. 在使用者名稱 中，輸入您為特定身分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 提供下列身分提供者：

- [使用服務受管使用者](#)
- [使用 AWS Directory Service 身分提供者](#)
- [使用自訂身分提供者](#)

6. 選擇進階以開啟進階網站設定對話方塊。在 SSH區段中，選擇身分驗證。

7. 對於私有金鑰檔案，瀏覽 並從檔案系統選擇SSH私有金鑰檔案。

 Note

如果 WinSCP 提議將SSH私有金鑰轉換為 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站台對話方塊中，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，針對轉接，選擇持久性。

對於啟用傳輸履歷/轉移至選項的暫存檔案名稱，請選擇停用。

 Note

如果您讓此選項保持啟用狀態，會增加上傳成本，大幅降低上傳效能。它也可能導致大型檔案上傳失敗。

12. 針對轉接，選擇背景，然後清除使用多個連線進行單一轉接核取方塊。

 Note

如果您選取此選項，大型檔案上傳可能會以無法預測的方式失敗。例如，可以建立產生 Amazon S3 費用的孤立分段上傳。也可能發生無聲資料損毀。

13. 執行檔案傳輸。

您可以使用 drag-and-drop方法來複製目標和來源視窗之間的檔案。您可以使用工具列圖示來上傳、下載、刪除、編輯或修改 Win 中的檔案屬性SCP。

 Note

如果您使用 Amazon EFS進行儲存，則不適用此備註。

嘗試變更遠端檔案屬性的命令，包括時間戳記，與 Amazon S3 等物件儲存系統不相容。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（或使用 SetStatOption中所述的 [避免setstat錯誤](#)）。若要這麼做，請在 WinSCP Transfer 設定對話方塊中停用設定許可上傳選項和保留時間戳記常用選項。

使用 Cyberduck

使用下列說明使用 Cyberduck 從命令列傳輸檔案。

AWS Transfer Family 使用 Cyberduck 傳輸檔案

1. 開啟 [Cyberduck](#) 用戶端。
2. 選擇開啟連線。
3. 在開啟連線對話方塊中，選擇通訊協定：SFTP（SSH 檔案傳輸通訊協定）、FTP-SSL（明確 TLS）或 AUTH FTP（檔案傳輸通訊協定）。
4. 對於伺服器，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。如需詳細資訊，請參閱[檢視 SFTP、FTPS和 FTP 伺服器詳細資訊](#)。

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，輸入下列內容：
 - 適用於 SFTP 的 **22**
 - **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. SFTP 如果已選取，則對於SSH私密金鑰，選擇或輸入SSH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，然後將其拖放至 Amazon S3 目錄（目標）。
- 在 Amazon S3 目錄（來源）中，選擇要傳輸的檔案，然後將其拖放至本機目錄（目標）。

使用 FileZilla

使用下列指示來使用 傳輸檔案 FileZilla。

FileZilla 設定檔案傳輸

1. 開啟 FileZilla 用戶端。
2. 選擇檔案 ，然後選擇 Site Manager 。
3. 在 Site Manager 對話方塊中，選擇新網站 。
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，請在加密 中，選擇下列其中一項：

- 僅使用純 FTP (不安全) – 用於 FTP
 - 如果可用TLS，請使用明確的 FTP - 適用於 FTPS
5. 對於主機名稱 ，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訊頁面上。如需詳細資訊，請參閱[檢視 SFTP、FTPS和 FTP 伺服器詳細資訊](#)。

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`

請務必取代 *hostname* 實際的伺服器端點。

6. 針對連接埠號碼 ，輸入下列內容：
 - 適用於 SFTP 的 **22**
 - **21** 適用於 FTP/FTPS
7. SFTP 如果選取，對於登入類型 ，選擇金鑰檔案 。

針對金鑰檔案，選擇或輸入SSH私有金鑰。

8. 針對使用者，輸入您在 中建立的使用者名稱[管理伺服器端點的使用者](#)。
9. 選擇連線。
10. 執行檔案傳輸。

 Note

如果您中斷進行中的檔案傳輸，AWS Transfer Family 可能會寫入 Amazon S3 儲存貯體中的部分物件。如果您中斷上傳，請檢查 Amazon S3 儲存貯體中的檔案大小是否符合來源物件的檔案大小，然後再繼續。

使用 Perl 用戶端

如果您使用 perl NET::SFTP::Foreign 用戶端，則必須將 `queue_size` 設定為 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 修訂需要此解決方法。

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 物件中繼資料](#)
- [Amazon S3 事件通知](#)

Amazon S3 物件中繼資料

作為物件中繼資料的一部分，您會看到名為 的索引鍵 `x-amz-meta-user-agent`，其值為 `AWSTransfer`，`x-amz-meta-user-agent-id` 而其值為 `username@server-id`。username 是上傳檔案的 Transfer Family 使用者，server-id 也是用於上傳的伺服器。您可以使用 Lambda 函數內 S3 物件 [HeadObject](#) 的操作來存取此資訊。

Key	Value
Content-Type	text/plain
x-amz-meta-user-agent	AWSTransfer
x-amz-meta-user-agent-id	sftp_user@s-

Amazon S3 事件通知

使用 Transfer Family 將物件上傳至 S3 儲存貯體時，[S3 事件通知結構](#)中的請求者欄位中RoleSessionName會包含 作為 [AWS:Role Unique Identifier]/username.sessionid@server-id。例如，以下是從複製到 S3 儲存貯體之檔案的 S3 存取日誌中的範例請求者欄位的內容。S3

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

在上方的請求者欄位中，會顯示名為 IAM的角色IamRoleName。如需設定 S3 事件通知的詳細資訊，請參閱 [Amazon Simple Storage Service 開發人員指南 中的設定 Amazon S3 事件通知](#)。如需 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，您可以找到如何使用 AWS Transfer Family或 AWS Directory Service for Microsoft Active Directory 自訂身分提供者新增使用者的相關資訊。

如果您使用服務管理的身分類型，您可以將使用者新增至已啟用檔案傳輸通訊協定的伺服器。執行此操作時，伺服器上的每個使用者名稱都必須是唯一的。

作為每個使用者屬性的一部分，您還可以存放該使用者的 Secure Shell (SSH) 公有金鑰。此程序使用的金鑰型身分驗證需要執行此操作。私有金鑰儲存在使用者電腦上的本機。當您的使用者使用用戶端

傳送身分驗證請求至伺服器時，您的伺服器會先確認使用者有權存取相關聯的SSH私有金鑰。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，並將 AWS Identity and Access Management (IAM) 角色指派給使用者。或者，您可以提供工作階段政策，以限制使用者只能存取 Amazon S3 儲存貯體的主目錄。

Important

AWS Transfer Family 會封鎖從身分驗證到SFTP伺服器的 1 或 2 個字元的使用者名稱。此外，我們也封鎖root使用者名稱。原因在於密碼掃描器嘗試大量惡意登入。

Amazon EFS與 Amazon S3

每個儲存選項的特徵：

- 若要限制存取：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 IDs
- 兩者都支援公有/私有金鑰
- 兩者都支援主目錄
- 兩者都支援邏輯目錄

Note

對於 Amazon S3，對邏輯目錄的大多數支援是透過 API/CLI。您可以使用主控台內的受限核取方塊，將使用者鎖定到其主目錄，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，您使用的參數取決於使用者的類型。

- 對於服務受管使用者，請在 中提供邏輯目錄值HomeDirectoryMappings。
- 對於自訂身分提供者使用者，請在 中提供邏輯目錄值HomeDirectoryDetails。

主題

- [使用服務受管使用者](#)
- [使用 AWS Directory Service 身分提供者](#)
- [使用自訂身分提供者](#)

使用服務受管使用者

視伺服器的網域設定而定，您可以將 Amazon S3 或 Amazon EFS 服務管理的使用者新增至伺服器。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受管使用者，請參閱 [的範例 CreateUser API](#)。

Note

對於服務受管使用者，限制為 2,000 個邏輯目錄項目。如需使用邏輯目錄的相關資訊，請參閱 [使用邏輯目錄來簡化 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](#)
- [管理服務受管使用者](#)

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，請依照本 Knowledge Center 文章所述步驟進行：[如何設定我的 AWS Transfer Family 伺服器以使用另一個 AWS 帳戶中的 Amazon Simple Storage Service 儲存貯體？](#)

將 Amazon S3 服務受管使用者新增至您的伺服器

1. 在開啟 AWS Transfer Family 主控台 <https://console.aws.amazon.com/transfer/>，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之伺服器的核取方塊。

3. 選擇新增使用者。
4. 在使用者組態區段中，針對使用者名稱 輸入使用者名稱。此使用者名稱必須至少為 3 個字元，最多為 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 '-'、句點 '.' 和符號 "@"。使用者名稱不能以連字號 '-'、句點 '.' 或符號 "@" 開頭。
5. 針對存取，選擇您先前建立的角色，該IAM角色可讓您存取 Amazon S3 儲存貯體。

您已使用 中的程序建立此IAM角色[建立IAM角色和政策](#)。該IAM角色包含提供 Amazon S3 儲存貯體存取權IAM的政策。它還包括與 AWS Transfer Family 服務的信任關係，如其他IAM政策所定義。如果您需要精細的存取控制，請參閱[使用 AWS Transfer Family 和 Amazon S3 部落格文章增強資料存取控制](#)。

6. (選用) 針對政策，選取下列其中一項：
 - 無
 - 現有政策
 - 從 中選取政策IAM：可讓您選擇現有的工作階段政策。選擇檢視以查看包含政策詳細資訊的JSON物件。
 - 根據主資料夾自動產生政策：會為您產生工作階段政策。選擇檢視以查看包含政策詳細資訊的JSON物件。

 Note

如果您選擇根據主資料夾 自動產生政策，請勿為此使用者選取限制。

若要進一步了解工作階段政策，請參閱 [建立IAM角色和政策](#)。若要進一步了解如何建立工作階段政策，請參閱 [為 Amazon S3 儲存貯體建立工作階段政策](#)。

7. 對於主目錄，選擇 Amazon S3 儲存貯體以存放要使用 傳輸的資料 AWS Transfer Family。輸入使用者使用其用戶端登入時所到達的home目錄路徑。

如果您將此參數保留空白，則會使用 Amazon S3 儲存貯體的root目錄。在此情況下，請確定您的IAM角色提供此root目錄的存取權。

 Note

我們建議您選擇包含使用者名稱的目錄路徑，這可讓您有效地使用工作階段政策。工作階段政策會將 Amazon S3 儲存貯體中的使用者存取權限制為該使用者的home目錄。

8. (選用) 對於受限，選取核取方塊，讓您的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

為使用者指派主目錄，並將使用者限制為該主目錄，應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，請使用工作階段政策。
如果您為此使用者選取限制，則無法根據主資料夾來選取自動產生政策，因為主資料夾不是受限制使用者的定義值。

9. 針對SSH公有金鑰，輸入SSH金鑰對的公有SSH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金鑰對的指示，請參閱 [為受服務管理的使用者產生SSH金鑰](#)。

10. (選用) 針對金鑰和值，輸入一或多個標籤作為鍵值對，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。

新使用者會出現在伺服器詳細資訊頁面的使用者區段中。

後續步驟：在後續步驟中，請繼續至 [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介面 (POSIX) 檔案許可模型來表示檔案擁有權。

- 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. 在開啟 AWS Transfer Family 主控台<https://console.aws.amazon.com/transfer/>，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，最多為 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 '-'、句點 '.' 和符號 "@"。使用者名稱不能以連字號 '-'、句點 '.' 或符號 "@" 開頭。
- b. 對於使用者 ID 和群組 ID，請注意下列事項：
 - 對於您建立的第一個使用者，建議您為群組 ID 和使用者 ID 輸入的值。這會授予 Amazon 的使用者管理員權限 EFS。
 - 對於其他使用者，輸入使用者 POSIX 的使用者 ID 和群組 ID。這些 IDs 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** 是可接受的，**012345** 是不可接受的。
- c. (選用) 對於次要群組 IDs，IDs 輸入每個使用者的一或多個額外 POSIX 群組，以逗號分隔。
- d. 針對 Access，選擇下列 IAM 角色：
 - 僅提供使用者存取您希望他們存取的 Amazon EFS 資源（檔案系統）。
 - 定義使用者可以和不可以執行的檔案系統操作。

我們建議您使用 IAM 角色來選取 Amazon EFS 檔案系統，並具有掛載存取和讀取/寫入許可。例如，以下兩個 AWS 受管政策的組合雖然相當寬鬆，會為您的使用者授予必要的許可：

- AmazonElasticFileSystemClientFullAccess
- AWSTransferConsoleFullAccess

如需詳細資訊，請參閱 [AWS Transfer Family Amazon Elastic File System 的部落格文章支援](#)。

- e. 對於主目錄，請執行下列動作：
 - 選擇您要用來儲存資料的 Amazon EFS 檔案系統，以便使用進行傳輸 AWS Transfer Family。
 - 決定是否將主目錄設定為受限制。將主目錄設定為受限制具有下列影響：
 - Amazon EFS 使用者無法存取該資料夾以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

當您選取限制選項時，不會為 Amazon EFS 使用者解析符號連結。

- (選用) 輸入使用者使用其用戶端登入時，要加入的主目錄路徑。

如果您未指定主目錄，則會使用 Amazon EFS 檔案系統的根目錄。在此情況下，請確定您的 IAM 角色提供此根目錄的存取權。

5. 針對 SSH 公有金鑰，輸入 SSH 金鑰對的公有 SSH 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 金鑰對的指示，請參閱 [為受服務管理的使用者產生 SSH 金鑰](#)。

6. (選用) 輸入使用者的任何標籤。對於金鑰和值，輸入一或多個標籤作為鍵值對，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。

新使用者會出現在伺服器詳細資訊頁面的使用者區段中。

您第一次 SFTP 存取 Transfer Family 伺服器時可能遇到的問題：

- 如果您執行 `sftp` 命令而提示未出現，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政策許可。您可以新增受 AWS 管政策，例如 `AmazonElasticFileSystemClientFullAccess`。

- 如果您在 `sftp` 提示 `pwd` 中輸入以檢視使用者的主目錄，您可能會看到下列訊息，其中 ***USER-HOME-DIRECTORY*** 是 SFTP 使用者的主目錄：

```
remote readdir("/USER-HOME-DIRECTORY"): No such file or directory
```


在此情況下，您應該能夠導覽至父目錄（`cd ..`），並建立使用者的主目錄（`mkdir username`）。

後續步驟 – 對於下一個步驟，請繼續至 [使用用戶端透過伺服器端點傳輸檔案](#)。

管理服務受管使用者

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SSH公有金鑰的資訊。

- [檢視使用者清單](#)
- [檢視或編輯使用者詳細資訊](#)
- [刪除使用者](#)
- [新增SSH公有金鑰](#)
- [刪除SSH公有金鑰](#)

尋找使用者清單

1. 在 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 欄中選擇識別符，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. 在 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 欄中選擇識別符，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訊頁面。

您可以選擇編輯，變更此頁面上的使用者屬性。

5. 在使用者詳細資訊頁面上，選擇使用者組態旁的編輯。

Edit configuration

User configuration

Access Info
User's IAM role for Amazon S3 access

Admin ▼ ↻

Policy Info
Scope down policy to apply to the user

☒ None
☐ Existing policy
☐ Select a policy from IAM

View

Home directory
User's login directory

Choose an S3 bucket ▼

Enter optional folder

☐ Restricted Info

Cancel Save

6. 在編輯組態頁面上，針對存取，選擇IAM您先前建立的角色，以存取您的 Amazon S3 儲存貯體。

您已使用 中的程序建立此IAM角色[建立IAM角色和政策](#)。該IAM角色包含提供 Amazon S3 儲存貯體存取權IAM的政策。它還包括與 AWS Transfer Family 服務的信任關係，如其他IAM政策所定義。

7. （選用）針對政策，選擇下列其中一項：

- 無
- 現有政策
- 從中選取政策IAM，以選擇現有政策。選擇檢視以查看包含政策詳細資訊的JSON物件。

若要進一步了解工作階段政策，請參閱 [建立IAM角色和政策](#)。若要進一步了解如何建立工作階段政策，請參閱 [為 Amazon S3 儲存貯體建立工作階段政策](#)。

8. 對於主目錄，選擇 Amazon S3 儲存貯體以存放要使用 傳輸的資料 AWS Transfer Family。輸入使用者使用其用戶端登入時所到達的home目錄路徑。

如果您將此參數保留空白，則會使用 Amazon S3 儲存貯體的root目錄。在此情況下，請確定您的IAM角色提供此root目錄的存取權。

 Note

我們建議您選擇包含使用者名稱的目錄路徑，這可讓您有效地使用工作階段政策。工作階段政策會將 Amazon S3 儲存貯體中的使用者存取權限制為該使用者的home目錄。

9. (選用) 針對限制，選取核取方塊，讓您的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

為使用者指派主目錄，並將使用者限制為該主目錄時，這應足以鎖定使用者對指定資料夾的存取權。當您需要套用進一步控制項時，請使用工作階段政策。

10. 選擇儲存，以儲存變更。

若要刪除使用者

1. 在開啟 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 欄中選擇識別符，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訊頁面。
5. 在使用者詳細資訊頁面上，選擇使用者名稱右側的刪除。
6. 在出現的確認對話方塊中，輸入字詞 **delete**，然後選擇刪除以確認您想要刪除使用者。

使用者會從使用者清單中刪除。

為使用者新增SSH公有金鑰

1. 在開啟 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訊頁面。
5. 選擇新增SSH公有金鑰，將新的SSH公有金鑰新增至使用者。

 Note

SSH 金鑰僅供針對 Secure Shell (SSH) 檔案傳輸通訊協定 () 啟用的伺服器使用 SFTP。如需有關如何產生SSH金鑰對的資訊，請參閱 [為受服務管理的使用者產生SSH金鑰](#)。

6. 對於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 金鑰的格式為 `ssh-rsa string`。若要產生SSH金鑰對，請參閱 [為受服務管理的使用者產生SSH金鑰](#)。

7. 選擇 Add key (新增金鑰)。

刪除使用者的SSH公有金鑰

1. 在開啟 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 欄中選擇識別符，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訊頁面。
5. 若要刪除公有金鑰，請選取其SSH金鑰核取方塊，然後選擇刪除。

使用 AWS Directory Service 身分提供者

本主題說明如何使用適用於的 AWS Directory Service 身分提供者 AWS Transfer Family。

主題

- [使用 AWS Directory Service for Microsoft Active Directory](#)
- [使用 AWS Directory Service for Azure Active Directory 網域服務](#)

使用 AWS Directory Service for Microsoft Active Directory

您可以使用 AWS Transfer Family 來驗證檔案傳輸最終使用者 AWS Directory Service for Microsoft Active Directory。它可無縫遷移依賴 Active Directory 身分驗證的檔案傳輸工作流程，而無需變更最終使用者的憑證或需要自訂授權方。

使用 AWS Managed Microsoft AD，您可以安全地透過 SFTP、FTPS 和 為存放在 Amazon Simple Storage Service (Amazon S3) 或 Amazon Elastic File System (Amazon) 中的資料提供 AWS Directory Service 使用者和群組存取權 EFS。如果您使用 Active Directory 來存放使用者的憑證，您現在有更簡單的方法可以為這些使用者啟用檔案傳輸。

您可以使用 Active Directory 連接器，AWS Managed Microsoft AD 在內部部署環境中或在 AWS 雲端中提供 Active Directory 群組的存取權。您可以讓已在 Microsoft Windows 環境中設定的使用者存取用於身分 AWS Managed Microsoft AD 的 AWS Transfer Family 伺服器，無論是在 AWS 雲端或其內部部署網路中。

Note

- AWS Transfer Family 不支援 Simple AD。
- Transfer Family 不支援跨區域 Active Directory 組態：我們僅支援與 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 來啟用現有 RADIUS 型 MFA 基礎設施的多重要素身分驗證 (MFA)。
- AWS Transfer Family 不支援 Managed Active Directory 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 AWS Directory Service 主控台建立一或多個 AWS Managed Microsoft AD 目錄。
2. 使用 Transfer Family 主控台來建立使用 AWS Managed Microsoft AD 作為其身分提供者的伺服器。
3. 從一或多個 AWS Directory Service 群組新增存取權。
4. 雖然並非必要，但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 Active Directory 領域](#)
- [選擇 AWS Managed Microsoft AD 作為您的身分提供者](#)
- [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 連線至伺服器 SSH \(Secure Shell \)](#)
- [使用樹系和信任 AWS Transfer Family 連線到自我管理的 Active Directory](#)

開始使用 之前 AWS Directory Service for Microsoft Active Directory

為您的 AD 群組提供唯一識別碼

您必須先為 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識別碼（SID）來執行此操作。您關聯的群組使用者可透過使用 AWS Transfer Family 啟用的通訊協定存取您的 Amazon S3 或 Amazon EFS 資源。

使用下列 Windows PowerShell 命令來擷取群組SID的，取代 *YourGroupName* 群組的名稱。

```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties * | Select SamAccountName, ObjectSid
```

Note

如果您使用 AWS Directory Service 作為身分提供者，且 userPrincipalName 和 SamAccountName 具有不同的值，則 AWS Transfer Family 接受 中的值 SamAccountName。Transfer Family 不接受 中指定的值 userPrincipalName。

將 AWS Directory Service 許可新增至您的角色

您也需要 AWS Directory Service API 許可才能使用 AWS Directory Service 作為身分提供者。需要或建議下列許可：

- ds:DescribeDirectories Transfer Family 需要 才能查詢目錄
- ds:AuthorizeApplication 需要 才能新增 Transfer Family 的授權
- ds:UnauthorizeApplication 建議移除任何臨時建立的資源，以防伺服器建立過程中發生問題

將這些許可新增至您用來建立 Transfer Family 伺服器的角色。如需這些許可的詳細資訊，請參閱 [AWS Directory Service API 許可：動作、資源和條件參考](#)。

使用 Active Directory 領域

當您考慮如何讓 Active Directory 使用者存取 AWS Transfer Family 伺服器時，請記住使用者的領域及其群組的領域。理想情況下，使用者的領域及其群組的領域應該相符。也就是說，使用者和群組都位於預設領域中，或兩者都位於信任領域中。如果不是這種情況，則 Transfer Family 無法驗證使用者。

您可以測試使用者，以確保組態正確。如需詳細資訊，請參閱 [測試使用者](#)。如果使用者/群組領域發生問題，您會收到錯誤，找不到使用者群組 的相關存取權。

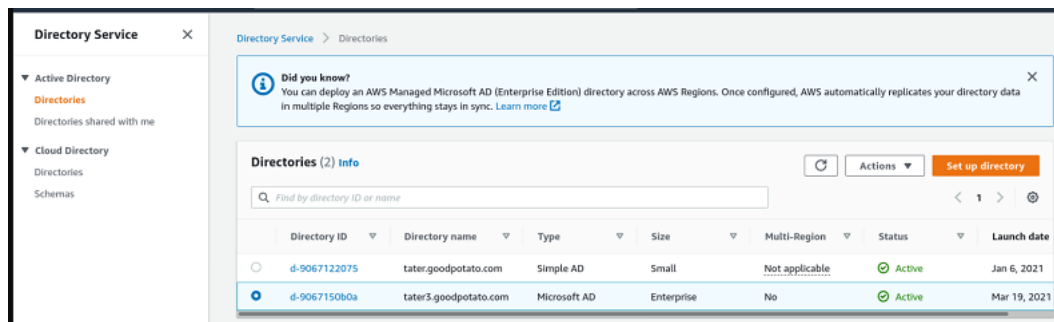
選擇 AWS Managed Microsoft AD 作為您的身分提供者

本節說明如何 AWS Directory Service for Microsoft Active Directory 搭配伺服器使用。

AWS Managed Microsoft AD 與 Transfer Family 搭配使用

1. 登入 AWS Management Console 並在 開啟 AWS Directory Service 主控台<https://console.aws.amazon.com/directoryservicev2/>。

使用 AWS Directory Service 主控台設定一或多個受管目錄。如需詳細資訊，請參閱《AWS Directory Service 管理員指南》中的 [AWS Managed Microsoft AD](#)。



2. 在 開啟 AWS Transfer Family 主控台<https://console.aws.amazon.com/transfer/>，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

如果您選擇 FTPS，則必須提供 AWS Certificate Manager 憑證。

4. 對於選擇身分提供者，選擇 AWS Directory Service。

Choose an identity provider

Identity provider

Identity provider type

An identity provider manages user access for authentication and authorization



Service managed

Create and manage users within the service



AWS Directory Service [Info](#)

Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS



Custom Identity Provider [Info](#)

Manage users by integrating an identity provider of your choice

Directory

TATER3

Cancel

Previous

Next

5. 目錄清單包含您已設定的所有受管目錄。從清單中選擇目錄，然後選擇下一個。

Note

- 不支援跨帳戶和共用目錄 AWS Managed Microsoft AD。
- 若要使用 Directory Service 作為身分提供者來設定伺服器，您需要新增一些 AWS Directory Service 許可。如需詳細資訊，請參閱 [開始使用 之前 AWS Directory Service for Microsoft Active Directory](#)。

6. 若要完成建立伺服器，請使用下列其中一個程序：

- [建立已啟用 SFTP的伺服器](#)
- [建立已啟用 FTPS的伺服器](#)
- [建立已啟用 FTP的伺服器](#)

在這些程序中，繼續執行選擇身分提供者之後的步驟。

 Important

AWS Directory Service 如果您在 Transfer Family 伺服器中使用 Microsoft AD 目錄，則無法刪除 中的 Microsoft AD 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具有使用上傳和下載已啟用通訊協定檔案的存取權 AWS Transfer Family。您可以建立存取權 來執行此操作。

 Note

使用者必須直接屬於您要授予存取權的群組。例如，假設 Bob 是使用者，他屬於 groupA，且 groupA 本身包含在 groupB 中。

- 如果您授予 groupA 的存取權，Bob 會獲得存取權。
- 如果您授予 groupB 的存取權（而不是 groupA），Bob 沒有存取權。

授予群組存取權

1. 在 開啟 AWS Transfer Family 主控台 <https://console.aws.amazon.com/transfer/>。
2. 導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。
4. 輸入您要存取此伺服器的 AWS Managed Microsoft AD 目錄SID的。

 Note

如需有關如何SID為您的群組尋找的資訊，請參閱 [the section called “開始使用 之前 AWS Directory Service for Microsoft Active Directory”](#)。

5. 針對存取，選擇群組的 AWS Identity and Access Management（IAM）角色。
6. 在政策區段中，選擇政策。預設設定為無。
7. 針對主目錄，選擇與群組的主目錄對應的 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儲存貯體部分。例如，若要將使用者限制為/filetest目錄下的自有資料夾，請在方塊中輸入下列文字。

```
/filetest/${transfer:UserName}
```

若要進一步了解如何建立工作階段政策，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。

- 輸入群組SID的。

 Note

如需有關如何尋找的資訊SID，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。

在存取區段中，會列出伺服器的存取。

The screenshot displays the AWS Transfer Family console interface. At the top, the 'Endpoint configuration' section shows the 'Availability Zone' as 'us-east-1a', the 'Subnet ID' as 'subnet-...', and the 'Private IPv4 Address' as '172.31.80.36'. Below this, the 'Accesses (1)' section features a search bar, an 'Actions' dropdown menu, and an 'Associate access' button. A table lists the access details with columns for 'External Id', 'Home directory', and 'Role'. The first entry shows 'S...', '/padbucket3', and 'ADGuy_S3_And_EFS'. The 'Additional details' section at the bottom includes 'Logging role' (Server activity not logged to Amazon CloudWatch), 'Server host key', 'Security Policy' (TransferSecurityPolicy-2018-11), and 'Domain' (Amazon S3). An 'Edit' button is located in the top right of the 'Additional details' section.

測試使用者

您可以測試使用者是否可以存取伺服器的 AWS Managed Microsoft AD 目錄。

Note

使用者必須正好位於端點組態頁面的存取區段中列出的一個群組（外部 ID）。如果使用者未處於任何群組中，或位於多個單一群組中，則不會授予該使用者存取權。

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. 對於身分提供者測試，輸入位於其中一個具有存取權群組中的使用者的登入憑證。
3. 選擇 測試。

您會看到成功的身分提供者測試，顯示選取的使用者已獲得伺服器存取權。

Identity provider testing

User configuration [Info](#)

Username

transferuser1

Password

Response

```
{
  "Response": {
    "homeDirectory": {"/":"/padbucket3"}, {"homeDirectoryDetails": null}, {"homeDirectoryType": "PATH"}, {"posixProfile":
    null}, {"publicKeys": null}, {"role": "arn:aws:iam::195886157073:role/ADGuy_SS_Aud_EFS"}, {"policy": null}, {"userName":
    "transferuser1"}, {"identityProviderType": null}, {"userConfigMessage": null}
  },
  "StatusCode": 200,
  "Message": ""
}
```

Cancel

Test

如果使用者屬於多個具有存取權的群組，則會收到下列回應。

```
"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

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。
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，您會看到不再列出此群組的存取權。

使用 連線至伺服器 SSH (Secure Shell)

設定伺服器和使用者之後，您可以使用 連線至伺服器，SSH並為具有存取權的使用者使用完整格式的使用者名稱。

```
sftp user@active-directory-domain@vpc-endpoint
```

例如：transferuserexample@mycompany.com@vpce-0123456abcdef-789xyz.vpc-svc-987654zyxabc.us-east-1.vpc.amazonaws.com。

此格式以聯合搜尋為目標，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。不過，在此情況下，Active Directory 程式碼必須搜尋聯合中的所有目錄。這可能會限制搜尋，即使使用者應具有存取權，身分驗證也可能會失敗。

驗證後，使用者會位於您在設定使用者時指定的主目錄中。

使用樹系和信任 AWS Transfer Family 連線到自我管理的 Active Directory

自我管理 Active Directory (AD) 中的使用者也可以 AWS IAM Identity Center 用於單一登入存取 AWS 帳戶和 Transfer Family 伺服器。若要這麼做，AWS Directory Service 具有下列可用選項：

- 單向森林信任（內部部署 Active Directory 的傳出 AWS Managed Microsoft AD 和傳入）僅適用於根網域。
- 對於子網域，您可以使用下列其中一項：
 - 在 AWS Managed Microsoft AD 和內部部署 Active Directory 之間使用雙向信任
 - 對每個子網域使用單向外部信任。

使用受信任網域連線至伺服器時，使用者需要指定受信任網域，例如 transferuserexample@mycompany.com。

使用 AWS Directory Service for Azure Active Directory 網域服務

- 若要利用現有的 Active Directory 樹系來滿足您的SFTP轉接需求，您可以使用 [Active Directory Connector](#)。
- 如果您想要 Active Directory 的優點和完全受管服務的高可用性，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 身分提供者](#)。

本主題說明如何使用 Active Directory Connector 和 [Azure Active Directory 網域服務 \(Azure ADDS\)](#) 透過 [Azure Active Directory](#) 來驗證 SFTP Transfer 使用者。

主題

- [開始使用 AWS Directory Service for Azure Active Directory 網域服務之前](#)
- [步驟 1：新增 Azure Active Directory 網域服務](#)
- [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](#)

開始使用 AWS Directory Service for Azure Active Directory 網域服務之前

對於 AWS，您需要下列項目：

- 在您使用 Transfer Family 伺服器的 AWS 區域中的虛擬私有雲端（VPC）
- 您的 VPC 中至少有兩個私有子網路 VPC
- VPC 必須有網際網路連線
- 用於與 Microsoft Azure VPN連線的客戶閘道和虛擬私有閘道 site-to-site

對於 Microsoft Azure，您需要下列項目：

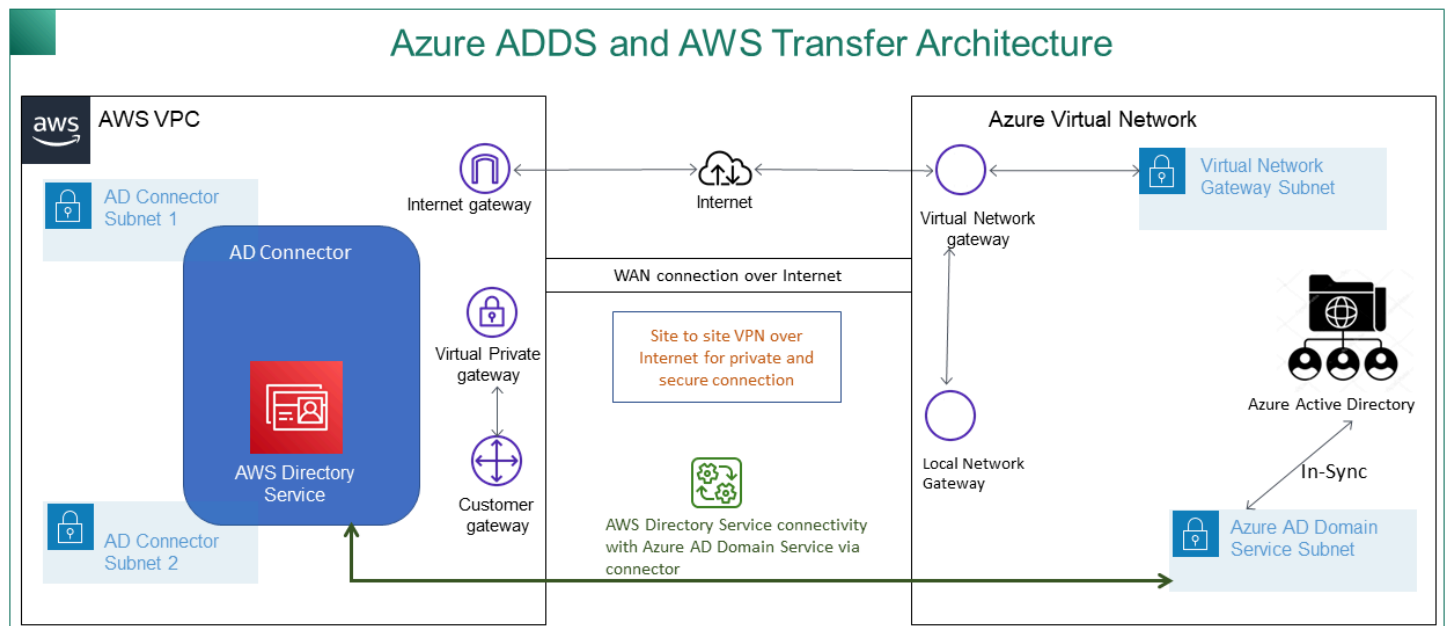
- Azure Active Directory 和 Active Directory 網域服務（Azure ADDS）
- Azure 資源群組
- Azure 虛擬網路
- VPN Amazon VPC與 Azure 資源群組之間的連線

Note

這可以透過原生IPSEC通道或使用 VPN 設備。在本主題中，我們會在 Azure Virtual 網路閘道與本機網路閘道之間使用IPSEC通道。必須設定通道，以允許 Azure ADDS端點與存放的子網路之間的流量 AWS VPC。

- 用於與 Microsoft Azure VPN連線的客戶閘道和虛擬私有閘道 site-to-site

下圖顯示開始之前所需的組態。



步驟 1：新增 Azure Active Directory 網域服務

預設情況下，Azure AD 不支援網域加入執行個體。若要執行網域聯結等動作，以及使用群組政策等工具，管理員必須啟用 Azure Active Directory 網域服務。如果您尚未新增 Azure AD DS，或現有的實作未與您希望 SFTP 轉接伺服器使用的網域建立關聯，則必須新增執行個體。

如需啟用 Azure Active Directory 網域服務（Azure ADDS）的相關資訊，[請參閱教學課程：建立和設定 Azure Active Directory 網域服務受管網域](#)。

Note

當您啟用 Azure 時 ADDS，請確定已針對您要連線 SFTP Transfer Server 的資源群組和 Azure AD 網域進行設定。

bob.us ...
Azure AD Domain Services

Search (Cmd+/) << Refresh Delete

Overview
Activity log
Access control (IAM)
Tags
Settings
Diagnostics

Configuration issues for your managed domain were detected. Run configuration diagnostics.

bob.us Running
[View health](#)

步驟 2：建立服務帳戶

Azure AD 必須有一個服務帳戶，屬於 Azure 中的管理群組ADDS。此帳戶會與 AWS Active Directory 連接器搭配使用。請確定此帳戶與 Azure 同步ADDS。

[Home](#) > [Default Directory](#) > [Users](#) > [bobatusa](#)

bobatusa | Profile ...
User

Diagnose and solve problems

Manage

- Profile
- Assigned roles
- Administrative units
- Groups
- Applications
- Licenses
- Devices
- Azure role assignments
- Authentication methods

Activity

- Sign-in logs
- Audit logs

bobatusa
bobsmith@xyz.com

SU

Creation time
10/6/2021, 1:32:27 AM

Identity

Name	First name	Last name
bobatusa	Bob	Smith

User Principal Name	User type
bobsmith@xyz.com	Member

User Sign-ins

Group memberships: 2

Oct 10 Oct 17 Oct 24 Oct 31

Tip

使用 SFTP通訊協定的 Transfer Family 伺服器不支援 Azure Active Directory 的多重要素驗證。Transfer Family 伺服器無法在使用者向進行身分驗證後提供MFA權杖SFTP。嘗試連線MFA之前，請務必停用。

multi-factor authentication
users service settings

Note: only users licensed to use Microsoft Online Services are eligible for Multi-Factor Authentication. [Learn more about how to license other users.](#)
Before you begin, take a look at the [multi-factor auth deployment guide](#).

View: Sign-in allowed users Multi-Factor Auth status: Any bulk update

☐	DISPLAY NAME ^	USER NAME	MULTI-FACTOR AUTH STATUS
☐	Christopher	admin@christopher.com	Disabled
☐	Robert	test@christopher.com	Disabled

Select a user

步驟 3：使用 AD Connector 設定 AWS 目錄

設定 Azure ADDS並建立服務帳戶，並在您的 AWS VPC 和 Azure Virtual 網路之間建立IPSECVPN通道後，您可以從任何 AWS EC2執行個體 ping Azure ADDS DNS IP 地址來測試連線。

確認連線作用中後，您可以在下面繼續。

使用 AD Connector 設定您的 AWS 目錄

1. 開啟 [Directory Service](#) 主控台，然後選取目錄。
2. 選取設定目錄。
3. 針對目錄類型，選擇 AD Connector。
4. 選取目錄大小，選取下一個，然後選取您的 VPC和子網路。
5. 選取下一個，然後依下列方式填寫欄位：
 - 目錄DNS名稱：輸入您用於 Azure 的網域名稱ADDS。
 - DNS IP 地址：輸入您的 Azure ADDS IP 地址。
 - 伺服器帳戶使用者名稱和密碼：輸入您在步驟 2 中建立的服務帳戶詳細資訊：建立服務帳戶。
6. 完成畫面以建立目錄服務。

現在目錄狀態應為作用中，並準備好與 SFTP Transfer 伺服器搭配使用。

Directory Service > Directories

 **Did you know?**
You can deploy an AWS Managed Microsoft AD (Enterprise Edition) directory across AWS Regions. Once configured, AWS automatically replicates your directory data in multiple Regions so everything stays in sync. [Learn more](#)

Directories (1) [Info](#)



Actions ▾

Set up directory

< 1 > 

	Directory ID ▾	Directory name ▾	Type ▾	Size ▾	Multi-Region ▾	Status ▾	Launch date ▾
☐	d-906752c0d7		AD Connector	Small	Not applicable	 Active	Nov 3, 2021

步驟 4：設定 AWS Transfer Family 伺服器

使用 SFTP 通訊協定和 AWS Directory Service 的身分提供者類型來建立 Transfer Family 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 伺服器中使用 Microsoft AD 目錄，則無法刪除 AWS 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具有使用上傳和下載已啟用通訊協定的檔案的存取權 AWS Transfer Family。您可以透過建立存取來執行此操作。

Note

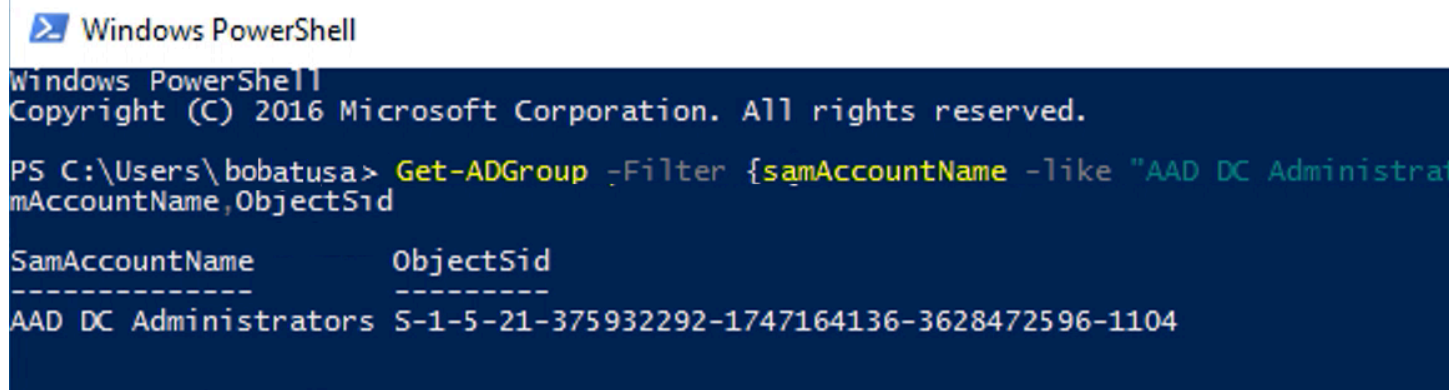
使用者必須直接屬於您要授予存取權的群組。例如，假設 Bob 是使用者，他屬於 groupA，且 groupA 本身包含在 groupB 中。

- 如果您授予 groupA 的存取權，Bob 會獲得存取權。
- 如果您授予 groupB 的存取權（而不是 groupA），Bob 就無法存取。

若要授予存取權，您需要擷取群組 SID 的。

使用下列 Windows PowerShell 命令來擷取群組SID的，取代 *YourGroupName* 群組的名稱。

```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties * | Select  
SamAccountName,ObjectSid
```



```
Windows PowerShell  
Copyright (C) 2016 Microsoft Corporation. All rights reserved.  
  
PS C:\Users\bobatusa> Get-ADGroup -Filter {samAccountName -like "AAD DC Administrat  
mAccountName,ObjectSid  
  
SamAccountName      ObjectSid  
-----  
AAD DC Administrators S-1-5-21-375932292-1747164136-3628472596-1104
```

授予對群組的存取權

1. 開啟 <https://console.aws.amazon.com/transfer/>。
2. 導覽至您的伺服器詳細資訊頁面，然後在存取區段中，選擇新增存取。
3. 輸入SID您從先前程序的輸出中收到的。
4. 針對存取，選擇群組 AWS Identity and Access Management 的角色。
5. 在政策區段中，選擇政策。預設值為 None (無)。
6. 針對主目錄，選擇與群組的主目錄對應的 S3 儲存貯體。
7. 選擇新增以建立關聯。

Transfer 伺服器的詳細資訊看起來應該類似以下內容：

Protocols	Identity provider
Protocols over which clients can connect to your server's endpoint SFTP	Identity provider type AWS Directory Service Directory ID d-123456789a

Accesses (1)				Actions ▾	Add access
< 1 >					
☐	External Id ▾	Home directory ▾	Role ▾		
☐	S-1-5-21-375932292-1747164136-3628472596-1104	/usr/bin/sftp	sftp-user-role ↗		

步驟 6：測試使用者

您可以測試（[測試使用者](#)）使用者是否可以存取您伺服器的 AWS Managed Microsoft AD 目錄。使用者必須正好位於端點組態頁面的存取區段中列出的一個群組（外部 ID）。如果使用者未處於任何群組中，或位於多個單一群組中，則不會授予該使用者存取權。

使用自訂身分提供者

若要驗證您的使用者，您可以將現有的身分提供者與搭配使用 AWS Transfer Family。您可以使用函數整合身分提供者，該 AWS Lambda 函數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[使用 AWS Lambda 整合您的身分提供者](#)。您也可以存取 CloudWatch 圖表以取得指標，例如在 AWS Transfer Family 管理主控台中傳輸的檔案數和位元組數，為您提供單一面板，以使用集中式儀表板監控檔案傳輸。

或者，您可以使用單一 Amazon API Gateway 方法提供 RESTful 介面。Transfer Family 會呼叫此方法，以連線至您的身分提供者，該提供者會驗證並授權您的使用者存取 Amazon S3 或 Amazon EFS。如果您需要 RESTful API 整合身分提供者，或如果您想要使用 AWS WAF 來利用其功能進行地理封鎖或速率限制請求，請使用此選項。如需詳細資訊，請參閱[使用 Amazon API Gateway 整合您的身分提供者](#)。

無論哪種情況，您都可以使用[AWS Transfer Family 主控台](#)或建立新的伺服器 [CreateServer](#) API 操作。

Note

我們有一個您可以參加的研討會，您可以在其中建置檔案傳輸解決方案。此解決方案 AWS Transfer Family 會利用受管 SFTP/FTPS 端點和 Amazon Cognito 和 DynamoDB 進行使用者管理。您可以[在這裡檢視此研討會的詳細資訊](#)。

AWS Transfer Family 提供下列選項，以使用自訂身分提供者。

- 使用 AWS Lambda 來連接您的身分提供者 – 您可以使用現有的身分提供者，並由 Lambda 函數提供支援。您提供 Lambda 函數的名稱。如需詳細資訊，請參閱[使用 AWS Lambda 整合您的身分提供者](#)。
- 使用 Amazon API Gateway 來連接您的身分提供者 – 您可以建立由 Lambda 函數支援的 API 閘道方法，以用作身分提供者。您提供 Amazon API Gateway URL 和調用角色。如需詳細資訊，請參閱[使用 Amazon API Gateway 整合您的身分提供者](#)。

對於任一選項，您也可以指定如何驗證。

- 密碼或金鑰 – 使用者可以使用其密碼或金鑰進行身分驗證。這是預設值。
- 密碼 ONLY – 使用者必須提供密碼才能連線。
- 金鑰 ONLY – 使用者必須提供其私有金鑰才能連線。
- 密碼 AND 金鑰 – 使用者必須提供其私有金鑰和密碼才能連線。伺服器會先檢查金鑰，如果金鑰有效，系統會提示輸入密碼。如果提供的私有金鑰與儲存的公有金鑰不相符，身分驗證會失敗。

使用多種身分驗證方法與您的自訂身分提供者進行身分驗證

使用多種身分驗證方法時，Transfer Family 伺服器會控制 AND 邏輯。Transfer Family 會將此視為兩個單獨的請求給您的自訂身分提供者：不過，它們會合併其效果。

這兩個請求都必須成功傳回正確的回應，才能完成身分驗證。Transfer Family 需要兩個回應才能完成，這表示它們包含所有必要的元素（角色、主目錄、政策和 POSIX 設定檔，如果您使用 Amazon EFS 進行儲存）。Transfer Family 也要求密碼回應不得包含公有金鑰。

公有金鑰請求必須與身分提供者有單獨的回應。使用 Password OR Key 或 Password AND Key 時，該行為保持不變。

SSH/SFTP 通訊協定會先使用公有金鑰身分驗證來挑戰軟體用戶端，然後請求密碼身分驗證。在允許使用者完成身分驗證之前，此操作要求兩者都成功。

主題

- [使用 AWS Lambda 整合您的身分提供者](#)
- [使用 Amazon API Gateway 整合您的身分提供者](#)

使用 AWS Lambda 整合您的身分提供者

建立連接至自訂身分提供者的 AWS Lambda 函數。您可以使用任何自訂身分提供者，例如 Okta、Secrets Manager、OneLogin 或包含授權和身分驗證邏輯的自訂資料存放區。

Note

建立使用 Lambda 作為身分提供者的 Transfer Family 伺服器之前，您必須建立 函數。如需 Lambda 函數的範例，請參閱 [Lambda 函數範例](#)。或者，您可以部署使用其中一個的 CloudFormation 堆疊 [Lambda 函數範本](#)。此外，請確定您的 Lambda 函數使用信任 Transfer Family 的資源型政策。如需政策範例，請參閱 [Lambda 資源型政策](#)。

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。對於選擇身分提供者，請選擇自訂身分提供者，如下列螢幕擷取畫面所示。

Choose an identity provider

Identity Provider for SFTP, FTPS, or FTP

Identity provider type

An identity provider manages user access for authentication and authorization

☐ Service managed

Create and manage users within the service

☐ AWS Directory Service [Info](#)

Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☒ Custom Identity Provider [Info](#)

Manage users by integrating an identity provider of your choice

☒ Use AWS Lambda to connect your identity provider [Info](#)

Invoke an AWS Lambda function to call your identity provider's API for user authentication and authorization

☐ Use Amazon API Gateway to connect your identity provider [Info](#)

Use a RESTful API method to call your identity provider's API for user authentication and authorization

AWS Lambda function

Choose a Lambda function



Authentication methods

Choose which authentication methods are required for users to connect to your server

☒ Password OR public key

☐ Password ONLY

☐ Public Key ONLY

☐ Password AND public key

Either a valid password or valid private key will be required during user authentication

Cancel

Previous

Next

Note

只有在您啟用 SFTP 做為 Transfer Family 伺服器的其中一個通訊協定時，才可選擇身分驗證方法。

- 請確定已選取預設值，使用 AWS Lambda 來連接您的身分提供者。
- 針對 AWS Lambda 函數，選擇 Lambda 函數的名稱。
- 填寫其餘方塊，然後選擇建立伺服器。如需建立伺服器之其餘步驟的詳細資訊，請參閱 [設定 SFTP、FTPS 或 FTP 伺服器端點](#)。

Lambda 資源型政策

您必須具有參考 Transfer Family 伺服器 and Lambda 的政策ARNs。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。政策會JSON作為字串逸出。

```
"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

在上述政策範例中，取代每個 *user input placeholder* 使用您自己的資訊。

事件訊息結構

從SFTP伺服器傳送至自訂授權方 Lambda 函數的事件訊息結構IDP如下所示。

```
{
  'username': 'value',
  'password': 'value',
  'protocol': 'SFTP',
  'serverId': 's-abcd123456',
```



```
'sourceIp': '192.168.0.100'  
}
```

其中 `username` 和 `password` 是傳送至伺服器的登入憑證值。

例如，您輸入下列命令進行連線：

```
sftp bobusa@server_hostname
```

然後，系統會提示您輸入密碼：

```
Enter password:  
mysecretpassword
```

您可以從 Lambda 函數內列印傳遞的事件，以從您的 Lambda 函數檢查此項目。它看起來應該類似於下列文字區塊。

```
{  
  'username': 'bobusa',  
  'password': 'mysecretpassword',  
  'protocol': 'SFTP',  
  'serverId': 's-abcd123456',  
  'sourceIp': '192.168.0.100'  
}
```

FTP 和 的事件結構類似FTPS：唯一的差異是這些值用於 `protocol` 參數，而不是 SFTP。

用於身分驗證的 Lambda 函數

若要實作不同的身分驗證策略，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 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 函數範本](#)
- [有效的 Lambda 值](#)
- [Lambda 函數範例](#)
- [測試您的組態](#)

Lambda 函數範本

您可以部署使用 Lambda 函數進行身分驗證的 AWS CloudFormation 堆疊。我們提供多種範本，使用登入憑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，以進一步自訂使用者存取權。

Note

您可以在範本中指定 FIPS 已啟用的安全政策 AWS CloudFormation，藉此透過 建立 FIPS 已啟用的 AWS Transfer Family 伺服器。可用的安全政策說明於 [的安全政策 AWS Transfer Family](#)

若要建立用於身分驗證的 AWS CloudFormation 堆疊

1. 在 <https://console.aws.amazon.com/cloudformation> 開啟 AWS CloudFormation 主控台。
2. 請遵循 AWS CloudFormation 使用者指南 中的 AWS CloudFormation 從現有範本部署 [堆疊](#) 的指示。
3. 使用下列其中一個範本來建立 Lambda 函數，以在 Transfer Family 中用於身分驗證。

- [Classic \(Amazon Cognito 堆疊範本](#)

用於在 中建立 AWS Lambda 以用作自訂身分提供者的基本範本 AWS Transfer Family。如果使用以公有金鑰為基礎的身分驗證，它會針對 Amazon Cognito 進行身分驗證，而公有金鑰會從 Amazon S3 儲存貯體傳回。部署之後，您可以修改 Lambda 函數程式碼，以執行不同的動作。

- [AWS Secrets Manager 堆疊範本](#)

使用 AWS Lambda 與 AWS Transfer Family 伺服器整合 Secrets Manager 作為身分提供者的基本範本。它會根據格式為 AWS Secrets Manager 的項目進行身分驗證 `aws/transfer/server-id/username`。此外，秘密必須保留傳回 Transfer Family 的所有使用者屬性的鍵值對。部署之後，您可以修改 Lambda 函數程式碼，以執行不同的動作。

- [Okta 堆疊範本](#)：使用 AWS Lambda 與 AWS Transfer Family 伺服器整合 Okta 為自訂身分提供者的基本範本。
- [Okta-mfa 堆疊範本](#)：使用 AWS Lambda 與 AWS Transfer Family 伺服器整合 Okta 與 MultiFactor 身分驗證的基本範本，作為自訂身分提供者。
- [Azure Active Directory 範本](#)：此堆疊的詳細資訊請參閱 [AWS Transfer Family 使用 Azure Active Directory 和 驗證 AWS Lambda](#) 的部落格文章。

部署堆疊之後，您可以在 CloudFormation 主控台的輸出索引標籤上檢視其詳細資訊。

部署其中一個堆疊是將自訂身分提供者整合到 Transfer Family 工作流程的最簡單方法。

有效的 Lambda 值

下表說明 Transfer Family 接受用於自訂身分提供者的 Lambda 函數值的詳細資訊。

Value	描述	必要
Role	指定角色的 Amazon Resource Name (ARN)，該IAM 角色可控制使用者存取您的 Amazon S3 儲存貯體或 Amazon EFS 檔案系統。附加至此角色的政策會決定在將檔案移入和移出 Amazon S3 或 Amazon EFS 檔案系統時，您要為使用者提供的存取層級。此IAM角色也應包含信任關係，允許伺服器在服務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 IDs (SecondaryGids)，可控制使用者對 Amazon EFS 檔案系統的存取。檔案系統中檔案和目錄上設定的POSIX許可決定了使用者在將檔案移入和移出 Amazon EFS 檔案系統時所取得的存取層級。	Amazon EFS 後端儲存體的必要項目

Value	描述	必要
PublicKeys	對此使用者有效的SSH公有金鑰值清單。空清單表示這不是有效的登入。密碼驗證期間不得傳回。	選用
Policy	適用於使用者工作階段政策，讓您可以在多個使用者之間使用相同的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。 - 如果您將其設定為 PATH，則使用者會在其檔案傳輸通訊協定用戶端中看到絕對 Amazon S3 儲存貯體或 Amazon EFS 路徑。 - 如果您將其設定為 LOGICAL，則必須在 HomeDirectoryDetails 參數中提供映射，以便您的使用者可看見 Amazon S3 或 Amazon EFS 路徑。	選用

Value	描述	必要
HomeDirectoryDetails	邏輯目錄映射，指定哪些 Amazon S3 或 Amazon EFS 路徑和金鑰應該可供使用者查看，以及您希望如何讓使用者看見。您必須指定 Entry 和 Target 對，其中 Entry 顯示如何顯示路徑，並且 Target 是實際的 Amazon S3 或 Amazon EFS 路徑。	如果 的值 HomeDirectoryType 為 <code>LOGICAL</code> ，則為必填
HomeDirectory	使用者使用用戶端登入伺服器的登陸目錄。	選用

Note

HomeDirectoryDetails 是 JSON 地圖的字串表示法。這與相反 PosixProfile，是實際的 JSON 地圖物件，PublicKeys 也是字串 JSON 陣列。如需語言特定的詳細資訊，請參閱程式碼範例。

Lambda 函數範例

本節展示了 NodeJS 和 Python 中的一些 Lambda 函數範例。

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訊都是範例，而且必須以您的實際值取代。

Logical home directory, NodeJS

下列 NodeJS 範例函數為具有 [邏輯主目錄](#) 的使用者提供詳細資訊。

```
// 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 範例函數提供具有路徑型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 範例函數提供具有路徑型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
```

測試您的組態

建立自訂身分提供者之後，您應該測試您的組態。

Console

使用 AWS Transfer Family 主控台測試您的組態

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. 輸入您在部署 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，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 的 IP 地址，請選擇伺服器通訊協定並輸入它們。

CLI

使用 測試您的組態 AWS CLI

1. 執行 [test-identity-provider](#) 命令。將每個 替換 *user input placeholder* 為您自己的資訊，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，使用者名稱為 `myuser`，密碼為 `MySuperSecretPassword`。
4. 如果您在部署 AWS CloudFormation 堆疊時設定伺服器通訊協定和來源 IP 地址，請輸入它們。

如果使用者身分驗證成功，測試會傳回 `StatusCode: 200` HTTP 回應、空字串 `Message: ""`（其中包含失敗原因）和 `Response` 欄位。

Note

在下面的回應範例中，Response 欄位是「分層」的JSON物件（轉換為可在程式中使用的扁平JSON字串），其中包含使用者角色和許可的詳細資訊。

```
{
  "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 整合您的身分提供者

本主題說明如何使用 AWS Lambda 函數來傳回 API Gateway 方法。如果您需要 RESTful API 整合身分提供者，或如果您想要使用 AWS WAF 來利用其功能進行地理封鎖或速率限制請求，請使用此選項。

使用API閘道整合身分提供者的限制

- 此組態不支援自訂網域。
- 此組態不支援私有API閘道 URL。

如果您需要上述任何一項，您可以使用 Lambda 作為身分提供者，而不需要 API Gateway。如需詳細資訊，請參閱 [使用 AWS Lambda 整合您的身分提供者](#)。

使用API閘道方法進行驗證

您可以建立API閘道方法，以用作 Transfer Family 的身分提供者。此方法為您提供高度安全的方式來建立和提供 APIs。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傳入 API 呼叫。如需API閘道服務的詳細資訊，請參閱[API閘道開發人員指南](#)。

API Gateway 提供名為的授權方法AWS_IAM，它會根據內部 AWS 使用的 AWS Identity and Access Management (IAM) 為您提供相同的身分驗證。如果您使用 啟用身分驗證AWS_IAM，只有具有明確呼叫 許可的呼叫者API才能到達 API的API閘道方法。

若要使用 API Gateway 方法作為 Transfer Family 的自訂身分提供者，請 IAM 為 API Gateway 方法啟用。作為此程序的一部分，您會為 IAM 角色提供 Transfer Family 使用閘道的許可。

 Note

若要提高安全性，您可以設定 Web 應用程式防火牆。AWS WAF 是 Web 應用程式防火牆，可讓您監控轉送至 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](#)。

若要使用 API Gateway 方法來使用 Transfer Family 進行自訂身分驗證

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 範本的改進](#)。

- a. 在 <https://console.aws.amazon.com/cloudformation> 開啟 AWS CloudFormation 主控台。
- b. 請遵循 AWS CloudFormation 使用者指南 中的 AWS CloudFormation 從現有範本部署 [堆疊](#) 的指示。
- c. 使用下列其中一個基本範本建立 AWS Lambda 後端 API 閘道方法，以用作 Transfer Family 中的自訂身分提供者。

- [基本堆疊範本](#)

根據預設，您的 API Gateway 方法會用作自訂身分提供者，以使用硬式編碼 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，以執行不同的動作。

- [AWS Secrets Manager 堆疊範本](#)

根據預設，您的 API Gateway 方法會根據格式為 `aws/transfer/`*server-id*`/`*username* 的 Secrets Manager 中的項目進行身分驗證。此外，秘密必須保留傳回 Transfer Family 的所有使用者屬性的鍵值對。部署之後，您可以修改 Lambda 函數程式碼，以執行不同的動作。如需詳細資訊，請參閱部落格文章 [啟用 AWS Transfer Family 使用的密碼身分驗證 AWS Secrets Manager](#)。

- [Okta 堆疊範本](#)

您的 API Gateway 方法與 Okta 整合，作為 Transfer Family 中的自訂身分提供者。如需詳細資訊，請參閱使用 [Okta 作為具有之身分提供者 AWS Transfer Family](#) 的部落格文章。

部署其中一個堆疊是將自訂身分提供者整合到 Transfer Family 工作流程的最簡單方法。每個堆疊都使用 Lambda 函數來支援以 API Gateway 為基礎的 API 方法。然後，您可以在 Transfer Family 中將 API 方法用作自訂身分提供者。根據預設，Lambda 函數會驗證名為 myuser 且密碼為的單一使用者 MySuperSecretPassword。部署之後，您可以編輯這些憑證或更新 Lambda 函數程式碼，以執行不同的動作。

 Important

建議您編輯預設使用者和密碼憑證。

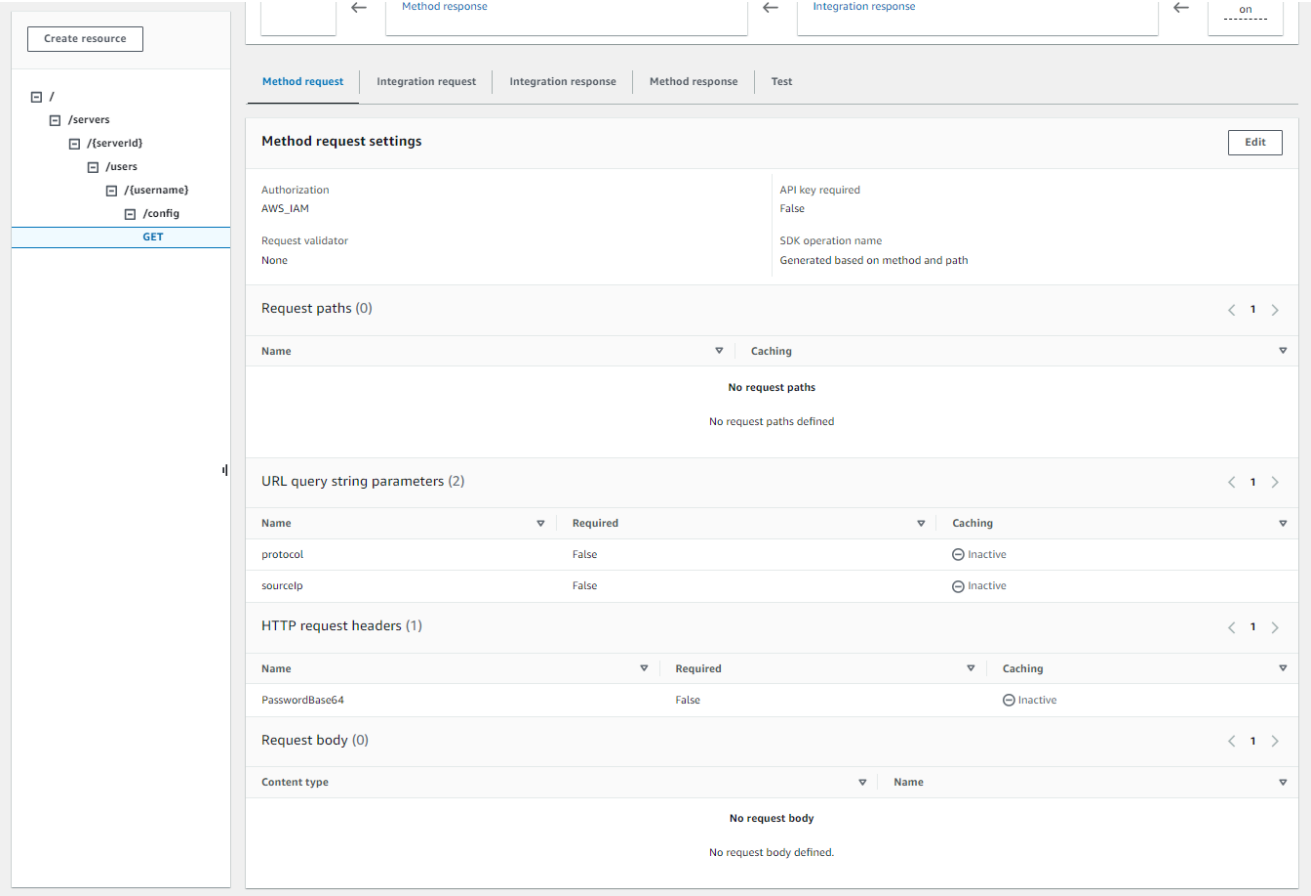
部署堆疊之後，您可以在 CloudFormation 主控台的輸出索引標籤上檢視其詳細資訊。這些詳細資訊包括堆疊的 Amazon Resource Name (ARN)、堆疊所建立 IAM 角色 ARN 的，以及新閘道 URL 的。

 Note

如果您使用自訂身分提供者選項為使用者啟用密碼型身分驗證，並啟用 API Gateway 提供的請求和回應記錄，API Gateway 會將使用者的密碼記錄到 Amazon CloudWatch Logs。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[API 閘道開發人員指南中的在閘道中設定 CloudWatch API 記錄](#)。API

2. 檢查伺服器的 API 閘道方法組態。若要執行此作業：

- a. 在開啟 API 閘道主控台 <https://console.aws.amazon.com/apigateway/>。
- b. 選擇 AWS CloudFormation 範本產生的 Transfer Custom Identity Provider 基本範本 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組態。



此時，您的API閘道已準備好進行部署。

3. 針對動作，選擇部署 API。針對部署階段，選擇產品，然後選擇部署。

成功部署API閘道方法後，請在階段 > 階段詳細資訊 中檢視其效能，如下列螢幕擷取畫面所示。

 Note

複製出現在畫面頂端的調用URL地址。您可能需要它進行下一個步驟。

The screenshot displays the AWS API Gateway console for a stage named 'prod'. The 'Stage details' section shows the following configuration:

Field	Value
Stage name	prod
API cache	Inactive
Rate	10000
Burst	5000
Web ACL	-
Client certificate	-
Invoke URL	https://[redacted].execute-api.us-east-1.amazonaws.com/prod

The 'Logs and tracing' section shows the following configuration:

Field	Value
CloudWatch logs	Error and info logs
Detailed metrics	Inactive
X-Ray tracing	Inactive
Custom access logging	Inactive

The 'Stage variables' section shows no variables associated with the stage.

4. 在 開啟 AWS Transfer Family 主控台 <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，請使用下列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，然後選擇使用 Amazon API Gateway 連線至您的身分提供者，如下列螢幕擷取畫面所示。

Choose an identity provider

Identity provider

Identity provider type
An identity provider manages user access for authentication and authorization

☐ **Service managed**
Create and manage users within the service

☐ **AWS Directory**
Service Info
Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☒ **Custom Identity Provider**
Info
Manage users by integrating an identity provider of your choice

☐ **Use AWS Lambda to connect your identity provider** **Info**
Invoke an AWS Lambda function to call your identity provider's API for user authentication and authorization

☒ **Use Amazon API Gateway to connect your identity provider** **Info**
Use a RESTful API method to call your identity provider's API for user authentication and authorization

Provide an Amazon API Gateway URL

https://abode1234.execute-api.us-east-2.amazonaws.com/prod

Role
IAM role for the service to invoke your Amazon API Gateway URL

Stack-name-TransferIdentityProviderRole-ABC123DEF456GHI

CancelPreviousNext

- 在提供 Amazon API Gateway URL 文字方塊中，貼上您在此程序的步驟 3 中建立的閘道端點的叫用 URL 地址。API
- 針對角色，選擇範本建立 IAM 的角色 AWS CloudFormation。此角色允許 Transfer Family 調用您的 API 閘道方法。

調用角色包含您在步驟 1 中為建立的 AWS CloudFormation 堆疊選取的堆疊名稱。其格式如下：**CloudFormation-stack-name-TransferIdentityProviderRole-ABC123DEF456GHI**。

- 填寫其餘方塊，然後選擇建立伺服器。如需建立伺服器之其餘步驟的詳細資訊，請參閱 [設定 SFTP、FTPS 或 FTP 伺服器端點](#)。

實作 API 閘道方法

若要為 Transfer Family 建立自訂身分提供者，您的 API Gateway 方法必須實作具有資源路徑的單一方法 `/servers/serverId/users/username/config`。*serverId* 和 *username* 值來自 RESTful

資源路徑。此外，請在方法請求 中將 `sourceIp` 和 新增 `protocol` 為 URL 查詢字串參數，如下圖所示。

Resources

Create resource

/servers/{serverId}/users/{username}/config - GET - Method execution

Update documentation Delete

ARN: arn:aws:execute-api:us-east-1:123456789012:*/GET/servers/{serverId}/users/{username}/config

Resource ID: aw4ihv

Client → Method request → Integration request → Lambda integration

← Method response ← Integration response

Method request Integration request Integration response Method response Test

Method request settings Edit

Authorization: AWS_IAM API key required: False

Request validator: None SDK operation name: Generated based on method and path

Request paths (0) < 1 >

Name	Caching
No request paths	
No request paths defined	

URL query string parameters (2) < 1 >

Name	Required	Caching
protocol	False	Inactive
sourceIp	False	Inactive

Note

使用者名稱必須至少為 3 個字元，最多為 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（-）、句點（.）和符號（@）。不過，使用者名稱不能以連字號（-）、句點（.）或符號（@）開頭。

如果 Transfer Family 嘗試為使用者進行密碼身分驗證，服務會提供 `Password:` 標頭欄位。如果沒有 `Password:` 標頭，Transfer Family 會嘗試使用公有金鑰身分驗證您的使用者。

當您使用身分提供者來驗證和授權最終使用者時，除了驗證其憑證之外，您還可以根據最終使用者使用的用戶端 IP 地址來允許或拒絕存取請求。您可以使用此功能來確保儲存在 S3 儲存貯體或 Amazon EFS 檔案系統中的資料只能透過您指定為受信任的 IP 地址，透過支援的通訊協定存取。若要啟用此功能，您必須在查詢字串 `sourceIp` 中包含。

如果您為伺服器啟用了多個通訊協定，並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，只要身分提供者已設定了每個通訊協定的特定憑證，您就可以這麼做。若要啟用此功能，您必須在 RESTful 資源路徑中包含 *protocol* 值。

Gateway API 方法應一律傳回 HTTP 狀態碼 200。任何其他 HTTP 狀態碼表示存取時發生錯誤 API。

Amazon S3 範例回應

回應內文範例是下列 Amazon S3 表單 JSON 的文件。

```
{
  "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

政策會 JSON 作為字串逸出。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\"}]
}"

```

下列回應範例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

回應內文範例是 Amazon 的下列表單JSON文件EFS。

```

{
  "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"
}

```

Role 欄位顯示已成功進行身分驗證。執行密碼身分驗證（提供Password:標頭時）時，您不需要提供SSH公有金鑰。如果無法驗證使用者，例如，如果密碼不正確，您的方法應該傳回未Role設定的回應。這種回應的範例是空JSON物件。

下列回應範例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。如需在 Transfer Family 中設定使用者政策的詳細資訊，請參閱 [管理存取控制](#)。

預設 Lambda 函數

若要實作不同的身分驗證策略，請編輯開道使用的 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 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（如果您執行密碼身分驗證）、伺服器 ID、通訊協定和用戶端 IP 地址。您可以使用這些輸入的組合來查詢您的身分提供者，並判斷是否應該接受登入。

Note

如果您為伺服器啟用了多個通訊協定，並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，只要身分提供者已設定了該通訊協定的特定憑證，您就可以這麼做。

對於檔案傳輸通訊協定（FTP），我們建議您透過 SSL（☐）維護與 Secure Shell（SSH）檔案傳輸通訊協定（SFTP）和檔案傳輸通訊協定分開的憑證FTPS。我們建議您維護的個別憑證，FTP因為與SFTP和不同FTPS，會以純文字FTP傳輸憑證。透過從SFTP或隔離FTP憑證FTPS，如果共用或公開FTP憑證，您的工作負載會使用SFTP或FTPS保持安全。

此範例函數會傳回角色和邏輯主目錄詳細資訊，以及公有金鑰（如果執行公有金鑰身分驗證）。

當您建立服務受管使用者時，您可以設定其主目錄，可以是邏輯或實體。同樣地，我們需要 Lambda 函數結果來傳遞所需的使用者實體或邏輯目錄結構。您設定的參數取決於的值 [HomeDirectoryType](#) 欄位。

- HomeDirectoryType 設定為 PATH – HomeDirectory 欄位接著必須是使用者可見的絕對 Amazon S3 儲存貯體字首或 Amazon EFS 絕對路徑。
- HomeDirectoryType 設定為 LOGICAL – 請勿設定 HomeDirectory 欄位。相反地，我們設定一個 HomeDirectoryDetails 欄位，提供所需的 Entry/Target 映射，類似於中描述的值 [HomeDirectoryDetails](#) 服務受管使用者的參數。

範例函數列於 [中 Lambda 函數範例](#)。

搭配使用的 Lambda 函數 AWS Secrets Manager

若要使用 AWS Secrets Manager 作為身分提供者，您可以在範例 AWS CloudFormation 範本中使用 Lambda 函數。Lambda 函數會使用您的憑證查詢 Secrets Manager 服務，如果成功，會傳回指定的秘密。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 函數的範例 AWS CloudFormation 範本，請前往 [提供的 Amazon S3 儲存貯 AWS Transfer Family](#) 體。

AWS CloudFormation 範本的改進

API Gateway 介面的改進已針對發佈 CloudFormation 的範本進行。範本現在搭配 API Gateway 使用 BASE64 編碼的密碼。如果沒有此增強功能，您現有的部署會繼續運作，但不允許使用字元超出基本美國 ASCII 字元集的密碼。

啟用此功能的範本變更如下：

- GetUserConfigRequest AWS::ApiGateway::Method 資源必須具有此 RequestTemplates 程式碼（斜體行是更新的行）

```
RequestTemplates:
  application/json: |
    {
      "username": "$util.urlDecode($input.params('username'))",
      "password":
        "$util.escapeJavaScript($util.base64Decode($input.params('PasswordBase64'))).replaceAll('\n', '\\n')",
      "protocol": "$input.params('protocol')",
      "serverId": "$input.params('serverId')",
      "sourceIp": "$input.params('sourceIp')",
    }
```

- 資源 RequestParameters 的 GetUserConfig 必須變更 才能使用 PasswordBase64 標頭（斜體行是更新的行）：

```
RequestParameters:
  method.request.header.PasswordBase64: false
  method.request.querystring.protocol: false
  method.request.querystring.sourceIp: false
```

檢查堆疊的範本是否為最新的

1. 在 <https://console.aws.amazon.com/cloudformation> 開啟 AWS CloudFormation 主控台。
2. 從堆疊清單中，選擇您的堆疊。
3. 從詳細資訊面板中，選擇範本索引標籤。
4. 尋找下列項目：
 - 搜尋 RequestTemplates，並確保您有此行：

```
"password":  
  "$util.escapeJavaScript($util.base64Decode($input.params('PasswordBase64'))).replaceAll(  
    \",\"\", \"'\", \"'\")",
```

- 搜尋 RequestParameters，並確保您有此行：

```
method.request.header.PasswordBase64: false
```

如果您看不到更新後的行，請編輯您的堆疊。如需如何更新 AWS CloudFormation 堆疊的詳細資訊，請參閱 [修改堆疊範本](#) AWS CloudFormation；使用者指南。

使用邏輯目錄來簡化 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，該結構使用使用者易用的名稱，當使用者連線到您的 Amazon S3 儲存貯體或 Amazon EFS 檔案系統時，即可瀏覽這些名稱。使用邏輯目錄時，您可以避免向最終使用者揭露絕對目錄路徑、Amazon S3 儲存貯體名稱和 EFS 檔案系統名稱。

Note

雖然這取決於您使用的工作階段政策和其他內部要求，但您通常不需要工作階段政策和邏輯目錄，以確保使用者僅存取您打算存取的檔案。如果您正在設定邏輯目錄，則請勿建立工作階段政策，因為同時擁有兩者可能會導致許可遭拒的錯誤。

您可以使用邏輯目錄，透過執行所謂 chroot 的操作，將使用者的根目錄設定為儲存階層中所需的位置。在此模式中，使用者無法導覽至您為其設定的主目錄或根目錄以外的目錄。

例如，雖然 Amazon S3 使用者的範圍已縮減為僅存取 `/mybucket/home/` `${transfer:UserName}`，但有些用戶端允許使用者將資料夾向上移動至 `/mybucket/home`。在此情況下，使用者只有在登出並再次登入 Transfer Family 伺服器後，才會回到其預期的主目錄。執行 `chroot` 操作可以防止發生這種情況。

您可以在儲存貯體和字首之間建立自己的目錄結構。如果您有工作流程預期無法複製到儲存貯體字首的特定目錄結構，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，其中目錄路徑參考檔案系統中的不同位置。

邏輯目錄 FILE 映射

`HomeDirectoryMapEntry` 資料類型現在包含 `Type` 參數。在此參數存在之前，您可以建立邏輯目錄映射，其中目標為檔案。如果您先前已建立任何類型的邏輯目錄映射，則必須明確 `Type` 地將設定為 `FILE`，否則這些映射將無法正常運作。

其中一個方法是呼叫 `UpdateUser` API，並將 `Type` 設定為 `FILE` 以進行現有映射。

使用邏輯目錄的規則

在建置邏輯目錄映射之前，您應該了解下列規則：

- 當 `Entry` 為 `"/`，您只能有一個映射，因為不允許重疊路徑。
- 邏輯目錄支援高達 2.1 MB 的映射（對於服務受管使用者，此限制為 2,000 個項目）。也就是說，包含映射的資料結構大小上限為 2.1 MB。如果您有許多映射，您可以計算映射的大小，如下所示：
 - 以格式寫下典型的映射 `{"Entry": "/entry-path", "Target": "/target-path"}`，其中 `entry-path` 和 `target-path` 是您將使用的實際值。
 - 計算該字串中的字元，然後新增一個（1）。
 - 將該數字乘以您擁有的伺服器對應數量。

如果您在步驟 3 中估計的數字小於 2.1 MB，則您的映射在可接受的限制內。

- 如果儲存貯體或檔案系統路徑已根據使用者名稱進行參數化，則目標可以使用 `${transfer:UserName}` 變數。
- 目標可以是不同儲存貯體或檔案系統中的路徑，但您必須確保映射的 AWS Identity and Access Management (IAM) 角色（回應中的 `Role` 參數）能夠存取這些儲存貯體或檔案系統。
- 請勿指定 `HomeDirectory` 參數，因為當您使用 `HomeDirectoryType` 參數的值時，`EntryTarget` 這些組會隱含此 LOGICAL 值。

- 目標必須以正斜線（ / ）字元開頭，但在指定時請勿使用正斜線（ / ）Target。例如， `/DOC-EXAMPLE-BUCKET/images` 是可接受的，但 `DOC-EXAMPLE-BUCKET/images` 和 `/DOC-EXAMPLE-BUCKET/images/` 是不可接受的。
- Amazon S3 是物件存放區，這表示資料夾是虛擬概念，沒有實際的目錄階層。如果您的應用程式從用戶端發出 stat 操作，則當您使用 Amazon S3 進行儲存時，所有內容都會分類為檔案。此行為會在 [使用 Amazon Simple Storage Service 使用者指南 中的資料夾整理 Amazon S3 主控台](#) 中的物件中加以說明。如果您的應用程式需要 stat 準確顯示某物件是否為檔案或資料夾，您可以使用 Amazon Elastic File System（AmazonEFS）作為 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類型：
 - 對於服務受管使用者，請在 中提供邏輯目錄值 `HomeDirectoryMappings`。
 - 對於自訂身分提供者使用者，請在 中提供邏輯目錄值 `HomeDirectoryDetails`。

Important

除非您選擇最佳化 Amazon S3 目錄的效能（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。避免此問題是考慮最佳化 Amazon S3 效能的原因。

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：

開啟每個使用者的邏輯目錄。建立或更新使用者 LOGICAL 時，請將 `HomeDirectoryType` 參數設定為 `LOGICAL`，藉此執行此操作。

```
"HomeDirectoryType": "LOGICAL"
```

chroot

針對 chroot，建立包含每個使用者的單一 Entry 和 Target 配對的目錄結構。根資料夾是 Entry 點，而 Target 是儲存貯體或檔案系統中要映射的位置。

Example for Amazon S3

```
[{"Entry": "/", "Target": "/mybucket/jane"}]
```


Example for Amazon EFS

```
[{"Entry": "/", "Target": "/fs-faa1a123/jane"}]
```

您可以使用如上一個範例的絕對路徑，也可以使用動態取代搭配的使用者名稱`${transfer:UserName}`，如下列範例所示。

```
[{"Entry": "/", "Target":  
"/mybucket/${transfer:UserName}"}]
```

在上述範例中，使用者會鎖定到其根目錄，並且無法在階層中向上移動。

虛擬目錄結構

對於虛擬目錄結構，只要使用者IAM的角色映射具有存取目標的許可，您就可以使用 S3 儲存貯體或 EFS 檔案系統中任何位置的目標建立多個 EntryTarget 配對，包括跨多個儲存貯體或檔案系統。

在下列虛擬結構範例中，當使用者登入時 AWS SFTP，他們位於具有 `/pics`、`/doc/reporting` 和子目錄的根目錄中 `/anotherpath/subpath/financials`。

Note

除非您選擇最佳化 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需要建立不存在的目錄。避免此問題是考慮最佳化 Amazon S3 效能的原因。
對於 Amazon EFS，您仍然需要管理員來建立邏輯映射或目錄。

```
[  
{"Entry": "/pics", "Target": "/bucket1/pics"},  
{"Entry": "/doc", "Target": "/bucket1/anotherpath/docs"},  
{"Entry": "/reporting", "Target": "/reportingbucket/Q1"},  
{"Entry": "/anotherpath/subpath/financials", "Target": "/reportingbucket/financials"}]
```

Note

您只能將檔案上傳到您映射的特定資料夾。這表示在上一個範例中，您無法上傳到 `/anotherpath` 或 `anotherpath/subpath` 目錄；只有 `anotherpath/subpath/financials`。您也無法直接對應到這些路徑，因為不允許重疊的路徑。

例如，假設您建立下列映射：

```
{
  "Entry": "/pics",
  "Target": "/mybucket/pics"
},
{
  "Entry": "/doc",
  "Target": "/mybucket/mydocs"
},
{
  "Entry": "/temp",
  "Target": "/mybucket"
}
```

您只能將檔案上傳至這些儲存貯體。當您第一次透過連線時sftp，系統會將您捨入根目錄 /。如果您嘗試將檔案上傳到該目錄，上傳會失敗。下列命令顯示範例序列：

```
sftp> pwd
Remote working directory: /
sftp> put file
Uploading file to /file
remote open("/file"): No such file or directory
```

若要上傳至任何 directory/sub-directory，您必須明確地將路徑映射至 sub-directory。

如需chroot為使用者設定邏輯目錄和 的詳細資訊，包括您可以下載和使用的 AWS CloudFormation 範本，請參閱 AWS 儲存部落格中的[使用 chroot 和邏輯目錄簡化您的 AWS SFTP結構](#)。

設定邏輯目錄範例

在此範例中，我們會建立使用者並指派兩個邏輯目錄。下列命令會使用邏輯目錄 pics和 建立新的使用者（適用於現有的 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，您可以使用與上一個相似 LOGICAL 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** 和 **/DOC-EXAMPLE-BUCKET2/test/mydocs** 尚未存在，使用者（或管理員）需要建立目錄。
- 當 **marymajor** 連線至伺服器並執行 `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。不過，在 **pics** 和 **doc**，她可以新增子目錄。
- 她新增至 **pics** 和 **doc** 的檔案會 **/DOC-EXAMPLE-BUCKET2/test/mydocs** 分別新增至 Amazon S3 路徑 **/DOC-EXAMPLE-BUCKET1/pics** 和 **/DOC-EXAMPLE-BUCKET2/test/mydocs**。
- 在此範例中，我們會指定兩個不同的儲存貯體來說明該可能性。不過，您可以將相同的儲存貯體用於您為使用者指定的多個或所有邏輯目錄。

設定 Amazon 的邏輯目錄 EFS

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來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，因為他們在邏輯主目錄 `mkdir` 上缺少許可。

如果使用者的主目錄不存在，而且他們執行 `ls` 命令，系統會回應如下：

```
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。

自訂 AWS Lambda 回應

您可以使用邏輯目錄搭配連線至自訂身分提供者的 Lambda 函數。若要這麼做，請在 Lambda 函數中指定 `HomeDirectoryType` 為 **LOGICAL**，並新增 `HomeDirectoryDetails` 參數的 `Entry` 和 `Target` 值。例如：

```
HomeDirectoryType: "LOGICAL"
HomeDirectoryDetails: "[{"Entry": "\\", \"Target\": \"//DOC-EXAMPLE-BUCKET/
theRealFolder"}]"
```

下列程式碼是自訂 Lambda 身分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

只有在您使用 API Gateway 方法作為自訂身分提供者時，才會傳回此 `Url`：行。

AWS Transfer Family SFTP 連接器

AWS Transfer Family SFTP 連接器會使用 SFTP通訊協定，在 Amazon 儲存體與外部合作夥伴之間建立傳送檔案和訊息的關係。您可以將檔案從 Amazon S3 傳送至外部的合作夥伴擁有目的地。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連接器只能用來連線至提供網際網路可存取端點的遠端SFTP伺服器。

檢視[AWS Transfer Family SFTP連接器](#)，以簡要介紹 Transfer Family 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](#)
- [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、與其相關聯的安全演算法、如何儲存秘密以保存憑證、有關格式化私有金鑰的詳細資訊，以及測試連接器的指示。

主題

- [建立SFTP連接器](#)
- [SFTP 連接器演算法](#)
- [儲存要與SFTP連接器搭配使用的秘密](#)
- [產生並格式化SFTP連接器私有金鑰](#)
- [測試SFTP連接器](#)

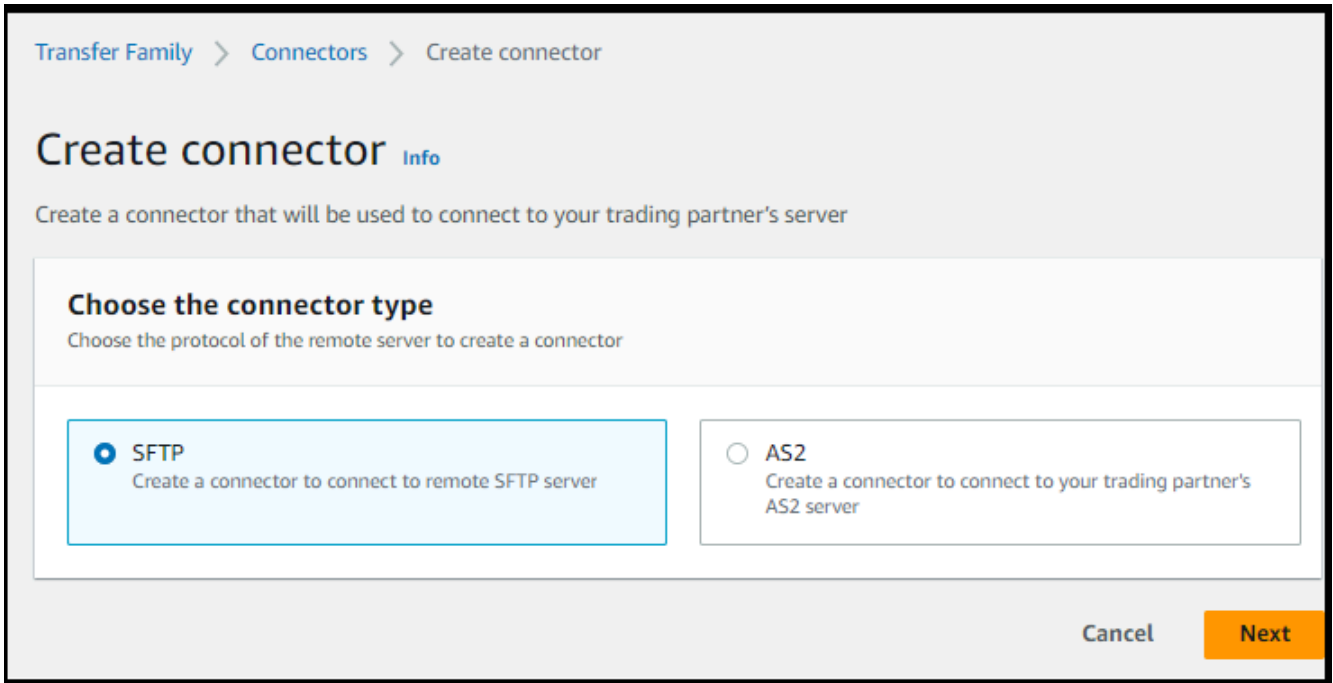
建立SFTP連接器

此程序說明如何使用 AWS Transfer Family 主控台或 建立SFTP連接器 AWS CLI。

Console

若要建立SFTP連接器

1. 在 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. 選擇SFTP連接器類型以建立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：
- 針對 URL，輸入URL遠端SFTP伺服器的。這URL必須格式化為 `sftp://partner-SFTP-server-url`，例如 `sftp://AnyCompany.com`。

Note

或者，您可以在 中提供連接埠號碼URL。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。

- 針對存取角色，選擇要使用的（ARN）角色的 Amazon Resource Name AWS Identity and Access Management（IAM）。
- 請確定此角色提供對請求中使用的檔案位置之父目錄的讀取和寫入存取權。
`StartFileTransfer`

- 請確定此角色提供 存取秘密的許可。 `secretsmanager:GetSecretValue`

 Note

在 政策中，您必須ARN為秘密指定。ARN 包含秘密名稱，但以六個隨機英數字元附加名稱。機密ARN的 具有下列格式。

```
arn:aws:secretsmanager:region:account-id:secret:aws/
transfer/SecretName-6RandomCharacters
```

- 請確定此角色包含信任關係，允許連接器在為使用者的傳輸請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](#)。

下列範例授予必要許可，以存取 *DOC-EXAMPLE-BUCKET* 在 Amazon S3 中，以及存放在 Secrets Manager 中的指定秘密。

```
{
  "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，範例會授予單一秘密的存取權。不過，您可以使用萬用字元，如果想要將相同IAM角色重複使用給多個使用者和秘密，則可以儲存工作。例如，下列資源陳述式會針對名稱開頭為 的所有秘密授予許可aws/transfer。

```
"Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/transfer/*"
```

您也可以將包含SFTP憑證的秘密存放在另一個 中 AWS 帳戶。如需啟用跨帳戶秘密存取的詳細資訊，請參閱[不同帳戶中使用者的 AWS Secrets Manager 秘密許可](#)。

- （選用）針對記錄角色，選擇連接器用來將事件推送至 CloudWatch 日誌IAM的角色。下列範例政策會列出記錄SFTP連接器事件的必要許可。

```

{
  "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/*"
    ]
  }]
}

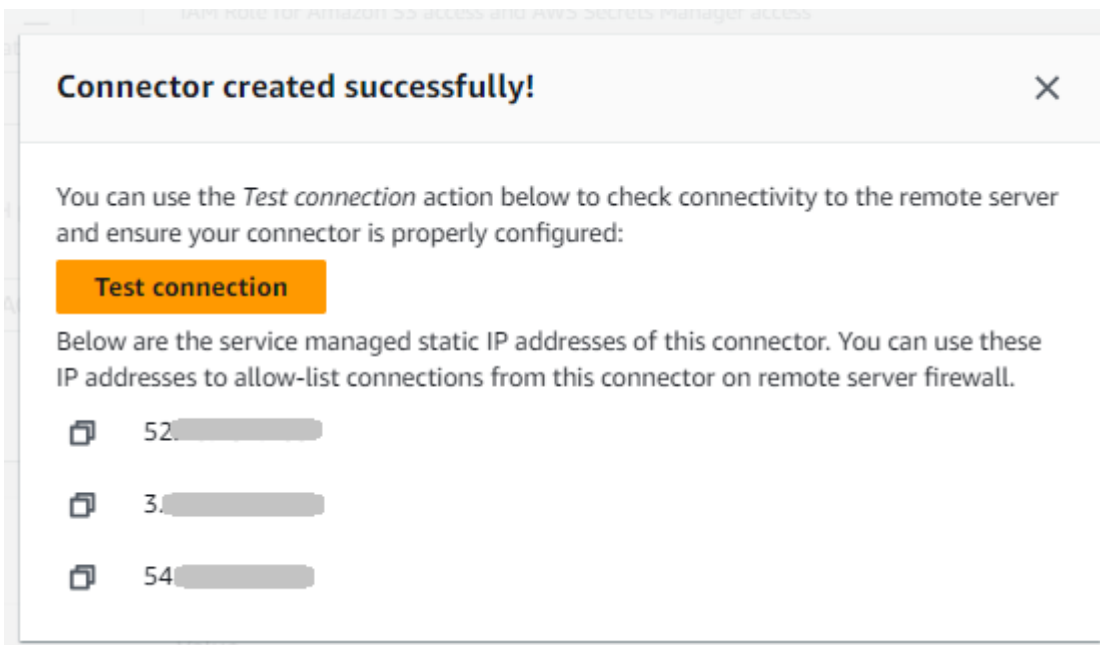
```

5. 在SFTP組態區段中，提供下列資訊：

- 對於 Connector 憑證，從下拉式清單中選擇 中 AWS Secrets Manager 包含SFTP使用者私有金鑰或密碼的秘密名稱。您必須建立秘密，並以特定方式存放。如需詳細資訊，請參閱 [儲存要與SFTP連接器搭配使用的秘密](#)。
- 信任的主機金鑰 – 貼到用來識別外部伺服器的主機金鑰公有部分。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。您可以針對SFTP伺服器使用 ssh-keyscan 命令來擷取必要的金鑰。如需有關 Transfer Family 支援的受信任主機金鑰格式和類型的詳細資訊，請參閱 [SFTPConnectorConfig](#)。

6. （選用）在標籤區段中，針對金鑰和值，輸入一或多個標籤作為鍵值對。

7. 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 地址清單和測試連線按鈕。使用 按鈕來測試新連接器的組態。



隨即出現 連接器頁面，並將新SFTP連接器的 ID 新增至清單。若要檢視連接器的詳細資訊，請參閱 [檢視SFTP連接器詳細資訊](#)。

CLI

您可以使用 [create-connector](#) 命令來建立連接器。若要使用此命令建立SFTP連接器，您必須提供下列資訊。

- URL 適用於遠端SFTP伺服器的。這URL必須格式化為 `sftp://partner-SFTP-server-url`，例如 `sftp://AnyCompany.com`。
- 存取角色。選擇要使用的（ARN）角色的 Amazon Resource Name AWS Identity and Access Management（IAM）。
 - 請確定此角色提供對請求中所用檔案位置之父目錄的讀取和寫入存取權。
`StartFileTransfer`
 - 請確定此角色提供 存取秘密的許可。 `secretsmanager:GetSecretValue`

Note

在 政策中，您必須ARN為秘密指定。ARN 包含秘密名稱，但以六個隨機英數字元附加名稱。機密ARN的 具有下列格式。

```
arn:aws:secretsmanager:region:account-id:secret:aws/transfer/SecretName-6RandomCharacters
```

- 請確定此角色包含信任關係，允許連接器在為使用者的傳輸請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](#)。

下列範例授予必要許可，以存取 `DOC-EXAMPLE-BUCKET` 在 Amazon S3 中，以及存放在 Secrets Manager 中的指定秘密。

```
{
  "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，範例會授予單一秘密的存取權。不過，您可以使用萬用字元，如果想要將相同IAM角色重複使用給多個使用者和秘密，則可以儲存工作。例如，下列資源陳述式會針對名稱開頭為的所有秘密授予許可aws/transfer。

```
"Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/transfer/*"
```

您也可以將包含SFTP憑證的秘密存放在另一個 AWS 帳戶。如需啟用跨帳戶秘密存取的詳細資訊，請參閱[不同帳戶中使用者的 AWS Secrets Manager 秘密許可](#)。

- (選用) 選擇要用來將事件推送至 CloudWatch 日誌的連接器IAM角色。下列範例政策會列出記錄SFTP連接器事件的必要許可。

```
{
  "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。
 - 在 中 AWS Secrets Manager 包含SFTP使用者私有金鑰或密碼的秘密 ARN 。
 - 主機金鑰的公有部分，用於識別外部伺服器。您可以視需要提供多個信任的主機金鑰。

提供資訊最簡單的方法是將SFTP資訊儲存到檔案中。例如，將下列範例文字複製到名為 的檔案testSFTPConfig.json。

```
// Listing for testSFTPConfig.json
{
  "UserSecretId": "arn:aws::secretsmanager:us-east-2:123456789012:secret:aws/transfer/example-username-key",
  "TrustedHostKeys": [
    "ssh-rsa AAAAabbbb...EEEE="
  ]
}
```

Note

SecretId 可以是整個 ARN 或秘密的名稱 (*example-username-key* 在上一個清單中)。

然後執行下列命令來建立連接器。

```
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
```

SFTP 連接器演算法

當您建立 SFTP 連接器時，下列安全演算法會連接至連接器。

Type	演算法
SSH 密碼	aes256-gcm@openssh.com
	aes128-gcm@openssh.com
	aes256-ctr
	aes192-ctr
SSH 金鑰交換方法 (KEX)	curve25519-sha256
	curve25519-sha256@libssh.org
	diffie-hellman-group16-sha512
	diffie-hellman-group18-sha512
	diffie-hellman-group-exchange-sha256
SSH MAC	hmac-sha2-512-etm@openssh.com

Type	演算法
	hmac-sha2-256-etm@openssh.com
	hmac-sha2-512
	hmac-sha2-256
SSH 主機金鑰	ecdsa-sha2-nistp256
	ecdsa-sha2-nistp384
	ecdsa-sha2-nistp521
	rsa-sha2-512
	rsa-sha2-256

儲存要與SFTP連接器搭配使用的秘密

您可以使用 Secrets Manager 來儲存SFTP連接器的使用者憑證。建立秘密時，您必須提供使用者名稱。此外，您可以提供密碼、私有金鑰或兩者。如需詳細資訊，請參閱 [SFTP 連接器配額](#)。

Note

當您將秘密存放在 Secrets Manager 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 Secrets Manager 中存放SFTP連接器的使用者憑證

1. 登入 AWS Management Console 並在 開啟 AWS Secrets Manager 主控台<https://console.aws.amazon.com/secretsmanager/>。
2. 在左側導覽窗格中，選擇秘密。
3. 在秘密頁面上，選擇儲存新的秘密。
4. 在選擇秘密類型頁面上，針對秘密類型，選擇其他類型的秘密。
5. 在金鑰/值對區段中，選擇金鑰/值索引標籤。
 - 金鑰 – 輸入 **Username**。

- 值 – 輸入授權連線至合作夥伴伺服器之使用者名稱。
6. 如果您想要提供密碼，請選擇新增列，然後在鍵/值對區段中選擇鍵/值索引標籤。

選擇新增列，然後在鍵/值對區段中，選擇鍵/值索引標籤。
 - 金鑰 – 輸入 **Password**。
 - 值 – 輸入使用者的密碼。
 7. 如果您想要提供私有金鑰，請參閱 [產生並格式化SFTP連接器私有金鑰](#)，其中說明如何輸入私有金鑰資料。

 Note

您輸入的私有金鑰資料必須與遠端SFTP伺服器中為此使用者儲存的公有金鑰相對應。

8. 選擇 Next (下一步)。
9. 在設定秘密頁面上，輸入秘密的名稱和描述。我們建議您使用的字首 **aws/transfer/** 做為名稱。例如，您可以命名秘密 **aws/transfer/connector-1**。
10. 選擇下一個，然後在設定輪換頁面上接受預設值。然後選擇下一步。
11. 在檢閱頁面上，選擇儲存以建立和儲存秘密。

產生並格式化SFTP連接器私有金鑰

有關產生公有/私有金鑰對的完整詳細資訊，請參閱 [在 macOS、Linux 或 Unix 上建立SSH金鑰](#)

例如，若要產生用於SFTP連接器的私有金鑰，下列範例命令會產生正確的金鑰類型（取代 *key_name* 使用金鑰對的實際檔案名稱）：

```
ssh-keygen -t rsa -b 4096 -m PEM -f key_name -N ""
```

 Note

當您建立要與SFTP連接器搭配使用的金鑰對時，請勿使用密碼片語。SFTP 組態必須具有空密碼才能正常運作。

此命令會建立RSA金鑰對，金鑰大小為 4096 位元。金鑰會以舊版PEM格式產生，這是 Transfer Family 與SFTP連接器秘密搭配使用的必要項目。金鑰會儲存在目前目錄中的 *key_name* (私有金鑰) 和 *key_name*.pub (公有金鑰) 中：即您執行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，藉此使用 ssh-keygen工具來轉換金鑰。

產生金鑰後，您必須確定私有金鑰已格式化為內嵌的新行字元 ("\n") JSON 格式。

使用 命令將現有的私有金鑰轉換為正確的格式 —JSON 格式，其中包含內嵌的新行字元。此處提供 jq和 Powershell 的範例。您可以使用任何工具或命令，將私有金鑰轉換為內嵌新行字元的JSON格式。

jq command

此範例使用 jq命令，可從 [Download jq](#) 下載。

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

例如，如果您的私有金鑰檔案位於 中 ~/.ssh/my_private_key，則命令如下所示。

```
jq -sR . ~/.ssh/my_private_key
```

這會以正確的格式 (包含內嵌的新行字元) 將金鑰輸出至標準輸出。

PowerShell

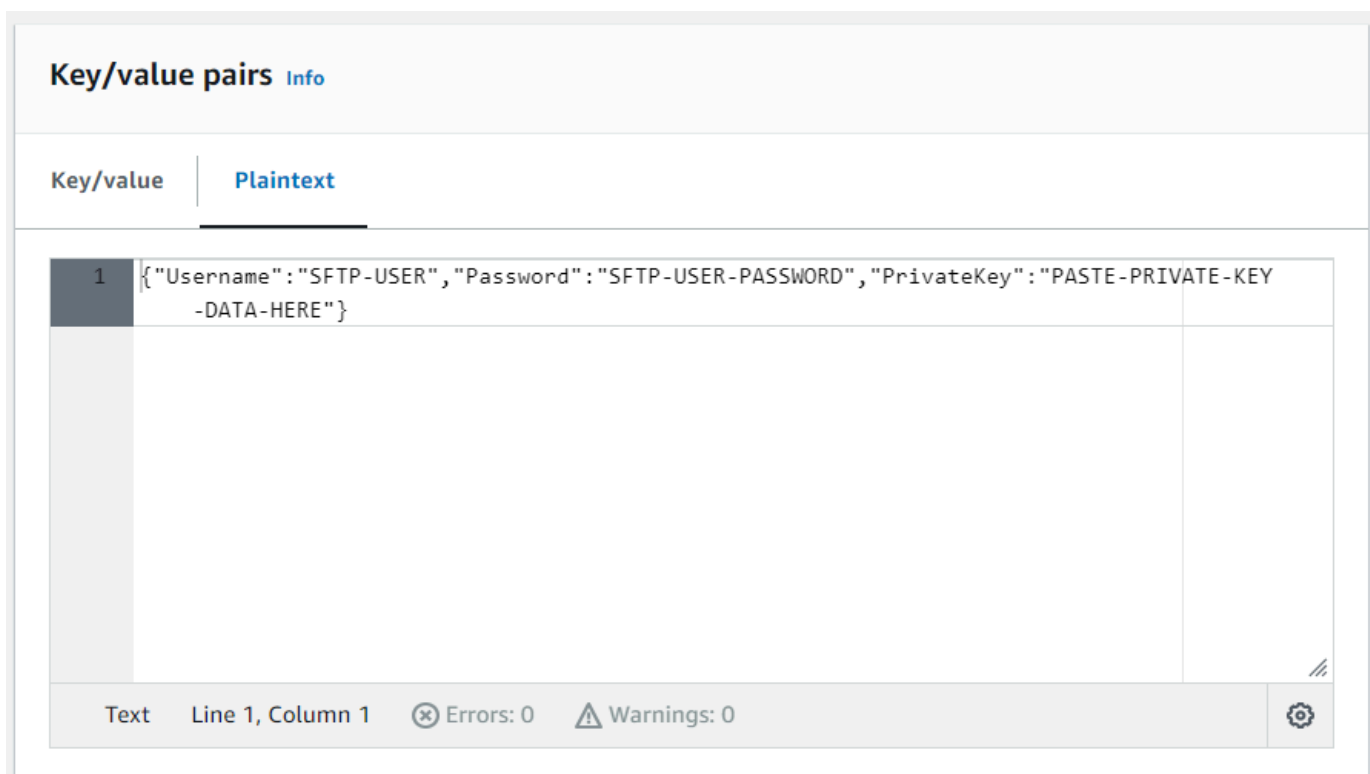
如果您使用的是 Windows，您可以使用 將金鑰 PowerShell 轉換為正確的格式。下列 Powershell 命令會將私有金鑰轉換為正確的格式。

```
Get-Content -Raw path-to-private-key-file | ConvertTo-Json
```


將私有金鑰資料新增至秘密，以搭配SFTP連接器使用

1. 在 Secrets Manager 主控台中，儲存其他類型的 Secret 時，選擇純文字索引標籤。文字應該是空的，只有開啟和關閉支架 {}。
2. 使用下列格式貼入您的使用者名稱、私有金鑰資料和/或密碼。針對私有金鑰資料，請從您在步驟 1 中執行的命令貼上輸出。

```
{"Username": "SFTP-USER", "Password": "SFTP-USER-PASSWORD", "PrivateKey": "PASTE-PRIVATE-KEY-DATA-HERE"}
```



如果您正確貼上私有金鑰資料，您應該會在選取金鑰/值索引標籤時看到以下內容。請注意，私有金鑰資料會顯示 line-by-line，而不是連續字串。

Secret value Info	
Retrieve and view the secret value.	
Key/value	Plaintext
Secret key	Secret value
Username	 SFTP-USER
Password	 SFTP-USER-PASSWORD
PrivateKey	 -----BEGIN RSA PRIVATE KEY----- MIIEpAIBAAKCAQEA... g... a... U... G... g... T... a... I... W... I... A... e... 5... 7... H... i... By...

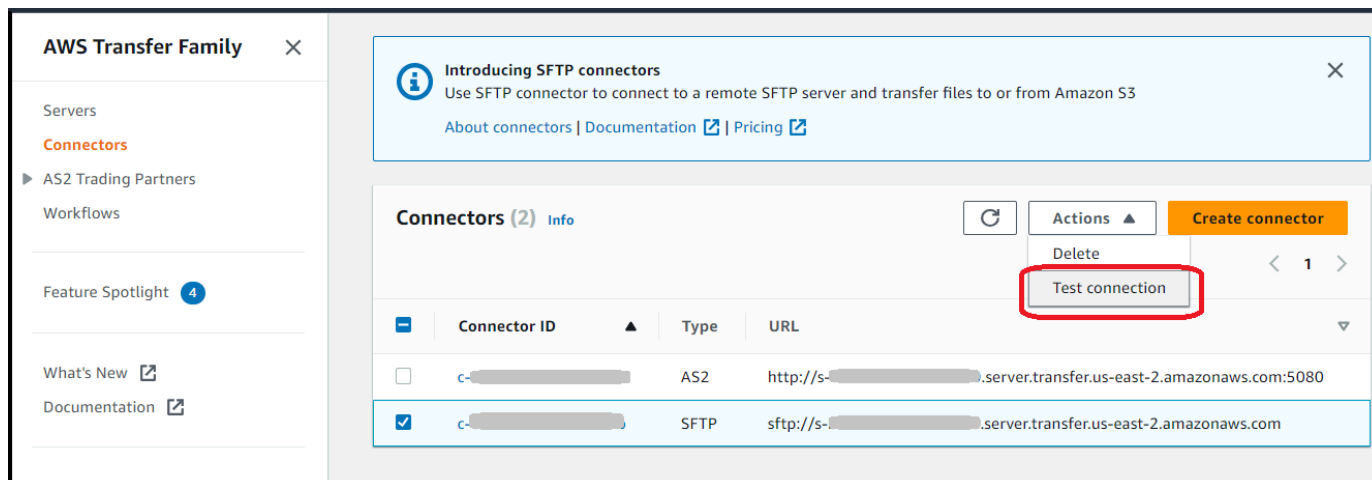
3. 繼續儲存要與SFTP連接器搭配使用的秘密步驟 8 中的程序，並遵循該程序直至結束。

測試SFTP連接器

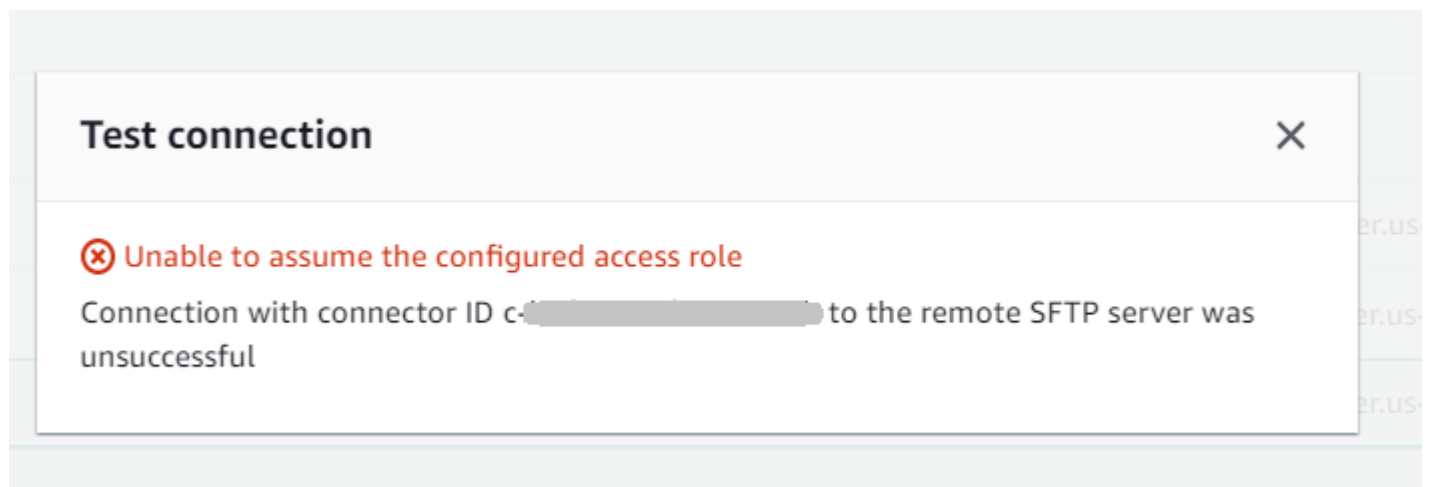
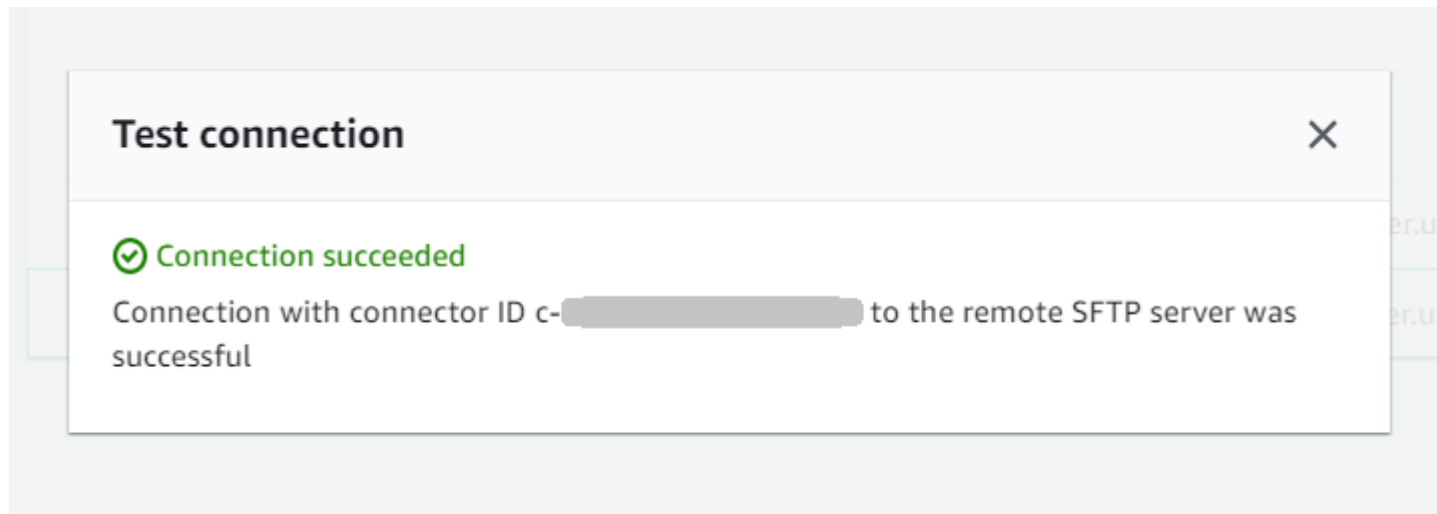
建立SFTP連接器後，建議您先測試連接器，然後再嘗試使用新連接器傳輸任何檔案。

測試SFTP連接器

1. 在開啟 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，然後選擇連接器。
3. 從動作功能表中，選擇測試連線。



系統會傳回訊息，指出測試是否通過或失敗。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 [TestConnection](#) API 文件。

使用SFTP連接器傳送和擷取檔案

SFTP 連接器可擴展 的功能 AWS Transfer Family，以與雲端和內部部署中的遠端伺服器通訊。您可以將遠端來源中產生和存放的資料與 AWS 託管資料倉儲整合，以進行分析、業務應用程式、報告和稽核。若要啟動檔案傳輸至遠端SFTP伺服器，您可以使用 [StartFileTransfer](#) API 操作，它使用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。

您可以檢查伺服器日誌來監控檔案傳輸。連接器活動會記錄到格式為 的日誌串流aws/transfer/*connector-id*，例如 aws/transfer/c-1234567890abcdef0。如果您未看到連接器的任何日誌，請確定您已指定具有連接器正確許可的記錄角色。

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) 命令。您可以指定下列參數，取決於您要傳送檔案（傳出傳輸）或接收檔案（傳入傳輸）。

- 傳出傳輸
 - send-file-paths 包含從 1 到 10 個來源檔案路徑，用於將檔案傳輸至合作夥伴的SFTP伺服器。
 - remote-directory-path 是將檔案傳送至客戶SFTP伺服器上的遠端路徑。
- 傳入傳輸
 - retrieve-file-paths 包含 1 到 10 個遠端路徑。每個路徑都會指定將檔案從合作夥伴的SFTP伺服器傳輸至 Transfer Family 伺服器的位置。
 - local-directory-path 是儲存檔案的 Amazon S3 位置（儲存貯體和選用字首）。

若要傳送檔案，您可以指定 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 */DOC-EXAMPLE-SOURCE-BUCKET/file2.txt* 位於 Amazon S3 儲存體中的名為 */DOC-EXAMPLE-SOURCE-BUCKET/file1.txt* 和 的檔案傳送至合作夥伴SFTP伺服器上的/tmp目錄。若要使用此範例命令，請將 取代 *DOC-EXAMPLE-SOURCE-BUCKET* 為您自己的儲存貯體。

```
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，您可以指定 `retrieve-file-paths` 和 `local-directory-path` 參數。下列範例會擷取合作夥伴SFTP伺服器上的檔案 `/my/remote/file1.txt` 和 `/my/remote/file2.txt`，並將其放置在 Amazon S3 位置 `/DOC-EXAMPLE-BUCKET/prefix`。若要使用此範例命令，請將取代 *user input placeholders* 為您自己的資訊。

```
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
```

上述範例會在SFTP伺服器上指定絕對路徑。您也可以使用相對路徑：即相對於SFTP使用者主目錄的路徑。例如，如果SFTP使用者是 `marymajor`，且其SFTP伺服器上的主目錄是 `/users/marymajor/`，則下列命令會 `/DOC-EXAMPLE-SOURCE-BUCKET/file1.txt` 傳送至 `/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
```

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。

主題

- [更新SFTP連接器](#)
- [檢視SFTP連接器詳細資訊](#)
- [SFTP 連接器配額](#)

更新SFTP連接器

若要變更連接器的現有參數值，您可以執行 `update-connector` 命令。下列命令會將 `connector-id` 區域中連接器 的秘密更新 `region-id` 為 `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連接器詳細資訊

您可以在 AWS Transfer Family 主控台中找到SFTP連接器的詳細資訊和屬性清單。

檢視連接器詳細資訊

1. 在 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 ID 欄中選擇識別符，以查看所選連接器的詳細資訊頁面。

您可以在SFTP連接器詳細資訊頁面上選擇編輯，變更連接器的屬性。

[Transfer Family](#) > [Connectors](#) > c-
C-
[Delete](#)

Connector configuration [Info](#) [Edit](#)

URL sftp://	Access role transfer-s3	Logging role role

SFTP configuration [Edit](#)

Connector credentials arn:aws:secretsmanager:us-	Trusted host keys 1. SHA256

Egress IP details [Info](#)

Service managed static IP addresses of this connector

	52.1
	3.
	54.

Tags (0) [Manage tags](#)

Q

< 1 >

Key	Value

Note

您可以執行下列 AWS Command Line Interface (AWS CLI) 命令，以取得大部分這些資訊，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 [DescribeConnector](#) 在API參考中。

SFTP 連接器配額

連接器有下列配額SFTP。AS2 連接器的配額如 所述[AS2 配額和限制](#)。若要請求增加可調整的配額，請參閱 中的[AWS 服務 配額](#)AWS 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
最大值 StartFile Transfer TPS	每個帳戶每秒 3 個請求	是
待定檔案傳輸的佇列大小上限	1000	否
檔案大小上限	50 GB (GiB	否
每個檔案的傳輸時間上限	6 小時	否
每個檔案的請求等待時間上限	6 小時	否
最短AccessRole 或LoggingRole 工作階段 持續時間	60 分鐘	否
並行檔案傳輸上限	每個連接器 1 個並行檔案傳輸	否
每個帳戶的每秒檔案傳輸請求 數目上限	3	是
每個帳戶的連接器數量上限 (SFTP和 AS2 連接器都有助 於此計數)	100	是
每個帳戶連接器的最大頻寬 (SFTP和 AS2 連接器都有助 於此值)	50 MBps	否

為了儲存SFTP連接器的憑證，每個 Secrets Manager 秘密都有關聯的配額。如果您使用相同的秘密來存放多種類型的金鑰，出於多種目的，您可能會遇到這些配額。

- 單一秘密的總長度：12,000 個字元
- **Password** 字串的長度上限：1024 個字元
- **PrivateKey** 字串的長度上限：8192 個字元
- **Username** 字串的長度上限：100 個字元

AWS Transfer Family 適用於 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 通訊協定對於具有合規要求的工作流程至關重要，這些要求依賴於在通訊協定中內建的資料保護和安全性功能。

Note

AS2 適用於 Transfer Family 的是 [Drummond 認證的](#)。

零售、生命科學、製造、金融服務和公用程式等產業的客戶 AS2，若依賴供應鏈、物流和付款工作流程，可以使用 AWS Transfer Family AS2 端點與其業務合作夥伴安全地交易。交易的資料可在 中原生存取，AWS 以進行處理、分析和機器學習。此資料也可用於與在 上執行的企業資源規劃 (ERP) 和客戶關係管理 (CRM) 系統整合 AWS。透過 AS2，客戶可以在 中大規模執行其 business-to-business (B2B) 交易，AWS 同時維護現有的業務合作夥伴整合和合規。

如果您是 Transfer Family 客戶，希望與具有 AS2 啟用之設定的伺服器之合作夥伴交換檔案，則設定涉及產生一個公有私有金鑰對進行加密，以及另一個用來簽署公有金鑰並與合作夥伴交換公有金鑰。

保護傳輸中的 AS2 承載通常涉及使用密碼編譯訊息語法 (CMS)，且通常使用加密和數位簽章來提供資料保護和對等身分驗證。已簽署的訊息處置通知 (MDN) 回應承載提供驗證 (不可否認)，確認訊息已收到並成功解密。

這些 CMS 承載和 MDN 回應的傳輸會透過 進行 HTTP。

Note

HTTPS AS2 目前不支援伺服器端點。TLS 終止目前是客戶的責任。

如需設定適用性聲明 2 (AS2) 組態的詳細 step-by-step 逐步解說，請參閱教學課程 [設定 AS2 組態](#)。

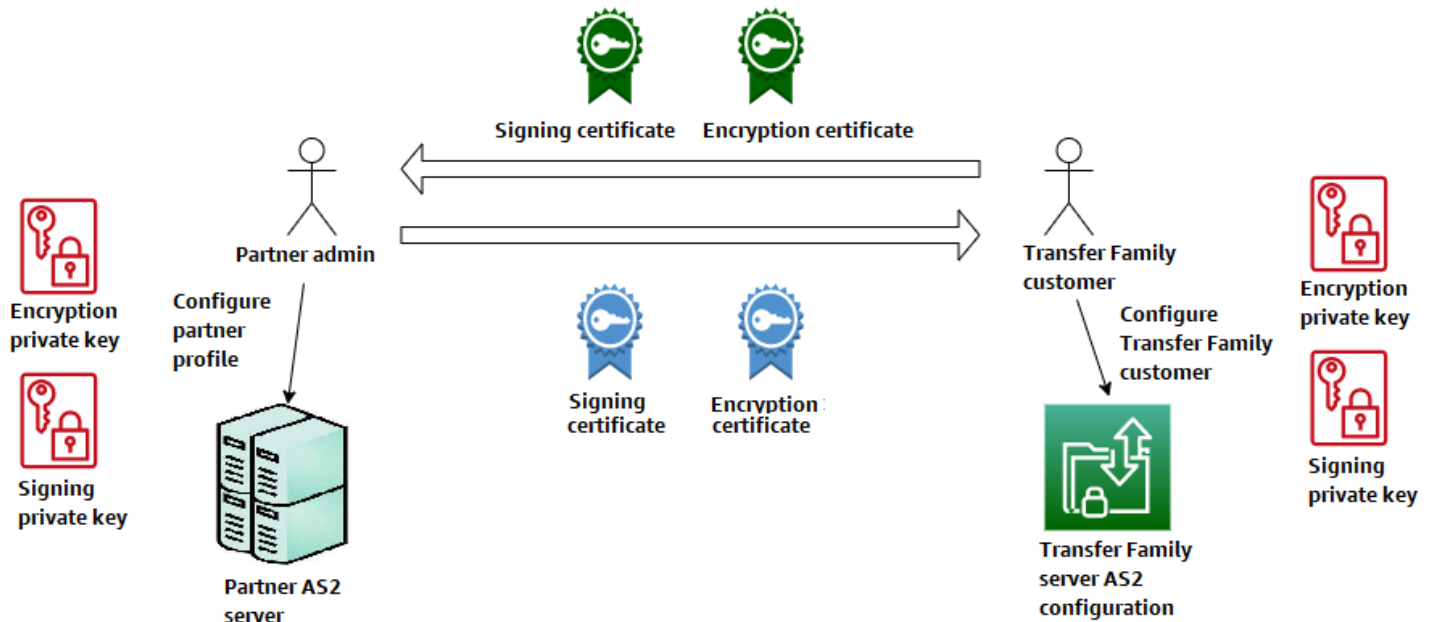
主題

- [AS2 使用案例](#)
- [設定 AS2](#)
- [設定 AS2 連接器](#)
- [管理 AS2 合作夥伴](#)

- [傳送和接收AS2訊息](#)
- [監控 AS2 使用情況](#)

AS2 使用案例

如果您是想要與已設定AS2伺服器之合作夥伴交換檔案 AWS Transfer Family 的客戶，則設定中最複雜的部分包括產生一個公有/私有金鑰對進行加密，以及另一個用來與合作夥伴簽署和交換公有金鑰。



考慮 AWS Transfer Family 搭配 使用 的下列變化AS2。

Note

交易合作夥伴是與該合作夥伴設定檔相關聯的合作夥伴。
下表MDN中的所有 提及皆假設已簽署 MDNs。

AS2 使用案例

僅限傳入使用案例

- 將加密AS2的訊息從交易合作夥伴傳輸到 Transfer Family 伺服器。

在此情況下，請執行下列操作：

1. 為您的交易合作夥伴和您自己建立設定檔。

2. 建立使用 AS2 通訊協定的 Transfer Family 伺服器。
3. 建立協議並將其新增至您的伺服器。
4. 使用私有金鑰匯入憑證並將其新增至您的設定檔，然後將公有金鑰匯入合作夥伴設定檔以進行加密。
5. 取得這些項目後，請將憑證的公有金鑰傳送給您的交易合作夥伴。

現在，您的合作夥伴可以傳送加密的訊息給您，您可以解密這些訊息，並將其存放在 Amazon S3 儲存貯體中。

- 將加密AS2的訊息從交易合作夥伴傳輸到 Transfer Family 伺服器，並新增簽署。

在此案例中，您仍然只執行傳入傳輸，但現在您希望合作夥伴簽署他們傳送的訊息。在此情況下，匯入交易合作夥伴的簽署公有金鑰（作為新增至合作夥伴設定檔的簽署憑證）。

- 將加密AS2的訊息從交易合作夥伴傳輸到 Transfer Family 伺服器，並新增簽署和傳送MDN回應。

在這種情況下，您仍然只進行傳入傳輸，但現在除了收到已簽署的承載之外，您的交易合作夥伴還希望收到已簽署的MDN回應。

1. 匯入您的公有和私有簽署金鑰（作為簽署憑證至您的設定檔）。
2. 將公有簽署金鑰傳送給您的交易合作夥伴。

僅限傳出使用案例

- 將加密AS2的訊息從 Transfer Family 伺服器傳輸到交易合作夥伴。

此案例類似於僅限傳入的傳輸使用案例，但您可以建立連接器，而不是將協議新增至AS2伺服器。在這種情況下，您可以將交易合作夥伴的公有金鑰匯入其設定檔。

- 將加密AS2的訊息從 Transfer Family 伺服器傳輸到交易合作夥伴，並新增簽署。

您仍然只進行傳出轉帳，但現在您的交易合作夥伴希望您簽署傳送給他們的訊息。

1. 匯入您的簽署私有金鑰（作為新增至設定檔的簽署憑證）。

2. 將公有金鑰傳送給您的貿易合作夥伴。

- 將加密AS2的訊息從 Transfer Family 伺服器傳輸到交易合作夥伴，並新增簽署和傳送MDN回應。

您仍然只進行傳出傳輸，但現在除了傳送已簽署的承載之外，還希望收到來自交易合作夥伴的已簽署MDN回應。

1. 您的貿易合作夥伴會傳送其公有簽署金鑰給您。

2. 匯入交易合作夥伴的公有金鑰（作為新增至合作夥伴設定檔的簽署憑證）。

傳入和傳出使用案例

- 在 Transfer Family 伺服器與交易合作夥伴之間，雙向傳輸加密AS2的訊息。

在此情況下，請執行下列操作：

- 為您的交易合作夥伴和您自己建立設定檔。
- 建立使用 AS2 通訊協定的 Transfer Family 伺服器。
- 建立協議並將其新增至您的伺服器。
- 建立連接器。
- 使用私有金鑰匯入憑證並將其新增至您的設定檔，然後將公有金鑰匯入合作夥伴設定檔以進行加密。
- 從您的交易合作夥伴接收公有金鑰，並將其新增至其設定檔以進行加密。
- 取得這些項目後，請將憑證的公有金鑰傳送給您的交易合作夥伴。

現在，您和您的交易合作夥伴可以交換加密的訊息，而且兩者都可以解密。您可以將收到的訊息儲存在 Amazon S3 儲存貯體中，而且合作夥伴可以解密和儲存您傳送給他們的訊息。

- 在 Transfer Family 伺服器與交易合作夥伴之間以雙向傳輸加密AS2的訊息，並新增簽署。

現在您和您的合作夥伴想要已簽署的訊息。

- 匯入您的簽署私有金鑰（作為新增至設定檔的簽署憑證）。
 - 將公有金鑰傳送給您的貿易合作夥伴。
 - 匯入交易合作夥伴簽署的公有金鑰，並將其新增至其設定檔。
- 在 Transfer Family 伺服器與交易合作夥伴之間雙向傳輸加密AS2的訊息，並新增簽署和傳送MDN回應。

現在，您想要交換已簽署的承載，而且您和您的交易合作夥伴都想要MDN回應。

- 您的貿易合作夥伴會傳送其公有簽署金鑰給您。
- 匯入交易合作夥伴的公有金鑰（作為您合作夥伴設定檔的簽署憑證）。
- 將公有金鑰傳送給您的交易合作夥伴。

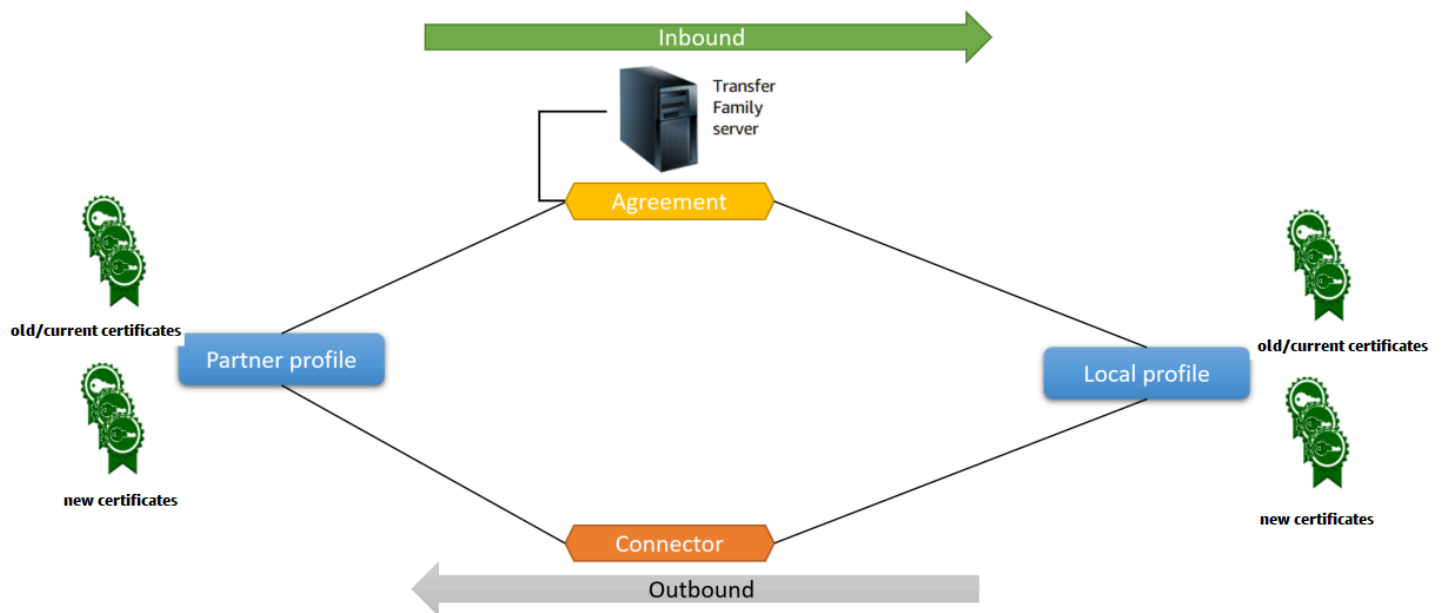
設定 AS2

若要建立已啟用 AS2的伺服器，您還必須指定下列元件：

- 協議 – 雙邊交易合作夥伴協議，或合作夥伴關係，定義交換訊息（檔案）的雙方之間的關係。若要定義協議，Transfer Family 結合了伺服器、本機設定檔、合作夥伴設定檔和憑證資訊。Transfer Family AS2- 傳入程序使用 協議。
- 憑證 – 公有金鑰（X.509）憑證用於訊息加密和驗證的AS2通訊。憑證也用於連接器端點。
- 本機設定檔和合作夥伴設定檔 – 本機設定檔定義本機 AS2（已啟用 Transfer Family 伺服器）組織或「派對」。同樣地，合作夥伴設定檔會定義 Transfer Family 外部的遠端合作夥伴組織。

雖然並非所有AS2啟用的伺服器都需要，但對於傳出傳輸，您需要連接器。連接器會擷取傳出連線的參數。將檔案傳送至客戶的外部非 AWS 伺服器時，需要連接器。

下圖顯示傳入和傳出程序中涉及的AS2物件之間的關係。



如需AS2組態範例 end-to-end，請參閱 [設定AS2組態](#)。

主題

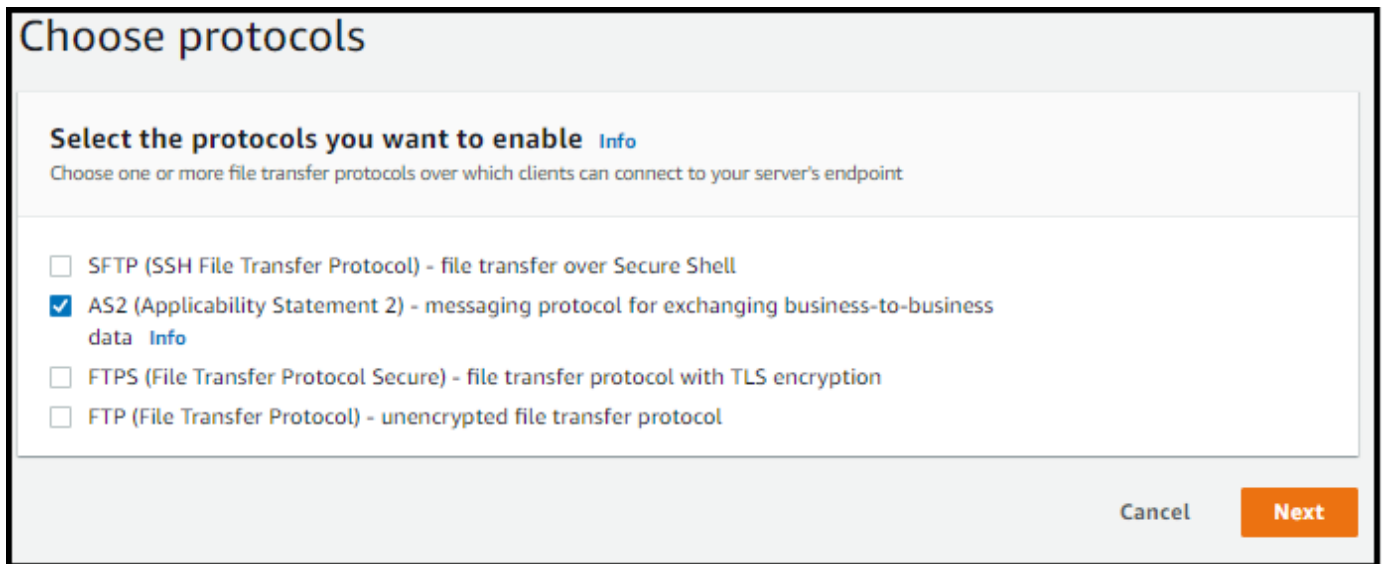
- [使用 Transfer Family 主控台建立AS2伺服器](#)
- [使用 範本建立示範 Transfer Family AS2堆疊](#)
- [AS2 組態和限制](#)
- [AS2 特徵和功能](#)

使用 Transfer Family 主控台建立AS2伺服器

此程序說明如何使用 Transfer Family 主控台建立已啟用 AS2的伺服器。如果您想要 AWS CLI 改為使用，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AS2已啟用的伺服器

1. 在開啟 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. 在選擇身分提供者頁面上，選擇下一個。

Note

對於 AS2，您無法選擇身分提供者，因為AS2通訊協定不支援基本身分驗證。相反地，您可以透過虛擬私有雲端（VPC）安全群組控制存取權。

5. 在選擇端點頁面上，執行下列動作：

Choose an endpoint

Endpoint configuration [Info](#)

Endpoint type
Select whether the endpoint will be publicly accessible or hosted inside your VPC

☐ Publicly accessible
Accessible over the internet

☒ VPC hosted [Info](#)
Access controlled using Security Groups

Access [Info](#)

☒ Internal

☐ Internet Facing

VPC
Select a VPC ID

[Create a VPC](#)

FIPS Enabled
Select whether the endpoint should comply with Federal Information Processing Standards (FIPS)

☐ FIPS Enabled endpoint

[Cancel](#) [Previous](#) [Next](#)

- a. 對於端點類型，選擇VPC託管以託管伺服器的端點。如需有關設定 VPC託管端點的資訊，請參閱 [在虛擬私有雲端中建立伺服器](#)。

Note

AS2 通訊協定不支援公開存取的端點。若要透過網際網路存取您的VPC端點，請在存取下選擇網際網路面向，然後提供您的彈性 IP 地址。

- b. 針對存取，選擇下列其中一個選項：
- 內部 – 選擇此選項，即可從 VPC和 VPC連線環境中提供存取權，例如透過 AWS Direct Connect 或 的內部部署資料中心VPN。

- 面向網際網路 – 選擇此選項，即可透過網際網路提供存取權，以及從您的 VPC 和 VPC 連線環境中提供存取權，例如透過 AWS Direct Connect 或 的內部部署資料中心VPN。

如果您選擇面向網際網路，請在出現提示時提供彈性 IP 地址。

- c. 對於 VPC，請選擇現有 或VPC選擇建立VPC以建立新的 VPC。
- d. 對於FIPS已啟用，請保持清除FIPS已啟用端點核取方塊。

 Note

FIPSAS2通訊協定不支援已啟用的端點。

- e. 選擇 Next (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將檔案儲存並存取為物件。

選擇 Next (下一步)。

7. 在設定其他詳細資訊頁面上，選擇您需要的設定。

 Note

如果您將任何其他通訊協定與一起設定AS2，則所有其他詳細資訊設定都會套用。不過，對於AS2通訊協定，唯一適用的設定是CloudWatch 記錄和標籤區段中的設定。即使設定 CloudWatch 記錄角色是選用的，我們仍強烈建議進行設定，以便您可以查看訊息的狀態並疑難排解組態問題。

8. 在檢閱和建立頁面上，檢閱您的選擇，以確保其正確無誤。
 - 如果您想要編輯任何設定，請選擇您要變更的步驟旁的編輯。

 Note

如果您編輯步驟，建議您在選擇編輯的步驟之後檢閱每個步驟。

- 如果您沒有變更，請選擇建立伺服器以建立伺服器。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。

Servers (1)								Actions ▾	Add user	Create server
							< 1 >			
☐	Hostname ▲	Server ID ▾	State ▾	Service managed users ▾	Endpoint type ▾	Domain ▾				
☐	-	s-	Starting	-	VPC	Amazon S3				

新伺服器變更為線上 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

我們提供獨立的 AWS CloudFormation 範本，以快速建立啟用 AS2的 Transfer Family 伺服器。範本會使用公有 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：

- 如果您從此範本建立堆疊，則會向您收取 AWS 所使用的資源費用。
- 範本會建立多個憑證，並將其放入 AWS Secrets Manager 以安全地存放。您可以視需要從 Secrets Manager 刪除這些憑證，因為使用此服務需要支付費用。在 Secrets Manager 中刪除這些憑證不會從 Transfer Family 伺服器中刪除。因此，示範堆疊的功能不受影響。不過，對於您要與生產AS2伺服器搭配使用的憑證，您可能想要使用 Secrets Manager 來管理和定期輪換儲存的憑證。
- 我們建議您僅使用 範本做為基礎，主要用於示範用途。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，並建立您可以在生產中使用的 AWS Lambda 函數。

從 CloudFormation 範本建立AS2已啟用的 Transfer Family 伺服器

1. 在 <https://console.aws.amazon.com/cloudformation> 開啟 AWS CloudFormation 主控台。
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 Next (下一步)。
7. 在指定堆疊詳細資訊頁面上，為您的堆疊命名，然後指定下列參數：

- 在下AS2，分別輸入 Local AS2 ID 和 Partner AS2 ID 的值，或接受預設值 local和 partner。

- 在網路下，輸入安全群組傳入 CIDR IP 的值，或接受預設值 `0.0.0.0/0`。

 Note

此值的CIDR格式會指定傳入伺服器流量所允許的 IP 地址AS2。預設值會 `0.0.0.0/0` 允許所有 IP 地址。

- 在一般下，輸入字首 的值，或接受預設值 `transfer-as2`。此字首會放置在堆疊建立的任何資源名稱之前。例如，如果您使用預設字首，Amazon S3 儲存貯體會命名為 `transfer-as2-TransferS3BucketName`。
8. 選擇 Next (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訊，然後選擇建立堆疊。

 Note

在頁面底部，在功能下，您必須確認 AWS CloudFormation 可能會建立 AWS Identity and Access Management (IAM) 資源。

建立堆疊後，您可以使用 AWS Command Line Interface ()，從合作夥伴伺服器將測試AS2訊息傳送至本機 Transfer Family 伺服器AWS CLI。系統會建立用於傳送測試訊息的範例 AWS CLI 命令，以及堆疊中的所有其他資源。

若要使用此範例命令，請前往堆疊的輸出索引標籤，然後複製 `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 使用者指南 [中的安裝或更新最新版本的 AWS CLI](#)。AWS Command Line Interface

範例命令具有下列格式：

```
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

此命令的版本包含堆疊中 `TransferS3BucketName` 和 `TransferConnectorId` 資源的實際值。

此範例命令包含兩個使用&&字串鏈結在一起的個別命令。

第一個命令會在儲存貯體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，將檔案從合作夥伴設定檔傳送至本機設定檔。Transfer Family 伺服器已設定協議，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，您應該會在儲存貯體中看到下列物件：

- `processed/` – 此資料夾包含描述傳輸JSON檔案和MDN回應的檔案。
- `processing/` – 此資料夾暫時包含正在處理的檔案，但在傳輸完成後，此資料夾應該是空的。
- *server-id*/ – 此資料夾是根據 Transfer Family 伺服器 ID 命名。它包含 `from-partner`（此資料夾會根據合作夥伴的 AS2 ID 動態命名），其中包含 `failed/`、`processed/` 和 `processing/` 資料夾。*/server-id/from-partner/processed/* 資料夾包含傳輸的文字檔案副本，以及對應的 JSON 和 MDN 檔案。
- `test.txt` – 此物件是已傳輸的（空）檔案。

AS2 組態和限制

本主題說明使用適用性聲明 2（AS2）通訊協定的傳輸支援的組態、功能和功能，包括接受的密碼和摘要。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 配額和限制](#)

AS2 支援的組態

簽署、加密、壓縮、MDN

對於傳入和傳出傳輸，下列項目為必要或選用項目：

- 加密 – 必要（用於HTTP傳輸，這是目前唯一支援的傳輸方法）。只有在 TLS終止的代理轉送，例如 Application Load Balancer（ALB）且X-Forwarded-Proto: https標頭存在時，才會接受未加密的訊息。
- 簽署 – 選用
- 壓縮 – 選用（目前唯一支援的壓縮演算法為 ZLIB）
- 訊息處置通知（MDN） – 選用

Ciphers

傳入和傳出傳輸都支援下列密碼：

- AES128_CBC
- AES192_CBC
- AES256_CBC
- 3DES（僅限向後相容性）

摘要

支援下列摘要：

- 傳入簽署和 MDN – SHA1、SHA256、SHA384、SHA512
- 傳出簽署和 MDN – SHA1、SHA256、SHA384、SHA512

MDN

對於MDN回應，支援某些類型，如下所示：

- 傳入傳輸 – 同步和非同步
- 傳出傳輸 – 僅限同步
- 簡易郵件傳輸通訊協定（SMTP）（電子郵件 MDN） – 不支援

傳輸

- 傳入傳輸 – 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 進行傳入傳輸，您可以在 Application Load Balancer 或 Network Load Balancer TLS 上終止。如中所述 [透過接收 AS2 訊息 HTTPS](#)。

- 傳出傳輸 – 如果您提供 HTTP URL，則還必須指定加密演算法。如果您提供 HTTPS URL，您可以選擇 NONE 為加密演算法指定。

AS2 配額和限制

本節討論的配額和限制 AS2

主題

- [AS2 配額](#)
- [處理秘密的配額](#)
- [已知限制](#)

AS2 配額

檔案 AS2 傳輸具有下列配額。若要請求增加可調整的配額，請參閱中的 [AWS 服務配額](#) AWS 一般參考。

AS2 配額

名稱	預設	可調整
每個伺服器的傳入 AS2 請求	每秒 25 個	否
每個伺服器正在進行的傳入 AS2 請求	100	否
每個檔案傳輸請求的檔案數量上限	10	否
每個連接器的傳出 AS2 請求進行中	100	否

名稱	預設	可調整
檔案大小上限（壓縮或未壓縮）	50 MiB	是
閒置逾時	350 秒	否
每個帳戶的合作夥伴設定檔數目上限	1000（每個合作夥伴設定檔最多 10 個憑證：不可調整）	是
每個帳戶的憑證數量上限	1000	是
每個帳戶的每秒檔案傳輸請求數目上限	3	是
每個帳戶的連接器數量上限（SFTP和 AS2 連接器都有助於此計數）	100	是
每個帳戶連接器的最大頻寬（SFTP和 AS2 連接器都有助於此值）	50 MBps	否
每個伺服器的協議數目上限	100	是

處理秘密的配額

AWS Transfer Family AWS Secrets Manager 代表使用基本身分驗證AS2的客戶呼叫。此外，Secrets Manager 會呼叫 AWS KMS。

Note

這些配額並非專門針對您使用 Transfer Family 的秘密：它們會在您 中的所有 服務之間共用 AWS 帳戶。

對於 Secrets Manager GetSecretValue，套用的配額是 DescribeSecret 和 GetSecretValue API 請求的合併速率，如[AWS Secrets Manager 配額](#)中所述。

Secrets Manager **GetSecretValue**

名稱	值	描述
DescribeSecret 和 GetSecret Value API 請求的合併速率	每個支援的區域：每秒 1 萬個	DescribeSecret 和 GetSecret Value API 請求合併後，每秒的交易上限。

對於 AWS KMS，下列配額適用於 Decrypt。如需詳細資訊，請參閱 [為每個 AWS KMS API 操作請求配額](#)

AWS KMS **Decrypt**

配額名稱	預設值 (每秒請求數)
密碼編譯操作 (對稱) 請求率	這些共用配額會隨 AWS 區域和請求中使用的 AWS KMS 金鑰類型而有所不同。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	自訂金鑰存放區請求配額會針對每個自訂金鑰存放區分別計算。

配額名稱	預設值 (每秒請求數)
 Note 此配額僅適用於使用外部金鑰存放區的情況。	- 每個 AWS CloudHSM 金鑰存放區 1,800 (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保持連線。除非用戶端傳送保持連線封包，否則連線會在閒置 350 秒後逾時。
- 若要讓服務接受並出現在 Amazon CloudWatch 日誌中的作用中協議，訊息必須包含有效的AS2標頭。
- 從接收訊息的伺服器 AWS Transfer Family AS2必須支援加密訊息語法 (CMS) 演算法保護屬性，以驗證訊息簽章，如 [RFC6211](#) 所定義。某些舊版 IBM Sterling 產品不支援此屬性。
- 重複訊息IDs會導致已處理/警告：重複文件訊息。
- AS2 憑證的金鑰長度必須至少為 2048 位元，最多為 4096 位元。
- 傳送訊息AS2或非同步MDNs至交易合作夥伴端點時HTTPS，訊息 或 MDNs必須使用由公有信任SSL憑證授權單位 (CA) 簽署的有效憑證。目前不支援自我簽署憑證。
- 端點必須支援 1.2 TLS版通訊協定和安全政策允許的密碼編譯演算法 (如 中所述的[安全政策 AWS Transfer Family](#))。
- 目前不支援相互 TLS (m TLS)。
- 目前不支援來自 1.2 AS2版的多個附件和憑證交換訊息 (CEM)。
- 目前僅支援傳出訊息的基本身分驗證。

AS2 特徵和功能

下表列出使用的 Transfer Family 資源可用的功能AS2。

AS2 功能

Transfer Family 為提供下列功能AS2。

功能	支援者 AWS Transfer Family
Drummond 認證	是
AWS CloudFormation 支援	是
Amazon CloudWatch 指標	是
SHA-2 個密碼編譯演算法	是
支援 Amazon S3	是
支援 Amazon EFS	否
排程的訊息	是 ¹
AWS Transfer Family 受管工作流程	否
憑證交換訊息 (CEM)	否
相互 TLS (m TLS)	否

1. [使用 Amazon 排程 AWS Lambda 函數 EventBridge](#)即可使用傳出排程訊息

AS2 傳送和接收功能

下表提供傳送和接收功能的清單 AWS Transfer Family AS2。

功能	傳入：使用伺服器接收	傳出：使用連接器傳送
TLS 加密傳輸 (HTTPS)	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 地址	是	是

功能	傳入：使用伺服器接收	傳出：使用連接器傳送
攜帶您自己的 IP 地址	是	否
多個檔案附件	否	否
基本身分驗證	否	是
AS2 重新啟動	不適用	否
每個訊息的自訂主題	不適用	否

1. Network Load Balancer (NLB) 提供傳入TLS加密傳輸

2. 傳出非TLS傳輸僅在啟用加密時可用

設定AS2連接器

連接器的目的是在交易合作夥伴之間建立對外傳輸的關係，將AS2檔案從 Transfer Family 伺服器傳送至外部的合作夥伴擁有目的地。對於連接器，您可以指定本機方、遠端合作夥伴及其憑證（透過建立本機和合作夥伴設定檔）。建立連接器後，您可以將資訊傳輸給交易合作夥伴。

Note

交易合作夥伴收到的訊息大小與 Amazon S3 中的物件大小不相符。發生此差異是因為AS2訊息在傳送之前將檔案包裝在信封中。因此，即使檔案是以壓縮方式傳送，檔案大小也可能會增加。因此，請確定交易合作夥伴的檔案大小上限大於您要傳送的檔案大小。

適用性陳述式 2（AS2）連接器在交易合作夥伴之間建立對外傳輸的關係。如需AS2連接器的詳細資訊，請參閱 [設定AS2連接器](#)。

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 改為使用，請參閱 [the section called “步驟 6：在您與您的合作夥伴之間建立連接器”](#)。

若要建立AS2連接器

1. 在 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 – 輸入傳出連線URL的。
 - 存取角色 – 選擇要使用的（ARN）角色的 Amazon Resource Name AWS Identity and Access Management（IAM）。請確定此角色提供對StartFileTransfer請求中所用檔案位置之父目錄的讀取和寫入存取權。此外，請確定角色提供您要使用 傳送之檔案的父目錄的讀取和寫入存取權StartFileTransfer。

 Note

如果您使用連接器的基本身分驗證，存取角色需要 機密的secretsmanager:GetSecretValue許可。如果使用客戶受管金鑰而不是AWS 受管金鑰 中的 加密秘密 AWS Secrets Manager，則角色也需要該金鑰的kms:Decrypt許可。如果您使用字首 為秘密命名aws/transfer/，則可以使用萬用字元（*）新增必要的許可，如[建立秘密 的範例許可](#)所示。

- 記錄角色（選用）– 選擇連接器用來將事件推送至 CloudWatch 日誌IAM的角色。
4. 在AS2組態區段中，選擇本機和合作夥伴設定檔、加密和簽署演算法，以及是否要壓縮傳輸的資訊。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的舊版用戶端，否則請勿選擇，因為它是較弱的加密演算法。
 - 主旨會用作與連接器一起傳送AS2的訊息中的subjectHTTP標頭屬性。
 - 如果您選擇建立沒有加密演算法的連接器，則必須指定 HTTPS作為通訊協定。
 5. 在MDN組態區段中，指定下列資訊：
 - 請求 MDN – 您可以選擇要求交易合作夥伴在成功透過 接收您的訊息MDN後，傳送 給您AS2。
 - 已簽署 MDN – 您可以選擇要求MDNs簽署。只有在您已選取請求 MDN時，才能使用此選項。
 6. 在基本身分驗證區段中，指定下列資訊。
 - 若要傳送登入憑證與傳出訊息，請選取啟用基本身分驗證。如果您不想傳送任何包含傳出訊息的憑證，請保持清除啟用基本身分驗證。
 - 如果您使用身分驗證，請選擇 或建立秘密。
 - 若要建立新的秘密，請選擇建立新的秘密，然後輸入使用者名稱和密碼。這些憑證必須與連線至合作夥伴端點的使用者相符。

Basic authentication [Info](#)

☒ **Enable Basic authentication - optional**
Select this option to authenticate with your trading partner's host using username and password credentials.

Basic authentication credentials [Info](#)
Choose the username and password credentials that will be used to authenticate with your trading partner's host.

☒ Create a new secret

☐ Choose an existing secret

Username

Password

 Update the access role associated with your connector to provide AWS Transfer Family with permission to read the secret containing your Basic authentication credentials.

- 若要使用現有秘密，請選擇選擇現有秘密，然後從下拉式功能表中選擇秘密。如需在 Secrets Manager 中建立正確格式化秘密的詳細資訊，請參閱 [啟用AS2連接器的基本身分驗證](#)。

[illegible]

7. 確認所有設定後，請選擇建立連接器以建立連接器。

隨即出現 連接器頁面，並將新連接器的 ID 新增至清單。若要檢視連接器的詳細資訊，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，下列安全演算法會連接至連接器。

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 連接器的基本身分驗證

當您建立或更新使用AS2通訊協定的 Transfer Family 伺服器時，您可以為傳出訊息新增基本身分驗證。您可以將身分驗證資訊新增至連接器來執行此操作。

Note

只有在您使用時，才能使用基本身分驗證HTTPS。

若要使用連接器的身分驗證，請在基本身分驗證區段中選取啟用基本身分驗證。啟用基本身分驗證後，您可以選擇建立新的秘密，或使用現有的秘密。在任何一種情況下，秘密中的憑證都會與使用此連接器的傳出訊息一起傳送。憑證必須與嘗試連線至交易合作夥伴遠端端點的使用者相符。

下列螢幕擷取畫面顯示已選取啟用基本身分驗證，以及建立已選取的新秘密。做出這些選擇後，您可以輸入秘密的使用者名稱和密碼。

Basic authentication [Info](#)

☒ **Enable Basic authentication - optional**
Select this option to authenticate with your trading partner's host using username and password credentials.

Basic authentication credentials [Info](#)
Choose the username and password credentials that will be used to authenticate with your trading partner's host.

☒ **Create a new secret**

☐ **Choose an existing secret**

Username

Password

 **Update the access role associated with your connector to provide AWS Transfer Family with permission to read the secret containing your Basic authentication credentials.**

下列螢幕擷取畫面顯示已選取啟用基本身分驗證，以及選擇現有的秘密。您的秘密必須採用正確的格式，如 中所述[啟用AS2連接器的基本身分驗證](#)。

[illegible]

啟用AS2連接器的基本身分驗證

當您為AS2連接器啟用基本身分驗證時，您可以在 Transfer Family 主控台中建立新的秘密，也可以使用您在 中建立的秘密 AWS Secrets Manager。無論哪種情況，您的秘密都會儲存在 Secrets Manager 中。

主題

- 在主控台中建立新的秘密
- 使用現有的 密碼
- 在 中建立秘密 AWS Secrets Manager

在主控台中建立新的秘密

當您在主控台中建立連接器時，您可以建立新的秘密。

若要建立新的秘密，請選擇建立新的秘密，然後輸入使用者名稱和密碼。這些憑證必須與連線至合作夥伴端點的使用者相符。

Basic authentication [Info](#)

☒ **Enable Basic authentication - optional**
Select this option to authenticate with your trading partner's host using username and password credentials.

Basic authentication credentials [Info](#)
Choose the username and password credentials that will be used to authenticate with your trading partner's host.

☒ Create a new secret
☐ Choose an existing secret

Username

Password

i Update the access role associated with your connector to provide AWS Transfer Family with permission to read the secret containing your Basic authentication credentials.

i Note

當您在主控台中建立新的秘密時，秘密的名稱會遵循以下命名慣例：**/aws/transfer/*connector-id***，其中 *connector-id* 是您建立之連接器的 ID。當您嘗試在 中尋找秘密時，請考慮這一點 AWS Secrets Manager。

使用現有的 密碼

當您在主控台中建立連接器時，您可以指定現有的秘密。

若要使用現有秘密，請選擇選擇現有秘密，然後從下拉式功能表中選擇秘密。如需在 Secrets Manager 中建立正確格式化秘密的詳細資訊，請參閱 [在中建立秘密 AWS Secrets Manager](#)。

[illegible]

在中建立秘密 AWS Secrets Manager

下列程序說明如何建立適當的秘密以搭配AS2連接器使用。

 Note

只有在您使用時，才能使用基本身分驗證HTTPS。

在 Secrets Manager 中儲存使用者憑證以進行AS2基本身分驗證

1. 登入 AWS Management Console 並在 開啟 AWS Secrets Manager 主控台<https://console.aws.amazon.com/secretsmanager/>。

2. 在左側導覽窗格中，選擇秘密。
3. 在秘密頁面上，選擇儲存新的秘密。
4. 在選擇秘密類型頁面上，針對秘密類型，選擇其他類型的秘密。
5. 在金鑰/值對區段中，選擇金鑰/值標籤。
 - 金鑰 – 輸入 **Username**。
 - 值 – 輸入獲授權連線至合作夥伴伺服器之使用者名稱。
6. 如果您想要提供密碼，請選擇新增列，然後在鍵/值對區段中選擇鍵/值索引標籤。

選擇新增列，然後在鍵/值對區段中，選擇鍵/值索引標籤。

 - 金鑰 – 輸入 **Password**。
 - value – 輸入使用者的密碼。
7. 如果您想要提供私有金鑰，請選擇新增列，然後在金鑰/值對區段中選擇金鑰/值標籤。
 - 金鑰 – 輸入 **PrivateKey**。
 - 值 – 輸入使用者的私有金鑰。此值必須以開放SSH格式儲存，且必須對應至遠端伺服器中為此使用者儲存的公有金鑰。
8. 選擇 Next (下一步)。
9. 在設定秘密頁面上，輸入秘密的名稱和描述。我們建議您使用的字首 **aws/transfer/** 做為名稱。例如，您可以為秘密命名 **aws/transfer/connector-1**。
10. 選擇下一個，然後在設定輪換頁面上接受預設值。然後選擇下一步。
11. 在檢閱頁面上，選擇儲存以建立和儲存秘密。

建立秘密之後，您可以在建立連接器時選擇秘密（請參閱 [設定AS2連接器](#)）。在您啟用基本身分驗證的步驟中，從可用秘密的下拉式清單中選擇秘密。

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 連接器的詳細資訊和屬性清單。AS2 連接器的屬性包括其 URL、角色、設定檔MDNs、標籤和監控指標。

這是檢視連接器詳細資訊的程序。

檢視連接器詳細資訊

1. 在開啟 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 ID 欄中選擇識別符，以查看所選連接器的詳細資訊頁面。

您可以選擇編輯，變更AS2連接器詳細資訊頁面上連接器的屬性。

Transfer Family > Connectors > c-
c-
Delete

Connector configuration Info Edit

URL [http://](#) Access role [Access role](#) Logging role [Logging role](#)

Communication settings Info

AS2-From header [partner-test](#) AS2-To header [local-test](#)

AS2 configuration Info Edit

Local profile [partner-test](#) Compression [Disabled](#) Encryption algorithm [AES256_CBC](#)
 Partner profile [local-test](#) Message Subject [View](#) Signing algorithm [SHA256](#)

MDN configuration Info Edit

Request MDN [Enabled](#) Signed MDN [Default to message signing algorithm: SHA256](#) Synchronization [Enabled](#)

Basic authentication Info Edit

Basic authentication [Enabled](#) Secret [aws/transfer-](#)

Tags (3) Manage tags

Key	Value
awscloudformationstack-name	
awscloudformationlogical-id	TransferConnector
awscloudformationstack-id	arn:

AS2 Monitoring

OutboundMessages 2 OutboundMessage OutboundFailedMessage OutboundFailedMessage

1h 3h 12h 1d 3d 1w

No data available. Try adjusting the dashboard time range.

Note

您可以執行下列 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 [DescribeConnector](#) 在API參考中。

管理AS2合作夥伴

本主題討論如何管理AS2憑證、設定檔和協議。

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。合作夥伴可以將相同的金鑰用於這兩個目的，或對每個目的使用單獨的金鑰。如果您有受信任第三方託管中存放的常見加密金鑰，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。使用單獨的簽署金鑰（您不代書），不會損害數位簽章的不可否認功能。

Note

AS2 憑證的金鑰長度必須至少為 2048 位元，最多為 4096 位元。

下列各點詳細說明在程序期間如何使用AS2憑證。

- 傳入 AS2
 - 交易合作夥伴會傳送簽署憑證的公有金鑰，此金鑰會匯入合作夥伴設定檔。
 - 本機方會傳送其加密和簽署憑證的公有金鑰。然後，合作夥伴匯入私有金鑰或金鑰。本機方可以傳送單獨的憑證金鑰以進行簽署和加密，也可以選擇將相同的金鑰用於這兩個目的。
- 傳出 AS2
 - 合作夥伴會傳送其加密憑證的公有金鑰，此金鑰會匯入合作夥伴設定檔。
 - 本機方會傳送憑證的公有金鑰以供簽署，並匯入憑證的私有金鑰以供簽署。

如需如何建立憑證的詳細資訊，請參閱 [the section called “步驟 1：為 建立憑證 AS2”](#)。

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 改為使用，請參閱 [the section called “步驟 3：將憑證匯入為 Transfer Family 憑證資源”](#)。

若要指定已啟用 AS2的憑證

1. 在 開啟 AWS Transfer Family 主控台<https://console.aws.amazon.com/transfer/>。

2. 在左側導覽窗格中的交易AS2合作夥伴 下，選擇憑證。
3. 選擇 Import certificate (匯入憑證)。
4. 在憑證描述區段中，輸入憑證的易識別名稱。請確定您可以透過憑證的描述來識別憑證的目的。此外，選擇憑證的角色。
5. 在憑證內容區段中，提供貿易合作夥伴的公有憑證，或本機憑證的公有和私有金鑰。
6. 在憑證使用區段中，選擇此憑證的目的。它可用於加密、簽署或兩者。

 Note

如果您選擇加密並簽署使用，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 ENCRYPTION，另一個使用值為 SIGNING。

7. 將適當的詳細資訊填入憑證內容區段。
 - 如果您選擇自我簽署憑證，則不會提供憑證鏈。
 - 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。
 - 如果此憑證是本機憑證，請貼在其私有金鑰中。
8. 選擇匯入憑證以完成程序，並儲存匯入憑證的詳細資訊。

AS2 憑證輪換

通常，憑證的有效期為六個月到一年。您可能已設定要長時間保留的設定檔。為了方便此操作，Transfer Family 提供憑證輪換。您可以為設定檔指定多個憑證，讓您繼續使用設定檔多年。Transfer Family 使用憑證簽署（選用）和加密（必要）。如果您願意，可以為這兩個目的指定單一憑證。

憑證輪換是使用較新的憑證取代舊過期憑證的程序。如果協議中的合作夥伴尚未為傳出傳輸設定新憑證，或可能正在傳送使用較新的憑證的期間內使用舊憑證簽署或加密的承載，則轉換是一種逐步的轉換，以避免中斷傳輸。新舊憑證都有效的中期稱為寬限期。

X.509 憑證具有 Not Before和 Not After 日期。不過，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，以控制哪些憑證用於傳出承載，以及哪些憑證接受傳入承載。

傳出憑證選擇會使用傳輸日期之前的值上限作為 Inactive Date。傳入程序接受介於 Not Before和 範圍內的憑證，Not After以及介於 Active Date和 範圍內的憑證Inactive Date。

下表說明為單一設定檔設定兩個憑證的一種可能方法。

兩個輪換中的憑證

名稱	NOT BEFORE (由憑證授權機構控制)	ACTIVE DATE (由 Transfer Family 設定)	INACTIVE DATE (由 Transfer Family 設定)	NOT AFTER (由憑證授權機構設定)
Cert1 (舊憑證)	2019-11-01	2020-01-01	2020-12-31	2024-01-01
Cert2 (較新的憑證)	2020-11-01	2020-06-01	2021-06-01	2025-01-01

注意下列事項：

- 當您 Inactive Date 為憑證指定 Active Date 和時，範圍必須在介於 Not Before 和 之間的範圍內 Not After。
- 建議您為每個設定檔設定多個憑證，確保合併後所有憑證的有效日期範圍涵蓋您想要使用該設定檔的時間長度。
- 建議您在較舊的憑證變為非作用中和較新的憑證變為作用中之間指定一些寬限期。在上述範例中，第一個憑證在 2020-12-31 之前不會變成非作用中，而第二個憑證在 2020-06-01 變為作用中，提供 6 個月的寬限期。從 2020-06-01 到 2020-12-31 期間，這兩個憑證都是作用中的。

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。如果您想要改為使用 AWS CLI，請參閱 [the section called “步驟 4：為您和交易合作夥伴建立設定檔”](#)。

建立AS2設定檔

- 在開啟 AWS Transfer Family 主控台 <https://console.aws.amazon.com/transfer/>。
- 在左側導覽窗格AS2的交易合作夥伴下，選擇設定檔，然後選擇建立設定檔。
- 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-fromas2-to，並識別交易合作夥伴關係，這會決定要使用的憑證等。
- 在設定檔類型區段中，選擇本機設定檔或合作夥伴設定檔。

- 在憑證區段中，從下拉式選單中選擇一或多個憑證。

Note

如果您想要匯入未列在下拉式功能表中的憑證，請選取匯入新的憑證。這會在匯入憑證畫面上開啟新的瀏覽器視窗。如需匯入憑證的程序，請參閱 [匯入AS2憑證](#)。

- (選用) 在標籤區段中，指定一或多個鍵值對，以協助識別此設定檔。
- 選擇建立設定檔以完成程序並儲存新設定檔。

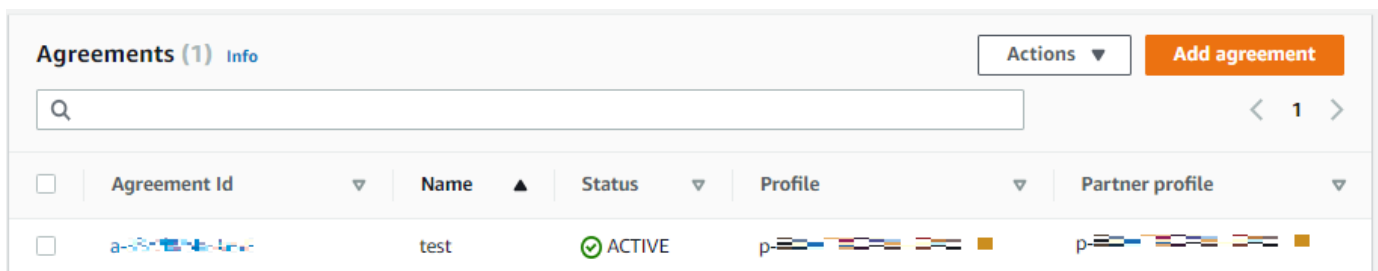
建立AS2協議

協議與 Transfer Family 伺服器相關聯。它們指定使用AS2通訊協定交換訊息或檔案的交易合作夥伴詳細資訊，方法是使用 Transfer Family 進行傳入傳輸，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協議。如果您想要 AWS CLI 改為使用，請參閱 [the section called “步驟 5：建立您與合作夥伴之間的協議”](#)。

為 Transfer Family 伺服器建立協議

- 在開啟 AWS Transfer Family 主控台 <https://console.aws.amazon.com/transfer/>。
- 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。
- 在伺服器詳細資訊頁面上，向下捲動至協議區段。



Agreements (1) Info					Actions	Add agreement
Q						
☐	Agreement Id	Name	Status	Profile	Partner profile	
☐	a-88888888-8888-8888-8888-888888888888	test	ACTIVE	p-88888888-8888-8888-8888-888888888888	p-88888888-8888-8888-8888-888888888888	

- 選擇新增協議。
- 填寫協議參數，如下所示：
 - 在協議組態區段中，輸入描述性名稱。請確定您可以根據協議的名稱來識別協議的目的。此外，請設定協議的狀態：作用中（依預設選取）或非作用中。
 - 在通訊組態區段中，選擇本機設定檔和合作夥伴設定檔。

- c. 在收件匣資料夾組態區段中，選擇 Amazon S3 儲存貯體來存放傳入檔案，以及可存取儲存貯體IAM的角色。或者，您可以輸入要用來將檔案儲存在儲存貯體中的字首（資料夾）。

例如，如果您**DOC-EXAMPLE-BUCKET**為儲存貯體輸入 **incoming**，並為字首輸入，傳入的檔案會儲存至 /DOC-EXAMPLE-BUCKET/incoming 資料夾。

- d. （選用）在標籤區段中新增標籤。
- e. 輸入協議的所有資訊後，請選擇建立協議。

新協議會出現在伺服器詳細資訊頁面的協議區段中。

傳送和接收AS2訊息

本節說明傳送和接收AS2訊息的程序。它還提供與AS2訊息相關聯的檔案名稱和位置的詳細資訊。

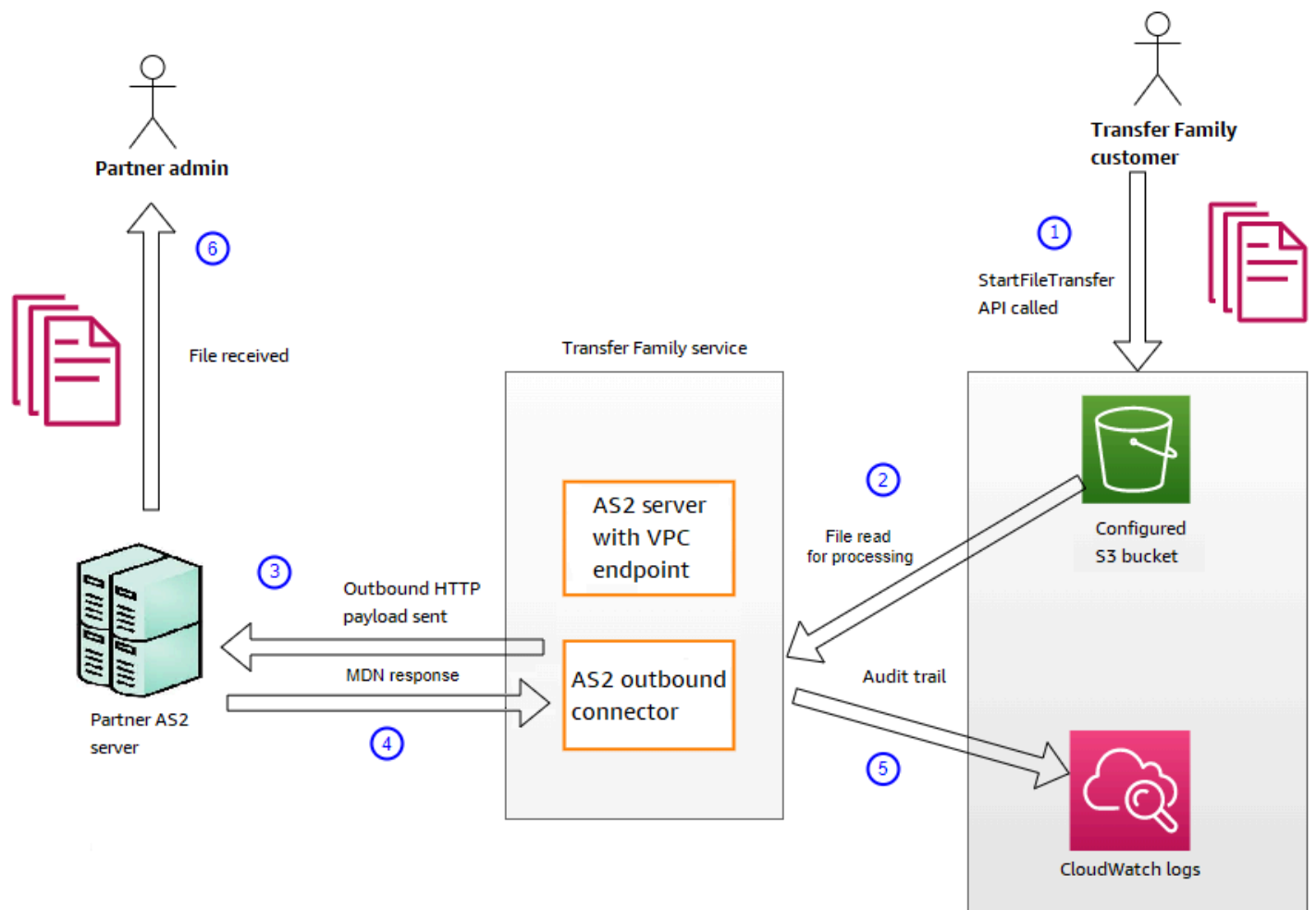
主題

- [AS2 傳送訊息程序](#)
- [接收AS2訊息程序](#)
- [透過 傳送和接收AS2訊息 HTTPS](#)
- [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](#)

AS2 傳送訊息程序

傳出程序定義為從 傳送至 AWS 外部用戶端或服務的訊息或檔案。傳出訊息的順序如下：

1. 管理員呼叫 start-file-transfer AWS Command Line Interface（AWS CLI）命令或 StartFileTransferAPI操作。此操作參考connector組態。
2. Transfer Family 偵測到新的檔案請求，並找到檔案。檔案會壓縮、簽署和加密。
3. 傳輸HTTP用戶端會執行HTTPPOST請求，將承載傳輸到合作夥伴的AS2伺服器。
4. 程序會傳回已簽署的MDN回應，並與HTTP回應內嵌（同步MDN）。
5. 當檔案在不同傳輸階段之間移動時，程序會將MDN回應接收和處理詳細資訊交付給客戶。
6. 遠端AS2伺服器可讓合作夥伴管理員使用解密和驗證的檔案。



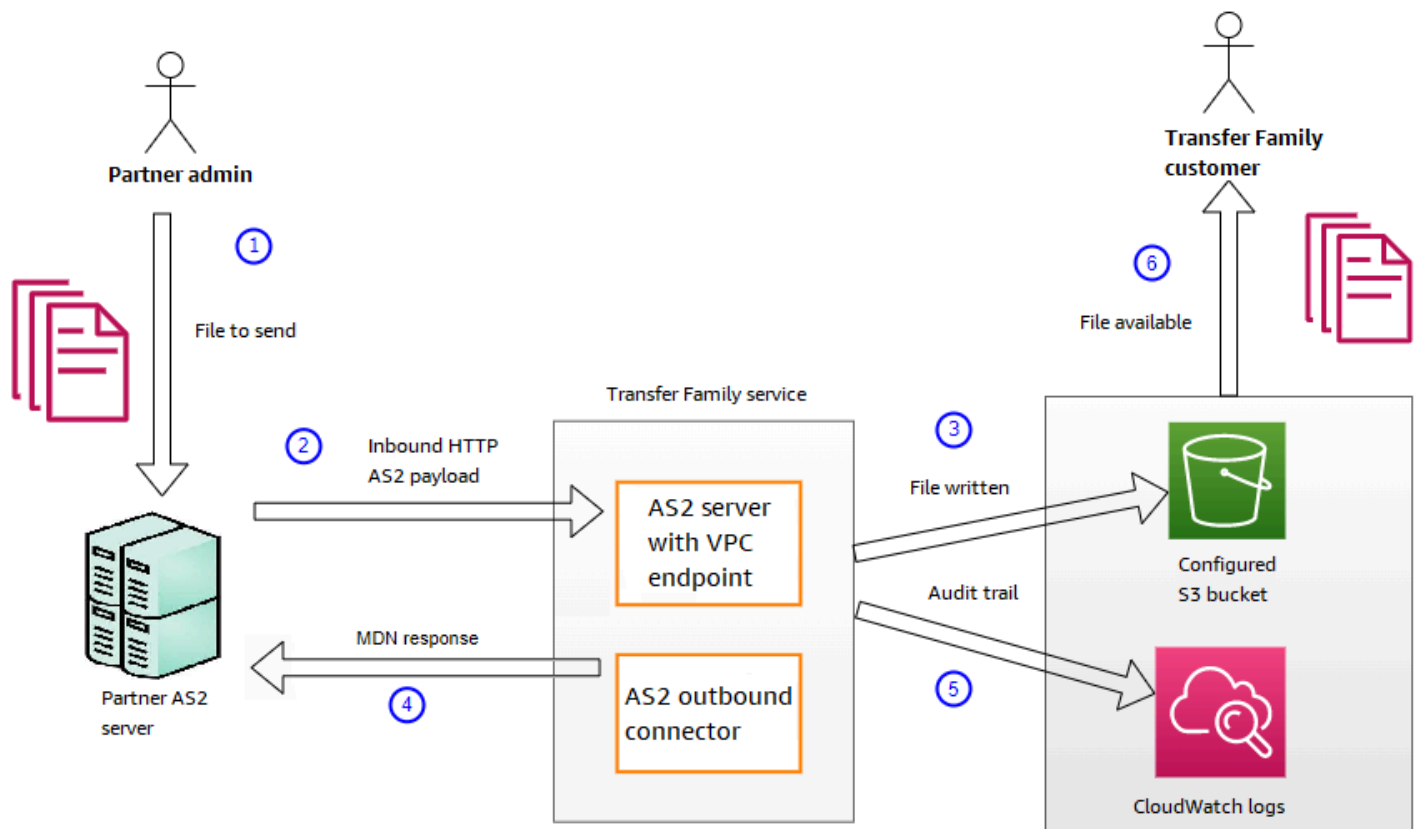
AS2 處理支援許多 RFC 4130 通訊協定，著重於常見的使用案例，以及與已啟用 AS2 的現有伺服器實作整合。如需支援組態的詳細資訊，請參閱 [AS2 支援的組態](#)。

接收AS2訊息程序

傳入程序定義為正在傳輸到 AWS Transfer Family 伺服器的訊息或檔案。傳入訊息的順序如下：

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伺服器會簽署和加密檔案內容，然後將HTTPPOST請求傳送至託管在 Transfer Family 上的AS2傳入端點。
3. 使用伺服器、合作夥伴、憑證和協議的設定值，Transfer Family 會解密並驗證AS2承載。檔案內容會儲存在設定的 Amazon S3 檔案存放區中。
4. 已簽署的MDN回應會與HTTP回應並列傳回，或透過個別HTTPPOST請求非同步傳回原始伺服器。
5. 稽核追蹤會寫入 Amazon，CloudWatch 其中包含交換的詳細資訊。

6. 解密的檔案可在名為 `inbox/processed` 的資料夾中使用 `inbox/processed`。



透過 傳送和接收AS2訊息 HTTPS

本節說明如何設定使用AS2通訊協定透過 傳送和接收訊息的 Transfer Family 伺服器HTTPS。

透過 AS2 傳送訊息 HTTPS

若要AS2使用 傳送訊息HTTPS，請使用下列資訊建立連接器：

- 針對 URL，指定 HTTPS URL
- 針對加密演算法，指定 NONE。
- 提供連接器的剩餘值，如 中所述[設定AS2連接器](#)。

透過 接收AS2訊息 HTTPS

AWS Transfer Family AS2 伺服器目前僅透過連接埠 5080 提供HTTP傳輸。不過，您可以使用您選擇的連接埠和憑證，TLS在 Transfer Family 伺服器VPC端點前方的負載平衡器上終止。透過此方法，您可以讓傳入AS2訊息使用 HTTPS。

先決條件

- VPC 必須與 Transfer Family 伺服器 AWS 區域 位於相同的 中。
- 您的子網路VPC必須位於您要使用伺服器的可用區域中。

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配置最多三個彈性 IP 地址。或者，您可以選擇攜帶自己的 IP 地址範圍 (BYOIP) 。

Note

彈性 IP 地址的數目必須與伺服器端點使用的可用區域數目相符。

設定 Network Load Balancer

在 中設定面向網際網路的網路Load Balancer (NLB) VPC。

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 開啟 Amazon Elastic Compute Cloud 主控台<https://console.aws.amazon.com/ec2/>。
2. 從導覽窗格中，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：
 - 針對名稱，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)。
 - 對於 IP address type (IP 地址類型)，請選擇 IPv4。
5. 在網路映射區段中，輸入下列資訊：

- 針對 VPC，選擇您建立的虛擬私有雲端（VPC）。
 - 在映射下，選擇與VPC伺服器端點使用的相同可用公有子網路相關聯的可用區域。
 - 針對每個子網路IPv4的地址，選擇您配置的其中一個彈性 IP 地址。
6. 在接聽程式和路由區段中，輸入下列資訊：
- 針對 rotocol (通訊協定)，選擇 TLS。
 - 針對連接埠，輸入 **5080**。
 - 針對預設動作，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，選擇預設SSL/TLS憑證區域中的憑證。
8. 選擇建立負載平衡器以建立您的 NLB。
9. （選用，但建議）開啟 Network Load Balancer 的存取日誌，以維護完整的稽核追蹤，如 [Network Load Balancer 的存取日誌](#) 中所述。

建議您執行此步驟，因為 終止了TLS連線NLB。因此，傳輸系列AS2 CloudWatch日誌群組中反映的來源 IP 地址是 NLB的私有 IP 地址，而不是交易合作夥伴的外部 IP 地址。

設定負載平衡器後，用戶端會透過自訂連接埠接聽程式與負載平衡器通訊。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後，系統會將您導向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。
 - 對於選擇目標類型，選擇 IP 地址。
 - 針對 Target group name (目標群組名稱)，輸入目標群組的名稱。
 - 針對 rotocol (通訊協定)，選擇 TCP。
 - 針對連接埠，輸入 **5080**。
 - 對於 IP address type (IP 地址類型)，請選擇 IPv4。
 - 針對 VPC，選擇您為 Transfer Family AS2 伺服器建立VPC的。
3. 在運作狀態檢查區段中，TCP選擇運作狀態檢查通訊協定。

4. 選擇 Next (下一步)。
5. 在註冊目標頁面上，輸入下列資訊：
 - 對於網路，請確認已指定您為 Transfer Family AS2 伺服器建立VPC的。
 - 針對IPv4地址，輸入 Transfer Family AS2 伺服器端點的私有IPv4地址。

如果您的伺服器有多個端點，請選擇新增IPv4地址以新增另一列，以輸入另一個IPv4地址。重複此程序，直到您為所有伺服器的端點輸入私有 IP 地址為止。

 - 確定連接埠設定為 **5080**。
 - 選擇包含為待定，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的程序，NLB並在指示處輸入新的目標群組。

從彈性 IP 地址測試對伺服器的存取

使用彈性 IP 地址或 Network Load Balancer DNS的名稱，透過自訂連接埠連線至伺服器。

Important

使用負載平衡器上設定的子網路的網路存取控制清單 (網路 ACLs)，從用戶端 IP 地址管理對伺服器的存取。網路ACL許可是在子網路層級設定，因此規則會套用至使用子網路的所有資源。您無法透過使用安全群組控制來自用戶端 IP 地址的存取，因為負載平衡器的目標類型設定為 IP 地址，而不是執行個體。因此，負載平衡器不會保留來源 IP 地址。如果 [Network Load Balancer 的運作狀態檢查](#)失敗，這表示負載平衡器無法連線至伺服器端點。若要對此問題進行疑難排解，請檢查下列項目：

- 確認伺服器端點的關聯安全群組允許來自負載平衡器上設定的子網路的傳入連線。負載平衡器必須能夠透過連接埠 5080 連線至伺服器端點。
- 確認伺服器的狀態為線上。

使用AS2連接器傳輸檔案

AS2 連接器會在交易合作夥伴之間建立關係，以將AS2訊息從 Transfer Family 伺服器傳輸到外部、合作夥伴擁有的目的地。

您可以使用 Transfer Family，參考連接器 ID 和檔案的路徑來AS2傳送訊息，如下列 `start-file-transfer` AWS Command Line Interface (AWS CLI) 命令所示：

```
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訊，請執行下列命令：

```
aws transfer list-connectors
```

`list-connectors` 命令會傳回連接器的連接器 IDs、URLs和 Amazon Resource Names (ARNs)。

若要傳回特定連接器的屬性，請使用您要使用的 ID 執行下列命令：

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

`describe-connector` 命令會傳回連接器的所有屬性，包括其 URL、角色、設定檔、訊息處置通知 (MDNs)、標籤和監控指標。

您可以檢視 JSON和 檔案，確認合作夥伴已成功收到MDN檔案。這些檔案是根據中所述的慣例命名 [檔案名稱和位置](#)。如果您在建立連接器時設定了記錄角色，您也可以檢查 CloudWatch 日誌是否有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](#)。如需建立AS2連接器的詳細資訊，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：

- 您可以在協議中指定基礎目錄。基礎目錄是 Amazon S3 儲存貯體名稱，如果有的話，會加上字首。例如：/DOC-EXAMPLE-BUCKET/AS2-folder。
- 如果成功處理傳入檔案，檔案（和對應的JSON檔案）會儲存至 /processed 資料夾。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
- 如果無法成功處理傳入的檔案，檔案（和對應的JSON檔案）會儲存至 /failed 資料夾。例如：/DOC-EXAMPLE-BUCKET/AS2-folder/failed。
- 傳輸的檔案會以 的形式存放在processed資料夾中 *original_filename.messageId.original_extension*。也就是說，傳輸的訊息 ID 會附加到檔案名稱，然後再附加到原始副檔名。
- JSON 檔案會建立並儲存為 *original_filename.messageId.original_extension.json*。除了要新增的訊息 ID 之外，字串.json也會附加到傳輸的檔案名稱。
- 訊息處置通知（MDN）檔案會建立並儲存為 *original_filename.messageId.original_extension.mdn*。除了要新增的訊息 ID 之外，字串.mdn也會附加到傳輸的檔案名稱。
- 如果有名為 的傳入檔案ExampleFileInS3Payload.dat，則會建立下列檔案：
 - 檔案 –

檔案名稱和位置 ExampleFileInS3Payload.c4d6b6c7-23ea-4b8c-9ada-0cb811dc8b35e44313c54b0a46a36.

- JSON –

ExampleFileInS3Payload.c4d6b6c7-23ea-4b8c-9ada-0cb811dc8b35@44313c54b0a46a36.

- MDN –

ExampleFileInS3Payload.c4d6b6c7-23ea-4b8c-9ada-0cb811dc8b35@44313c54b0a46a36.

對於傳出傳輸，命名類似，沒有傳入訊息檔案的差異，而且傳輸訊息的傳輸 ID 也會新增至檔案名稱。傳輸 ID 會由 StartFileTransferAPI 操作傳回（或當另一個程序或指令碼呼叫此操作時）。

- transfer-id 是與檔案傳輸相關聯的識別符。所有屬於 StartFileTransfer 呼叫的請求都會共用 transfer-id。
- 基礎目錄與您用於來源檔案的路徑相同。也就是說，基礎目錄是您在 StartFileTransferAPI 操作或 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
```

如果您執行此命令，MDN 且 JSON 檔案儲存在 /DOC-EXAMPLE-BUCKET/AS2-folder/processed（用於成功傳輸）或 /DOC-EXAMPLE-BUCKET/AS2-folder/failed（用於傳輸失敗）中。

- JSON 檔案會建立並儲存為 *original_filename.transferId.messageId.original_extension.json*。
- MDN 檔案會建立並儲存為 *original_filename.transferId.messageId.original_extension.mdn*。
- 如果有名為的傳出檔案 ExampleFileOutTestOutboundSyncMdn.dat，則會建立下列檔案：
 - JSON – ExampleFileOutTestOutboundSyncMdn.dedf4601-4e90-4043-b16b-579af35e0d83.fbe18db8-7361-42ff-8ab6-49ec1e435f34@c9c705f0baaaabaa.dat.json
 - MDN – ExampleFileOutTestOutboundSyncMdn.dedf4601-4e90-4043-b16b-579af35e0d83.fbe18db8-7361-42ff-8ab6-49ec1e435f34@c9c705f0baaaabaa.dat.mdn

您也可以檢查 CloudWatch 日誌以檢視傳輸的詳細資訊，包括任何失敗的。

狀態碼

下表列出當您或合作夥伴傳送訊息時，可以記錄到 CloudWatch 日誌的所有狀態碼AS2。不同的訊息處理步驟適用於不同的訊息類型，且僅用於監控。COMPLETED 和 FAILED 狀態代表處理中的最後一個步驟，且會顯示在JSON檔案中。

代碼	描述	處理完成？
PROCESSING	訊息正在轉換為其最終格式。 例如，解壓縮和解密步驟都具有此狀態。	否
MDN_TRANSMIT	訊息處理正在傳送MDN回應。	否
MDN_RECEIVE	訊息處理正在接收MDN回應。	否
COMPLETED	訊息處理已成功完成。此狀態包括MDN傳送傳入訊息或MDN驗證傳出訊息的。	是
FAILED	訊息處理失敗。如需錯誤代碼的清單，請參閱 AS2 錯誤代碼 。	是

範例JSON檔案

本節列出傳入和傳出傳輸的範例JSON檔案，包括用於成功傳輸和失敗傳輸的範例檔案。

成功傳輸的範例傳出檔案：

```
{
  "requester-content-type": "application/octet-stream",
  "message-subject": "File xyzTest from MyCompany_0ID to partner YourCompany",
  "requester-file-name": "TestOutboundSyncMdn-9lmCr79hV.dat",
  "as2-from": "MyCompany_0ID",
  "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/as2testcell10000/openAs2/
TestOutboundSyncMdn-9lmCr79hV.dat",
"as2-message-id": "fbe18db8-7361-42ff-8ab6-49ec1e435f34@c9c705f0baaaabaa",
"timestamp": "2022-07-11T06:30:10.791274Z"
}

```

未成功傳輸的範例傳出檔案：

```

{
"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/as2IntegCell10002/openAs2/
openAs2TestOutboundWrongAs2Ids-necco-3VYn5n8wE.dat",
"timestamp": "2022-07-11T21:17:24.802378Z"
}

```

成功傳輸的傳入檔案範例：

```

{
"requester-content-type": "application/EDI-X12",
"subject": "File openAs2TestInboundAsyncMdn-necco-5Ab6bTfC0.dat sent from MyCompany
to PartnerA",
"client-ip": "10.0.109.105",
"requester-file-name": "openAs2TestInboundAsyncMdn-necco-5Ab6bTfC0.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-5Ab6bTfC0.OPENAS2-11072022233606+0000-5dab0452-0ca1-4f9b-b622-fba84effff3c@MyCompany_OID_PartnerA_OID.dat",
  "server-id": "s-5f7422b04c2447ef9",
  "timestamp": "2022-07-11T23:36:36.105030Z"
}
```

未成功傳輸的傳入檔案範例：

```
{
  "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，[請參閱 Amazon CloudWatch 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。

指標	描述
	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 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 <i>send-file-path</i> - 無法取得憑證 ErrorCode : <i>#</i> <i>#</i>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。

代碼	錯誤	說明和解析度
		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。

代碼	錯誤	說明和解析度
CREDENTIALS_RETRIEVAL_FAILED	1. 密碼管理員中找不到密碼。 2. 無法存取 Secrets Manager。 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。	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。 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，請參閱處理秘密的配額。
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# <i>ID</i> 。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。
INSUFFICIENT_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	- 郵件標頭有問題。 - 無法剖析機密 JSON。 機密 JSON 與預期的格式不符。 - 密碼必須是 JSON 字串。 - 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。 - 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。 - 請確保密碼值與記錄的格式相符，如中所述啟用AS2連接器的基本身分驗證。 - 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。 - 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。

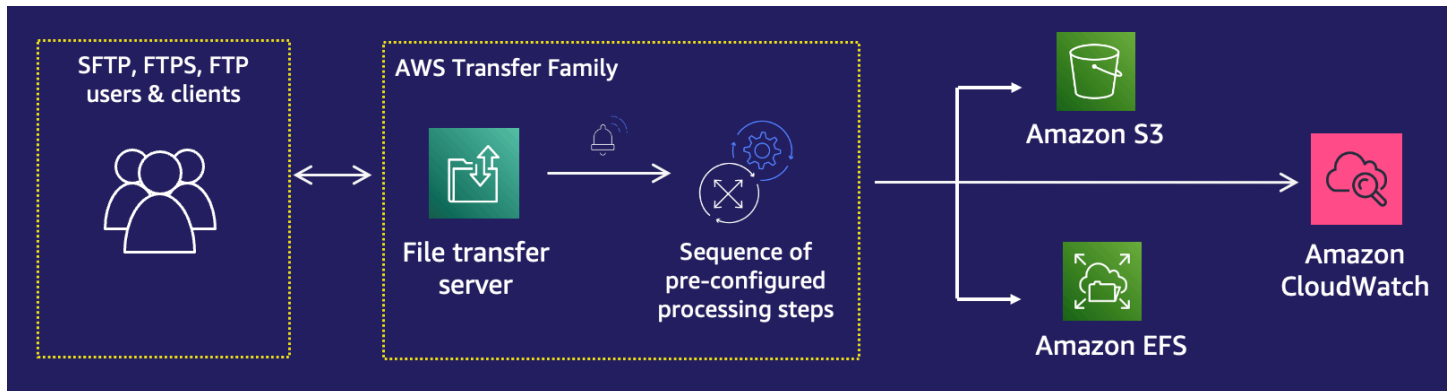
代碼	錯誤	說明和解析度
MDN_RESPONSE_INDICATES_DECRYPTION_FAILED	不適用	接收者無法解密訊息內容。協力廠商將 MDN 傳回給「Transfer Family 列」，且 處置修正因子 錯誤：驗證失敗。
MDN_RESPONSE_INDICATES_INSUFFICIENT_MESSAGE_SECURITY	不適用	接收者希望郵件經過簽署或加密，但事實並非如此。協力廠商將 MDN 傳回至「Transfer Family」，且 處置修正因子 錯誤為：。insufficient-message-security 在連接器上啟用簽署和/或加密，以符合交易夥伴的期望。
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 受管工作流程

AWS Transfer Family 支援檔案處理的受管工作流程。透過受管工作流程，您可以在檔案透過 SFTP、FTPS 或 傳輸之後啟動工作流程。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 稽核和可見性中受益。



透過協調檔案處理任務，受管工作流程可協助您在下游應用程式取用資料之前先行處理資料。此類檔案處理任務可能包括：

- 將檔案移至使用者特定的資料夾。
- 將檔案解密為工作流程的一部分。
- 標記檔案。
- 透過建立 AWS Lambda 函數並將其連接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文章，請參閱[使用 AWS Transfer Family 受管工作流程自訂檔案交付通知。](#)）

若要快速複寫和標準化組織中跨多個業務單位的常見上傳後檔案處理任務，您可以使用基礎設施作為程式碼（ IaC 部署工作流程。您可以指定要在完整上傳的檔案上啟動的受管工作流程。您也可以指定不同的受管工作流程，以便在因為過早中斷連線而僅部分上傳的檔案上啟動。內建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日誌，您可以稽核以追蹤資料譜系。

若要開始使用，請執行下列任務：

1. 設定工作流程以包含預先處理動作，例如根據您的需求複製、標記和其他步驟。如需詳細資訊，請參閱 [建立工作流程](#)。

2. 設定執行角色，轉移系列用於執行工作流程。如需詳細資訊，請參閱 [IAM 工作流程的政策](#)。
3. 將工作流程映射至伺服器，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

- 若要監控工作流程執行，請參閱 [使用 Transfer Family 的 CloudWatch 指標](#)。
- 如需詳細的執行日誌和疑難排解資訊，請參閱 [使用 Amazon 對工作流程相關錯誤進行故障診斷 CloudWatch](#)。
- 我們有一個您可以參加的研討會，您可以在其中建置檔案傳輸解決方案。此解決方案 AWS Transfer Family 會利用 受管 SFTP/FTPS 端點和 Amazon Cognito 和 DynamoDB 進行使用者管理。您可以在[這裡檢視此研討會的詳細資訊](#)。
- 檢視[AWS Transfer Family 受管工作流程](#)，以取得 Transfer Family 工作流程的簡介。

主題

- [建立工作流程](#)
- [使用預先定義的步驟](#)
- [使用自訂檔案處理步驟](#)
- [IAM 工作流程的政策](#)
- [工作流程的例外處理](#)
- [監控工作流程執行](#)
- [從範本建立工作流程](#)
- [從 Transfer Family 伺服器移除工作流程](#)
- [受管工作流程的限制](#)

如需使用受管工作流程的更多說明，請參閱下列資源：

- [AWS Transfer Family 受管工作流程](#) 示範影片
- [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，主控台的大多數區段都可以使用內容說明面板。

工作流程有兩種步驟：

- 名義步驟 – 名義步驟是您要套用至傳入檔案的檔案處理步驟。如果您選擇多個標稱步驟，則每個步驟都會以線性順序處理。
- 例外處理步驟 – 例外處理常式是檔案處理步驟，可在任何標稱步驟失敗或導致驗證錯誤時 AWS Transfer Family 執行。

建立工作流程

1. 在 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。
 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。此描述會顯示在工作流程頁面上。
 5. 在額定步驟區段中，選擇新增步驟。新增一或多個步驟。
 - a. 從可用的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 “使用預先定義的步驟”](#)。
 - b. 選擇下一個，然後設定步驟的參數。
 - c. 選擇下一個，然後檢閱步驟的詳細資訊。
 - d. 選擇建立步驟以新增步驟並繼續。
 - e. 視需要繼續新增步驟。工作流程中的步驟數目上限為 8。
 - f. 新增所有必要的標稱步驟後，向下捲動至例外處理常式 – 選用區段，然後選擇新增步驟。
- 
- Note
- 為了即時通知您故障，我們建議您設定例外處理常式，並在工作流程失敗時執行步驟。
6. 若要設定例外處理常式，請以與上述相同的方式新增步驟。如果檔案造成任何步驟擲回例外狀況，則會逐一叫用例外狀況處理常式。
 7. （選用）向下捲動至標籤區段，並為工作流程新增標籤。

8. 檢閱組態，然後選擇建立工作流程。

Important

建立工作流程後，您無法對其進行編輯，因此請務必仔細檢閱組態。

設定和執行工作流程

在執行工作流程之前，您需要將其與 Transfer Family 伺服器建立關聯。

設定 Transfer Family 對上傳的檔案執行工作流程

1. 在開啟 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。
 - 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，建立新的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訊區段，然後選擇編輯。

Note

根據預設，伺服器沒有任何相關聯的工作流程。您可以使用其他詳細資訊區段，將工作流程與選取的伺服器建立關聯。

4. 在編輯其他詳細資訊頁面的受管工作流程區段中，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，請選擇建立新工作流程來建立工作流程。

- 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擔任的角色。如需詳細資訊，請參閱 [IAM 工作流程的政策](#)。選擇 Save (儲存)。

Managed workflows [Info](#)

Workflow for complete file uploads
Select the workflow that AWS Transfer Family should run on all files that are uploaded in full via this server

w-

Create a new Workflow

Workflow for partial file uploads
Select the workflow that Transfer Family should run on all files that are only partially uploaded via this server

w-

Create a new Workflow

Managed workflows execution role [Info](#)
Select the role that AWS Transfer Family should assume when executing a workflow

Note

如果您不再希望工作流程與伺服器建立關聯，您可以移除關聯。如需詳細資訊，請參閱 [從 Transfer Family 伺服器移除工作流程](#)。

執行工作流程

若要執行工作流程，您可以將檔案上傳到使用相關聯工作流程設定的 Transfer Family 伺服器。

Note

每當您從伺服器移除工作流程並將其取代為新的工作流程，或更新伺服器組態（這會影響工作流程的執行角色）時，您必須等待約 10 分鐘，才能執行新的工作流程。Transfer Family 伺服器快取工作流程詳細資訊，伺服器重新整理其快取需要 10 分鐘。

此外，您必須登出任何作用中 SFTP 工作階段，然後在 10 分鐘等待期後重新登入，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
>
```

上傳檔案後，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 Logs 來追蹤執行的步驟及其執行狀態。

檢視工作流程詳細資訊

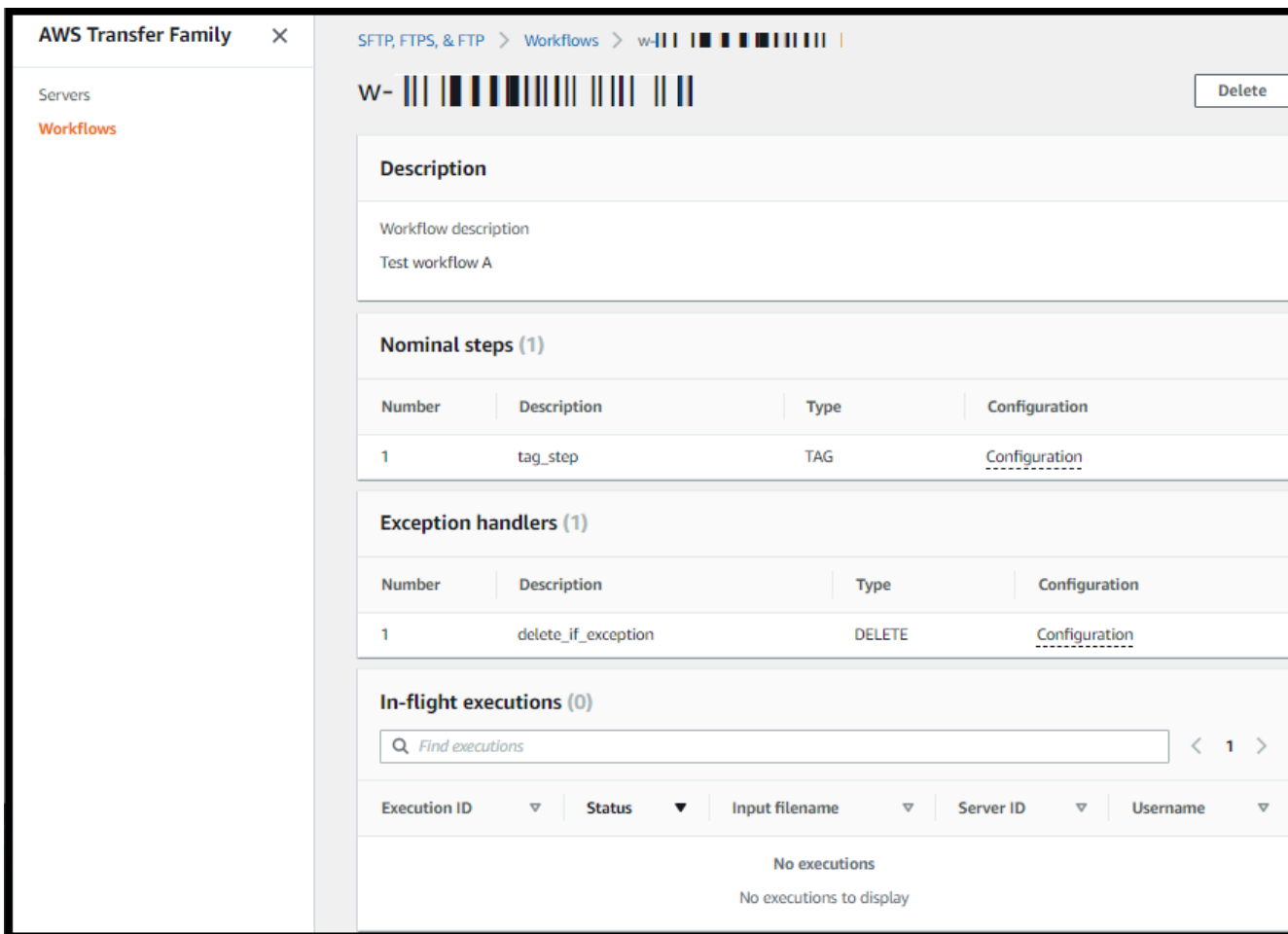
您可以檢視先前建立的工作流程或工作流程執行的詳細資訊。若要檢視這些詳細資訊，您可以使用主控台或 AWS Command Line Interface (AWS CLI)。

Console

檢視工作流程詳細資訊

1. 在 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。
3. 在工作流程頁面上，選擇工作流程。

工作流程詳細資訊頁面隨即開啟。



CLI

若要檢視工作流程詳細資訊，請使用 `describe-workflow` CLI 命令，如下列範例所示。將工作流程 ID 取代 `w-1234567890abcdef0` 為您自己的值。如需詳細資訊，請參閱 AWS CLI 命令參考 中的 [describe-workflow](#)。

```
# 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/"
            }
          }
        },
        "OnError": {
          "Name": "Copy to shared",
          "FileLocation": {
            "S3FileLocation": {
              "Bucket": "DOC-EXAMPLE-BUCKET",
              "Key": "home/shared_files/"
            }
          }
        },
        "OnException": {}
      }
    ],
    "OnError": {}
  }
}
```

如果您的工作流程是作為 AWS CloudFormation 堆疊的一部分建立的，您可以使用 AWS CloudFormation 主控台（<https://console.aws.amazon.com/cloudformation>）管理工作流程。

Transfer Family > Workflows > workflow-stack-name

Workflow Stack

Delete

This workflow belongs to the AWS CloudFormation stack **WorkflowStack**. [Manage this stack](#) on the CloudFormation console.

Description

Workflow description

-

Nominal steps (1) [Info](#)

Number	Description	Type	Configuration
1	tagFileForArchive	TAG	Details

Exception handlers (0) [Info](#)

Number	Description	Type	Configuration

使用預先定義的步驟

建立工作流程時，您可以選擇新增本主題中討論的下列其中一個預先定義步驟。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](#)
- [解密檔案](#)
- [標籤檔案](#)
- [刪除檔案](#)
- [工作流程的命名變數](#)
- [範例標籤和刪除工作流程](#)

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，您只能將複製檔案步驟與 Amazon S3 搭配使用。

下列複製檔案步驟會將檔案複製到file-test目的地儲存貯體中的test資料夾。

如果複製檔案步驟不是工作流程的第一個步驟，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傳的原始檔案。您可以使用此功能製作原始檔案的多個複本，同時保持來源檔案的完整，以供檔案封存和記錄保留。如需範例，請參閱[範例標籤和刪除工作流程](#)。

Configure copy parameters

Step name

File location

Select the file location to use as an input for this step

☒ Copy the file created from previous step to a new location

Input file is selected from the previous step's output

☐ Copy the original source file to a new location

Originally uploaded file

Destination bucket name

Destination key prefix

If you are copying files into a folder, specify / at the end of the prefix name. Use `${transfer:UserName}` or `${transfer:UploadDate}` to parametrize destination prefix by username or upload date respectively.

☐ Overwrite existing

提供儲存貯體和金鑰詳細資訊

您必須提供副本檔案步驟目的地的儲存貯體名稱和金鑰。金鑰可以是路徑名稱或檔案名稱。金鑰是否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，其名稱不會變更。如果最後一個字元是英數字元，則上傳的檔案會重新命名為索引鍵值。在此情況下，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。

- 如果選取覆寫現有檔案，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，則不會發生任何情況，工作流程處理也會停止。

i Tip

如果在相同的檔案路徑上執行並行寫入，可能會在覆寫檔案時產生非預期的行為。

例如，如果您的金鑰值為 `test/`，則上傳的檔案會複製到 `test` 資料夾。如果您的金鑰值為 `test/today`，則您上傳的每個檔案都會複製到 `test` 資料夾中名為 `today` 的檔案（並選取覆寫現有檔案），而每個後續檔案都會覆寫上一個檔案。

i Note

Amazon S3 支援儲存貯體與物件，且沒有任何階層。不過，您可以在物件金鑰名稱中使用字首和分隔符號來暗示階層，並以類似於資料夾的方式整理資料。

在複製檔案步驟中使用具名變數

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}` 作為變數，將檔案複製到上傳檔案之指定使用者的目的地位置，或根據目前日期。

在下列範例中，如果使用者 `richard-roe` 上傳檔案，則會將其複製到 `file-test2/richard-roe/processed/` 資料夾。如果使用者 `mary-major` 上傳檔案，則會將其複製到 `file-test2/mary-major/processed/` 資料夾。

Configure parameters

Configure copy parameters

Step name

dynamic-copy

Destination bucket name

file-test2 ▼

Destination key prefix

If you are copying files into a folder, specify / at the end of the prefix name. Use `${transfer:UserName}` or `${transfer:UploadDate}` to parametrize destination prefix by username or upload date respectively.

`${transfer:UserName}/processed`

☐ Overwrite existing

同樣地，您可以使用 `${transfer:UploadDate}` 作為變數，將檔案複製到名為目前日期的目的地位置。在下列範例中，如果您在 2022 年 2 月 1 日 `${transfer:UploadDate}/processed` 日將目的地設定為 `file-test2/2022-02-01/processed/` 資料夾，上傳的檔案會複製到 `file-test2/2022-02-01/processed/` 資料夾。

Configure copy parameters

Step name

dynamic-copy-date

Destination bucket name

file-test2

Destination key prefix

If you are copying files into a folder, specify / at the end of the prefix name. Use `${transfer:UserName}` or `${transfer:UploadDate}` to parametrize destination prefix by username or upload date respectively.

`${transfer:UploadDate}/processed`

☐ Overwrite existing

您也可以將這兩個變數結合其功能使用。例如：

- 您可以將目的地金鑰字首設定為 **folder/\${transfer:UserName}/\${transfer:UploadDate}/**，這會建立巢狀資料夾，例如 folder/marymajor/2023-01-05/。
- 您可以將目的地金鑰字首設定為 **folder/\${transfer:UserName}-\${transfer:UploadDate}/**，以串連兩個變數，例如 folder/marymajor-2023-01-05/。

IAM 複製步驟的許可

若要讓複製步驟成功，請確定工作流程的執行角色包含下列許可。

```
{
  "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

只有在您未選取覆寫現有的 時，才需要此 `s3:ListBucket` 許可。此許可會檢查您的儲存貯體，以查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，而且可以直接寫入。

如果您的 Amazon S3 檔案有標籤，您需要將一或兩個許可新增至IAM政策。

- `s3:GetObjectTagging` 為未進行版本控制的 Amazon S3 檔案新增。
- `s3:GetObjectVersionTagging` 為版本化的 Amazon S3 檔案新增。

解密檔案

AWS 儲存部落格有一個文章，說明如何使用 和 加密 [PGP和解密檔案、加密和解密檔案 AWS Transfer Family](#)。

在工作流程中使用PGP解密

Transfer Family 內建支援 Pretty Good Privacy (PGP) 解密。您可以在透過 SFTP、FTPS或上傳至 FTP Amazon Simple Storage Service (Amazon S3) 或 Amazon Elastic File System (Amazon) 的檔案上使用PGP解密EFS。

若要使用PGP解密功能，您必須建立並儲存用於檔案解密的PGP私有金鑰。然後，您的使用者可以在將檔案上傳至 Transfer Family 伺服器之前，使用對應的PGP加密金鑰來加密檔案。收到加密的檔案後，您可以在工作流程中解密這些檔案。如需詳細教學，請參閱[設定用於解密檔案的受管工作流程](#)。

在工作流程中使用PGP解密

1. 識別 Transfer Family 伺服器以託管您的工作流程，或建立新的工作流程。您需要有伺服器 ID，才能將PGP金鑰 AWS Secrets Manager 以正確的 secret 名稱存放在其中。
2. 將PGP索引鍵存放在所需的 secret 名稱 AWS Secrets Manager 下。如需詳細資訊，請參閱 [管理 PGP 金鑰](#)。工作流程可以根據 Secrets Manager 中的 secret 名稱，自動找到要用於解密的正確 PGP 金鑰。

Note

當您將 secret 存放在 Secrets Manager 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 金鑰對加密檔案。（如需支援的用戶端清單，請參閱 [支援的 PGP 用戶端](#)。）如果您使用命令列，請執行下列命令。若要使用此命令，`username@example.com` 請以您用來建立 PGP 金鑰對的電子郵件地址取代。`testfile.txt` 以您要加密的檔案名稱取代。

```
gpg -e -r username@example.com testfile.txt
```

4. 將加密的檔案上傳至 Transfer Family 伺服器。
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

解密步驟會解密上傳到 Amazon S3 或 Amazon EFS 作為工作流程一部分的加密檔案。如需設定解密的詳細資訊，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，您必須指定解密檔案的目的地。如果檔案已存在於目的地位置，您也必須選取是否覆寫現有檔案。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。

在您選擇步驟的解密檔案類型後，便會顯示設定參數頁面。填寫設定 PGP 解密參數區段的值。

可用的選項如下所示：

- 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 檔案系統作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金鑰字首。若要依使用者名稱參數化目的地金鑰字首，請在`${transfer:UserName}`目的地金鑰字首輸入。同樣地，若要依上傳日期參數化目的地金鑰字首，請輸入`${Transfer:UploadDate}`目的地金鑰字首。
- 如果您選擇 Amazon EFS，則必須提供目的地檔案系統和路徑。

Note

您在此處選擇的儲存選項必須與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，會收到錯誤。

- 覆寫現有檔案 – 如果您上傳檔案，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：
 - 如果選取覆寫現有檔案，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，則不會發生任何情況，工作流程處理也會停止。

Tip

如果在相同的檔案路徑上執行並行寫入，可能會在覆寫檔案時產生非預期的行為。

下列螢幕擷取畫面顯示您可以為解密檔案步驟選擇的選項範例。

Step 1
Choose step type

Step 2
Configure parameters

Step 3
Review and create

Configure parameters

Configure PGP decryption parameters

Store your PGP private key(s) and passphrase(s) in AWS Secrets Manager. [Learn more](#)

Refer to the [AWS Transfer Family pricing page](#) for pricing details.

Step name

decrypt step example

File location

Select the file location to use as an input for this step

☒ Apply on the file created from the previous step
Input file is selected from the previous step's output

☐ Apply on the original file
Originally uploaded file

Destination for decrypted files

Choose an S3 bucket or an EFS file system for storing decrypted files.

☒ Amazon S3
Store your decrypted files as Amazon S3 objects

☐ Amazon EFS
Store your decrypted files in an EFS file system

Destination bucket name

example-bucket

Destination key prefix

If you are decrypting files into a folder, specify / at the end of the prefix name. Use `${transfer:UserName}` or `${transfer:UploadDate}` to parametrize the destination prefix by username or upload date respectively.

`${transfer:UserName}`

☐ Overwrite existing
Overwrite if a file with the same file name already exists at the destination.

IAM 解密步驟的許可

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許可。

```
{
    "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

只有在您未選取覆寫現有 時，才需要此s3:ListBucket許可。此許可會檢查您的儲存貯體，以查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，只需寫入它即可。

如果您的 Amazon S3 檔案有標籤，您需要將一或兩個許可新增至IAM政策。

- s3:GetObjectTagging 為未進行版本控制的 Amazon S3 檔案新增。
- s3:GetObjectVersionTagging 為版本化的 Amazon S3 檔案新增。

標籤檔案

若要標記傳入檔案以進行進一步的下游處理，請使用標籤步驟。輸入您要指派給傳入檔案的標籤值。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` 和 `clean` 作為標籤索引鍵和值。

Configure tag parameters

Step name
tag scan

File location
Select the file location to use as an input for this step

☒ Tag the file created from previous step
Input file is selected from the previous step's output

☐ Tag the original source file
Originally uploaded file

Tags

Key	Value
scan_outcome	clean

Remove tag

Add tag

若要讓標籤步驟成功，請確定工作流程的執行角色包含下列許可。

```
{
    "Sid": "Tag",
    "Effect": "Allow",
    "Action": [
        "s3:PutObjectTagging",
        "s3:PutObjectVersionTagging"
    ],
    "Resource": [
        "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
    ]
}
```

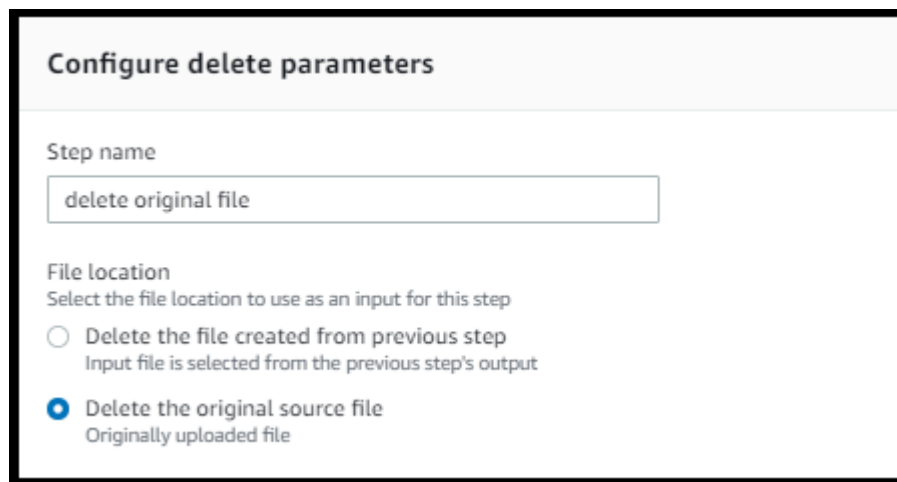
Note

如果您的工作流程包含在複製或解密步驟之前執行的標籤步驟，您需要將一或兩個許可新增至 IAM 政策。

- `s3:GetObjectTagging` 為未進行版本控制的 Amazon S3 檔案新增。
- `s3:GetObjectVersionTagging` 為版本化的 Amazon S3 檔案新增。

刪除檔案

若要從上一個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。



Configure delete parameters

Step name

delete original file

File location

Select the file location to use as an input for this step

☐ Delete the file created from previous step
Input file is selected from the previous step's output

☒ Delete the original source file
Originally uploaded file

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許可。

```
{
    "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 支援下列具名變數。

- 根據上傳檔案的使用者`${transfer:UserName}`，使用 將檔案複製或解密至目的地。
- 使用 `${transfer:UploadDate}` 以根據目前日期將檔案複製或解密至目的地位置。

範例標籤和刪除工作流程

下列範例說明一個工作流程，該工作流程會標記需要由下游應用程式處理的傳入檔案，例如資料分析平台。標記傳入檔案後，工作流程接著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. 在 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。
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。此描述會顯示在工作流程頁面上。
5. 新增第一個步驟（複製）。
 - a. 在額定步驟區段中，選擇新增步驟。
 - b. 選擇複製檔案，然後選擇下一個。
 - c. 輸入步驟名稱，然後選擇目的地儲存貯體和金鑰字首。

The screenshot shows the AWS Transfer Family console interface for configuring a new step. On the left, a sidebar lists three steps: 'Step 1 Choose step type', 'Step 2 Configure parameters' (which is the active step), and 'Step 3 Review and create'. The main area is titled 'Configure parameters' and contains a section 'Configure copy parameters'. This section includes three input fields: 'Step name' with the value 'copy-step-first-step', 'Destination bucket name' with a dropdown menu showing 'example-bucket', and 'Destination key prefix' with the value 'test/'. Below these fields is a checkbox labeled 'Overwrite existing' which is currently unchecked. A note for the 'Destination key prefix' field states: 'If you are copying files into a folder, specify / at the end of the prefix name. Use \${transfer:UserName} or \${transfer:UploadDate} to parametrize destination prefix by username or upload date respectively.'

- d. 選擇下一個，然後檢閱步驟的詳細資訊。
 - 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. 在額定步驟區段中，選擇新增步驟。
 - b. 選擇標籤檔案，然後選擇下一個。
 - c. 輸入步驟名稱。
 - d. 對於檔案位置，選取標記從上一個步驟建立的檔案。
 - e. 輸入Key (索引鍵) 和 Value (值)。

Configure tag parameters

Step name
tag scan

File location
Select the file location to use as an input for this step

☒ Tag the file created from previous step
Input file is selected from the previous step's output

☐ Tag the original source file
Originally uploaded file

Tags

Key	Value
scan_outcome	clean

Remove tag

Add tag

- f. 選擇下一個，然後檢閱步驟的詳細資訊。
 - g. 選擇建立步驟以新增步驟並繼續。
7. 新增第三個步驟（刪除）。
- a. 在額定步驟區段中，選擇新增步驟。
 - b. 選擇刪除檔案，然後選擇下一個。

Configure delete parameters

Step name
delete original file

File location
Select the file location to use as an input for this step

☐ Delete the file created from previous step
Input file is selected from the previous step's output

☒ Delete the original source file
Originally uploaded file

- 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. 選擇下一個，然後檢閱步驟的詳細資訊。
 - f. 選擇建立步驟以新增步驟並繼續。
8. 檢閱工作流程組態，然後選擇建立工作流程。

CLI

範例標籤和移動工作流程

1. 將下列程式碼儲存至 檔案；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}"
    }
}
]

```

第一步會將上傳的檔案複製到新的 Amazon S3 位置。第二個步驟會將標籤（鍵值對）新增至複製到新位置的檔案（`previous.file`）。最後，第三個步驟會刪除原始檔案（`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

此步驟假設您已擁有 Transfer Family 伺服器，且您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 自帶檔案處理邏輯 AWS Lambda。到達檔案時，Transfer Family 伺服器會叫用包含自訂檔案處理邏輯的 Lambda 函數，例如加密檔案、掃描惡意軟體或檢查不正確的檔案類型。在下列範例中，目標 AWS Lambda 函數用於處理上一個步驟的輸出檔案。

Configure custom parameters

Step name
custom file processing step

File location
Select the file location to use as an input for this step

☒ Apply custom processing to the file created from previous step
Input file is selected from the previous step's output

☐ Apply custom processing to the original source file
Originally uploaded file

Target
am:aws:lambda:us-east-2:1234567... ▼

Timeout (seconds)
60

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](#)。例如事件（包括傳入 Lambda 的檔案位置），請參閱[檔案上傳 AWS Lambda 時傳送至的範例事件](#)。

使用自訂工作流程步驟時，您必須設定 Lambda 函數以呼叫 [SendWorkflowStepState](#) API 操作。會 [SendWorkflowStepState](#) 通知工作流程執行，該步驟已完成，並顯示成功或失敗狀態。

態。SendWorkflowStepState API 操作的狀態會根據 Lambda 函數的結果，叫用線性序列中的例外處理常式步驟或標稱步驟。

如果 Lambda 函數失敗或逾時，則步驟會失敗，您會在 CloudWatch 日誌StepErrored中看到。如果 Lambda 函數是標稱步驟的一部分，且函數回應SendWorkflowStepState為Status="FAILURE"或逾時，則流程會繼續進行例外處理常式步驟。在此情況下，工作流程不會繼續執行其餘（如果有的話）標稱步驟。如需詳細資訊，請參閱[工作流程的例外處理](#)。

呼叫 SendWorkflowStepState API 操作時，您必須傳送下列參數：

```
{
  "ExecutionId": "string",
  "Status": "string",
  "Token": "string",
  "WorkflowId": "string"
}
```

您可以從執行 Lambda ExecutionId函數時傳遞的輸入事件WorkflowId中擷取 Token、和（範例如下列各節所示）。Status 值可以是 SUCCESS或 FAILURE。

若要能夠從 Lambda 函數呼叫 SendWorkflowStepStateAPI操作，您必須使用[推出 Managed Workflows](#) 後發佈的 AWS SDK版本。

連續使用多個 Lambda 函數

當您依序使用多個自訂步驟時，檔案位置選項的運作方式會與僅使用單一自訂步驟時不同。Transfer Family 不支援將 Lambda 處理的檔案轉傳回做為下一個步驟的輸入。因此，如果您有多個自訂步驟都設定為使用 previous.file選項，則它們都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定義的步驟（標籤、複製、解密或刪除），則此previous.file設定的運作方式也會有所不同。如果預先定義的步驟設定為使用previous.file設定，預先定義的步驟會使用與自訂步驟相同的輸入檔案。來自自訂步驟的已處理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 作為儲存體，且您的工作流程包含對原始上傳的檔案執行動作的自訂步驟，則後續步驟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考來自自訂步驟輸出的更新檔案。

例如，假設您在工作流程中有下列三個步驟。

- 步驟 1 – 上傳名為 的檔案 `example-file.txt`。
- 步驟 2 - 叫用 Lambda 函數，該函數 `example-file.txt` 會以某種方式變更。
- 步驟 3 – 嘗試對更新版本的 執行進一步處理 `example-file.txt`。

如果您將步驟 3 `sourceFileLocation` 的設定為 `${original.file}`，步驟 3 會使用從伺服器將檔案上傳到步驟 1 中儲存的原始檔案位置。如果您使用 `${previous.file}` 作為步驟 3，步驟 3 會重複使用步驟 2 作為輸入的檔案位置。

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"
  },
}
```

發生此錯誤是因為自訂步驟修改的實體標籤（ETag），`example-file.txt` 使其與原始檔案不相符。

Note

如果您使用 Amazon，則不會發生此行為，EFS 因為 Amazon EFS 不會使用實體標籤來識別檔案。

檔案上傳 AWS Lambda 時傳送至 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，其中網域是使用 Amazon S3 設定。另一個範例使用 Transfer Family 伺服器，其中網域使用 Amazon EFS。

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": "MTg0N2Y3N2UtNWl5Ny00ZmZlLTk5YTgtZTU3YzViYjllNmZm",
  "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 函數會擷取有關執行狀態的資訊，然後呼叫 [SendWorkflowStepState](#) API 操作，將狀態傳回至步驟的工作流程：SUCCESS 或 FAILURE。在函數呼叫 [SendWorkflowStepState](#) API 操作之前，您可以設定 Lambda 根據您的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)
    }
```

IAM 自訂步驟的許可

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許可。

```
{
    "Sid": "Custom",
    "Effect": "Allow",
    "Action": [
        "lambda:InvokeFunction"
    ],
    "Resource": [
        "arn:aws:lambda:region:account-id:function:function-name"
    ]
}
```

IAM 工作流程的政策

當您將工作流程新增至伺服器時，必須選取執行角色。伺服器在執行工作流程時使用此角色。如果角色沒有適當的許可，AWS Transfer Family 則無法執行工作流程。

本節描述一組可用於執行工作流程的 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 檔案有標籤，您需要將一或兩個許可新增至IAM政策。

- `s3:GetObjectTagging` 為未進行版本控制的 Amazon S3 檔案新增。
- `s3:GetObjectVersionTagging` 為版本化的 Amazon S3 檔案新增。

為您的工作流程建立執行角色

1. 建立新的IAM角色，並將 AWS 受管政策 `AWSTransferFullAccess` 新增至角色。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. 建立具有下列許可的另一個政策，並將其連接至您的角色。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. 當您將工作流程新增至伺服器時，請儲存此角色並指定為執行角色。

Note

當您建構IAM角色時，AWS 建議您盡可能限制工作流程對資源的存取。

工作流程信任關係

工作流程執行角色也需要與 建立信任關係 `transfer.amazonaws.com`。若要為 建立信任關係 AWS Transfer Family，請參閱 [建立信任關係](#)。

當您建立信任關係時，您也可以採取步驟來避免混淆代理問題。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

如果您有包含標記、複製和解密步驟的工作流程，您可以使用下列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/*"
    }
]
}

```

執行角色範例：執行函數和刪除

在此範例中，您有一個叫用 AWS Lambda 函數的工作流程。如果工作流程刪除上傳的檔案，且具有例外處理常式步驟來對上一個步驟中失敗的工作流程執行採取動作，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"
    ]
  }
]
}

```

工作流程的例外處理

如果在工作流程執行期間發生任何錯誤，則會執行您指定的例外處理步驟。您可以指定工作流程的錯誤處理步驟，方式與指定工作流程的標稱步驟相同。例如，假設您已以名義步驟設定自訂處理，以驗證傳入的檔案。如果檔案驗證失敗，例外處理步驟可以傳送電子郵件給管理員。

下列範例工作流程包含兩個步驟：

- 檢查上傳檔案是否為 CSV 格式的標稱步驟
- 例外處理步驟，會在上傳的檔案不是 CSV 格式且名義步驟失敗時傳送電子郵件

若要啟動例外處理步驟，標稱步驟中的 AWS Lambda 函數必須以 `回應Status="FAILURE"`。如需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”](#)。

w-1234567890abcdef0 Delete			
Description Workflow description Check for CSV files			
Nominal steps (1) Info			
Number	Description	Type	Configuration
1	is-CSV	CUSTOM	Details
Exception handlers (1) Info			
Number	Description	Type	Configuration
1	send-email	CUSTOM	Details

監控工作流程執行

Amazon 會 AWS 雲端 即時 CloudWatch 監控您的 AWS 資源和您在 中執行的應用程式。您可以使用 Amazon CloudWatch 來收集和追蹤指標，這些指標是您可以針對工作流程測量的變數。您可以使用 Amazon 檢視工作流程指標和合併日誌 CloudWatch。

CloudWatch 記錄工作流程

CloudWatch 提供工作流程進度和結果的合併稽核和記錄。

檢視工作流程的 Amazon CloudWatch 日誌

1. 在 開啟 Amazon CloudWatch 主控台 <https://console.aws.amazon.com/cloudwatch/>。
2. 在左側導覽窗格中，選擇日誌，然後選擇日誌群組。
3. 在日誌群組頁面上的導覽列上，為您的 AWS Transfer Family 伺服器選擇正確的區域。
4. 選擇與伺服器對應的日誌群組。

例如，如果您的伺服器 ID 為 s-1234567890abcdef0，您的日誌群組為 /aws/transfer/s-1234567890abcdef0。

5. 在伺服器的日誌群組詳細資訊頁面上，會顯示最新的日誌串流。您要探索的使用者有兩個日誌串流：

- 每個 Secure Shell (SSH) 檔案傳輸通訊協定 (SFTP) 工作階段各一個。
- 一個用於正在為伺服器執行的工作流程。工作流程的日誌串流格式為 *username.workflowID.uniqueStreamSuffix*。

例如，如果您的使用者是 mary-major，您有下列日誌串流：

```
mary-major-east.1234567890abcdef0  
mary.w-abcdef01234567890.021345abcdef6789
```

Note

此範例中列出的 16 位數英數字元識別碼為虛構。您在 Amazon 中看到的值 CloudWatch 不同。

的日誌事件頁面mary-major-usa-east.1234567890abcdef0會顯示每個使用者工作階段的詳細資訊，而mary.w-abcdef01234567890.021345abcdef6789日誌串流包含工作流程的詳細資訊。

以下是 的日誌串流範例mary.w-abcdef01234567890.021345abcdef6789，以包含複製步驟的工作流程（w-abcdef01234567890）為基礎。

```
{
  "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 為工作流程提供數個指標。您可以檢視上一分鐘有多少工作流程執行開始、成功完成和失敗的指標。Transfer Family 的所有 CloudWatch 指標都說明於 [中 使用 Transfer Family 的 CloudWatch 指標](#)。

從範本建立工作流程

您可以部署堆疊 AWS CloudFormation，以從範本建立工作流程和伺服器。此程序包含一個範例，您可以用來快速部署工作流程。

建立建立 AWS Transfer Family 工作流程和伺服器的 AWS CloudFormation 堆疊

1. 在 <https://console.aws.amazon.com/cloudformation> 開啟 AWS CloudFormation 主控台。
2. 將下列程式碼儲存至 檔案。

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"
        }
    ]
}

```

```
}
}
}
}
}
```

- 將下列項目取代為您的實際值。
 - Replace (取代) *workflow-execution-role-arn* 使用 ARN 做為實際工作流程執行角色。例如 `arn:aws:transfer:us-east-2:111122223333:workflow/w-1234567890abcdef0`
 - `arn:aws:lambda:region:account-id:function:function-name` 將取代為 Lambda 函數ARN的。例如：`arn:aws:lambda:us-east-2:123456789012:function:example-lambda-idp`。
- 請遵循 AWS CloudFormation 使用者指南 中的 AWS CloudFormation 從現有範本部署[堆疊](#)的指示。

部署堆疊之後，您可以在 CloudFormation 主控台的輸出索引標籤中檢視其詳細資訊。範本會 AWS Transfer Family SFTP 建立新的伺服器，以使用者服務受管使用者，以及新的工作流程，並將工作流程與新伺服器建立關聯。

從 Transfer Family 伺服器移除工作流程

如果您已將工作流程與 Transfer Family 伺服器建立關聯，且現在想要移除該關聯，您可以使用主控台或以程式設計方式進行。

Console

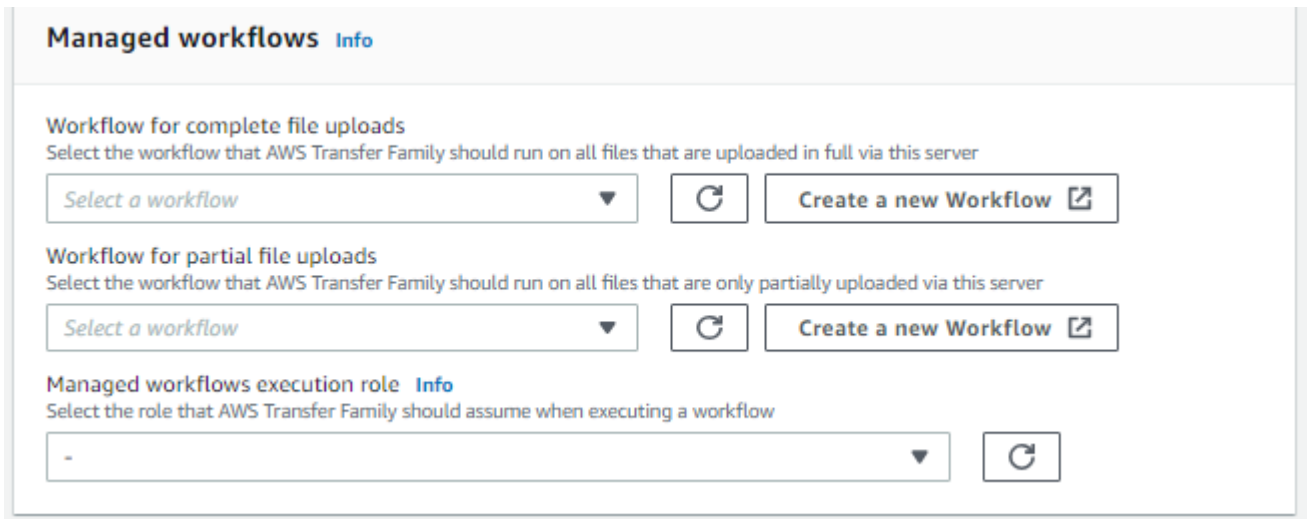
從 Transfer Family 伺服器移除工作流程

1. 在開啟 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 欄中選擇伺服器的識別符。
4. 在伺服器的詳細資訊頁面上，向下捲動至其他詳細資訊區段，然後選擇編輯。
5. 在編輯其他詳細資訊頁面的受管工作流程區段中，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（ - ），以完成檔案上傳。

- 如果尚未清除，請從部分檔案上傳的工作流程清單中選擇破折號 (-)。
- 從受管工作流程執行角色 的角色清單中選取破折號 (-)。

如果您沒有看到破折號，請向上捲動直到您看到破折號，因為它是每個選單中的第一個值。

畫面應如下所示。



The screenshot shows the 'Managed workflows' section in the AWS Transfer Family console. It contains three main sections:

- Workflow for complete file uploads**: A dropdown menu with 'Select a workflow' and a refresh button. A 'Create a new Workflow' button with an external link icon is also present.
- Workflow for partial file uploads**: A dropdown menu with 'Select a workflow' and a refresh button. A 'Create a new Workflow' button with an external link icon is also present.
- Managed workflows execution role**: A dropdown menu with '-' selected and a refresh button.

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 `OnPartialUpload` 參數提供空引數。

從 中 AWS CLI，執行下列命令：

```
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`，則命令如下：

```
aws transfer update-server --server-id s-01234567890abcdef --workflow-details  
'{"OnPartialUpload":[],"OnUpload":[]}'
```

受管工作流程的限制

限制

下列限制目前適用於的上傳後處理工作流程 AWS Transfer Family。

- 不支援跨帳戶和跨區域 AWS Lambda 函數。不過，只要 AWS Identity and Access Management (IAM) 政策已正確設定，您就可以跨帳戶複製。
- 對於所有工作流程步驟，工作流程存取的任何 Amazon S3 儲存貯體都必須與工作流程本身位於相同區域。
- 對於解密步驟，解密目的地必須符合區域和備份存放區的來源（例如，如果要解密的檔案存放在 Amazon S3 中，則指定的目的地也必須在 Amazon S3 中）。
- 僅支援非同步自訂步驟。
- 自訂步驟逾時是近似值。也就是說，逾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，則工作流程不會知道延遲。
- 如果您超過限流限制，Transfer Family 不會將工作流程操作新增至佇列。
- 大小為 0 的檔案不會啟動工作流程。大小大於 0 的檔案會啟動相關聯的工作流程。

限制

此外，下列功能限制適用於 Transfer Family 的工作流程：

- 每個帳戶每個區域的工作流程數量限制為 10 個。
- 自訂步驟的逾時上限為 30 分鐘。
- 工作流程中的步驟數目上限為 8。
- 每個工作流程的標籤數量上限為 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存放 3 個PGP私有金鑰。
- 解密檔案的大小上限為 10 GB。
- 我們會使用爆量容量為 100 且補充率為 1 的[權杖儲存貯體](#)系統來調節新的執行率。
- 每當您從伺服器移除工作流程並將其取代為新的工作流程，或更新伺服器組態（這會影響工作流程的執行角色）時，您必須等待約 10 分鐘，才能執行新的工作流程。Transfer Family 伺服器快取工作流程詳細資訊，伺服器重新整理其快取需要 10 分鐘。

此外，您必須登出任何作用中SFTP工作階段，然後在 10 分鐘等待期後重新登入，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 之伺服器主機金鑰的資訊。

主題

- [檢視伺服器清單](#)
- [刪除伺服器](#)
- [檢視 SFTP、FTPS 和 FTP 伺服器詳細資訊](#)
- [檢視 AS2 伺服器詳細資訊](#)
- [編輯伺服器詳細資訊](#)
- [管理 SFTP 已啟用 之伺服器的主機金鑰](#)
- [監控主控台中的用量](#)

檢視伺服器清單

在 AWS Transfer Family 主控台上，您可以找到位於所選 AWS 區域中的所有伺服器清單。

尋找存在於 AWS 區域中的伺服器清單

- 在 開啟 AWS Transfer Family 主控台 <https://console.aws.amazon.com/transfer/>。

如果您在目前 AWS 區域中有一或多個伺服器，主控台會開啟以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區域。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、FTPS 和 FTP 伺服器詳細資訊](#)。

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

系統會針對啟用存取端點的每個通訊協定向您收費，直到您刪除伺服器為止。

⚠ Warning

刪除伺服器會導致刪除其所有使用者。使用伺服器存取的儲存貯體中的資料不會遭到刪除，且具有這些 Amazon S3 儲存貯體權限 AWS 的使用者仍可存取。

Console

使用主控台刪除伺服器

1. 在開啟 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. 選取您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，輸入字詞 **delete**，然後選擇刪除以確認您想要刪除伺服器。

伺服器會從伺服器頁面中刪除，您將不再收到該伺服器的費用。

AWS CLI

使用 刪除伺服器 CLI

1. (選用) 執行下列命令，以檢視您要永久刪除之伺服器的詳細資訊。

```
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。

2. 執行下列命令來刪除伺服器。

```
aws transfer delete-server --server-id your-server-id
```

如果成功，命令會刪除伺服器，而不會傳回任何資訊。

檢視 SFTP、FTPS和 FTP 伺服器詳細資訊

您可以找到個別 AWS Transfer Family 伺服器的詳細資訊和屬性清單。伺服器屬性包括通訊協定、身分提供者、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. 在開啟 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 欄中選擇識別符，以查看伺服器詳細資訊頁面，如下所示。

您可以選擇編輯來變更此頁面上的伺服器屬性。如需有關編輯伺服器詳細資訊的詳細資訊，請參閱 [編輯伺服器詳細資訊](#)。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](#)。

Protocols Edit	Identity provider Edit
Protocols over which clients can connect to your server's endpoint • SFTP	Identity provider type Info Custom - AWS Lambda AWS Lambda function test-UserAuthenticationLambda 

Note

截至 2022 年 9 月，伺服器主機金鑰描述和日期匯入值為新值。引入這些值是為了支援多個主機金鑰功能。此功能需要遷移在引入多個主機金鑰之前正在使用的任何單一主機金鑰。

已遷移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，您為已遷移主機金鑰看到的日期會對應至您在伺服器主機金鑰遷移之前以任何方式修改伺服器的日期。

遷移的唯一金鑰是您最舊或唯一的伺服器主機金鑰。任何其他金鑰都有其從您匯入時起算的實際日期。此外，遷移的金鑰具有描述，可讓您輕鬆識別已遷移的金鑰。

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。

Additional details Edit

Log group /aws/transfer/s-	Domain Amazon S3	Login display banner View the display message
Logging role Info AWSTransferLoggingAccess	Workflow for complete uploads w-	SetStat option Ignore
Server host key Info SHA256:	Workflow for partial uploads -	TLS session resumption -
Security Policy Info TransferSecurityPolicy-2020-06	Managed workflows execution role transfer-workflows-	Passive IP -

檢視AS2伺服器詳細資訊

您可以找到個別 AWS Transfer Family 伺服器的詳細資訊和屬性清單。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非同步輸出 IP MDN 地址。

Protocols Edit

Protocols over which clients can connect to your server's endpoint

- AS2

Identity provider Edit

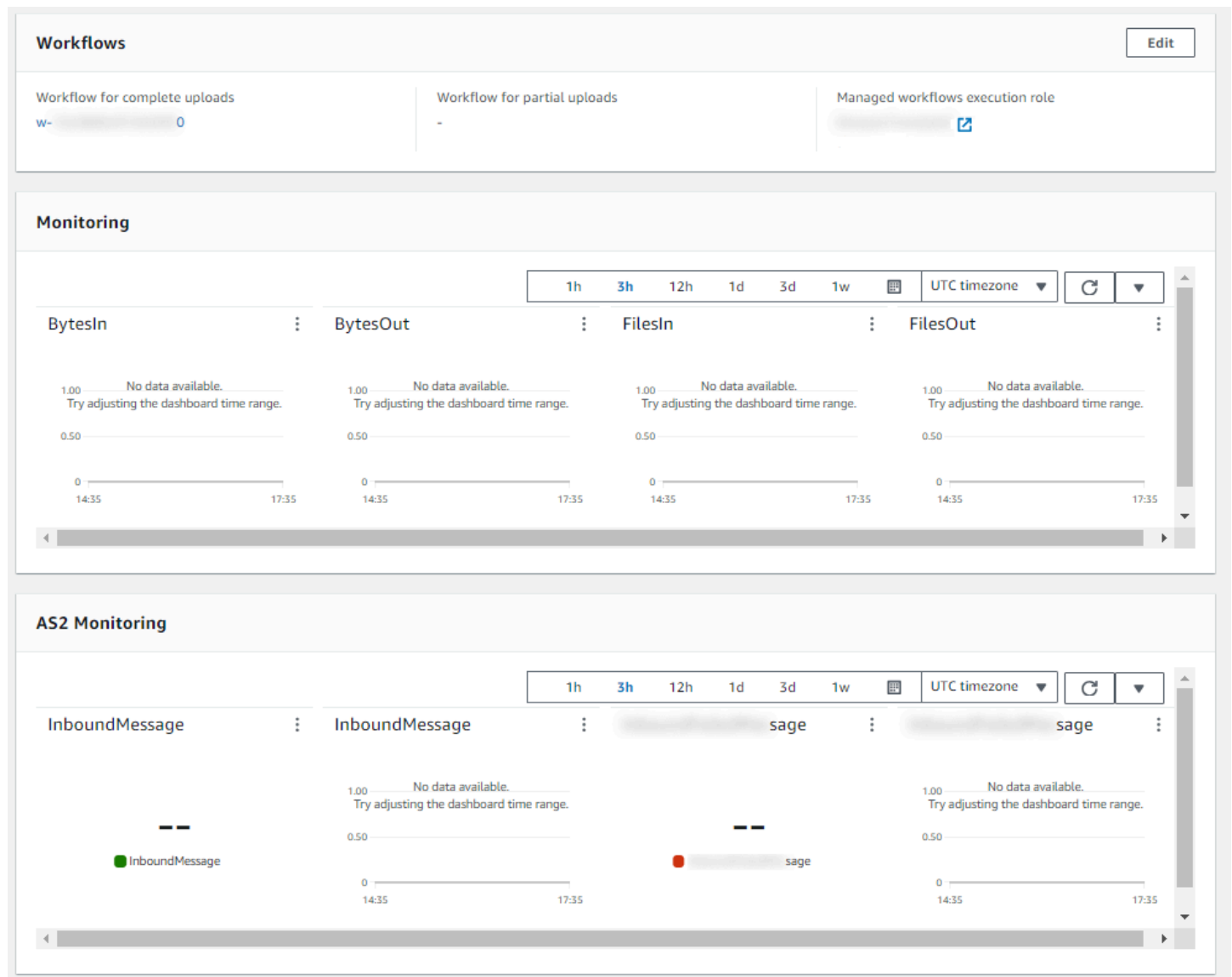
AS2 Auth
Basic authentication is not supported for AS2. Access can be controlled through VPC security groups.

每個AS2伺服器都會指派三個靜態 IP 地址。使用這些 IP 地址透過 MDNs向交易合作夥伴傳送非同步AS2。

AS2 asynchronous MDN egress IP details

Below are the service managed static IP addresses used for sending your asynchronous MDNs to trading partners over AS2

AS2 伺服器詳細資訊頁面的底部包含任何連接工作流程的詳細資訊，以及監控和標記資訊。



編輯伺服器詳細資訊

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](#)
- [編輯您的記錄組態](#)
- [編輯安全政策](#)

- [變更伺服器的受管工作流程](#)
- [變更伺服器的顯示橫幅](#)
- [讓伺服器處於線上或離線狀態](#)

編輯伺服器的組態

1. 在開啟 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 欄中選擇識別符，以查看伺服器詳細資訊頁面，如下所示。

您可以選擇編輯，變更此頁面上的伺服器屬性：

- 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](#)。
- 若要新增協議，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SFTP已啟用之伺服器的主機金鑰](#)。
- 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 [編輯您的記錄組態](#)。
 - 若要變更安全政策，請參閱 [編輯安全政策](#)。
 - 若要變更伺服器主機金鑰，請參閱 [管理SFTP已啟用之伺服器的主機金鑰](#)。
 - 若要變更伺服器的受管工作流程，請參閱 [變更伺服器的受管工作流程](#)。
 - 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](#)。
- 在其他組態下，您可以編輯下列資訊：

- **SetStat 選項**：啟用此選項，以忽略用戶端嘗試在您上傳至 Amazon S3 儲存貯體的檔案 SETSTAT 上使用時所產生的錯誤。如需其他詳細資訊，請參閱 [ProtocolDetails](#) 主題中的 SetStatOption 文件。
- **TLS 工作階段恢復**：提供機制，在 FTPS 工作階段的控制和資料連線之間繼續或共用交涉的秘密金鑰。如需其他詳細資訊，請參閱 [ProtocolDetails](#) 主題中的 TlsSessionResumptionMode 文件。
- **被動 IP**：表示 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。如需其他詳細資訊，請參閱 [ProtocolDetails](#) 主題中的 PassiveIp 文件。
- 若要啟動或停止伺服器，請參閱 [讓伺服器處於線上或離線狀態](#)。
- 若要刪除伺服器，請參閱 [刪除伺服器](#)。
- 若要編輯使用者屬性，請參閱 [管理存取控制](#)。

Protocols Edit	Identity provider Edit
Protocols over which clients can connect to your server's endpoint • SFTP	Identity provider type Info Custom - AWS Lambda AWS Lambda function test-UserAuthenticationLambda ↗

Note

截至 2022 年 9 月，伺服器主機金鑰描述和日期匯入值是新的。引入這些值是為了支援多個主機金鑰功能。此功能需要遷移在引入多個主機金鑰之前正在使用的任何單一主機金鑰。

已遷移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，您為已遷移主機金鑰看到的日期會對應至您在伺服器主機金鑰遷移之前以任何方式修改伺服器的日期。

遷移的唯一金鑰是您最舊或唯一的伺服器主機金鑰。任何其他金鑰都有從您匯入時開始的實際日期。此外，遷移的金鑰具有描述，可讓您輕鬆將其識別為已遷移。

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。

Additional details

Edit

Log group /aws/transfer/s-	Domain Amazon S3	Login display banner View the display message
Logging role Info AWSTransferLoggingAccess	Workflow for complete uploads w-	SetStat option Ignore
Server host key Info SHA256:	Workflow for partial uploads -	TLS session resumption -
Security Policy Info TransferSecurityPolicy-2020-06	Managed workflows execution role transfer-workflows	Passive IP -

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接至伺服器的端點。

編輯通訊協定

- 在伺服器詳細資訊頁面上，選擇通訊協定 旁的編輯。
- 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）– 檔案傳輸 SSH

如需的詳細資訊SFTP，請參閱 [建立已啟用 SFTP的伺服器](#)。

- 檔案傳輸通訊協定安全（FTPS）– 使用TLS加密進行檔案傳輸

如需的詳細資訊FTP，請參閱 [建立已啟用 FTPS的伺服器](#)。

- 檔案傳輸通訊協定（FTP）– 未加密的檔案傳輸

如需的詳細資訊FTPS，請參閱 [建立已啟用 FTP的伺服器](#)。

Note

如果您只為 啟用現有伺服器SFTP，且您想要新增 FTPS 和 FTP，則必須確保擁有與 和 相容的適當身分提供者FTPS和端點類型設定FTP。

Edit protocols

Select the protocols you want to enable [Info](#)

Choose one or more file transfer protocols over which clients can connect to your server's endpoint

- ☐ SFTP (SSH File Transfer Protocol) - file transfer over Secure Shell
- ☐ AS2 (Applicability Statement 2) - messaging protocol for exchanging business-to-business data [Info](#)
- ☐ FTPS (File Transfer Protocol Secure) - file transfer protocol with TLS encryption
- ☐ FTP (File Transfer Protocol) - unencrypted file transfer protocol

[Cancel](#) [Save](#)

如果您選擇 FTPS，您必須選擇儲存在 AWS Certificate Manager（ACM）中的憑證，當用戶端透過 連線到伺服器時，該憑證將用於識別您的伺服器FTPS。

若要請求新的公有憑證，請參閱 AWS Certificate Manager 使用者指南 中的[請求公有憑證](#)。

若要將現有憑證匯入 ACM，請參閱 使用者指南 中的[將憑證匯入 ACM](#)。AWS Certificate Manager

若要FTPS透過私有 IP 地址請求私有憑證，請參閱 AWS Certificate Manager 使用者指南 中的[請求私有憑證](#)。

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

憑證必須是指定 FQDN 或 IP 地址的有效 SSL/TLS X.509 第 3 版憑證，以及發行者的相關資訊。

Choose protocols

Select the protocols you want to enable [Info](#)

Choose one or more file transfer protocols over which clients can connect to your server's endpoint

- ☐ SFTP (SSH File Transfer Protocol) - file transfer over Secure Shell
- ☐ AS2 (Applicability Statement 2) - messaging protocol for exchanging business-to-business data [Info](#)
- ☒ FTPS (File Transfer Protocol Secure) - file transfer protocol with TLS encryption
- ☐ FTP (File Transfer Protocol) - unencrypted file transfer protocol

AWS Certificate Manager (ACM) certificate [Info](#)

Server certificate

Choose a certificate stored in ACM which will be used to identify your server when clients connect to it over FTPS

[↕](#) [↻](#)

[Cancel](#) [Next](#)

3. 選擇 Save (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，對於自訂身分提供者，您可以變更某些設定，這取決於您是使用 Lambda 函數還是 API Gateway。無論哪種情況，如果您的伺服器使用 SFTP 通訊協定，都可以編輯身分驗證方法。

- 如果您使用 Lambda 作為身分提供者，您可以變更基礎 Lambda 函數。

Transfer Family > Servers > s- [redacted] > Edit identity provider

Edit identity provider

Identity Provider for SFTP, FTPS, or FTP

Identity provider type
An identity provider manages user access for authentication and authorization

☐ **Service managed**
Create and manage users within the service

☐ **AWS Directory Service** [Info](#)
Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☐ **Custom Identity Provider** [Info](#)
Manage users by integrating an identity provider of your choice

☐ **Use AWS Lambda to connect your identity provider** [Info](#)
Invoke an AWS Lambda function to call your identity provider's API for user authentication and authorization

☐ **Use Amazon API Gateway to connect your identity provider** [Info](#)
Use a RESTful API method to call your identity provider's API for user authentication and authorization

AWS Lambda function

▼

Authentication methods
Choose which authentication methods are required for users to connect to your server

☒ Password OR public key

☐ Password ONLY

☐ Public Key ONLY

☐ Password AND public key

 Either a valid password or valid private key will be required during user authentication

Cancel

Save

- 如果您使用API閘道作為身分提供者，則可以更新閘道URL或調用角色，或兩者。

Transfer Family > Servers > s-[redacted] > Edit identity provider

Edit identity provider

Identity Provider for SFTP, FTPS, or FTP

Identity provider type
An identity provider manages user access for authentication and authorization

☐ **Service managed**
Create and manage users within the service

☐ **AWS Directory Service** [Info](#)
Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☐ **Custom Identity Provider** [Info](#)
Manage users by integrating an identity provider of your choice

☐ **Use AWS Lambda to connect your identity provider** [Info](#)
Invoke an AWS Lambda function to call your identity provider's API for user authentication and authorization

☒ **Use Amazon API Gateway to connect your identity provider** [Info](#)
Use a RESTful API method to call your identity provider's API for user authentication and authorization

Provide an Amazon API Gateway URL

Invocation role
IAM role for the service to invoke your Amazon API Gateway URL

Authentication methods
Choose which authentication methods are required for users to connect to your server

☒ Password OR public key

☐ Password ONLY

☐ Public Key ONLY

☐ Password AND public key

Either a valid password or valid private key will be required during user authentication

Cancel

Save

編輯伺服器端點

在 AWS Transfer Family 主控台上，您可以修改伺服器端點類型和自訂主機名稱。

編輯伺服器端點詳細資訊

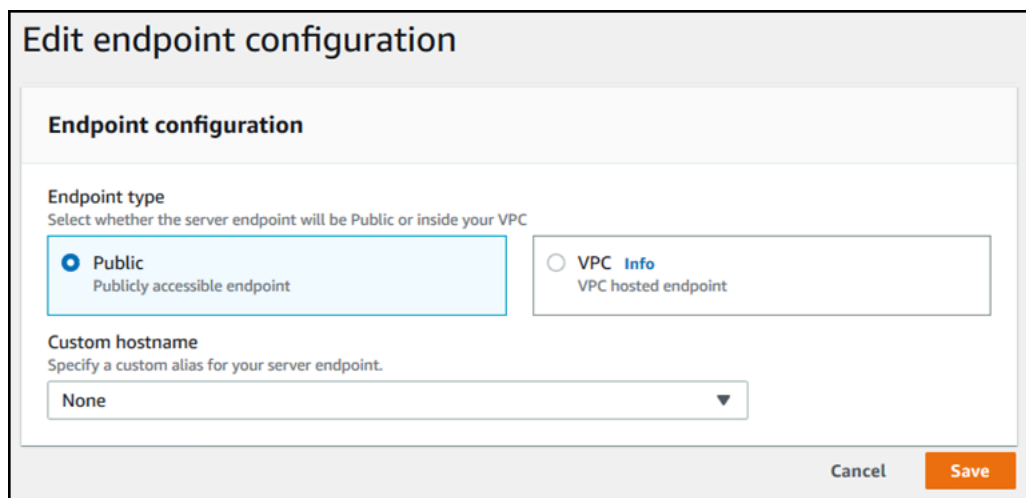
1. 在伺服器詳細資訊頁面上，選擇端點詳細資訊 旁的編輯。
2. 在編輯端點組態頁面上，針對端點類型，選擇下列其中一項：
 - 公開 – 此選項可讓您的伺服器透過網際網路存取。
 - VPC – 此選項可讓您的伺服器在虛擬私有雲端（VPC）中存取。如需的相關資訊VPC，請參閱 [在虛擬私有雲端中建立伺服器](#)。
3. 針對自訂主機名稱，選擇下列其中一項：

您可以取得 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 Route 53 DNS 別名 – 若要使用 Route DNS 53 中自動為您建立的別名，請選擇此選項。
- 其他 DNS – 若要使用已在外部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的名稱，DNS以及服務可以解決DNS的名稱。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。若要了解如何 AWS Transfer Family 使用 Route 53 將流量從自訂網域路由至伺服器端點，請參閱 [使用自訂主機名稱](#)。



4. 選擇 Save (儲存)。您會返回伺服器詳細資訊頁面。

編輯您的記錄組態

在 AWS Transfer Family 主控台上，您可以變更記錄組態。

Note

如果 Transfer Family 在您建立伺服器時為您建立 CloudWatch 記錄IAM角色，則該IAM角色稱為 AWSTransferLoggingAccess。您可以將其用於所有 Transfer Family 伺服器。

編輯您的記錄組態

1. 在伺服器詳細資訊頁面上，選擇其他詳細資訊旁的編輯。
2. 根據您的組態，選擇記錄角色、結構化JSON記錄或兩者。如需詳細資訊，請參閱[更新伺服器的記錄](#)。

編輯安全政策

此程序說明如何使用 AWS Transfer Family 主控台或 變更 Transfer Family 伺服器的安全政策 AWS CLI。

Note

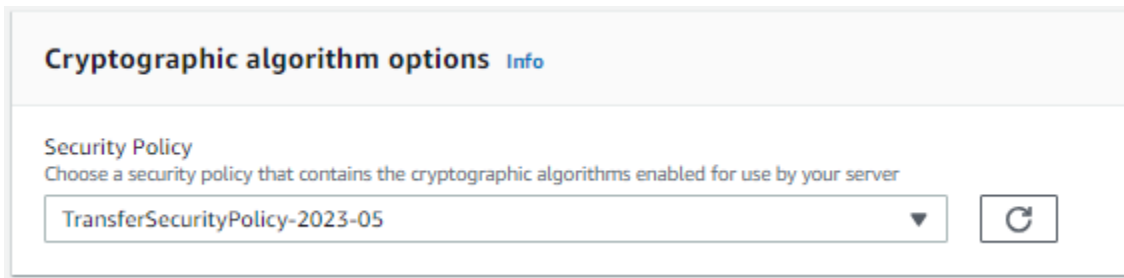
如果您的端點FIPS已啟用，則您無法將FIPS安全政策變更為非FIPS安全政策。

Console

使用主控台編輯安全政策

1. 在伺服器詳細資訊頁面上，選擇其他詳細資訊旁的編輯。
2. 在密碼編譯演算法選項區段中，選擇包含伺服器啟用之密碼編譯演算法的安全政策。

如需關於安全政策的詳細資訊，請參閱[的安全政策 AWS Transfer Family](#)。



Cryptographic algorithm options [Info](#)

Security Policy
Choose a security policy that contains the cryptographic algorithms enabled for use by your server

TransferSecurityPolicy-2023-05 

3. 選擇 Save (儲存)。

您會返回伺服器詳細資訊頁面，您可以在其中看到更新的安全政策。

AWS CLI

使用 編輯安全政策 CLI

1. 執行下列命令，以檢視連接到您伺服器的目前安全政策。

```
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，伺服器的安全政策為 TransferSecurityPolicy-2018-11。

2. 請務必將安全政策的確切名稱提供給 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

可用的安全政策名稱會列在 [中的安全政策 AWS Transfer Family](#)。

如果成功，命令會傳回下列程式碼，並更新伺服器的安全政策。

```
{
```

```
"ServerId": "your-server-id"
}
```

變更伺服器的受管工作流程

在 AWS Transfer Family 主控台上，您可以變更與伺服器相關聯的受管工作流程。

若要變更受管工作流程

1. 在伺服器詳細資訊頁面上，選擇其他詳細資訊旁的編輯。
2. 在編輯其他詳細資訊頁面的受管工作流程區段中，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，請選擇建立新工作流程來建立工作流程。

- 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擔任的角色。如需詳細資訊，請參閱[IAM 工作流程的政策](#)。選擇 Save (儲存)。

The screenshot shows the 'Managed workflows' section in the AWS Transfer Family console. It contains three main sections:

- Workflow for complete file uploads**: A dropdown menu with a placeholder 'w-' and a refresh button. A 'Create a new Workflow' button with an external link icon is also present.
- Workflow for partial file uploads**: A dropdown menu with a placeholder 'w-' and a refresh button. A 'Create a new Workflow' button with an external link icon is also present.
- Managed workflows execution role**: A dropdown menu with a placeholder and a refresh button.

3. 選擇 Save (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。

若要變更顯示橫幅

1. 在伺服器詳細資訊頁面上，選擇其他詳細資訊旁的編輯。
2. 在編輯其他詳細資訊頁面的顯示橫幅區段中，輸入可用顯示橫幅的文字。
3. 選擇 Save (儲存)。您會返回伺服器詳細資訊頁面。

讓伺服器處於線上或離線狀態

在 AWS Transfer Family 主控台上，您可以讓伺服器連線或離線。

讓伺服器上線

1. 在開啟 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)。

伺服器從離線切換到線上可能需要幾分鐘的時間。

Note

當您停止伺服器使其離線時，您目前仍在為該伺服器累積服務費用。若要消除額外的伺服器型費用，請刪除該伺服器。

讓伺服器離線

1. 在開啟 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)。

當伺服器啟動或關閉時，伺服器無法用於檔案操作。主控台不會顯示啟動中和停止中狀態。

如果您找到錯誤條件START_FAILED或 STOP_FAILED，請聯絡 AWS 支援 以協助解決您的問題。

管理SFTP已啟用 之伺服器的主機金鑰

Important

如果您不打算將現有使用者從已啟用 SFTP的現有伺服器遷移至已啟用 SFTP的新版伺服器，請忽略本節。

意外變更伺服器的主機金鑰可能造成破壞。根據您的SFTP用戶端設定方式，它可能會立即失敗，並顯示沒有受信任主機金鑰存在的訊息，或出現威脅的提示。如果有用於自動化連線的指令碼，它們很可能也會失敗。

根據預設，會為您的SFTP啟用的伺服器 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。只有在您計劃將現有使用者從已啟用 SFTP的現有伺服器移至SFTP已啟用的新伺服器時，才能執行此操作。

為了防止再次提示您的使用者驗證SFTP已啟用 之伺服器的真實性，請將內部部署伺服器的主機金鑰匯入SFTP已啟用的伺服器。這樣做也會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 主控台可讓您指定和新增所有伺服器的伺服器主機金鑰，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](#)
- [輪換伺服器主機金鑰](#)
- [其他伺服器主機金鑰資訊](#)

新增其他伺服器主機金鑰

在 AWS Transfer Family 主控台上，您可以新增其他伺服器主機金鑰。新增其他不同格式的主機金鑰對於識別用戶端連線到伺服器以及改善您的安全設定檔很有用。例如，如果您的原始金鑰是RSA金鑰，您可以新增其他ECDSA金鑰。

Note

SFTP 用戶端會使用其擁有的第一個公有金鑰進行連線，該公有金鑰可以符合其中一個作用中伺服器金鑰。

若要新增其他伺服器主機金鑰

1. 在 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SFTP通訊協定的伺服器。
3. 在伺服器詳細資訊頁面上，向下捲動至伺服器主機金鑰區段。

Server host keys (1)						Actions	Add host key
☐	Host key ID	Fingerprint	Description	Key type	Date imported		
☐	hostkey-	SHA256: [fingerprint]	ECDSA server host key	ecdsa-sha2-nistp256	2022-08-26		

4. 選擇新增主機金鑰。

隨即顯示新增伺服器主機金鑰頁面。

5. 在伺服器主機金鑰區段中，輸入 RSA、ECDSA或 ED25519 私有金鑰，用於在用戶端透過啟用SFTP的伺服器連線至伺服器時識別您的伺服器。

Note

當您建立伺服器主機金鑰時，請務必指定 `-N ""`（無密碼片語）。如需如何產生金鑰對的詳細資訊，在 [macOS、Linux 或 Unix 上建立SSH金鑰](#)，請參閱。

Server Host Key [Info](#)

Private key - *optional*

Upload an RSA, ECDSA, or ED25519 private key that will be used to identify your SFTP server when clients connect to it. Additional keys can be added once the server is created.

Enter an optional RSA, ECDSA, or ED25519 key

Description - *optional*

Add a description to differentiate between multiple private keys

Enter optional description

 You can ignore this section unless you are migrating users from an existing SFTP server.

6. (選用) 新增描述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)。您會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 操作並提供新的主機金鑰。如果您建立新的 SFTP 啟用的伺服器，您會在 [the section called “CreateServer”](#) API 操作中提供主機金鑰作為參數。您也可以使用 AWS CLI 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 SFTP 已啟用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 AWS Transfer Family 主控台上，您可以刪除伺服器主機金鑰。

若要刪除伺服器主機金鑰

1. 在開啟 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SFTP通訊協定的伺服器。
3. 在伺服器詳細資訊頁面上，向下捲動至伺服器主機金鑰區段。

Server host keys (1)						Actions ▾	Add host key
						< 1 >	
☐	Host key ID ▾	Fingerprint ▾	Description ▲	Key type ▾	Date imported ▾		
☐	hostkey-	SHA256: ██████████	ECDSA server host key	ecdsa-sha2-nistp256	2022-08-26		

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，輸入字詞 **delete**，然後選擇刪除，以確認您想要刪除主機金鑰。

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操作並提供伺服器 ID 和主機金鑰 ID。

下列範例delete-host-key AWS CLI 命令會刪除指定SFTP已啟用 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
```

輪換伺服器主機金鑰

您可以定期輪換伺服器主機金鑰。

Note

Transfer Family 使用每個演算法的第一個新增金鑰作為作用中主機金鑰。您每個SFTP伺服器最多可以關聯 10 個主機金鑰，但在任何特定時間，每個演算法只有一個金鑰處於作用中狀態。

例如，假設您已將下列一組伺服器主機金鑰新增至伺服器。

伺服器主機金鑰

主機金鑰類型	新增至伺服器的日期	作用中？
RSA	2020 年 4 月 1 日	否

主機金鑰類型	新增至伺服器的日期	作用中？
ECDSA	2020 年 2 月 1 日	否
ED25519	2019 年 12 月 1 日	否
RSA	2019 年 10 月 1 日	是
ECDSA	2019 年 6 月 1 日	是
ED25519	2019 年 3 月 1 日	是

每個演算法的最舊金鑰處於作用中狀態。如果您移除在 2019 年 10 月 1 日新增的 RSA 金鑰，則您在 2020 年 4 月 1 日新增的 RSA 金鑰會變成作用中。

若要輪換伺服器主機金鑰

1. 新增伺服器主機金鑰。此程序會在 [中說明新增其他伺服器主機金鑰](#)。
2. 刪除一個或多個您先前新增的相同類型的主機金鑰。此程序會在 [中說明刪除伺服器主機金鑰](#)。
3. 請確定相同類型的最早剩餘金鑰是您要啟用的金鑰。

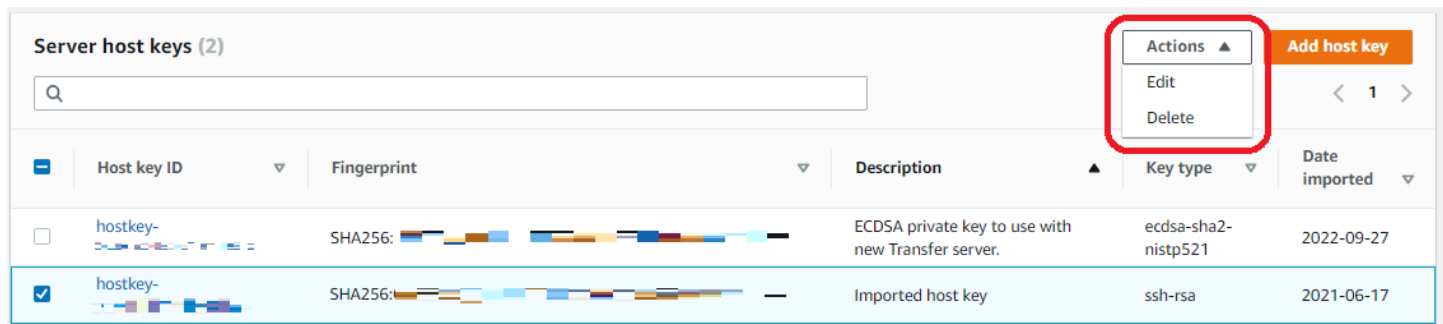
其他伺服器主機金鑰資訊

您可以選取主機金鑰以顯示該金鑰的詳細資訊。

The screenshot shows the AWS Transfer Family console interface. The breadcrumb navigation at the top reads: Transfer Family > Servers > s-... > Hostkey: hostkey-... . The main heading is 'hostkey-...' with a 'Delete' button to its right. Below this is a section titled 'Host key configuration' with an 'Edit' button. The configuration details are as follows:

Fingerprint SHA256: [fingerprint]	Key type ssh-rsa
Description Imported host key	Date imported Fri, 09 Jul 2021 16:51:20 GMT
Amazon Resource Name (ARN) arn:aws:transfer:us-east-2:[:host-key/s-.../hostkey-...]	

您可以刪除主機金鑰，或從伺服器詳細資訊畫面上的動作選單編輯其描述。選取主機金鑰，然後從功能表中選擇適當的動作。



監控主控台中的用量

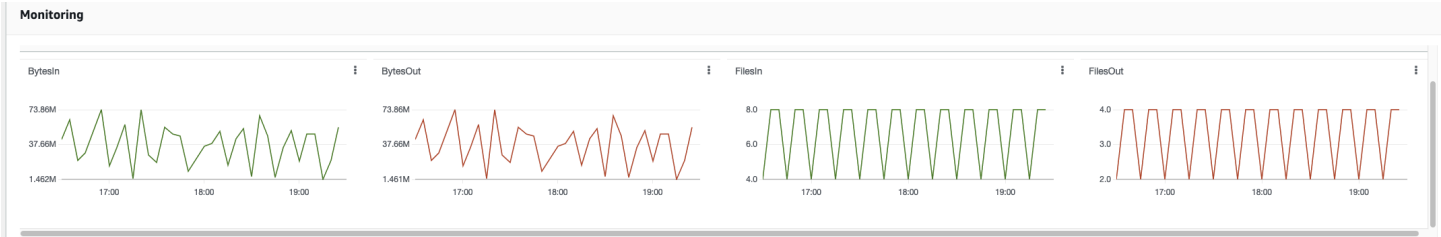
您可以在伺服器詳細資訊頁面上取得伺服器指標的相關資訊。這為您提供單一位置來監控檔案傳輸工作負載。您可以追蹤已與合作夥伴交換的檔案數量，並使用集中式儀表板密切追蹤其用量。如需詳細資訊，請參閱 [檢視 SFTP、FTPS 和 FTP 伺服器詳細資訊](#)。下表說明適用於 Transfer Family 的指標。

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	從伺服器傳輸的位元組總數。 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，此指標代表接收的訊息數量。 單位：計數 期間：5 分鐘
	FilesOut	從伺服器傳輸的檔案總數。

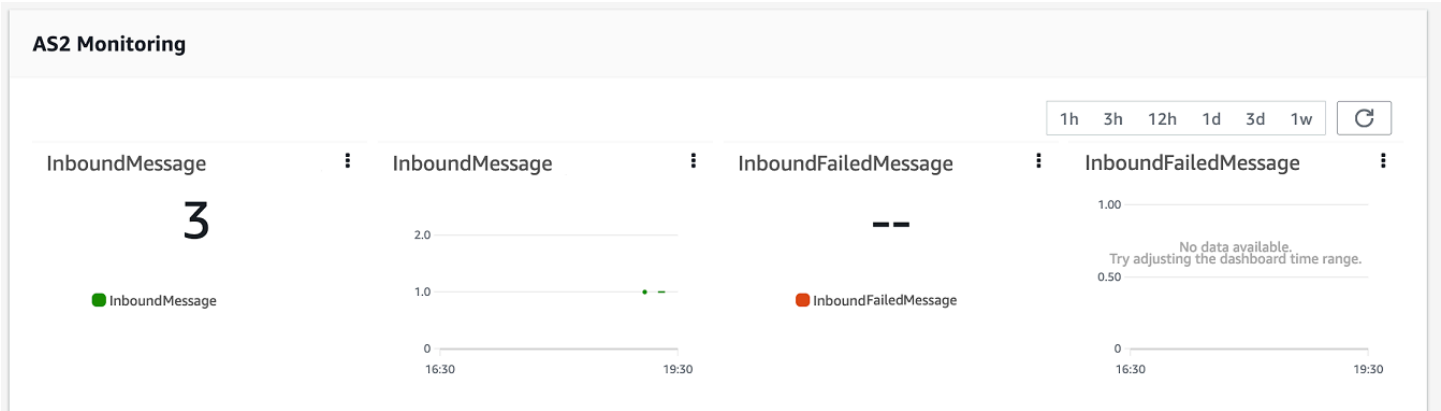
命名空間	指標	描述
		單位：計數 期間：5 分鐘
	InboundMessage	成功從交易合作夥伴收到AS2的訊息總數。 單位：計數 期間：5 分鐘
	InboundFailedMessage	未成功從交易合作夥伴收到AS2的訊息總數。也就是說，交易合作夥伴傳送訊息，但 Transfer Family 伺服器無法成功處理。 單位：計數 期間：5 分鐘
	OnPartialUploadExecutionsStarted	在伺服器上啟動的工作流程執行總數 on-partial-upload。 單位：計數 期間：1 分鐘
	OnPartialUploadExecutionsSuccessful	伺服器上成功 on-partial-upload執行工作流程的總數。 單位：計數 期間：1 分鐘
	OnPartialUploadExecutionsFailed	在伺服器上執行工作流程失敗 on-partial-upload的總數。 單位：計數 期間：1 分鐘
	OnUploadExecutionsStarted	在伺服器上啟動的工作流程執行總數。 單位：計數 期間：1 分鐘

命名空間	指標	描述
	OnUploadExecutionsSuccess	在伺服器上成功執行工作流程的總數。 單位：計數 期間：1 分鐘
	OnUploadExecutionsFailed	在伺服器上執行失敗的工作流程總數。 單位：計數 期間：1 分鐘

監控區段包含四個個別圖形。這些圖表顯示傳入、傳出位元組、傳入檔案和傳出檔案。



對於已啟用AS2通訊協定的伺服器，AS2監控資訊下方有一個監控區段。本節包含傳入訊息數量的詳細資訊，包括成功和失敗。



若要在自己的視窗中開啟選取的圖形，請選擇展開圖示 ()。您也可以按一下圖形的垂直省略號圖示 ()。

() ,

開啟包含下列項目的下拉式選單：

- 放大 – 在自己的視窗中開啟選取的圖形。
- 重新整理 – 使用最新的資料重新載入圖形。
- 在指標中檢視 – 在 Amazon 中開啟對應的指標詳細資訊 CloudWatch。
- 檢視日誌 – 在 中開啟對應的日誌群組 CloudWatch。

管理存取控制

您可以使用（IAM）政策來控制使用者對 AWS Transfer Family 資源的 AWS Identity and Access Management 存取。IAM 政策是一種陳述式，通常採用 JSON 格式，允許特定層級的資源存取。您可以使用 IAM 政策來定義要允許使用者執行和不執行的檔案操作。您也可以使用 IAM 政策來定義您要授予使用者存取權的 Amazon S3 儲存貯體或儲存貯體。若要為使用者指定這些政策，您可以為建立 AWS Transfer Family 具有相關 IAM 政策和信任關係 IAM 的角色。

每個使用者都會指派一個 IAM 角色。AWS Transfer Family 使用 IAM 的角色類型稱為服務角色。當使用者登入您的伺服器時，會 AWS Transfer Family 假設映射到使用者 IAM 的角色。若要了解如何建立提供使用者存取 Amazon S3 儲存貯體 IAM 的角色，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](#)。

您可以使用 IAM 政策中的特定許可，授予 Amazon S3 物件的僅寫入存取權。如需詳細資訊，請參閱 [授予僅寫入和列出檔案的能力](#)。

AWS Storage Blog 包含文章，詳細說明如何設定最低權限存取。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，您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

- [允許對 Amazon S3 儲存貯體進行讀取和寫入存取](#)
- [為 Amazon S3 儲存貯體建立工作階段政策](#)
- [防止使用者在 S3 儲存貯體 mkdir 中執行](#)

允許對 Amazon S3 儲存貯體進行讀取和寫入存取

本節說明如何建立允許讀取和寫入特定 Amazon S3 儲存貯體存取權 IAM 的政策。將具有此 IAM 政策 IAM 的角色指派給您的使用者，可讓該使用者存取指定的 Amazon S3 儲存貯體。

下列政策提供 Amazon S3 儲存貯體的程式設計讀取、寫入和標記存取權。只有在您需要啟用跨帳戶存取時，才需要 GetObjectACL 和 PutObjectACL 陳述式。也就是說，您的 Transfer Family 伺服器需要存取不同帳戶中的儲存貯體。

```
{
  "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。由於這些資源不同，因此使用不同的 Amazon Resource Names () 來指定這些資源 ARNs。

若要進一步限制使用者只能存取指定 Amazon S3 儲存貯體的 home 字首，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 AWS Identity and Access Management (IAM) 政策，將使用者限制為 Amazon S3 儲存貯體的特定部分。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。

當您需要將相同存取權授予使用者群組，以存取 Amazon S3 儲存貯體的特定部分時，您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

工作階段政策的長度上限為 2048 個字元。如需更多詳細資訊，請參閱 API 參考中 `CreateUser` 動作 [的政策請求參數](#)。

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 Managed Policy 中使用上述變數。您也無法在 IAM 角色定義中使用它們作為政策變數。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政策中使用 `${aws:Username}` 變數。此變數是指 IAM 使用者名稱，而不是所需的使用者名稱 AWS Transfer Family。

下列程式碼顯示工作階段政策範例。

```
{
  "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

上述政策範例假設使用者已將主目錄設定為包含尾斜線，以表示它是目錄。另一方面，如果您設定的使用者HomeDirectory沒有尾斜線，則應將其納入政策中。

在先前的範例政策中，請注意 `transfer:HomeFolder`、`transfer:HomeBucket` 和 `transfer:HomeDirectory` 政策參數的使用。這些參數是針對為使用者設定的 `HomeDirectory` 設定，如 [HomeDirectory](#) 和 中所述 [實作API閘道方法](#)。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` 參數會以 `HomeDirectory` 參數的剩餘部分取代。
- `transfer:HomeDirectory` 參數已移除正斜線 (/)，因此可在 Resource 陳述式中將其用作 S3 Amazon Resource Name (ARN) 的一部分。

 Note

如果您使用的是邏輯目錄，也就是使用者的 `homeDirectoryType` 是 `LOGICAL`，則不支援這些政策參數 (`HomeBucket`、`HomeDirectory` 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` 會變成 `home/bob/amazon/stuff/`。

第一個 "Sid" 允許使用者列出從 開始的所有目錄 `/home/bob/amazon/stuff/`。

第二個 "Sid" 限制使用者對 `put` 相同路徑 的 `get` 存取 `/home/bob/amazon/stuff/`。

實施上述政策後，當使用者登入時，他們只能存取主目錄中的物件。在連線時間，會將這些變數 AWS Transfer Family 取代為使用者的適當值。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。此方法可減少管理使用者存取 Amazon S3 儲存貯體 IAM 的角色和政策管理的額外負荷。

您也可以使用工作階段政策，根據您的業務需求自訂每個使用者的存取權。如需詳細資訊，請參閱 IAM 使用者指南 中的 [AssumeRole AssumeRoleWithSAML](#)、和 [許可 AssumeRoleWithWebIdentity](#)。

 Note

AWS Transfer Family 會儲存政策 JSON，而不是政策的 Amazon Resource Name (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。您可以在使用者組態區段的政策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政策。

```
aws transfer update-user --server-id server --user-name user --policy \
    "$(aws iam get-policy-version --policy-arn policy --version-id version --
    output json)"
```

防止使用者在 S3 儲存貯體 `mkdir` 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 IAM 的政策，但也會在金鑰結尾為 `/`（正斜線）時拒絕。下列範例政策允許使用者將檔案上傳至 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

第二個資源列讓使用者無法透過執行 `put my-file DOC-EXAMPLE-BUCKET/new-folder/my-file`。

記錄 AWS Transfer Family

AWS Transfer Family 與 AWS CloudTrail 和 Amazon CloudWatch. 整合 CloudTrail , CloudWatch 並提供不同但互補的目的：

- CloudTrail 是一項 AWS 服務，可建立在 中採取動作的記錄 AWS 帳戶。它會持續監控和記錄主控台登入、AWS Command Line Interface 命令和 SDK/API API 呼叫等活動的呼叫。這可讓您保留 的日誌，其中包含誰在何時以及從何地採取了哪些動作。透過提供環境中 AWS 所有活動的歷史記錄，CloudTrail 協助稽核、存取管理和合規。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控服務。它收集指標和日誌，以提供資源使用率、應用程式效能和整體系統運作狀態的可見性。CloudWatch 有助於操作任務，例如疑難排解問題、設定警示和自動擴展。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](#)
- [的 Amazon CloudWatch 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": "AAAA4FFF5HHHHH6NNWWW:user1",
    "arn": "arn:aws:sts::123456789102:assumed-role/Admin/user1",
    "accountId": "123456789102",
    "accessKeyId": "AAAA52C2WWWWW3BB4Z",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2018-12-18T20:03:57Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AAAA4FFF5HHHHH6NNWWW",
        "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"
}

```

的 Amazon CloudWatch 記錄 AWS Transfer Family

Amazon 會 AWS 即時 CloudWatch 監控您的 AWS Transfer Family 資源和您在 上執行的應用程式。您可以使用 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 和您使用之所有其他 AWS 服務的指標。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，您可以監控要傳輸至 Transfer Family 伺服器的檔案，並使用該資料來判斷是否需要部署其他伺服器來處理增加的負載。您也可以使用此資料來停止或刪除使用不足的執行個體以節省成本。

主題

- [建立、更新和檢視伺服器的日誌記錄](#)
- [管理工作流程的記錄](#)
- [設定 CloudWatch 記錄角色](#)
- [檢視 Transfer Family 日誌串流](#)
- [建立 Amazon CloudWatch 警示](#)
- [將 Amazon S3 API 呼叫記錄到 S3 存取日誌](#)
- [限制混淆代理問題的範例](#)
- [CloudWatch 轉移系列的記錄結構](#)
- [CloudWatch 日誌項目範例](#)
- [使用 Transfer Family 的 CloudWatch 指標](#)
- [AWS 使用者通知 搭配 使用 AWS Transfer Family](#)

建立、更新和檢視伺服器的日誌記錄

對於所有 AWS Transfer Family 伺服器，您可以選擇兩個記錄選項：LoggingRole（用於記錄連接到伺服器的工作流程）或 StructuredLogDestinations。使用 StructuredLogDestinations 的優點包括：

- 以結構化JSON格式接收日誌。
- 使用 Amazon CloudWatch Logs Insights JSON 查詢您的日誌，自動探索格式化欄位。
- 跨 AWS Transfer Family 資源共用日誌群組可讓您將多個伺服器的日誌串流合併為單一日誌群組，讓您更輕鬆地管理監控組態和日誌保留設定。
- 建立可新增至 CloudWatch 儀表板的彙總指標和視覺化。
- 使用日誌群組來建立合併日誌指標、視覺化效果和儀表板，以追蹤用量和效能資料。

LoggingRole 或 的選項 StructuredLogDestinations 會分別設定和控制。對於每個伺服器，您可以設定一種或兩種記錄方法，或將伺服器設定為沒有任何記錄（雖然不建議這麼做）。

如果您使用 Transfer Family 主控台建立新伺服器，則預設會啟用記錄。建立伺服器之後，您可以使用 UpdateServerAPI 呼叫來變更記錄組態。如需詳細資訊，請參閱 [StructuredLogDestinations](#)。

目前，對於工作流程，如果您想要啟用記錄功能，您必須指定記錄角色：

- 如果您使用 `CreateServer` 或 `UpdateServer` API 呼叫將工作流程與伺服器建立關聯，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，您需要明確地將記錄角色連接到伺服器。
- 如果您使用 Transfer Family 主控台建立伺服器並連接工作流程，日誌會傳送至名稱中包含伺服器 ID 的日誌群組。格式為 `/aws/transfer/server-id`，例如 `/aws/transfer/s-1111aaaa2222bbbb3`。伺服器日誌可以傳送至此相同的日誌群組或不同的日誌群組。

在主控台中建立和編輯伺服器的記錄考量事項

- 透過主控台建立的新伺服器僅支援結構化JSON記錄，除非工作流程連接至伺服器。
- 對於您在主控台中建立的新伺服器，沒有記錄選項。
- 現有伺服器可以隨時透過主控台啟用結構化JSON日誌記錄。
- 透過主控台啟用結構化JSON記錄會停用現有的記錄方法，以免向客戶重複收費。例外狀況是工作流程已連接至伺服器。
- 如果您啟用結構化JSON日誌記錄，則無法稍後透過主控台停用。
- 如果您啟用結構化JSON日誌記錄，您可以隨時透過主控台變更日誌群組目的地。
- 如果您啟用結構化JSON記錄，則如果您透過 啟用這兩種記錄類型，則無法透過主控台編輯記錄角色API。例外狀況是，如果您的伺服器已連接工作流程。不過，記錄角色會繼續出現在其他詳細資訊中。

記錄使用 API 或 建立和編輯伺服器的考量事項 SDK

- 如果您透過 建立新伺服器API，則可以設定記錄類型或兩種類型，或選擇不記錄。
- 對於現有伺服器，可隨時啟用和停用結構化JSON日誌記錄。
- API 您可以隨時透過 變更日誌群組。
- API 您可以隨時透過 變更記錄角色。

若要啟用結構化記錄，您必須使用下列許可登入 帳戶

- `logs:CreateLogDelivery`
- `logs>DeleteLogDelivery`
- `logs:DescribeLogGroups`
- `logs:DescribeResourcePolicies`
- `logs:GetLogDelivery`

- logs:ListLogDeliveries
- logs:PutResourcePolicy
- logs:UpdateLogDelivery

範例政策可在 章節中取得[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

當您建立新的伺服器時，您可以在設定其他詳細資訊頁面上指定現有的日誌群組，或建立新的日誌群組。

Transfer Family > Servers > Create server

Step 1
Choose protocols

Step 2
Choose an identity provider

Step 3
Choose an endpoint

Step 4
Choose a domain

Step 5
Configure additional details

Step 6
Review and create

Configure additional details

Logging [Info](#)

Log group [Info](#)
Choose the CloudWatch log group where your events will be delivered in a structured JSON format

☒ Create a new log group ☐ Choose an existing log group

Logging role [Info](#)
Choose the IAM role that will be used to deliver events to your CloudWatch logs

☐ Create a new role ☐ Choose an existing role

Info Logging role is only required when selecting a workflow in the Managed workflows section below.

如果您選擇現有的日誌群組，您必須選取與 相關聯的日誌群組 AWS 帳戶。

Transfer Family > Servers > Create server

Step 1
Choose protocols

Step 2
Choose an identity provider

Step 3
Choose an endpoint

Step 4
Choose a domain

Step 5
Configure additional details

Step 6
Review and create

Configure additional details

Logging Info

Log group Info
Choose the CloudWatch log group where your events will be delivered in a structured JSON format

☐ Create a new log group ☒ Choose an existing log group

Logging role Info
Choose the IAM role that will be used to deliver events to your CloudWatch logs

☐ Create a new role ☐ Choose an existing role

Note Logging role is only required when selecting a workflow in the Managed workflows section below.

如果您選擇建立日誌群組，CloudWatch 主控台（<https://console.aws.amazon.com/cloudwatch/>）會開啟建立日誌群組頁面。如需詳細資訊，請參閱在[日誌中建立 CloudWatch 日誌群組](#)。

更新伺服器的記錄

記錄的詳細資訊取決於您更新的案例。

Note

當您選擇結構化JSON記錄時，可能會發生延遲，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JSON格式記錄。這可能會導致未記錄的事件。不會有任何服務中斷，但您應該在變更記錄方法後的第一個小時內小心傳輸檔案，因為日誌可能會遭到捨棄。

如果您要編輯現有的伺服器，您的選項取決於伺服器的狀態。

- 伺服器已啟用記錄角色，但尚未啟用結構化JSON記錄。

Edit additional details

Logging [Info](#)

Log group [Info](#)

Choose an existing log group from the dropdown or create a new log group in Amazon CloudWatch

☒ Enable structured JSON logging

/aws/transfer/scooter ▼



Create log group [↗](#)

Enabling the structured JSON log format will override your existing logging configuration. Potential changes include new log format and log group.

Logging Role [Info](#)

Select an existing role from your account

AWSTransferLoggingAccess ▼



Workflows events will be delivered to a log group labelled with the server ID.

- 伺服器未啟用任何記錄。

Edit additional details

Logging [Info](#)

Log group [Info](#)

Choose an existing log group from the dropdown or create a new log group in Amazon CloudWatch

☐ Enable structured JSON logging

Choose an existing log group ▼



Create log group [↗](#)

Logging Role [Info](#)

Select an existing role from your account

Choose a role ▼



Logging role is only required when selecting a workflow in the Managed workflows section below.

- 伺服器已啟用結構化JSON記錄，但尚未指定記錄角色。

Edit additional details

Logging [Info](#)

Log group [Info](#)

Choose an existing log group from the dropdown or create a new log group in Amazon CloudWatch

☒ Enable structured JSON logging

/aws/transfer/ ▼



Create log group [↗](#)

Logging Role [Info](#)

Select an existing role from your account

Choose a role ▼



Logging role is only required when selecting a workflow in the Managed workflows section below.

- 伺服器已啟用結構化JSON記錄，並且還指定了記錄角色。

Edit additional details

Logging [Info](#)

Log group [Info](#)

Choose an existing log group from the dropdown or create a new log group in Amazon CloudWatch

☒ Enable structured JSON logging

/aws/transfer/s-



Create log group [↗](#)

Logging Role [Info](#)

Select an existing role from your account

AWSTransferLoggingAccess



[i](#) Workflows events will be delivered to a log group labelled with the server ID.

檢視伺服器組態

伺服器組態頁面的詳細資訊取決於您的案例：

根據您的案例，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。

Additional details Edit		
Log group -	Domain Amazon S3	Login display banner View the display message
Logging role Info -	Workflow for complete uploads -	SetStat option Ignore
Server host key Info SHA256: [redacted]	Workflow for partial uploads -	TLS session resumption -
Security Policy Info TransferSecurityPolicy-2018-11	Managed workflows execution role -	Passive IP -

- 已啟用結構化JSON記錄。

Additional details Edit

Log group /aws/transfer/s[redacted]	Domain Amazon S3	Login display banner View the display message
Logging role Info -	Workflow for complete uploads -	SetStat option Ignore
Server host key Info SHA256:[redacted] [redacted]	Workflow for partial uploads -	TLS session resumption -
Security Policy Info TransferSecurityPolicy-2020-06	Managed workflows execution role -	Passive IP -

- 已啟用記錄角色，但未啟用結構化JSON記錄。

Additional details Edit

Log group -	Domain Amazon S3	Login display banner View the display message
Logging role Info AWSTransferLoggingAccess	Workflow for complete uploads w-[redacted]	SetStat option Ignore
Server host key Info SHA256:lx39/[redacted] [redacted]	Workflow for partial uploads -	TLS session resumption -
Security Policy Info TransferSecurityPolicy-2018-11	Managed workflows execution role [redacted] execution-role [redacted]	Passive IP -

- 這兩種類型的記錄（記錄角色和結構化JSON記錄）都已啟用。

Additional details

Edit

Log group /aws/transfer/s-	Domain Amazon S3	Login display banner View the display message
Logging role Info AWSTransferLoggingAccess	Workflow for complete uploads w-	SetStat option Ignore
Server host key Info SHA256:	Workflow for partial uploads -	TLS session resumption -
Security Policy Info TransferSecurityPolicy-2020-06	Managed workflows execution role transfer-workflows	Passive IP -

管理工作流程的記錄

CloudWatch 提供工作流程進度和結果的合併稽核和記錄。此外，為工作流程 AWS Transfer Family 提供數個指標。您可以檢視上一分鐘有多少工作流程執行開始、成功完成和失敗的指標。Transfer Family 的所有 CloudWatch 指標都說明於 [中 使用 Transfer Family 的 CloudWatch 指標](#)。

檢視工作流程的 Amazon CloudWatch 日誌

1. 在 開啟 Amazon CloudWatch 主控台 <https://console.aws.amazon.com/cloudwatch/>。
2. 在左側導覽窗格中，選擇日誌，然後選擇日誌群組。
3. 在日誌群組頁面上的導覽列上，為您的 AWS Transfer Family 伺服器選擇正確的區域。
4. 選擇與伺服器對應的日誌群組。

例如，如果您的伺服器 ID 為 s-1234567890abcdef0，您的日誌群組為 /aws/transfer/s-1234567890abcdef0。

5. 在伺服器的日誌群組詳細資訊頁面上，會顯示最新的日誌串流。您正在探索的使用者有兩個日誌串流：
 - 每個 Secure Shell (SSH) 檔案傳輸通訊協定 (SFTP) 工作階段各一個。
 - 一個用於正在為伺服器執行的工作流程。工作流程的日誌串流格式為 *username.workflowID.uniqueStreamSuffix*。

例如，如果您的使用者是 mary-major，您有下列日誌串流：

```
mary-major-east.1234567890abcdef0
mary.w-abcdef01234567890.021345abcdef6789
```

Note

此範例中列出的 16 位數英數字元識別碼為虛構。您在 Amazon 中看到的值 CloudWatch 不同。

的日誌事件頁面mary-major-usa-east.1234567890abcdef0會顯示每個使用者工作階段的詳細資訊，而mary.w-abcdef01234567890.021345abcdef6789日誌串流包含工作流程的詳細資訊。

以下是 的日誌串流範例mary.w-abcdef01234567890.021345abcdef6789，以包含複製步驟的工作流程（w-abcdef01234567890）為基礎。

```
{
  "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，您可以建立資源型IAM政策和提供該存取資訊IAM的角色。

若要啟用 Amazon CloudWatch 記錄，請先建立啟用 CloudWatch記錄IAM的政策。然後，您可以建立角色並將政策連接至該IAM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。如需的詳細資訊 CloudWatch，請參閱 [Amazon 使用者指南 中的什麼是 Amazon CloudWatch？](#) 和 [什麼是 Amazon 日誌？ CloudWatch](#)。 CloudWatch

使用下列範例IAM政策來允許 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，對於 **Resource**，請取代 *region-id* 以及 *AWS ##* 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 日誌政策。

若要建立 IAM 角色並附加政策

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，確定已選擇 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，新增 `aws:SourceAccount` 和 `aws:SourceArn` 條件索引鍵，以保護自己免受混淆代理問題的影響。如需更多詳細資訊，請參閱下列文件：
 - 與 建立信任關係的程序 AWS Transfer Family：[建立信任關係](#)
 - 混淆代理問題的描述：[混淆代理問題](#)
3. 在連接許可政策區段中，找到並選擇您剛建立的 CloudWatch 日誌政策，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. 若要檢視日誌，請選擇伺服器 ID 以開啟伺服器組態頁面，然後選擇檢視日誌。系統會將您重新導向至 CloudWatch 主控台，您可以在其中查看日誌串流。

在伺服器的 CloudWatch 頁面上，您可以查看使用者身分驗證（成功和失敗）、資料上傳（PUT 操作）和資料下載（GET 操作）的記錄。

檢視 Transfer Family 日誌串流

檢視 Transfer Family 伺服器日誌

1. 導覽至伺服器的詳細資訊頁面。
2. 選擇 檢視日誌 。這會開啟 Amazon CloudWatch。
3. 顯示所選伺服器的日誌群組。

The screenshot displays the AWS CloudWatch console interface. On the left is a navigation sidebar with sections like 'Dashboards', 'Alarms', 'Logs', 'Metrics', 'X-Ray traces', 'Events', 'Application monitoring', and 'Insights'. The 'Logs' section is expanded, showing 'Log groups' and 'Logs Insights'. The main content area shows the details for a specific log group, identified by its ARN: `arn:aws:logs:us-east-2:5[redacted]:log-group:/aws/transfer/s-[redacted]:*`. The details include creation time (2 years ago), retention (Never expire), and stored bytes (39.39 MB). Below the details, there are tabs for 'Log streams', 'Metric filters', 'Subscription filters', 'Contributor Insights', 'Tags', and 'Data protection - new'. The 'Log streams' tab is active, showing a list of 10 log streams. The first stream is 'ERRORS', and the others are prefixed with 'scooterstack4-'. Each stream entry includes a checkbox, the stream name, and a 'Last event' timestamp.

4. 您可以選取日誌串流，以顯示串流的詳細資訊和個別項目。
 - 如果有 的清單ERRORS，您可以選擇它來檢視伺服器最新錯誤的詳細資訊。

CloudWatch > Log groups > /aws/transfer/s- > ERRORS

Log events

You can use the filter bar below to search for and match terms, phrases, or values in your log events. [Learn more about filter patterns](#)

Timestamp	Message
There are older events to load. Load more.	
2023-03-23T16:08:29.281-04:00	ERRORS AUTH_FAILURE Method=password User=ubuntu Message= SourceIP=
2023-03-23T16:08:30.979-04:00	ERRORS AUTH_FAILURE Method=password User=ubuntu Message= SourceIP=
2023-03-23T16:08:32.647-04:00	ERRORS AUTH_FAILURE Method=password User=ubuntu Message= SourceIP=
2023-03-23T16:08:34.306-04:00	ERRORS AUTH_FAILURE Method=password User=ubuntu Message= SourceIP=
2023-03-23T16:08:36.010-04:00	ERRORS AUTH_FAILURE Method=password User=ubuntu Message= SourceIP=
2023-03-23T16:08:37.659-04:00	ERRORS AUTH_FAILURE Method=password User=ubuntu Message= SourceIP=
2023-03-23T16:12:33.307-04:00	ERRORS AUTH_FAILURE Method=password User=scooterstack4 Message="Missing POSIX profile" SourceIP=
2023-03-23T16:12:34.943-04:00	ERRORS AUTH_FAILURE Method=password User=scooterstack4 Message="Missing POSIX profile" SourceIP=
2023-03-23T16:12:56.857-04:00	ERRORS AUTH_FAILURE Method=password User=debian Message= SourceIP=
2023-03-23T16:12:58.430-04:00	ERRORS AUTH_FAILURE Method=password User=debian Message= SourceIP=
2023-03-23T16:13:00.106-04:00	ERRORS AUTH_FAILURE Method=password User=debian Message= SourceIP=

- 選擇任何其他項目以查看日誌串流範例。

CloudWatch > Log groups > /aws/transfer/s- > scooterstack4.

Log events

You can use the filter bar below to search for and match terms, phrases, or values in your log events. [Learn more about filter patterns](#)

Timestamp	Message
No older events at this moment. Retry	
2023-03-23T16:19:43.747-04:00	scooterstack4. CONNECTED SourceIP= User=scooterstack4 HomeDir=/fs- scooterstack4. CONNECTED SourceIP= User=scooterstack4 HomeDir=/fs- Client=SSH-2.0- OpenSSH_7.4 Role=arn:aws:iam:: :role/ Kex=
2023-03-23T16:19:47.030-04:00	scooterstack4. DISCONNECTED scooterstack4. DISCONNECTED
No newer events at this moment. Auto retry paused. Resume	

- 如果您的伺服器具有與其相關聯的受管工作流程，您可以檢視工作流程執行的日誌。

Note

工作流程的日誌串流格式為 `username.workflowId.uniqueStreamSuffix`。例如，`decrypt-user.w-a1111222233334444.aaaa1111bbbb2222` 可以是使用者 **decrypt-user** 和工作流程的日誌串流名稱 **w-a1111222233334444**。

CloudWatch > Log groups > /aws/transfer/s- > decrypt-user.w-

Log events
You can use the filter bar below to search for and match terms, phrases, or values in your log events. [Learn more about filter patterns](#)

Actions Create metric filter

Filter events Clear 1m 30m 1h 12h Custom Display

Timestamp	Message
	There are older events to load. Load more .
2023-03-21T13:37:57.795-04:00	{ "type": "StepStarted", "details": { "input": { "fileLocation": { "backingStore": "S3", "bucket": "...", "key": "decrypt-...
2023-03-21T14:12:02.850-04:00	{ "type": "StepStarted", "details": { "input": { "fileLocation": { "backingStore": "S3", "bucket": "...", "key": "decrypt-...
	<pre>{ "type": "StepStarted", "details": { "input": { "fileLocation": { "backingStore": "S3", "bucket": "...", "key": "decrypt-user/test.json.gpg", "versionId": "...", "etag": "..." } } }, "stepType": "DECRYPT", "stepName": "decrypt-step" }, "workflowId": "w-...", "executionId": "...", "transferDetails": { "serverId": "s-...", "username": "decrypt-user", "sessionId": "..." } }</pre>
2023-03-21T14:12:03.464-04:00	{ "type": "StepCompleted", "details": { "output": {} }, "stepType": "DECRYPT", "stepName": "decrypt-step", "workflowId": "w-..."

Note

對於任何展開的日誌項目，您可以選擇複製，將項目複製到剪貼簿。如需 CloudWatch 日誌的詳細資訊，請參閱[檢視日誌資料](#)。

建立 Amazon CloudWatch 警示

下列範例示範如何使用 AWS Transfer Family 指標 建立 Amazon CloudWatch 警示FilesIn。

CDK

```
new cloudwatch.Metric({
  namespace: "AWS/Transfer",
  metricName: "FilesIn",
  dimensionsMap: { ServerId: "s-000000000000000000" },
  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-000000000000000000
  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提出的 S3 請求](#)，RoleSessionName 會用來顯示擔任哪個IAM角色來服務檔案傳輸。它也會顯示其他資訊，例如用於傳輸的使用者名稱、工作階段 ID 和伺服器 ID。格式包含在[AWS:Role Unique Identifier]/

username.sessionid@server-id請求者欄位中。例如，以下是從複製到 S3 儲存貯體之檔案的 S3 存取日誌中的範例請求者欄位的內容。S3

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

在上方的請求者欄位中，會顯示名為 IAM 的角色 IamRoleName。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](#)。

限制混淆代理問題的範例

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 AWS，跨服務模擬可能會導致混淆代理問題。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，取代每個 *user input placeholder* 使用您自己的資訊。
在這些範例中，如果您的伺服器未連接任何工作流程，您可以移除工作流程 ARN 的詳細資訊。

下列範例記錄/調用政策允許 帳戶中的任何伺服器（和工作流程）擔任 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/調用政策允許特定伺服器（和 workflow）擔任角色。

```

{
  "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 密碼編譯演算法)	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 密碼編譯演算法)	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 workflow	{「類型」: CustomStepInvoked 「,」詳細資訊」: {"輸出": {"令牌": "MZM4MG5 下 EzMy 午 00 Yjlz LWI3OG MtYz U4OGI2 ZjQyMz E5"}, "步 驟類型": "自定義", "stepName": "EFS-s3_c opy_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" } }

CloudWatch 日誌項目範例

本主題顯示日誌項目範例。

主題

- [轉移工作階段日誌項目範例](#)
- [SFTP 連接器的日誌項目範例](#)
- [金鑰交換演算法失敗的日誌項目範例](#)

轉移工作階段日誌項目範例

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。

下列日誌項目反映連線至 Transfer Family 伺服器SFTP的使用者。

```
{
  "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SFTP使用者將檔案上傳至其 Amazon S3 儲存貯體。

```
{
  "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"
}
```

下列日誌項目反映SFTP使用者中斷與其SFTP工作階段的連線。首先，用戶端會關閉與儲存貯體的連線，然後用戶端會中斷SFTP連線工作階段。

```
{
  "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 連接器的日誌項目範例

本節包含成功和失敗傳輸的範例日誌。日誌會產生到名為 的日誌群組`/aws/transfer/connector-id`，其中 *connector-id* 是SFTP連接器的識別符。

Note

只有在您執行StartFileTransfer命令時才會產生SFTP連接器的日誌項目。

此日誌項目適用於成功完成的傳輸。

```
{
  "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"
  }

```

此日誌項目適用於逾時的傳輸，因此未成功完成。

```

{
  "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"
}

```

先向日誌範例中某些金鑰欄位的說明。

- `timestamp` 代表日誌新增至 的時間 CloudWatch。 `start-time`和 `end-time` 對應至連接器實際啟動和完成傳輸的時間。
- `transfer-id` 是為每個`start-file-transfer`請求指派的唯一識別符。如果使用者在單一`start-file-transfer`API呼叫中傳遞多個檔案路徑，則所有檔案都會共用相同的 `transfer-id`。
- `file-transfer-id` 是為每個傳輸的檔案產生的唯一值。請注意， 的初始部分`file-transfer-id`與 相同`transfer-id`。

金鑰交換演算法失敗的日誌項目範例

本節包含金鑰交換演算法（KEX）失敗的範例日誌。這些是來自結構化ERRORS日誌的日誌串流範例。

此日誌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"
}
```

此日誌項目是不相符的範例KEX。

```
{
  "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 指標

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 [監控主控台中的用量](#)

您可以使用 CloudWatch 指標取得伺服器的相關資訊。指標代表發佈至 的定時資料點集 CloudWatch。使用指標時，您必須指定 Transfer Family 命名空間、指標名稱和[維度](#)。如需指標的詳細資訊，請參閱 Amazon CloudWatch 使用者指南 中的[指標](#)。

下表說明 Transfer Family 的 CloudWatch 指標。

命名空間	指標	描述
AWS/Transfer	BytesIn	傳輸到伺服器的位元組總數。

命名空間	指標	描述
		單位：計數 期間：5 分鐘
	BytesOut	從伺服器傳輸的位元組總數。 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，此指標代表接收的訊息數量。 單位：計數 期間：5 分鐘
	FilesOut	從伺服器傳輸的檔案總數。 單位：計數 期間：5 分鐘
	InboundMessage	成功從交易合作夥伴收到AS2的訊息總數。 單位：計數 期間：5 分鐘
	InboundFailedMessage	未成功從交易合作夥伴收到AS2的訊息總數。也就是說，交易合作夥伴傳送訊息，但 Transfer Family 伺服器無法成功處理。 單位：計數 期間：5 分鐘

命名空間	指標	描述
	OnPartialUploadExecutionsStarted	在伺服器上啟動的工作流程執行總數 on-partial-upload。 單位：計數 期間：1 分鐘
	OnPartialUploadExecutionsSuccess	在伺服器上成功 on-partial-upload執行工作流程的總數。 單位：計數 期間：1 分鐘
	OnPartialUploadExecutionsFailed	在伺服器上執行工作流程失敗 on-partial-upload的總數。 單位：計數 期間：1 分鐘
	OnUploadExecutionsStarted	在伺服器上啟動的工作流程執行總數。 單位：計數 期間：1 分鐘
	OnUploadExecutionsSuccess	在伺服器上成功執行工作流程的總數。 單位：計數 期間：1 分鐘
	OnUploadExecutionsFailed	在伺服器上執行失敗的工作流程總數。 單位：計數 期間：1 分鐘

轉移系列維度

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 ID。

AWS 使用者通知 搭配 使用 AWS Transfer Family

若要收到 AWS Transfer Family 事件的通知，您可以使用 [AWS 使用者通知](#) 設定各種交付管道。當事件符合您指定的規則時，您會收到通知。

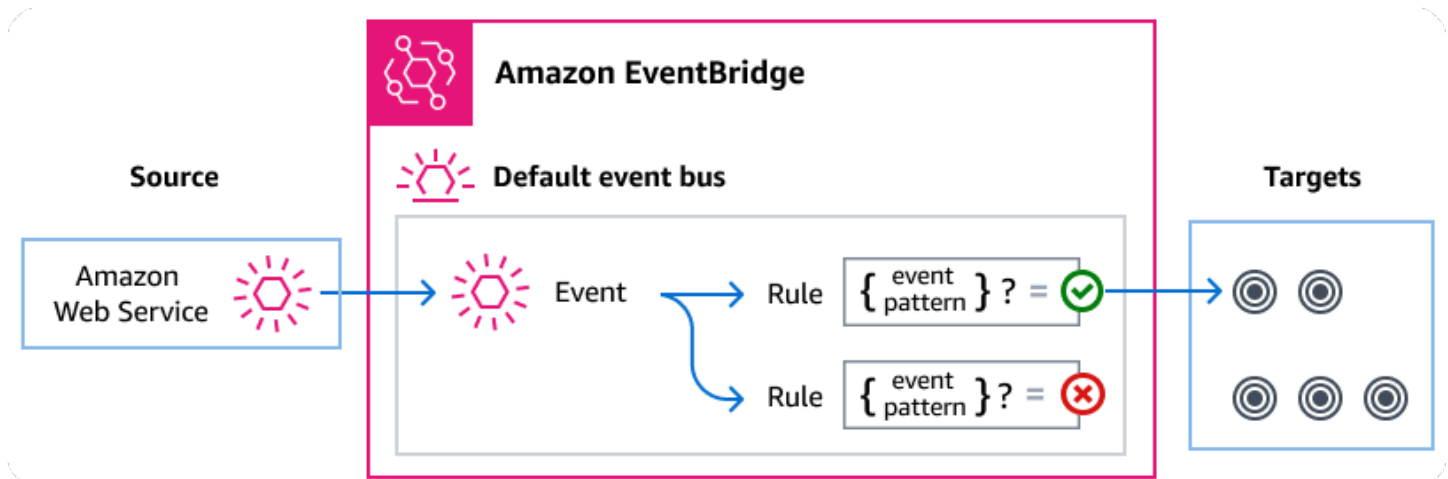
您可以透過多個管道接收事件通知，包括電子郵件、[Amazon Q 聊天應用程式的開發人員](#) 聊天通知或 [AWS Console Mobile Application](#) 推送通知。您也可以在[主控台通知中心](#)中看到通知。使用者通知 支援彙總，可減少您在特定事件期間收到的通知數量。

如需詳細資訊，請參閱 使用者指南 中的[使用 AWS Transfer Family 受管工作流程部落格文章自訂檔案交付通知](#)，以及[什麼是 AWS 使用者通知？](#)。AWS 使用者通知

使用 管理 Transfer Family 事件 Amazon EventBridge

Amazon EventBridge 是一種無伺服器服務，使用事件將應用程式元件連接在一起，可讓您更輕鬆地建置可擴展的事件驅動型應用程式。事件驅動架構是一種建置鬆散耦合軟體系統的方式，可透過發射和回應事件來共同運作。事件代表資源或環境中的變更。

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，預設事件匯流排會自動在每個 AWS 帳戶中佈建。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，以便在事件到達時對其進行評估。每個規則都會檢查事件是否與規則的事件模式相符。如果事件相符，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 許可](#)
- [其他 EventBridge 資源](#)
- [Transfer Family 事件詳細資訊參考](#)

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盡最大努力交付至指定的目標，不過，某些事件可能會不按順序交付。

下列事件由 產生 Transfer Family。如需詳細資訊，請參閱 Amazon EventBridge 使用者指南 中的 [EventBridge 事件](#)。

SFTP、FTPS和 FTP 伺服器事件

事件詳細資訊類型	描述
FTP 檔案伺服器下載已完成	已成功下載FTP通訊協定的檔案。
FTP 檔案伺服器下載失敗	嘗試下載 FTP通訊協定的檔案失敗。
FTP 檔案伺服器上傳已完成	已成功上傳FTP通訊協定的檔案。
FTP 檔案伺服器上傳失敗	嘗試上傳 FTP通訊協定的檔案失敗。
FTPS 檔案伺服器下載已完成	已成功下載FTPS通訊協定的檔案。
FTPS 檔案伺服器下載失敗	嘗試下載 FTPS通訊協定的檔案失敗。
FTPS 檔案伺服器上傳已完成	已成功上傳FTPS通訊協定的檔案。
FTPS 檔案伺服器上傳失敗	嘗試上傳 FTPS通訊協定的檔案失敗。
SFTP 伺服器檔案下載已完成	已成功下載SFTP通訊協定的檔案。
SFTP 伺服器檔案下載失敗	嘗試下載 SFTP通訊協定的檔案失敗。
SFTP 伺服器檔案上傳已完成	已成功上傳SFTP通訊協定的檔案。
SFTP 伺服器檔案上傳失敗	嘗試上傳 SFTP通訊協定的檔案失敗。

SFTP 連接器事件

事件詳細資訊類型	描述
SFTP 連接器檔案傳送已完成	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 連接器檔案擷取已完成	從遠端SFTP伺服器到連接器的檔案傳輸已成功完成。

事件詳細資訊類型	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。

A2S 事件

事件詳細資訊類型	描述
AS2 承載接收已完成	已收到AS2訊息的承載。
AS2 承載接收失敗	尚未收到AS2訊息的承載。
AS2 承載傳送已完成	訊息的承載AS2已成功傳送。
AS2 承載傳送失敗	AS2 訊息的承載無法傳送。
AS2 MDN 接收已完成	已收到訊息AS2的訊息處置通知。
AS2 MDN 接收失敗	尚未收到訊息AS2的訊息處置通知。
AS2 MDN 傳送已完成	訊息的訊息處置通知AS2已成功傳送。
AS2 MDN 傳送失敗	訊息的訊息處置通知AS2無法傳送。

使用 EventBridge 規則傳送 Transfer Family 事件

如果您想要 EventBridge 預設事件匯流排將 Transfer Family 事件傳送至目標，則必須建立包含符合所需 Transfer Family 事件中資料之事件模式的規則。

您可以遵循下列一般步驟來建立規則：

1. 為指定以下內容的規則建立事件模式：

- Transfer Family 是規則正在評估的事件來源。
- (選用) 要比對的任何其他事件資料。

如需詳細資訊，請參閱[???](#)。

2. (選用) 建立輸入轉換器，在將資訊 EventBridge 傳送至規則的目標之前，自訂事件中的資料。

如需詳細資訊，請參閱 EventBridge 使用者指南 中的[輸入轉換](#)。

3. 指定您要 EventBridge 交付符合事件模式之事件的目標。

目標可以是其他服務 AWS、軟體即服務 SaaS) 應用程式、API目的地或其他自訂端點。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說明，請參閱 EventBridge 使用者指南 中的[建立對事件做出反應的規則](#)。

建立事件的事件模式 Transfer Family

當 將事件 Transfer Family 交付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，來判斷事件是否應交付至規則的目標。事件模式符合所需 Transfer Family 事件中的資料。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，來源為 `aws.transfer`。
- (選用) detail-type 包含要比對之事件類型的陣列的屬性。
- (選用) detail 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 的所有事件 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"}]
}
```

下列事件模式範例符合使用者的成功SFTP下載 *username*:

```
{
  "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 使用者指南 中的[事件模式](#)。

測試 中 Transfer Family 事件的事件模式 EventBridge

您可以使用 EventBridge 沙盒來快速定義和測試事件模式，而無需完成建立或編輯規則的更廣泛程序。您可以使用沙盒定義事件模式，並使用範例事件來確認模式符合所需的事件。EventBridge 可讓您直接從沙盒使用該事件模式來建立新規則。

如需詳細資訊，請參閱 EventBridge 使用者指南 中的[使用 EventBridge 沙盒測試事件模式](#)。

Amazon EventBridge 許可

Transfer Family 不需要任何額外的許可，即可將事件傳遞至 Amazon EventBridge。

您指定的目標可能需要特定許可或組態。如需針對目標使用特定服務的詳細資訊，請參閱 Amazon EventBridge 使用者指南 中的[Amazon EventBridge 目標](#)。

其他 EventBridge 資源

如需如何使用 EventBridge 處理和管理事件的詳細資訊，請參閱 [Amazon EventBridge 使用者指南](#) 中的下列主題。

- 如需事件匯流排運作方式的詳細資訊，請參閱[Amazon EventBridge 事件匯流排](#)。
- 如需事件結構的資訊，請參閱[事件](#)。

- 如需將事件與規則比對時 EventBridge 要使用的事件模式的相關資訊，請參閱[事件模式](#)。
- 如需建立規則以指定哪些事件 EventBridge 程序的相關資訊，請參閱[規則](#)。
- 如需如何指定傳送 EventBridge 相符事件之服務或其他目的地的相關資訊，請參閱[目標](#)。

Transfer Family 事件詳細資訊參考

AWS 服務中的所有事件都有一組通用的欄位，其中包含事件的中繼資料。這些中繼資料可以包括作為事件來源 AWS 的服務、事件產生的時間、事件發生的帳戶和區域，以及其他。如需這些一般欄位的定義，請參閱 Amazon EventBridge 使用者指南 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。下列參考定義了各種 Transfer Family 事件的詳細資訊欄位。

當您使用 EventBridge 來選取和管理 Transfer Family 事件時，請考慮下列事項：

- 來自的所有事件 source 的欄位 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。

如需建構事件模式以讓規則符合 Transfer Family 事件的相關資訊，請參閱 Amazon EventBridge 使用者指南 中的[事件模式](#)。

如需事件及其 EventBridge 處理方式的詳細資訊，請參閱 Amazon EventBridge 使用者指南 中的[Amazon EventBridge 事件](#)。

主題

- [SFTP、FTPS和 FTP 伺服器事件](#)
- [SFTP 連接器事件](#)
- [AS2 事件](#)

SFTP、FTPS和 FTP 伺服器事件

以下是 SFTP、FTPS和 FTP 伺服器事件的詳細資訊欄位：

- FTP 檔案伺服器下載已完成
- FTP 檔案伺服器下載失敗
- FTP 檔案伺服器上傳已完成
- FTP 檔案伺服器上傳失敗
- FTPS 檔案伺服器下載已完成
- FTPS 檔案伺服器下載失敗
- FTPS 檔案伺服器上傳已完成
- FTPS 檔案伺服器上傳失敗
- SFTP 伺服器檔案下載已完成
- SFTP 伺服器檔案下載失敗
- SFTP 伺服器檔案上傳已完成
- SFTP 伺服器檔案上傳失敗

source 和 detail-type 欄位包含如下，因為其中包含 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 使用者指南 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，該值是先前列出的其中一個 FTPS、SFTP 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，資料包含下列項目：

failure-code

傳輸失敗原因的類別。數值: `PARTIAL_UPLOAD` | `PARTIAL_DOWNLOAD` | `UNKNOWN_ERROR`

status-code

傳輸是否成功。值：`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

涉及傳輸之用戶端的 IP 地址

failure-message

對於失敗的傳輸，傳輸失敗的原因詳細資訊。

end-timestamp

為了成功傳輸，檔案完成處理時的時間戳記。

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

執行傳輸的使用者。

session-id

傳輸工作階段的唯一識別符。

start-timestamp

若要成功傳輸，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（正在使用 Amazon EFS 的儲存體）。

```
{
  "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 事件，其中在FTP伺服器上成功完成上傳（Amazon S3 正在使用的儲存體）。

```
{  
  "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訊欄位：

- SFTP 連接器檔案傳送已完成
- SFTP 連接器檔案傳送失敗
- SFTP 連接器檔案擷取已完成
- SFTP 連接器檔案擷取失敗

source 和 detail-type 欄位包含如下，因為其中包含 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 使用者指南 中的[事件結構參考](#)。

```
{
  . . . ,
  "detail-type": "string",
  "source": "aws.transfer",
  . . . ,
  "detail": {
    "operation" : "string",
    "connector-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",
    "bytes" : "number",
    "local-file-location" : {
      "domain" : "string",
      "bucket" : "string",
      "key" : "string"
    },
  },
}
```

detail-type

識別事件的類型。

對於此事件，該值是先前列出的SFTP連接器事件名稱之一。

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，資料包含下列項目：

`operation`

`StartFileTransfer` 請求是傳送還是擷取檔案。值：SEND|RETRIEVE。

`connector-id`

正在使用之SFTP連接器的唯一識別符。

`transfer-id`

傳輸事件的唯一識別符（`StartFileTransfer`請求）。

`file-transfer-id`

要傳輸之檔案的唯一識別碼。

`url`

URL 合作夥伴AS2或SFTP端點的。

`file-path`

正在傳送或擷取的位置和檔案。

`status-code`

傳輸是否成功。值：FAILED | COMPLETED。

`failure-code`

對於失敗的傳輸，傳輸失敗的原因代碼。

`failure-message`

對於失敗的傳輸，傳輸失敗的原因詳細資訊。

`start-timestamp`

若要成功傳輸，檔案處理開始時的時間戳記。

`end-timestamp`

若要成功傳輸，檔案處理完成時的時間戳記。

`local-directory-path`

對於RETRIEVE請求，放置擷取檔案的位置。

remote-directory-path

對於SEND請求，將檔案放置在合作夥伴SFTP伺服器上的檔案目錄。這是RemoteDirectoryPath使用者傳遞給StartFileTransfer請求的值。您可以在合作夥伴的伺服器上指定預設目錄SFTP。如果是這樣，此欄位為空。

bytes

要傳輸的位元組數。失敗傳輸的值為 0。

local-file-location

此參數包含 AWS 儲存檔案位置的詳細資訊。

domain

使用的儲存體。目前，唯一的值是 S3。

bucket

Amazon S3 中物件的容器。

key

指派給 Amazon S3 中物件的名稱。

Example SFTP 連接器檔案傳送失敗範例事件

下列範例顯示 SFTP 連接器嘗試將檔案傳送至遠端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的範例事件

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"
    }
  }
}
```

AS2 事件

以下是AS2事件的詳細資訊欄位：

- AS2 承載接收已完成
- AS2 承載接收失敗
- AS2 承載傳送已完成
- AS2 承載傳送失敗
- AS2 MDN 接收已完成
- AS2 MDN 接收失敗
- AS2 MDN 傳送已完成
- AS2 MDN 傳送失敗

source 和 detail-type 欄位包含如下，因為其中包含 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 使用者指南 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，該值是先前列出的AS2事件之一。

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，它也會識別MDN檔案的儲存貯體和金鑰。

file-bucket

Amazon S3 中物件的容器。

file-key

指派給 Amazon S3 中物件的名稱。

json-bucket

對於 COMPLETED或 FAILED傳輸，JSON檔案的容器。

json-key

對於 COMPLETED或 FAILED傳輸，指派給 Amazon S3 中JSON檔案的名稱。

mdn-bucket

對於MDN事件，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，訊息處置的文字描述。

mdn-message-id

對於MDN事件，MDN訊息的唯一 ID。

disposition

對於MDN事件，處置的類別。

bytes

訊息中的位元組數。

as2-from

傳送訊息的交易AS2合作夥伴。

as2-message-id

要傳輸之AS2訊息的唯一識別碼。

as2-to

接收訊息的交易AS2合作夥伴。

connector-id

對於從 Transfer Family 伺服器傳送至交易合作夥伴AS2的訊息，使用AS2連接器的唯一識別符。

client-ip

對於伺服器事件（從交易合作夥伴傳輸到 Transfer Family 伺服器），涉及傳輸之用戶端的 IP 地址。

agreement-id

對於伺服器事件，則為AS2協議的唯一識別符。

server-id

對於伺服器事件，只有 Transfer Family 伺服器的唯一 ID。

requester-file-name

對於承載事件，傳輸期間所接收檔案的原始名稱。

message-subject

訊息主旨的文字描述。

start-timestamp

若要成功傳輸，檔案處理開始時的時間戳記。

end-timestamp

若要成功傳輸，檔案處理完成時的時間戳記。

status-code

對應AS2訊息傳輸程序狀態的程式碼。有效值：COMPLETED | FAILED | PROCESSING。

failure-code

對於失敗的傳輸，傳輸失敗原因的類別。

failure-message

對於失敗的傳輸，傳輸失敗的原因詳細資訊。

transfer-id

傳輸事件的唯一識別符。

Example AS2 承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

的雲端安全 AWS 是最高優先順序。身為 AWS 客戶，您受益於資料中心和網路架構，這些架構是為了滿足最安全敏感組織的需求而建置。

安全是 AWS 和 之間的共同責任。[共同責任模型](#) 將此描述為雲端的安全和雲端內的安全：

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

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

使用 時的合規責任 AWS 服務 取決於資料的敏感度、您公司的合規目標，以及適用的法律和法規。AWS 提供下列資源以協助合規：

- [安全與合規快速入門指南](#) – 這些部署指南討論架構考量，並提供以 AWS 安全與合規為重點的基準環境部署步驟。
- [Amazon Web Services 上HIPAA安全和合規的架構](#) – 本白皮書說明了公司如何使用 AWS 來建立 HIPAA符合 資格的應用程式。

Note

並非所有 AWS 服務 都HIPAA符合資格。如需詳細資訊，請參閱[HIPAA合格服務參考](#)。

- [AWS 合規資源](#) – 此工作手冊和指南集可能適用於您的產業和位置。
- [AWS 客戶合規指南](#) – 透過合規的角度了解共同的責任模型。本指南摘要說明跨多個架構（包括國家標準和技術研究所（）NIST、支付卡產業安全標準委員會（PCI）和國際標準化組織（ISO））保護 AWS 服務 指南並映射至安全控制的最佳實務。
- AWS Config 開發人員指南中的[使用規則評估資源](#) – AWS Config 服務會評估資源組態是否符合內部實務、產業準則和法規。
- [AWS Security Hub](#) – 這 AWS 服務 可讓您全面檢視 內的安全狀態 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱 [Security Hub controls reference](#)。
- [AWS Audit Manager](#) – 這 AWS 服務 可協助您持續稽核 AWS 用量，以簡化您管理風險的方式，以及遵守法規和業界標準的方式。

本文件可協助您了解如何在使用時套用共同的責任模型 AWS Transfer Family。下列主題說明如何設定 AWS Transfer Family 以符合您的安全和合規目標。您也會了解如何使用 AWS 其他服務來協助您監控和保護 AWS Transfer Family 資源。

主題

- [的安全政策 AWS Transfer Family](#)
- [搭配使用混合後量子金鑰交換 AWS Transfer Family](#)
- [中的資料保護 AWS Transfer Family](#)
- [的身分和存取管理 AWS Transfer Family](#)
- [的合規驗證 AWS Transfer Family](#)
- [中的復原能力 AWS Transfer Family](#)
- [中的基礎設施安全 AWS Transfer Family](#)
- [新增 Web 應用程式防火牆](#)
- [預防跨服務混淆代理人](#)
- [AWS Transfer Family 的受管政策](#)

的安全政策 AWS Transfer Family

中的伺服器安全政策 AWS Transfer Family 可讓您限制與伺服器相關聯的一組密碼編譯演算法（訊息驗證碼（MACs）、金鑰交換（KEXs）和密碼套件）。如需支援的密碼編譯演算法清單，請參閱 [密碼編譯演算法](#)。如需支援與伺服器主機金鑰和服務受管使用者金鑰搭配使用的金鑰演算法清單，請參閱 [使用者和伺服器金鑰支援的演算法](#)。

Note

我們強烈建議將您的伺服器更新為最新的安全政策。我們最新的安全政策為預設值。任何使用 CloudFormation 和建立 Transfer Family 伺服器的客戶都會自動指派最新的政策。如果您擔心用戶端相容性，請明確陳述您希望在建立或更新伺服器時使用的安全政策，而不是使用預設政策，這些政策可能會變更。

若要變更伺服器的安全政策，請參閱 [編輯安全政策](#)。

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、合規的受管檔案傳輸解決方案](#)。

主題

- [密碼編譯演算法](#)
- [TransferSecurityPolicy-2024 年 1 月](#)
- [TransferSecurityPolicy-2023 年 5 月](#)
- [TransferSecurityPolicy-2022 年 3 月](#)
- [TransferSecurityPolicy-2020 年 6 月](#)
- [TransferSecurityPolicy-2018 年 11 月](#)
- [TransferSecurityPolicy-FIPS-2024 年 1 月](#)
- [TransferSecurityPolicy-FIPS-2023 年 5 月](#)
- [TransferSecurityPolicy-FIPS-2020 年 6 月](#)
- [發佈 Quantum 安全政策](#)

Note

TransferSecurityPolicy-2024-01 是使用主控台、API或 建立伺服器時連接至伺服器的預設安全政策CLI。

密碼編譯演算法

對於主機金鑰，我們支援下列演算法：

- rsa-sha-256
- rsa-sha-512
- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384
- ecdsa-sha2-nistp512
- ssh-ed25519

此外，2018 和 2020 安全政策允許 ssh-rsa。

Note

請務必了解RSA金鑰類型 — 永遠是 `ssh-rsa` — 與RSA主機金鑰演算法之間的區別，而主機金鑰演算法可以是任何支援的演算法。

以下是每個安全政策支援的密碼編譯演算法清單。

- Note**
- 在下表和政策中，請注意下列演算法類型的使用方式。
- SFTP 伺服器僅在 `SshCiphers`、`SshKexs`和 `SshMacs`區段中使用演算法。
 - FTPS 伺服器僅在 `TlsCiphers`區段中使用演算法。
 - FTP 伺服器，因為它們不使用加密，所以請勿使用任何這些演算法。

安全政策	2024-01	2023-05	2022-03	2020-06	FIPS-2024 年 1 月	FIPS-2023 年 5 月	FIPS-2020 年 6 月	2018-11
SshCiphers								
aes128-ctr	◆			◆	◆		◆	◆
aes128-gcm@openssh.com	◆	◆	◆	◆	◆	◆	◆	◆
aes192-ctr	◆	◆	◆	◆	◆	◆	◆	◆
aes256-ctr	◆	◆	◆	◆	◆	◆	◆	◆
aes256-gcm	◆	◆	◆	◆	◆	◆	◆	◆

安全政策	2024-01	2023-05	2022-03	2020-06	FIPS-2024 年 1 月	FIPS-2023 年 5 月	FIPS-2020 年 6 月	2018-11
m@openssh.com								
chacha20-poly1305@openssh.com				◆				◆
SshKexs								
curve25519-sha256	◆	◆	◆					◆
curve25519-sha256@libssh.org	◆	◆	◆					◆
diffie-hellman-group14 軸1								◆
diffie-hellman-group14-sha256				◆		◆		◆
diffie-hellman-group16-sha512	◆	◆	◆	◆	◆	◆	◆	◆

安全政策	2024-01	2023-05	2022-03	2020-06	FIPS-2024 年 1 月	FIPS-2023 年 5 月	FIPS-2020 年 6 月	2018-11
diffie-hellman-group18-sha512	◆	◆	◆	◆	◆	◆	◆	◆
diffie-hellman-group-exchange-sha256		◆	◆	◆		◆	◆	◆
ecdh-nist-p256-kurve-512r3-sha256-d00@openquantumsafe.org	◆				◆			
ecdh-nist-p384-kurve-768r3-sha384-d00@openquantumsafe.org	◆				◆			

安全政策	2024-01	2023-05	2022-03	2020-06	FIPS-2024 年 1 月	FIPS-2023 年 5 月	FIPS-2020 年 6 月	2018-11
ecdh-nistp521-kyber-1024r3-sha512-d00@openquantumsafe.org	◆				◆			
ecdh-sha2-nistp256	◆			◆	◆		◆	◆
ecdh-sha2-nistp384	◆			◆	◆		◆	◆
ecdh-sha2-nistp521	◆			◆	◆		◆	◆
x25519-kyber-512r3-sha256-d00@amazon.com	◆							
SshMacs								

安全政策	2024-01	2023-05	2022-03	2020-06	FIPS-2024 年 1 月	FIPS-2023 年 5 月	FIPS-2020 年 6 月	2018-11
hmac-sha1								◆
hmac-sha1-etm@openssh.com								◆
hmac-sha2-256			◆	◆			◆	◆
hmac-sha2-256-etm@openssh.com	◆	◆	◆	◆	◆	◆	◆	◆
hmac-sha2-512			◆	◆			◆	◆
hmac-sha2-512-etm@openssh.com	◆	◆	◆	◆	◆	◆	◆	◆
umac-128-etm@openssh.com				◆				◆

安全政策	2024-01	2023-05	2022-03	2020-06	FIPS-2024 年 1 月	FIPS-2023 年 5 月	FIPS-2020 年 6 月	2018-11
umac-128@openssh.com				◆				◆
umac-64-etm@openssh.com								◆
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	◆	◆	◆	◆	◆	◆	◆	◆

安全政策	2024-01	2023-05	2022-03	2020-06	FIPS-2024 年 1 月	FIPS-2023 年 5 月	FIPS-2020 年 6 月	2018-11
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	◆	◆	◆	◆	◆	◆	◆	◆
TLS_RSA_WITH_AES_128_CBC_SHA256								◆
TLS_RSA_WITH_AES_256_CBC_SHA256								◆

TransferSecurityPolicy-2024 年 1 月

下列顯示 TransferSecurityPolicy-2024-01 安全政策。

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

```
}  
}
```

TransferSecurityPolicy-2023 年 5 月

以下顯示 TransferSecurityPolicy-2023-05 安全政策。

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

TransferSecurityPolicy-2022 年 3 月

下列顯示 TransferSecurityPolicy-2022-03 安全政策。

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

TransferSecurityPolicy-2020 年 6 月

以下顯示 TransferSecurityPolicy-2020-06 安全政策。


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

TransferSecurityPolicy-2018 年 11 月

以下顯示 TransferSecurityPolicy-2018-11 安全政策。

```
{
  "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"
  ]
}
}

```

TransferSecurityPolicy-FIPS-2024 年 1 月

下列顯示 TransferSecurityPolicy-FIPS-2024-01 安全政策。

Note

FIPS 服務端點和 TransferSecurityPolicy-FIPS-2024-01 安全政策僅適用於某些 AWS 區域。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-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"
    ]
}

```

TransferSecurityPolicy-FIPS-2023 年 5 月

的 FIPS 憑證詳細資訊 AWS Transfer Family 請參閱 <https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search/all>

以下顯示 TransferSecurityPolicy-FIPS-2023-05 安全政策。

Note

FIPS 服務端點和 TransferSecurityPolicy-FIPS-2023-05 安全政策僅適用於某些 AWS 區域。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"
    ]
}

```

TransferSecurityPolicy-FIPS-2020 年 6 月

的 FIPS 憑證詳細資訊 AWS Transfer Family 請參閱 <https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search/all>

下列顯示 TransferSecurityPolicy-FIPS-2020-06 安全政策。

Note

FIPS 服務端點和 TransferSecurityPolicy-FIPS-2020-06 安全政策僅適用於某些 AWS 區域。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"
  ]
}
}

```

發佈 Quantum 安全政策

此表列出 Transfer Family 後量子安全政策的演算法。這些政策會在 [中詳細說明](#)[搭配 使用混合後量子金鑰交換 AWS Transfer Family](#)。

政策清單遵循資料表。

安全政策	TransferSecurityPolicy-PQ-SH-Experimental-2023-04	TransferSecurityPolicy-PQSS H-FIPS-Experimental-2023-04
SSH ciphers		
aes128-ctr		◆
aes128-gcm@openssh.com	◆	◆
aes192-ctr	◆	◆
aes256-ctr	◆	◆
aes256-gcm@openssh.com	◆	◆
KEXs		
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	◆	
diffie-hellman-group14-sha256		◆
diffie-hellman-group16-sha512	◆	◆
diffie-hellman-group18-sha512	◆	◆
ecdh-sha2-nistp384		◆
ecdh-sha2-nistp521		◆

安全政策	TransferSecurityPolicy-PQ-SH-Experimental-2023-04	TransferSecurityPolicy-PQSSH-FIPS-Experimental-2023-04
diffie-hellman-group-exchange-sha256	◆	◆
ecdh-sha2-nistp256		◆
curve25519-sha256@libssh.org	◆	
curve25519-sha256	◆	
MACs		
hmac-sha2-256-etm@openssh.com	◆	◆
hmac-sha2-256	◆	◆
hmac-sha2-512-etm@openssh.com	◆	◆
hmac-sha2-512	◆	◆
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	◆	◆

安全政策	TransferSecurityPolicy-PQ-S SH-Experimental-2023-04	TransferSecurityPolicy-PQSS H-FIPS-Experimental-2023-04
TLS_ECDHE_RSA_WITH AES_128_GCM_SHA256	◆	◆
TLS_ECDHE_RSA_WITH AES_256_CBC_SHA384	◆	◆
TLS_ECDHE_RSA_WITH AES_256_GCM_SHA384	◆	◆

TransferSecurityPolicy-PQ-SSH-Experimental-2023-04

下列顯示 TransferSecurityPolicy-PQ-SSH-Experimental-2023-04 安全政策。

```
{
  "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"
    ]
}

```

TransferSecurityPolicy-PQSSH-FIPS-Experimental-2023-04

以下顯示 TransferSecurityPolicy-PQ-SSH-FIPS-Experimental-2023-04 安全政策。

```

{
  "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"
    ],
  },
}

```

```
    "SshMac": [
        "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"
    ]
}
```

搭配 使用混合後量子金鑰交換 AWS Transfer Family

AWS Transfer Family 支援 Secure Shell (SSH) 通訊協定的混合後量子金鑰建立選項。需要後量子金鑰建立，因為已經可以記錄網路流量，並儲存它以供未來由稱為store-now-harvest-later攻擊的量子電腦進行解密。

當您連線至 Transfer Family 時，您可以使用此選項，以安全傳輸進出 Amazon Simple Storage Service (Amazon S3) 儲存體或 Amazon Elastic File System (Amazon) 的檔案EFS。中的後量子混合金鑰建立會SSH引入後量子金鑰建立機制，此機制會與傳統金鑰交換演算法搭配使用。SSH 使用傳統密碼套件建立的金鑰可安全使用目前的技術進行暴力攻擊。不過，未來大規模量子運算出現後，傳統加密並不預期會保持安全。

如果您的組織依賴透過 Transfer Family 連線傳遞的資料的長期機密性，您應該考慮在大規模的量子電腦可供使用之前遷移到量子後密碼編譯的計劃。

為了保護今天加密的資料免受潛在的未來攻擊，AWS 正與密碼編譯社群一起參與開發 quantum 抗性或 quantum 後演算法。我們已在 Transfer Family 中實作混合後量子金鑰交換密碼套件，這些套件結合了傳統元素和後量子元素。

這些混合密碼套件可在大多數區域中用於生產工作負載 AWS。不過，由於混合密碼套件的效能特性和頻寬需求與傳統金鑰交換機制不同，我們建議您在 Transfer Family 連線上測試這些套件。

在 Post-Quantum 密碼編譯安全部落格文章中[進一步了解量子後密碼編譯](#)。

內容

- [關於 中的量子後混合金鑰交換 SSH](#)
- [量子後混合金鑰建立如何在 Transfer Family 中運作](#)
 - [為什麼選擇 Kyber ?](#)
 - [量子後混合SSH金鑰交換和密碼編譯要求 \(FIPS 140 \)](#)
- [在 Transfer Family 中測試量子後混合金鑰交換](#)
 - [在SFTP端點上啟用後量子混合金鑰交換](#)
 - [設定支援量子後混合金鑰交換的SFTP用戶端](#)
 - [在 中確認量子後混合金鑰交換 SFTP](#)

關於 中的量子後混合金鑰交換 SSH

Transfer Family 支援量子後混合金鑰交換密碼套件，其同時使用傳統橢圓曲線 Diffie-Hellman (ECDH) 金鑰交換演算法和 CRYSTALS Kyber。Kyber 是 [National Institute for Standards and Technology \(NIST \)](#) 指定為第一個標準量子後金鑰協議演算法的公有金鑰加密和金鑰建立演算法。

用戶端和伺服器仍會進行ECDH金鑰交換。此外，伺服器會封裝用戶端後量子KEM公有金鑰的後量共用秘密，該金鑰會在用戶端的SSH金鑰交換訊息中公告。此策略結合了傳統金鑰交換的高度保證，以及建議的後量子金鑰交換的安全性，有助於確保只要無法破壞 ECDH或後量子共用秘密，交握都會受到保護。

量子後混合金鑰建立如何在 Transfer Family 中運作

AWS 最近宣布支援 中SFTP檔案傳輸中的後量子金鑰交換 AWS Transfer Family。Transfer Family business-to-business使用 SFTP 和其他通訊協定安全地擴展至 AWS 儲存服務的檔案傳輸。SFTP 是檔案傳輸通訊協定 (FTP) 更安全的版本，可透過 執行SSH。Transfer Family 的後量化金鑰交換支援提高透過 進行資料傳輸的安全標準SFTP。

Transfer Family 中的後量子混合金鑰交換SFTP支援包括結合後量子演算法 Kyber-512, Kyber-768 和 Kyber-1024，以及ECDH超過 P256, P384, P521 或 Curve25519 曲線。下列對應的SSH金鑰交換方法會在[後量子混合SSH金鑰交換草稿](#) 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稿朝向標準化發展，或當核准 Kyber NIST 演算法時而變更。

為什麼選擇 Kyber？

AWS 致力於支援標準化且可互操作的演算法。Kyber 是第一個由 Post[NIST-Quantum Cryptography 專案](#)為標準化選取的量子後加密演算法。有些標準主體已將 Kyber 整合到通訊協定中。在某些 AWS API 端點 TLS 中 AWS 已支援 Kyber。

作為此承諾的一部分，AWS 已將提案草案提交至 IETF，以取得量子後密碼編譯，該密碼編譯將 Kyber 與 NIST 核准的曲線結合，例如的 P256SSH。為了協助增強客戶的安全性，在 SFTP 中 AWS 實作和 SSH 遵循該草案的後置金鑰交換。我們計劃支援未來的更新，直到我們的提案被採用 IETF 並成為標準。

新的金鑰交換方法（列於第節[量子後混合金鑰建立如何在 Transfer Family 中運作](#)）可能會隨著草稿朝向標準化發展，或當 NIST 核准 Kyber 演算法時變更。

Note

對於 TLS AWS KMS（請參閱[TLS 搭配使用混合後量子](#)）、和端點，的量子後演算法支援目前可用於中的量子後混合 AWS KMS 金鑰交換。AWS Certificate Manager AWS Secrets Manager API

量子後混合 SSH 金鑰交換和密碼編譯要求（FIPS 140）

對於需要 FIPS 合規的客戶，Transfer Family SSH 會使用 140 認證的開放原始碼密碼編譯程式庫 AWS-LC，在 AWS FIPS 中提供 FIPS 核准的密碼編譯。Transfer Family 中 TransferSecurityPolicy-PQ-SSH-FIPS-Experimental-2023-04 中支援的後量子混合金鑰交換方法根據 [NIST 的 SP 800-56Cr2（第 2 節）](#) 獲得 FIPS 核准。法國的德國聯邦資訊安全辦公室（[BSI](#)）和 Agence nationale de la sécurité des systèmes d'information（[ANSSI](#)）也建議採用此類量子後混合金鑰交換方法。

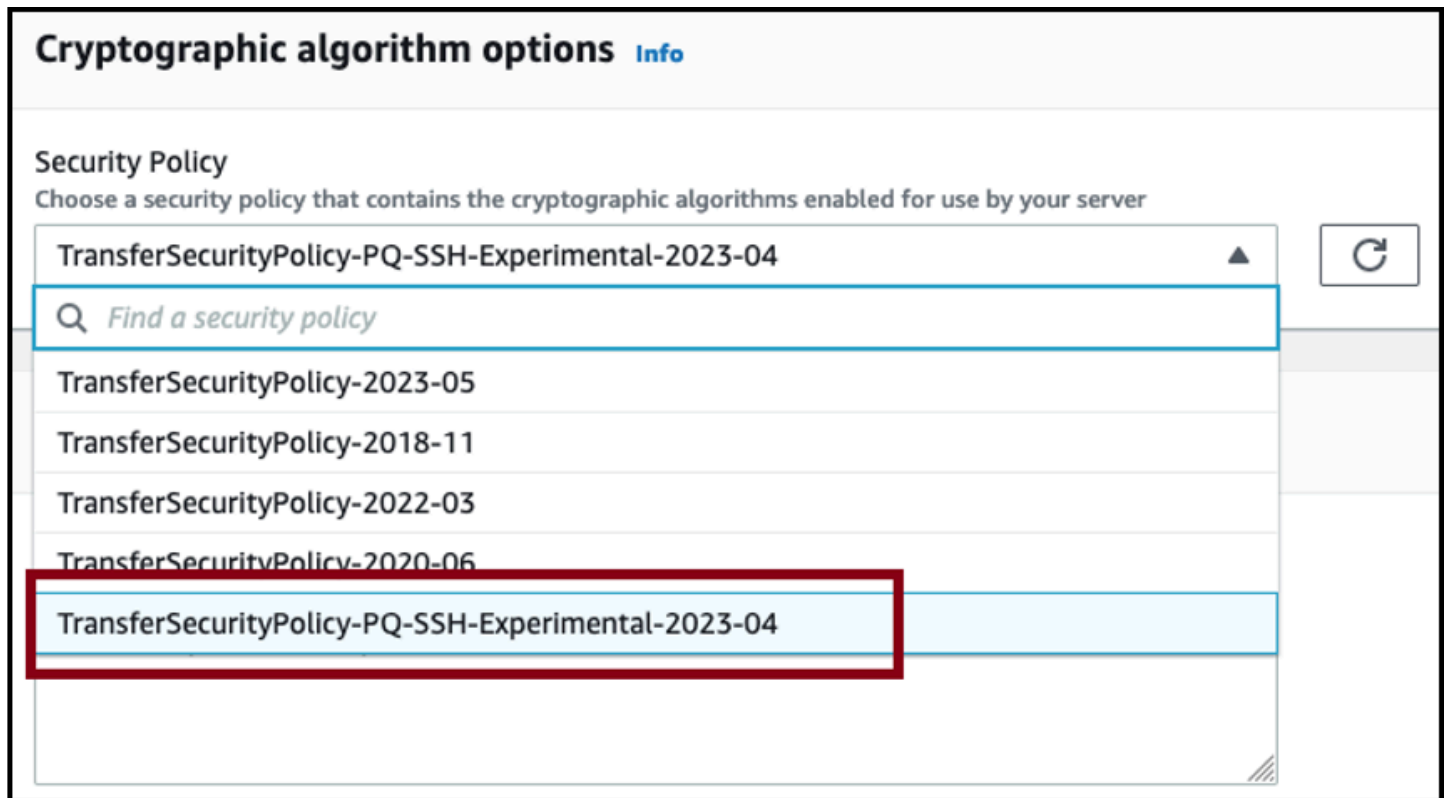
在 Transfer Family 中測試量子後混合金鑰交換

本節說明您測試量子後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金鑰交換](#)。
2. 遵循上述草擬規格中的指引，使用支援量子後混合金鑰交換的SFTP用戶端（例如 [設定支援量子後混合金鑰交換的SFTP用戶端](#)）。
3. 使用 Transfer Family 伺服器傳輸檔案。
4. [在中確認量子後混合金鑰交換 SFTP](#)。

在SFTP端點上啟用後量子混合金鑰交換

您可以在 Transfer Family 中建立新SFTP伺服器端點時選擇SSH政策，或編輯現有SFTP端點中的密碼編譯演算法選項。下列快照顯示您更新SSH政策的 AWS Management Console 範例。



支援後量子金鑰交換SSH的政策名稱為 TransferSecurityPolicy-PQ-SSH-Experimental-2023-04 和 TransferSecurityPolicy-PQ-SSHFIPS-Experimental-2023-04。如需 Transfer Family 政策的詳細資訊，請參閱 [的安全政策 AWS Transfer Family](#)。

設定支援量子後混合金鑰交換的SFTP用戶端

在 SFTP Transfer Family 端點中選取正確的后量子SSH政策後，您可以在 Transfer Family SFTP中實驗後量子值。您可以遵循上述草擬規格中的指引，使用支援量子後混合金鑰交換的SFTP用戶端（例如 [OQS Open SSH](#)）。

OQS OpenSSH 是 OpenSSH 的開放原始碼叉，它 SSH 使用 為 加入保護 quantum 密碼編譯 liboqs。liboqs 是實作 quantum 的開放原始碼 C 程式庫。OQS OpenSSH 和 liboqs 是 Open Quantum Safe (OQS) 專案的一部分。

若要在 Transfer Family SFTP with OQS Open 中測試量子後混合金鑰交換 SSH，您需要如專案的所述建置 OQS OpenSSH [README](#)。建置 OQS Open 之後 SSH，您可以使用 後量混合金鑰交換方法執行範例 SFTP 用戶端以連線至 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，使用您自己的資訊取代下列項目：

- Replace (取代) *username_private_key_PEM_file* 使用 SFTP 使用者的私有金鑰 PEM 編碼檔案
- Replace (取代) *username* 使用 SFTP 使用者名稱
- Replace (取代) *server-id* 使用 Transfer Family 伺服器 ID
- Replace (取代) *region-id* 包含 Transfer Family 伺服器所在的實際區域

在 中確認量子後混合金鑰交換 SFTP

若要確認 SFTP 與 Transfer Family 的 SSH 連線期間已使用後量子混合金鑰交換，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 Open Quantum Safe OpenSSH 用戶端，輸出看起來應該類似於以下內容（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.Transfer.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混合ecdh-nistp384-kyber-768r3-sha384-d00@openquantumsafe.org方法進行，並成功建立SFTP工作階段。

中的資料保護 AWS Transfer Family

AWS [共同責任模型](#)適用於 AWS Transfer Family (Transfer Family) 中的資料保護。如本模型所述，AWS 負責保護執行所有 AWS Cloud 的全域基礎設施。您負責維護在此基礎設施上託管內容的控制權。此內容包含您使用之 AWS 服務的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱[資料隱私權 FAQ](#)。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。

為了資料保護目的，我們建議您保護 AWS 帳戶憑證，並使用 AWS Identity and Access Management () 設定個別使用者帳戶 IAM。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：

- 對每個帳戶使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源通訊。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控制項。
- 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 FIPS 存取 AWS 時需要 140-2 個經過驗證的密碼編譯模組 API，請使用 FIPS 端點。如需可用 FIPS 端點的詳細資訊，請參閱 [聯邦資訊處理標準 \(FIPS \) 140-2](#)。

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 Name (名稱) 欄位。這包括當您使用主控台、或 使用 Transfer Family API AWS CLI 或其他 AWS 服務時 AWS SDKs。您在 Transfer Family 服務組態或其他服務組態中輸入的任何組態資料，都可能被擷取以包含在診斷日誌中。當您將 URL 提供給外部伺服器時，請勿在 中包含憑證資訊，URL 以驗證您對該伺服器的請求。

相反地，從上傳和下載操作進出 Transfer Family 伺服器的資料會被視為完全私有，絕不存在於加密通道之外，例如 SFTP 或 FTPS 連線。只有授權人員才能存取此資料。

主題

- [Amazon S3 中的資料加密](#)
- [金鑰管理](#)

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。物件使用伺服器端加密搭配 Amazon S3 受管金鑰 (SSE-S3) 或 AWS Key Management Service (AWS KMS) 受管金鑰 (SSE-) 進行加密 KMS。如需伺服器端加密的相關資訊，請參閱 Amazon Simple Storage Service 使用者指南 中的 [使用伺服器端加密保護資料](#)。

下列步驟說明如何加密 中的資料 AWS Transfer Family。

若要允許 加密 AWS Transfer Family

1. 啟用 Amazon S3 儲存貯體的預設加密。如需指示，請參閱 [Amazon S3 Simple Storage Service 使用者指南 中的 S3 儲存貯體的 Amazon S3 預設加密](#)。
2. 更新連接至使用者的 AWS Identity and Access Management (IAM) 角色政策，以授予所需的 AWS Key Management Service (AWS KMS) 許可。
3. 如果您為使用者使用工作階段政策，則工作階段政策必須授予必要的 AWS KMS 許可。

下列範例顯示IAM政策，在 AWS Transfer Family 搭配啟用 AWS KMS 加密的 Amazon S3 儲存貯體使用時，授予所需的最低許可。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

您在此政策中指定的KMS金鑰 ID 必須與步驟 1 中為預設加密指定的金鑰 ID 相同。金鑰政策中 AWS KMS 必須允許根或使用者使用IAM的角色。如需 AWS KMS 金鑰政策的相關資訊，請參閱 AWS Key Management Service 開發人員指南 [中的使用金鑰政策 AWS KMS](#)。

金鑰管理

在本節中，您可以找到有關SSH金鑰的資訊，包括如何產生金鑰以及如何輪換金鑰。如需使用 Transfer Family AWS Lambda 搭配 管理金鑰的詳細資訊，請參閱部落格文章[使用 A AWS Transfer Family 和 啟用使用者自助式金鑰管理 AWS Lambda](#)。

 Note

AWS Transfer Family 接受 RSA、ECDSA和 ED25519金鑰。

本節也說明如何產生和管理 Pretty Good Privacy (PGP) 金鑰。

主題

- [使用者和伺服器金鑰支援的演算法](#)
- [為受服務管理的使用者產生SSH金鑰](#)
- [輪換SSH索引鍵](#)
- [產生和管理PGP金鑰](#)
- [支援的PGP用戶端](#)

使用者和伺服器金鑰支援的演算法

使用者和伺服器金鑰對支援下列金鑰演算法 AWS Transfer Family。

 Note

如需在工作流程中使用 與PGP解密搭配使用的演算法，請參閱[PGP金鑰對支援的演算法](#)。

- 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

我們支援 `ssh-rsa` SHA1 的舊版安全政策。如需詳細資訊，請參閱 [密碼編譯演算法](#)。

為受服務管理的使用者產生SSH金鑰

您可以設定伺服器，使用服務受管身分驗證方法驗證使用者，其中使用者名稱和SSH金鑰存放在服務中。使用者的公有SSH金鑰會以使用者屬性的形式上傳到伺服器。伺服器會將此金鑰用作標準金鑰型身分驗證程序的一部分。每個使用者可以在具有個別伺服器的檔案中擁有多個公有SSH金鑰。如需每個使用者可儲存的金鑰數量限制，請參閱 中的 [AWS Transfer Family 端點和配額](#) Amazon Web Services 一般參考。

作為服務受管身分驗證方法的替代方案，您可以使用自訂身分提供者或 來驗證使用者 AWS Directory Service for Microsoft Active Directory。如需詳細資訊，請參閱 [使用自訂身分提供者](#) 或 [使用 AWS Directory Service 身分提供者](#)。

伺服器只能使用一種方法（服務受管、目錄服務或自訂身分提供者）來驗證使用者，且在建立伺服器後無法變更該方法。

主題

- [在 macOS、Linux 或 Unix 上建立SSH金鑰](#)
- [在 Microsoft Windows 上建立SSH金鑰](#)
- [將SSH2公有金鑰轉換為PEM格式](#)

在 macOS、Linux 或 Unix 上建立SSH金鑰

在 macOS、Linux 或 Unix 作業系統上，您可以使用 `ssh-keygen` 命令來建立SSH公有金鑰和SSH私有金鑰，也稱為金鑰對。

在 macOS、Linux 或 Unix 作業系統上建立SSH金鑰

1. 在 macOS、Linux 或 Unix 作業系統上，開啟命令終端機。
2. AWS Transfer Family 接受 RSA-、ECDSA- 和 ED25519 格式化金鑰。根據您要產生的金鑰對類型選擇適當的命令。

Note

在下列範例中，我們不會指定密碼片語：在此情況下，該工具會要求您輸入密碼片語，然後重複進行驗證。建立複雜密碼可為私有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：如果忘記密碼，則必須建立新的金鑰。

不過，如果您要產生伺服器主機金鑰，則必須在命令中指定 `-N ""` 選項（或在出現提示時按 **Enter** 兩次）來指定空密碼，因為 Transfer Family 伺服器無法在啟動時請求密碼。

- 若要產生 RSA 4096 位元金鑰對：

```
ssh-keygen -t rsa -b 4096 -f key_name
```

- 若要產生 ECDSA 521 位元金鑰對（ECDSA 位元大小為 256、384 和 521）：

```
ssh-keygen -t ecdsa -b 521 -f key_name
```

- 若要產生 ED25519 金鑰對：

```
ssh-keygen -t ed25519 -f key_name
```

Note

key_name 是 SSH 金鑰對檔案名稱。

下列顯示 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:
SHA256:8tDDwPmanTFcEzjTwPGETVW0GW1nVz+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金鑰對現已準備就緒，可供使用。請依照步驟 3 和 4 來存放受服務管理的使用者的SSH公有金鑰。這些使用者在 Transfer Family 伺服器端點上傳輸檔案時，會使用 金鑰。

3. 導覽至 `key_name.pub` 檔案並開啟。
4. 複製文字並將其貼到服務受管使用者的SSH公有金鑰中。
 - a. 在 開啟 AWS Transfer Family 主控台 <https://console.aws.amazon.com/transfer/>，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. 選取您要為其新增公有金鑰的使用者。
 - d. 在SSH公有金鑰窗格中，選擇新增SSH公有金鑰。

The screenshot shows the 'User: OneUser' configuration page in the AWS Transfer Family console. The breadcrumb trail is 'Transfer Family > Servers > s-[server icon] > User: OneUser'. At the top right are 'View logs' and 'Delete' buttons. The main section is titled 'User configuration' with an 'Edit' button. It is divided into two columns. The left column contains 'Role' (with a link to the role) and 'Posix Profile' (showing User ID: 2001, Group ID: 2001, and Secondary Group IDs: -). The right column contains 'Policy' (with a 'View' button) and 'Home directory' (showing '/fs-[path]' and 'Restricted'). Below this is the 'SSH public keys (1)' section, which includes a 'Delete' button, an 'Add SSH public key' button, and a pagination control showing '1'. A table below lists the keys with columns for 'Date imported' and 'Fingerprint'. One key is listed with a date of '6/14/2022, 12:53:34 PM' and a SHA256 fingerprint.

Transfer Family > Servers > s-[server icon] > User: OneUser

User: OneUser

[View logs](#) [Delete](#)

User configuration [Edit](#)

Role [role icon] Role	Policy View
Posix Profile User ID 2001 Group ID 2001 Secondary Group IDs -	Home directory /fs-[path] Restricted

SSH public keys (1) [Delete](#) [Add SSH public key](#)

< 1 >

☐	Date imported	Fingerprint
☐	6/14/2022, 12:53:34 PM	SHA256-[fingerprint]

- e. 將產生的公有金鑰文字貼到SSH公有金鑰文字方塊，然後選擇新增金鑰。

The screenshot shows the 'Add key' dialog in the AWS Transfer Family console. The breadcrumb trail is 'Transfer Family > Servers > s-[server icon] > OneUser > Add key'. The main heading is 'Add key'. Below it is a section titled 'SSH public keys'. Under this section, there is a link for 'SSH public key Info' and a prompt 'Paste the contents of SSH public key'. A large text input field is provided with the placeholder text 'Enter SSH public key'. At the bottom right of the dialog are 'Cancel' and 'Add key' buttons.

Transfer Family > Servers > s-[server icon] > OneUser > Add key

Add key

SSH public keys

[SSH public key Info](#)
Paste the contents of SSH public key

Enter SSH public key

[Cancel](#) [Add key](#)

新的金鑰會列在SSH公有金鑰窗格中。

SSH public keys (2)			Delete	Add SSH public key
			< 1 >	
☐	Date imported	Fingerprint		
☐	6/14/2022, 12:53:34 PM	SHA256:-		
☐	10/20/2022, 4:26:51 PM	SHA256:-		

在 Microsoft Windows 上建立SSH金鑰

Windows 使用略有不同的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 P uTTYgen 以適當的格式建立SSH金鑰對。您也可以使用 P uTTYgen 將產生的私有金鑰轉換為 ssh-keygen .ppk 檔案。

Note

如果您使用非 .ppk 格式的私有金鑰檔案展示 WinSCP，該用戶端會提議將金鑰轉換為 .ppk 格式。

如需在 Windows uTTYgen 上使用 P 建立SSH金鑰的教學課程，請參閱 [SSH.com 網站](https://www.ssh.com)。

將SSH2公有金鑰轉換為PEM格式

AWS Transfer Family 僅接受PEM格式化公有金鑰。如果您有SSH2公有金鑰，則需要將其轉換。SSH2 公有金鑰的格式如下：

```

---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-20160402"
AAAAB3NzaC1yc2EAAAABJQAAAQEAiL0jjDdFqK/kYThqKt7THrjABTPWvXmB3URI
:
:
---- END SSH2 PUBLIC KEY ----

```

PEM 公有金鑰具有下列格式：

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAA...
```

執行下列命令，將SSH2格式化的公有金鑰轉換為PEM格式化的公有金鑰。Replace (取代) *ssh2-key* 您的SSH2金鑰名稱，以及 *PEM-key* 您的PEM金鑰名稱。


```
ssh-keygen -i -f ssh2-key.pub > PEM-key.pub
```

轉換SSH索引鍵

為了安全起見，我們建議您轉換SSH金鑰的最佳實務。通常，此轉換會指定為安全政策的一部分，並以某些自動化方式實作。根據安全層級，對於高度敏感的通訊，SSH金鑰對只能使用一次。這樣做可消除任何因存放金鑰所帶來的風險。不過，儲存SSH憑證一段時間，並設定不會對使用者造成過度負擔的間隔比較常見。常見的間隔是三個月。

有兩種方法可用來執行SSH金鑰轉換：

- 在主控台上，您可以上傳新的SSH公有金鑰並刪除現有的SSH公有金鑰。
- 您可以使用 更新現有使用者API，方法是使用 [DeleteSshPublicKey](#) API刪除使用者的 Secure Shell (SSH) 公有金鑰，以及 [ImportSshPublicKey](#) API將新的 Secure Shell (SSH) 公有金鑰新增至使用者帳戶。

Console

在主控台中執行金鑰轉換

1. 在 開啟 AWS Transfer Family 主控台 <https://console.aws.amazon.com/transfer/>。
2. 導覽至伺服器頁面。
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 下，選取您要轉換其SSH公有金鑰的使用者核取方塊，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訊頁面，然後選擇新增SSH公有金鑰以查看新增金鑰頁面。

5. 輸入新的SSH公有金鑰，然後選擇新增金鑰。

Important

SSH 公有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，金鑰以 `ecdsa-sha2-nistp256`、`ecdsa-sha2-nistp384`或開頭`ecdsa-sha2-nistp521`，取決於您產生的金鑰大小。開始字串後面接著 *string*，類似於其他金鑰類型。

您會返回使用者詳細資訊頁面，而您剛輸入的新SSH公有金鑰會顯示在SSH公有金鑰區段中。

6. 選取您要刪除之舊金鑰的核取方塊，然後選擇刪除。
7. 輸入單字 來確認刪除操作`delete`，然後選擇刪除。

API

若要使用 執行金鑰輪換 API

1. 在 macOS、Linux 或 Unix 作業系統上，開啟命令終端機。
2. 輸入下列命令，擷取您要刪除的SSH金鑰。若要使用此命令，*serverID*請以 Transfer Family 伺服器的伺服器 ID 取代，並以*username*您的使用者名稱取代。

```
aws transfer describe-user --server-id='serverID' --user-name='username'
```

命令會傳回使用者的詳細資訊。複製 "SshPublicKeyId": 欄位的內容。稍後，您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。若要使用此命令，*serverID*請以 Transfer Family 伺服器的伺服器 ID 取代，*username*以使用者名稱取代，並以新公有金鑰的*public-key*指紋取代。

```
aws transfer import-ssh-public-key --server-id='serverID' --user-name='username'  
  --ssh-public-key-body='public-key'
```

如果命令成功，則不會傳回輸出。

4. 最後，執行下列命令來刪除舊金鑰。若要使用此命令，*serverID*請以 Transfer Family 伺服器的伺服器 ID 取代，*username*以使用者名稱取代，並以您在此程序的步驟 2 中複製的*keyID-from-step-2*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. (選用) 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

您可以使用 Pretty Good Privacy (PGP) 解密搭配 Transfer Family 與工作流程處理的檔案。若要在工作流程步驟中使用解密，您必須提供PGP金鑰。

AWS 儲存部落格有一個文章，說明如何使用 [PGP和 加密和解密檔案、加密和解密檔案 AWS Transfer Family](#)。

產生PGP金鑰

您用來產生PGP金鑰的方法取決於您的作業系統和您正在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來安裝 gpg。根據您的 Linux 發行版本，下列其中一個命令應該適用於您。

```
sudo yum install gnupg
```

```
sudo apt-get install gnupg
```

對於 Windows 或 macOS，您可以從 <https://gnupg.org/download/> 下載所需內容。

安裝PGP金鑰產生器軟體後，請執行 `gpg --full-gen-key`或 `gpg --gen-key`命令以產生金鑰對。

Note

如果您使用的是 2GnuPG.3.0 版或更新版本，則必須執行 `gpg --full-gen-key`。當提示要建立的金鑰類型時，請選擇 RSA或 ECC。不過，如果您選擇 ECC，請務必選擇 NIST 或 BrainPool 橢圓曲線。請勿選擇 Curve 25519。

PGP金鑰對支援的演算法

PGP 金鑰對支援下列演算法：

- RSA
- 高端
- ECC:
 - NIST
 - BrainPool

 Note

不支援 Curve25519 金鑰。

有用的gpg子命令

以下是 的一些實用于命令gpg：

- `gpg --help` – 此命令會列出可用的選項，並可能包含一些範例。
- `gpg --list-keys` – 此命令會列出您已建立的所有金鑰對的詳細資訊。
- `gpg --fingerprint` – 此命令會列出所有金鑰對的詳細資訊，包括每個金鑰的指紋。
- `gpg --export -a user-name` – 此命令會匯出產生金鑰時*user-name*所使用的 金鑰的公有金鑰部分。

管理 PGP 金鑰

若要管理PGP金鑰，您必須使用 AWS Secrets Manager。

 Note

您的秘密名稱包含 Transfer Family 伺服器 ID。這表示在將PGP金鑰資訊存放在 之前，您應該已經識別或建立伺服器 AWS Secrets Manager。

如果您想要為所有使用者使用一個金鑰和密碼片語，您可以將PGP金鑰區塊資訊存放在秘密名稱 `aws/transfer/server-id@pgp-default`，其中 *server-id* 是 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，則會使用此預設金鑰。

或者，您可以為特定使用者建立金鑰。在此情況下，秘密名稱的格式為 `aws/transfer/server-id/user-name`，其中 與執行 Transfer Family 伺服器工作流程的使用者*user-name*相符。

Note

每個 Transfer Family 伺服器、每個使用者最多可以存放 3 個PGP私有金鑰。

設定PGP金鑰以搭配解密使用

1. 根據您GPG使用的 版本，執行下列其中一個命令來產生不使用 Curve 25519 加密演算法的PGP金鑰對。

- 如果您使用的是 2.3.0 **GnuPG**版或更新版本，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**，您可以選擇橢圓曲線**BrainPool**的 **NIST**或。如果您gpg --gen-key改為執行，則會建立使用 ECC Curve 25519 加密演算法的金鑰對，我們目前不支援該PGP金鑰。

- 對於 2.3.0 **GnuPG**之前的 版本，您可以使用下列命令，因為 RSA是預設加密類型。

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

⚠ Important

在金鑰產生過程中，您必須提供密碼和電子郵件地址。請務必記下這些值。在本程序中 AWS Secrets Manager 稍後將金鑰的詳細資訊輸入 時，您必須提供密碼片語。而且，您必須提供相同的電子郵件地址，才能在下一個步驟中匯出私有金鑰。

2. 執行下列命令以匯出私有金鑰。若要使用此命令，請將 取代`private.pgp`為要儲存私有金鑰區塊的檔案名稱，以及`marymajor@example.com`您在產生金鑰對時使用的電子郵件地址。

```
gpg --output private.pgp --armor --export-secret-key marymajor@example.com
```

3. 使用 AWS Secrets Manager 來存放您的PGP金鑰。
 - a. 登入 AWS Management Console 並在 開啟 AWS Secrets Manager 主控台<https://console.aws.amazon.com/secretsmanager/>。
 - b. 在左側導覽窗格中，選擇秘密。

- c. 在秘密頁面上，選擇儲存新的秘密。
- d. 在選擇秘密類型頁面上，針對秘密類型，選取其他類型的秘密。
- e. 在鍵/值對區段中，選擇鍵/值索引標籤。
 - 金鑰 – 輸入 **PGPPrivateKey**。

 Note

您必須確實輸入**PGPPrivateKey**字串：請勿在字元之前或之間新增任何空格。

- 值 – 將私有金鑰的文字貼到值欄位中。您可以在本程序中稍早匯出金鑰時指定的檔案（例如 `private.pgp`）中找到私有金鑰的文字。金鑰開頭為 `-----BEGIN PGP PRIVATE KEY BLOCK-----`，結尾為 `-----END PGP PRIVATE KEY BLOCK-----`。

 Note

請確定文字區塊僅包含私有金鑰，也不包含公有金鑰。

- f. 選取新增列，然後在鍵/值對區段中，選擇鍵/值索引標籤。
 - 金鑰 – 輸入 **PGPPassphrase**。

 Note

您必須確實輸入**PGPPassphrase**字串：請勿在字元之前或之間新增任何空格。

- value – 輸入您在產生PGP金鑰對時使用的密碼片語。

Choose secret type

Secret type [Info](#)

☐ Credentials for Amazon RDS database
 ☐ Credentials for Amazon DocumentDB database
 ☐ Credentials for Amazon Redshift cluster

☐ Credentials for other database
 ☒ Other type of secret
API key, OAuth token, other.

Key/value pairs [Info](#)

Key/value	Plaintext	
PGPPrivateKey	-----BEGIN PGP PRIVATE KEY BLOCK-----	Remove
PGPPassphrase	mypassphrase	Remove
+ Add row		

Encryption key [Info](#)

You can encrypt using the KMS key that Secrets Manager creates or a customer managed KMS key that you create.

[Add new key](#) [🔗](#)

Note

您最多可以新增 3 組金鑰和密碼片語。若要新增第二組，請新增兩列，然後 PGPPassphrase2 輸入 鍵的 PGPPrivateKey2 和 ，然後貼到另一個私有金鑰和密碼片語中。若要新增第三組，金鑰值必須為 PGPPrivateKey3 和 PGPPassphrase3。

- g. 選擇 Next (下一步)。
- h. 在設定秘密頁面上，輸入秘密的名稱和描述。
 - 如果您要建立預設金鑰，亦即任何 Transfer Family 使用者都可以使用的金鑰，請輸入 **aws/transfer/*server-id*/epgp-default**。*server-id* 以包含具有解密步驟之工作流程的伺服器 ID 取代。
 - 如果您要建立金鑰以供特定 Transfer Family 使用者使用，請輸入 **aws/transfer/*server-id*/*user-name***。*server-id* 以包含具有解密步驟之工作流程的伺服器 ID 取代，並以執行工作流程 *user-name* 的使用者名稱取代。*user-name* 會儲存在 Transfer Family 伺服器正在使用的身分提供者中。

- i. 選擇下一步，並接受設定輪換頁面上的預設值。然後選擇下一步。
- j. 在檢閱頁面上，選擇儲存以建立和儲存秘密。

下列螢幕擷取畫面顯示marymajor特定 Transfer Family 伺服器的使用者詳細資訊。此範例顯示三個金鑰及其對應的密碼片語。

The screenshot shows the AWS Secrets Manager console for a secret named `/aws/transfer/s-.../marymajor`. The secret details section shows the encryption key as `aws/secretsmanager`, the secret name as `/aws/transfer/s-.../marymajor`, and the secret ARN as `arn:aws:secretsmanager:us-east-2:...:secret:/aws/transfer/s-.../marymajor-...`. The secret description states: "Contains the PGP secret keys and corresponding passphrases to use for user marymajor on Transfer Family server s-...".

The secret value section shows the secret value in plaintext. It contains a table with two columns: Secret key and Secret value.

Secret key	Secret value
PGPPrivateKey	-----BEGIN PGP PRIVATE KEY BLOCK-----
PGPPassphrase	mypassphrase
PGPPrivateKey2	-----BEGIN PGP PRIVATE KEY BLOCK-----
PGPPassphrase2	mypassphrase2
PGPPrivateKey3	-----BEGIN PGP PRIVATE KEY BLOCK-----
PGPPassphrase3	mypassphrase3

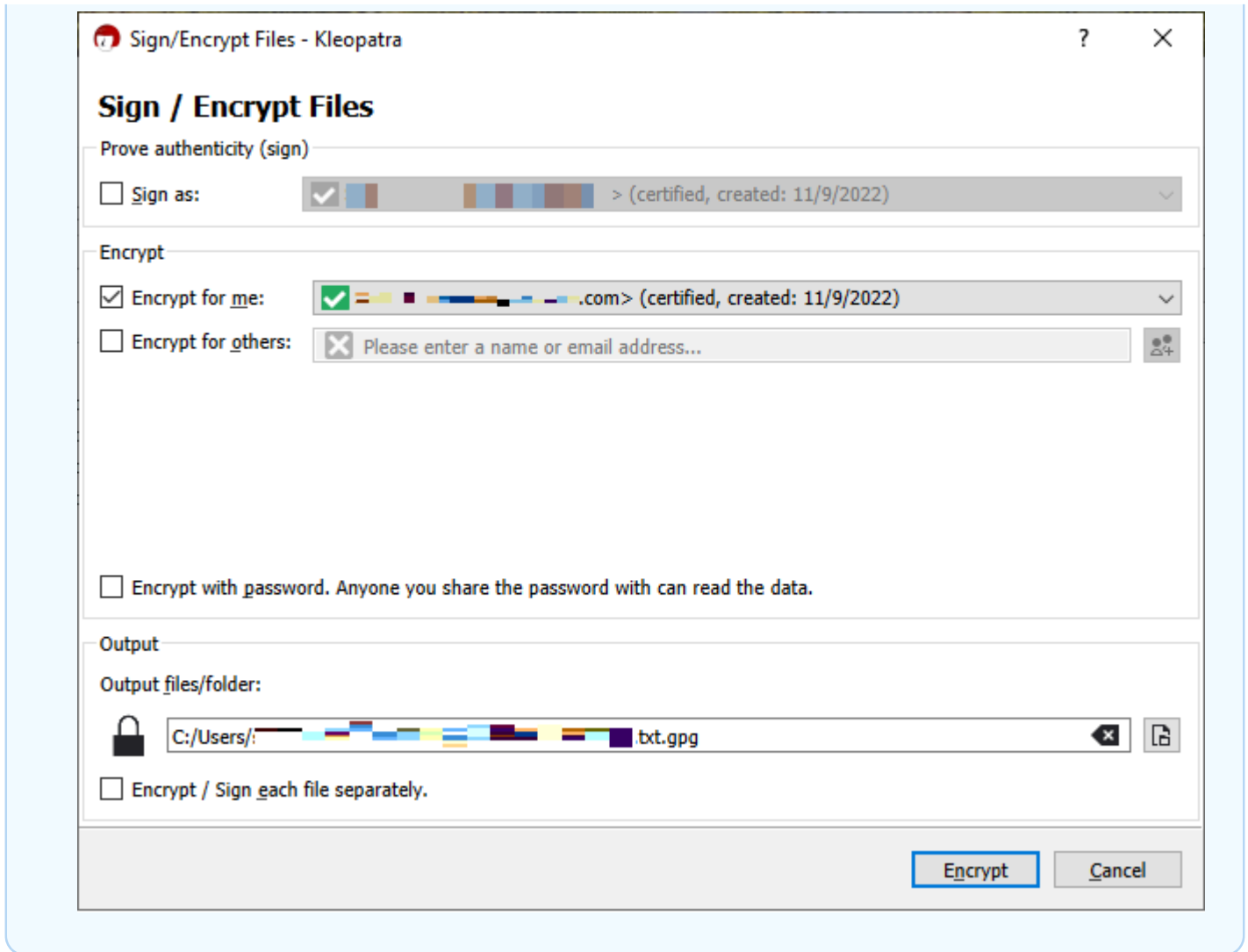
支援的PGP用戶端

下列用戶端已使用 Transfer Family 進行測試，可用於產生PGP金鑰，以及加密您打算使用工作流程解密的檔案。

- Gpg4win + Kleopatra。

Note

當您選取簽署/加密檔案時，請務必清除簽署為的選擇：我們目前不支援簽署加密檔案。



- 主要 GnuPG 版本：2.4、2.3、2.2、2.0 和 1.4。

請注意，其他PGP用戶端可能也適用，但只有此處提到的用戶端已經過 Transfer Family 測試。

的身分和存取管理 AWS Transfer Family

AWS Identity and Access Management (IAM) 是一種 AWS 服務，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員控制誰可以驗證（登入）和授權（具有許可）使用 AWS Transfer Family 資源。IAM 是 AWS 服務 您可以免費使用的。

主題

- [物件](#)
- [使用身分驗證](#)

- [使用政策管理存取權](#)
- [AWS Transfer Family 如何使用 IAM](#)
- [AWS Transfer Family 身分型政策範例](#)
- [AWS Transfer Family 標籤型政策範例](#)
- [對 AWS Transfer Family 身分和存取權進行故障診斷](#)

物件

使用 AWS Identity and Access Management (IAM) 的方式會有所不同，具體取決於您在 中執行的工作 AWS Transfer Family。

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

服務管理員 – 如果您負責公司 AWS Transfer Family 的資源，您可能擁有 的完整存取權 AWS Transfer Family。您的任務是判斷您的服務使用者應該存取哪些 AWS Transfer Family 功能和資源。然後，您必須向IAM管理員提交請求，以變更服務使用者的許可。請檢閱此頁面上的資訊，以了解 的基本概念 IAM。若要進一步了解貴公司如何IAM搭配 使用 AWS Transfer Family，請參閱 [AWS Transfer Family 如何使用 IAM](#)。

IAM 管理員 – 如果您是IAM管理員，您可能想要了解如何撰寫政策以管理 存取權的詳細資訊 AWS Transfer Family。若要檢視您可以在 中使用的以 AWS Transfer Family 身分為基礎的政策範例IAM，請參閱 [AWS Transfer Family 身分型政策範例](#)。

使用身分驗證

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

您可以使用透過身分來源提供的憑證，以聯合身分 AWS 身分登入 。 AWS IAM Identity Center (IAM Identity Center) 使用者、您公司的單一登入身分驗證，以及您的 Google 或 Facebook 憑證，都是聯合身分的範例。當您以聯合身分登入時，您的管理員先前會使用 IAM角色設定身分聯合。當您 AWS 使用聯合存取 時，您會間接擔任 角色。

根據您身分的使用者類型，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 使用者指南 中的[如何登入 AWS 帳戶](#)您的 。 AWS 登入

如果您以 AWS 程式設計方式存取，AWS 會提供軟體開發套件（SDK）和命令列介面（CLI），以使用您的憑證以密碼編譯方式簽署您的請求。如果您不使用 AWS 工具，則必須自行簽署請求。如需使用建議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身分驗證（MFA）來提高帳戶的安全性。若要進一步了解，請參閱 AWS IAM Identity Center 使用者指南中的[多重要素驗證](#)，以及 IAM 使用者指南 中的[使用多重要素驗證（MFA）AWS](#)。

AWS 帳戶根使用者

當您建立時 AWS 帳戶，您會從一個登入身分開始，該身分可以完全存取帳戶中的所有 AWS 服務和資源。此身分稱為 AWS 帳戶根使用者，透過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。如需需要您以根使用者身分登入的任務完整清單，請參閱 IAM 使用者指南 中的[需要根使用者憑證的任務](#)。

聯合身分

最佳實務是，要求人類使用者，包括需要管理員存取權的使用者，使用 AWS 服務臨時憑證與身分提供者聯合來存取。

聯合身分是來自您的企業使用者目錄、Web 身分提供者、AWS Directory Service、身分中心目錄，或使用透過身分來源提供的 AWS 服務憑證存取的任何使用者。當聯合身分存取時 AWS 帳戶，它們會擔任角色，而角色會提供臨時憑證。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，或者您可以連線並同步到您身分來源中的一組使用者 AWS 帳戶和群組，以便在所有和應用程式中使用。如需 IAM Identity Center 的相關資訊，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 中具有單一個人或應用程式特定許可 AWS 帳戶的身分。如果可能，我們建議您依賴臨時憑證，而不是建立具有密碼和存取金鑰等長期憑證 IAM 的使用者。不過，如果您有特定的使用案例需要 IAM 使用者長期憑證，建議您輪換存取金鑰。如需詳細資訊，請參閱 IAM 使用者指南 中的[定期輪換需要長期憑證的使用案例存取金鑰](#)。

[IAM 群組](#)是指定 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，您可以擁有一名為的群組 IAMAdmins，並授予該群組管理 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。若要進一步了解，請參閱 IAM 使用者指南 中的[何時建立IAM使用者（而非角色）](#)。

IAM 角色

[IAM 角色](#)是 中具有特定許可 AWS 帳戶 的身分。它類似於IAM使用者，但與特定人員無關。您可以透過 AWS Management Console 切換IAM角色 暫時在 中擔任角色。https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-console.html您可以呼叫 AWS CLI 或 AWS API 操作，或使用自訂 來擔任角色URL。如需使用角色方法的詳細資訊，請參閱 IAM 使用者指南 中的[使用IAM角色](#)。

IAM 具有臨時憑證的角色在下列情況下很有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需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，您可以設定許可集。若要控制身分在身分驗證後可以存取的內容，IAM Identity Center 會將許可集與 中的角色相關聯IAM。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](#)。
- 臨時IAM使用者許可 – IAM使用者或角色可以擔任IAM角色，暫時接受特定任務的不同許可。
- 跨帳戶存取 – 您可以使用 IAM角色，允許不同帳戶中的某人（受信任的主體）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。不過，使用某些 AWS 服務，您可以將政策直接連接至資源（而不是使用角色作為代理）。若要了解跨帳戶存取的角色與資源型政策之間的差異，請參閱 IAM 使用者指南 中的[IAM角色與資源型政策有何不同](#)。
- 跨服務存取 – 有些 AWS 服務 使用其他 中的功能 AWS 服務。例如，當您在 服務中撥打電話時，該服務通常會在 Amazon 中執行應用程式EC2或在 Amazon S3 中儲存物件。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
- 轉送存取工作階段（FAS） – 當您使用IAM使用者或角色在 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 使用呼叫的委託人許可 AWS 服務，並結合請求向下游服務 AWS 服務 提出請求。FAS 只有在服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會發出請求。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[轉送存取工作階段](#)。
- 服務角色 – 服務角色是服務代表您執行動作時擔任[IAM的角色](#)。IAM 管理員可以從 內部建立、修改和刪除服務角色IAM。如需詳細資訊，請參閱 使用者指南 中的[建立角色以將許可委派給 AWS 服務](#)。IAM

- 服務連結角色 – 服務連結角色是連結至的服務角色類型 AWS 服務。服務可以擔任代表您執行動作角色。服務連結角色會顯示在您的 中 AWS 帳戶，並由 服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。
- 在 Amazon 上執行的應用程式 EC2 – 您可以使用 IAM 角色來管理在 EC2 執行個體上執行的應用程式的臨時憑證，以及提出 AWS CLI 或 AWS API 請求。最好將存取金鑰存放在 EC2 執行個體中。若要將 AWS 角色指派給 EC2 執行個體並將其提供給其所有應用程式，您可以建立連接至執行個體的執行個體設定檔。執行個體設定檔包含 角色，並啟用在 EC2 執行個體上執行的程式，以取得臨時憑證。如需詳細資訊，請參閱 IAM 使用者指南 中的 [使用 IAM 角色將許可授予在 Amazon EC2 執行個體上執行的應用程式](#)。

若要了解如何使用 IAM 角色或 IAM 使用者，請參閱 IAM 使用者指南 中的 [建立 IAM 角色（而非使用者）的時機](#)。

使用政策管理存取權

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

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

預設情況下，使用者和角色沒有許可。若要授予使用者對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，使用者可以擔任角色。

IAM 無論您用來執行操作的方法為何，政策都會定義動作的許可。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該政策的使用者可以從 AWS Management Console、AWS CLI 或 AWS 取得角色資訊 API。

身分型政策

身分型政策是 JSON 許可政策文件，您可以附加到身分，例如 IAM 使用者、使用者群組或角色。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型政策，請參閱 IAM 使用者指南 中的 [建立 IAM 政策](#)。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管政策是獨立的政策，您可以連接到 中的多個使用者、群組和角色 AWS 帳戶。受管政策包括 AWS 受

管政策和客戶受管政策。若要了解如何在受管政策或內嵌政策之間進行選擇，請參閱 IAM 使用者指南中的在[受管政策與內嵌政策之間進行選擇](#)。

資源型政策

資源型政策是您連接至資源JSON的政策文件。資源型政策的範例包括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](#)。主體可以包括帳戶、使用者、角色、聯合使用者或 AWS 服務。

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

存取控制清單 (ACLs)

存取控制清單 (ACLs) 控制哪些主體 (帳戶成員、使用者或角色) 具有存取資源的許可。ACLs 類似於資源型政策，雖然它們不使用JSON政策文件格式。

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

其他政策類型

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

- 許可界限 – 許可界限是一項進階功能，您可以在其中設定身分型政策可授予IAM實體 (IAM使用者或角色) 的最大許可。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 Principal 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需許可界限的詳細資訊，請參閱 IAM 使用者指南中的[IAM實體許可界限](#)。
- 服務控制政策 (SCPs) – SCPs是在 中指定組織或組織單位 (OU) 最大許可JSON的政策 AWS Organizations。AWS Organizations 是一項用於分組和集中管理您企業擁有 AWS 帳戶之多個的服務。如果您啟用組織中的所有功能，則可以將服務控制政策 (SCPs) 套用至任何或所有帳戶。SCP 限制成員帳戶中實體的許可，包括每個 AWS 帳戶根使用者。如需 Organizations 和 的詳細資訊SCPs，請參閱 AWS Organizations 使用者指南中的[如何SCPs運作](#)。
- 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。如需詳細資訊，請參閱 IAM 使用者指南中的[工作階段政策](#)。

多種政策類型

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

AWS Transfer Family 如何使用 IAM

使用 AWS Identity and Access Management (IAM) 管理對 的存取之前 AWS Transfer Family，您應該了解哪些IAM功能可與 搭配使用 AWS Transfer Family。若要取得 AWS Transfer Family 和其他 AWS 服務如何與 搭配使用的高階檢視IAM，請參閱 IAM 使用者指南 中的[AWS 使用的 服務IAM](#)。

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

透過身分IAM型政策，您可以指定允許或拒絕的動作和資源，以及允許或拒絕動作的條件。AWS Transfer Family 支援特定動作、資源和條件索引鍵。若要了解您在JSON政策中使用的所有元素，請參閱 AWS Identity and Access Management 使用者指南 中的[IAMJSON政策元素參考](#)。

動作

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

JSON 政策的 Action元素說明您可以用來允許或拒絕政策中存取的動作。政策動作通常具有與相關聯 AWS API操作相同的名稱。有一些例外狀況，例如沒有相符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。

中的政策動作在動作之前 AWS Transfer Family 使用下列字首：transfer:。例如，若要授予某人建立伺服器的許可，透過 Transfer Family CreateServerAPI操作，您可以在其政策中包含 transfer:CreateServer動作。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 中 [由 定義的動作 AWS Transfer Family](#)。

資源

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

Resource JSON 政策元素會指定動作套用的物件。陳述式必須包含 Resource 或 NotResource 元素。最佳實務是使用其 [Amazon Resource Name \(ARN \) 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": "*" 
```

Transfer Family 伺服器資源具有下列 ARN。

```
arn:aws:transfer:${Region}:${Account}:server/${ServerId}
```

例如，若要在陳述式中指定 s-01234567890abcdef Transfer Family 伺服器，請使用下列 ARN。

```
"Resource": "arn:aws:transfer:us-east-1:123456789012:server/s-01234567890abcdef"
```

如需有關 格式的詳細資訊 ARNs，請參閱服務授權參考 中的 [Amazon Resource Names \(ARNs \)](#)，或使用者指南 [IAM ARNs](#) 中的 [IAM](#)

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/*"
```


有些 AWS Transfer Family 動作會在多個資源上執行，例如IAM政策中使用的資源。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 伺服器和使用者的政策。若要在單一陳述式中指定多個資源，ARNs請以逗號分隔。

```
"Resource": [  
    "resource1",  
    "resource2"  
]
```

若要查看 AWS Transfer Family 資源清單，請參閱服務授權參考 中 [由 定義的資源類型 AWS Transfer Family](#)。

條件索引鍵

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

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

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

您也可以在指定條件時使用預留位置變數。例如，只有在IAM使用者使用其IAM使用者名稱標記時，您才能授予使用者存取資源的許可。如需詳細資訊，請參閱 IAM 使用者指南 中的 [IAM政策元素：變數和標籤](#)。

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

AWS Transfer Family 會定義自己的一組條件金鑰，並支援使用某些全域條件金鑰。若要查看 AWS Transfer Family 條件金鑰清單，請參閱服務授權參考 中的 [的條件金鑰 AWS Transfer Family](#)。

範例

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

AWS Transfer Family 資源型政策

資源型政策是JSON政策文件，用於指定指定主體可以在 AWS Transfer Family 資源上執行的動作，以及在哪些條件下執行的動作。Amazon S3 支援 Amazon S3 的資源型許可政策 *buckets*。資源型政策可讓您以每個資源為基礎，將用量許可授予其他帳戶。您也可以使用資源型政策，允許 AWS 服務存取您的 Amazon S3 *buckets*。

若要啟用跨帳戶存取，您可以將另一個帳戶中的整個帳戶或IAM實體指定為[資源型政策中的主體](#)。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當主體和資源位於不同的 AWS 帳戶中時，您還必須授予主體實體存取資源的許可。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角色與資源型政策有何不同](#)。

Amazon S3 服務僅支援一種名為的資源型政策 *bucket* 政策，連接至 *bucket*。此政策定義哪些主體實體（帳戶、使用者、角色和聯合使用者）可以對物件執行動作。

範例

若要檢視 AWS Transfer Family 資源型政策的範例，請參閱 [AWS Transfer Family 標籤型政策範例](#)。

以 AWS Transfer Family 標籤為基礎的授權

您可以將標籤連接至 AWS Transfer Family 資源，或將請求中的標籤傳遞至 AWS Transfer Family。如需根據標籤控制存取，請使用 `transfer:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，在政策的[條件元素](#)中，提供標籤資訊。如需如何使用標籤控制 AWS Transfer Family 資源存取的資訊，請參閱 [AWS Transfer Family 標籤型政策範例](#)。

AWS Transfer Family IAM 角色

[IAM 角色](#)是您 AWS 帳戶中具有特定許可的實體。

搭配 使用臨時憑證 AWS Transfer Family

您可以使用臨時憑證來登入聯合、擔任IAM角色或擔任跨帳戶角色。您可以透過呼叫 AWS STS API [AssumeRole](#)或 等操作來取得臨時安全憑證[GetFederationToken](#)。

AWS Transfer Family 支援使用臨時憑證。

AWS Transfer Family 身分型政策範例

根據預設，IAM使用者和角色沒有建立或修改 AWS Transfer Family 資源的許可。他們也無法使用 AWS Management Console AWS CLI、或 AWS 執行任務API。IAM 管理員必須建立IAM政策，授予

使用者和角色許可，以對所需的指定資源執行特定API操作。然後，管理員必須將這些政策連接到需要這些許可IAM的使用者或群組。

若要了解如何使用這些範例政策文件建立身分IAM型JSON政策，請參閱 [AWS Identity and Access Management 使用者指南](#) 中的 [在 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

身分型政策會決定某人是否可以建立、存取或刪除您帳戶中 AWS Transfer Family 的資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用受AWS 管政策，將許可授予許多常見使用案例。它們可在您的 中使用 AWS 帳戶。我們建議您定義特定於使用案例 AWS 的客戶受管政策，以進一步減少許可。如需詳細資訊，請參閱 IAM 使用者指南 中的 [AWS 受管政策](#)或 [AWS 任務功能的受管政策](#)。
- 套用最低權限許可 – 當您使用IAM政策設定許可時，只會授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的詳細資訊，請參閱 IAM 使用者指南 [中的政策和許可IAM](#)。
- 使用IAM政策中的條件來進一步限制存取：您可以將條件新增至政策，以限制對動作和資源的存取。例如，您可以撰寫政策條件來指定所有請求都必須使用 傳送SSL。如果透過特定 使用服務動作，例如 AWS 服務，您也可以使用 條件來授予其存取權 AWS CloudFormation。如需詳細資訊，請參閱 IAM 使用者指南 中的[IAMJSON政策元素：條件](#)。
- 使用 IAM Access Analyzer 驗證您的IAM政策以確保安全且功能許可 – IAM Access Analyzer 會驗證新的和現有的政策，讓政策遵循IAM政策語言（JSON）和IAM最佳實務。IAM Access Analyzer 提供超過 100 個政策檢查和可行建議，協助您撰寫安全且功能正常的政策。如需詳細資訊，請參閱 IAM 使用者指南 中的[IAM存取分析器政策驗證](#)。
- 需要多重要素身分驗證（MFA）– 如果您有需要IAM使用者或 根使用者的案例 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。若要在呼叫API操作MFA時要求，請將MFA條件新增至您的政策。如需詳細資訊，請參閱 IAM 使用者指南 中的[設定 MFA受保護的API存取](#)。

如需 中最佳實務的詳細資訊IAM，請參閱 IAM 使用者指南 [中的安全最佳實務IAM](#)。

使用 AWS Transfer Family 主控台

若要存取 AWS Transfer Family 主控台，您必須具有一組最低許可。這些許可必須允許您列出和檢視 AWS 帳戶中 AWS Transfer Family 資源的詳細資訊。如果您建立的身分型政策比最低必要許可更嚴格，則主控台將無法與該政策針對實體（IAM 使用者或角色）正常運作。如需詳細資訊，請參閱 AWS Identity and Access Management 使用者指南 中的 [新增許可給使用者](#)。

對於僅對 AWS CLI 或 進行呼叫的使用者，您不需要允許最低主控台許可 AWS API。相反地，僅允許存取與您嘗試執行API的操作相符的動作。

允許使用者檢視他們自己的許可

此範例示範如何建立政策，允許使用者檢視連接至其IAM使用者身分的內嵌和受管政策。此政策包含在主控台上完成此動作或使用 AWS CLI 或 以程式設計方式完成此動作的許可 AWS API。

```
{
  "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 標籤型政策範例

以下是如何根據標籤控制對 AWS Transfer Family 資源的存取的範例。

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 資源上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。如需標記資源的詳細資訊，請參閱 [標記 AWS 資源](#) AWS 一般參考。

在 AWS Transfer Family 中，資源可以具有標籤，而某些動作可以包含標籤。建立 IAM 政策時，您可以使用標籤條件金鑰來控制下列項目：

- 哪些使用者可以根據 AWS Transfer Family 資源擁有的標籤，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。

透過使用標籤型存取控制，您可以套用比 API 層級更精細的控制。您也可以套用比使用資源型存取控制更多的動態控制。您可以根據請求（請求標籤）中提供的標籤，建立允許或拒絕操作 IAM 的政策。您也可以根據正在操作的資源（資源標籤）上的標籤建立 IAM 政策。一般而言，資源標籤是針對已存在於資源上的標籤，當您將標籤新增至資源或從資源中移除標籤時，請求標籤就是。

如需標籤條件索引鍵的完整語法和語義，請參閱 IAM 使用者指南 中的 [使用資源標籤控制 AWS 對資源的存取](#)。如需使用 API Gateway 指定 IAM 政策的詳細資訊，請參閱 [開發人員指南](#) 中的 [控制 API 對具有 IAM 許可的資源的存取](#)。API

範例 1：根據資源標籤拒絕動作

您可以拒絕根據標籤對資源執行動作。如果使用者或伺服器資源標記了金鑰和值 TagResource，則下列範例政策會拒絕 DescribeServer、UntagResource、StartServer、StopServer、stage 和 DescribeUser 操作。

```

{
    "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：根據資源標籤允許動作

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標記了 金鑰和 值，則下列範例政策允許 TagResource UntagResource DescribeServer、StartServer StopServer、stage 和 DescribeUser 操作 prod。

```

{
  "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：拒絕根據請求標籤建立使用者或伺服器

下列範例政策包含兩個陳述式。如果標籤的成本中心金鑰沒有值，則第一個陳述式會拒絕對所有資源執行CreateServer操作。

如果標籤的成本中心金鑰包含除 1、2 或 3 以外的任何其他值，則第二個陳述式會拒絕CreateServer操作。

Note

此政策允許建立或刪除資源，其中包含名為 的金鑰，costcenter以及 1、2或 的值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"
        ]
      }
    }
  ]
}

```

對 AWS Transfer Family 身分和存取權進行故障診斷

使用下列資訊來協助您診斷和修正使用 AWS Transfer Family 時可能遇到的常見問題IAM。

主題

- [我無權在 中執行動作 AWS Transfer Family](#)
- [我無權執行 iam : PassRole](#)
- [我想要允許 AWS 帳戶外的人員存取我的 AWS Transfer Family 資源](#)

我無權在 中執行動作 AWS Transfer Family

如果 AWS Management Console 告訴您未獲授權執行動作，則必須聯絡管理員尋求協助。您的管理員是為您提供簽署憑證的人員。

當mateojacksonIAM使用者嘗試使用主控台檢視有關 的詳細資訊時，會發生下列錯誤範例 *widget* 但沒有transfer:*GetWidget*許可。

```

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。

我無權執行 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。

當名為 marymajor IAM 的使用者嘗試使用主控台在 中執行動作時，會發生下列錯誤範例 AWS Transfer Family。但是，動作請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。

下列範例政策包含將角色傳遞至 的許可 AWS Transfer Family。

```
{
  "Version": "2012-10-17",
  "Statement": [
    { "Action": "iam:PassRole",
      "Resource": "arn:aws::iam::123456789012:role/*",
      "Effect": "Allow"
    }
  ]
}
```

我想要允許 AWS 帳戶外的人員存取我的 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。對於支援資源型政策或存取控制清單（ACLs）的服務，您可以使用這些政策來授予人員對資源的存取權。

如需進一步了解，請參閱以下內容：

- 若要了解 是否 AWS Transfer Family 支援這些功能，請參閱 [AWS Transfer Family 如何使用 IAM](#)。
- 若要了解如何 AWS 帳戶 在您擁有的 資源之間提供存取權，請參閱 IAM 使用者指南 中的 [在您擁有 AWS 帳戶 的另一個資源中為IAM使用者提供存取權](#)。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱 使用者指南 中的 [提供存取權給第三方 AWS 帳戶 擁有](#)。IAM

- 若要了解如何透過身分聯合提供存取權，請參閱 IAM 使用者指南 中的[為外部驗證的使用者提供存取權（身分聯合）](#)。
- 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 角色與資源型政策有何不同](#)。

的合規驗證 AWS Transfer Family

第三方稽核人員 AWS Transfer Family 會在多個合規計畫中評估 的安全性和 AWS 合規性。其中包括 SOC、PCI、HIPAA 和其他。如需完整清單，請參閱[AWS 依合規計畫範圍中的服務](#)。

如需特定合規計畫範圍內 AWS 的服務清單，請參閱[AWS 依合規計畫範圍中的服務](#)。如需一般資訊，請參閱 [AWS 合規計畫](#)。

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 AWS Transfer Family 取決於資料的敏感度、您公司的合規目標，以及適用的法律和法規。AWS 提供下列資源來協助合規：

- [安全性和合規快速入門指南](#) – 這些部署指南討論架構考量，並提供在 上部署以安全性和合規為中心之基準環境的步驟 AWS。
- [HIPAA 安全和合規的架構白皮書](#) – 此白皮書描述了公司如何使用 AWS 來建立 HIPAA 合規的應用程式。
- [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](#) – AWS 此服務會評估資源組態是否符合內部實務、產業準則和法規。
- [AWS Security Hub](#) – AWS 此服務提供 內安全狀態的全面檢視 AWS，協助您檢查是否符合安全產業標準和最佳實務。

中的復原能力 AWS Transfer Family

AWS 全域基礎設施是以 AWS 區域和可用區域為基礎。AWS 區域提供多個實體隔離和隔離的可用區域，這些區域與低延遲、高輸送量和高冗餘聯網連接。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 支援最多 3 個可用區域，並由自動擴展的備援機群支援，以滿足您的連線和傳輸請求。

注意下列事項：

- 對於公有端點：
 - 服務內建可用區域層級備援
 - 每個 AZ 都有備援機群。
 - 此備援會自動提供
- 如需虛擬私有雲端（VPC）中的端點，請參閱 [在虛擬私有雲端中建立伺服器](#)。

另請參閱

- 如需 AWS 區域 和 可用區域的詳細資訊，請參閱[AWS 全域基礎設施](#)。
- 如需如何使用以延遲為基礎的路由建置以增加備援並盡可能降低網路延遲的範例，請參閱部落格文章[將 AWS Transfer Family 伺服器的網路延遲降到最低](#)。

中的基礎設施安全 AWS Transfer Family

作為受管服務，AWS Transfer Family 受到 AWS 全球網路安全的保護。如需有關 AWS 安全服務以及如何 AWS 保護基礎設施的資訊，請參閱 [AWS Cloud Security](#)。若要使用基礎設施安全性的最佳實務來設計您的 AWS 環境，請參閱 Security Pillar AWS Well-Architected Framework 中的[基礎設施保護](#)。

您可以使用 AWS 已發佈的 API 呼叫，AWS Transfer Family 透過網路存取。使用者端必須支援下列專案：

- Transport Layer Security（TLS）。我們需要 TLS 1.2 和 建議 TLS 1.3。
- 具有完美前向秘密（PFS）的加密套件，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，必須使用與 IAM 委託人相關聯的存取金鑰 ID 和秘密存取金鑰來簽署請求。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 Web 應用程式防火牆，可協助保護 Web 應用程式和 APIs 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，根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 請求。如需詳細資訊，請參閱[使用 AWS WAF 來保護您的 APIs](#)。

若要新增 AWS WAF

1. 在 開啟API閘道主控台<https://console.aws.amazon.com/apigateway/>。
2. 在APIs導覽窗格中，然後選擇您的自訂身分提供者範本。
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 Application Firewall (WAF) 下，針對 Web ACL，選擇ACL您要與此階段相關聯的 Web。
 - 如果您需要的 Web ACL 不存在，則需要執行下列動作來建立 Web：
 1. 選擇建立 Web ACL。
 2. 在 AWS WAF服務首頁上，選擇建立 Web ACL。
 3. 在 Web ACL詳細資訊 中，針對名稱，輸入 Web 的名稱ACL。
 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. 對於規則類型，選擇 IP 集以識別 IP 地址的特定清單。
 6. 針對規則，輸入規則的名稱。
 7. 對於 IP 組，選擇現有的 IP 組。若要建立 IP 集，請參閱[建立 IP 集](#)。
 8. 若要使用 IP 地址作為原始地址，請在標頭 中選擇 IP 地址。
 9. 對於標頭欄位名稱，輸入 SourceIP。
 10. 針對標頭 中的位置，選擇第一個 IP 地址。
 11. 對於遺失 IP 地址 的後援，根據您要如何處理標頭中無效（或遺失）IP 地址，選擇相符或不相符。
 12. 針對動作，選擇 IP 集的動作。
 13. 對於不符合任何規則 請求的預設 Web ACL動作，請選擇允許或封鎖，然後按一下下一步。
 14. 對於步驟 4 和 5，選擇下一步。
 15. 在檢閱和建立 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 Transfer Family AWS Web 應用程式防火牆安全性的相關資訊，請參閱 AWS 儲存部落格中的[AWS Transfer Family 使用 AWS 應用程式防火牆和 Amazon API Gateway 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 AWS 中，跨服務模擬可能會導致混淆代理問題。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，以使用其許可來對其他客戶的資源採取行動，其不應以其他方式擁有存取許可。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 中的[混淆代理問題](#)。

我們建議在資源政策中使用 `aws:SourceArn` 和 `aws:SourceAccount` 全域條件內容索引鍵，以限制 AWS Transfer Family 對資源的許可。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。

防止混淆代理問題的最有效方法是使用您要允許之資源的確切 Amazon Resource Name (ARN)。如果您要指定多個資源，請將 `aws:SourceArn` 全域內容條件索引鍵與萬用字元 (`*`) 搭配使用，以用於的未知部分 ARN。例如：`arn:aws:transfer::region::account-id:server/*`。

AWS Transfer Family 使用以下類型的角色：

- 使用者角色 – 允許服務受管使用者存取必要的 Transfer Family 資源。AWS Transfer Family 會在 Transfer Family 使用者 的背景中擔任此角色 ARN。
- 存取角色 – 僅提供正在傳輸的 Amazon S3 檔案的存取權。對於傳入 AS2 傳輸，存取角色會使用 Amazon Resource Name (ARN) 作為合約。對於傳出 AS2 傳輸，存取角色會使用 ARN 連接器的。
- 調用角色 – 與 Amazon API Gateway 搭配使用，作為伺服器的自訂身分提供者。Transfer Family 會在 Transfer Family 伺服器 的內容中擔任此角色 ARN。
- 記錄角色 – 用於將項目記錄到 Amazon CloudWatch。Transfer Family 使用此角色記錄成功和失敗詳細資訊，以及檔案傳輸的相關資訊。Transfer Family 會在 Transfer Family 伺服器 的內容中擔任此角色 ARN。對於傳出 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 的內容中擔任此角色 ARN。

如需詳細資訊，請參閱 IAM 使用者指南 [中的政策和許可 IAM](#)。

Note

在下列範例中，取代每個 *user input placeholder* 使用您自己的資訊。

Note

在我們的範例中，我們同時使用 ArnLike 和 ArnEquals。它們的功能相同，因此您可以在建構政策時使用它們。Transfer Family 文件用於條件包含萬用字元 ArnLike 時，並 ArnEquals 指示完全相符的條件。

AWS Transfer Family 使用者角色跨服務混淆代理預防

下列範例政策允許 帳戶中任何伺服器的任何使用者擔任 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/*"
        }
      }
    }
  ]
}
```

下列範例政策允許特定伺服器的任何使用者擔任 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/*"
      }
    }
  }
]
}

```

下列範例政策允許特定伺服器的特定使用者擔任 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代理預防

下列範例政策允許 帳戶中的任何工作流程擔任 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/*"
        }
      }
    }
  ]
}
```

下列範例政策允許特定工作流程擔任角色。

```
{
  "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代理預防

Note

下列範例可用於記錄和調用角色。

在這些範例中，如果您的伺服器未連接任何工作流程，您可以移除工作流程ARN的詳細資訊。

下列範例記錄/調用政策允許 帳戶中的任何伺服器（和工作流程）擔任 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/調用政策允許特定伺服器（和工作流程）擔任角色。

```
{
  "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 受管政策

若要將許可新增至使用者、群組和角色，使用 AWS 受管政策比自行撰寫政策更容易。[建立 AWS Identity and Access Management \(IAM\) 客戶受管政策](#)需要時間和專業知識，為您的團隊提供他們所需的許可。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 受管政策的詳細資訊，請參閱 IAM 使用者指南 中的[AWS 受管政策](#)。如需所有 AWS 受管政策的詳細清單，請參閱 [AWS 受管政策參考指南](#)。

AWS 服務會維護和更新 AWS 受管政策。您無法變更 AWS 受管政策中的許可。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 受管政策中移除許可，因此政策更新不會破壞現有的許可。

此外，AWS 支援跨多個 服務之任務函數的受管政策。例如，ReadOnlyAccess AWS 受管政策提供所有 AWS 服務和資源的唯讀存取權。服務啟動新功能時，會為新操作和資源 AWS 新增唯讀許可。如需任務函數政策的清單和說明，請參閱 IAM 使用者指南 中的[AWS 任務函數的受管政策](#)。

AWS 受管政策：AWSTransferConsoleFullAccess

此AWSTransferConsoleFullAccess政策透過 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` – 准許擷取憑證的清單 Amazon Resource Names (ARNs) 和每個的網域名稱ARN。
- `ec2:DescribeAddresses` – 准許描述一或多個彈性 IP 地址。
- `ec2:DescribeAvailabilityZones` – 准許描述一個或多個可供您使用的可用區域。
- `ec2:DescribeNetworkInterfaces` – 准許描述一或多個彈性網路介面。
- `ec2:DescribeSecurityGroups` – 准許描述一或多個安全群組。
- `ec2:DescribeSubnets` – 准許描述一或多個子網路。
- `ec2:DescribeVpcs` – 准許描述一或多個虛擬私有雲端 (VPCs) 。
- `ec2:DescribeVpcEndpoints` – 准許描述一或多個VPC端點。
- `health:DescribeEventAggregates` – 傳回每個事件類型的事件數目 (問題、排程變更和帳戶通知) 。
- `iam:GetPolicyVersion` – 准許擷取指定受管政策版本的相關資訊，包括政策文件。
- `iam:ListPolicies` – 准許列出所有受管政策。
- `iam:ListRoles` – 准許列出具有指定路徑字首IAM的角色。
- `iam:PassRole` – 准許將IAM角色傳遞至 Transfer Family。如需更多詳細資訊，請參閱[授予使用者將角色傳遞至的許可 AWS 服務](#)。
- `route53:ListHostedZones` – 准許取得與目前相關聯的公有和私有託管區域清單 AWS 帳戶。
- `s3:ListAllMyBuckets` – 准許列出請求已驗證寄件者擁有的所有儲存貯體。
- `transfer:*` – 准許存取 Transfer Family 資源。星號 (*) 會授予所有資源的存取權。

```
{
  "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 受管政策：AWSTransferFullAccess

此AWSTransferFullAccess政策提供 Transfer Family 服務的完整存取權。

許可詳細資訊

此政策包含以下許可。

- `transfer:*` – 准許存取 Transfer Family 資源。星號 (*) 會授予所有 資源的存取權。
- `iam:PassRole` – 准許將IAM角色傳遞至 Transfer Family。如需更多詳細資訊，請參閱[授予使用者將角色傳遞至 的許可 AWS 服務](#)。

- `ec2:DescribeAddresses` – 准許描述一或多個彈性 IP 地址。
- `ec2:DescribeNetworkInterfaces` – 准許描述一或多個網路介面。
- `ec2:DescribeVpcEndpoints` – 准許描述一或多個VPC端點。

```
{
  "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 受管政策：AWSTransferLoggingAccess

此AWSTransferLoggingAccess政策授予 AWS Transfer Family 完整存取權，以建立日誌串流和群組，並將日誌事件放入您的帳戶。

許可詳細資訊

此政策包含 的下列許可 Amazon CloudWatch Logs。

- `CreateLogStream` – 准許主體建立日誌串流。
- `DescribeLogStreams` – 准許主體列出日誌群組的日誌串流。
- `CreateLogGroup` – 准許主體建立日誌群組。
- `PutLogEvents` – 准許主體將一批日誌事件上傳到日誌串流。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS 受管政策：AWSTransferReadOnlyAccess

此AWSTransferReadOnlyAccess政策提供 Transfer Family 服務的唯讀存取權。

許可詳細資訊

此政策包含 Transfer Family 的下列許可。

- `DescribeUser` – 准許主體檢視使用者的描述。
- `DescribeServer` – 准許主體檢視伺服器的描述。
- `ListUsers` – 准許主體列出伺服器的使用者。
- `ListServers` – 准許主體列出帳戶的伺服器。
- `TestIdentityProvider` – 准許主體測試設定的身分提供者是否正確設定。
- `ListTagsForResource` – 准許主體列出資源的標籤。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "transfer:DescribeUser",
        "transfer:DescribeServer",
        "transfer:ListUsers",
        "transfer:ListServers",
        "transfer:TestIdentityProvider",
        "transfer:ListTagsForResource"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS 將系列更新轉移至 AWS 受管政策

檢視自此服務開始追蹤這些變更以來，AWS Transfer Family 受 AWS 管政策更新的詳細資訊。如需此頁面變更的自動提醒，請訂閱[的文件歷史記錄 AWS Transfer Family](#)頁面上的RSS摘要。

變更	描述	日期
文件更新	已為每個 Transfer Family 受管政策新增區段。	2022 年 1 月 27 日
AWSTransferReadOnlyAccess – 更新現有政策	AWS Transfer Family 新增了允許政策讀取的許可 AWS Managed Microsoft AD。	2021 年 9 月 30 日
AWS Transfer Family 已開始追蹤變更	AWS Transfer Family 已開始追蹤其 AWS 受管政策的變更。	2021 年 6 月 15 日

疑難排解 AWS Transfer Family

使用下列資訊來協助您診斷和修正使用時可能遇到的常見問題 AWS Transfer Family。

如需 Transfer Family IAM 中的問題，請參閱 [對 AWS Transfer Family 身分和存取權進行故障診斷](#)。

主題

- [對服務受管使用者進行故障診斷](#)
- [對 Amazon API Gateway 問題進行故障診斷](#)
- [對加密 Amazon S3 儲存貯體的政策進行故障診斷](#)
- [對身分驗證問題進行故障診斷](#)
- [對受管工作流程問題進行故障診斷](#)
- [對工作流程解密問題進行故障診斷](#)
- [對 Amazon EFS 問題進行故障診斷](#)
- [對身分提供者進行測試的疑難排解](#)
- [為您的 SFTP 連接器新增受信任主機金鑰的故障診斷](#)
- [對檔案上傳問題進行故障診斷](#)
- [對 ResourceNotFound 例外狀況進行疑難排解](#)
- [連接器 SFTP 問題疑難排解](#)
- [針對 AS2 問題進行故障診斷](#)

對服務受管使用者進行故障診斷

本節說明下列問題的可能解決方案。

主題

- [Amazon EFS 服務受管使用者疑難排解](#)
- [對公有金鑰內文太長進行故障診斷](#)
- [新增 SSH 公有金鑰故障診斷失敗](#)

Amazon EFS 服務受管使用者疑難排解

Description

您執行 `sftp` 命令，但提示不會出現，而是看到下列訊息：

```
Couldn't canonicalize: Permission denied
Need cwd
```

原因

您 AWS Identity and Access Management (IAM) 使用者的角色沒有存取 Amazon Elastic File System (Amazon EFS) 的許可。

解決方案

增加使用者角色的政策許可。您可以新增受 AWS 管政策，例如 `AmazonElasticFileSystemClientFullAccess`。

對公有金鑰內文太長進行故障診斷

Description

當您嘗試建立服務受管使用者時，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

您可能正在輸入公有 PGP 金鑰主體的金鑰，AWS Transfer Family 且不支援服務受管使用者的 PGP 金鑰。

解決方案

如果 PGP 金鑰是以 RSA 為基礎，您可以將其轉換為 PEM 格式。例如，Ubuntu 在此提供轉換工具：<https://manpages.ubuntu.com/manpages/xenial/man1/openpgp2ssh.1.html>

新增 SSH 公有金鑰故障診斷失敗

Description

當您嘗試為受服務管理的使用者新增公有金鑰時，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 格式化公有金鑰，AWS Transfer Family 且不支援服務受管使用者的 SSH2 格式化公有金鑰。

解決方案

您需要將金鑰轉換為 OpenSSH 格式。此程序會在 [中說明將SSH2公有金鑰轉換為PEM格式](#)。

對 Amazon API Gateway 問題進行故障診斷

本節說明下列 API 閘道問題的可能解決方案。

主題

- [身分驗證失敗太多](#)
- [連線已關閉](#)

身分驗證失敗太多

Description

當您嘗試使用 Secure Shell (SSH) 檔案傳輸通訊協定 (SFTP) 連線至伺服器時，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

您可能為使用者輸入了不正確的密碼。請再次嘗試輸入正確的密碼。

如果密碼正確，問題可能是由於角色 Amazon Resource Name (ARN) 無效所造成。若要確認這是問題，請測試您伺服器的身分提供者。如果您看到類似以下內容的回應，則角色只是 ARN 預留位置，如所有零的角色 ID 值所示：

```
{
  "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

將預留位置角色取代ARN為具有存取伺服器許可的實際角色。

更新角色

1. 在 <https://console.aws.amazon.com/cloudformation> 開啟 AWS CloudFormation 主控台。
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，然後選擇參數索引標籤。
4. 選擇更新。在更新堆疊頁面上，選擇使用目前範本，然後選擇下一個。
5. UserRoleArn 將取代為具有足夠許可ARN的角色，以存取 Transfer Family 伺服器。

Note

若要授予必要的許可，您可以將 AmazonAPIGatewayAdministrator 和 AmazonS3FullAccess 受管政策新增至您的角色。

6. 選擇下一個，然後再次選擇下一個。檢閱中 **stack** 頁面，選取我確認 AWS CloudFormation 可能會建立IAM資源，然後選擇更新堆疊。

連線已關閉

Description

當您嘗試使用 Secure Shell (SSH) 檔案傳輸通訊協定 (SFTP) 連線至伺服器時，您會收到下列錯誤：

```
Connection closed
```

原因

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

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](#)。

對加密 Amazon S3 儲存貯體的政策進行故障診斷

Description

您有一個加密的 Amazon S3 儲存貯體，用來儲存 Transfer Family 伺服器。如果您嘗試將檔案上傳到伺服器，則會收到錯誤 Couldn't close file: Permission denied。

如果您檢視伺服器日誌，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

您IAM使用者的政策沒有存取加密儲存貯體的許可。

解決方案

您必須在政策中指定其他許可，才能授予所需的 AWS Key Management Service (AWS KMS) 許可。如需詳細資訊，請參閱 [Amazon S3 中的資料加密](#)。

對身分驗證問題進行故障診斷

本節說明下列身分驗證問題的可能解決方案。

主題

- [驗證失敗 —SSH/SFTP](#)
- [Managed AD 不相符領域問題](#)
- [其他身分驗證問題](#)

驗證失敗 —SSH/SFTP

Description

當您嘗試使用 Secure Shell (SSH) 檔案傳輸通訊協定 (SFTP) 連線至伺服器時，您會收到類似下列訊息：

```
Received disconnect from 3.130.115.105 port 22:2: Too many authentication failures
Authentication failed.
```

Note

如果您使用API閘道並收到此錯誤，請參閱 [身分驗證失敗太多](#)。

原因

您尚未為使用者新增RSA金鑰對，因此您必須改用密碼進行身分驗證。

解決方案

當您執行 `sftp` 命令時，請指定 `-o PubkeyAuthentication=no` 選項。此選項會強制系統請求您的密碼。例如：

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

Managed AD 不相符領域問題

Description

使用者的領域及其群組領域必須相符。它們必須都位於預設領域中，或者它們都必須位於受信任領域中。

原因

如果使用者及其群組不相符，則轉接系列無法驗證使用者。如果您測試使用者的身分提供者，您會收到錯誤。找不到與使用者群組 相關聯的存取權。

解決方案

參考使用者領域中符合群組領域（預設或受信任）的群組。

其他身分驗證問題

Description

您會收到身分驗證錯誤，而且其他疑難排解都無法運作

原因

您可能已指定邏輯目錄的目標，其中包含正斜線或尾斜線（/）。

解決方案

更新您的邏輯目錄目標，以確保其以斜線開頭，且不包含尾斜線。例如，`/DOC-EXAMPLE-BUCKET/images` 是可接受的，但 `DOC-EXAMPLE-BUCKET/images` 和 `/DOC-EXAMPLE-BUCKET/images/` 是不可接受的。

對受管工作流程問題進行故障診斷

本節說明下列工作流程問題的可能解決方案。

主題

- [使用 Amazon 對工作流程相關錯誤進行故障診斷 CloudWatch](#)
- [對工作流程複製錯誤進行故障診斷](#)

使用 Amazon 對工作流程相關錯誤進行故障診斷 CloudWatch

Description

如果您的工作流程發生問題，您可以使用 Amazon CloudWatch 來調查原因。

原因

可能有幾個原因。使用 Amazon CloudWatch Logs 進行調查。

解決方案

Transfer Family 會向 CloudWatch Logs 發出工作流程執行狀態。下列類型的工作流程錯誤可能會出現在 CloudWatch 日誌中：

- "type": "StepErrored"
- "type": "ExecutionErrored"
- "type": "ExecutionThrottled"

- "Service failure on starting workflow"

您可以使用不同的篩選條件和模式語法來篩選工作流程的執行日誌。例如，您可以在 CloudWatch 日誌中建立日誌篩選條件，以擷取包含 ExecutionErrored 訊息的工作流程執行日誌。如需詳細資訊，請參閱 Amazon CloudWatch [Logs 使用者指南 中的使用訂閱和篩選條件和模式語法即時處理日誌資料](#)。

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/FilterAndPatternSyntax.html>

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"}}
```

在此，StepErrored 表示工作流程中的步驟已產生錯誤。在單一工作流程中，您可以設定多個步驟。此錯誤會告訴您錯誤發生的步驟，並提供錯誤訊息。在此特定範例中，該步驟設定為標記檔案；然而，不支援在 Amazon 檔案系統中標記 EFS 檔案，因此步驟會產生錯誤。

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，且如果該步驟無法執行，則整體工作流程會失敗。

Executionthrottled

如果工作流程以比系統可支援的速度更快的速度觸發，則執行會受到限制。此日誌訊息表示您必須降低工作流程的執行速率。如果您無法縮減工作流程執行率，請聯絡 AWS 支援 聯絡。 [AWS](#)

啟動工作流程時發生服務失敗

每當您從伺服器移除工作流程並將其取代為新的工作流程，或更新伺服器組態（這會影響工作流程的執行角色）時，您必須等待約 10 分鐘，才能執行新的工作流程。Transfer Family 伺服器快取工作流程詳細資訊，伺服器重新整理其快取需要 10 分鐘。

此外，您必須登出任何作用中 SFTP 工作階段，然後在 10 分鐘等待期後重新登入，以查看變更。

對工作流程複製錯誤進行故障診斷

Description

如果您正在執行包含複製上傳檔案步驟的工作流程，您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

來源檔案位於與目的地儲存貯體 AWS 區域 不同的 Amazon S3 儲存貯體中。

解決方案

如果您正在執行包含複製步驟的工作流程，請確定來源和目的地儲存貯體位於相同的 中 AWS 區域。

對工作流程解密問題進行故障診斷

Description

您的解密工作流程失敗，日誌訊息類似以下內容：

```
{
```



```

    "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 模式和相關聯的解密工作流程步驟。在上傳至 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FIPS核准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區塊密碼模式) 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，然後重新加密。下列程序說明您必須採取的步驟。

編輯您的PGP金鑰

1. 識別您必須透過執行編輯的金鑰 `gpg --list-keys`

這會傳回金鑰清單。每個金鑰都有類似下列的詳細資訊：

```

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`。

系統會回應有關 GnuPG 程式和指定金鑰的詳細資訊。

4. 在gpg>提示中，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偏好演算法。

5. 我們希望編輯 金鑰以保留除 以外的所有演算法OCB。執行 setpref命令，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
```

這會傳回下列詳細資訊：

```
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 進行更新，然後在提示確認變更時輸入您的密碼。
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。

對 Amazon EFS問題進行故障診斷

本節說明下列 Amazon EFS問題的可能解決方案。

主題

- [對遺失POSIX的設定檔進行故障診斷](#)
- [使用 Amazon 對邏輯目錄進行故障診斷 EFS](#)

對遺失POSIX的設定檔進行故障診斷

Description

如果您為伺服器使用 Amazon EFS儲存體，且使用自訂身分提供者，則必須提供 POSIX 設定檔給 AWS Lambda 函數。

原因

其中一個可能的原因，是我們用來建立 AWS Lambda Amazon API Gateway 方法的範本目前不包含 POSIX資訊。

如果您確實提供POSIX資訊，Transfer Family 可能無法正確剖析您用來提供POSIX資訊的格式。

解決方案

請確定您為 PosixProfile 參數提供 JSON元素給 Transfer Family。

例如，如果您使用的是 Python，則可以在剖析 PosixProfile 參數的位置新增以下行：

```
if PosixProfile:
    response_data["PosixProfile"] = json.loads(PosixProfile)
```

或者，在 JavaScript，您可以新增以下行，其中 *uid-value* 和 *gid-value* 分別代表使用者 ID（UID）和群組 ID（GID）的整數為 0 或更高：

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

這些程式碼範例會將 PosixProfile 參數作為JSON物件傳送至 Transfer Family，而不是字串。

此外，在 AWS Secrets Manager，您必須儲存 PosixProfile 參數，如下所示。*your-gid* 使用 *your-uid* 和 的實際值取代 GID 和 UID。

```
{"Uid": your-uid, "Gid": your-gid, "SecondaryGids": []}
```

使用 Amazon 對邏輯目錄進行故障診斷 EFS

Description

如果使用者的主目錄不存在，而且他們執行ls命令，系統會回應如下：

```
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來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，因為他們在邏輯主目錄mkdir上缺少 的許可。

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。

對身分提供者進行測試的疑難排解

Description

如果您使用主控台或 TestIdentityProvider API 呼叫來測試身分提供者，Response 欄位會是空的。例如：

```
{
  "Response": "{}",
  "StatusCode": 200,
  "Message": ""
}
```

原因

最可能的原因是身分驗證因使用者名稱或密碼不正確而失敗。

解決方案

請確定您使用使用者正確的憑證，並視需要更新使用者名稱或密碼。

為您的SFTP連接器新增受信任主機金鑰的故障診斷

Description

當您建立或編輯SFTP連接器時，且您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

如果您貼入正確的公有金鑰，問題可能是您已包含金鑰comment的部分。目前 AWS Transfer Family 不接受金鑰的註解部分。

解決方案

當您將金鑰貼到文字欄位中時，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，並僅貼到 鍵的 部分，直到 並包含 ==。

```
ssh-rsa AAAA...==
```

對檔案上傳問題進行故障診斷

本節說明下列檔案上傳問題的可能解決方案。

主題

- [對 Amazon S3 檔案上傳錯誤進行故障診斷](#)
- [對無法讀取的檔案名稱進行故障診斷](#)

對 Amazon S3 檔案上傳錯誤進行故障診斷

Description

當您嘗試使用 Transfer Family 將檔案上傳至 Amazon S3 儲存體時，會收到下列錯誤訊息：AWS 傳輸不支援隨機存取寫入 S3 物件。

原因

當您將 Amazon S3 用於伺服器的儲存時，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 作為儲存，請停用用戶端軟體提及使用多個連線進行單次傳輸的任何選項。

對無法讀取的檔案名稱進行故障診斷

Description

您會在部分上傳的檔案中看到檔案名稱損毀。使用者有時會遇到檔案名稱中某些字元的問題FTP和SFTP傳輸，例如謗音、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交涉檔案名稱的字元編碼，但 Amazon S3 和 Amazon EFS 則不允許。相反地，它們需要 UTF-8 字元編碼。因此，某些字元的轉譯不正確。

解決方案

若要解決此問題，請檢閱用戶端應用程式是否有檔案名稱字元編碼，並確認其設定為 UTF-8。

對ResourceNotFoundException例外狀況進行疑難排解

Description

您會收到找不到資源的錯誤。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

接收ResourceNotFoundException訊息有幾個原因。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 Transfer Family 伺服器位於 us-east-2，則您將收到未知的資源例外狀況。

如需設定預設區域的詳細資訊，請參閱[使用 進行快速組態aws configure](#)。

解決方案

將區域參數新增至API命令，以明確指定在何處尋找特定資源。

```
aws transfer -describe-server --server-id server-id --region us-east-2
```

連接器SFTP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

當金鑰交換交涉失敗時，您會收到錯誤。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

確保遠端伺服器支援錯誤訊息中列出的至少一個用戶端主機金鑰演算法。如需支援的演算法清單，請參閱 [SFTP 連接器演算法](#)。

其他SFTP連接器問題

Description

您在執行 後收到錯誤StartFileTransfer，但不知道問題的原因，而且只有連接器 ID 會在API呼叫後傳回。

原因

此錯誤可能有幾個原因。若要疑難排解，建議您測試連接器並搜尋 CloudWatch 日誌。

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 測試連接器 [TestConnection](#) API 命令。
- 檢視連接器的 CloudWatch 日誌：請參閱 [SFTP 連接器的日誌項目範例](#)。本主題提供SFTP連接器日誌項目的範例，以及可協助您尋找適當日誌的命名慣例。

針對 AS2 問題進行故障診斷

此處說明了啟用適用性聲明 2（AS2）的伺服器的錯誤訊息和疑難排解提示：[AS2 錯誤代碼](#)。

API 參考

下列各節記錄 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 是一項安全傳輸服務，可讓您透過下列通訊協定，在 Amazon Simple Storage Service (Amazon S3) 儲存體中來回傳輸檔案：

- 安全殼層 (SSH) 檔案傳輸通訊協定 (SFTP)
- 檔案傳輸通訊協定安全 (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金融服務、醫療保健、廣告和零售等不同產業的資料交換工作流程。AWS Transfer Family 可簡化檔案傳輸工作流程遷移至的過程 AWS。

若要使用 AWS Transfer Family 服務，您可以在您選擇的 AWS 區域中初始化伺服器。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。伺服器是向請求檔案操作的實體 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 OFFLINE）的服務帳單，以及傳輸的資料量。

請求檔案操作的伺服器必須知道使用者。使用者會由使用者名稱來識別，並指派給伺服器。使用者名稱用於驗證請求。伺服器只能有一個身分驗證方法：`AWS_DIRECTORY_SERVICE`、`AWS_LAMBDA_SERVICE_MANAGED`或 `API_GATEWAY`。

您可以使用下列任一身分提供者類型來驗證使用者：

- 對於 `SERVICE_MANAGED`，SSH公有金鑰會與使用者屬性存放在伺服器上。使用者可以在檔案中有一或多個SSH公有金鑰，用於`SERVICE_MANAGED`身分驗證方法。當用戶端請求`SERVICE_MANAGED`方法的檔案操作時，用戶端會提供使用者名稱和SSH私有金鑰，該金鑰已驗證，並提供存取權。
- 您可以透過選取身分驗證方法，使用 Microsoft Active Directory 群組管理使用者`AWS_DIRECTORY_SERVICE`身分驗證和存取。
- 您可以使用 連線到自訂身分提供者 AWS Lambda。選擇`AWS_LAMBDA`身分驗證方法。
- 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 使用來自身分提供者的API呼叫來驗證使用者請求。此方法在API通話`API_GATEWAY`中稱為 `Custom`。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。

使用者會被指派一個政策，其自身與 Amazon S3 儲存貯體之間具有信任關係。他們可以存取部分或所有儲存貯體。若要讓伺服器代表使用者行事，伺服器必須繼承使用者的信任關係。建立包含信任關係的 AWS Identity and Access Management (IAM) 角色，該角色會獲指派`AssumeRole`動作。然後，伺服器可以像使用者一樣執行檔案操作。

具有`home`目錄屬性集的使用者，該目錄（或資料夾）將作為檔案操作的目標和來源。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、使用者和角色都由其 Amazon Resource Name () 識別ARN。您可以將鍵值對的標籤指派給具有的實體ARN。標籤是可用於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。

下列慣例是以 AWS Transfer Family ID 格式觀察到的：

- `ServerId` 值採用 `s-01234567890abcdef` 的形式。
- `SshPublicKeyId` 值採用 `key-01234567890abcdef` 的形式。

Amazon Resource Name (ARN) 格式採用下列格式：

- 對於伺服器，ARNs請採用 表單`arn:aws:transfer:region:account-id:server/server-id`。

伺服器的範例ARN為：`arn:aws:transfer:us-east-1:123456789012:server/s-01234567890abcdef`。

- 對於使用者，請ARNs採用 表單`arn:aws:transfer:region:account-id:user/server-id/username`。

例如，`arn:aws:transfer:us-east-1:123456789012:user/s-01234567890abcdef/user1`。

DNS 使用中的項目（端點）如下所示：

- API 端點採用 形式`transfer.region.amazonaws.com`。
- 伺服器端點採用 `server.transfer.region.amazonaws.com` 的形式。

如需依 AWS 區域劃分的 Transfer Family 端點清單，請參閱中的[AWS Transfer Family 端點和配額](#) AWS 一般參考。

的此API介面參考 AWS Transfer Family 包含程式設計介面的文件，可用於管理 AWS Transfer Family。參考結構如下：

- 如需API動作的字母順序清單，請參閱 [Actions](#)。
- 如需資料類型的字母順序清單，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

與其實際執行 命令，您可以搭配任何API呼叫使用 `--generate-cli-skeleton` 參數來產生和顯示參數範本。然後，您可以使用產生的範本來自訂和使用 作為後續命令的輸入。如需詳細資訊，請參閱[產生和使用參數骨架檔案](#)。

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](#)
- [StartFileTransfer](#)
- [StartServer](#)
- [StopServer](#)
- [TagResource](#)
- [TestConnection](#)
- [TestIdentityProvider](#)
- [UntagResource](#)
- [UpdateAccess](#)
- [UpdateAgreement](#)
- [UpdateCertificate](#)
- [UpdateConnector](#)
- [UpdateHostKey](#)
- [UpdateProfile](#)
- [UpdateServer](#)
- [UpdateUser](#)

CreateAccess

管理員使用 `CreateAccess` 來選擇目錄中哪些群組應該有權使用 透過已啟用的通訊協定上傳和下載檔案 AWS Transfer Family。例如，Microsoft Active Directory 可能包含 50,000 個使用者，但只有一小部分需要能夠將檔案傳輸至伺服器。管理員可以使用 `CreateAccess` 將存取權限制為需要此能力的正確使用者集。

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](#)》。

請求接受下列JSON格式的資料。

[ExternalId](#)

識別目錄中特定群組所需的唯一識別碼。您關聯的群組使用者可透過使用的已啟用通訊協定存取您的 Amazon S3 或 Amazon EFS 資源 AWS Transfer Family。如果您知道群組名稱，則可以使用 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以 Active Directory 群組的名稱取代。

用來驗證此參數的規則運算式是由大寫和小寫英數字元組成的字串，不含空格。您也可以包含底線或以下任何字元：=, .@ : /-

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](#)

邏輯目錄映射，可指定使用者應看到哪些 Amazon S3 或 Amazon EFS 路徑和金鑰，以及您希望如何使其可見。您必須指定 Entry和 Target對，其中 Entry顯示如何顯示路徑，並且Target是實際的 Amazon S3 或 Amazon EFS 路徑。如果您只指定目標，則會顯示為原樣。您也必須確保 AWS Identity and Access Management (IAM) 角色提供對 中路徑的存取權Target。只有在 設定為 時，才能HomeDirectoryType設定此值LOGICAL。

以下是 Entry和 Target對範例。

```
[ { "Entry": "/directory1", "Target": "/bucket_name/home/mydirectory" } ]
```

在大多數情況下，您可以使用此值來取代工作階段政策，將使用者鎖定到指定的主目錄 ("chroot")。若要這麼做，您可以將 Entry 設定為 `/` 並將 Target 設定為 HomeDirectory 參數值。

以下是的 Entry 和 Target 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。最多 50000 個項目。

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。如果您將其設定為 PATH，則使用者會看到絕對 Amazon S3 儲存貯體或 Amazon EFS 路徑，就像在其檔案傳輸通訊協定用戶端一樣。如果您將其設定為 LOGICAL，則需要在 `HomeDirectoryMappings` 中提供映射，以了解如何讓使用者看見 Amazon S3 或 Amazon EFS 路徑。

Note

如果 HomeDirectoryType 是 LOGICAL，您必須使用 HomeDirectoryMappings 參數提供映射。另一方面，如果 HomeDirectoryType 是 PATH，則您使用 HomeDirectory 參數提供絕對路徑。您無法在範本 HomeDirectoryMappings 中同時擁有 HomeDirectory 和 `HomeDirectoryType`。

類型：字串

有效值: PATH | LOGICAL

必要：否

[Policy](#)

適用於使用者的工作階段政策，讓您可以在多個使用者之間使用相同的 AWS Identity and Access Management (IAM) 角色。此政策會減少使用者對其 Amazon S3 儲存貯體部分存取權的範圍。

您可以在此政策內使用的變數包括 `${Transfer:UserName}`、`${Transfer:HomeDirectory}` 和 `${Transfer:HomeBucket}`。

 Note

此政策僅適用於的網域ServerId為 Amazon S3 時。Amazon EFS 不會使用工作階段政策。

對於工作階段政策，會將政策 AWS Transfer Family 儲存為 JSON Blob，而不是政策的 Amazon Resource Name (ARN)。您可以將政策儲存為 BlobJSON，並將其傳遞到Policy引數中。

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 參考 [AssumeRole](#) 中的。AWS Security Token Service API

類型：字串

長度限制：長度下限為 0。長度上限為 2048。

必要：否

[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 IDs (SecondaryGids)，可控制使用者對 Amazon EFS 檔案系統的存取。檔案系統中檔案和目錄上設定的POSIX許可決定了使用者在將檔案移入和移出 Amazon EFS 檔案系統時所取得的存取層級。

類型：[PosixProfile](#) 物件

必要：否

[Role](#)

(ARN) 角色的 Amazon Resource Name AWS Identity and Access Management (IAM)，可控制使用者對 Amazon S3 儲存貯體或 Amazon EFS 檔案系統的存取。附加至此角色的政策會決定在將檔案移入和移出 Amazon S3 儲存貯體或 Amazon EFS 檔案系統時，您要為使用者提供的存取層級。此IAM角色也應包含信任關係，允許伺服器在服務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

長度限制條件：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，服務會傳回 HTTP 200 個回應。

服務會以 JSON 格式傳回下列資料。

ExternalId

群組的外部識別碼，其使用者可透過使用的已啟用通訊協定存取您的 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

使用者所連接之伺服器的識別碼。

類型：字串

長度限制條件：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](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式不正確的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceExistsException

請求的資源不存在，或存在於命令指定的區域以外的區域。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

HTTP 狀態碼：500

另請參閱

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)

- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

CreateAgreement

建立協議。協議是 AWS Transfer Family 伺服器與AS2程序之間的雙邊交易合作夥伴協議或合作夥伴關係。協議定義伺服器與 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。

合作夥伴會以 識別PartnerProfileId，而AS2程序則以 識別LocalProfileId。

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](#)》。

請求接受下列JSON格式的資料。

[AccessRole](#)

連接器用於使用 AS2或 SFTP通訊協定傳送檔案。針對存取角色，提供要使用 AWS Identity and Access Management 的角色的 Amazon Resource Name (ARN)。

對於AS2連接器

使用 AS2，您可以呼叫StartFileTransfer並指定請求參數 中的檔案路徑來傳送檔案SendFilePaths。我們使用檔案的父目錄（例如--send-file-paths /bucket/dir/file.txt，對於，父目錄為 /bucket/dir/）暫時存放已處理AS2的訊息檔案、MDN在我們從

合作夥伴收到時存放，以及撰寫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。

如果您為AS2連接器使用基本身分驗證，存取角色需要秘密的secretsmanager:GetSecretValue許可。如果秘密是使用客戶受管金鑰而非 Secrets Manager 中的 AWS 受管金鑰加密，則角色也需要該金鑰的kms:Decrypt許可。

對於SFTP連接器

請確定存取角色提供對StartFileTransfer請求中所用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 secretsmanager:GetSecretValue許可 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符。

類型：字串

長度限制條件：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

長度限制條件：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。這是協議使用的特定伺服器。

類型：字串

長度限制條件：固定長度為 19。

模式：s-([0-9a-f]{17})

必要：是

Status

協議的狀態。協議可以是 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，服務會傳回 HTTP 200 個回應。

服務會以 JSON 格式傳回下列資料。

[AgreementId](#)

協議的唯一識別符。使用此 ID 刪除或更新合約，以及任何其他需要您指定合約 ID 的 API 通話。

類型：字串

長度限制條件：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](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式不正確的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceExistsException

請求的資源不存在，或存在於命令指定的區域以外的區域。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

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 協議，並傳回 協議 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 呼叫會傳回新協議的協議 ID。

```
{
```

```
"AgreementId": "a-11112222333344444"  
}
```

另請參閱

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

CreateConnector

建立連接器，該連接器會擷取 AS2 或 SFTP 通訊協定連線的參數。對於 AS2，傳送檔案至外部託管 AS2 伺服器時需要連接器。對於 SFTP，傳送檔案至 SFTP 伺服器或從伺服器接收檔案時，需要連接器 SFTP。如需連接器的詳細資訊，請參閱[設定 AS2 連接器](#)和[建立 SFTP 連接器](#)。

Note

您必須只指定一個組態物件：針對 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",
  "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](#)》。

請求接受下列JSON格式的資料。

[AccessRole](#)

連接器用於使用 AS2 或 SFTP 通訊協定傳送檔案。針對存取角色，提供要使用 AWS Identity and Access Management 的角色的 Amazon Resource Name (ARN)。

對於AS2連接器

使用 AS2，您可以呼叫 `StartFileTransfer` 並指定請求參數 中的檔案路徑來傳送檔案 `SendFilePaths`。我們使用檔案的父目錄（例如 `--send-file-paths /bucket/dir/file.txt`，對於，父目錄為 `/bucket/dir/`）暫時存放已處理AS2的訊息檔案、在我們從合作夥伴收到MDN時存放，以及撰寫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。

如果您為AS2連接器使用基本身分驗證，存取角色需要秘密的 `secretsmanager:GetSecretValue` 許可。如果秘密是使用客戶管理金鑰而非 `Secrets Manager` 中的 AWS 受管金鑰加密，則角色也需要該金鑰的 `kms:Decrypt` 許可。

對於SFTP連接器

請確定存取角色提供對 `StartFileTransfer` 請求中所用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 `secretsmanager:GetSecretValue` 許可 `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](#)

(ARN) 角色的 Amazon Resource Name AWS Identity and Access Management (IAM) , 允許連接器開啟 Amazon S3 事件 CloudWatch 的記錄。設定時, 您可以在 CloudWatch 日誌中檢視連接器活動。

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

[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。標籤是為任何目的連接到連接器的中繼資料。

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](#)

URL 合作夥伴AS2或SFTP端點的。

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，服務會傳回 200 HTTP 個回應。

服務會以 JSON 格式傳回下列資料。

ConnectorId

連接器的唯一識別符，在API呼叫成功後傳回。

類型：字串

長度限制條件：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](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式不正確的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceExistsException

請求的資源不存在，或存在於命令指定的區域以外的區域。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

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，依下列方式取代項目：

- `url`：URL為交易合作夥伴的AS2伺服器提供。
- `your-IAM-role-for-bucket-access`：可存取您用來存放檔案的 Amazon S3 儲存貯體IAM的角色。
- 將 ARN用於您的記錄角色，其中包含您的 AWS 帳戶 ID。
- 提供包含AS2連接器組態參數的檔案路徑。AS2 連接器組態物件說明於 [As2ConnectorConfig](#)。

```
// 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，依下列方式取代項目：

- `sftp-server-url`：URL為您交換檔案的SFTP伺服器提供。
- `your-IAM-role-for-bucket-access`：可存取您用來存放檔案的 Amazon S3 儲存貯體IAM的角色。
- 將 ARN用於您的記錄角色，其中包含您的 AWS 帳戶 ID。
- 提供包含SFTP連接器組態參數的檔案路徑。SFTP 連接器組態物件說明於 [SftpConnectorConfig](#)。

```
// 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 ID。

回應範例

```
{  
  "ConnectorId": "a-11112222333344444"
```



```
}
```

另請參閱

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

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](#)》。

請求接受下列JSON格式的資料。

As2Id

As2Id 是 AS2-name，如 [RFC4130](#) 中所定義。對於傳入傳輸，這是從合作夥伴AS2傳送訊息的AS2-From標頭。對於傳出連接器，這是使用 StartFileTransferAPI操作傳送給合作夥伴AS2的訊息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

長度限制條件：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 以建立本機設定檔。本機設定檔代表 AS2 已啟用的 Transfer Family 伺服器組織或方。
- 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 設定檔的鍵值對。

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

```
{
  "ProfileId": "string"
}
```

回應元素

如果動作成功，服務會傳回 200 HTTP 個回應。

服務會以 JSON 格式傳回下列資料。

[ProfileId](#)

AS2 設定檔的唯一識別碼，在 API 呼叫成功後傳回。

類型：字串

長度限制條件：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](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式不正確的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

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

下列範例會建立設定檔，並傳回設定檔 ID。

憑證IDs會在您執行 `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設定檔 ID。

```
{  
  "ProfileId": "p-11112222333344444"  
}
```

另請參閱

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 .NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

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](#)》。

請求接受下列JSON格式的資料。

Certificate

(ARN) 憑證的 Amazon Resource Name AWS Certificate Manager (ACM)。當 Protocols 設定為 FTPS 時，此為必要項目。

若要請求新的公有憑證，請參閱 AWS Certificate Manager 使用者指南 中的[請求公有憑證](#)。

若要將現有憑證匯入 ACM，請參閱 使用者指南 中的[將憑證匯入 ACM](#)。 AWS Certificate Manager

若要FTPS透過私有 IP 地址請求私有憑證，請參閱 AWS Certificate Manager 使用者指南 中的[請求私有憑證](#)。

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

憑證必須是指定 FQDN 或 IP 地址的有效 SSL/TLS X.509 第 3 版憑證，以及發行者的相關資訊。

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。有兩個可用網域：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

為您的伺服器設定的虛擬私有雲端 (VPC) 端點設定。當您在 中託管端點時VPC，您只能讓 中的資源存取端點VPC，也可以連接彈性 IP 地址，讓用戶端透過網際網路存取端點。您 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

您希望您的伺服器使用的端點類型。您可以選擇讓伺服器的端點公開存取（PUBLIC），或在 中託管它VPC。使用託管在 中的端點VPC，您只能限制對伺服器和資源的存取，VPC或選擇直接將彈性 IP 地址連接到網際網路，使其面向網際網路。

Note

2021 年 5 月 19 日後，AWS 帳戶 如果您的帳戶未在 2021 年 5 月 19 日之前建立伺服器，您將無法在 EndpointType=VPC_ENDPOINT中使用 建立伺服器。如果您已 AWS 帳戶 在 2021 年 5 月 19 日或之前在 EndpointType=VPC_ENDPOINT中使用 建立伺服器，則不會受到影響。在此日期之後，請使用 EndpointType=VPC。

如需詳細資訊，請參閱[停止使用 VPC_ENDPOINT](#)。

建議使用 VPC 作為 EndpointType。透過此端點類型，您可以選擇直接將最多三個彈性 IPv4地址（BYO 包含 IP）與伺服器的端點建立關聯，並使用VPC安全群組來限制用戶端公有 IP 地址的流量。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

用於SFTP已啟用 RSA之伺服器的 ECDSA、或 ED25519 私有金鑰。您可以新增多個主機金鑰，以防您想要輪換金鑰，或擁有一組使用不同演算法的作用中金鑰。

使用下列命令來產生沒有密碼的 RSA 2048 位元金鑰：

```
ssh-keygen -t rsa -b 2048 -N "" -m PEM -f my-new-server-key.
```

針對 -b選項使用最小值 2048。您可以使用 3072 或 4096 建立更強大的金鑰。

使用下列命令來產生沒有密碼的 ECDSA 256 位元金鑰：

```
ssh-keygen -t ecdsa -b 256 -N "" -m PEM -f my-new-server-key.
```

-b 的選項的有效值ECDSA為 256、384 和 521。

使用下列命令來產生沒有複雜密碼的ED25519金鑰：

```
ssh-keygen -t ed25519 -N "" -f my-new-server-key.
```

對於所有這些命令，您可以使用您選擇的字串my-new-server-key取代。

Important

如果您不打算將現有使用者從已啟用 SFTP的現有伺服器遷移至新的伺服器，請勿更新主機金鑰。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 使用者指南 中的[更新SFTP已啟用 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](#)

當 IdentityProviderType 設定為 AWS_DIRECTORY_SERVICE、AWS_LAMBDA或 時為必要API_GATEWAY。接受陣列，其中包含在 中使用目錄AWS_DIRECTORY_SERVICE或叫用客戶提供的身分驗證 所需的所有資訊API，包括API閘道 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 服務中存放和存取使用者憑證。

使用 AWS_DIRECTORY_SERVICE 可讓您存取內部部署環境 AWS Directory Service for Microsoft Active Directory 或使用 AWS AD Connector 的 或 Microsoft Active Directory 中的 Active Directory 群組。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。此API_GATEWAY設定要求您提供 Amazon API Gateway 端點URL，以使用 IdentityProviderDetails 參數呼叫以進行身分驗證。

使用 `AWS_LAMBDA` 值直接使用 AWS Lambda 函數作為您的身分提供者。如果您選擇此值，您必須在 `IdentityProviderDetails` 資料類型 ARN 的 `Function` 參數中指定 Lambda 函數的。

類型：字串

有效值：`SERVICE_MANAGED` | `API_GATEWAY` | `AWS_DIRECTORY_SERVICE` | `AWS_LAMBDA`

必要：否

[LoggingRole](#)

(ARN) 角色的 Amazon Resource Name AWS Identity and Access Management (IAM)，允許伺服器開啟 Amazon S3 或 Amazon 的 Amazon CloudWatch 記錄 `EFSevents`。設定時，您可以在 CloudWatch 日誌中檢視使用者活動。

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。

- 若要指示被動模式（適用於 FTP 和 FTPS 通訊協定），請使用 `PassiveIp` 參數。輸入單一虛線四元 IPv4 地址，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 `SETSTAT` 命令並上傳檔案，而不需要對 SFTP 用戶端進行任何變更，請將值設定為 `ENABLE_NO_OP`。如果您將 `SetStatOption` 參數設定為 `ENABLE_NO_OP`，Transfer Family 會產生 Amazon CloudWatch Logs 的日誌項目，以便您判斷用戶端何時 `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 來恢復最近的交涉工作階段，請使用 `TlsSessionResumptionMode` 參數。
- `As2Transports` 表示 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（Secure Shell（SSH）檔案傳輸通訊協定）：檔案傳輸 SSH
- FTPS（檔案傳輸通訊協定安全）：使用 TLS 加密進行檔案傳輸
- FTP（檔案傳輸通訊協定）：未加密的檔案傳輸
- AS2（適用性陳述式 2）：用於傳輸結構化 business-to-business 資料

Note

- 如果您選擇 FTPS，您必須選擇儲存在 AWS Certificate Manager (ACM) 中的憑證，當用戶端透過連線到伺服器時，該憑證可用來識別您的伺服器FTPS。
- 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。

有效值:SFTP | FTP | FTPS | AS2

必要：否

S3StorageOptions

指定是否最佳化 Amazon S3 目錄的效能。此選項根據預設為停用。

根據預設，主目錄映射具有 TYPE的 DIRECTORY。如果您啟用此選項，則HomeDirectoryMapEntryTypeFILE如果您想要映射具有檔案目標，則需要將 明確設定為。

類型：[S3StorageOptions](#) 物件

必要：否

SecurityPolicyName

指定連接至伺服器的安全政策名稱。

類型：字串

長度限制：長度下限為 0。長度上限為 100。

模式：TransferSecurityPolicy-.+

必要：否

[StructuredLogDestinations](#)

指定伺服器日誌的傳送目的地日誌群組。

若要指定日誌群組，您必須ARN為現有日誌群組提供。在此情況下，日誌群組的格式如下：

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日誌群組，您可以清除該群組，並在update-server通話中提供此參數的空值，從而實際上關閉結構化日誌。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)。當伺服器工作階段在檔案仍在上傳時中斷連線時，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，服務會傳回 200 HTTP 個回應。

服務會以 JSON 格式傳回下列資料。

[ServerId](#)

建立之伺服器的服務指派識別碼。

類型：字串

長度限制條件：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 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式不正確的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceExistsException

請求的資源不存在，或存在於命令指定的區域以外的區域。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

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 建立新的伺服器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

如需在其中一種語言特定的 API中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

CreateUser

建立使用者，並將其與已啟用檔案傳輸通訊協定的現有伺服器建立關聯。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、儲存使用者的公有金鑰，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](#)》。

請求接受下列JSON格式的資料。

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

邏輯目錄映射，指定使用者應看到哪些 Amazon S3 或 Amazon EFS 路徑和金鑰，以及您希望如何使其可見。您必須指定 Entry 和 Target 對，其中 Entry 顯示如何顯示路徑，並且 Target 是實際的 Amazon S3 或 Amazon EFS 路徑。如果您只指定目標，則會顯示為原樣。您也必須確保 AWS Identity and Access Management (IAM) 角色提供對中路徑的存取權 Target。只有在設定為時，才能 HomeDirectoryType 設定此值 LOGICAL。

以下是 Entry 和 Target 對範例。

```
[ { "Entry": "/directory1", "Target": "/bucket_name/home/mydirectory" } ]
```

在大多數情況下，您可以使用此值來取代工作階段政策，將使用者鎖定到指定的主目錄 (`"chroot"`)。若要這麼做，您可以將 Entry 設定為 `/` 並將 Target 設定為使用者登入時，其主目錄應看到的值。

以下是的 Entry 和 Target 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。最多 50000 個項目。

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。如果您將其設定為 PATH，則使用者會看到絕對 Amazon S3 儲存貯體或 Amazon EFS 路徑，就像在其檔案傳輸通訊協定用戶端一樣。如果您將其設定為 LOGICAL，則需要在 [中](#) 提供映射，[HomeDirectoryMappings](#)以了解如何讓使用者看見 Amazon S3 或 Amazon EFS 路徑。

Note

如果 `HomeDirectoryType` 是 LOGICAL，您必須使用 `HomeDirectoryMappings` 參數提供映射。另一方面，如果 `HomeDirectoryType` 是 PATH，您可以使用 `HomeDirectory` 參數提供絕對路徑。您無法在範本 `HomeDirectoryMappings` 中同時擁有 `HomeDirectory` 和 `HomeDirectoryMappings`。

類型：字串

有效值:PATH | LOGICAL

必要：否

[Policy](#)

適用於使用者的工作階段政策，讓您可以在多個使用者之間使用相同的 AWS Identity and Access Management (IAM) 角色。此政策會減少使用者對其 Amazon S3 儲存貯體部分存取權的範圍。您可以在此政策內使用的變數包括 `${Transfer:UserName}`、`${Transfer:HomeDirectory}` 和 `${Transfer:HomeBucket}`。

Note

此政策僅適用於 `ServerId` 為 Amazon S3 時。Amazon EFS 不會使用工作階段政策。
對於工作階段政策，會將政策 AWS Transfer Family 儲存為 JSON Blob，而不是政策的 Amazon Resource Name (ARN)。您可以將政策儲存為 BlobJSON，並將其傳遞至 `Policy` 引數中。

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 安全權杖服務參考 [AssumeRole](#) 中的 。 AWS API

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POSIX身分，包括使用者 ID (Uid)、群組 ID (Gid) 和任何次要群組 IDs (SecondaryGids)，以控制使用者對 Amazon EFS 檔案系統的存取。在 Amazon 檔案和目錄上設定的POSIX許可EFS決定了使用者在傳輸檔案進出 Amazon EFS 檔案系統時所取得的存取層級。

類型：[PosixProfile](#) 物件

必要：否

[Role](#)

(ARN) 角色的 Amazon Resource Name AWS Identity and Access Management (IAM)，可控制使用者對 Amazon S3 儲存貯體或 Amazon EFS 檔案系統的存取。附加至此角色的政策會決定在將檔案移入和移出 Amazon S3 儲存貯體或 Amazon EFS 檔案系統時，您要為使用者提供的存取層級。此IAM角色還應包含信任關係，允許伺服器在為使用者的傳輸請求提供服務時存取您的資源。

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

長度限制條件：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 Secure Shell (SSH) 金鑰公有部分。

三個標準SSH公有金鑰格式元素為 <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、ecdsa-sha2-nistp384或 ecdsa-sha2-nistp521，取決於您產生的金鑰大小。

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，服務會傳回 HTTP 200 個回應。

服務會以 JSON 格式傳回下列資料。

[ServerId](#)

使用者所連接之伺服器的識別碼。

類型：字串

長度限制條件：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](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式錯誤的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceExistsException

請求的資源不存在，或存在於命令指定的區域以外的區域。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

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，例如 `createUserParameters`，然後執行 `create-user` 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

如需在其中一種語言特定 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 .NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

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](#)》。

請求接受下列JSON格式的資料。

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 函數需要傳回FAILURE至呼叫API，以啟動例外步驟。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。

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，僅在 S3 上支援複製和標記。

對於檔案位置，您可以指定 Amazon S3 儲存貯體和金鑰，或 Amazon EFS 檔案系統 ID 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。

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，服務會傳回 HTTP 200 個回應。

服務會以 JSON 格式傳回下列資料。

[WorkflowId](#)

工作流程的唯一識別碼。

類型：字串

長度限制條件：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

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式不正確的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceExistsException

請求的資源不存在，或存在於命令指定的區域以外的區域。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

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

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 .NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

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](#)》。

請求接受下列JSON格式的資料。

ExternalId

識別目錄中特定群組所需的唯一識別碼。您關聯的群組使用者可透過使用的已啟用通訊協定存取您的 Amazon S3 或 Amazon EFS 資源 AWS Transfer Family。如果您知道群組名稱，則可以使用 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以 Active Directory 群組的名稱取代。

用來驗證此參數的規則運算式是由大寫和小寫英數字元組成的字串，不含空格。您也可以包含底線或以下任何字元：=, .@ : /-

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

系統指派的唯一識別碼，適用於已指派此使用者的伺服器。

類型：字串

長度限制條件：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，服務會傳回 200 HTTP 回應，其中內 HTTP 文為空白。

錯誤

如需所有動作常見錯誤的資訊，請參閱[常見錯誤](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式不正確的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

HTTP 狀態碼：500

另請參閱

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

DeleteAgreement

刪除所提供 中指定的協議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](#)》。

請求接受下列JSON格式的資料。

AgreementId

協議的唯一識別符。當您建立協議時，會傳回此識別碼。

類型：字串

長度限制條件：固定長度為 19。

模式：a-([0-9a-f]{17})

必要：是

ServerId

與您要刪除之協議相關聯的伺服器識別碼。

類型：字串

長度限制條件：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，服務會傳回 200 HTTP 回應，其中內HTTP文為空白。

錯誤

如需所有動作常見錯誤的資訊，請參閱[常見錯誤](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式不正確的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

HTTP 狀態碼：500

另請參閱

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 .NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

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](#)》。

請求接受下列JSON格式的資料。

CertificateId

您要刪除之憑證物件的識別碼。

類型：字串

長度限制條件：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，服務會傳回 200 HTTP 回應，其中內HTTP文為空白。

錯誤

如需所有動作常見錯誤的資訊，請參閱[常見錯誤](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式不正確的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

HTTP 狀態碼：500

另請參閱

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

DeleteConnector

刪除所提供 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](#)》。

請求接受下列JSON格式的資料。

ConnectorId

連接器的唯一識別符。

類型：字串

長度限制條件：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，服務會傳回 200 HTTP 回應，其中內HTTP文為空白。

錯誤

如需所有動作常見錯誤的資訊，請參閱[常見錯誤](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式錯誤的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

HTTP 狀態碼：500

另請參閱

如需在其中一種語言特定 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

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](#)》。

請求接受下列JSON格式的資料。

HostKeyId

您要刪除之主機金鑰的識別碼。

類型：字串

長度限制條件：固定長度為 25。

模式：hostkey-[0-9a-f]{17}

必要：是

ServerId

包含您要刪除之主機金鑰的伺服器識別碼。

類型：字串

長度限制條件：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，服務會傳回 200 HTTP 回應，其中內HTTP文為空白。

錯誤

如需所有動作常見錯誤的資訊，請參閱[常見錯誤](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式不正確的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

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

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 .NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)

- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

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](#)》。

請求接受下列JSON格式的資料。

ProfileId

您要刪除之設定檔的識別碼。

類型：字串

長度限制條件：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，服務會傳回 200 HTTP 回應，其中內HTTP文為空白。

錯誤

如需所有動作常見錯誤的資訊，請參閱[常見錯誤](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式錯誤的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

HTTP 狀態碼：500

另請參閱

如需在其中一種語言特定 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

DeleteServer

刪除您指定的已啟用檔案傳輸通訊協定的伺服器。

此操作不會傳回任何回應。

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](#)》。

請求接受下列JSON格式的資料。

ServerId

伺服器執行個體的唯一系統指派識別符。

類型：字串

長度限制條件：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，服務會傳回 200 HTTP 回應，其中內HTTP文為空白。

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

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式不正確的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

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，則不會傳回任何內容。

回應範例

```
{
```

```
}
```

另請參閱

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

DeleteSshPublicKey

刪除使用者的 Secure Shell (SSH) 公有金鑰。

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](#)》。

請求接受下列JSON格式的資料。

ServerId

系統指派的唯一識別符，適用於使用者指派至檔案傳輸協定啟用伺服器執行個體。

類型：字串

長度限制條件：固定長度為 19。

模式：s-([0-9a-f]{17})

必要：是

SshPublicKeyId

用於參考使用者特定SSH金鑰的唯一識別符。

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

唯一字串，用於識別要刪除公有金鑰的使用者。

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，服務會傳回 200 HTTP 回應，其中內 HTTP 文為空白。

錯誤

如需所有動作常見錯誤的資訊，請參閱[常見錯誤](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式不正確的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

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SSH公有金鑰。

請求範例

```
{
  "ServerId": "s-01234567890abcdef",
  "SshPublicKeyId": "MyPublicKey",
  "UserName": "my_user"
}
```

另請參閱

如需在其中一種語言特定的 API中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

DeleteUser

刪除屬於您指定已啟用檔案傳輸通訊協定之伺服器的使用者。

此操作不會傳回任何回應。

Note

當您從伺服器刪除使用者時，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](#)》。

請求接受下列JSON格式的資料。

ServerId

系統指派的唯一識別符，適用於已將使用者指派給該執行個體的伺服器執行個體。

類型：字串

長度限制條件：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，服務會傳回 200 HTTP 回應，其中內 HTTP 文為空白。

錯誤

如需所有動作常見錯誤的資訊，請參閱[常見錯誤](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式不正確的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

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

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

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

長度限制條件：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，服務會傳回 200 HTTP 回應，其中內HTTP文為空白。

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

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式錯誤的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

HTTP 狀態碼：500

另請參閱

如需在其中一種語言特定 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

DescribeAccess

描述指派給特定檔案傳輸協定啟用伺服器的存取權，如其ServerId屬性及其所識別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](#)》。

請求接受下列JSON格式的資料。

ExternalId

識別目錄中特定群組所需的唯一識別碼。您關聯的群組使用者可透過使用的已啟用通訊協定存取您的 Amazon S3 或 Amazon EFS 資源 AWS Transfer Family。如果您知道群組名稱，則可以使用 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以 Active Directory 群組的名稱取代。

用來驗證此參數的規則運算式是由大寫和小寫英數字元組成的字串，不含空格。您也可以包含底線或以下任何字元：=, .@ : /-

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

已指派此存取權之伺服器的系統指派唯一識別碼。

類型：字串

長度限制條件：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，服務會傳回 HTTP 200 個回應。

服務會以 JSON 格式傳回下列資料。

Access

連接存取之伺服器的外部識別碼。

類型：[DescribedAccess](#) 物件

[ServerId](#)

已指派此存取權之伺服器的系統指派唯一識別碼。

類型：字串

長度限制條件：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](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式不正確的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

HTTP 狀態碼：500

另請參閱

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)

- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

DescribeAgreement

描述 識別的協議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](#)》。

請求接受下列JSON格式的資料。

AgreementId

協議的唯一識別符。當您建立協議時，會傳回此識別碼。

類型：字串

長度限制條件：固定長度為 19。

模式：a-([0-9a-f]{17})

必要：是

ServerId

與協議相關聯的伺服器識別碼。

類型：字串

長度限制條件：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，服務會傳回 200 HTTP 個回應。

服務會以 JSON 格式傳回下列資料。

Agreement

指定協議的詳細資訊，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 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式不正確的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

HTTP 狀態碼：500

另請參閱

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

DescribeCertificate

描述 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

長度限制條件：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，服務會傳回 HTTP 200 個回應。

服務會以 JSON 格式傳回下列資料。

Certificate

指定憑證的詳細資訊，傳回為物件。

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](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式錯誤的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

HTTP 狀態碼：500

另請參閱

如需在其中一種語言特定 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

DescribeConnector

描述 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](#)》。

請求接受下列JSON格式的資料。

ConnectorId

連接器的唯一識別符。

類型：字串

長度限制條件：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",
  "ServiceManagedEgressIpAddresses": [ "string" ],
  "SftpConfig": {
    "TrustedHostKeys": [ "string" ],
    "UserSecretId": "string"
  },
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ],
  "Url": "string"
}
```

回應元素

如果動作成功，服務會傳回 HTTP 200 個回應。

服務會以 JSON 格式傳回下列資料。

[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](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式不正確的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

HTTP 狀態碼：500

另請參閱

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

DescribeExecution

您可以使用 `DescribeExecution` 來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訊。

如果您為未進行中的執行提供 ID，或者執行不符合指定的工作流程 ID，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](#)》。

請求接受下列JSON格式的資料。

ExecutionId

用於執行工作流程的唯一識別碼。

類型：字串

長度限制條件：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

長度限制條件：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，服務會傳回 200 HTTP 個回應。

服務會以 JSON 格式傳回下列資料。

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

長度限制條件：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](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式不正確的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

HTTP 狀態碼：500

另請參閱

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

DescribeHostKey

傳回 HostKeyId 和 指定的主機金鑰詳細資訊 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](#)》。

請求接受下列JSON格式的資料。

HostKeyId

您想要描述的主機金鑰的識別碼。

類型：字串

長度限制條件：固定長度為 25。

模式：hostkey-[0-9a-f]{17}

必要：是

ServerId

包含您想要描述之主機金鑰的伺服器識別碼。

類型：字串

長度限制條件：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，服務會傳回 HTTP 200 個回應。

服務會以 JSON 格式傳回下列資料。

[HostKey](#)

傳回指定主機金鑰的詳細資訊。

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](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式不正確的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

HTTP 狀態碼：500

另請參閱

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

DescribeProfile

傳回 指定的設定檔詳細資訊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](#)》。

請求接受下列JSON格式的資料。

ProfileId

您想要描述之設定檔的識別碼。

類型：字串

長度限制條件：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，服務會傳回 200 HTTP 個回應。

服務會以 JSON 格式傳回下列資料。

[Profile](#)

指定設定檔的詳細資訊，傳回為物件。

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](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式不正確的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

HTTP 狀態碼：500

另請參閱

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

DescribeSecurityPolicy

描述連接至已啟用檔案傳輸通訊協定之伺服器的安全政策。回應包含安全政策屬性的說明。如需安全政策的詳細資訊，請參閱[使用安全政策](#)。

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](#)》。

請求接受下列JSON格式的資料。

SecurityPolicyName

指定連接至伺服器的安全政策名稱。

類型：字串

長度限制：長度下限為 0。長度上限為 100。

模式：TransferSecurityPolicy-.*

必要：是

回應語法

```
{
  "SecurityPolicy": {
    "Fips": boolean,
    "SecurityPolicyName": "string",
    "SshCiphers": [ "string" ],
    "SshKexs": [ "string" ],
    "SshMacs": [ "string" ],
    "TlsCiphers": [ "string" ]
  }
}
```

回應元素

如果動作成功，服務會傳回 200 HTTP 個回應。

服務會以 JSON 格式傳回下列資料。

[SecurityPolicy](#)

包含安全政策屬性的陣列。

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](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式不正確的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

HTTP 狀態碼：500

範例

範例

下列範例命令會將安全政策名稱作為引數，並傳回指定安全政策的演算法。

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

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

DescribeServer

描述您透過傳遞 `ServerId` 參數指定的已啟用檔案傳輸通訊協定的伺服器。

回應包含伺服器屬性的說明。當您將 `EndpointType` 設定為 `VPC`，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](#)》。

請求接受下列JSON格式的資料。

ServerId

伺服器的系統指派唯一識別碼。

類型：字串

長度限制條件：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，服務會傳回 200 HTTP 個回應。

服務會以 JSON 格式傳回下列資料。

Server

陣列，其中包含具有ServerID您指定之 的伺服器屬性。

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](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式不正確的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

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 的一個用量 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

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 .NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

DescribeUser

描述指派給特定檔案傳輸協定啟用伺服器的使用者，如其ServerId屬性所識別。

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](#)》。

請求接受下列JSON格式的資料。

ServerId

系統指派的唯一識別碼，適用於已指派此使用者的伺服器。

類型：字串

長度限制條件：固定長度為 19。

模式：s-([0-9a-f]{17})

必要：是

UserName

指派給一或多個伺服器的使用者名稱。使用者名稱是登入憑證的一部分，可用來使用 AWS Transfer Family 服務和執行檔案傳輸任務。

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，服務會傳回 HTTP 200 個回應。

服務會以 JSON 格式傳回下列資料。

ServerId

系統指派的唯一識別碼，適用於已指派此使用者的伺服器。

類型：字串

長度限制條件：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 使用者屬性。

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](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式錯誤的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

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.amazonaws.com",
        "SshPublicKeyId": "key-abcde12345fghik67"
      }
    ],
    "Tags": [],
    "UserName": "bob-test"
  }
}
```

另請參閱

如需在其中一種語言特定 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 .NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)

- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

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

長度限制條件：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，服務會傳回 HTTP 200 個回應。

服務會以 JSON 格式傳回下列資料。

[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](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式不正確的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

HTTP 狀態碼：500

另請參閱

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

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](#)》。

請求接受下列JSON格式的資料。

ActiveDate

選擇性日期，指定憑證變為作用的時間。

類型：Timestamp

必要：否

Certificate

- 對於 CLI，會以 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

選擇性的憑證清單，構成匯入憑證的鏈。

類型：字串

長度限制：長度下限為 1。長度上限為 2097152。

模式：`[\u0009\u000A\u000D\u0020-\u00FF]*`

必要：否

Description

有助於識別憑證的簡短描述。

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

InactiveDate

選擇性日期，指定憑證變為停用的時間。

類型：Timestamp

必要：否

PrivateKey

- 對於 CLI，請以 URI 格式提供私有金鑰的檔案路徑。例如，`--private-key file://encryption-key.pem`。或者，您可以提供私有金鑰檔案的原始內容。
- 針對 SDK，指定私有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

指定此憑證用於簽署或加密。

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，服務會傳回 HTTP 200 個回應。

服務會以 JSON 格式傳回下列資料。

[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

長度限制條件：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](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式不正確的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

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，我們提供憑證和憑證鏈檔案的內容。針對 SDK 命令使用此格式。

```
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，除了我們為私有金鑰、憑證和憑證鏈檔案提供檔案位置。如果您使用的是 `awscli`，則此版本的命令無法運作SDK。

```
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

如需在其中一種語言特定的 API中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

ImportHostKey

將主機金鑰新增至 ServerId 參數指定的伺服器。

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](#)》。

請求接受下列JSON格式的資料。

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

金鑰對的私有SSH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](#)

包含您匯入之主機金鑰的伺服器識別碼。

類型：字串

長度限制條件：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鍵值對。

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

```
{
  "HostKeyId": "string",
  "ServerId": "string"
}
```

回應元素

如果動作成功，服務會傳回 HTTP 200 個回應。

服務會以 JSON 格式傳回下列資料。

[HostKeyId](#)

傳回匯入金鑰的主機金鑰識別符。

類型：字串

長度限制條件：固定長度為 25。

模式：hostkey-[0-9a-f]{17}

ServerId

傳回包含匯入金鑰的伺服器識別碼。

類型：字串

長度限制條件：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](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式不正確的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceExistsException

請求的資源不存在，或存在於命令指定的區域以外的區域。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

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

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

ImportSshPublicKey

將 Secure Shell (SSH) 公有金鑰新增至 Transfer Family 使用者，該使用者由 UserName 指定給已啟用特定檔案傳輸通訊協定的伺服器，並由 識別ServerId。

回應會傳回 UserName的值、ServerId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](#)》。

請求接受下列JSON格式的資料。

[ServerId](#)

伺服器的系統指派唯一識別碼。

類型：字串

長度限制條件：固定長度為 19。

模式：s-([0-9a-f]{17})

必要：是

[SshPublicKeyBody](#)

金鑰對的公SSH有金鑰部分。

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

指派給一或多個伺服器的 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，服務會傳回 200 HTTP 個回應。

服務會以 JSON 格式傳回下列資料。

ServerId

伺服器的系統指派唯一識別碼。

類型：字串

長度限制條件：固定長度為 19。

模式：`s-([0-9a-f]{17})`

SshPublicKeyId

系統匯入的公有金鑰名稱。

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](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式不正確的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceExistsException

請求的資源不存在，或存在於命令指定的區域以外的區域。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

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

此命令會匯入存放在id_ecdsa.pub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

如果您執行上一個命令，系統會傳回下列資訊。

```
{
  "ServerId": "s-021345abcdef6789",
  "SshPublicKeyId": "key-1234567890abcdef0",
  "UserName": "jane-doe"
}
```

另請參閱

如需在其中一種語言特定的 API中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)

- [AWS SDK 適用於 Ruby V3](#)

ListAccesses

列出您在伺服器上擁有的所有存取權的詳細資訊。

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](#)》。

請求接受下列JSON格式的資料。

MaxResults

指定SIDs要傳回的存取數目上限。

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呼叫取得其他結果時，輸出中會傳回 NextToken 參數。然後，您可以在後續命令中傳遞至 NextToken 參數，以繼續列出其他存取權。

類型：字串

長度限制：長度下限為 1。長度上限為 6144。

必要：否

ServerId

系統指派的唯一識別碼，適用於已指派使用者給伺服器的伺服器。

類型：字串

長度限制條件：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，服務會傳回 HTTP 200 個回應。

服務會以 JSON 格式傳回下列資料。

[Accesses](#)

傳回您指定ServerId值的存取權及其屬性。

類型：[ListedAccess](#) 物件陣列

[NextToken](#)

當您可以從ListAccesses呼叫取得其他結果時，輸出中會傳回 NextToken 參數。然後，您可以在後續命令中傳遞至 NextToken 參數，以繼續列出其他存取權。

類型：字串

長度限制：長度下限為 1。長度上限為 6144。

ServerId

系統指派的唯一識別碼，適用於已指派使用者給伺服器的伺服器。

類型：字串

長度限制條件：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](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidNextTokenException

傳遞的NextToken參數無效。

HTTP 狀態碼：400

InvalidRequestException

當用戶端提交格式錯誤的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

HTTP 狀態碼：500

另請參閱

如需在其中一種語言特定 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

ListAgreements

傳回ServerId您提供的伺服器所識別的協議清單。如果您想要將結果限制為特定數字，請提供MaxResults 參數的值。如果您先前執行 命令並收到 的值NextToken，您可以提供該值，以繼續列出您離開的協議。

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](#)》。

請求接受下列JSON格式的資料。

[MaxResults](#)

要傳回的協議數目上限。

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呼叫取得其他結果時，輸出中會傳回 NextToken 參數。然後，您可以在後續命令中傳遞至 NextToken 參數，以繼續列出其他協議。

類型：字串

長度限制：長度下限為 1。長度上限為 6144。

必要：否

[ServerId](#)

您想要合約清單的伺服器識別碼。

類型：字串

長度限制條件：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，服務會傳回 HTTP 200 個回應。

服務會以 JSON 格式傳回下列資料。

[Agreements](#)

傳回陣列，其中每個項目都包含協議的詳細資訊。

類型：[ListedAgreement](#) 物件陣列

[NextToken](#)

傳回權杖，如果有的話，您可以使用該權杖ListAgreements再次呼叫並接收其他結果。

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](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidNextTokenException

傳遞的 NextToken 參數無效。

HTTP 狀態碼：400

InvalidRequestException

當用戶端提交格式不正確的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

HTTP 狀態碼：500

另請參閱

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 .NET](#)
- [AWS SDK 適用於 C++](#)

- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

ListCertificates

傳回已匯入的目前憑證清單 AWS Transfer Family。如果您想要將結果限制為特定數字，請提供 `MaxResults` 參數的值。如果您先前執行命令並收到 `NextToken` 參數的值，您可以提供該值，以繼續從上次停止的位置列出憑證。

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](#)》。

請求接受下列JSON格式的資料。

[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` 呼叫取得其他結果時，輸出中會傳回 `NextToken` 參數。然後，您可以在後續命令中傳遞至 `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，服務會傳回 HTTP 200 個回應。

服務會以 JSON 格式傳回下列資料。

[Certificates](#)

傳回ListCertificates呼叫中指定的憑證陣列。

類型：[ListedCertificate](#) 物件陣列

[NextToken](#)

傳回下一個權杖，您可以使用它來列出下一個憑證。

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](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidNextTokenException

傳遞的NextToken參數無效。

HTTP 狀態碼：400

InvalidRequestException

當用戶端提交格式錯誤的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

HTTP 狀態碼：500

另請參閱

如需在其中一種語言特定 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

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](#)》。

請求接受下列JSON格式的資料。

MaxResults

要傳回的連接器數量上限。

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` 呼叫取得其他結果時，輸出中會傳回 `NextToken` 參數。然後，您可以在後續命令中傳遞至 `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，服務會傳回 HTTP 200 個回應。

服務會以 JSON 格式傳回下列資料。

[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](#)

傳回權杖，如果有的話，您可以使用該權杖 `ListConnectors` 再次呼叫並接收其他結果。

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](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidNextTokenException

傳遞的 `NextToken` 參數無效。

HTTP 狀態碼：400

InvalidRequestException

當用戶端提交格式不正確的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

HTTP 狀態碼：500

另請參閱

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

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，ListExecutions會傳回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](#)》。

請求接受下列JSON格式的資料。

[MaxResults](#)

指定要傳回的執行數目上限。

類型：整數

有效範圍：最小值為 1。最大值為 1000。

必要：否

[NextToken](#)

ListExecutions 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，以繼續列出其他執行。

例如，這對於分頁非常有用。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 API 來呼叫 max-results：

```
aws transfer list-executions --max-results 10
```

這會將前 10 個執行的詳細資訊，以及指標（NextToken）傳回第十一個執行。您現在可以API再次呼叫，並提供您收到NextToken的值：

```
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 11 號到 20 號。然後，您可以重複呼叫，直到所有 100 個執行的詳細資訊都傳回為止。

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

長度限制條件：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，服務會傳回 HTTP 200 個回應。

服務會以 JSON 格式傳回下列資料。

[Executions](#)

傳回ListedExecution陣列中每個執行的詳細資訊。

類型：[ListedExecution](#) 物件陣列

[NextToken](#)

ListExecutions 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，以繼續列出其他執行。

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

長度限制條件：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](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidNextTokenException

傳遞的NextToken參數無效。

HTTP 狀態碼：400

InvalidRequestException

當用戶端提交格式錯誤的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

HTTP 狀態碼：500

另請參閱

如需在其中一種語言特定 API中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)

- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

ListHostKeys

傳回 ServerId 參數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](#)》。

請求接受下列JSON格式的資料。

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

有未傳回的其他結果時，會傳回NextToken參數。您可以使用該值進行後續呼叫，ListHostKeys以繼續列出結果。

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的伺服器識別碼。

類型：字串

長度限制條件：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，服務會傳回 HTTP 200 個回應。

服務會以 JSON 格式傳回下列資料。

[HostKeys](#)

傳回陣列，其中每個項目都包含主機金鑰的詳細資訊。

類型：[ListedHostKey](#) 物件陣列

[NextToken](#)

傳回權杖，如果有的話，您可以使用該權杖ListHostKeys再次呼叫並接收其他結果。

類型：字串

長度限制：長度下限為 1。長度上限為 6144。

ServerId

傳回包含所列主機金鑰的伺服器識別碼。

類型：字串

長度限制條件：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](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidNextTokenException

傳遞的 NextToken 參數無效。

HTTP 狀態碼：400

InvalidRequestException

當用戶端提交格式不正確的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

HTTP 狀態碼：500

另請參閱

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

ListProfiles

傳回系統設定檔的清單。如果您想要將結果限制為特定數字，請提供 `MaxResults` 參數的值。如果您先前執行 命令並收到 的值 `NextToken`，您可以提供該值，以繼續列出您離開位置的設定檔。

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](#)》。

請求接受下列JSON格式的資料。

[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](#)

有未傳回的其他結果時，會傳回 `NextToken` 參數。您可以使用該值進行後續呼叫，`ListProfiles` 以繼續列出結果。

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，服務會傳回 HTTP 200 個回應。

服務會以 JSON 格式傳回下列資料。

[NextToken](#)

傳回權杖，如果有的話，您可以使用該權杖ListProfiles再次呼叫並接收其他結果。

類型：字串

長度限制：長度下限為 1。長度上限為 6144。

[Profiles](#)

傳回陣列，其中每個項目都包含設定檔的詳細資訊。

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 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidNextTokenException

傳遞的NextToken參數無效。

HTTP 狀態碼：400

InvalidRequestException

當用戶端提交格式錯誤的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

HTTP 狀態碼：500

另請參閱

如需在其中一種語言特定 API中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)

- [AWS SDK 適用於 Ruby V3](#)

ListSecurityPolicies

列出連接至檔案傳輸協定啟用伺服器的安全政策。

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](#)》。

請求接受下列JSON格式的資料。

[MaxResults](#)

指定要傳回作為ListSecurityPolicies查詢回應的安全政策數目。

類型：整數

有效範圍：最小值為 1。最大值為 1000。

必要：否

[NextToken](#)

從ListSecurityPolicies命令取得其他結果時，輸出中會傳回 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政策。

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，服務會傳回 200 HTTP 個回應。

服務會以 JSON 格式傳回下列資料。

NextToken

當您可以從ListSecurityPolicies操作取得其他結果時，輸出中會傳回 NextToken 參數。在下列命令中，您可以傳入 NextToken 參數以繼續列出安全政策。

類型：字串

長度限制：長度下限為 1。長度上限為 6144。

SecurityPolicyNames

列出的安全政策陣列。

類型：字串陣列

長度限制：長度下限為 0。長度上限為 100。

模式：TransferSecurityPolicy-.+

錯誤

如需所有動作常見錯誤的資訊，請參閱[常見錯誤](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidNextTokenException

傳遞的 NextToken 參數無效。

HTTP 狀態碼：400

InvalidRequestException

當用戶端提交格式不正確的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

HTTP 狀態碼：500

範例

範例

下列範例列出所有可用安全政策的名稱。

請求範例

```
aws transfer list-security-policies
```

回應範例

```
{
  "SecurityPolicyNames": [
    "TransferSecurityPolicy-2022-03",
    "TransferSecurityPolicy-FIPS-2020-06",
    "TransferSecurityPolicy-2018-11",
    "TransferSecurityPolicy-2023-05",
    "TransferSecurityPolicy-FIPS-2023-05",
    "TransferSecurityPolicy-2020-06"
  ]
}
```

另請參閱

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 .NET](#)

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

ListServers

列出與您 AWS 帳戶相關聯的已啟用檔案傳輸通訊協定的伺服器。

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](#)》。

請求接受下列JSON格式的資料。

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命令取得其他結果時，輸出中會傳回 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，服務會傳回 HTTP 200 個回應。

服務會以 JSON 格式傳回下列資料。

[NextToken](#)

當您可以從ListServers操作取得其他結果時，輸出中會傳回 NextToken 參數。在下列命令中，您可以傳遞 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。

[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 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidNextTokenException

傳遞的NextToken參數無效。

HTTP 狀態碼：400

InvalidRequestException

當用戶端提交格式錯誤的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

HTTP 狀態碼：500

範例

範例

下列範例列出存在於 中的伺服器 AWS 帳戶。

請注意，範例NextToken值不是真實值：它們旨在指示如何使用 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

如需在其中一種語言特定 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 .NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

ListTagsForResource

列出與您指定的 Amazon Resource Name (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](#)》。

請求接受下列JSON格式的資料。

Arn

請求與特定 Amazon Resource Name () 相關聯的標籤ARN。ARN 是特定 AWS 資源的識別符，例如伺服器、使用者或角色。

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請求回應的標籤數目。

類型：整數

有效範圍：最小值為 1。最大值為 1000。

必要：否

NextToken

當您請求ListTagsForResource操作的其他結果時，輸入中會傳回NextToken參數。然後，您可以在後續命令中傳遞至 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，服務會傳回 HTTP 200 個回應。

服務會以 JSON 格式傳回下列資料。

Arn

ARN 您指定列出 標籤的。

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呼叫取得其他結果時，輸出中會傳回 NextToken 參數。然後，您可以在後續命令中傳遞至 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

指派給資源的鍵值對，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](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidNextTokenException

傳遞的NextToken參數無效。

HTTP 狀態碼：400

InvalidRequestException

當用戶端提交格式錯誤的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

HTTP 狀態碼：500

範例

範例

下列範例列出具有ARN您指定之 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 的一個用量 ListTagsForResource。

回應範例

```
{
  "Tags": [
    {
      "Key": "Name",
      "Value": "MyServer"
    }
  ]
}
```

另請參閱

如需在其中一種語言特定 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 .NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

ListUsers

列出您透過傳遞 `ServerId` 參數所指定的檔案傳輸通訊協定啟用伺服器的使用者。

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](#)》。

請求接受下列JSON格式的資料。

[MaxResults](#)

指定要傳回作為ListUsers請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，輸出中會傳回 `NextToken` 參數。然後，您可以將 傳遞NextToken至後續ListUsers命令，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](#)

系統指派的唯一識別碼，適用於已指派使用者給伺服器的伺服器。

類型：字串

長度限制條件：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，服務會傳回 HTTP 200 個回應。

服務會以 JSON 格式傳回下列資料。

NextToken

當您可以從ListUsers呼叫取得其他結果時，輸出中會傳回 NextToken 參數。然後，您可以在後續命令中傳遞至 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

指派給使用者之伺服器的系統指派唯一識別碼。

類型：字串

長度限制條件：固定長度為 19。

模式：s-([0-9a-f]{17})

Users

傳回指定ServerId值的 Transfer Family 使用者及其屬性。

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](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidNextTokenException

傳遞的 NextToken 參數無效。

HTTP 狀態碼：400

InvalidRequestException

當用戶端提交格式不正確的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

HTTP 狀態碼：500

範例

範例

ListUsers API 呼叫會傳回與您指定的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

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

ListWorkflows

列出與目前 區域 AWS 帳戶 之 相關聯的所有工作流程。

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](#)》。

請求接受下列JSON格式的資料。

[MaxResults](#)

指定要傳回的工作流程數目上限。

類型：整數

有效範圍：最小值為 1。最大值為 1000。

必要：否

[NextToken](#)

ListWorkflows 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，服務會傳回 HTTP 200 個回應。

服務會以 JSON 格式傳回下列資料。

[NextToken](#)

ListWorkflows 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](#)

傳回Description每個工作流程的 WorkflowId、Arn和。

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](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidNextTokenException

傳遞的 NextToken 參數無效。

HTTP 狀態碼：400

InvalidRequestException

當用戶端提交格式不正確的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

HTTP 狀態碼：500

另請參閱

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

SendWorkflowStepState

傳送非同步自訂步驟的回呼。

在工作流程的自訂步驟執行期間 `ExecutionId`、`WorkflowId`、和 `Token` 會傳遞至目標資源。您必須將那些包含其回呼，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》](#)。

請求接受下列JSON格式的資料。

ExecutionId

用於執行工作流程的唯一識別碼。

類型：字串

長度限制條件：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

指示指定的步驟是否成功或失敗。

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

長度限制條件：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，服務會傳回 200 HTTP 回應，其中內 HTTP 文為空白。

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

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式不正確的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

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

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

StartFileTransfer

開始在本機 AWS 儲存體和遠端AS2或SFTP伺服器之間進行檔案傳輸。

- 對於AS2連接器，您可以指定 ConnectorId和一或多個 SendFilePaths，以識別您要傳輸的檔案。
- 對於SFTP連接器，檔案傳輸可以是傳出或傳入。在這兩種情況下，您都會指定 ConnectorId。根據傳輸方向，您也可以指定下列項目：
 - 如果您要將檔案從合作夥伴的SFTP伺服器傳輸到 Amazon Web Services 儲存體，您可以指定一或多個 RetrieveFilePaths 來識別要傳輸的檔案，以及指定目的地資料夾LocalDirectoryPath的。
 - 如果您要從 AWS 儲存體將檔案傳輸到合作夥伴的SFTP伺服器，您可以指定一或多個 SendFilePaths 來識別要傳輸的檔案，以及指定目的地資料夾RemoteDirectoryPath的。

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](#)》。

請求接受下列JSON格式的資料。

ConnectorId

連接器的唯一識別符。

類型：字串

長度限制條件：固定長度為 19。

模式：c-([0-9a-f]{17})

必要：是

LocalDirectoryPath

對於傳入傳輸，會為一或多個從合作夥伴的SFTP伺服器傳輸的檔案LocalDirectoryPath指定目的地。

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

對於傳出傳輸，會RemoteDirectoryPath指定一或多個檔案的目的地，這些檔案會傳輸至合作夥伴的SFTP伺服器。如果您未指定 RemoteDirectoryPath，傳輸檔案的目的地會是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。每個字串代表一個傳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 儲存體的一或多個來源路徑。每個字串代表一次傳出檔案傳輸的來源檔案路徑。例如：
`DOC-EXAMPLE-BUCKET/myfile.txt`。

 Note

`DOC-EXAMPLE-BUCKET` 以其中一個實際儲存貯體取代。

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，服務會傳回 HTTP 200 個回應。

服務會以 JSON 格式傳回下列資料。

TransferId

傳回檔案傳輸的唯一識別符。

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](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式錯誤的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

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

下列範例會開始將AS2檔案從 Transfer Family 伺服器傳輸至遠端交易合作夥伴的端點。 *DOC-EXAMPLE-BUCKET* 以其中一個實際儲存貯體取代。

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

下列範例會開始將檔案從本機 AWS 儲存傳輸到遠端SFTP伺服器。

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/fromTransferFamilyServer"
}
```

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/toTransferFamily/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

如需在其中一種語言特定 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

StartServer

將啟用檔案傳輸通訊協定之伺服器的狀態從 OFFLINE 變更為 ONLINE。它不會影響已經是 的伺服器 ONLINE。ONLINE 伺服器可以接受和處理檔案傳輸任務。

狀態 STARTING 表示伺服器處於中繼狀態，可能是無法完全回應，或無法完全上線。的值 START_FAILED 可以指示錯誤條件。

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》](#)。

請求接受下列 JSON 格式的資料。

ServerId

您啟動之伺服器的系統指定唯一識別碼。

類型：字串

長度限制條件：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，服務會傳回 200 HTTP 回應，其中內 HTTP 文為空白。

錯誤

如需所有動作常見錯誤的資訊，請參閱 [常見錯誤](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式不正確的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

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

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

StopServer

將啟用檔案傳輸通訊協定之伺服器的狀態從 ONLINE 變更為 OFFLINE。OFFLINE 伺服器無法接受和處理檔案傳輸任務。與伺服器綁定的資訊，例如伺服器和使用者的屬性，不受停止伺服器的影響。

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。

狀態 STOPPING 表示伺服器處於中繼狀態，可能是無法完全回應，或並非完全離線。的值 STOP_FAILED 可以指示錯誤條件。

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](#)》。

請求接受下列 JSON 格式的資料。

ServerId

您停止之伺服器的系統指派唯一識別碼。

類型：字串

長度限制條件：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，服務會傳回 200 HTTP 回應，其中內HTTP文為空白。

錯誤

如需所有動作常見錯誤的資訊，請參閱[常見錯誤](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式錯誤的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

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

如需在其中一種語言特定 API中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

TagResource

將鍵值對連接至資源，如其 Amazon Resource Name (ARN) 所識別。資源是使用者、伺服器、角色和其他實體。

此通話未傳回任何回應。

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](#)》。

請求接受下列JSON格式的資料。

Arn

特定 AWS 資源的 Amazon Resource Name (ARN)，例如伺服器、使用者或角色。

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 ARNs 的鍵值對，可用來依類型分組和搜尋資源。您可以將此中繼資料連接到資源（伺服器、使用者、工作流程等）以用於任何用途。

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，服務會傳回 200 HTTP 回應，其中內HTTP文為空白。

錯誤

如需所有動作常見錯誤的資訊，請參閱[常見錯誤](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式錯誤的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

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 的一個用量 TagResource。

回應範例

HTTP 200 response with an empty HTTP body.

另請參閱

如需在其中一種語言特定 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

TestConnection

測試您的SFTP連接器是否已成功設定。強烈建議您呼叫此操作，以測試您在本機 AWS 儲存體和交易合作夥伴的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](#)》。

請求接受下列JSON格式的資料。

ConnectorId

連接器的唯一識別符。

類型：字串

長度限制條件：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，服務會傳回 HTTP 200 個回應。

服務會以 JSON 格式傳回下列資料。

ConnectorId

傳回您正在測試之連接器物件的識別碼。

類型：字串

長度限制條件：固定長度為 19。

模式：c-([0-9a-f]{17})

Status

ERROR 如果測試失敗，會傳回 OK 以取得成功測試。

類型：字串

StatusMessage

Connection succeeded 如果測試成功，則傳回。或者，如果測試失敗，會傳回描述性錯誤訊息。下列清單提供疑難排解詳細資訊，具體取決於您收到的錯誤訊息。

- 確認您的秘密名稱與 Transfer Role 許可中的秘密名稱相符。
- 在連接器組態 URL 中驗證伺服器，並確認登入憑證在連接器之外成功運作。
- 確認秘密存在且格式正確。
- 確認連接器組態中的受信任主機金鑰符合 ssh-keyscan 輸出。

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](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式不正確的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

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

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 .NET](#)
- [AWS SDK 適用於 C++](#)

- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

TestIdentityProvider

如果已啟用檔案傳輸通訊協定IdentityProviderType之伺服器的 是 AWS_DIRECTORY_SERVICE或 API_Gateway， 會測試您的身分提供者是否已成功設定。強烈建議您在建立伺服器時立即呼叫此操作，以測試您的身分驗證方法。如此一來，您就可以對身分提供者整合的問題進行疑難排解，以確保使用者能夠成功使用 服務。

ServerId 和 UserName 是必要參數。ServerProtocol、 SourceIp和 UserPassword 皆為選用。

注意下列事項：

- TestIdentityProvider 如果伺服器的 為 `API_GATEWAY`，IdentityProviderType則無法使用 `SERVICE_MANAGED`。
- TestIdentityProvider 不適用於 金鑰：它只接受密碼。
- TestIdentityProvider 可以測試處理金鑰和密碼的自訂身分提供者的密碼操作。
- 如果您為任何參數提供任何不正確的值，則Response欄位為空白。
- 如果您為使用服務受管使用者的伺服器提供伺服器 ID，您會收到錯誤：

```
An error occurred (InvalidRequestException) when calling the
TestIdentityProvider operation: s-server-ID not configured for external
auth
```

- 如果您為無法識別實際傳輸伺服器的--server-id參數輸入伺服器 ID，則會收到下列錯誤：

```
An error occurred (ResourceNotFoundException) when calling the
TestIdentityProvider operation: Unknown server.
```

您的伺服器可能位於不同的區域。您可以新增下列項目來指定區域：`--region region-code`，例如`--region us-east-2`在美國東部（ 俄亥俄 ）指定伺服器。

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](#)》。

請求接受下列JSON格式的資料。

[ServerId](#)

特定伺服器的系統指派識別符。該伺服器的使用者身分驗證方法會使用使用者名稱和密碼進行測試。

類型：字串

長度限制條件：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）
- 檔案傳輸通訊協定安全（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](#)

要測試之帳戶的來源 IP 地址。

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，服務會傳回 200 HTTP 個回應。

服務會以 JSON 格式傳回下列資料。

Message

指出測試是否成功的訊息。

Note

如果傳回空字串，最可能的原因是身分驗證因使用者名稱或密碼不正確而失敗。

類型：字串

Response

從 API Gateway 或 Lambda 函數傳回的回應。

類型：字串

StatusCode

來自 API Gateway 或 Lambda 函數的回應HTTP狀態碼。

類型：整數

Url

用於驗證使用者的 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](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式不正確的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

HTTP 狀態碼：500

範例

範例

下列請求會傳回來自身分提供者的訊息，指出使用者名稱和密碼組合是可搭配 使用的有效身分 AWS Transfer Family。

請求範例

```
{
  "ServerID": "s-01234567890abcdef",
  "UserName": "my_user",
  "UserPassword": "MyPassword-1"
}
```

範例

下列回應顯示成功測試的範例回應。

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多個具有存取權的群組。

```
"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提供者，您可以輸入下列命令來測試您的使用者：

```
aws transfer test-identity-provider --server-id s-0123456789abcdefg --user-  
name myuser
```

其中 s-0123456789abcdefg 是您的傳輸伺服器，而 myuser 是自訂使用者的使用者名稱。

如果命令成功，您的回應類似於以下內容：

- AWS 帳戶 ID 為 012345678901
- 使用者角色是 user-role-api-gateway
- 主目錄是 myuser-bucket
- 公有金鑰是公有金鑰
- 叫用URL是叫用-URL

```
{  
  "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

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

UntagResource

從資源分離鍵值對，如其 Amazon Resource Name (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](#)》。

請求接受下列JSON格式的資料。

Arn

將移除標籤的資源值。Amazon Resource Name (ARN) 是特定 AWS 資源的識別符，例如伺服器、使用者或角色。

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 的鍵值對ARNs，可用於依類型分組和搜尋資源。此中繼資料可以基於任何目的連接到資源。

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，服務會傳回 200 HTTP 回應，其中內HTTP文為空白。

錯誤

如需所有動作常見錯誤的資訊，請參閱[常見錯誤](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式不正確的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

HTTP 狀態碼：500

範例

範例

下列範例會移除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 的一個用量 UntagResource。

回應範例

HTTP 200 response with an empty HTTP body.

另請參閱

如需在其中一種語言特定的 API中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

UpdateAccess

可讓您更新 ServerID 和 參數中指定的存取 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](#)》。

請求接受下列JSON格式的資料。

ExternalId

識別目錄中特定群組所需的唯一識別碼。您關聯的群組使用者可透過使用的已啟用通訊協定存取您的 Amazon S3 或 Amazon EFS 資源 AWS Transfer Family。如果您知道群組名稱，則可以使用 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以 Active Directory 群組的名稱取代。

用來驗證此參數的規則運算式是由大寫和小寫英數字元組成的字串，不含空格。您也可以包含底線或任何下列字元：=, .@ : /-

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](#)

邏輯目錄映射，可指定使用者應看到哪些 Amazon S3 或 Amazon EFS 路徑和金鑰，以及您希望如何使其可見。您必須指定 Entry 和 Target 對，其中 Entry 顯示如何顯示路徑，並且 Target 是實際的 Amazon S3 或 Amazon EFS 路徑。如果您只指定目標，則會顯示為原樣。您也必須確保 AWS Identity and Access Management (IAM) 角色提供對中路徑的存取權 Target。只有在設定為時，才能 HomeDirectoryType 設定此值 LOGICAL。

以下是 Entry 和 Target 對範例。

```
[ { "Entry": "/directory1", "Target": "/bucket_name/home/mydirectory" } ]
```

在大多數情況下，您可以使用此值來取代工作階段政策，將使用者鎖定到指定的主目錄 ("chroot")。若要這麼做，您可以將 Entry 設定為 /，並將 Target 設定為 HomeDirectory 參數值。

以下是的 Entry 和 Target 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。最多 50000 個項目。

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。如果您將其設定為 PATH，則使用者會看到絕對 Amazon S3 儲存貯體或 Amazon EFS 路徑，就像在其檔案傳輸通訊協定用戶端一樣。如果您將其設定為 LOGICAL，則需要在 中提供映射，HomeDirectoryMappings 以了解如何讓使用者看見 Amazon S3 或 Amazon EFS 路徑。

Note

如果 HomeDirectoryType 是 LOGICAL，您必須使用 HomeDirectoryMappings 參數提供映射。另一方面，如果 HomeDirectoryType 是 PATH，則您使用 HomeDirectory 參數提供絕對路徑。您無法在範本 HomeDirectoryMappings 中同時擁有 HomeDirectory 和 。

類型：字串

有效值:PATH | LOGICAL

必要：否

[Policy](#)

適用於使用者的工作階段政策，讓您可以在多個使用者之間使用相同的 AWS Identity and Access Management (IAM) 角色。此政策會減少使用者對其 Amazon S3 儲存貯體部分存取權的範圍。您可以在此政策內使用的變數包括 \${Transfer:UserName}、\${Transfer:HomeDirectory} 和 \${Transfer:HomeBucket}。

 Note

此政策僅適用於的網域ServerId為 Amazon S3 時。Amazon EFS 不會使用工作階段政策。

對於工作階段政策，會將政策 AWS Transfer Family 儲存為 JSON Blob，而不是政策的 Amazon Resource Name (ARN)。您可以將政策儲存為 JSON Blob，並將其傳遞至Policy引數中。

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 安全權杖服務參考 [AssumeRole](#) 中的。AWS API

類型：字串

長度限制：長度下限為 0。長度上限為 2048。

必要：否

[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 IDs (SecondaryGids)，可控制使用者對 Amazon EFS 檔案系統的存取。在檔案系統中的檔案和目錄上設定的POSIX許可決定了使用者在將檔案移入和移出 Amazon EFS 檔案系統時獲得的存取層級。

類型：[PosixProfile](#) 物件

必要：否

[Role](#)

(ARN) 角色的 Amazon Resource Name AWS Identity and Access Management (IAM)，可控制使用者對 Amazon S3 儲存貯體或 Amazon EFS 檔案系統的存取。附加至此角色的政策會決定在將檔案移入和移出 Amazon S3 儲存貯體或 Amazon EFS 檔案系統時，您要為使用者提供的存取層級。此IAM角色也應包含信任關係，允許伺服器在服務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

長度限制條件：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，服務會傳回 200 HTTP 個回應。

服務會以 JSON 格式傳回下列資料。

ExternalId

群組的外部識別碼，其使用者可透過使用 AWS Transfer Family 啟用的通訊協定存取您的 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

使用者所連接之伺服器的識別碼。

類型：字串

長度限制條件：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](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式不正確的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceExistsException

請求的資源不存在，或存在於命令指定的區域以外的區域。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

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

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

UpdateAgreement

更新現有協議的一些參數。ServerId 為您要更新的協議提供 AgreementId 和 `ServerId`，以及要更新的參數的新值。

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](#)》。

請求接受下列JSON格式的資料。

[AccessRole](#)

連接器用於使用 AS2 或 SFTP 通訊協定傳送檔案。針對存取角色，提供要使用 AWS Identity and Access Management 的角色的 Amazon Resource Name (ARN)。

對於AS2連接器

使用 AS2 時，您可以呼叫 `StartFileTransfer` 並指定請求參數中的檔案路徑來傳送檔案 `SendFilePaths`。我們使用檔案的父目錄（例如 `--send-file-paths /bucket/dir/file.txt`，對於 `StartFileTransfer`，父目錄為 `/bucket/dir/`）來暫時存放已處理 AS2 的訊息檔案、MDN 在我們從合作夥伴收到時存放，以及撰寫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。

如果您為 AS2 連接器使用基本身分驗證，存取角色需要秘密的 `secretsmanager:GetSecretValue` 許可。如果秘密是使用客戶受管金鑰而非 `Secrets Manager` 中的 AWS 受管金鑰加密，則角色也需要該金鑰的 `kms:Decrypt` 許可。

對於SFTP連接器

請確定存取角色提供對StartFileTransfer請求中所用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 `secretsmanager:GetSecretValue` 許可 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

協議的唯一識別符。當您建立協議時，會傳回此識別碼。

類型：字串

長度限制條件：固定長度為 19。

模式：`a-([0-9a-f]{17})`

必要：是

BaseDirectory

若要變更所傳輸檔案的登陸目錄（資料夾），請提供您要使用的儲存貯體資料夾；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，請為協議提供簡短描述。

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符。

若要變更本機設定檔識別符，請在此處提供新值。

類型：字串

長度限制條件：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符。若要變更合作夥伴設定檔識別符，請在此處提供新值。

類型：字串

長度限制條件：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。這是協議使用的特定伺服器。

類型：字串

長度限制條件：固定長度為 19。

模式：`s-([0-9a-f]){17}`

必要：是

Status

您可以更新協議的狀態，可啟用非作用中協議或反向協議。

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，服務會傳回 HTTP 200 個回應。

服務會以 JSON 格式傳回下列資料。

[AgreementId](#)

協議的唯一識別符。當您建立協議時，會傳回此識別碼。

類型：字串

長度限制條件：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](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式錯誤的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceExistsException

請求的資源不存在，或存在於命令指定的區域以外的區域。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

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

如需在其中一種語言特定 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

UpdateCertificate

更新憑證的作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](#)》。

請求接受下列JSON格式的資料。

ActiveDate

選擇性日期，指定憑證變為作用的時間。

類型：Timestamp

必要：否

CertificateId

您正在更新的憑證物件的識別碼。

類型：字串

長度限制條件：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

回應語法

```
{  
  "CertificateId": "string"  
}
```

回應元素

如果動作成功，服務會傳回 HTTP 200 個回應。

服務會以 JSON 格式傳回下列資料。

CertificateId

傳回您正在更新之憑證物件的識別碼。

類型：字串

長度限制條件：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](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式不正確的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

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作用中日期，將作用中日期設定為 2022 年 1 月 16 日 16 : 12 : 07 UTC -5 小時。

請求範例

```
aws transfer update-certificate --certificate-id c-abcdefgh123456hijk --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-abcdefgh123456hijk"
```

另請參閱

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

UpdateConnector

更新現有連接器的某些參數。提供您要更新的ConnectorId連接器的 ，以及要更新參數的新值。

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",
  "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](#)》。

請求接受下列JSON格式的資料。

[AccessRole](#)

連接器用於使用 AS2或 SFTP通訊協定傳送檔案。針對存取角色，提供要使用 AWS Identity and Access Management 的角色的 Amazon Resource Name (ARN)。

對於AS2連接器

使用 AS2時，您可以呼叫StartFileTransfer並指定請求參數 中的檔案路徑來傳送檔案SendFilePaths。我們使用檔案的父目錄（例如--send-file-paths /bucket/dir/

file.txt，對於，父目錄為 /bucket/dir/) 來暫時存放已處理AS2的訊息檔案、MDN在我們從合作夥伴收到時存放，以及撰寫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。

如果您為AS2連接器使用基本身分驗證，存取角色需要秘密的secretsmanager:GetSecretValue許可。如果秘密是使用客戶受管金鑰而非 Secrets Manager 中的 AWS 受管金鑰加密，則角色也需要該金鑰的kms:Decrypt許可。

對於SFTP連接器

請確定存取角色提供對StartFileTransfer請求中所用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 secretsmanager:GetSecretValue許可 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](#)

連接器的唯一識別符。

類型：字串

長度限制條件：固定長度為 19。

模式：c-([0-9a-f]{17})

必要：是

[LoggingRole](#)

(ARN) 角色的 Amazon Resource Name AWS Identity and Access Management (IAM) , 允許連接器開啟 Amazon S3 事件 CloudWatch 的記錄。設定時, 您可以在 CloudWatch 日誌中檢視連接器活動。

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

[SftpConfig](#)

包含SFTP連接器物件參數的結構。

類型: [SftpConnectorConfig](#) 物件

必要: 否

[Url](#)

URL 合作夥伴AS2或SFTP端點的。

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, 服務會傳回 HTTP 200 個回應。

服務會以 JSON 格式傳回下列資料。

ConnectorId

傳回您要更新之連接器物件的識別碼。

類型：字串

長度限制條件：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](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式錯誤的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceExistsException

請求的資源不存在，或存在於命令指定的區域以外的區域。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

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

如需在其中一種語言特定 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

UpdateHostKey

更新 ServerId 和 HostKeyId 參數所指定的主機金鑰描述。

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](#)》。

請求接受下列JSON格式的資料。

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

您更新之主機金鑰的識別碼。

類型：字串

長度限制條件：固定長度為 25。

模式：hostkey-[0-9a-f]{17}

必要：是

[ServerId](#)

包含您要更新之主機金鑰的伺服器識別碼。

類型：字串

長度限制條件：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，服務會傳回 200 HTTP 個回應。

服務會以 JSON 格式傳回下列資料。

[HostKeyId](#)

傳回已更新主機金鑰的主機金鑰識別符。

類型：字串

長度限制條件：固定長度為 25。

模式：hostkey-[0-9a-f]{17}

[ServerId](#)

傳回包含已更新主機金鑰之伺服器的伺服器識別符。

類型：字串

長度限制條件：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](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式不正確的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

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

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 .NET](#)
- [AWS SDK 適用於 C++](#)

- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

UpdateProfile

更新現有設定檔的一些參數。提供您要更新的ProfileId設定檔的，以及要更新參數的新值。

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](#)》。

請求接受下列JSON格式的資料。

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

長度限制條件：固定長度為 22。

模式：cert-([0-9a-f]{17})

必要：否

ProfileId

您正在更新的設定檔物件的識別碼。

類型：字串

長度限制條件：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，服務會傳回 HTTP 200 個回應。

服務會以 JSON 格式傳回下列資料。

ProfileId

傳回要更新之設定檔的識別碼。

類型：字串

長度限制條件：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](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式不正確的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

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

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

UpdateServer

建立伺服器後，更新已啟用檔案傳輸通訊協定的伺服器屬性。

UpdateServer 呼叫會傳回您更新ServerId之伺服器的。

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](#)》。

請求接受下列JSON格式的資料。

Certificate

AWS Certificate Manager (ARN) 憑證的 Amazon Resource Name (ACM)。當 Protocols 設定為 FTPS 時，此為必要項目。

若要請求新的公有憑證，請參閱 AWS Certificate Manager 使用者指南中的[請求公有憑證](#)。

若要將現有憑證匯入 ACM，請參閱 Certificate Manager 使用者指南中的[將憑證匯入 ACM](#)。AWS

若要FTPS透過私有 IP 地址請求私有憑證，請參閱 AWS Certificate Manager 使用者指南中的[請求私有憑證](#)。

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

憑證必須是指定 FQDN 或 IP 地址的有效 SSL/TLS X.509 第 3 版憑證，以及發行者的相關資訊。

類型：字串

長度限制：長度下限為 0。長度上限為 1600。

必要：否

[EndpointDetails](#)

為您的伺服器設定的虛擬私有雲端（VPC）端點設定。當您在 中託管端點時 VPC，您只能讓 中的資源存取端點 VPC，也可以連接彈性 IP 地址，讓用戶端透過網際網路存取端點。您 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。您可以選擇讓伺服器的端點公開存取（PUBLIC），或在 中託管它 VPC。使用託管在 中的端點 VPC，您只能限制對伺服器和資源的存取，VPC 或選擇直接將彈性 IP 地址連接到網際網路，使其面向網際網路。

Note

2021 年 5 月 19 日後，如果您的帳戶在 2021 年 5 月 19 日之前尚未建立伺服器，您將無法 `EndpointType=VPC_ENDPOINT` 在 AWS 帳戶中使用 建立伺服器。如果您已 `EndpointType=VPC_ENDPOINT` 在 2021 年 5 月 19 日或之前在 AWS 帳戶中使用 建立伺服器，則不會受到影響。在此日期之後，請使用 `EndpointType=VPC`。如需詳細資訊，請參閱 [停止使用 VPC_ENDPOINT](#)。建議使用 VPC 作為 `EndpointType`。透過此端點類型，您可以選擇直接將最多三個彈性 IPv4 地址（BYO 包含 IP）與伺服器的端點建立關聯，並使用 VPC 安全群組來限制用戶端公有 IP 地址的流量。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](#)

用於SFTP已啟用 RSA之伺服器的 ECDSA、或 ED25519 私有金鑰。您可以新增多個主機金鑰，以防您想要輪換金鑰，或擁有一組使用不同演算法的作用中金鑰。

使用下列命令來產生不含密碼片語的 RSA 2048 位元金鑰：

```
ssh-keygen -t rsa -b 2048 -N "" -m PEM -f my-new-server-key.
```

針對 -b選項使用最小值 2048。您可以使用 3072 或 4096 建立更強大的金鑰。

使用下列命令來產生沒有密碼的 ECDSA 256 位元金鑰：

```
ssh-keygen -t ecdsa -b 256 -N "" -m PEM -f my-new-server-key.
```

-b 的選項的有效值ECDSA為 256、384 和 521。

使用下列命令來產生沒有複雜密碼的ED25519金鑰：

```
ssh-keygen -t ed25519 -N "" -f my-new-server-key.
```

對於所有這些命令，您可以使用您選擇的字串my-new-server-key取代。

Important

如果您不打算將現有使用者從已啟用 SFTP的現有伺服器遷移至新的伺服器，請勿更新主機金鑰。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 使用者指南 中的[更新SFTP已啟用 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](#)

包含呼叫客戶身分驗證API方法所需的所有資訊的陣列。

類型：[IdentityProviderDetails](#) 物件

必要：否

[LoggingRole](#)

(ARN) 角色的 Amazon Resource Name AWS Identity and Access Management (IAM)，允許伺服器開啟 Amazon S3 或 Amazon 的 Amazon CloudWatch 記錄Events。設定時，您可以在 CloudWatch 日誌中檢視使用者活動。

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。

- 若要指示被動模式（適用於 FTP 和 FTPS 通訊協定），請使用 `PassiveIp` 參數。輸入單一點四 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 `SETSTAT` 命令並上傳檔案，而不需要對 SFTP 用戶端進行任何變更，請將值設定為 `ENABLE_NO_OP`。如果您將 `SetStatOption` 參數設定為 `ENABLE_NO_OP`，Transfer Family 會產生 Amazon CloudWatch Logs 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 來恢復最近的交涉工作階段，請使用 `TlsSessionResumptionMode` 參數。
- `As2Transports` 表示 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（Secure Shell（SSH）檔案傳輸通訊協定）：檔案傳輸 SSH
- FTPS（檔案傳輸通訊協定安全）：使用 TLS 加密進行檔案傳輸
- FTP（檔案傳輸通訊協定）：未加密的檔案傳輸
- AS2（適用性陳述式 2）：用於傳輸結構化 business-to-business 資料

Note

- 如果您選擇 FTPS，您必須選擇儲存在 AWS Certificate Manager（ACM）中的憑證，當用戶端透過連線到伺服器時，該憑證可用來識別您的伺服器 FTPS。

- 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。

有效值:SFTP | FTP | FTPS | AS2

必要：否

[S3StorageOptions](#)

指定是否最佳化 Amazon S3 目錄的效能。此選項根據預設為停用。

根據預設，主目錄映射具有 TYPE 的 DIRECTORY。如果您啟用此選項，則 HomeDirectoryMapEntryType FILE 如果您想要映射具有檔案目標，則需要將 明確設定為。

類型：[S3StorageOptions](#) 物件

必要：否

[SecurityPolicyName](#)

指定連接至伺服器的安全政策名稱。

類型：字串

長度限制：長度下限為 0。長度上限為 100。

模式：TransferSecurityPolicy-.*+

必要：否

ServerId

Transfer Family 使用者所指派之伺服器執行個體的系統指派唯一識別碼。

類型：字串

長度限制條件：固定長度為 19。

模式：s-([0-9a-f]{17})

必要：是

StructuredLogDestinations

指定伺服器日誌的傳送目的地日誌群組。

若要指定日誌群組，您必須ARN為現有日誌群組提供。在此情況下，日誌群組的格式如下：

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日誌群組，您可以清除該群組，並在update-server通話中提供此參數的空值，並實際上關閉結構化日誌。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)。當伺服器工作階段在檔案仍在上傳時中斷連線時，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，服務會傳回 HTTP 200 個回應。

服務會以 JSON 格式傳回下列資料。

[ServerId](#)

Transfer Family 使用者所指派之伺服器的系統指派唯一識別碼。

類型：字串

長度限制條件：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UpdateServer呼叫 作為VPC端點類型且伺服器 VpcEndpointID 未處於可用狀態的檔案傳輸通訊協定啟用伺服器時，就會擲回此例外狀況。

HTTP 狀態碼：400

InternalServiceError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式錯誤的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceExistsException

請求的資源不存在，或存在於命令指定的區域以外的區域。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

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中移除任何相關聯的工作流程。

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

如需在其中一種語言特定 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 .NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)

- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

UpdateUser

將新屬性指派給使用者。您傳遞的參數會修改下列任何或所有項目：和ServerId您指定的主目錄、角色UserName和政策。

回應會傳回UserName已更新使用者的 ServerId和。

在主控台中，您可以在建立或更新使用者時選取限制。這可確保使用者無法存取主目錄以外的任何內容。設定此行為的程式設計方法是更新使用者。將 HomeDirectoryType設定為 LOGICAL，並使用 HomeDirectoryMappings Entry指定為根（/）和 Target作為其主目錄。

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，以便其在主控台組態顯示選取的限制旗標。

```
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](#)》。

請求接受下列JSON格式的資料。

[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](#)

邏輯目錄映射，可指定使用者應看到哪些 Amazon S3 或 Amazon EFS 路徑和金鑰，以及您希望如何使其可見。您必須指定 Entry 和 Target 對，其中 Entry 顯示如何顯示路徑，並且 Target 是實際的 Amazon S3 或 Amazon EFS 路徑。如果您只指定目標，則會顯示為原樣。您也必須確保 AWS Identity and Access Management (IAM) 角色提供對中路徑的存取權 Target。只有在設定為時，才能 HomeDirectoryType 設定此值 LOGICAL。

以下是 Entry 和 Target 對範例。

```
[ { "Entry": "/directory1", "Target": "/bucket_name/home/mydirectory" } ]
```

在大多數情況下，您可以使用此值來取代工作階段政策，將使用者鎖定到指定的主目錄 ("chroot")。若要執行此操作，您可以將 Entry 設定為 '/' 並 Target 設定為 HomeDirectory 參數值。

以下是的 Entry 和 Target 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。最多 50000 個項目。

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。如果您將其設定為 PATH，則使用者會看到絕對 Amazon S3 儲存貯體或 Amazon EFS 路徑，就像在其檔案傳輸通訊協定用戶端一樣。如果您將其設定為 LOGICAL，則需要在 中提供映射，HomeDirectoryMappings 以了解如何讓使用者看見 Amazon S3 或 Amazon EFS 路徑。

Note

如果 HomeDirectoryType 是 LOGICAL，您必須使用 HomeDirectoryMappings 參數提供映射。另一方面，如果 HomeDirectoryType 是 PATH，則您使用 HomeDirectory 參數提供絕對路徑。您無法在範本 HomeDirectoryMappings 中同時擁有 HomeDirectory 和 。

類型：字串

有效值:PATH | LOGICAL

必要：否

[Policy](#)

適用於使用者的工作階段政策，讓您可以在多個使用者之間使用相同的 AWS Identity and Access Management (IAM) 角色。此政策會減少使用者對其 Amazon S3 儲存貯體部分存取權的範圍。您可以在此政策內使用的變數包括 \${Transfer:UserName}、\${Transfer:HomeDirectory} 和 \${Transfer:HomeBucket}。

Note

此政策僅適用於的網域 ServerId 為 Amazon S3 時。Amazon EFS 不會使用工作階段政策。

對於工作階段政策，會將政策 AWS Transfer Family 儲存為 JSON Blob，而不是政策的 Amazon Resource Name (ARN)。您可以將政策儲存為 BlobJSON，並將其傳遞到 Policy 引數中。

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 安全權杖服務參考 [AssumeRole](#) 中的 `AssumeRole`。AWS API

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 POSIX 身分，包括使用者 ID (Uid)、群組 ID IDs (Gid) 和任何次要群組 (SecondaryGids)，以控制使用者對 Amazon Elastic File Systems (Amazon EFS) 的存取。檔案系統中檔案和目錄上設定的 POSIX 許可決定了使用者在傳輸檔案進出 Amazon EFS 檔案系統時所取得的存取層級。

類型：[PosixProfile](#) 物件

必要：否

[Role](#)

(ARN) 角色的 Amazon Resource Name AWS Identity and Access Management (IAM)，可控制使用者對 Amazon S3 儲存貯體或 Amazon EFS 檔案系統的存取。附加至此角色的政策會決定在將檔案移入和移出 Amazon S3 儲存貯體或 Amazon EFS 檔案系統時，您要為使用者提供的存取層級。此 IAM 角色也應包含信任關係，允許伺服器在服務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](#)

系統指派的唯一識別碼，用於使用者指派至的 Transfer Family 伺服器執行個體。

類型：字串

長度限制條件：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，服務會傳回 HTTP 200 個回應。

服務會以 JSON 格式傳回下列資料。

ServerId

帳戶所指派之 Transfer Family 伺服器執行個體的系統指派唯一識別碼。

類型：字串

長度限制條件：固定長度為 19。

模式：s-([0-9a-f]{17})

UserName

指派給請求中指定之伺服器執行個體的使用者的唯一識別符。

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](#)。

InternalServerError

當 AWS Transfer Family 服務發生錯誤時，就會擲回此例外狀況。

HTTP 狀態碼：500

InvalidRequestException

當用戶端提交格式不正確的請求時，就會擲回此例外狀況。

HTTP 狀態碼：400

ResourceNotFoundException

當 AWS Transfer Family 服務找不到資源時，就會擲回此例外狀況。

HTTP 狀態碼：400

ServiceUnavailableException

請求失敗，因為 AWS Transfer Family 服務無法使用。

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

如需在其中一種語言特定的 API中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK 適用於 。NET](#)
- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)

- [AWS SDK 適用於 Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK 適用於 PHP V3](#)
- [AWS SDK 適用於 Python](#)
- [AWS SDK 適用於 Ruby V3](#)

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傳出程序，以將 AWS Transfer Family 客戶與交易合作夥伴連線。

目錄

BasicAuthSecretId

為 AS2 Connectors 提供基本身分驗證支援API。若要使用基本身分驗證，您必須在 中提供秘密的名稱或 Amazon Resource Name (ARN) AWS Secrets Manager。

此參數的預設值為 null，表示未針對連接器啟用基本身分驗證。

如果連接器應使用基本身分驗證，則秘密必須是下列格式：

```
{ "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憑證。

注意下列事項：

- 您正在 Secrets Manager 中儲存這些憑證，而不是直接將它們傳遞到此 API。
- 如果您使用 API、SDKs或 CloudFormation 來設定連接器，則必須先建立秘密，才能啟用基本身分驗證。不過，如果您使用 AWS 管理主控台，您可以讓系統為您建立秘密。

如果您先前已啟用連接器的基本身分驗證，您可以使用 UpdateConnectorAPI呼叫來停用連接器。例如，如果您使用 CLI，您可以執行下列命令來移除基本身分驗證：

```
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AS2檔案是否壓縮。

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該DES_EDE3_CBC演算法的舊版用戶端，否則請勿使用該演算法，因為它是較弱的加密演算法。
- 您只能指定 連接器URL的 NONE是否使用 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符。

類型：字串

長度限制條件：固定長度為 19。

模式：p-([0-9a-f]{17})

必要：否

MdnResponse

用於傳出請求（從 AWS Transfer Family 伺服器到合作夥伴AS2伺服器），以判斷傳輸的合作夥伴回應是同步還是非同步。指定下列任一值：

- SYNC：系統會預期同步MDN回應，確認檔案已成功傳輸（或未傳輸）。
- 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SigningAlgorithm使用 的值。

類型：字串

有效值:SHA256 | SHA384 | SHA512 | SHA1 | NONE | DEFAULT

必要：否

MessageSubject

在與連接器一起傳送AS2的訊息中用作SubjectHTTP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

連接器合作夥伴設定檔的唯一識別符。

類型：字串

長度限制條件：固定長度為 19。

模式：p-([0-9a-f]{17})

必要：否

SigningAlgorithm

用來簽署與連接器一起傳送AS2之訊息的演算法。

類型：字串

有效值:SHA256 | SHA384 | SHA512 | SHA1 | NONE

必要：否

另請參閱

如需在其中一種語言特定的 API中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

CopyStepDetails

每個步驟類型都有自己的StepDetails結構。

目錄

DestinationFileLocation

指定要複製之檔案的位置。在此`{Transfer:UploadDate}`欄位中，使用`{Transfer:UserName}`或，依使用者名稱或上傳日期將目的地字首參數化。

- 將的值設定為`DestinationFileLocation${Transfer:UserName}`，將上傳的檔案複製到 Amazon S3 儲存貯體，該儲存貯體前面加上上傳檔案的 Transfer Family 使用者名稱。
- 將的值設定為`DestinationFileLocation${Transfer:UploadDate}`，以將上傳的檔案複製到 Amazon S3 儲存貯體，該儲存貯體的字首為上傳日期。



Note

系統會根據檔案上傳到的日期，解析UploadDate為 YYYY-MM-DD 的日期格式UTC。

類型：[InputFileLocation](#) 物件

必要：否

Name

步驟的名稱，用作識別符。

類型：字串

長度限制：長度下限為 0。長度上限為 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具有相同名稱的檔案，則行為如下：

- 如果 OverwriteExisting是 TRUE，現有檔案會取代為正在處理的檔案。

- 如果 `OverwriteExisting` 是 `FALSE`，則不會發生任何情況，而且工作流程處理會停止。

類型：字串

有效值: `TRUE` | `FALSE`

必要：否

SourceFileLocation

指定要使用哪個檔案作為工作流程步驟的輸入：上一個步驟的輸出，或工作流程的原始上傳檔案。

- 若要使用上一個檔案作為輸入，請輸入 `${previous.file}`。在此情況下，此工作流程步驟會使用上一個工作流程步驟的輸出檔案作為輸入。這是預設值。
- 若要使用原始上傳的檔案位置作為此步驟的輸入，請輸入 `${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

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

CustomStepDetails

每個步驟類型都有自己的StepDetails結構。

目錄

Name

步驟的名稱，用作識別符。

類型：字串

長度限制：長度下限為 0。長度上限為 30。

模式：`[\w-]*`

必要：否

SourceFileLocation

指定要使用哪個檔案作為工作流程步驟的輸入：上一個步驟的輸出，或工作流程的原始上傳檔案。

- 若要使用上一個檔案作為輸入，請輸入 `${previous.file}`。在此情況下，此工作流程步驟會使用上一個工作流程步驟的輸出檔案作為輸入。這是預設值。
- 若要使用原始上傳的檔案位置作為此步驟的輸入，請輸入 `${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ARN的 Lambda 函數的。

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

步驟逾時，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

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

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。在此`{Transfer:UploadDate}`欄位中，使用`{Transfer:UserName}`或`{Transfer:UploadDate}`，依使用者名稱或上傳日期將目的地字首參數化。

- 將 `DestinationFileLocation` 的值設定為 `DestinationFileLocation{Transfer:UserName}`，以將上傳的檔案解密為 Amazon S3 儲存貯體，該儲存貯體前面加上上傳檔案的 Transfer Family 使用者名稱。
- 將 `DestinationFileLocation` 的值設定為 `DestinationFileLocation{Transfer:UploadDate}`，以將上傳的檔案解密為以上傳日期為前綴的 Amazon S3 儲存貯體。



Note

系統會根據檔案上傳到的日期，解析`UploadDate`為 YYYY-MM-DD 的日期格式UTC。

類型：[InputFileLocation](#) 物件

必要：是

Type

使用的加密類型。目前，此值必須為 PGP。

類型：字串

有效值:PGP

必要：是

Name

步驟的名稱，用作識別符。

類型：字串

長度限制：長度下限為 0。長度上限為 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具有相同名稱的檔案，則行為如下：

- 如果 OverwriteExisting 是 TRUE，現有檔案會取代為正在處理的檔案。
- 如果 OverwriteExisting 是 FALSE，則不會發生任何情況，而且工作流程處理會停止。

類型：字串

有效值:TRUE | FALSE

必要：否

SourceFileLocation

指定要使用哪個檔案作為工作流程步驟的輸入：上一個步驟的輸出，或工作流程的原始上傳檔案。

- 若要使用上一個檔案作為輸入，請輸入 `${previous.file}`。在此情況下，此工作流程步驟會使用上一個工作流程步驟的輸出檔案作為輸入。這是預設值。
- 若要使用原始上傳的檔案位置作為此步驟的輸入，請輸入 `${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

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

DeleteStepDetails

步驟的名稱，用於識別刪除步驟。

目錄

Name

步驟的名稱，用作識別符。

類型：字串

長度限制：長度下限為 0。長度上限為 30。

模式：`[\w-]*`

必要：否

SourceFileLocation

指定要使用哪個檔案作為工作流程步驟的輸入：上一個步驟的輸出，或工作流程的原始上傳檔案。

- 若要使用上一個檔案作為輸入，請輸入 `${previous.file}`。在此情況下，此工作流程步驟會使用上一個工作流程步驟的輸出檔案作為輸入。這是預設值。
- 若要使用原始上傳的檔案位置作為此步驟的輸入，請輸入 `${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

如需在其中一種語言特定 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

DescribedAccess

描述指定之存取的屬性。

目錄

ExternalId

識別目錄中特定群組所需的唯一識別碼。您關聯的群組使用者可透過使用的已啟用通訊協定存取您的 Amazon S3 或 Amazon EFS 資源 AWS Transfer Family。如果您知道群組名稱，則可以使用 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以 Active Directory 群組的名稱取代。

用來驗證此參數的規則運算式是由大寫和小寫英數字元組成的字串，不含空格。您也可以包含底線或任何下列字元：=, .@ : /-

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

邏輯目錄映射，可指定使用者應看到哪些 Amazon S3 或 Amazon EFS 路徑和金鑰，以及您希望如何使其可見。您必須指定 Entry 和 Target 對，其中 Entry 顯示如何顯示路徑，並且 Target 是實際的 Amazon S3 或 Amazon EFS 路徑。如果您只指定目標，則會顯示為原樣。您也必須確保 AWS Identity and Access Management (IAM) 角色提供對中路徑的存取權 Target。只有在設定為時，才能 HomeDirectoryType 設定此值 LOGICAL。

在大多數情況下，您可以使用此值，而不是工作階段政策來鎖定對指定主目錄 ("chroot") 的關聯存取。若要這麼做，您可以將 Entry 設定為 '/' 並 Target 設定為 HomeDirectory 參數值。

類型：[HomeDirectoryMapEntry](#) 物件陣列

陣列成員：項目數下限為 1。最多 50000 個項目。

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。如果您將其設定為 PATH，則使用者會看到絕對 Amazon S3 儲存貯體或 Amazon EFS 路徑，就像在其檔案傳輸通訊協定用戶端一樣。如果您將其設定為 LOGICAL，則需要在 中提供映射，HomeDirectoryMappings 以了解如何讓使用者看見 Amazon S3 或 Amazon EFS 路徑。

Note

如果 HomeDirectoryType 是 LOGICAL，您必須使用 HomeDirectoryMappings 參數提供映射。另一方面，如果 HomeDirectoryType 是 PATH，則您使用 HomeDirectory 參數提供絕對路徑。您無法在範本 HomeDirectoryMappings 中同時擁有 HomeDirectory 和 。

類型：字串

有效值:PATH | LOGICAL

必要：否

Policy

適用於使用者在工作階段政策，讓您可以在多個使用者之間使用相同的 AWS Identity and Access Management (IAM) 角色。此政策會減少使用者對其 Amazon S3 儲存貯體部分存取權的範圍。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

完整的POSIX身分，包括使用者 ID (Uid)、群組 ID (Gid) 和任何次要群組 IDs (SecondaryGids)，可控制使用者對 Amazon EFS 檔案系統的存取。在檔案系統中的檔案和目錄上設定的POSIX許可決定了使用者在將檔案移入和移出 Amazon EFS 檔案系統時獲得的存取層級。

類型：[PosixProfile](#) 物件

必要：否

Role

(ARN) 角色的 Amazon Resource Name AWS Identity and Access Management (IAM)，可控制使用者對 Amazon S3 儲存貯體或 Amazon EFS 檔案系統的存取。附加至此角色的政策會決定在將檔案移入和移出 Amazon S3 儲存貯體或 Amazon EFS 檔案系統時，您要為使用者提供的存取層級。此IAM角色也應包含信任關係，允許伺服器在服務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

如需在其中一種語言特定的 API中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

DescribedAgreement

描述協議的屬性。

目錄

Arn

合約的唯一 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

AccessRole

連接器用於使用 AS2或 SFTP通訊協定傳送檔案。針對存取角色，提供要使用 AWS Identity and Access Management 的角色的 Amazon Resource Name (ARN)。

對於AS2連接器

使用 AS2時，您可以呼叫StartFileTransfer並指定請求參數 中的檔案路徑來傳送檔案SendFilePaths。我們使用檔案的父目錄（例如--send-file-paths /bucket/dir/file.txt，對於，父目錄為 /bucket/dir/）來暫時存放已處理AS2的訊息檔案、MDN在我們從合作夥伴收到時存放，以及撰寫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。

如果您為AS2連接器使用基本身分驗證，存取角色需要秘密的secretsmanager:GetSecretValue許可。如果秘密是使用客戶受管金鑰而非 Secrets Manager 中的 AWS 受管金鑰加密，則角色也需要該金鑰的kms:Decrypt許可。

對於SFTP連接器

請確定存取角色提供對StartFileTransfer請求中所用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 secretsmanager:GetSecretValue許可 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

協議的唯一識別符。當您建立協議時，會傳回此識別碼。

類型：字串

長度限制條件：固定長度為 19。

模式：`a-([0-9a-f]{17})`

必要：否

BaseDirectory

使用AS2通訊協定傳輸之檔案的登陸目錄（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符。

類型：字串

長度限制條件：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

長度限制條件：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

長度限制條件：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

如需在其中一種語言特定 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

DescribedCertificate

描述憑證的屬性。

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。長度上限為 2097152。

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

長度限制條件：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。長度上限為 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

指定此憑證用於簽署或加密。

類型：字串

有效值:SIGNING | ENCRYPTION

必要：否

另請參閱

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

DescribedConnector

描述連接器的參數，如 所識別ConnectorId。

目錄

Arn

連接器的唯一 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

AccessRole

連接器用於使用 AS2或 SFTP通訊協定傳送檔案。針對存取角色，提供要使用 AWS Identity and Access Management 的角色的 Amazon Resource Name (ARN)。

對於AS2連接器

使用 AS2，您可以呼叫StartFileTransfer並指定請求參數 中的檔案路徑來傳送檔案SendFilePaths。我們使用檔案的父目錄（例如--send-file-paths /bucket/dir/file.txt，對於，父目錄為 /bucket/dir/）暫時存放已處理AS2的訊息檔案、在我們從合作夥伴收到MDN時存放，以及撰寫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。

如果您為AS2連接器使用基本身分驗證，存取角色需要秘密的secretsmanager:GetSecretValue許可。如果秘密是使用客戶管理金鑰而非 Secrets Manager 中的 AWS 受管金鑰加密，則角色也需要該金鑰的kms:Decrypt許可。

對於SFTP連接器

請確定存取角色提供對StartFileTransfer請求中所用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 secretsmanager:GetSecretValue許可 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

連接器的唯一識別符。

類型：字串

長度限制條件：固定長度為 19。

模式：`c-([0-9a-f]{17})`

必要：否

LoggingRole

(ARN) 角色的 Amazon Resource Name AWS Identity and Access Management (IAM)，允許連接器開啟 Amazon S3 事件 CloudWatch 的記錄。設定時，您可以在 CloudWatch 日誌中檢視連接器活動。

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

ServiceManagedEgressIpAddresses

此連接器的輸出 IP 地址清單。這些 IP 地址會在您建立連接器時自動指派。

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

URL 合作夥伴AS2或SFTP端點的。

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

如需在其中一種語言特定的 API中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

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碼。

類型：字串

長度限制條件：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：如果正在複製檔案，則這是初始（而不是目的地）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

完整的POSIX身分，包括使用者 ID (Uid)、群組 ID (Gid) 和任何次要群組 IDs (SecondaryGids)，可控制使用者對 Amazon EFS 檔案系統的存取。檔案系統中檔案和目錄上設定的POSIX許可決定了使用者在將檔案移入和移出 Amazon EFS 檔案系統時所取得的存取層級。

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OnExceptionSteps結構。

類型：[ExecutionResults](#) 物件

必要：否

ServiceMetadata

與工作流程相關聯的工作階段詳細資訊容器物件。

類型：[ServiceMetadata](#) 物件

必要：否

Status

狀態為其中一個執行。可以是進行中、已完成、遇到例外狀況或處理例外狀況。

類型：字串

有效值:IN_PROGRESS | COMPLETED | EXCEPTION | HANDLING_EXCEPTION

必要：否

另請參閱

如需在其中一種語言特定的 API中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)

- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

DescribedHostKey

伺服器主機金鑰的詳細資訊。

目錄

Arn

主機金鑰的唯一 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

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

公有金鑰指紋，這是用於識別較長公有金鑰的短位元組序列。

類型：字串

必要：否

HostKeyId

主機金鑰的唯一識別符。

類型：字串

長度限制條件：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鍵值對。

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

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

如需在其中一種語言特定 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)

- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

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 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

As2Id

As2Id 是 AS2-name，如 [RFC4130](#) 中所定義。對於傳入傳輸，這是從合作夥伴AS2傳送訊息的AS2-From標頭。對於傳出連接器，這是使用 StartFileTransferAPI操作傳送給合作夥伴AS2的訊息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

長度限制條件：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設定檔的唯一識別符。

類型：字串

長度限制條件：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

如需在其中一種語言特定的 API中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

DescribedSecurityPolicy

描述指定之安全政策的屬性。如需安全政策的詳細資訊，請參閱[使用安全政策](#)。

目錄

SecurityPolicyName

指定連接至伺服器的安全政策名稱。

類型：字串

長度限制：長度下限為 0。長度上限為 100。

模式：TransferSecurityPolicy-.*+

必要：是

Fips

指定此政策是否啟用聯邦資訊處理標準（FIPS）。

類型：布林值

必要：否

SshCiphers

在連接到伺服器的安全政策中指定已啟用的安全 Shell（SSH）密碼加密演算法。

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

在連接到伺服器的安全政策中指定已啟用的SSH金鑰交換（KEX）加密演算法。

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

在連接到伺服器的安全政策中指定已啟用SSH的訊息驗證碼（ MAC ）加密演算法。

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

在連接到伺服器的安全政策中指定已啟用的 Transport Layer Security（ TLS ）密碼加密演算法。

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

另請參閱

如需在其中一種語言特定 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

DescribedServer

描述指定的檔案傳輸通訊協定啟用伺服器屬性。

目錄

Arn

指定伺服器的唯一 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

As2ServiceManagedEgressIpAddresses

此伺服器的輸出 IP 地址清單。這些 IP 地址僅適用於使用AS2通訊協定的伺服器。它們用於傳送非同步 MDNs。

這些 IP 地址會在您建立AS2伺服器時自動指派。此外，如果您更新現有的伺服器並新增AS2通訊協定，也會指派靜態 IP 地址。

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 AWS Certificate Manager (ACM) 憑證ARN的。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。

類型：字串

有效值:S3 | EFS

必要：否

EndpointDetails

為您的伺服器設定的虛擬私有雲端（VPC）端點設定。當您在 中託管端點時VPC，您只能讓 中的資源存取端點VPC，也可以連接彈性 IP 地址，讓用戶端透過網際網路存取端點。您 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

定義伺服器連線的端點類型。如果您的伺服器已連線至VPC端點，則無法透過公有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-encodedSHA256指紋。此值等同於 `ssh-keygen -l -f my-new-server-key` 命令的輸出。

類型：字串

必要：否

IdentityProviderDetails

指定呼叫客戶提供身分驗證的資訊API。當伺服器的 為 `AWS_DIRECTORY_SERVICE`或時`IdentityProviderType`，不會填入此欄位`SERVICE_MANAGED`。

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 服務中存放和存取使用者憑證。

使用 `AWS_DIRECTORY_SERVICE` 可讓您存取內部部署環境 AWS Directory Service for Microsoft Active Directory 或使用 AWS AD Connector 的 或 Microsoft Active Directory 中的 Active Directory 群組。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。此 `API_GATEWAY` 設定要求您提供 Amazon API Gateway 端點 URL，以使用 `IdentityProviderDetails` 參數呼叫以進行身分驗證。

使用 `AWS_LAMBDA` 值直接使用 AWS Lambda 函數作為您的身分提供者。如果您選擇此值，您必須在 `IdentityProviderDetails` 資料類型 ARN 的 `Function` 參數中指定 Lambda 函數的。

類型：字串

有效值：`SERVICE_MANAGED` | `API_GATEWAY` | `AWS_DIRECTORY_SERVICE` | `AWS_LAMBDA`

必要：否

LoggingRole

(ARN) 角色的 Amazon Resource Name AWS Identity and Access Management (IAM)，允許伺服器開啟 Amazon S3 或 Amazon 的 Amazon CloudWatch 記錄 `EFSevents`。設定時，您可以在 CloudWatch 日誌中檢視使用者活動。

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。

- 若要指示被動模式（適用於 FTP 和 FTPS 通訊協定），請使用 `PassiveIp` 參數。輸入單一點四 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 `SETSTAT` 命令並上傳檔案，而不需要對 SFTP 用戶端進行任何變更，請將值設定為 `ENABLE_NO_OP`。如果您將 `SetStatOption` 參數設定為 `ENABLE_NO_OP`，Transfer Family 會產生 Amazon CloudWatch Logs 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 來恢復最近的交涉工作階段，請使用 `TlsSessionResumptionMode` 參數。
- `As2Transports` 表示 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 (Secure Shell (SSH) 檔案傳輸通訊協定)：檔案傳輸 SSH
- FTPS (檔案傳輸通訊協定安全)：使用TLS加密進行檔案傳輸
- FTP (檔案傳輸通訊協定)：未加密的檔案傳輸
- AS2 (適用性陳述式 2)：用於傳輸結構化 business-to-business 資料

Note

- 如果您選擇 FTPS，您必須選擇儲存在 AWS Certificate Manager (ACM) 中的憑證，當用戶端透過 連線到伺服器時，該憑證可用來識別您的伺服器FTPS。
- 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。

有效值:SFTP | FTP | FTPS | AS2

必要：否

S3StorageOptions

指定是否最佳化 Amazon S3 目錄的效能。此選項根據預設為停用。

根據預設，主目錄映射具有 TYPE 的 DIRECTORY。如果您啟用此選項，則 HomeDirectoryMapEntryType FILE 如果您想要映射具有檔案目標，則需要將 明確設定為。

類型：[S3StorageOptions](#) 物件

必要：否

SecurityPolicyName

指定連接至伺服器的安全政策名稱。

類型：字串

長度限制：長度下限為 0。長度上限為 100。

模式：TransferSecurityPolicy-.+

必要：否

ServerId

指定您實例化之伺服器的唯一系統指派識別碼。

類型：字串

長度限制條件：固定長度為 19。

模式：s-([0-9a-f]{17})

必要：否

State

描述的伺服器條件。的值 ONLINE 表示伺服器可接受任務和傳輸檔案。State 的值 OFFLINE 表示伺服器無法執行檔案傳輸操作。

STARTING 和 的狀態 STOPPING 表示伺服器處於中繼狀態，可能是無法完全回應，或並非完全離線。START_FAILED 或 的值 STOP_FAILED 可以指示錯誤條件。

類型：字串

有效值:OFFLINE | ONLINE | STARTING | STOPPING | START_FAILED | STOP_FAILED

必要：否

StructuredLogDestinations

指定伺服器日誌的傳送目的地日誌群組。

若要指定日誌群組，您必須ARN為現有日誌群組提供。在此情況下，日誌群組的格式如下：

`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日誌群組，您可以清除該群組，並在update-server通話中提供此參數的空值，並實際上關閉結構化日誌。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

指定您可以用來搜尋並分組指派給所述伺服器的金鑰值對。

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

UserCount

指定指派給您使用 指定的伺服器的使用者數量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)。當伺服器工作階段在檔案仍在上傳時中斷連線時，會發生部分上傳。

類型：[WorkflowDetails](#) 物件

必要：否

另請參閱

如需在其中一種語言特定 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

DescribedUser

描述指定的使用者屬性。

目錄

Arn

為請求描述的使用者指定唯一的 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

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

邏輯目錄映射，可指定使用者應看到哪些 Amazon S3 或 Amazon EFS 路徑和金鑰，以及您希望如何使其可見。您必須指定 Entry 和 Target 對，其中 Entry 顯示如何顯示路徑，並且 Target 是實際的 Amazon S3 或 Amazon EFS 路徑。如果您只指定目標，則會顯示為原樣。您也必須確保

AWS Identity and Access Management (IAM) 角色提供對 中路徑的存取權Target。只有在 設定為 時，才能HomeDirectoryType設定此值LOGICAL。

在大多數情況下，您可以使用此值來取代工作階段政策，將使用者鎖定至指定的主目錄 ("chroot")。若要這麼做，您可以將 Entry設定為 '/' 並Target設定為 HomeDirectory 參數值。

類型：[HomeDirectoryMapEntry](#) 物件陣列

陣列成員：項目數下限為 1。最多 50000 個項目。

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。如果您將其設定為 PATH，則使用者會看到絕對 Amazon S3 儲存貯體或 Amazon EFS 路徑，就像在其檔案傳輸通訊協定用戶端一樣。如果您將其設定為 LOGICAL，則需要在 中提供映射，HomeDirectoryMappings以了解如何讓使用者看見 Amazon S3 或 Amazon EFS 路徑。

Note

如果 HomeDirectoryType是 LOGICAL，您必須使用 HomeDirectoryMappings 參數提供映射。另一方面，如果 HomeDirectoryType是 PATH，則您使用 HomeDirectory 參數提供絕對路徑。您無法在範本HomeDirectoryMappings中同時擁有 HomeDirectory和。

類型：字串

有效值:PATH | LOGICAL

必要：否

Policy

適用於使用者的工作階段政策，讓您可以在多個使用者之間使用相同的 AWS Identity and Access Management (IAM) 角色。此政策會減少使用者對其 Amazon S3 儲存貯體部分存取權的範圍。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POSIX身分，包括使用者 ID (Uid)、群組 ID IDs (Gid) 和任何次要群組 (SecondaryGids)，以控制使用者對 Amazon Elastic File System (Amazon EFS) 檔案系統的存取。在檔案系統中的檔案和目錄上設定的POSIX許可決定了使用者在將檔案移入和移出 Amazon EFS 檔案系統時獲得的存取層級。

類型：[PosixProfile](#) 物件

必要：否

Role

(ARN) 角色的 Amazon Resource Name AWS Identity and Access Management (IAM)，可控制使用者對 Amazon S3 儲存貯體或 Amazon EFS 檔案系統的存取。附加至此角色的政策會決定在將檔案移入和移出 Amazon S3 儲存貯體或 Amazon EFS 檔案系統時，您要為使用者提供的存取層級。此IAM角色也應包含信任關係，允許伺服器在服務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

指定為描述的使用者存放的安全 Shell (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

指定所請求使用者的鍵值對。標籤可用於搜尋和分組各種用途的使用者。

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

指定請求描述的使用者名稱。使用者名稱用於身分驗證目的。這是使用者登入伺服器時將使用的字串。

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：否

另請參閱

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

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 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

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。

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。

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

長度限制條件：固定長度為 19。

模式：`w-([a-z0-9]{17})`

必要：否

另請參閱

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

EfsFileLocation

指定工作流程中使用的檔案檔案位置詳細資訊。僅適用於使用 Amazon Elastic File Systems (Amazon EFS) 進行儲存。

目錄

FileSystemId

Amazon 指派的檔案系統的識別碼EFS。

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

工作流程所使用的資料夾路徑名稱。

類型：字串

長度限制：長度下限為 1。長度上限為 65536。

模式：[^\x00]+

必要：否

另請參閱

如需在其中一種語言特定的 API中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

EndpointDetails

為您的檔案傳輸協定啟用伺服器設定的虛擬私有雲端（VPC）端點設定。使用VPC端點時，您只能限制對伺服器和資源的存取VPC。若要控制傳入網際網路流量，請叫用 `UpdateServerAPI` 並將彈性 IP 地址連接至伺服器的端點。

Note

2021 年 5 月 19 日後，如果您的帳戶在 2021 年 5 月 19 日之前尚未建立伺服器，您將無法 `EndpointType=VPC_ENDPOINT` 在 AWS 帳戶中使用 建立伺服器。如果您已 `EndpointType=VPC_ENDPOINT` 在 2021 年 5 月 19 日或之前在 AWS 帳戶中使用 建立伺服器，則不會受到影響。在此日期之後，請使用 `EndpointType=VPC`。如需詳細資訊，請參閱 [停止使用 VPC_ENDPOINT](#)。

目錄

AddressAllocationIds

將彈性 IP 地址連接至伺服器端點IDs所需的地址配置清單。

地址配置 ID 對應彈性 IP 地址的配置 ID。此值可以從 Amazon EC2 [Address](#) 資料類型 `allocationId` 的欄位擷取。擷取此值的一種方法是呼叫 EC2 [DescribeAddresses](#) API。

此為選用參數。如果您想要讓VPC端點面向公有，請設定此參數。如需詳細資訊，請參閱為您的 [伺服器 建立面向網際網路的端點](#)。

Note

此屬性只能設定如下：

- `EndpointType` 必須設定為 VPC
- Transfer Family 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。
- 伺服器必須已填入 `SubnetIds`（`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 IDs，您還必須指定三個地址配置 IDs。

- 呼叫 `UpdateServerAPI` 以設定或變更此參數。

類型：字串陣列

必要：否

`SecurityGroupIds`

IDs 可連接至伺服器端點的安全群組清單。

 Note

只有當 `EndpointType` 設為 `VPC` 時，才能設定此屬性。

[UpdateServer](#) API 只有在您將 `EndpointType` 從 `PUBLIC` 或 變更為 `VPC_ENDPOINT` 時，才能編輯 中的 `SecurityGroupIds` 屬性VPC。若要在建立伺服器VPC端點後變更相關聯的安全群組，請使用 Amazon EC2 [ModifyVpcEndpoint](#) API。

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 中託管伺服器端點IDs所需的子網路清單VPC。

 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 端點的識別符。

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_ENDPOINT](#)。

類型：字串

長度限制條件：固定長度為 22。

模式：`vpce-[0-9a-f]{17}`

必要：否

`VpcId`

託管VPC伺服器端點的 VPC識別符。

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

如需在其中一種語言特定的 API中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

ExecutionError

針對在工作流程執行期間發生的錯誤，指定錯誤訊息和類型。

目錄

Message

指定對應的描述性訊息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，則複製步驟會發生。
- **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**，因為只有 S3 檔案可以標記。
- **CUSTOM_STEP_FAILED**：當自訂步驟提供表示失敗的回呼時，便會發生。
- **INTERNAL_SERVER_ERROR**：可能因各種原因而發生的完全捕獲錯誤。
- **NOT_FOUND**：當請求的實體，例如複製步驟的來源檔案不存在時，就會發生。
- **PERMISSION_DENIED**：如果您的政策不包含完成工作流程中一或多個步驟的正確許可，則會發生。
- **TIMEOUT**：在執行逾時時發生。



Note

您可以TimeoutSeconds為自訂步驟設定，範圍從 1 秒到 1800 秒（30 分鐘）。

- **THROTTLED**：如果您超過每秒一個工作流程的新執行補充速率，就會發生。

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

如需在其中一種語言特定 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

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

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

ExecutionStepResult

指定步驟的下列詳細資訊：錯誤（如果有）、輸出（如果有）和步驟類型。

目錄

Error

如果錯誤是在執行指定的工作流程步驟期間發生，請指定錯誤的詳細資訊。

類型：[ExecutionError](#) 物件

必要：否

Outputs

套用為 檔案標籤的鍵/值對值。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。長度上限為 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

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

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識別符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 詳細資訊，例如儲存貯體ETag、等。

類型：[S3FileLocation](#) 物件

必要：否

另請參閱

如需在其中一種語言特定的 API中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

HomeDirectoryMapEntry

代表物件，包含 HomeDirectoryMappings 的項目和目標。

以下是的 Entry和 Target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

指定映射的類型。FILE 如果您想要映射指向檔案，請將類型設定為 `FILE`，或DIRECTOR將目錄設定為 `DIRECTORY`。

Note

根據預設，當您建立 Transfer Family 伺服器DIRECTOR時，主目錄映射具有 `FILE` 的 `Type`。FILE 如果您想要映射具有檔案目標，則需要明確Type地將 `Type` 設定為 `FILE`。

類型：字串

有效值:FILE | DIRECTORY

必要：否

另請參閱

如需在其中一種語言特定的 API中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

IdentityProviderDetails

傳回啟用檔案傳輸通訊協定之伺服器使用者正在使用的使用者身分驗證類型的相關資訊。伺服器只能有一個身分驗證方法。

目錄

DirectoryId

您要用作身分提供者之 AWS Directory Service 目錄的識別碼。

類型：字串

長度限制條件：固定長度為 12。

模式：d-[0-9a-f]{10}

必要：否

Function

ARN Lambda 函數用於 Identity 提供者的。

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

此參數僅適用於您的 IdentityProviderType 為 的情況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，以及僅自訂身分提供者，您可以指定使用密碼、SSH 金鑰對或兩者進行身分驗證。

- `PASSWORD` - 使用者必須提供其密碼才能連線。
- `PUBLIC_KEY` - 使用者必須提供其私有金鑰才能連線。
- `PUBLIC_KEY_OR_PASSWORD` - 使用者可以使用其密碼或金鑰進行身分驗證。這是預設值。
- `PUBLIC_KEY_AND_PASSWORD` - 使用者必須提供其私有金鑰和密碼才能連線。伺服器會先檢查金鑰，如果金鑰有效，系統會提示輸入密碼。如果提供的私有金鑰與儲存的公有金鑰不相符，身分驗證會失敗。

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

如需在其中一種語言特定 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

InputFileLocation

指定正在處理之檔案的位置。

目錄

EfsFileLocation

指定要解密之 Amazon Elastic File System (Amazon EFS) 檔案的詳細資訊。

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

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

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。您關聯的群組使用者可透過使用的已啟用通訊協定存取您的 Amazon S3 或 Amazon EFS 資源 AWS Transfer Family。如果您知道群組名稱，則可以使用 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以 Active Directory 群組的名稱取代。

用來驗證此參數的規則運算式是由大寫和小寫英數字元組成的字串，不含空格。您也可以包含底線或任何下列字元：=, .@ : /-

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。如果您將其設定為 PATH，則使用者會看到絕對 Amazon S3 儲存貯體或 Amazon EFS 路徑，就像在其檔案傳輸通訊協定用戶端一樣。如果您將其設定為 LOGICAL，則需要在 中提供映射，HomeDirectoryMappings以了解如何讓使用者看見 Amazon S3 或 Amazon EFS 路徑。

Note

如果 HomeDirectoryType是 LOGICAL，您必須使用 HomeDirectoryMappings 參數提供映射。另一方面，如果 HomeDirectoryType是 PATH，則您使用 HomeDirectory 參數提供絕對路徑。您無法在範本HomeDirectoryMappings中同時擁有 HomeDirectory和。

類型：字串

有效值:PATH | LOGICAL

必要：否

Role

(ARN) 角色的 Amazon Resource Name AWS Identity and Access Management (IAM)，可控制使用者對 Amazon S3 儲存貯體或 Amazon EFS 檔案系統的存取。附加至此角色的政策會決定在將檔案移入和移出 Amazon S3 儲存貯體或 Amazon EFS 檔案系統時，您要為使用者提供的存取層級。此IAM角色也應包含信任關係，允許伺服器在服務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

如需在其中一種語言特定的 API中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

ListedAgreement

描述協議的屬性。

目錄

AgreementId

協議的唯一識別符。當您建立協議時，會傳回此識別碼。

類型：字串

長度限制條件：固定長度為 19。

模式：a-([0-9a-f]{17})

必要：否

Arn

指定協議的 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：否

Description

協議的目前描述。您可以呼叫 UpdateAgreement 操作並提供新的描述來變更它。

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符。

類型：字串

長度限制條件：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符。

類型：字串

長度限制條件：固定長度為 19。

模式：p-([0-9a-f]{17})

必要：否

ServerId

協議的唯一識別符。

類型：字串

長度限制條件：固定長度為 19。

模式：s-([0-9a-f]{17})

必要：否

Status

協議可以是 ACTIVE 或 INACTIVE。

類型：字串

有效值:ACTIVE | INACTIVE

必要：否

另請參閱

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

ListedCertificate

描述憑證的屬性。

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 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：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

長度限制條件：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

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

指定此憑證用於簽署或加密。

類型：字串

有效值:SIGNING | ENCRYPTION

必要：否

另請參閱

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

ListedConnector

傳回指定連接器的詳細資訊。

目錄

Arn

指定連接器的 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：否

ConnectorId

連接器的唯一識別符。

類型：字串

長度限制條件：固定長度為 19。

模式：c-([0-9a-f]{17})

必要：否

Url

URL 合作夥伴AS2或SFTP端點的 。

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

如需在其中一種語言特定的 API中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

ListedExecution

傳回指定執行的屬性。

目錄

ExecutionId

用於執行工作流程的唯一識別碼。

類型：字串

長度限制條件：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：如果正在複製檔案，則這是初始（而不是目的地）檔案位置。

類型：[FileLocation](#) 物件

必要：否

ServiceMetadata

與工作流程相關聯的工作階段詳細資訊容器物件。

類型：[ServiceMetadata](#) 物件

必要：否

Status

狀態為其中一個執行。可以是進行中、已完成、遇到例外狀況或處理例外狀況。

類型：字串

有效值:IN_PROGRESS | COMPLETED | EXCEPTION | HANDLING_EXCEPTION

必要：否

另請參閱

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

ListedHostKey

傳回指定的主機金鑰屬性。

目錄

Arn

主機金鑰的唯一 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

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。您可以呼叫 UpdateHostKey 操作並提供新的描述來變更它。

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

公有金鑰指紋，這是用於識別較長公有金鑰的短位元組序列。

類型：字串

必要：否

HostKeyId

主機金鑰的唯一識別符。

類型：字串

長度限制條件：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

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

ListedProfile

傳回指定之設定檔的屬性。

目錄

Arn

指定設定檔的 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：否

As2Id

As2Id 是 AS2-name，如 [RFC4130](#) 中所定義。對於傳入傳輸，這是從合作夥伴AS2傳送訊息的AS2-From標頭。對於傳出連接器，這是使用 StartFileTransferAPI操作傳送給合作夥伴AS2的訊息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設定檔的唯一識別符。

類型：字串

長度限制條件：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

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

ListedServer

傳回指定的已啟用檔案傳輸通訊協定之伺服器的屬性。

目錄

Arn

指定要列出的伺服器的唯一 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

Domain

指定用於檔案傳輸的儲存系統網域。

類型：字串

有效值:S3 | EFS

必要：否

EndpointType

指定伺服器連線的VPC端點類型。如果您的伺服器已連線至VPC端點，則無法透過公有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 服務中存放和存取使用者憑證。

使用 `AWS_DIRECTORY_SERVICE` 可讓您存取內部部署環境 AWS Directory Service for Microsoft Active Directory 或使用 AWS AD Connector 的 或 Microsoft Active Directory 中的 Active Directory 群組。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。此 `API_GATEWAY` 設定要求您提供 Amazon API Gateway 端點 URL，以使用 `IdentityProviderDetails` 參數呼叫以進行身分驗證。

使用 `AWS_LAMBDA` 值直接使用 AWS Lambda 函數作為您的身分提供者。如果您選擇此值，您必須在 `IdentityProviderDetails` 資料類型 ARN 的 `Function` 參數中指定 Lambda 函數的。

類型：字串

有效值: `SERVICE_MANAGED` | `API_GATEWAY` | `AWS_DIRECTORY_SERVICE` | `AWS_LAMBDA`

必要：否

LoggingRole

(ARN) 角色的 Amazon Resource Name AWS Identity and Access Management (IAM)，允許伺服器開啟 Amazon S3 或 Amazon 的 Amazon CloudWatch 記錄 `EFSevents`。設定時，您可以在 CloudWatch 日誌中檢視使用者活動。

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符。

類型：字串

長度限制條件：固定長度為 19。

模式：`s-([0-9a-f]{17})`

必要：否

State

描述的伺服器條件。的值 `ONLINE` 表示伺服器可接受任務和傳輸檔案。State 的值 `OFFLINE` 表示伺服器無法執行檔案傳輸操作。

STARTING 和 的狀態STOPPING表示伺服器處於中繼狀態，可能是無法完全回應，或並非完全離線。START_FAILED 或 的值STOP_FAILED可以指示錯誤條件。

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 指定的伺服器的使用者數量ServerId。

類型：整數

必要：否

另請參閱

如需在其中一種語言特定的 API中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

ListedUser

傳回您指定的使用者屬性。

目錄

Arn

為您要了解的使用者提供唯一的 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

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。如果您將其設定為 PATH，則使用者會看到絕對 Amazon S3 儲存貯體或 Amazon EFS 路徑，就像在其檔案傳輸通訊協定用戶端一樣。如果您將其設定為 LOGICAL，則需要在 中提供映射，HomeDirectoryMappings以了解如何讓使用者看見 Amazon S3 或 Amazon EFS 路徑。

Note

如果 `HomeDirectoryType` 是 `LOGICAL`，您必須使用 `HomeDirectoryMappings` 參數提供映射。另一方面，如果 `HomeDirectoryType` 是 `PATH`，您可以使用 `HomeDirectory` 參數提供絕對路徑。您無法在範本 `HomeDirectoryMappings` 中同時擁有 `HomeDirectory` 和 `HomeDirectoryMappings`。

類型：字串

有效值: `PATH` | `LOGICAL`

必要：否

Role

(ARN) 角色的 Amazon Resource Name AWS Identity and Access Management (IAM)，可控制使用者對 Amazon S3 儲存貯體或 Amazon EFS 檔案系統的存取。附加至此角色的政策會決定在將檔案移入和移出 Amazon S3 儲存貯體或 Amazon EFS 檔案系統時，您要為使用者提供的存取層級。此 IAM 角色還應包含信任關係，允許伺服器在為使用者的傳輸請求提供服務時存取您的資源。

Note

此 IAM 角色可控制使用者對具有 `Domain=S3` 之伺服器的 Amazon S3 儲存貯體的存取權，或控制具有 `Domain=EFS` 之伺服器 EFS 的檔案系統存取權。附加至此角色的政策會決定在將檔案移入和移出 S3 儲存貯體或 EFS 檔案系統時，您要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 公有金鑰數目。

類型：整數

必要：否

UserName

指定ARN指定其的使用者名稱。使用者名稱用於身分驗證目的。

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

如需在其中一種語言特定 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

ListedWorkflow

包含工作流程的識別碼、文字描述和 Amazon Resource Name (ARN)。

目錄

Arn

指定工作流程的唯一 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：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

長度限制條件：固定長度為 19。

模式：w-([a-z0-9]{17})

必要：否

另請參閱

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

LoggingConfiguration

由記錄角色和日誌群組名稱組成。

目錄

LoggingRole

(ARN) 角色的 Amazon Resource Name AWS Identity and Access Management (IAM) , 允許伺服器開啟 Amazon S3 或 Amazon 的 Amazon CloudWatch 記錄EFSevents。設定時, 您可以在 CloudWatch 日誌中檢視使用者活動。

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

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs , 請參閱下列內容:

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

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 IDs (SecondaryGids)，可控制使用者對 Amazon EFS 檔案系統的存取。檔案系統中檔案和目錄上設定的POSIX許可決定了使用者在將檔案移入和移出 Amazon EFS 檔案系統時所取得的存取層級。

目錄

Gid

此使用者用於所有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POSIX使用者用於所有EFS操作的使用者 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IDs用於所有EFS操作的次要POSIX群組。

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

如需在其中一種語言特定的 API中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

ProtocolDetails

為伺服器設定的通訊協定設定。

目錄

As2Transports

指示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 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[設定防火牆後方的FTPS伺服器或NAT搭配 AWS Transfer Family](#)。

特殊值

AUTO 和 0.0.0.0 是 PassiveIp 參數的特殊值。根據預設，該值PassiveIp=AUTO會指派給FTP並FTPS輸入伺服器。在此情況下，伺服器會自動回應回應IPs中的其中一個端點PASV。PassiveIp=0.0.0.0 具有更唯一的應用程式來使用它。例如，如果您有高可用性（HA）Network Load Balancer（NLB）環境，其中有 3 個子網路，您只能使用 PassiveIp 參數指定單一 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。這會告訴用戶端使用與 Control 連線相同的 IP 地址，並將所有 AZs 用於其連線。不過請注意，並非所

有FTP用戶端都支援PassiveIp=0.0.0.0回應。FileZilla 而 WinSCP 確實支援回應。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。

有些SFTP檔案傳輸用戶端可以嘗試使用 命令來變更遠端檔案的屬性，包括時間戳記和許可，例如上傳檔案SETSTAT時。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 值設定為 ENABLE_NO_OP，讓 Transfer Family 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。雖然SetStatOptionENABLE_NO_OP設定會忽略錯誤，但確實會在 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

如果您想要保留檔案的原始時間戳記，並使用 修改其他檔案屬性SETSTAT，則可以使用 Amazon EFS做為 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 工作階段恢復提供一種機制，在FTPS工作階段的控制項和資料連線之間繼續或共用交涉秘密金鑰。

會TlsSessionResumptionMode判斷伺服器是否透過唯一的工作階段 ID 來繼續最近的交涉工作階段。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，並為每個請求建立新的TLS工作階段。
- **ENABLED**：伺服器會處理和接受正在執行TLS工作階段恢復的用戶端。伺服器不會拒絕不執行TLS工作階段恢復用戶端處理的用戶端資料連線。
- **ENFORCED**：伺服器會處理和接受正在執行TLS工作階段恢復的用戶端。伺服器拒絕不執行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，如果您選擇強制執行TLS工作階段恢復，您可以防止來自未執行通訊協定交涉之FTPS用戶端的任何連線。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

如需在其中一種語言特定的 API中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

S3FileLocation

指定工作流程中使用的檔案檔案位置詳細資訊。僅適用於使用 S3 儲存體的情況。

目錄

Bucket

指定包含使用中檔案的 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。僅ETag反映物件的內容，而不是其中繼資料。

類型：字串

長度限制：長度下限為 1。長度上限為 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

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

S3InputFileLocation

指定客戶輸入 Amazon S3 檔案位置。如果在 內使用 `copyStepDetails.DestinationFileLocation`，則應該是 S3 複製目的地。

您需要提供儲存貯體和金鑰。金鑰可以代表路徑或檔案。這取決於您是否以正斜線（/）字元結束索引鍵值。如果最後一個字元是 "/"，則您的檔案會複製到 資料夾，其名稱不會變更。如果最終字元是英數字元，則上傳的檔案會重新命名為路徑值。在此情況下，如果具有該名稱的檔案已存在，則會覆寫該檔案。

例如，如果您的路徑是 `shared-files/bob/`，則上傳的檔案會複製到 `shared-files/bob/`、資料夾。如果您的路徑為 `shared-files/today`，則每個上傳的檔案都會複製到 `shared-files` 資料夾，並命名為 `today`：每次上傳都會覆寫舊版的 `bob` 檔案。

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

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

S3StorageOptions

為您的伺服器設定的 Amazon S3 儲存選項。

目錄

DirectoryListingOptimization

指定是否最佳化 Amazon S3 目錄的效能。此選項根據預設為停用。

根據預設，主目錄映射具有 TYPE 的 DIRECTORY。如果您啟用此選項，則 FILE 如果您想要映射具有檔案目標，則需要明確地將 HomeDirectoryMapEntry Type 設定為 。

類型：字串

有效值:ENABLED | DISABLED

必要：否

另請參閱

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

S3Tag

指定在執行標記步驟期間指派給檔案的鍵值對。

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

對應至金鑰的值。

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

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

ServiceMetadata

與工作流程相關聯的工作階段詳細資訊容器物件。

目錄

UserDetails

伺服器 ID () ServerId、工作階段 ID (SessionId) 和使用者 (UserName) 組成 UserDetails。

類型：[UserDetails](#) 物件

必要：是

另請參閱

如需在其中一種語言特定的 API中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

SftpConnectorConfig

包含SFTP連接器物件的詳細資訊。連接器物件用於在合作夥伴的SFTP伺服器之間傳輸檔案。

Note

由於SftpConnectorConfig資料類型用於建立和更新SFTP連接器、其參數，TrustedHostKeys並UserSecretId標記為不需要。這有點誤導，因為更新現有SFTP連接器時不需要，但在建立新SFTP連接器時也是必要的。

目錄

TrustedHostKeys

主機金鑰或金鑰的公有部分，用於識別您要連線的外部伺服器。您可以針對SFTP伺服器使用 `ssh-keyscan` 命令來擷取必要的金鑰。

三個標準SSH公有金鑰格式元素為 `<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`<comment>`的部分。

對於受信任的主機金鑰、AWS Transfer Family 接受RSA和ECDSA金鑰。

- 對於RSA金鑰，`<key type>`字串為 `ssh-rsa`。
- 對於ECDSA金鑰，`<key type>`字串為 `ecdsa-sha2-nistp256`、`ecdsa-sha2-nistp384`或 `ecdsa-sha2-nistp521`，取決於您產生的金鑰大小。

執行此命令以擷取SFTP伺服器主機金鑰，其中伺服器SFTP名稱為 `ftp.host.com`。

```
ssh-keyscan ftp.host.com
```

這會將公有主機金鑰列印為標準輸出。

```
ftp.host.com ssh-rsa AAAAB3Nza...<long-string-for-public-key
```

將此字串複製並貼到`create-connector`命令TrustedHostKeys的欄位，或主控台中的信任的主機金鑰欄位。

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

包含SFTP使用者私有金鑰、密碼或兩者的秘密（在 AWS Secrets Manager 中）識別符。識別符必須是秘密的 Amazon Resource Name（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

如需在其中一種語言特定的 API中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

SshPublicKey

提供與啟用特定檔案傳輸通訊協定之伺服器（由識別SSH）的 Transfer Family 使用者相關聯的公有安全 Shell（）金鑰相關資訊ServerId。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。使用者可以在特定伺服器上存放與其使用者名稱相關聯的多個SSH公有金鑰。

目錄

DateImported

指定將公有金鑰新增至 Transfer Family 使用者的日期。

類型：Timestamp

必要：是

SshPublicKeyBody

指定 指定的SSH公有金鑰內容PublicKeyId。

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 SshPublicKeyId 參數包含公有金鑰的識別符。

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

如需在其中一種語言特定的 API中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

Tag

為特定資源建立鍵值對。標籤是中繼資料，可用來搜尋資源並針對各種用途分組。您可以將標籤套用至伺服器、使用者和角色。標籤金鑰可能需要多個值。例如，若要將伺服器分組用於會計目的，您可以建立名為 Group 的標籤，並將值 Accounting Research 和 指派給該群組。

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

包含您指派給您建立之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

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

TagStepDetails

每個步驟類型都有自己的StepDetails結構。

用於在 workflows 步驟執行期間標記檔案的金鑰/值對。

目錄

Name

步驟的名稱，用作識別符。

類型：字串

長度限制：長度下限為 0。長度上限為 30。

模式：`[\w-]*`

必要：否

SourceFileLocation

指定要使用哪個檔案作為 workflow 步驟的輸入：上一個步驟的輸出，或 workflow 的原始上傳檔案。

- 若要使用上一個檔案作為輸入，請輸入 `${previous.file}`。在此情況下，此 workflow 步驟會使用上一個 workflow 步驟的輸出檔案作為輸入。這是預設值。
- 若要使用原始上傳的檔案位置作為此步驟的輸入，請輸入 `${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/值對的陣列。

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

如需在其中一種語言特定 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

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

Transfer 伺服器執行個體的系統指派唯一識別碼。

類型：字串

長度限制條件：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

對應工作流程之工作階段的系統指派唯一識別碼。

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

如需在其中一種語言特定 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

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)。當伺服器工作階段在檔案仍在上傳時中斷連線時，會發生部分上傳。

目錄

ExecutionRole

包含 Transfer 可以承擔的 S3EFS、和 Lambda 操作的必要許可，以便所有工作流程步驟都可以在所需資源上操作

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

長度限制條件：固定長度為 19。

模式：w-([a-z0-9]{17})

必要：是

另請參閱

如需在其中一種語言特定的 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)

- [AWS SDK 適用於 Ruby V3](#)

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。

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":[]}'
```

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

如需在其中一種語言特定 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

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

叫用 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訊。

包含下列值：

- 描述性名稱
- 要解密來源檔案的 Amazon S3 或 Amazon Elastic File System (Amazon EFS) 位置。
- 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。
- 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

如需在其中一種語言特定 API 中使用此功能的詳細資訊 AWS SDKs，請參閱下列內容：

- [AWS SDK 適用於 C++](#)
- [AWS SDK for Go](#)
- [AWS SDK 適用於 Java V2](#)
- [AWS SDK 適用於 Ruby V3](#)

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 開發應用程式時，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 所有其他列出的標題都是 HTTP 交易中使用的常見標題。

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。 <pre>Content-Type: application/x-amz-json-1.1</pre>
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。 <pre>Host: transfer. <i>region</i>.amazonaws.com</pre>
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，格式為年月日「海里曼斯」Z。 <pre>x-amz-date: <i>YYYYMMDD'T'HHMMSS'Z'</i></pre>

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。 <pre>x-amz-target: TransferService. <i>operationName</i></pre> 您可以從 API 清單中找到 operationName 值 (例如 <code>ListServers</code>)。 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串。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，則必須納入安全字串。

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 1 月 16 日

變更	描述	日期
與 Amazon 整合 EventBridge	AWS Transfer Family 現在會自動將事件發佈至 Amazon EventBridge 以進行所有檔案傳輸操作。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
新增新的安全政策	AWS Transfer Family 已新增新的FIPS和非FIPS安全政策。此外，指派給伺服器的預設安全政策始終是最新的安全政策。如需詳細資訊，請參閱 的安全政策 AWS Transfer Family 。	2024 年 2 月 5 日
支援SFTP連接器和 的靜態 IP 地址 AS2	Transfer Family 現在提供 SFTP連接器 和 的靜態 IP 地址AS2。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，我們會為來自AS2伺服器的非同步MDN回應引入靜態 IP 地址。	2024 年 1 月 16 日
使用者指南已重新組織，以更接近最新版本的 AWS Transfer Family。	Transfer Family 自指南發起以來已新增多個功能，因此需要重組指南。	2024 年 1 月 3 日

變更	描述	日期
邏輯目錄映射增強功能 Amazon S3 列出效能最佳化	Transfer Family 現在支援高達 2.1 MB 的邏輯目錄映射。您現在可以宣告使用者映射是否是檔案。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，您現在可以最佳化列出 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 伺服器啟用替代非標準連接埠。如需詳細資訊，請參閱 在虛擬私有雲端中建立伺服器 。	2023 年 11 月 17 日
支援SFTP連接器	SFTP 連接器可擴展 的功能 AWS Transfer Family ，以與雲端和內部部署中的遠端伺服器通訊。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
支援AS2基本身分驗證	Transfer Family 現在支援針對使用適用性聲明 2（AS2）通訊協定的伺服器使用基本身分驗證。如需詳細資訊，請參閱 AS2 連接器的基本身分驗證 。	2023 年 6 月 30 日

變更	描述	日期
支援結構化JSON記錄	Transfer Family 現在支援將結構化JSON日誌交付至 Amazon CloudWatch、將日誌蒸汽分組為自訂日誌群組，以及跨通訊協定執行常見日誌查詢。如需詳細資訊，請參閱 的 Amazon CloudWatch 記錄 AWS Transfer Family 。	2023 年 6 月 24 日
支援多種身分驗證方法	Transfer Family 支援使用密碼、公有/私有金鑰對或兩者進行身分驗證。這適用於使用 SFTP通訊協定和自訂身分提供者的伺服器。如需詳細資訊，請參閱 建立已啟用 SFTP的伺服器 。	2023 年 5 月 17 日
透過使用工作流程傳輸系列程序的檔案支援 Pretty Good Privacy (PGP) 解密	Transfer Family 內建支援 Pretty Good Privacy (PGP) 解密。您可以在透過 SFTP、FTPS或上傳至 FTP Amazon Simple Storage Service (Amazon S3) 或 Amazon Elastic File System (Amazon) 的檔案上使用 PGP解密EFS。如需詳細資訊，請參閱 產生和管理PGP金鑰 和 在工作流程中使用PGP解密 。	2022 年 12 月 21 日
完全受管支援具有 Transfer Family 伺服器的適用性聲明 2 (AS2) 檔案傳輸通訊協定	您可以使用AS2通訊協定建立伺服器，以傳送和接收來自 AWS 環境內部或外部的交易合作夥伴的資訊。如需詳細資訊，請參閱 設定 AS2 。	2022 年 7 月 25 日

變更	描述	日期
建立伺服器時支援顯示橫幅	您可以在建立伺服器時新增自訂訊息。您可以顯示驗證前訊息（所有通訊協定）和驗證後訊息（適用於 FTP 和 FTPS 伺服器）。如需詳細資訊，請參閱 「建立已啟用 SFTP 的伺服器」 、 「建立已啟用 FTPS 的伺服器」 或 「建立已啟用 FTP 的伺服器」 。	2022 年 2 月 17 日
支援 AWS Lambda 作為身分提供者	您現在可以透過 AWS Lambda 其 Transfer Family 伺服器使用連線至自訂身分提供者。先前，您必須提供 Amazon API Gateway URL 才能整合自訂身分提供者。如需詳細資訊，請參閱 使用 AWS Lambda 整合您的身分提供者 。	2021 年 11 月 16 日
支援受管檔案傳輸工作流程	受管檔案傳輸工作流程可針對您目前手動執行的常見任務，提供上傳後處理摘要。如需詳細資訊，請參閱 AWS Transfer Family 受管工作流程 。	2021 年 9 月 2 日
的支援 AWS Directory Service for Microsoft Active Directory	除了服務受管和自訂身分提供者之外，您現在可以使用 AWS Directory Service for Microsoft Active Directory 管理使用者存取以進行身分驗證和授權。如需詳細資訊，請參閱 使用 AWS Directory Service 身分提供者 。	2021 年 5 月 24 日

變更	描述	日期
新的 AWS 區域	AWS Transfer Family 現在可在非洲（開普敦）區域使用。如需 Transfer Family 端點的詳細資訊，請參閱 AWS Transfer Family 中的端點和配額 AWS 一般參考 。	2021 年 2 月 24 日
新的 AWS 區域	AWS Transfer Family 現在可在亞太區域（香港）和中東（巴林）區域使用。如需 Transfer Family 端點的詳細資訊，請參閱 AWS Transfer Family 中的端點和配額 AWS 一般參考 。	2021 年 2 月 17 日
支援 Amazon EFS 作為資料存放區	Transfer Family 現在支援傳入和傳出 Amazon Elastic File System（Amazon）的檔案傳輸EFS。Amazon EFS 是簡單、可擴展、完全受管的彈性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 6 日
的支援 AWS WAF	Transfer Family 現在支援 AWS WAF，這是一個 Web 應用程式防火牆，可協助保護 Web 應用程式和API操作免受攻擊。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
支援虛擬私有雲端（VPC）中的多個安全群組	您現在可以將多個安全群組連接到中的伺服器VPC。如需詳細資訊，請參閱 在虛擬私有雲端中建立伺服器 。	2020 年 10 月 15 日

變更	描述	日期
新的 AWS 區域	Transfer Family 現在可在 AWS GovCloud (US) 區域中使用。如需 AWS GovCloud (US) 區域 Transfer Family 端點的詳細資訊，請參閱 AWS Transfer Family 中的端點和配額 AWS 一般參考。如需在 AWS GovCloud (US) 區域中使用 Transfer Family 的相關資訊，請參閱 使用者指南 AWS Transfer Family 中的。AWS GovCloud (US)	2020 年 9 月 30 日
具有支援密碼編譯演算法的安全政策現在可以連接至您的伺服器	您現在可以將包含一組支援密碼編譯演算法的安全政策連接至您的伺服器。如需詳細資訊，請參閱 的安全政策 AWS Transfer Family 。	2020 年 8 月 12 日
支援聯邦資訊處理標準 (FIPS) 端點	FIPS 啟用的端點現在可在北美中使用 AWS 區域。如需可用區域的資訊，請參閱中的 AWS Transfer Family 端點和配額 AWS 一般參考。若要 FIPS 為 SFTP 啟用的伺服器端點啟用，請參閱 建立已啟用 SFTP 的伺服器 。若要 FIPS 為 FTPS 啟用的伺服器端點啟用，請參閱 建立已啟用 FTPS 的伺服器 。若要 FIPS 為 FTP 啟用的伺服器端點啟用，請參閱 建立已啟用 FTP 的伺服器 。	2020 年 8 月 12 日

變更	描述	日期
使用者名稱字元長度增加和其他允許的字元	使用者名稱現在可以包含於符號 (@) 和句點 (.) ，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
支援自動建立 Amazon CloudWatch 記錄 AWS Identity and Access Management (IAM) 角色	Transfer Family 現在支援自動建立 CloudWatch 記錄 IAM 角色，以檢視最終使用者活動。如需詳細資訊，請參閱「 建立已啟用 SFTP 的伺服器 」、「 建立已啟用 FTPS 的伺服器 」或「 建立已啟用 FTP 的伺服器 」。	2020 年 7 月 30 日
AWS Transfer Family 現在支援來源 IP 做為授權的因素。	Transfer Family 新增了使用最終使用者的來源 IP 地址作為授權因素的支援，可讓您在透過安全檔案傳輸通訊協定 (SFTP) 、透過 SSL (FTPS) 進行檔案傳輸通訊協定或檔案傳輸通訊協定 () 授權存取時套用額外的安全層 FTP。如需詳細資訊，請參閱 使用自訂身分提供者 。	2020 年 6 月 9 日

變更	描述	日期
AWS 的轉移現在SFTP為 AWS Transfer Family，並新增對 FTP和 的支援FTPS。	您現在可以針對使用者的檔案傳輸使用兩個額外的通訊協定：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 SSL（FTPS）支援之外 AWS，使用者可以FTP在中移動、執行、保護和整合（SFTP）和純文字FTP型工作流程。	2020 年 4 月 23 日
支援虛擬私有雲端（VPC）安全群組和彈性 IP 地址	您現在可以使用安全群組建立傳入 IP 地址的允許清單，為伺服器提供額外的安全層。您也可以將彈性 IP 地址與伺服器的端點建立關聯。透過這樣做，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 在虛擬私有雲端中建立伺服器 。	2020 年 1 月 10 日
支援在 中作業 VPC	您現在可以在 中建立伺服器 VPC。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，而不必透過公有網際網路。如需詳細資訊，請參閱 在虛擬私有雲端中建立伺服器 。	2019 年 3 月 27 日
第一個版本的 AWS Transfer Family 已發行。	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。