



使用者指南

AWS Transfer Family



AWS Transfer Family: 使用者指南

Copyright © 2026 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
先決條件	8
區域、端點和配額	8
註冊 AWS	8
設定儲存	9
設定 Amazon S3 儲存貯體	10
設定 Amazon EFS 檔案系統	14
建立 IAM 角色和政策	17
建立使用者角色	18
工作階段政策的運作方式	21
讀取/寫入存取政策範例	23
Transfer Family 教學課程	27
開始使用伺服器端點	28
先決條件	28
步驟 1：登入 AWS Transfer Family 主控台	29
步驟 2：建立啟用 SFTP 的伺服器	29
步驟 3：新增服務受管使用者	30
步驟 4：使用用戶端傳輸檔案	31
建立解密工作流程	33
步驟 1：設定執行角色	33
步驟 2：建立受管工作流程	35
步驟 3：將工作流程新增至伺服器並建立使用者	36
步驟 4：建立 PGP 金鑰對	37
步驟 5：將 PGP 私有金鑰存放在 AWS Secrets Manager	38
步驟 6：加密檔案	39
步驟 7：執行工作流程並檢視結果	39
建立和使用 SFTP 連接器	40
連接器輸出類型	41
步驟 1：建立必要的支援資源	42
步驟 2：建立和測試 SFTP 連接器	48
步驟 3：使用 SFTP 連接器傳送和擷取檔案	53
建立 Transfer Family 伺服器以用作遠端 SFTP 伺服器的程序	57

使用自訂身分提供者	60
先決條件	60
步驟 1：建立 CloudFormation 堆疊	60
步驟 2：檢查伺服器的 API Gateway 方法組態	61
步驟 3：檢視 Transfer Family 伺服器詳細資訊	62
步驟 4：測試您的使用者是否可以連線到伺服器	64
步驟 5：測試 SFTP 連線和檔案傳輸	64
步驟 6：限制對儲存貯體的存取	65
如果使用 Amazon EFS，請更新 Lambda	67
設定 AS2 組態	68
步驟 1：建立 AS2 的憑證	69
步驟 2：將憑證匯入為 Transfer Family 憑證資源	72
步驟 3：為您和您的交易合作夥伴建立設定檔	74
步驟 4：建立使用 AS2 通訊協定的 Transfer Family 伺服器	74
步驟 5：建立您與合作夥伴之間的協議	77
步驟 6：在您和合作夥伴之間建立連接器	79
步驟 7：使用 Transfer 系列測試透過 AS2 交換檔案	80
設定基本 Web 應用程式	82
先決條件	82
步驟 1：建立必要的支援資源	82
步驟 2：建立 Transfer Family Web 應用程式	83
步驟 3：設定儲存貯體的跨來源資源共用 (CORS)	84
步驟 4：將使用者新增至 Transfer Family Web 應用程式	85
步驟 5：在 Amazon S3 中註冊位置並建立存取授權	86
步驟 6：以使用者身分存取 Transfer Family Web 應用程式	88
後續步驟	89
將 Okta 整合為 Web 應用程式的身分提供者	90
設定具有選擇性多儲存貯體存取權的 Web 應用程式	92
先決條件	92
步驟 1：建立 Transfer Family Web 應用程式	93
步驟 2：設定 S3 存取的 IAM 角色	93
步驟 3：設定 S3 存取授權	96
步驟 4：註冊 S3 儲存貯體位置	96
步驟 5：建立存取授權	96
步驟 6：設定 S3 儲存貯體的 CORS 政策	97
步驟 7：測試組態	98

結論	98
適用於 SFTP、FTPS、FTP 的 Transfer 系列	99
身分提供者選項	99
AWS Transfer Family 端點類型矩陣	101
設定 Transfer Family 伺服器端點	104
建立啟用 SFTP 的伺服器	105
建立啟用 FTPS 的伺服器	112
建立啟用 FTP 的伺服器	120
在 VPC 中建立伺服器	127
使用自訂主機名稱	148
FTP/FTPS NLB 考量事項	152
透過伺服器端點傳輸檔案	152
可用的 SFTP/FTPS/FTP 命令	155
尋找您的 Amazon VPC 端點	156
避免 setstat 錯誤	158
使用 OpenSSH	32
使用 WinSCP	160
使用 Cyberduck	31
使用 FileZilla	163
使用 Perl 用戶端	164
使用 LFTP	164
上傳後處理	164
SFTP 訊息	165
管理使用者	167
Amazon EFS 與 Amazon S3	168
邏輯目錄	168
Active Directory 群組配額	169
服務受管使用者	170
自訂身分提供者	178
MS AD 的目錄服務	211
Entra ID 的目錄服務	221
使用邏輯目錄	228
了解 chroot 和目錄結構	228
使用邏輯目錄的規則	229
實作邏輯目錄	230
設定邏輯目錄範例	233

設定 Amazon EFS 的邏輯目錄	235
自訂 AWS Lambda 回應	235
存取 FSx for NetApp ONTAP 檔案系統	236
概觀	237
先決條件	237
FSx 儲存如何與 Transfer 系列搭配使用	238
為 FSx 建立 S3 存取點	239
搭配 FSx 使用 S3 存取點別名	241
設定 FSx 儲存的 Transfer 系列	243
管理 FSx 儲存體的使用者	244
設定檔案傳輸用戶端	246
對 FSx 儲存體進行故障診斷	247
Transfer Family Web 應用程式	249
AWS 區域 適用於 Transfer Family Web 應用程式	249
AWS Transfer Family Web 應用程式的瀏覽器相容性	250
如何建立 Transfer Family Web 應用程式	250
設定您的身分提供者	252
設定 IAM 角色	254
設定 Transfer Family Web 應用程式	256
建立 Transfer Family Web 應用程式	257
IP 定址	258
在 VPC 中建立 Transfer Family Web 應用程式	259
建立 Transfer Family Web 應用程式	260
建立後步驟	261
跨來源資源共用 (CORS) 政策	261
限制特定 VPC 端點的存取	263
將使用者或群組指派或新增至 Transfer Family Web 應用程式	263
為您的儲存貯體設定跨來源資源共用 (CORS)	267
設定 Amazon S3 存取授權	269
使用自訂 URL	274
記錄 Transfer Family Web 應用程式	277
啟用 Amazon S3 資料事件	277
身分驗證日誌範例	280
檢視日誌項目	287
對 Web 應用程式進行故障診斷	287
故障診斷網路錯誤	288

對未顯示的已設定儲存貯體進行故障診斷	288
對自訂 URL 錯誤進行故障診斷	289
對其他錯誤進行故障診斷	289
Web 應用程式中出現重複的 S3 儲存貯體	290
最終使用者說明	290
Web 應用程式配額	291
IAM Identity Center 使用者	291
第三方最終使用者	292
Transfer Family 最終使用者介面	293
可用動作	293
SFTP 連接器	296
建立 SFTP 連接器	296
選擇 SFTP 連接器輸出類型	297
選擇 IP 定址模式	298
將憑證儲存至 Secrets Manager 中	299
使用服務管理的輸出建立 SFTP 連接器	300
使用 VPC 型輸出建立 SFTP 連接器	310
測試 SFTP 連接器	320
VPC 連線	321
使用 SFTP 連接器	322
傳輸檔案	322
列出遠端目錄的內容	324
移動和刪除遠端伺服器上的檔案	326
監控 SFTP 連接器	327
使用連接器 API 查詢檔案傳輸請求的狀態	328
在 Amazon EventBridge 中檢視 SFTP 連接器事件	328
在 Amazon CloudWatch 中檢視 SFTP 連接器日誌	328
監控 VPC 輸出類型連接器	328
管理 SFTP 連接器	330
更新 SFTP 連接器	330
檢視 SFTP 連接器詳細資訊	331
SFTP 連接器的配額	332
SFTP 連接器的配額	332
擴展 SFTP 連接器	334
參考架構	334
部落格文章	335

研討會	335
解決方案	335
VPC 參考架構	335
AS2 的 Transfer 系列	338
AS2 使用案例	339
AS2 CloudFormation 範本	342
自訂 AS2 範本	343
測試您的 AS2 部署	343
AS2 範本部署的最佳實務	344
設定 AS2	344
AS2 組態	345
AS2 配額	347
AS2 功能	350
管理 AS2 憑證	351
匯入 AS2 憑證	352
AS2 憑證輪換	353
建立 AS2 設定檔	355
建立 AS2 伺服器	356
使用 Transfer Family 主控台建立 AS2 伺服器	356
使用範本建立 AS2 伺服器	359
建立 AS2 協議	362
設定 AS2 連接器	363
建立 AS2 連接器	364
AS2 連接器演算法	366
AS2 連接器的基本身分驗證	367
啟用 AS2 連接器的基本身分驗證	368
檢視連接器詳細資訊	371
傳輸 AS2 訊息	373
接收 AS2 訊息	374
設定 AS2 的 HTTPS	375
使用 AS2 連接器傳輸檔案	380
檔案名稱和位置	382
狀態碼	385
範例 JSON 檔案	385
AS2 的自訂 HTTP 標頭	387
範本概觀	388

運作方式	388
主要功能	388
實作詳細資訊	389
部署和使用	390
監控 AS2	391
AS2 狀態碼	392
AS2 錯誤代碼	393
憑證過期監控	401
DaysUntilExpiry 指標	401
憑證監控的最佳實務	402
警示組態範例	402
管理檔案處理工作流程	404
建立工作流程	406
設定和執行工作流程	407
檢視工作流程詳細資訊	409
使用預先定義的步驟	412
複製檔案	412
解密檔案	417
標籤檔案	423
刪除檔案	424
工作流程的命名變數	425
範例標籤和刪除工作流程	425
使用自訂檔案處理步驟	430
連續使用多個 Lambda 函數	431
在自訂處理之後存取檔案	432
檔案上傳 AWS Lambda 時傳送至 的範例事件	433
自訂工作流程步驟的範例 Lambda 函數	434
自訂步驟的 IAM 許可	435
工作流程的 IAM 政策	435
工作流程信任關係	437
範例執行角色：解密、複製和標記	437
範例執行角色：執行 函數並刪除	439
工作流程的例外狀況處理	440
監控工作流程執行	441
工作流程的 CloudWatch 記錄	441
工作流程的 CloudWatch 指標	444

從範本建立工作流程	444
從 Transfer Family 伺服器移除工作流程	448
限制	449
管理伺服器	451
檢視伺服器清單	451
刪除伺服器	451
檢視 SFTP 伺服器詳細資訊	453
檢視 AS2 伺服器詳細資訊	454
IPv6 支援	455
IPv6 限制	456
設定伺服器的 IPv6	456
將 ALB 用於雙堆疊 AS2 公有伺服器	457
編輯伺服器詳細資訊	458
編輯檔案傳輸通訊協定	461
編輯伺服器端點	463
編輯記錄	464
編輯安全政策	465
變更受管工作流程	466
變更伺服器的顯示橫幅	467
將您的伺服器置於線上或離線狀態	467
編輯身分提供者組態	468
變更為服務受管身分提供者	469
變更為 AWS Directory Service	469
變更為自訂身分提供者	469
身分提供者轉換期間的使用者保留	473
變更身分提供者時的重要考量	474
管理伺服器主機金鑰	474
何時匯入主機金鑰	475
新增額外的伺服器主機金鑰	476
刪除伺服器主機金鑰	477
輪換伺服器主機金鑰	478
其他伺服器主機金鑰資訊	479
在主控台中監控用量	480
管理存取控制	486
建立 S3 儲存貯體存取政策	486
建立工作階段政策	488

工作階段政策範例	489
工作階段政策的巢狀取代	491
動態許可管理	492
了解 Transfer Family 許可架構	492
許可管理的兩種方法	492
實作工作階段政策	493
依使用者類型實作	494
範例：使用工作階段政策簡化角色管理	494
CloudTrail 日誌記錄	497
啟用 CloudTrail 記錄	498
啟用 Amazon S3 資料事件	499
建立伺服器的範例日誌項目	499
資料存取日誌	501
成功存取資料的範例日誌項目	501
常見的資料存取操作	503
CloudWatch 記錄功能	504
Transfer Family 的 CloudWatch 記錄類型	504
建立伺服器的記錄	506
建立伺服器的記錄	508
更新伺服器的記錄	509
檢視伺服器組態	512
管理工作流程的記錄	514
設定 CloudWatch 的角色	517
檢視 Transfer Family 日誌串流	519
建立 Amazon CloudWatch 警示	522
記錄對 S3 存取日誌的 S3 API 呼叫	523
限制混淆代理人問題的範例	523
Transfer 系列適用的 CloudWatch 日誌結構	525
Transfer Family 的 JSON 結構化日誌	525
Transfer Family 的舊版日誌	528
CloudWatch 日誌項目範例	531
轉移工作階段日誌項目範例	531
SFTP 連接器的範例日誌項目	533
VPC Lattice 連接器的範例日誌項目	535
金鑰交換演算法失敗的範例日誌項目	536
使用 CloudWatch 指標	536

Transfer 系列維度	540
使用者通知	540
CloudWatch 查詢	541
使用 管理事件 EventBridge	544
Transfer Family 事件	544
SFTP、FTPS 和 FTP 伺服器事件	545
SFTP 連接器事件	547
AS2 事件	548
傳送 Transfer Family 事件	549
建立事件模式	550
測試事件 Transfer Family 的事件模式	551
許可	551
其他資源	551
事件詳細參照	552
伺服器事件	552
連接器事件	559
AS2 事件	566
安全	573
VPC 連線安全性優點	574
VPC Lattice 安全模型	574
VPC 連線的安全最佳實務	574
伺服器的安全政策	575
密碼編譯演算法	576
安全政策詳細資訊	587
SFTP 連接器的安全政策	605
密碼編譯演算法	605
SFTP 連接器安全政策詳細資訊	605
後量子安全政策	608
關於 SSH 中的後量子混合金鑰交換	609
使用方式	609
測試方式	610
資料保護	613
Transfer 系列中的資料加密	614
靜態加密	615
金鑰管理	616
演算法概觀	616

SSH 身分驗證	617
PGP 演算法	618
產生 SSH 金鑰	619
輪換 SSH 金鑰	624
產生 PGP 金鑰	627
管理 PGP 金鑰	628
支援的 PGP 用戶端	631
身分與存取管理	633
目標對象	633
使用身分驗證	633
使用政策管理存取權	635
AWS Transfer Family 如何使用 IAM	636
身分型政策範例	640
標籤型政策範例	642
對 身分與存取進行疑難排解	645
IAM 條件鍵	647
法規遵循驗證	649
恢復能力	649
APIs 的 VPC 端點	650
使用 VPC 端點政策控制存取	650
建立 VPC 端點	651
基礎設施安全性	652
NLB 和 NAT 考量事項	652
VPC 連線基礎設施安全性	653
Web 應用程式防火牆	654
預防跨服務混淆代理人	655
Transfer Family 使用者角色	656
Transfer 系列工作流程角色	658
Transfer 系列連接器角色	659
Transfer 系列記錄/調用角色	661
AWS 受管政策	662
AWSTransferConsoleFullAccess	663
AWSTransferFullAccess	663
AWSTransferLoggingAccess	663
AWSTransferReadOnlyAccess	663
政策更新	663

Transfer 系列 Terraform 模組	664
SFTP 伺服器	664
SFTP 連接器	664
AS2	664
B2B 資料交換	665
對 Transfer 系列進行故障診斷	666
驗證問題	666
身分驗證失敗 - SSH/SFTP	667
Managed AD 不相符領域問題	667
超過 Active Directory 群組限制	668
其他身分驗證問題	668
對 Amazon API Gateway 問題進行故障診斷	669
對測試您的身分提供者進行故障診斷	670
Web 應用程式中的重複 Amazon S3 儲存貯體	290
SFTP 連接器問題	671
針對為您的 SFTP 連接器新增受信任主機金鑰進行故障診斷	672
金鑰交涉失敗	672
SFTP 連接器限流	673
最佳化 SFTP 連接器效能	673
故障診斷 VPC 連線問題	674
其他 SFTP 連接器問題	677
SFTP 連線問題	677
疑難排解 SFTP 連線問題	677
疑難排解 SFTP 用戶端問題	678
對檔案上傳問題進行故障診斷	678
故障診斷 VPC 輸出類型 SFTP 連接器問題	679
自訂身分提供者問題	681
故障診斷 API Gateway 整合錯誤	681
故障診斷 Lambda 函數逾時	683
對一致的 Lambda 逾時問題進行故障診斷	683
故障診斷例外KeyError狀況	684
工作流程問題	684
對受管工作流程問題進行故障診斷	684
對工作流程解密問題進行故障診斷	687
EFS 問題	690
對 Amazon EFS 問題進行故障診斷	691

儲存和加密問題	693
對加密 Amazon S3 儲存貯體的政策進行故障診斷	693
對ResourceNotFound例外狀況進行故障診斷	694
監控和提醒問題	694
對遺失或不完整的 CloudWatch 指標進行故障診斷	694
故障診斷遺失的 EventBridge 事件	695
跨區域轉移問題	696
對跨區域傳輸許可問題進行故障診斷	697
對跨區域傳輸效能問題進行故障診斷	698
Terraform 部署問題	699
故障診斷 Terraform 資源建立失敗	699
故障診斷 Terraform 狀態管理問題	700
WAF 整合問題	701
對封鎖合法流量的 WAF 進行故障診斷	701
對與自訂身分提供者的 WAF 整合進行故障診斷	702
服務受管使用者問題	702
對服務受管使用者進行故障診斷	703
AS2 問題	704
疑難排解 AS2 問題	704
AS2 憑證問題	704
AS2 MDN 接收問題	705
憑證過期監控問題	705
API 參考	707
提出 API 請求	708
Transfer Family 必要請求標頭	708
Transfer Family 請求輸入和簽署	709
錯誤回應	709
可用程式庫	711
身分提供者	712
慣例	713
ID 格式	713
ARN 格式	713
DNS 和端點	714
API 端點	714
伺服器端點	715
文件歷史紀錄	716

..... dccxxvi

什麼是 AWS Transfer Family ?

AWS Transfer Family 是一種安全傳輸服務，可讓您將檔案傳入和傳出 AWS 儲存服務。Transfer Family 是 AWS 雲端平台的一部分。AWS Transfer Family 提供透過 SFTP、AS2、FTPS、FTP 和 Web 瀏覽器型傳輸直接傳入和傳出 AWS 儲存服務的全受管支援。您可以無縫遷移、自動化和監控檔案傳輸工作流程，方法是維護現有的用戶端組態以進行身分驗證、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[開始使用 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 支援在下列 AWS 儲存服務之間傳輸資料。

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

AWS Transfer Family 支援透過下列通訊協定傳輸資料：

- 安全檔案傳輸通訊協定 (SFTP)：第 3 版

官方 IETF 文件在這裡：[SSH 檔案傳輸通訊協定 draft-ietf-secsh-filexfer-02.txt](#)。

- 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)
- 瀏覽器型傳輸

Note

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

檔案傳輸通訊協定用於金融服務、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的遷移 AWS。

以下是搭配 Amazon S3 使用 Transfer Family 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。

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

- 資料分佈
- 供應鏈
- 內容管理
- Web 服務應用程式

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

- 具有合規要求的工作流程，這些工作流程依賴於在通訊協定中內建資料保護和安全性功能
- 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

以下是使用 Transfer Family Web 應用程式的一些常見使用案例：

- 簡化對 Amazon S3 中資料的存取，讓更多且多樣化的業務使用者
- 人力資源的集中式資料存取管理
- 透過受管界面視覺化 Amazon S3 Access Grants

使用 Transfer Family，您可以在 AWS（或受管檔案傳輸 Web 介面）中存取已啟用檔案傳輸通訊協定的伺服器，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。對於伺服器，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。

對於 Transfer Family Web 應用程式，判斷您的組態設定並套用選用的自訂。完成此操作後，您的使用者可以登入並直接在 Amazon S3 之間傳輸資料。

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。
- 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 做為資料存放區，您可以取得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 可隨需擴展至 PB 級，而不會中斷應用程式，並可隨著您新增和移除檔案而自動擴展及縮減。這有助於消除佈建和管理容量以適應成長的需求。
- 全受管的無伺服器檔案傳輸工作流程服務，可讓您輕鬆地設定、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。

在下列各節中，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說明、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，請參閱下列內容：

- [AWS Transfer Family 運作方式](#)
- [先決條件](#)
- [AWS Transfer Family 伺服器端點入門](#)
- [Transfer Family Web 應用程式](#)

AWS Transfer Family 運作方式

AWS Transfer Family 是一項全受管 AWS 服務，可讓您透過下列通訊協定或 Web 瀏覽器，將檔案傳入和傳出 Amazon Simple Storage Service (Amazon S3) 儲存體或 Amazon Elastic File System (Amazon EFS) 檔案系統：

- 安全檔案傳輸通訊協定 (SFTP)：第 3 版

官方 IETF 文件在這裡：[SSH 檔案傳輸通訊協定 draft-ietf-secsh-filexfer-02.txt](#)。

- 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)
- 瀏覽器型傳輸

AWS Transfer Family 支援最多 3 個可用區域，並由自動擴展、備援機群支援您的連線和傳輸請求。如需如何使用以延遲為基礎的路由來建置更高備援並將網路延遲降至最低的範例，請參閱部落格文章 [將網路延遲與 SFTP 伺服器的 AWS 傳輸降至最低](#)。

Transfer Family Managed File Transfer Workflows (MFTW) 是一種全受管的無伺服器檔案傳輸工作流程服務，可讓您輕鬆地設定、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 自動化各種處理步驟，例如複製、標記、掃描、篩選、壓縮/解壓縮，以及加密/解密使用 Transfer Family 傳輸的資料。這可為追蹤和可稽核性提供端對端可見性。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：

- [OpenSSH](#) – 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。

AWS 提供下列 Transfer Family 研討會。

- 建置檔案傳輸解決方案，以利用 AWS Transfer Family 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。
- 在啟用 AS2 的情況下建置 Transfer Family 端點，以及 Transfer Family AS2 連接器 您可以 [在這裡](#) 檢視此研討會的詳細資訊。
- 建置解決方案，提供規範性指引和實作實驗室，了解如何在上建置可擴展且安全的檔案傳輸架構，AWS 而不需要修改現有的應用程式或管理伺服器基礎設施。您可以 [在這裡](#) 檢視此研討會的詳細資訊。

與 Transfer Family 相關的部落格文章

下表列出包含 Transfer Family 客戶實用資訊的部落格文章。資料表依反向時間順序排列，因此最近的文章位於資料表的開頭。

部落格文章標題和連結	Date
將 Okta 部署為的自訂身分提供者 AWS Transfer Family	2025 年 8 月 11 日

部落格文章標題和連結	Date
使用 自動化paper-to-electronic醫療保健宣告處理 AWS	2025 年 5 月 29 日
如何使用 AWS Transfer Family 和 GuardDuty 保護惡意軟體	2025 年 4 月 30 日
FICO 如何使用 將檔案傳輸與 ETL 自動化進行現代化 AWS Transfer Family	2025 年 4 月 24 日
宣布適用於全受管 Amazon S3 檔案傳輸的 AWS Transfer Family Web 應用程式	2024 年 12 月 1 日
改善伺服器安全性的 AWS Transfer Family 六個秘訣	2024 年 9 月 24 日
使用 的自訂身分提供者簡化 Active Directory 身分驗證 AWS Transfer Family	2024 年 8 月 12 日
使用 AWS Transfer Family SFTP 連接器和 PGP 加密來架構安全且合規的受管檔案傳輸	2024 年 5 月 16 日
透過 AWS Transfer Family 和 Amazon S3 使用 Amazon Cognito 做為身分提供者 Amazon S3	2024 年 5 月 14 日
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 PGP 和 加密和解密檔案 AWS Transfer Family	2023 年 6 月 21 日
AWS Transfer Family 使用 Azure Active Directory 和 向 驗證 AWS Lambda	2022 年 12 月 15 日

部落格文章標題和連結	Date
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
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
AWS Transfer Family 使用 啟用密碼身分驗證 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 將 Amazon EFS 用於	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

部落格文章標題和連結	Date
使用 SFTP 伺服器的 AWS 傳輸將網路延遲降至最低	2020 年 2 月 19 日
SFTP 伺服器的提升和轉移遷移至 AWS	2020 年 2 月 12 日
使用 chroot 和邏輯目錄簡化 AWS SFTP 結構	2019 年 9 月 26 日
透過 使用 Okta 做為身分提供者 AWS Transfer Family	2019 年 5 月 30 日

先決條件

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。此信任關係可讓 Transfer Family 擔任 IAM 角色來存取您的儲存貯體，以便為使用者的檔案傳輸請求提供服務。

如需 AWS Transfer Family 伺服器 IPv6 支援的相關資訊，請參閱管理伺服器章節[Transfer Family 伺服器的 IPv6 支援](#)中的。

主題

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

Transfer Family 伺服器支援的 AWS 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 AWS 帳戶的服務資源或操作的最大數量。在本指南中，您可以在 [AS2 配額](#) 和 [中找到配額](#)[SFTP 連接器的配額](#)。

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。

對於 Transfer Family Web 應用程式，支援的區域會列在 [中 AWS 區域 適用於 Transfer Family Web 應用程式](#)。如需與 Transfer Family Web 應用程式相關的配額，請參閱 [Web 應用程式配額](#)。

註冊 AWS

當您註冊 Amazon Web Services (AWS) 時，AWS 您的帳戶會自動註冊所有服務 AWS，包括 AWS Transfer Family。您只需支付實際使用服務的費用。

如果您已經有 AWS 帳戶，請跳到下一個任務。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，請完成下列步驟來建立一個。

註冊 AWS 帳戶

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

部分註冊程序需接收來電或簡訊，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，請將管理存取權指派給使用者，並且僅使用根使用者來執行[需要根使用者存取權的任務](#)。

如需有關定價和 AWS 定價計算工具 用來取得使用 Transfer Family 之成本預估的資訊，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 AWS Transfer Family 伺服器搭配使用的儲存體

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

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 系列設定 Amazon EFS 使用者](#)
 - [在 Amazon EFS 上設定 Transfer Family 使用者](#)
 - [建立 Amazon EFS 根使用者](#)
 - [支援的 Amazon EFS 命令](#)

設定 Amazon S3 儲存貯體

AWS Transfer Family 會存取您的 Amazon S3 儲存貯體來為使用者的傳輸請求提供服務，因此您需要提供 Amazon S3 儲存貯體，做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

您不需要使用位於相同 AWS 區域中的伺服器和 Amazon S3 儲存貯體，但我們建議這樣做作為最佳實務。

當您設定使用者時，您會為每個使用者指派一個 IAM 角色。此角色會決定他們對 Amazon S3 儲存貯體的存取層級。

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

Note

您可以使用 Amazon S3 物件鎖定，以防止物件在固定的時間長度內或無限期遭到覆寫。這與其他服務一樣適用於 Transfer Family。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共用資料集的精細存取。您可以在任何使用 S3 儲存貯體名稱的地方使用 S3 存取點別名。您可以在 Amazon S3 中為具有存取 Amazon S3 儲存貯體中共用資料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、第二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。若要實作上述的精細存取控制，您可以建立 S3 存取點，其中包含將非對稱存取權授予不同團隊的政策。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搭配 Transfer Family 伺服器使用 S3 存取點，請參閱[使用 AWS Transfer Family 和 Amazon S3 增強資料存取控制](#)部落格文章。

 Note

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

Amazon S3 HeadObject 行為

 Note

當您建立或更新 Transfer Family 伺服器時，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 中不是一級概念，而是以物件索引鍵為基礎。AWS Transfer Family 會以正斜線字元 (/) 分割物件的索引鍵，將最後一個元素視為檔案名稱，然後在相同路徑下將具有相同字首的檔案名稱分組在一起，來推斷目錄路徑。當您使用 `mkdir` 或使用 Amazon S3 主控台建立空目錄時，會建立零位元組物件來代表資料夾的路徑。這些物件的索引鍵結尾為正斜線。這些零位元組物件描述於 [Amazon S3 使用者指南中的使用資料夾在 Amazon S3 主控台中組織物件](#)。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 會為每個物件發出 HeadObject 請求（如需詳細資訊，請參閱 Amazon Simple Storage Service API 參考中的 [HeadObject](#)）。使用 Amazon S3 做為 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，您必須擁有 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，呼叫會失敗並出現存取遭拒的錯誤，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。

在這種情況下，您可以新增 AWS Identity and Access Management (IAM) 政策條件來授予存取權，該條件只會為結尾為斜線 (/) 的物件新增 GetObject 許可。此條件可防止對檔案的 GetObject 呼叫（因此無法讀取），但允許使用者列出和周遊資料夾。下列範例政策僅提供 Amazon S3 儲存貯體的寫入和清單存取權。若要使用此政策，請將 `amzn-s3-demo-bucket` 為儲存貯體的名稱。

 Note

若要解決 WinSCP 的上傳行為，請務必新增 `"arn:aws:s3:::amzn-s3-demo-bucket/*.filepart"` 列，如下列範例政策所列。這行可確保正確處理 `.filepart` 物件，以防止失敗。

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



```
    ]
  }
]
}
```

Note

此政策不允許使用者附加檔案。換句話說，獲指派此政策的使用者無法開啟檔案來新增內容或修改內容。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。此問題的建議解決方案是啟用最佳化目錄以減少延遲。

例如，假設您進入主目錄，而且您有 10,000 個子目錄。換句話說，Amazon 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。您可以在伺服器建立或更新程序期間設定其他詳細資訊畫面中設定此選項。這些程序會在 [設定 SFTP、FTPS 或 FTP 伺服器端點](#) 主題下詳細說明。

Note

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

如果您未或無法最佳化目錄，此問題的替代解決方案是刪除所有零位元組物件。注意下列事項：

- 空白目錄將不再存在。目錄只會因為其名稱位於物件的金鑰中而存在。
- 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。

最後，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)，為使用者的傳輸請求提供服務。因此，您必須提供 Amazon EFS 檔案系統，做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個帳戶中，則檔案系統政策必須為使用者角色提供明確許可。

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](#)。

- 當您設定使用者時，您會為每個使用者指派一個 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 AWS Transfer Family 和 Amazon EFS 如何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界面 (POSIX) 檔案許可模型來代表檔案擁有權。

在 POSIX 中，系統中的使用者分為三種不同的許可類別：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)：對共用的檔案和目錄需要相同存取權的一組使用者。
- 其他 (o)：所有其他可存取系統的使用者，但擁有者和群組成員除外。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）都與先前提到的三組許可相關聯。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 風格的系統上，會將使用者和群組對應到數字識別符，Amazon EFS 會利用這些識別符來表示檔案所有權。對於 Amazon EFS，物件由單一擁有者和單一群組擁有。當使用者嘗試存取檔案系統物件時，Amazon EFS 會利用這些對應的數字 ID 來檢查權限。

為 Transfer 系列設定 Amazon EFS 使用者

在設定 Amazon EFS 使用者之前，您可以執行下列其中一項操作：

- 您可以在 Amazon EFS 中建立使用者和設定其主資料夾。如需詳細資訊，請參閱 [在 Amazon EFS 上設定 Transfer Family 使用者](#)。
- 如果您願意新增根使用者，您可以 [建立 Amazon EFS 根使用者](#)。

Note

Transfer Family 伺服器不支援 Amazon EFS 存取點來設定 POSIX 許可。Transfer Family 使用者的 POSIX 設定檔（如上節所述）可讓您設定 POSIX 許可。這些許可是在使用者層級設定，以根據 UID、GID 和次要 GIDs 進行精細存取。

在 Amazon EFS 上設定 Transfer Family 使用者

Transfer Family 會將使用者映射到您指定的 UID/GID 和目錄。如果 UID/GID/directories 指派給使用者之前建立它們。EFS 有關建立 Amazon EFS 使用者的詳細資訊，請參閱《Amazon Amazon Elastic File System 使用者指南》中的 [在網路檔案系統 \(NFS\) 層級使用使用者、群組和許可](#)。

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

1. 使用 [PosixProfile](#) 欄位映射 Transfer Family 中使用者的 EFS UID 和 GID。
2. 如果您希望使用者在登入時在特定資料夾中啟動，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 EFS 互動的範例 Lambda 函數，請參閱 [在無伺服器應用程式中使用適用於 AWS Lambda 的 Amazon EFS](#)。

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 EFS 的邏輯目錄](#) 一節。

建立 Amazon EFS 根使用者

如果您的組織習慣透過 SFTP/FTPS 為使用者組態啟用根使用者存取權，您可以建立 UID 和 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，並為其他使用者指派 POSIX ID 擁有者。此選項的優點是不需要掛載 Amazon EFS 檔案系統。

執行中所述的步驟[新增 Amazon EFS 服務受管使用者](#)，並針對使用者 ID 和群組 ID，輸入 0（零）。

Tip

請勿讓此超級使用者帳戶存在超過必要的時間。或者，如果您確實保留根使用者帳戶，請確定您妥善保護根使用者帳戶。

支援的 Amazon EFS 命令

適用於的 Amazon EFS 支援下列命令 AWS Transfer Family。

- `cd`
- `ls/dir`
- `pwd`
- `put`
- `get`
- `rename`
- `chown`：只有根目錄（也就是 `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`：支援根群組或檔案擁有者，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

本主題說明可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。它也說明工作階段政策的運作方式，並提供範例使用者角色。

AWS Transfer Family 使用下列類型的角色：

- 使用者角色 – 允許服務受管使用者存取必要的 Transfer Family 資源。會在 Transfer Family 使用者 ARN 的內容中 AWS Transfer Family 擔任此角色。
- 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，存取角色會使用協議的 Amazon Resource Name (ARN)。對於傳出 AS2 傳輸，存取角色會使用連接器的 ARN。
- 調用角色 – 與 Amazon API Gateway 搭配使用，做為伺服器的自訂身分提供者。Transfer Family 會在 Transfer Family 伺服器 ARN 的內容中擔任此角色。
- 記錄角色 – 用於將項目記錄到 Amazon CloudWatch。Transfer Family 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 ARN 的內容中擔任此角色。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 ARN 的內容中擔任此角色。

除了這些角色之外，您也可以使用工作階段政策。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，這是一個有用的捷徑。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 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，您會對使用者存取做出許多決策。這些決策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，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。在此程序中，您會為使用者提供存取 Amazon S3 儲存貯體或 Amazon EFS 檔案系統的權限，該系統是檔案操作的目標或來源。若要執行此作業，請遵循下列高層級步驟，稍後會詳細進行說明：

建立使用者角色

1. 建立 IAM 政策 AWS Transfer Family。如 [為 建立 IAM 政策 AWS Transfer Family](#) 中所述。
2. 建立 IAM 角色並連接新的 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 [建立信任關係](#) 中所述。

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 <https://console.aws.amazon.com/iam/> 中開啟 IAM 主控台。
2. 在導覽窗格中，選擇 Policies (政策)，然後選擇 Create policy (建立政策)。
3. 在 Create Policy (建立政策) 頁面上，選擇 JSON 標籤。
4. 在出現的編輯器中，將編輯器的內容取代為您要連接到 IAM 角色的 IAM 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，您會建立 IAM 角色並將新的 IAM 政策連接到它。

為 建立 IAM 角色 AWS Transfer Family

1. 在導覽窗格中，選擇角色，然後選擇建立角色。

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，尋找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)。

接著，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 文件會在條件包含萬用字元 `ArnLike` 時使用，`ArnEquals` 並指出完全相符的條件。

1. 在 IAM 主控台中，選擇您剛建立的角色。
2. 在 Summary (摘要) 頁面上，選擇 Trust relationships (信任關係)，然後選擇 Edit trust relationship (編輯信任關係)。
3. 在編輯信任關係編輯器中，確定服務為 `"transfer.amazonaws.com"`。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，將每個 **#####** 取代為您自己的資訊。

如需混淆代理人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 IAM 角色，AWS Transfer Family 允許代表您呼叫 AWS 服務。您連接至您建立的 IAM 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。

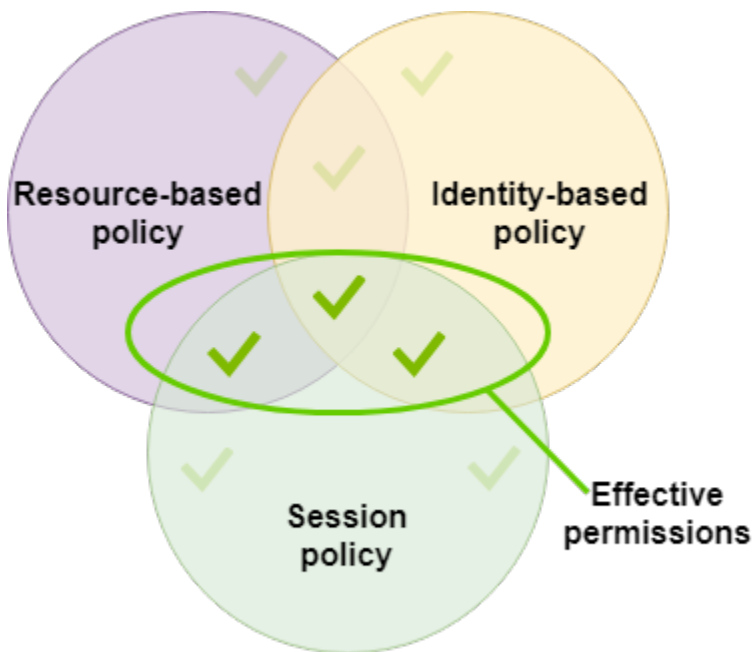
另請參閱

- 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 控制檔案系統資料存取](#)。

工作階段政策的運作方式

當管理員建立角色時，該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，限制使用者只能存取其主目錄。

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，工作階段政策是做為參數傳遞的進階政策。工作階段政策有助於鎖定使用者，讓他們只能存取物件字首包含其使用者名稱的儲存貯體部分。下圖顯示工作階段政策的許可是工作階段政策和資源型政策的交集，以及工作階段政策和身分型政策的交集。



如需詳細資訊，請參閱《IAM 使用者指南》中的[工作階段政策](#)。

在 AWS Transfer Family 中，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[資料保護和加密](#)。
- 若要使用工作階段政策根據使用者屬性建立存取許可，而不為每個使用者建立單獨的 IAM 角色，請參閱[動態許可管理方法](#)。

```

{
  "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結尾斜線，以表示它是目錄。另一方面，如果您設定的使用者HomeDirectory沒有結尾斜線，則應該將其包含在政策中。

在先前的範例政策中，請注意 `transfer:HomeFolder`、`transfer:HomeBucket` 和 `transfer:HomeDirectory` 政策參數的使用方式。這些參數是針對為使用者設定的 HomeDirectory 所設定，如 [HomeDirectory](#) 和 中所述 [實作您的 API Gateway 方法](#)。這些參數具有下列定義：

- `transfer:HomeBucket` 參數會取代為 的第一個元件HomeDirectory。
- `transfer:HomeFolder` 參數會替換為HomeDirectory參數的剩餘部分。
- `transfer:HomeDirectory` 參數已移除正斜線 (/)，因此可以做為Resource陳述式中 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` 已設定為 `/home`。
- `transfer:HomeFolder` 已設定為 `/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"限制使用者對相同路徑的 `put` 和 `get` 存取`/home/bob/amazon/stuff/`。

讀取/寫入存取政策範例

授予 Amazon S3 儲存貯體的讀取/寫入存取權

下列範例政策會 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：

- 將 `amzn-s3-demo-bucket` 取代為您的 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。
- 只有在正在存取的 Amazon S3 儲存貯體上啟用版本控制時，才需要 `GetObjectVersion` 和 `DeleteObjectVersion` 陳述式。

 Note

如果您曾經為儲存貯體啟用版本控制，則需要這些許可，因為您只能在 Amazon S3 中暫停版本控制，無法將其完全關閉。如需詳細資訊，請參閱 [「未版本控制」](#)、[「啟用版本控制」](#) 和 [「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:::amzn-s3-demo-bucket"
      ]
    },
    {
      "Sid": "HomeDirObjectAccess",
      "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:::amzn-s3-demo-bucket/*"
}
]
}

```

授予檔案系統對 Amazon EFS 檔案系統中檔案的存取權

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 EFS 檔案系統中檔案的根檔案系統存取權。

Note

在下列範例中，將##取代為您的區域、將 *account-id* 取代為檔案所在的帳戶，並將 *file-system-id* 取代為 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:us-east-1:123456789012: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:us-east-1:123456789012: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](#) - 使用服務受管使用者建立 SFTP Transfer Family 伺服器，並使用用戶端傳輸檔案。
- [設定和使用 SFTP 連接器](#) - 設定 SFTP 連接器，以在 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](#) - 將 Amazon API Gateway 方法設定為將檔案上傳至 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](#) - 建立受管工作流程來解密檔案、將加密的檔案上傳到 Amazon S3，以及檢視解密的內容。
- [設定 AS2 組態](#) - 設定 AS2 Transfer Family 伺服器，包括憑證匯入、設定檔和協議建立、選用的 AS2 連接器組態，以及測試。
- 下列教學課程會引導您建立和設定 Transfer Family Web 應用程式。選擇最適合您需求的教學課程：

[教學課程：設定基本 Transfer Family Web 應用程式](#) - 了解如何建立和設定 Transfer Family Web 應用程式。

[教學課程：設定具有選擇性多儲存貯體存取權的 AWS Transfer Family Web 應用程式](#) - 為單一使用者設定具有精細 Amazon S3 儲存貯體許可的 Transfer Family Web 應用程式。

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](#)
- [教學課程：設定基本 Transfer Family Web 應用程式](#)
- [教學課程：設定具有選擇性多儲存貯體存取權的 AWS Transfer Family Web 應用程式](#)

AWS Transfer Family 伺服器端點入門

使用此教學課程來開始使用 AWS Transfer Family (Transfer 系列)。您將了解如何使用 Amazon S3 儲存體建立具備可公開存取端點的 SFTP 伺服器、新增具有服務受管身分驗證的使用者，以及使用 Cyberduck 傳輸檔案。

主題

- [先決條件](#)
- [步驟 1：登入 AWS Transfer Family 主控台](#)
- [步驟 2：建立啟用 SFTP 的伺服器](#)
- [步驟 3：新增服務受管使用者](#)
- [步驟 4：使用用戶端傳輸檔案](#)

先決條件

開始之前，請務必完成 中的要求[先決條件](#)。在此設定中，您會建立 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 AWS 使用的其他服務需要許可，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 傳入和傳出檔案的使用者，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 SFTP 使用者建立 Transfer Family 資源的許可。
- 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，或為登入伺服器的使用者角色時，才需要 IAMFullAccess（或特別是允許建立 IAM 角色的政策）。
- 若要建立和刪除 VPC 伺服器類型，您需要將動作 ec2:CreateVpcEndpoint 和 ec2:DeleteVpcEndpoints 新增至您的政策。如需基於安全考量限制 VPC 端點存取的資訊，請參閱 [限制 Transfer Family 伺服器的 VPC 端點存取](#)。

 Note

AmazonS3FullAccess 和 IAMFullAccess 政策本身不需要用於的一般用途 AWS Transfer Family。它們在此處顯示為簡單的方法，以確保涵蓋您需要的所有許可。此外，這些是 AWS 受管政策，這是可供所有 AWS 客戶使用的標準政策。您可以檢視這些政策中的個別許可，並判斷用於您用途所需的最小集合。

步驟 1：登入 AWS Transfer Family 主控台

登入 Transfer Family

1. 登入 AWS 管理主控台 並在 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
2. 針對帳戶 ID 或別名，輸入您的 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. 選擇登入。

步驟 2：建立啟用 SFTP 的伺服器

Secure Shell (SSH) 檔案傳輸通訊協定 (SFTP) 是一種網路通訊協定，用於透過網際網路安全地傳輸資料。通訊協定支援 SSH 的完整安全性和身分驗證功能。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。

建立啟用 SFTP 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，選擇受管服務以在 Transfer Family 中存放使用者身分和金鑰，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，針對密碼編譯演算法選項，選擇安全政策，其中包含啟用供伺服器使用的密碼編譯演算法。我們最新的安全政策是預設值：如需詳細資訊，請參閱 [AWS Transfer Family 伺服器的安全政策](#)。

 Note

只有在您為伺服器新增受管工作流程時，才選擇為 CloudWatch 記錄建立新角色。CloudWatch 若要記錄伺服器事件，您不需要建立 IAM 角色。

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。

在新伺服器的狀態變更為線上之前，可能需要幾分鐘的時間。此時，您的伺服器可以執行檔案操作，但您必須先建立使用者。如需建立使用者的詳細資訊，請參閱 [管理伺服器端點的使用者](#)。

步驟 3：新增服務受管使用者

將使用者新增至啟用 SFTP 的伺服器

1. 在伺服器頁面上，選取要新增使用者的伺服器。
2. 選擇新增使用者。
3. 在使用者組態區段中，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 '@'。使用者名稱開頭不能是連字號 '-'、句點 '.' 或符號 '@'。
4. 針對 Access，選擇您在 中建立的 IAM 角色 [建立 IAM 角色和政策](#)。此 IAM 角色包含 IAM 政策，其中包含存取 Amazon S3 儲存貯體的許可，以及與服務的信任關係 AWS Transfer Family。中概述的程序 [建立信任關係](#) 說明如何建立適當的信任關係。
5. 針對政策，選擇無。
6. 針對主目錄，選擇您要用於存放傳輸資料的 Amazon S3 儲存貯體 AWS Transfer Family。輸入 home 目錄的路徑。這是您的使用者使用用戶端登入時看到的目錄。

我們建議您使用包含使用者名稱的目錄路徑，以便您可以選擇使用工作階段政策。工作階段政策會將 Amazon S3 儲存貯體中的使用者存取權限制在該使用者的 home 目錄。如需使用工作階段政策的詳細資訊，請參閱 [工作階段政策的運作方式](#)。

如果您願意，可以將此參數保留空白，以使用 Amazon S3 儲存貯體的 root 目錄。如果您選擇此選項，請確定您的 IAM 角色提供目錄的 root 存取權。

7. 選取限制核取方塊，以防止您的使用者存取其home目錄外的任何內容。這也可防止使用者看到 Amazon S3 儲存貯體名稱或資料夾名稱。
8. 針對 SSH 公有金鑰，以 `ssh-rsa <string>` 格式輸入 SSH 金鑰對的公有 SSH 金鑰部分。

您的金鑰必須由 服務驗證，才能新增您的新使用者。如需如何產生 SSH 金鑰對的詳細資訊，請參閱 [為服務受管使用者產生 SSH 金鑰](#)。

9. （選用）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。
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 OpenSSH 的程序。

主題

- [使用 Cyberduck](#)
- [使用 OpenSSH](#)

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. 在伺服器中，輸入您的伺服器端點。伺服器端點位於伺服器詳細資訊頁面上，請參閱 [檢視 SFTP、FTPS 和 FTP 伺服器詳細資訊](#)。
5. 對於連接埠號碼，輸入 **22** 表示 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 私有金鑰，選擇或輸入 SSH 私有金鑰。
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，選擇您要傳輸的檔案，然後將它們拖放到 Amazon S3 目錄（目標）。
- 在 Amazon S3 目錄（來源）中，選擇您要傳輸的檔案，然後將它們拖放到您的本機目錄（目標）。

使用 OpenSSH

使用下列說明使用 OpenSSH 從命令列傳輸檔案。

Note

此用戶端僅適用於啟用 SFTP 的伺服器。

AWS Transfer Family 使用 OpenSSH 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. 出現提示時，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，而 `transfer-key` 是 SSH 私有金鑰。這裡 `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 /amzn-s3-demo-bucket/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 /amzn-s3-demo-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。本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 儲存部落格有一篇文章，說明如何簡單地解密檔案，而無需使用 Transfer Family Managed 工作流程撰寫任何程式碼、[使用 PGP 和 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[工作流程的 IAM 政策](#)。

Note

在建立執行角色的過程中，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啟動您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*。amzn-s3-demo-bucket 將取代為您上傳加密檔案的 Amazon S3 儲存貯體名稱。

 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 中所述[使用預先定義的步驟](#)。自訂步驟所需的許可如 中所述[自訂步驟的 IAM 許可](#)。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "WorkflowsS3Permissions",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:PutObject",
        "s3:PutObjectTagging",
        "s3:ListBucket",
        "s3:PutObjectTagging",
        "s3:PutObjectVersionTagging",
        "s3:DeleteObjectVersion",
        "s3:DeleteObject"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*",
        "arn:aws:s3:::amzn-s3-demo-bucket"
      ]
    },
    {
      "Sid": "DecryptSecret",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
    }
  ]
}
```

```
"Resource": "arn:aws:secretsmanager:us-east-1:123456789012: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 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
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**。
 - 在名義步驟區段中，選擇新增步驟。
4. 針對選擇步驟類型，選擇解密檔案，然後選擇下一步。
5. 在設定參數對話方塊中，指定下列項目：
 - 輸入描述性步驟名稱，例如 **decrypt-step**。步驟名稱中不允許空格。
 - 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 中建立的 IAM 政策 `amzn-s3-demo-bucket` 中指定為的相同 Amazon S3 儲存貯體。
 - 針對目的地金鑰字首，輸入您要在目的地儲存貯體中存放解密檔案的字首（資料夾）名稱，例如 **decrypted-files/**。

Note

請務必將結尾斜線 (/) 新增至字首。

- 在本教學課程中，請清除覆寫現有的。清除此設定時，如果您嘗試解密具有現有檔案相同名稱的檔案，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，因此無需設定其他步驟。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。下一個步驟將需要此 ID。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

現在您已有一個具有解密步驟的工作流程，您必須將其與 Transfer Family 伺服器建立關聯。本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。

將工作流程連接到伺服器之後，您必須建立可 SFTP 到伺服器的使用者，並觸發工作流程執行。

設定 Transfer Family 伺服器以執行工作流程

1. 在 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
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 中建立的 IAM 角色 [步驟 1：設定執行角色](#)。
5. 捲動至頁面底部，然後選擇儲存以儲存變更。

請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 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
2. 在左側導覽窗格中，選擇伺服器，然後選擇您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，選擇可存取您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 `amzn-s3-demo-bucket`。
- 對於 SSH 公有金鑰，請將 貼入對應至您擁有之私有金鑰的公有金鑰。如需詳細資訊，請參閱[為服務受管使用者產生 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](#)。

產生 PGP 金鑰對

1. 在本教學課程中，您可以使用 `gpg`(GnuPG) 2.0.22 版用戶端來產生使用 RSA 做為加密演算法的 PGP 金鑰對。針對此用戶端，請執行下列命令，並提供電子郵件地址和密碼短語。您可以使用任何您喜歡的名稱或電子郵件地址。請務必記住您使用的值，因為您稍後需要在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。如果您選擇 ECC，您可以從 [中](#)選擇橢圓曲線 Curve25519 的 NISTBrainPool 和 [中](#)。

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.gpg --armor --export-secret-key user@example.com
```

此命令會將私有金鑰匯出至 **workflow-tutorial-key.gpg** 檔案。您可以為輸出檔案命名任何您喜歡的名稱。您也可以在新增私有金鑰檔案後將其刪除 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，以便在工作流程對上傳的檔案執行解密步驟時，工作流程可以找到私有金鑰。

Note

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

在 Secrets Manager 中存放 PGP 私有金鑰

1. 登入 AWS 管理主控台，並在 <https://console.aws.amazon.com/secretsmanager/> 開啟 AWS Secrets Manager 主控台。
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. 在鍵/值對區段中，選擇鍵/值索引標籤。
 - 金鑰 – 輸入 **PGPPrivateKey**。
 - value – 將私有金鑰的文字貼到值欄位中。
6. 選擇新增資料列，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 金鑰對時所使用的密碼短語 [步驟 4：建立 PGP 金鑰對](#)。
7. 選擇下一步。
8. 在設定秘密頁面上，輸入秘密的名稱和描述。您可以為特定使用者或可供所有使用者使用的秘密建立秘密。如果您的伺服器 ID 為 **s-11112222333344445**，您可以如下所示命名秘密。
 - 若要為所有使用者建立預設秘密，請命名秘密 **aws/transfer/s-11112222333344445/@pgp-default**。
 - 若要僅為您先前建立的使用者建立秘密，請將秘密命名為 **aws/transfer/s-11112222333344445/decrypt-user**。
9. 選擇下一步，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，選擇存放以建立和存放秘密。

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 程式來加密要在工作流程中使用的檔案。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，請將 *marymajor@example.com* 取代為您建立 PGP 金鑰對時使用的電子郵件地址。
- `--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 **testfile.txt** 的檔案。

Important

加密檔案以搭配 AWS Transfer Family 工作流程使用時，請務必使用 `-r` 參數來指定非匿名收件人。匿名加密（未指定收件人）可能會導致工作流程中的解密失敗，因為系統無法識別要用於解密的金鑰。此問題的偵錯資訊可在取得[對匿名收件人加密問題進行故障診斷](#)。

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

- 開啟命令終端機。
- 執行下列命令，*your-endpoint* 將取代為您實際的端點，並將 *transfer-key* 取代為您使用者的 SSH 私有金鑰：

```
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: /amzn-s3-demo-bucket/decrypt-user
```

您的目錄會反映 Amazon S3 儲存貯體的名稱。

4. 執行下列命令來上傳檔案並觸發工作流程以執行：

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

5. 對於解密檔案的目的地，您在建立工作流程時指定 `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
```

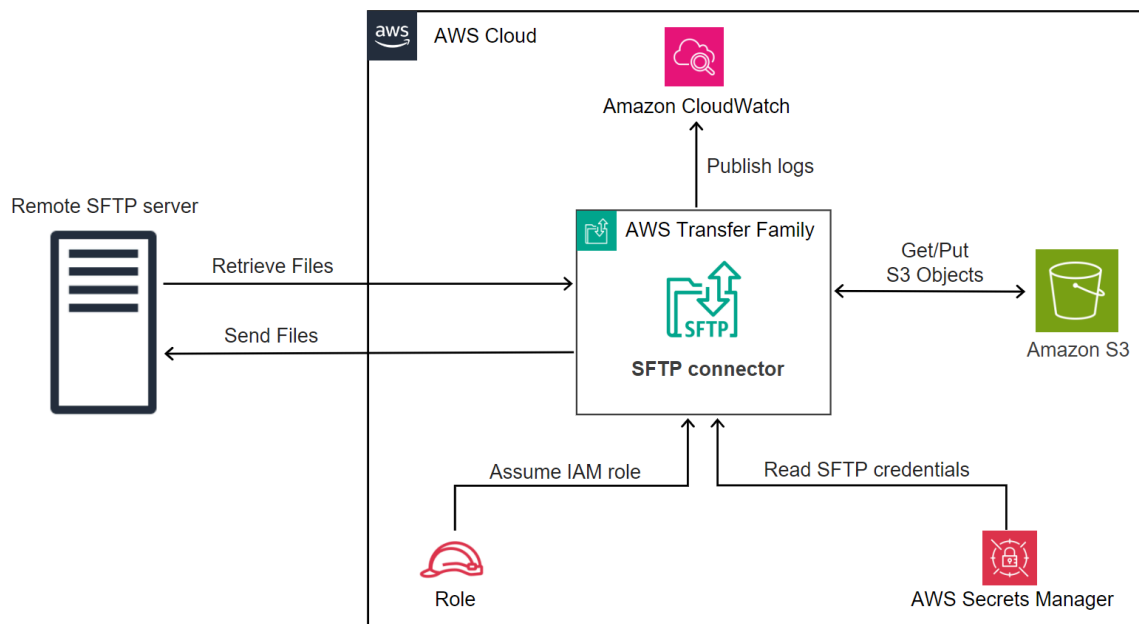
如果成功，`ls` 命令會列出 `testfile.txt` 檔案。您可以下載此檔案，並確認它與您先前加密的原始檔案相同。

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、合作夥伴擁有的目的地。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具有服務受管和 VPC_LATTICE 輸出類型的 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 登入資料 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。您可以選擇服務受管輸出（使用 AWS 受管基礎設施）或 VPC 輸出（使用跨 VPC 資源存取透過 VPC 路由）。IAM 角色用於允許存取 Amazon S3 儲存貯體和存放在 Secrets Manager 中的登入資料。您也可以登入 Amazon CloudWatch。



下列部落格文章提供使用 SFTP 連接器建置 MFT 工作流程的參考架構，包括在使用 SFTP 連接器將檔案傳送到遠端 SFTP 伺服器之前，先使用 PGP 加密檔案：[使用 AWS Transfer Family SFTP 連接器和 PGP 加密來架構安全且合規的受管檔案傳輸。](#)

連接器輸出類型

SFTP 連接器支援兩種輸出類型，可決定連接器將流量路由到遠端 SFTP 伺服器的方式：

- **SERVICE_MANAGED**（預設）：將 AWS Transfer Family 受管基礎設施與靜態 IP 地址用於傳出連線。
- **VPC**：使用跨 VPC 資源存取透過 VPC 路由流量，啟用私有端點連線和使用您自己的 NAT 閘道。

本教學課程涵蓋這兩種輸出類型。當您需要以下項目時，請選擇 VPC 輸出類型：

- 連線至 VPC 中的私有 SFTP 伺服器（私有 IP 地址）
- 透過 Direct Connect 或 VPN 連線至內部部署 SFTP 伺服器
- 透過 VPC 路由公有端點流量以進行安全控制
- 使用您自己的彈性 IP 地址進行傳出連線

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。在本教學課程中，我們使用 AWS Transfer Family 伺服器做為遠端 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：[建立具有必要許可的 IAM 角色](#)。
- 建立使用 SFTP 通訊協定的 Transfer Family 伺服器，以及使用 SFTP 連接器在 SFTP 伺服器之間傳輸檔案的服務受管使用者：[建立 Transfer Family SFTP 伺服器和使用者的使用者](#)。
- 建立 AWS Secrets Manager 秘密，以存放 SFTP 連接器用來登入遠端 SFTP 伺服器的登入資料：[在 Amazon 中建立和存放秘密 AWS Secrets Manager](#)。

對於 VPC 輸出類型連接器，您也需要：

- 具有適當子網路和安全群組的 VPC
- 資源閘道（至少需要 2 個可用區域）：[建立資源閘道（僅限 VPC 輸出類型）](#)。
- 指向 SFTP 伺服器的資源組態：[建立資源組態（僅限 VPC 輸出類型）](#)。如需詳細資訊，請參閱《Amazon VPC Lattice 使用者指南》中的[資源組態](#)。

建立 Amazon S3 儲存貯體

建立 Amazon S3 儲存貯體

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

在本教學課程中，我們的儲存貯體位於 **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[如何建立 S3 儲存貯體？](#) Amazon Simple Storage Service 使用者指南中的。

建立具有必要許可的 IAM 角色

針對存取角色，建立具有下列許可的政策。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListingOfUserFolder",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket"
      ]
    },
    {
      "Sid": "HomeDirObjectAccess",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
    },
    {
      "Sid": "GetConnectorSecretValue",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
    }
  ]
}
```

```
"Resource": "arn:aws:secretsmanager:us-west-2:111122223333:secret:aws/transfer/SecretName-6RandomCharacters"
    }
  ]
}
```

取代項目，如下所示：

- 對於 `amzn-s3-demo-bucket`，教學課程使用 `sftp-server-storage-east`。
- 對於 `##`，教學課程使用 `us-east-1`。
- 針對 `account-id`，使用您的 AWS 帳戶 ID。
- 對於 `SecretName-6RandomCharacters`，我們 `using sftp-connector1` 是名稱（秘密會有自己的六個隨機字元）。

您還必須確保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](#)。

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

我們需要將秘密存放在 Secrets Manager 中，以存放 SFTP 連接器的使用者登入資料。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。如需關於定價的資訊，請參閱 [AWS Secrets Manager 定價](#)。

開始存放秘密的程序之前，請擷取私有金鑰並將其格式化。私有金鑰必須對應至遠端 SFTP 伺服器上為使用者設定的公有金鑰。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。

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

這會以正確的格式（含內嵌換行字元）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 連接器的使用者登入資料

1. 登入 AWS 管理主控台 並在 <https://console.aws.amazon.com/secretsmanager/> 開啟 AWS Secrets Manager 主控台。
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. 在鍵/值對區段中，選擇鍵/值索引標籤。
 - 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. 在空雙引號 ("") 之間貼上私有金鑰的文字（稍早儲存）。

您的畫面應如下所示（索引鍵資料呈現灰色）。



7. 選擇下一步。
8. 在設定秘密頁面上，輸入秘密的名稱。在本教學課程中，我們將秘密命名為 **aws/transfer/sftp-connector1**。
9. 選擇下一步，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，選擇存放以建立和存放秘密。

建立資源閘道（僅限 VPC 輸出類型）

對於 VPC 輸出類型連接器，您需要在 VPC 中建立資源閘道。資源閘道可做為跨 VPC 資源存取的進入點。

建立資源閘道

1. 執行下列命令來建立資源閘道（將 VPC ID 和子網路 IDs 取代為您的值）：

```
aws vpc-lattice create-resource-gateway \  
  --name my-sftp-resource-gateway \  
  --vpc-identifier vpc-12345678 \  
  --subnet-ids subnet-12345678 subnet-87654321
```

 Note

資源閘道需要至少 2 個可用區域中的子網路。

2. 請注意回應中的資源閘道 ID，以便在下一個步驟中使用。

建立資源組態（僅限 VPC 輸出類型）

建立指向 SFTP 伺服器的資源組態。這可以是 VPC 中伺服器的私有 IP 地址，或外部伺服器的公有 DNS 名稱。如需資源組態的詳細資訊，請參閱《Amazon VPC Lattice 使用者指南》中的[資源組態](#)。

建立資源組態

1. 對於私有 SFTP 伺服器，請執行：

```
aws vpc-lattice create-resource-configuration \  
  --name my-sftp-resource-config \  
  --port-ranges 22 \  
  --type SINGLE \  
  --resource-gateway-identifier rgw-12345678 \  
  --resource-configuration-definition ipResource={ipAddress="10.0.1.100"}
```

2. 對於公有 SFTP 伺服器（僅限 DNS 名稱），請執行：

```
aws vpc-lattice create-resource-configuration \  
  --name my-public-sftp-resource-config \  
  --port-ranges 22 \  
  --type SINGLE \  
  --resource-gateway-identifier rgw-12345678 \  
  --resource-configuration-definition dnsResource={domainName="sftp.example.com"}
```

 Note

公有端點必須使用 DNS 名稱，而不是 IP 地址。

3. 建立連接器時，請注意來自 回應的資源組態 ARN。

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之所有資源的 SFTP 連接器。如需詳細資訊，請參閱[建立 SFTP 連接器](#)。

建立 SFTP 連接器

1. 在 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
2. 在左側導覽窗格中，選擇 SFTP 連接器，然後選擇建立 SFTP 連接器。
3. 針對輸出類型，選擇下列其中一項：
 - 服務受管（預設）：將 AWS Transfer Family 受管基礎設施與靜態 IP 地址用於傳出連線。
 - VPC Lattice：使用跨 VPC 資源存取透過 VPC 路由流量。選擇此選項進行私有端點連線，或使用您自己的 NAT 閘道。

Important

您無法在建立連接器後變更輸出類型。請根據您的連線需求謹慎選擇。

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

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

以 Transfer Family 伺服器 ID 取代 **1111aaaa2222bbbb3**。

- 針對存取角色，輸入我們先前建立的角色 **sftp-connector-role**。
- 針對資源組態 ARN（僅限 VPC Lattice 輸出類型），輸入您先前建立的資源組態 ARN：

```
arn:aws:vpc-lattice:us-east-1:account-id:resourceconfiguration/rcfg-12345678
```

- 針對記錄角色，選擇在主體元素 `transfer.amazonaws.com` 中包含具有之信任政策的角色。

秘訣：除了將 Transfer Family 新增為信任的實體之外，您還可以將 `AWSTransferLoggingAccess` AWS 受管政策新增至角色。此政策會在 [AWSTransferLoggingAccess](#) 中詳細說明。

Connector configuration

Egress type [Info](#)
Choose your SFTP connector's egress type: either directly over public internet, or via your VPC environment

☒ **Service managed**
Connect to public endpoints over the internet. The connector will present service-provided static IP addresses to remote server.

☐ **VPC Lattice**
Connect to public or private endpoints through your VPC. The connector will present elastic IP address from your VPC's CIDR range to remote server.

URL
Enter the URL of remote server to which you need to connect using the SFTP connector

URL of the remote (target) SFTP server

Access role [Info](#)
IAM Role for Amazon S3 access and AWS Secrets Manager access

▼

↺

Logging role - optional [Info](#)
IAM role for the connector to push events to your CloudWatch logs

▼

↺

5. 在 SFTP 組態區段中，提供下列資訊：

- 針對 Connector 登入資料，選擇包含 SFTP 登入資料之 Secrets Manager 資源的名稱。針對教學課程，選擇 **aws/transfer/sftp-connector1**。
- 對於信任的主機金鑰，請貼入主機金鑰的公有部分。您可以ssh-keyscan為 SFTP 伺服器執行來擷取此金鑰。如需如何格式化和存放信任主機金鑰的詳細資訊，請參閱 [SftpConnectorConfig](#) 資料類型文件。
- 針對最大並行連線，選取從 1 到 5 的整數值：預設值為 5。

SFTP configuration [Info](#)**Connector credentials** [Info](#)

Select a secret from AWS Secrets Manager containing the username and SSH private key, or username and password, to be used to connect to the remote server

aws/transfer/sftp-connector1 ▼



[Store a new secret](#)

Trusted host keys - optional [Info](#)

Enter the public portion of the host key(s) that is used to identify the remote server you need to connect to. You can enter the trusted host key(s) now, or add them after creating the connector by using the host key information returned by the TestConnection action.

Connections to the remote server are established only if it's SSH fingerprint matches one of the provided trusted host key(s).

ssh-rsa AAAAE

[Remove](#)

[Add trusted host key](#)

Maximum concurrent connections [Info](#)

Select the maximum number of concurrent connections that your connector can create to the remote server

5 ▼

6. 確認所有設定後，請選擇建立連接器以建立 SFTP 連接器。

您也可以使用 建立連接器 AWS Command Line Interface。

- 若要使用服務管理的輸出建立 SFTP 連接器，請執行下列命令：

```
aws transfer create-connector \
  --url "sftp://s-1111aaaa2222bbbb3.server.transfer.us-east-1.amazonaws.com" \
  --access-role "arn:aws::iam::account-id:role/sftp-connector-role" \
  --sftp-config UserSecretId="aws/transfer/sftp-connector1",TrustedHostKeys="ssh-rsa AAAAB3NzaC..."
```

- 若要使用 VPC 型輸出建立 SFTP 連接器，請執行下列命令：

```
aws transfer create-connector \
  --url "sftp://my.sftp.server.com:22" \
  --access-role "arn:aws::iam::account-id:role/sftp-connector-role" \
  --sftp-config UserSecretId="aws/transfer/sftp-connector1",TrustedHostKeys="ssh-rsa AAAAB3NzaC..." \
  --egress-config VpcLattice={ResourceConfigurationArn="arn:aws:vpc-lattice:us-east-1:account-id:resourceconfiguration/rcfg-12345678",PortNumber=22}
```

建立 SFTP 連接器後，建議您在嘗試使用新連接器傳輸任何檔案之前進行測試。

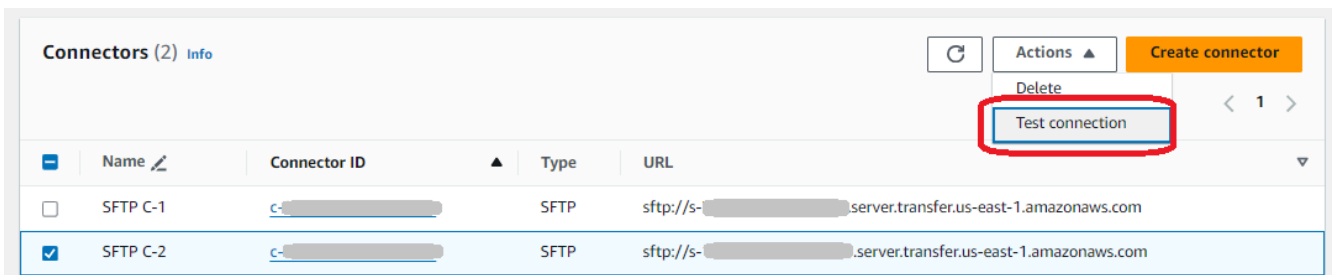
Note

對於 VPC 輸出類型連接器，DNS 解析可能需要幾分鐘才能建立。在此期間，連接器狀態將為 PENDING，TestConnection 並將傳回「無法使用連接器」。等待狀態變成 ACTIVE 再嘗試傳輸檔案。

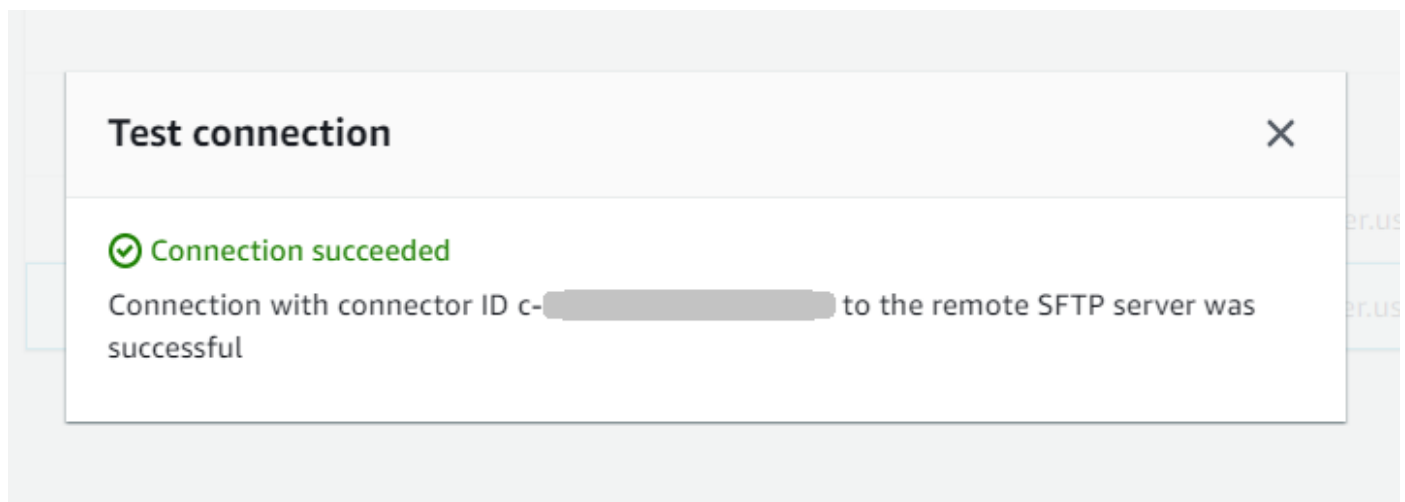
Test a connector using the console

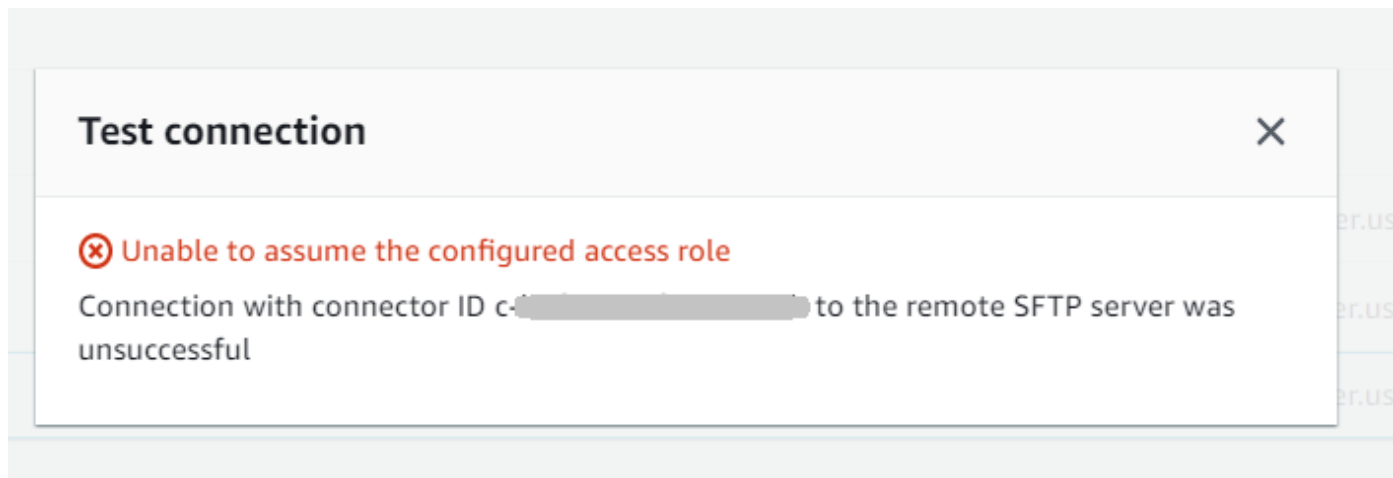
測試 SFTP 連接器

1. 在 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
2. 在左側導覽窗格中，選擇 SFTP 連接器，然後選取連接器。
3. 從動作功能表中，選擇測試連線。



系統會傳回訊息，指出測試通過或失敗。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，請在命令提示字元中執行下列命令（以實際連接器 ID 取代 **### 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"
}
```

當您描述 VPC 輸出類型連接器時，回應會包含新欄位：

```
{
  "Connector": {
    "AccessRole": "arn:aws:iam::219573224423:role/sftp-connector-role",
    "Arn": "arn:aws:transfer:us-east-1:219573224423:connector/c-5dfa309ccabf40759",
    "ConnectorId": "c-5dfa309ccabf40759",
```



```
{
  "Status": "ACTIVE",
  "EgressConfig": {
    "ResourceConfigurationArn": "arn:aws:vpc-lattice:us-east-1:025066256552:resourceconfiguration/rcfg-079259b27a357a190",
  },
  "EgressType": "VPC",
  "ServiceManagedEgressIpAddresses": null,
  "SftpConfig": {
    "TrustedHostKeys": [ "ssh-rsa AAAAB3NzaC..." ],
    "UserSecretId": "aws/transfer/sftp-connector1"
  },
  "Url": "sftp://my.sftp.server.com:22"
}
```

請注意，VPC 輸出類型連接器為 `ServiceManagedEgressIpAddresses` `null`，因為流量會透過 VPC 路由，而非 AWS 受管基礎設施。

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

本教學課程針對來源和目的地儲存位置使用 Amazon S3 儲存貯體。如果您的 SFTP 伺服器不使用 Amazon S3 儲存體，則無論您在下列命令 `sftp-server-storage-east` 中看到何處，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 `SEND-to-SERVER.txt` 的檔案從 Amazon S3 儲存傳送至 SFTP 伺服器。
- 我們將名為 `RETRIEVE-to-S3.txt` 的檔案從 SFTP 伺服器擷取到 Amazon S3 儲存。

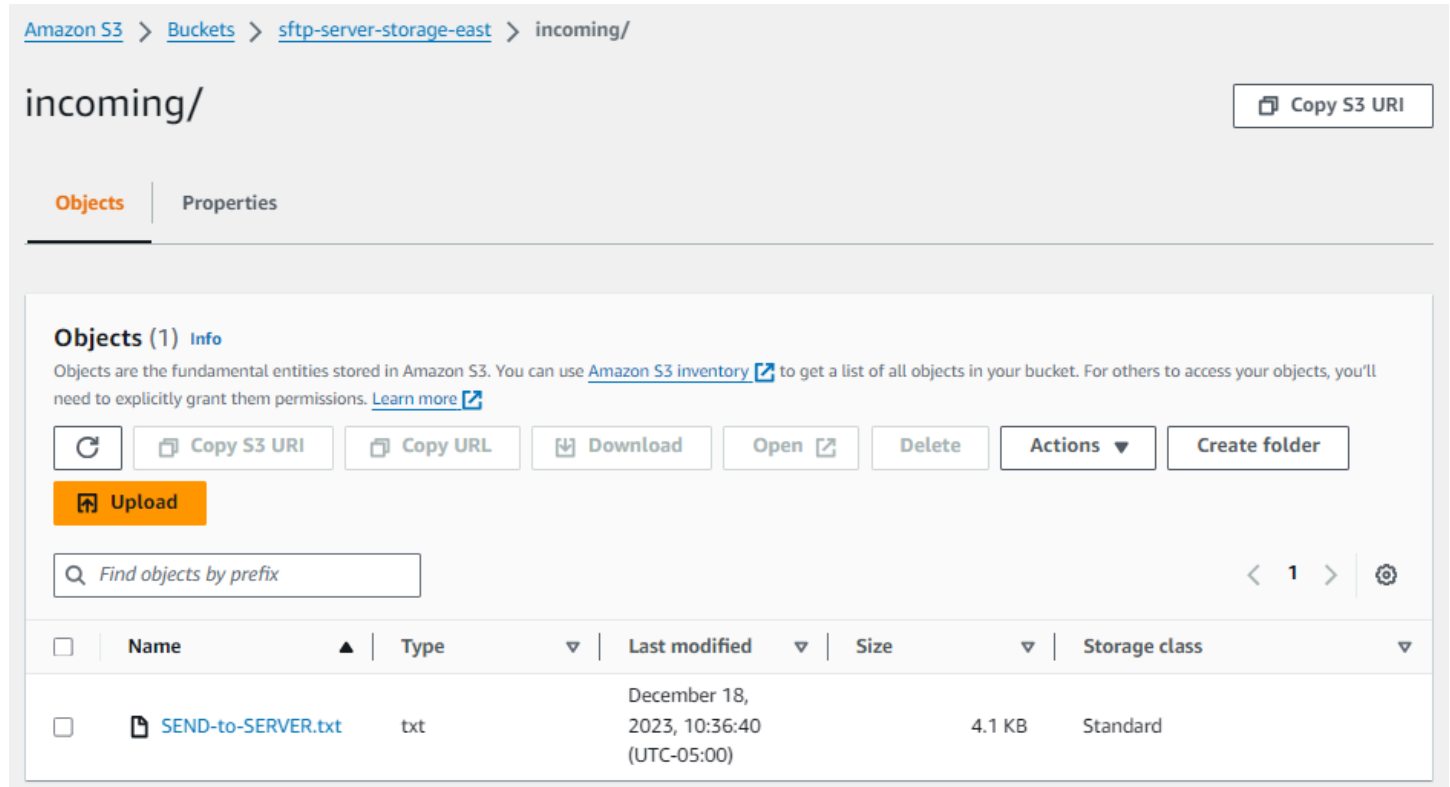
Note

在下列命令中，將 *connector-id* 取代為您的連接器 ID。

首先，我們會將檔案從 Amazon S3 儲存貯體傳送至遠端 SFTP 伺服器。從命令提示字元中，執行下列命令：

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

您的儲存 sftp-server-storage-east 貯體現在看起來應該像這樣。



如果您未如預期看到檔案，請檢查您的 CloudWatch 日誌。

檢查您的 CloudWatch 日誌

1. 在 <https://console.aws.amazon.com/cloudwatch/> : // 開啟 Amazon CloudWatch 主控台
2. 從左側導覽功能表中選取日誌群組。
3. 在搜尋列中輸入您的連接器 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": "/sftp-server-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": "account-id",
  "connector-arn": "arn:aws:transfer:us-east-1:account-id: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。

接著，我們將檔案從 SFTP 伺服器擷取到 Amazon S3 儲存貯體。從命令提示字元中，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 "/sftp-server-
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。

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](#)

Refresh
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder

Upload

Find objects by prefix < 1 > ⚙

☐	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": "account-id",
  "connector-arn": "arn:aws:transfer:us-east-1:account-id:connector/c-connector-id",
  "local-directory-path": "/sftp-server-storage-east/incoming"
}
```

故障診斷 VPC 輸出類型連接器

如果您遇到 VPC 輸出類型連接器的問題，請檢查下列項目：

- 連接器狀態為待定：VPC 連接器的 DNS 解析可能需要幾分鐘的時間。等待狀態變成 ACTIVE，再嘗試連線。
- 連線逾時：確認安全群組允許資源閘道子網路與目標 SFTP 伺服器之間的連接埠 22 流量。
- 資源組態錯誤：確保您的資源組態指向正確的 IP 地址或 DNS 名稱，且資源閘道與您的 SFTP 伺服器位於相同的 VPC 中（適用於私有端點）。如需詳細資訊，請參閱《Amazon VPC Lattice 使用者指南》中的[資源組態](#)。
- 公有端點問題：對於公有端點，請確定您在資源組態中使用 DNS 名稱，而不是 IP 地址。確認您的 VPC 具有用於傳出網際網路存取的 NAT 閘道。
- 可用區域可用性：資源閘道需要至少 2 個可用區域中的子網路。並非所有 AZs 都支援 VPC Lattice - 請檢查您區域中支援的 AZs。

VPC 輸出類型的成本考量：

- VPC Lattice 以資源提供者的身分收取 0.006/GB 的資料處理費用（直接由 VPC Lattice 計費）
- AWS Transfer Family 會吸收每 GB 0.01 USD 的資源消費者成本（前 1 PB）
- 對於透過 VPC 的公有端點，可能需要支付額外的 NAT Gateway 和資料傳輸費用
- 除了標準 0.40 USD/GB 的資料處理費之外，沒有額外的 Transfer Family 費用

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。典型的 SFTP 連接器使用者擁有自己的遠端 SFTP 伺服器。請參閱 [建立 Transfer Family SFTP 伺服器和使用者的](#)。
- 由於我們使用 Transfer Family 伺服器，因此我們也使用服務管理的 SFTP 使用者。此外，為了簡化起見，我們結合此使用者存取 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與 Transfer Family 伺服器無關的個別 SFTP 使用者。請參閱 [建立 Transfer Family SFTP 伺服器和使用者的](#)。
- 在本教學課程中，由於我們將 Amazon S3 儲存體用於遠端 SFTP 伺服器，因此我們需要建立第二個儲存貯體 **sftp-server-storage-east**，以便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

大多數使用者不需要建立 Transfer Family SFTP 伺服器和使用者的，因為您已有 SFTP 伺服器與使用者，而且您可以使用此伺服器往返傳輸檔案。不過，為了簡化本教學課程，我們使用 Transfer Family 伺服器做為遠端 SFTP 伺服器。

遵循中所述的程序來[建立啟用 SFTP 的伺服器](#)建立伺服器，並[步驟 3：新增服務受管使用者](#)新增使用者。以下是我們用於教學課程的使用者詳細資訊：

- 建立您的服務受管使用者 `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`。在本教學課程中，我們為 SFTP 使用者和存取 SFTP 連接器使用相同的 IAM 角色。當您為組織建立連接器時，您可能會有個別的使用者和存取角色。
- 伺服器主機金鑰：您需要在建立連接器時使用伺服器主機金鑰。您可以 `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

在本教學課程中，我們使用單一的合併角色。我們同時將此角色用於 SFTP 使用者，以及連接器的存取。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` 存放在 Secrets Manager 中的名為 `SECRET_NAME` 的秘密。針對教學課程，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:::sftp-server-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:::sftp-server-storage-east/*"
    ]
},
{
    "Sid": "GetConnectorSecretValue",
    "Effect": "Allow",
    "Action": [
        "secretsmanager:GetSecretValue"
    ],
    "Resource": "arn:aws:secretsmanager:us-east-1:111122223333: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](#)和其他基本功能做為範例。

主題

- [先決條件](#)
- [步驟 1：建立 CloudFormation 堆疊](#)
- [步驟 2：檢查伺服器的 API Gateway 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到伺服器](#)
- [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 EFS，請更新 Lambda](#)

先決條件

在 中建立 Transfer Family 資源之前 CloudFormation，請先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. 視您使用的儲存體而定，請參閱下列文件：
 - 若要建立 Amazon S3 儲存貯體，請參閱[如何建立 S3 儲存貯體？](#) Amazon Simple Storage Service 使用者指南中的。
 - 若要建立 Amazon EFS 檔案系統，請參閱[設定 Amazon EFS 檔案系統](#)。
2. 若要建立使用者角色，請參閱[建立 IAM 角色和政策](#)

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

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 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，選擇選擇現有範本。
4. 複製此連結、[基本堆疊範本](#)，並將其貼入 Amazon S3 URL 欄位。
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 UserPassword 的預設值。
 - 針對 UserHomeDirectory，輸入您先前建立之儲存體 (Amazon S3 儲存貯體或 Amazon EFS 檔案系統) 的詳細資訊。
 - 將預設 UserRoleArn 取代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 SFTP 連線到伺服器時，您會提供私有金鑰而非密碼。
7. 選擇下一步，然後在設定堆疊選項頁面上再次選擇下一步。
8. 檢閱您要建立之堆疊的詳細資訊，然後選擇建立堆疊。

 Note

在頁面底部的功能下，您必須確認 CloudFormation 可能會建立 IAM 資源。

步驟 2：檢查伺服器的 API Gateway 方法組態

 Note

為了提高安全性，您可以設定 Web 應用程式防火牆。AWS WAF 是一種 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](#)。

 請勿啟用 API Gateway 快取

將 API Gateway 方法用作 Transfer Family 的自訂身分提供者時，請勿啟用 API Gateway 方法的快取。快取對身分驗證請求不適當且無效，因為：

- 每個身分驗證請求都是唯一的，並且需要即時回應，而不是快取的回應

- 快取沒有好處，因為 Transfer Family 永遠不會將重複或重複的請求傳送至 API Gateway
- 啟用快取會導致 API Gateway 以不相符的資料回應，導致對身分驗證請求的回應無效

檢查伺服器的 API Gateway 方法組態並進行部署

1. 在以下網址開啟 API Gateway 主控台：<https://console.aws.amazon.com/apigateway/>。
2. 選擇 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 prod，然後選擇部署。

成功部署 API Gateway 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。下一個步驟將需要它。

步驟 3：檢視 Transfer Family 伺服器詳細資訊

當您使用 範本建立 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 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 ARN 中，例如 s-1111222233344445。

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

伺服器 ID 符合 TransferServer 資源顯示的 ID CloudFormation。

步驟 4：測試您的使用者是否可以連線到伺服器

若要測試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 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
2. 在伺服器頁面上，選擇您的新伺服器，選擇動作，然後選擇測試。
3. 在使用者名稱欄位中輸入登入資料的文字，然後在密碼欄位中輸入。這些是您部署 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 `Status Code: 200` HTML 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，請將其中一個 API Gateway AWS 受管政策新增至您用於 API 的角色。

步驟 5：測試 SFTP 連線和檔案傳輸

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。

- 如果您使用的是密碼，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. 出現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 CloudFormation 堆疊設定下列參數：

- CreateServer：true
- UserHomeDirectory：/amzn-s3-demo-bucket1
- UserName：myuser
- UserPassword：MySuperSecretPassword

Important

這是範例密碼。當您設定 API Gateway 方法時，請務必輸入強式密碼。

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

UserPublicKey1 是您作為公有/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。連接到 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:::amzn-s3-demo-bucket1"
    },
    {
      "Sid": "VisualEditor1",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObjectAcl",
        "s3:GetObject",
        "s3:DeleteObjectVersion",
        "s3:DeleteObject",
        "s3:PutObjectAcl",
        "s3:GetObjectVersion"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*"
    }
  ]
}
```

若要使用 SFTP 連線至伺服器，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，您可以透過執行 pwd 命令來檢視該主目錄。例如：

```
sftp> pwd
Remote working directory: /amzn-s3-demo-bucket1
```

使用者無法檢視主目錄上方的任何目錄。例如：

```
sftp> pwd
Remote working directory: /amzn-s3-demo-bucket1
sftp> cd ..
sftp> ls
Couldn't read directory: Permission denied
```

如果使用 Amazon EFS，請更新 Lambda

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

將 Posix 設定檔新增至 Lambda 函數

1. 開啟位於 <https://console.aws.amazon.com/lambda/> 的 Lambda 主控台。
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，**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 中，在 Policy 和 之間新增下列行 HomeDirectory：

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

其中 **uid-value** 和 **gid-value** 是整數 0 或更高，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

本教學課程會逐步解說如何使用 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-enabled 伺服器，已準備好接受來自範例交易合作夥伴的 AS2 訊息。您也會有一個連接器，可用來傳送 AS2 訊息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 AWS Command Line Interface 《使用者指南》中的 [安裝或更新最新版本的 AWS CLI](#)。

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

此程序會在 中說明 [步驟 1：建立 AS2 的憑證](#)。

2. 匯入您在步驟 1 中建立的憑證。

此程序說明於 [步驟 2：將憑證匯入為 Transfer Family 憑證資源](#)。

3. 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。

此程序說明於 [步驟 3：為您和您的交易合作夥伴建立設定檔](#)。

4. 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。

此程序說明於 [步驟 4：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，僅限傳入傳輸。如果您只執行傳出傳輸，則不需要 Transfer Family 伺服器。

5. 建立您與交易合作夥伴之間的協議。

此程序說明於 [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。

此程序說明於 [步驟 6：在您和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。

此程序說明於 [步驟 7：使用 Transfer 系列測試透過 AS2 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 AS2-enabled 合作夥伴伺服器。
- 透過虛擬私有雲端 (VPC) 端點，從連接埠 5080 上 AS2-enabled 合作夥伴伺服器接收檔案。

步驟 1：建立 AS2 的憑證

AS2 交換中的雙方都需要 X.509 憑證。您可以透過任何您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，然後簽署次級憑證。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。

若要透過合作夥伴傳輸檔案，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。
- 您的貿易合作夥伴會傳送其公有金鑰給您，而您會將公有金鑰傳送給他們。
- 您的交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 GUI 管理金鑰，[Portecle](#)是您可以使用的一個選項。

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。如果您要做為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：每個交易合作夥伴各一組。在此情況下，您不需要產生兩個根憑證授權單位 (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，使用您的 root-ca-key.pem 檔案建立自我簽署憑證。

```
/usr/bin/openssl req \  
-x509 -new -nodes -sha256 \  
-days 1825 \  
-subj "/C=US/ST=MA/L=Boston/O=TransferFamilyCustomer/OU=IT-dept/CN=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	組織所在國家/地區的兩個字母代碼。
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

有些 AS2-enabled 伺服器，例如 OpenAS2，會要求您使用相同的憑證來簽署和加密。在這種情況下，您可以匯入相同的私有金鑰和憑證，以達成這兩個目的。若要這樣做，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. 接著，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已簽章的憑證。

```
/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：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）。

 Note

如果您有同時包含憑證及其鏈結的檔案，您可以僅使用 `certificate` 參數將該檔案提供給 `import-certificate` 命令。例如：

```
aws transfer import-certificate --usage ENCRYPTION --certificate  
file://combined-cert-and-chain-file.pem
```

如果您使用 `certificate` 參數來上傳憑證及其鏈結，請勿使用 `certificate-chain` 參數。

如果您結合憑證及其鏈結，您的金鑰會使用傳統 PEM 標準進行格式化，其中包括每 64 個字元換行「\n」。儲存的憑證在功能上等同於您上傳的憑證，唯一的差別是透過的 `DescribeCertificate` 回應 AWS CLI 將包含這些換行字元。

```
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*。

接著，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 3：為您和您的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本機 AS2 設定檔。此命令會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，合作夥伴的 AS2 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，將 *MYCORP* 取代為您組織的名稱，並將 *PARTNER-COMPANY* 取代為您交易合作夥伴組織的名稱。

步驟 4：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-enabled 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-enabled 的伺服器。目前，Transfer Family 僅支援使用 AS2 通訊協定的 VPC 端點類型和 Amazon S3 儲存。

當您使用 `create-server` 命令為 Transfer Family AS2-enabled 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 VPC 端點至網際網路，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：

- VPC 的 ID（例如 `vpc-abcdef01`）。
- VPC 子網路 IDs（例如 `subnet-abcdef01`、`netnet-abcdef01`、`netnet-021345ab`）。
- 允許來自您交易合作夥伴 TCP 連接埠 5080 上傳入流量的安全群組的一或多個 IDs（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透過 VPN 連接到 VPC，則需要網際網路閘道。如需詳細資訊，請參閱「Amazon VPC 使用者指南」中的 [使用網際網路閘道連接至網際網路](#)。

建立 AS2-enabled 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）您可以將 VPC 端點設為公有。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 地址更新伺服器，然後再次啟動伺服器。

```
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 DNS 記錄，其中包含伺服器的公有 IP 地址。若要讓您的交易合作夥伴存取 伺服器，請為他們提供下列資訊。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

您提供給交易合作夥伴的完整 URL 如下：

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

- 若要測試是否可存取AS2-enabled伺服器，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，您會收到 HTTP 狀態碼 400（無效的請求）回應，因為您未傳送有效的 AS2 訊息。

- 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，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
```

- 如果您在 VPC 中連線，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 會將結構化 JSON 格式的訊息狀態記錄到 Amazon CloudWatch logs。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](#)。請記下您剛建立之 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故障診斷。

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

協議結合了兩個設定檔（本機和合作夥伴）、其憑證，以及允許雙方之間傳入 AS2 傳輸的伺服器組態。您可以執行下列命令來列出您的項目。

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

此步驟需要具有對儲存貯體之讀取/寫入存取權的 Amazon S3 儲存貯體和 IAM 角色。建立此角色的說明與 Transfer Family SFTP、FTP 和 FTPS 通訊協定相同，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：

- 存放 AS2 檔案的 Amazon S3 儲存貯體名稱（和物件字首，如有指定）。建議您為不同的檔案類型指定不同的目錄。
- 可存取儲存貯體之 IAM 角色的 ARN
- 您的 Transfer Family 伺服器 ID
- 您的設定檔 ID 和合作夥伴的設定檔 ID

將下列程式碼儲存到檔案中，例如 `agreementDetails.json`。將每個 *user input placeholder* 替換成您自己的資訊。

```
{
  "Description": "ExampleAgreementName",
  "ServerId": "your-server-id",
  "LocalProfileId": "your-profile-id",
  "PartnerProfileId": "your-partner-profile-id",
  "AccessRole": "arn:aws:iam::111111111111:role/TransferAS2AccessRole",
  "Status": "ACTIVE",
  "PreserveFilename": "ENABLED",
  "EnforceMessageSigning": "ENABLED",
  "CustomDirectories": {
    "FailedFilesDirectory": "/amzn-s3-demo-destination-bucket/AS2-failed",
    "MdnFilesDirectory": "/amzn-s3-demo-destination-bucket/AS2-mdn",
    "PayloadFilesDirectory": "/amzn-s3-demo-destination-bucket/AS2-payload",
    "StatusFilesDirectory": "/amzn-s3-demo-destination-bucket/AS2-status",
    "TemporaryFilesDirectory": "/amzn-s3-demo-destination-bucket/AS2-temp"
  }
}
```

Note

若要使用單一基礎目錄而非個別目錄，請從先前的程式碼中移除 `CustomDirectories` 該行及其個別目錄行，並改用下列參數：

`"BaseDirectory": "/amzn-s3-demo-destination-bucket/AS2-inbox"`

請勿同時使用基本目錄和個別目錄參數，否則命令將會失敗。

然後執行以下命令。

```
aws transfer create-agreement --cli-input-json file://agreementDetails.json
```

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：在您和合作夥伴之間建立連接器

此程序說明如何使用 建立 AS2 連接器 AWS CLI。如果您想要改用 Transfer Family 主控台，請參閱 [the section called “設定 AS2 連接器”](#)。

您可以使用 StartFileTransfer API 操作，透過連接器將存放在 Amazon S3 中的檔案傳送到交易合作夥伴的 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",
  "PreserveContentType": "FALSE",
  "SigningAlgorithm": "SHA256"
}
```

Note

對於 EncryptionAlgorithm，除非您必須支援需要的舊版用戶端，否則請勿指定 DES_EDE3_CBC 演算法，因為它是一種較弱的加密演算法。

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：使用 Transfer 系列測試透過 AS2 交換檔案

從您的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 地址的 DNS 名稱。子網域是您的 AWS Transfer Family 伺服器 ID（格式為 s-1234567890abcdef0）。以下列格式將您的伺服器 URL 提供給您的交易合作夥伴。

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

如果您未將公有彈性 IP 地址與 VPC 端點建立關聯，請查詢 VPC 端點的主機名稱，該端點可以透過連接埠 5080 上的交易合作夥伴 HTTP POST 接受 AS2 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 ID 為 vpce-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您的 VPC 內，才能存取您的 VPC 端點（例如透過 AWS PrivateLink 或 VPN）。以下列格式將您的 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，下列 URL 顯示先前命令中預留位置的範例值。

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

在此範例中，成功的傳輸會存放在您在 `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` 和的檔案 `myfile2.txt`，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 `/amzn-s3-demo-destination-bucket/AS2-inbox/processed/myfile1.messageId.txt` 和 `/amzn-s3-demo-destination-bucket/AS2-inbox/processed/myfile2.messageId.txt`。

如果您在建立 Transfer Family 伺服器時設定記錄角色，您也可以檢查 CloudWatch 日誌是否有 AS2 訊息的狀態。

將檔案傳送至您的交易合作夥伴

您可以使用 Transfer Family 透過參考連接器 ID 和檔案路徑來傳送 AS2 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 "/amzn-s3-demo-source-bucket/myfile1.txt" "/amzn-s3-demo-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 IDs、URLs 和 Amazon Resource Name (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 MDN 檔案，確認合作夥伴已成功收到檔案。這些檔案是根據中所述的慣例命名 [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。

教學課程：設定基本 Transfer Family Web 應用程式

本教學課程會逐步解說如何設定 Transfer Family Web 應用程式。Transfer Family Web 應用程式可啟用簡單的界面，透過 Web 瀏覽器在 Amazon S3 之間來回傳輸資料。如需此功能的詳細文件，請參閱 [Transfer Family Web 應用程式](#)。

Web 應用程式教學課程：先決條件

- 建立的帳戶執行個體或組織執行個體 AWS IAM Identity Center。如需詳細資訊，請參閱 [為 Transfer Family Web 應用程式設定您的身分提供者](#)。

如果您不是使用 IAM Identity Center 做為身分提供者，會將 [Okta 整合為 Web 應用程式的身分提供者](#) 說明如何使用替代（在此案例中為 Okta）身分提供者。

- 您需要使用 Amazon S3 儲存貯體來與 Transfer Family Web 應用程式互動。如需詳細資訊，請參閱 [設定 Amazon S3 儲存貯體](#)

Note

本教學假設您使用身分提供者的 IAM Identity Center 目錄，如果不是這種情況，請在繼續本教學課程 [為 Transfer Family Web 應用程式設定您的身分提供者](#) 之前參閱。

完成教學課程後，您的使用者可以登入並與您建立的 Web 應用程式互動。

步驟 1：建立必要的支援資源

您需要將使用者新增至 IAM Identity Center 目錄。您也需要兩個角色：一個用於做為 Web 應用程式的身分持有者角色，第二個用於設定 Amazon S3 存取授權。在本教學課程中，我們允許 AWS 服務為我們建立這些角色。

若要新增使用者

1. 登入 AWS 管理主控台 並在 <https://console.aws.amazon.com/singlesignon/> 開啟 AWS IAM Identity Center 主控台。
2. 從左側導覽窗格中，選擇使用者。
3. 選擇新增使用者並指定使用者詳細資訊。

指定使用者名稱、電子郵件地址和其他必要資訊。您可以選擇向使用者傳送電子郵件，其中包含設定其密碼的指示，也可以產生一次性密碼來與他們共用。

4. 選擇下一步，並選擇性地將新使用者指派給一或多個群組。
5. 選擇下一步並檢閱您的選擇。

如果一切看起來都不錯，請選擇新增使用者，使用您指定的詳細資訊建立新使用者。

在本教學課程中，範例使用者為 Bob Stiles、使用者名稱公告和電子郵件地址 bobstiles@example.com。

步驟 2：建立 Transfer Family Web 應用程式

建立 Transfer Family Web 應用程式

1. 登入 AWS 管理主控台 並在 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
2. 在左側導覽窗格中，選擇 Web 應用程式。
3. 選擇建立 Web 應用程式。

對於身分驗證存取，請注意，服務會自動尋找您設定為先決條件的 AWS IAM Identity Center 執行個體。

4. 在許可類型窗格中，選取建立並使用新的服務角色。服務會為您建立身分承載角色。身分承載角色在其工作階段中包含已驗證使用者的身分。
5. 在 Web 應用程式單位窗格中，接受預設值 1，或視需要調整為較高的值。
6. 新增標籤以協助您組織 Web 應用程式。在教學課程中，輸入金鑰的名稱，並為值輸入教學課程 Web 應用程式的名稱。

Tip

您可以在建立 Web 應用程式清單頁面直接編輯 Web 應用程式名稱。

7. 選擇下一步以開啟設計 Web 應用程式頁面。在此畫面上，提供下列資訊。

您可以選擇性地為您的 Web 應用程式提供標題。您也可以上傳標誌和 favicon 的影像檔案。

- 針對頁面標題，自訂使用者連線至 Web 應用程式時看到的瀏覽器索引標籤標題。如果您未輸入頁面標題的任何內容，則預設為 Transfer Web App。

- 對於標誌，請上傳映像檔案。標誌影像的檔案大小上限為 50 KB。
- 針對 favicon，上傳映像檔案。Favicon 的檔案大小上限為 20 KB。

8. 選擇下一步，然後選擇建立 Web 應用程式。

若要提供品牌體驗，您可以為使用者提供自訂 URL，以存取 Transfer Family Web 應用程式。如需詳細資訊，請參閱[使用自訂 URL 更新您的存取端點](#)。

步驟 3：設定儲存貯體的跨來源資源共用 (CORS)

您必須為 Web 應用程式使用的所有儲存貯體設定跨來源資源共用 (CORS)。CORS 組態是定義規則的文件，用於識別您允許存取儲存貯體的原始伺服器。如需 CORS 的詳細資訊，請參閱[設定跨來源資源共用 \(CORS\)](#)。

為您的 Amazon S3 儲存貯體設定跨來源資源共用 (CORS)

1. 登入 AWS 管理主控台，並在 <https://console.aws.amazon.com/s3/>：// 開啟 Amazon S3 主控台。
2. 從左側導覽面板中選擇儲存貯體，然後在搜尋對話方塊中搜尋儲存貯體，然後選擇許可索引標籤。
3. 在跨來源資源共用 (CORS) 中，選擇編輯並貼上下列程式碼。將 *AccessEndpoint* 取代為 Web 應用程式的實際存取端點。請勿輸入結尾斜線，因為當使用者嘗試登入您的 Web 應用程式時，這樣做會導致錯誤。
 - 不正確的範例：<https://webapp-c7bf3423.transfer-webapp.us-east-2.on.aws/>
 - 正確的範例：<https://webapp-c7bf3423.transfer-webapp.us-east-2.on.aws>

如果您要為多個 Web 應用程式重複使用儲存貯體，請將其 Web 應用程式存取端點附加至 AllowedOrigins 清單。

```
[
  {
    "AllowedHeaders": [
      "*"
    ],
    "AllowedMethods": [
      "GET",
      "PUT",
      "POST",
      "DELETE",
```



```
    "HEAD",
  ],
  "AllowedOrigins": [
    "https://AccessEndpoint"
  ],
  "ExposeHeaders": [
    "last-modified",
    "content-length",
    "etag",
    "x-amz-version-id",
    "content-type",
    "x-amz-request-id",
    "x-amz-id-2",
    "date",
    "x-amz-cf-id",
    "x-amz-storage-class",
    "access-control-expose-headers"
  ],
  "MaxAgeSeconds": 3000
}
]
```

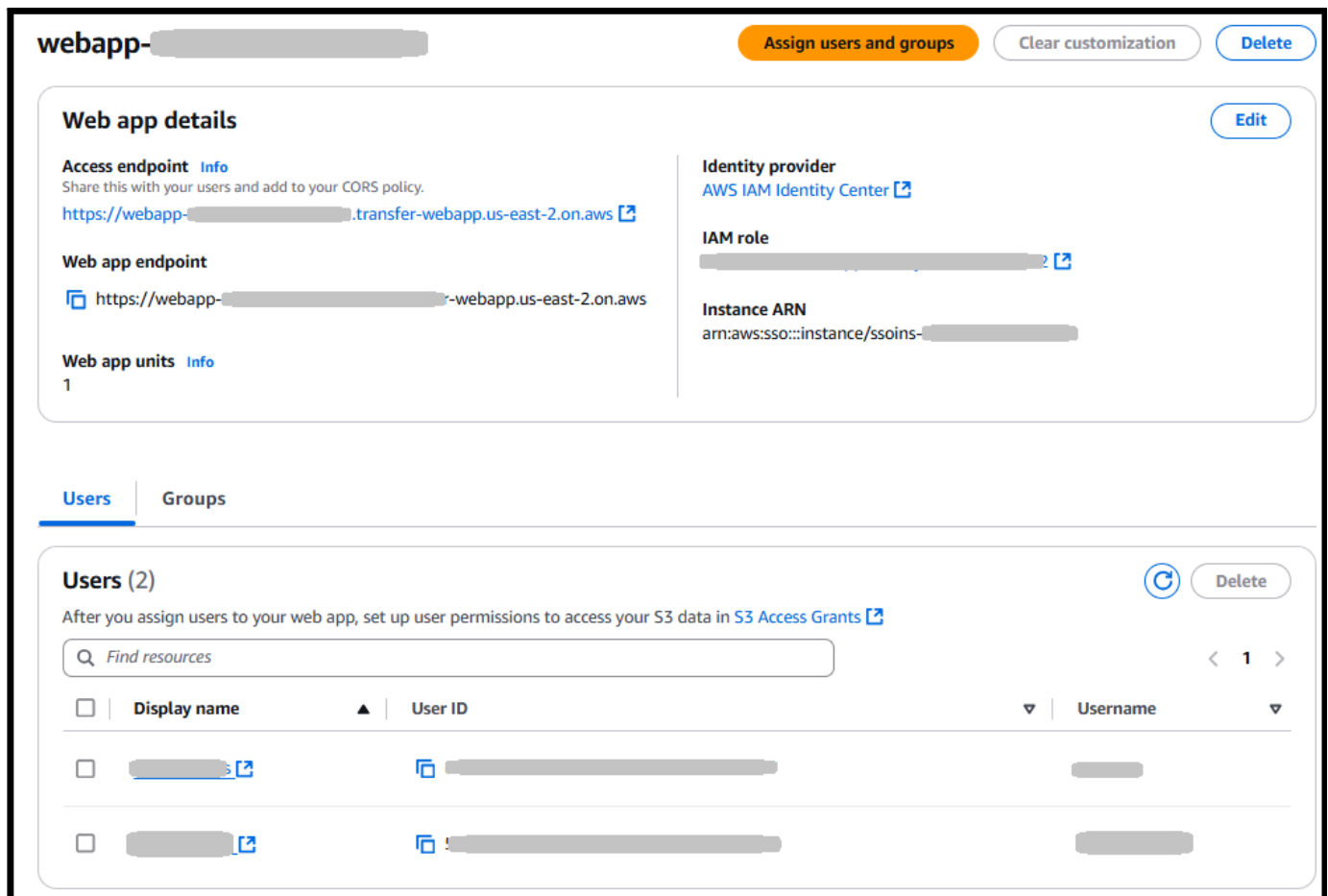
4. 選擇儲存變更以更新 CORS。

步驟 4：將使用者新增至 Transfer Family Web 應用程式

新增您先前在 IAM Identity Center 中建立的使用者。

將使用者指派給 Transfer Family Web 應用程式

1. 導覽至您先前建立的 Web 應用程式。
2. 選擇指派使用者和群組。



3. 若要指派您先前在 IAM Identity Center 中建立的使用者，請選取指派現有的使用者和群組，然後選取下一步。
 - a. 依顯示名稱搜尋使用者。請注意，在您開始輸入搜尋條件之前，不會顯示任何使用者。若要新增 **Bob Stiles**，請在搜尋方塊中輸入 bob。如果您找不到您的使用者，請導覽至 IAM Identity Center 管理主控台、尋找使用者，然後在此處複製並貼上其顯示名稱。
 - b. 選擇 **Bob Stiles** 使用者，然後選擇指派。

步驟 5：在 Amazon S3 中註冊位置並建立存取授權

將使用者指派給 Web 應用程式後，您需要註冊儲存貯體並為該使用者建立存取授權。

Note

您必須先擁有 S3 Access Grants 執行個體，才能繼續。如需詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的[建立 S3 存取授權執行個體](#)。

註冊位置並建立存取授權

1. 登入 AWS 管理主控台，並在 <https://console.aws.amazon.com/s3/>：// 開啟 Amazon S3 主控台。
2. 從左側導覽窗格中選擇存取授權。
3. 選擇檢視詳細資訊，以查看 S3 Access Grants 執行個體的詳細資訊。
4. 選取位置索引標籤，然後選擇註冊位置。
5. 請提供下列資訊。
 - 對於範圍，瀏覽儲存貯體或輸入儲存貯體的名稱，並選擇性地輸入字首。請注意，範圍開頭為字串 **s3://**。
 - 針對 IAM 角色，選擇建立新角色，讓 Amazon S3 建立角色。此角色允許 S3 Access Grants 存取您指定的位置範圍。

Amazon S3 > Access Grants > US East (N. Virginia) us-east-1: default > Register location

Register location [Info](#)

Registering a location for S3 your S3 Access Grants instance assigns an IAM role the permission to get temporary credentials to access resources within the specified scope.

Location [Info](#)

Location scope [Info](#)

You can't edit the location scope after registering the location.

Scope

[View](#) [Browse S3](#)

Format for all buckets: s3://
Format for bucket: s3://<bucket>
Format for prefix: s3://<bucket>/<prefix-with-path>

Permissions

This IAM role allows S3 Access Grants to access your specified location scope.

To ensure the role has proper permissions to access the location scope, consult the [list of permissions](#).

IAM role [Info](#)

This IAM role allows S3 Access Grants to access your specified location scope.

☒ Create new role

☐ Choose from existing IAM roles

☐ Enter IAM role ARN

[Cancel](#) [Register location](#)

選擇註冊位置以繼續。

6. 選取授予索引標籤，然後選擇建立授予，並提供下列詳細資訊。
 - 針對位置，選取瀏覽位置，然後選擇您在上一個步驟中註冊的位置。
 - 對於 Subprefix，輸入 * 以指出存取授權會套用至整個儲存貯體。

- 針對許可，選取讀取和寫入。
- 針對承授者類型，從 IAM Identity Center 選擇目錄身分。
- 針對目錄身分類型，選取使用者。
- 在 IAM Identity Center 使用者/ID 中，複製並貼上的使用者 ID **Bob Stiles**。此 ID 可在 Transfer Family Web 應用程式的使用者窗格中取得。

7. 選擇建立授予。

存取授權已建立。

步驟 6：以使用者身分存取 Transfer Family Web 應用程式

現在，我們會導覽至 Web 應用程式的 URL，並以先前指派的使用者身分登入。

登入 Transfer Family Web 應用程式

1. 導覽至您的 Web 應用程式
2. 從 Web 應用程式詳細資訊窗格中選擇存取端點。

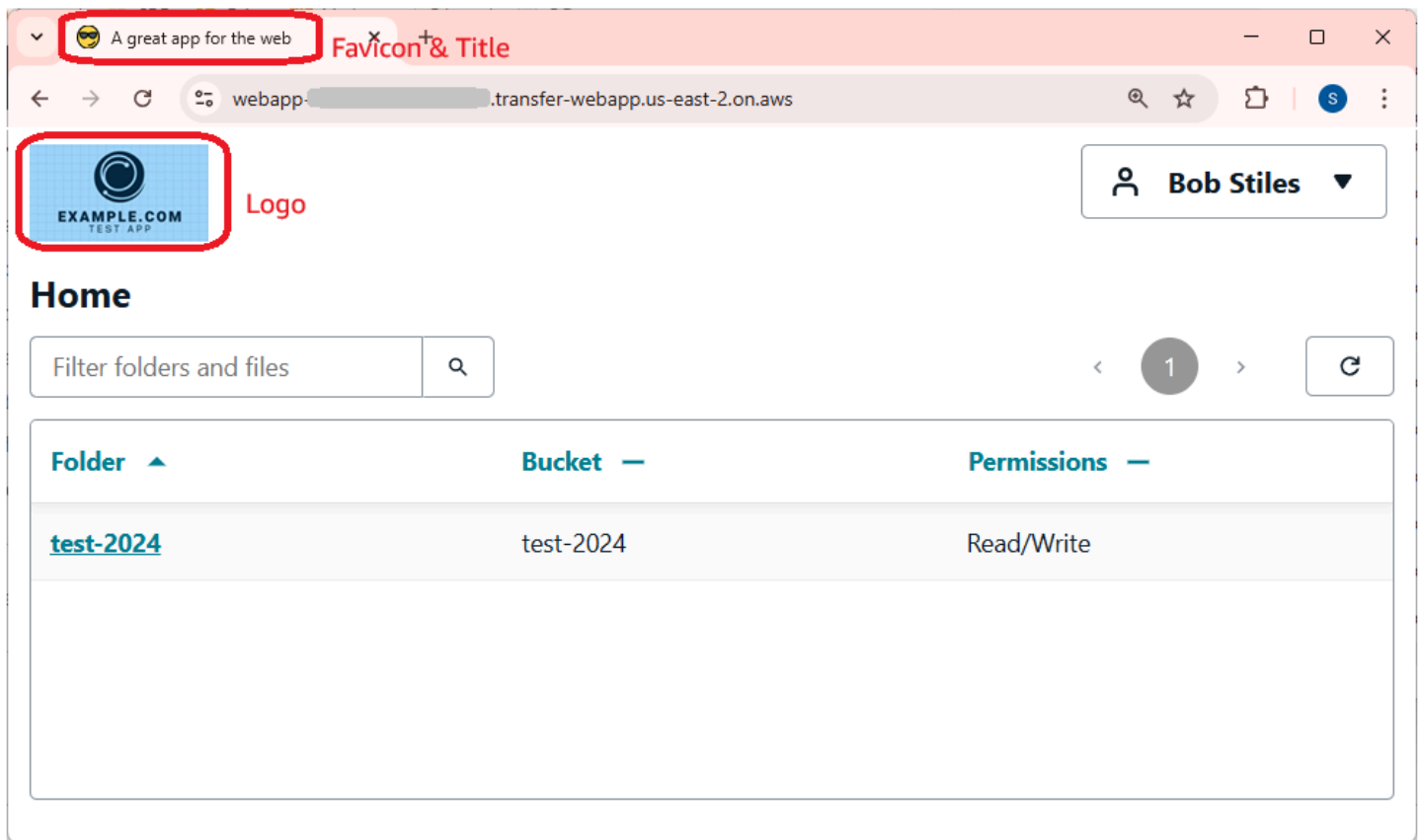
The screenshot shows the AWS IAM Identity Center console interface. At the top, there's a header for a web application named 'webapp-'. It includes buttons for 'Assign users and groups', 'Clear customization', and 'Delete'. Below this is a 'Web app details' section with an 'Edit' button. The 'Access endpoint' is highlighted with a red box and contains the URL 'https://webapp-.transfer-webapp.us-east-2.on.aws'. Other details include the 'Identity provider' (AWS IAM Identity Center), 'IAM role' (AWSTransferWebAppIdentityBearer-us-east-2), and 'Instance ARN'. Below the details is a 'Users' tab with a 'Users (1)' section. A table lists the assigned user, 'Bob Stiles', with a red box highlighting the row. The table has columns for 'Display name', 'User ID', and 'Username'.

Display name	User ID	Username
Bob Stiles		bobstiles

3. 在登入畫面上，輸入您建立的使用者 **bobstiles**，然後選取下一步。

4. 輸入系統在建立時指派給此使用者的密碼，然後選取下一步。
5. 如果您的組織需要多重要素驗證 (MFA)，則需要立即設定。如果沒有，請跳到步驟 6。
 - a. 您會收到註冊 MFA 裝置的畫面。選擇其中一個可用的選項，然後選取下一步。
 - b. 執行為此使用者設定 MFA 的必要步驟：這些步驟取決於您選擇的 MFA 選項。
 - c. 您可能需要為使用者設定新密碼：如果需要，請現在執行此操作。系統也可能要求您使用設定的新 MFA 登入資料再次登入。

您的使用應該會看到類似以下的畫面。請注意，此螢幕擷取畫面包含 favicon 和標誌的自訂。



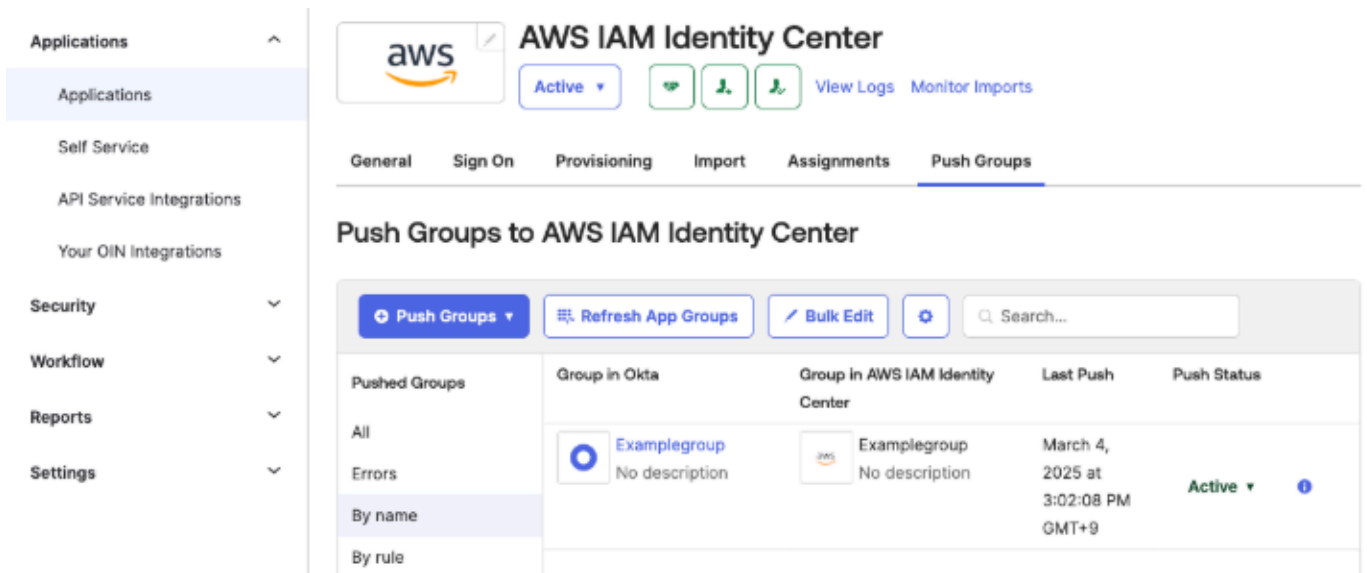
後續步驟

您已成功設定具有標準 S3 儲存貯體存取的基本 Transfer Family Web 應用程式。如果您需要更精細地控制儲存貯體許可，例如允許使用者從一個儲存貯體下載並上傳到另一個儲存貯體，請參閱 [教學課程：設定具有選擇性多儲存貯體存取權的 AWS Transfer Family Web 應用程式](#)。

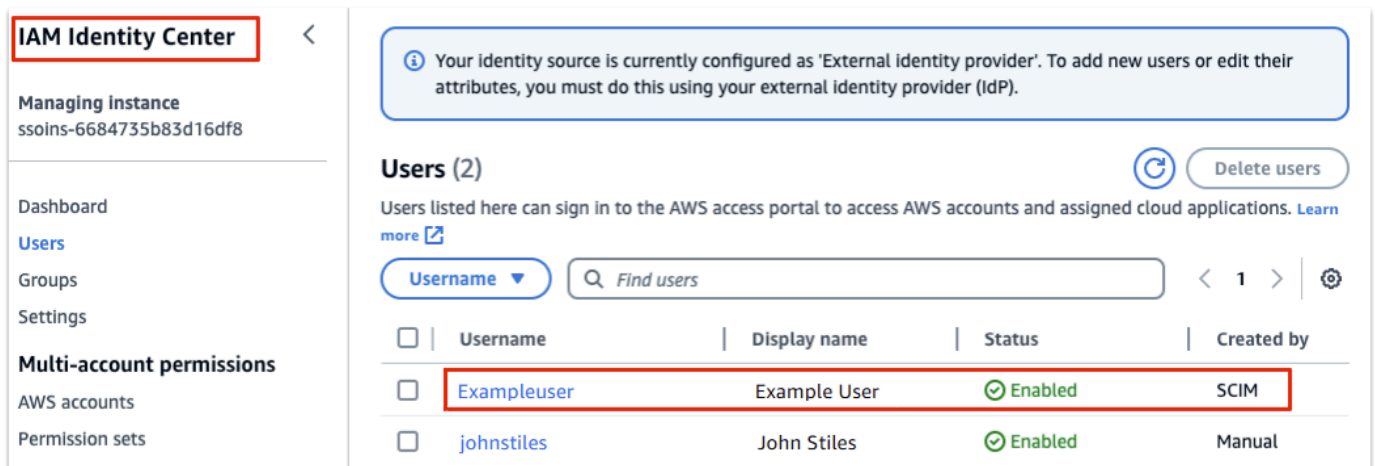
將 Okta 整合為 Web 應用程式的身分提供者

您可以將外部身分提供者與 Transfer Family Web 應用程式整合。本節說明如何將 Okta 設定為您的身分提供者。

1. 在 Okta 中，建立使用者、群組和應用程式。如需如何執行此操作的詳細資訊，請參閱[使用 Okta 和 IAM Identity Center 設定 SAML 和 SCIM](#)。



2. 連接 Okta 並從 Okta 匯入使用者和群組 AWS IAM Identity Center。請遵循[使用 Okta 和 IAM Identity Center 設定 SAML 和 SCIM 中的步驟 1–4](#)。



IAM Identity Center

Managing instance
ssoins-6684735b83d16df8

Dashboard
Users
Groups
Settings

Multi-account permissions
AWS accounts
Permission sets

Information: Your identity source is currently configured as 'External identity provider'. To add new groups or edit their memberships, you must do this using your external identity provider.

Groups (2) Refresh Delete group

With groups, you can grant or deny permissions to groups of workforce users, rather than having to apply those permissions to each user. [Learn more](#)

Find groups by group name

☐	Group name	Users	Description	Created by
☐	Examplegroup	1 user	-	SCIM
☐	dev	1 user	-	Manual

3. 確認 IAM Identity Center 中的身分來源是 SAML 2.0。

Settings

Details

Configure your identity source and multi-factor authentication settings for use when managing access to your AWS accounts, resources, and cloud applications.

Instance name - Edit [redacted]	Instance ID ssoins-[redacted]	Organization ID AWS Organizations not enabled
Region US East (Ohio) us-east-2	Date created Thursday, November 14, 2024 at 4:11:19 PM EST	Instance ARN arn:aws:sso:::instance/ssoins-[redacted]

Identity source | Authentication | Management | Tags

Identity source Actions

Choose the directory where you want to manage your users and groups. [Learn More](#)

Identity source
External identity provider

Authentication method SAML 2.0	Provisioning method SCIM

AWS access portal URL
[https://\[redacted\].awsapps.com/start](#)

Identity store ID
[d-\[redacted\]](#)

Issuer URL
[https://identitycenter.amazonaws.com/ssoins-\[redacted\]](#)

4. 指派您的使用者和群組，如中所述[步驟 4：將使用者新增至 Transfer Family Web 應用程式](#)。

5. 若要避免您的使用者在登入 Web 應用程式時需要使用 MFA，請在 Okta 中執行下列步驟。
 - a. 從 Okta 管理員主控台存取 **【應用程式】 - 【應用程式】**，然後選取 AWS IAM Identity Center 應用程式。
 - b. 在登入索引標籤上，選取 **【使用者身分驗證】 - 編輯**。
 - c. 僅選取密碼。

在您執行教學課程的所有其他步驟之後，您的使用者應該可以透過在 Web 瀏覽器中導覽至 Web 應用程式的存取端點來存取 Transfer Family Web 應用程式。

教學課程：設定具有選擇性多儲存貯體存取權的 AWS Transfer Family Web 應用程式

本教學課程將引導您為單一使用者設定具有特定 Amazon S3 儲存貯體許可的 Transfer Family Web 應用程式。您將了解如何設定解決方案，允許使用者從一個儲存貯體下載並上傳至另一個儲存貯體，同時維護安全性。這是進階教學課程，以基本教學課程涵蓋的概念為基礎。如果您是初次使用 AWS Transfer Family Web 應用程式，請考慮從 [開始教學課程：設定基本 Transfer Family Web 應用程式](#)。

先決條件

在開始本教學課程之前，需要滿足以下條件：

- 在與 AWS Transfer Family Web 應用程式相同的區域中設定的 IAM Identity Center。請注意，AWS 對於所有區域，每個 AWS 帳戶僅允許一個 IAM Identity Center 執行個體。
- 在 IAM Identity Center 中至少設定一個使用者。
- 兩個 S3 儲存貯體：一個用於下載，另一個用於上傳。

Note

本教學課程與基本 Web 應用程式教學課程共用許多先決條件。如需設定 IAM Identity Center 和建立使用者的詳細資訊，請參閱 [教學課程：設定基本 Transfer Family Web 應用程式](#)。

步驟 1：建立 Transfer Family Web 應用程式

建立 Transfer Family Web 應用程式

1. 登入 AWS 管理主控台 並在 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
2. 在左側導覽窗格中，選擇 Web 應用程式。
3. 選擇建立 Web 應用程式。

對於身分驗證存取，請注意，服務會自動尋找您設定為先決條件的 AWS IAM Identity Center 執行個體。

4. 在許可類型窗格中，選取建立並使用新的服務角色。服務會為您建立身分承載角色。身分承載角色在其工作階段中包含已驗證使用者的身分。
5. 在 Web 應用程式單位窗格中，接受預設值 1，或視需要調整為較高的值。
6. 新增標籤以協助您組織 Web 應用程式。在教學課程中，輸入金鑰的名稱，並為值輸入教學課程 Web 應用程式的名稱。

Tip

您可以在建立 Web 應用程式清單頁面直接編輯 Web 應用程式名稱。

7. 選擇下一步以開啟設計 Web 應用程式頁面。在此畫面上，提供下列資訊。

您可以選擇性地為您的 Web 應用程式提供標題。您也可以上傳標誌和 favicon 的影像檔案。

- 針對頁面標題，自訂使用者連線至 Web 應用程式時看到的瀏覽器索引標籤標題。如果您未輸入頁面標題的任何內容，則預設為 Transfer Web App。
- 對於標誌，請上傳映像檔案。標誌影像的檔案大小上限為 50 KB。
- 針對 favicon，上傳映像檔案。Favicon 的檔案大小上限為 20 KB。

8. 選擇下一步，然後選擇建立 Web 應用程式。

步驟 2：設定 S3 存取的 IAM 角色

您需要建立兩個 IAM 角色：一個只能下載存取第一個儲存貯體，另一個只能上傳存取第二個儲存貯體。

兩個角色的信任政策

針對兩個 IAM 角色使用以下信任政策：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AccessGrantsTrustPolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "access-grants.s3.amazonaws.com"
      },
      "Action": [
        "sts:AssumeRole",
        "sts:SetSourceIdentity",
        "sts:SetContext"
      ]
    }
  ]
}
```

下載儲存貯體的 IAM 政策

使用下列政策建立 IAM 角色，以唯讀存取您的下載儲存貯體：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ObjectLevelReadPermissions",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetObjectVersionAcl",
        "s3:ListMultipartUploadParts",
        "s3:ListBucket"
      ]
    }
  ],
}
```

```

        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket1/*",
            "arn:aws:s3:::amzn-s3-demo-bucket1"
        ]
    }
}

```

Important

以下載儲存貯體的實際名稱取代 amzn-s3-demo-bucket1。

上傳儲存貯體的 IAM 政策

使用下列政策建立另一個 IAM 角色，以寫入存取您的上傳儲存貯體：

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ObjectLevelWritePermissions",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutObjectVersionAcl",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:AbortMultipartUpload",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket2/*",
        "arn:aws:s3:::amzn-s3-demo-bucket2"
      ]
    }
  ]
}

```

 Important

使用上傳儲存貯體的實際名稱取代 amzn-s3-demo-bucket2。

步驟 3：設定 S3 存取授權

1. 在開啟 S3 主控台 <https://console.aws.amazon.com/s3/>。
2. 在導覽窗格中，選擇存取授權。
3. 按一下建立 S3 存取授權執行個體。
4. 選取新增 IAM Identity Center 執行個體選項，然後輸入身分中心執行個體 ARN。
5. 按一下下一步，然後按一下取消以完成建立 S3 Access Grants 執行個體，而不繼續進行其他步驟。

此步驟會建立 S3 Access Grants 執行個體。您現在將註冊位置並建立存取授權。

步驟 4：註冊 S3 儲存貯體位置

使用 S3 Access Grants 將兩個 S3 儲存貯體註冊為位置：

1. 在 S3 Access Grants 主控台中，導覽至位置並按一下註冊位置。
2. 在位置範圍下，選擇特定 S3 儲存貯體進行下載 (amzn-s3-demo-bucket1)。
3. 當系統提示您選擇 IAM 角色時，請選取您先前建立的下載 IAM 角色。
4. 完成註冊程序。
5. 重複此程序以註冊上傳儲存貯體 (amzn-s3-demo-bucket2)，並在出現提示時選取上傳 IAM 角色。

步驟 5：建立存取授權

建立兩個授與，每個註冊的位置各一個：

1. 在 S3 存取授權主控台中，導覽至授權，然後按一下建立授權。
2. 在位置中，按一下瀏覽位置，然後選取下載儲存貯體位置 (amzn-s3-demo-bucket1)。
3. 在子字首（選用）中，輸入 * 以允許存取整個儲存貯體，或指定類似的路徑 folder1/folder2/* 來限制對特定字首的存取。

使用 會將授予範圍*設定為 `s3://bucket-name/*`，允許存取整個儲存貯體。若要僅允許存取特定字首，請輸入類似的路徑 `folder1/folder2/*`，這會將授予範圍設定為 `s3://bucket-name/folder1/folder2/*`。

4. 在許可和存取下，選取下載儲存貯體的讀取。
5. 在承授者類型中，從 IAM Identity Center 選擇目錄身分。
6. 針對 IAM 主體類型，選取使用者，然後輸入 IAM Identity Center 使用者的使用者 ID。
7. 完成授予建立程序。
8. 重複此程序為上傳儲存貯體 (amzn-s3-demo-bucket2) 建立授予，但為許可選取讀寫。

步驟 6：設定 S3 儲存貯體的 CORS 政策

設定兩個 S3 儲存貯體的 CORS 政策，以允許透過 AWS Transfer Family WebApp 存取：

1. 開啟 S3 主控台並導覽至您的下載儲存貯體 (amzn-s3-demo-bucket1)。
2. 選取許可索引標籤。
3. 向下捲動至跨來源資源共用 (CORS) 區段，然後按一下編輯。
4. 新增下列 CORS 組態，將 *WebAppEndpoint* 取代為您實際的 WebApp 端點 URL：

您可以在 WebApps 下的 AWS Transfer Family 主控台中找到您的 Web 應用程式端點 URL。WebApps 它看起來與 `https://webapp-*****.transfer-webapp.us-west-2.on.aws` 類似。

```
[
  {
    "AllowedHeaders": [
      "*"
    ],
    "AllowedMethods": [
      "GET",
      "PUT",
      "POST",
      "DELETE",
      "HEAD"
    ],
    "AllowedOrigins": [
      "https://WebAppEndpoint"
    ],
    "ExposeHeaders": [
```

```
        "last-modified",
        "content-length",
        "etag",
        "x-amz-version-id",
        "content-type",
        "x-amz-request-id",
        "x-amz-id-2",
        "date",
        "x-amz-cf-id",
        "x-amz-storage-class",
        "access-control-expose-headers"
    ],
    "MaxAgeSeconds": 3000
}
```

5. 按一下 Save changes (儲存變更)。
6. 重複上傳儲存貯體 (amzn-s3-demo-bucket2) 的程序。

步驟 7：測試組態

1. 開啟您的 AWS Transfer Family Web 應用程式 URL。您可以在 AWS Transfer Family 主控台的存取端點欄位的 WebApps 下找到此 URL。
2. 使用您使用存取授權設定的 IAM Identity Center 使用者憑證登入。
3. 登入後，您應該會在首頁上看到這兩個 S3 位置。
4. 導覽至下載儲存貯體 (amzn-s3-demo-bucket1)，並確認您可以下載檔案，但無法上傳。
5. 導覽至上傳儲存貯體 (amzn-s3-demo-bucket2)，並確認您可以上傳檔案。

結論

您已成功為單一使用者設定具有選擇性 S3 儲存貯體存取權的 AWS Transfer Family WebApp。此設定允許使用者從一個儲存貯體下載並上傳至另一個儲存貯體，同時透過 IAM 角色和 S3 Access Grants 維護安全性。

此方法可以透過為每個使用者在 S3 Access Grants 中建立額外的授權，以精細控制儲存貯體存取許可，進而擴展到多個使用者。如需基本 Web 應用程式設定的資訊，請參閱 [教學課程：設定基本 Transfer Family Web 應用程式](#)。

設定 SFTP、FTPS 或 FTP 伺服器端點

本主題提供使用一或多個 SFTP、FTPS 和 FTP 通訊協定建立和使用 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](#)
- [FTP 和 FTPS Network Load Balancer 考量事項](#)
- [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](#)
- [使用 Transfer 系列存取 FSx for NetApp ONTAP 檔案系統](#)

身分提供者選項

AWS Transfer Family 提供多種方法來驗證和管理使用者。下表比較您可以與 Transfer Family 搭配使用的可用身分提供者。

Action	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

Action	AWS Transfer Family 服務受管	AWS Managed Microsoft AD	Amazon API Gateway	AWS Lambda
邏輯主目錄	是	是	是	是
參數化存取（以使用者名稱為基礎）	是	是	是	是
臨機操作存取結構	是	否	是	是
AWS WAF	否	否	是	否

備註：

- IAM 用於控制 Amazon S3 後端儲存的存取，POSIX 用於 Amazon EFS。
- 臨機操作是指在執行時間傳送使用者設定檔的能力。例如，您可以透過將使用者名稱做為變數傳遞，將使用者登陸其主目錄中。
- 如需的詳細資訊 AWS WAF，請參閱 [新增 Web 應用程式防火牆](#)。
- 有一篇部落格文章說明使用與 Microsoft Entra ID（先前稱為 Azure AD）整合的 Lambda 函數做為 Transfer Family 身分提供者。如需詳細資訊，請參閱[AWS Transfer Family 使用 Azure Active Directory 向驗證和 AWS Lambda](#)。
- 我們提供數種 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，您可以建立啟用 SFTP 的伺服器、啟用 FTPS 的伺服器、啟用 FTP 的伺服器或 AS2-enabled 伺服器。

下一步驟

- [建立啟用 SFTP 的伺服器](#)
- [建立啟用 FTPS 的伺服器](#)
- [建立啟用 FTP 的伺服器](#)
- [設定 AS2](#)

AWS Transfer Family 端點類型矩陣

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

端點類型矩陣

特性	公有	VPC - 網際網路	VPC - 內部	VPC_Endpoint (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 VPC 中的任何特殊組態。	透過網際網路以及 VPC 和 VPC 連線環境內的，例如透過 Direct Connect 或 VPN 的現場部署資料中心。	從 VPC 和 VPC 連線環境內，例如透過 Direct Connect 或 VPN 的現場部署資料中心。	從 VPC 和 VPC 連線環境內，例如透過 Direct Connect 或 VPN 的現場部署資料中心。
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。這些可以是擁有 AWS 的 IP 地址或您自己的 IP 地址 (使用您自己的 IP 地址)。連接到端點的彈性 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 地址的允許清單。	若要允許依來源 IP 地址存取，您可以使用連接至伺服器端點	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	若要允許依來源 IP 地址存取，您可以使用連接至伺服器端點

特性	公有	VPC - 網際網路	VPC - 內部	VPC_Endpoint (已棄用)
	端點可公開存取，並接聽透過連接埠 22 的流量。  Note 對於 VPC 託管的端點，SFTP Transfer Family 伺服器可以透過連接埠 22 (預設值)、2222 或 22000 操作。	的安全群組，以及連接至端點所在子網路的網路 ACLs。	全群組，以及連接至端點所在子網路的網路存取控制清單 (網路 ACLs)。	的安全群組，以及連接至端點所在子網路的網路 ACLs。
用戶端防火牆允許清單	您必須允許伺服器的 DNS 名稱。 由於 IP 地址可能會有所變更，請避免將 IP 地址用於用戶端防火牆允許清單。	您可以允許伺服器的 DNS 名稱或連接到伺服器的彈性 IP 地址。	您可以允許私有 IP 地址或端點的 DNS 名稱。	您可以允許私有 IP 地址或端點的 DNS 名稱。

特性	公有	VPC - 網際網路	VPC - 內部	VPC_Endpoint (已棄用)
IP 地址類型	IPv4 (預設) 或 雙堆疊 (IPv4 和 IPv6)	僅限 IPv4 (不支 援雙堆疊)	IPv4 (預設) 或 雙堆疊 (IPv4 和 IPv6)	僅限 IPv4 (不支 援雙堆疊)

Note

VPC_ENDPOINT 端點類型現在已棄用，無法用於建立新伺服器。不使用 EndpointType=VPC_ENDPOINT，請使用 VPC 端點類型 (EndpointType=VPC)，您可以將其用作內部或網際網路面向，如上表所述。

- 如需棄用的詳細資訊，請參閱 [停止使用 VPC_ENDPOINT](#)。
- 如需管理 VPC 端點許可的資訊，請參閱 [限制 Transfer Family 伺服器的 VPC 端點存取](#)。

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

- 使用具有內部存取權的 VPC 端點，以便只有 VPC 或 VPC 連線環境中的用戶端才能存取伺服器，例如透過 Direct Connect 或 VPN 的現場部署資料中心。
- 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，僅允許來自託管使用者用戶端之特定 IP 地址的流量。
- 如果您需要密碼型身分驗證，並搭配伺服器使用自訂身分提供者，則最佳實務是密碼政策可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。這可以降低但不能消除連接埠掃描器和機器人探測伺服器的風險，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 NLB 的 IP 地址，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 SSH 進行檔案傳輸。如需詳細資訊，請參閱[the section called “建立啟用 SFTP 的伺服器”](#)。

Note

我們提供建立 SFTP Transfer Family 伺服器 AWS CDK 的範例。此範例使用 TypeScript，並可在 GitHub [上取得](#)。

- 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 “建立啟用 FTP 的伺服器”](#)。
- 適用性聲明 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 CloudFormation 堆疊以供示範之用。此程序說明於 [使用 範本建立示範 Transfer 系列 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，並且想要透過多個通訊協定使用相同的使用者名稱來提供存取權，只要身分提供者已設定特定於通訊協定的登入資料，您就可以這麼做。對於 FTP，我們建議您維護與 SFTP 和 FTPS 不同的登入資料。這是因為與 SFTP 和 FTPS 不同，FTP 會以純文字傳輸登入資料。透過從 SFTP 或 FTPS 隔離 FTP 憑證，如果共用或公開 FTP 憑證，則使用 SFTP 或 FTPS 的工作負載會保持安全。

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。除了指派一或多個通訊協定給伺服器之外，您也可以指派下列其中一種身分提供者類型：

- 使用 SSH 金鑰管理的服務。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 for Microsoft Active Directory](#)。
- 自訂身分提供者。Transfer Family 提供多種使用自訂身分提供者的選項，如 [使用自訂身分提供者](#) 主題所述。

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

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，並以金鑰/值對的標籤形式將中繼資料新增至伺服器。

Important

執行個體化伺服器和資料傳輸會產生成本。如需有關定價和 AWS 定價計算工具 用來取得使用 Transfer Family 之成本預估的資訊，請參閱 [AWS Transfer Family 定價](#)。

建立啟用 SFTP 的伺服器

Secure Shell (SSH) 檔案傳輸通訊協定 (SFTP) 是一種網路通訊協定，用於透過網際網路安全地傳輸資料。通訊協定支援 SSH 的完整安全性和身分驗證功能。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。

請注意下列事項

- Transfer Family 的 SFTP 伺服器透過連接埠 22 運作。對於 VPC 託管的端點，SFTP Transfer Family 伺服器也可以透過連接埠 2222、2223 或 22000 操作。如需詳細資訊，請參閱[在虛擬私有雲端中建立伺服器](#)。
- 公有端點無法透過安全群組限制流量。若要搭配 Transfer Family 伺服器使用安全群組，您必須在虛擬私有雲端 (VPC) 內託管伺服器的端點，如中所述[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，並可在 GitHub [上取得](#)。
- 如需如何在 VPC 內部署 Transfer Family 伺服器的逐步解說，請參閱[使用 IP 允許清單來保護您的 AWS Transfer Family 伺服器](#)。

建立啟用 SFTP 的伺服器

1. 在 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台，然後從導覽窗格中選取伺服器，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，選擇您要用來管理使用者存取的身分提供者。您有下列選項：
 - 服務受管 – 您可以將使用者身分和金鑰存放在其中 AWS Transfer Family。
 - AWS Directory Service for Microsoft Active Directory – 您提供一個 Directory Service 目錄來存取端點。如此一來，您就可以使用儲存在 Active Directory 中的登入資料來驗證您的使用者。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 for Microsoft Active Directory](#)。

Note

- 不支援跨帳戶和共用目錄 AWS Managed Microsoft AD。
 - 若要使用 Directory Service 做為您的身分提供者來設定伺服器，您需要新增一些 Directory Service 許可。如需詳細資訊，請參閱[在您開始使用之前 AWS Directory Service for Microsoft Active Directory](#)。
- 自訂身分提供者 – 選擇下列其中一個選項：
 - 使用 AWS Lambda 連接您的身分提供者 – 您可以使用 Lambda 函數支援的現有身分提供者。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 連接您的身分提供者 – 您可以建立由 Lambda 函數支援的 API Gateway 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





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. 選擇下一步。

5. 在選擇端點中，執行下列動作：

- 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](#)。
- 對於 IP 地址類型，請選擇 IPv4（預設）以獲得回溯相容性，或選擇雙堆疊來啟用 IPv4 和 IPv6 連線至您的端點。

 Note

雙堆疊模式可讓您的 Transfer Family 端點與啟用 IPv4 和 IPv6 的用戶端通訊。這可讓您逐步從 IPv4 轉換到 IPv6 型系統，而不需要一次全部切換。

- c. (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](#)。

- d. (選用) 對於啟用 FIPS，選取啟用 FIPS 端點核取方塊，以確保端點符合聯邦資訊處理標準 (FIPS)。

 Note

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

- e. 選擇下一步。

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

- 選擇 Amazon S3 以儲存和存取檔案，做為所選通訊協定的物件。
- 選擇 Amazon EFS，透過選取的通訊協定在 Amazon EFS 檔案系統中存放和存取您的檔案。

選擇下一步。

7. 在設定其他詳細資訊中，執行下列動作：

- a. 針對記錄，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，則必須選取與您的相關聯的日誌群組 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 [CloudWatch Logs 中建立日誌群組](#)。

- 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，選擇安全政策，其中包含啟用供伺服器使用的密碼編譯演算法。我們最新的安全政策是預設值：如需詳細資訊，請參閱 [AWS Transfer Family 伺服器的安全政策](#)。

- d. (選用) 對於伺服器主機金鑰，輸入 RSA、ED25519 或 ECDSA 私有金鑰，用於在用戶端透過 SFTP 連線到伺服器時識別伺服器。您也可以新增描述，以區分多個主機金鑰。

建立伺服器之後，您可以新增其他主機金鑰。如果您想要輪換金鑰，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。

- e. (選用) 對於標籤，對於索引鍵和值，輸入一或多個標籤做為索引鍵/值對，然後選擇新增標籤。
- f. 選擇下一步。
- g. 您可以最佳化 Amazon S3 目錄的效能。例如，假設您進入主目錄，而且您有 10,000 個子目錄。換句話說，Amazon 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。

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

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，在驗證前顯示橫幅文字方塊中，輸入您要在使用者驗證之前向他們顯示的文字訊息。
- 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](#) 中的 SetStatOption 文件。

- TLS 工作階段恢復：只有在您已啟用 FTPS 做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 做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

i 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

i 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項目，請選擇步驟旁的編輯。

i 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。

在新伺服器的狀態變更為線上之前，可能需要幾分鐘的時間。此時，您的伺服器可以執行檔案操作，但您必須先建立使用者。如需建立使用者的詳細資訊，請參閱 [管理伺服器端點的使用者](#)。

建立啟用 FTPS 的伺服器

透過 SSL 的檔案傳輸通訊協定 (FTPS) 是 FTP 的延伸。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。

Note

如需 Network Load Balancer 的重要考量，請參閱 [避免將 NLBs 和 NATs 放在 AWS Transfer Family 伺服器前面](#)。

建立啟用 FTPS 的伺服器

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

對於伺服器憑證，選擇存放在 AWS Certificate Manager (ACM) 中的憑證，當用戶端透過 FTPS 連線到伺服器時，該憑證將用於識別您的伺服器，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 AWS Certificate Manager 《使用者指南》中的 [將憑證匯入 ACM](#)。

若要透過私有 IP 地址請求私有憑證以使用 FTPS，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，並包含發行者的相關資訊。

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

- AWS Directory Service for Microsoft Active Directory – 您提供 Directory Service 目錄來存取端點。如此一來，您就可以使用儲存在 Active Directory 中的登入資料來驗證您的使用者。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 for Microsoft Active Directory](#)。

 Note

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

- 自訂身分提供者 – 選擇下列其中一個選項：
 - 使用 AWS Lambda 連接您的身分提供者 – 您可以使用 Lambda 函數支援的現有身分提供者。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 連接您的身分提供者 – 您可以建立由 Lambda 函數支援的 API Gateway 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

To choose an authentication method, enable SFTP as one of the protocols selected in Step 1

Cancel

Previous

Next

4. 選擇下一步。
5. 在選擇端點中，執行下列動作：

Note

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

- a. 針對端點類型，選擇 VPC 託管端點類型以託管伺服器的端點。如需設定 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) 對於啟用 FIPS，選取啟用 FIPS 端點核取方塊，以確保端點符合聯邦資訊處理標準 (FIPS)。

 Note

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

- c. 選擇下一步。

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，將檔案儲存和存取為所選通訊協定的物件。
- 選擇 Amazon EFS，透過選取的通訊協定在 Amazon EFS 檔案系統中存放和存取您的檔案。

選擇下一步。

7. 在設定其他詳細資訊中，執行下列動作：

- a. 針對記錄，請指定現有的日誌群組或建立新的日誌群組（預設選項）。

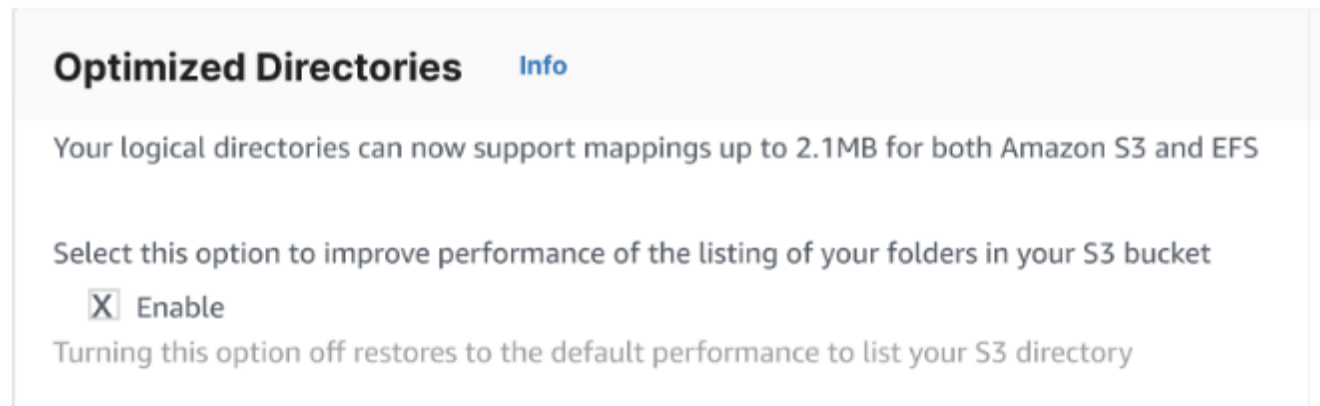
如果您選擇建立日誌群組，CloudWatch 主控台 (<https://console.aws.amazon.com/cloudwatch/>：//) 會開啟建立日誌群組頁面。如需詳細資訊，請參閱在 [CloudWatch Logs 中建立日誌群組](#)。

- 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，選擇安全政策，其中包含啟用供伺服器使用的密碼編譯演算法。我們最新的安全政策是預設值：如需詳細資訊，請參閱 [AWS Transfer Family 伺服器的安全政策](#)。

- d. 對於伺服器主機金鑰，請保留空白。
- e. (選用) 對於標籤，對於索引鍵和值，輸入一個或多個標籤作為索引鍵/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，而且您有 10,000 個子目錄。換句話說，Amazon 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。

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



- g. 選擇下一步。
- h. (選用) 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日訊息 (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給他們的文字訊息，然後在驗證後顯示橫幅文字方塊中，輸入您希望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：提供一種機制，可在 FTPS 工作階段的控制和資料連線之間繼續或共用交涉的私密金鑰。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。

在新伺服器的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。

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

Note

如需 Network Load Balancer 的重要考量，請參閱 [避免將 NLBs 和 NATs 放在 AWS Transfer Family 伺服器前面](#)。

建立啟用 FTP 的伺服器

1. 在 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台，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。
3. 在選擇身分提供者中，選擇您要用來管理使用者存取的身分提供者。您有下列選項：
 - AWS Directory Service for Microsoft Active Directory – 您提供 Directory Service 目錄來存取端點。如此一來，您就可以使用儲存在 Active Directory 中的登入資料來驗證您的使用者。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 for Microsoft Active Directory](#)。

Note

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

- 自訂身分提供者 – 選擇下列其中一個選項：

- 使用 AWS Lambda 連接您的身分提供者 – 您可以使用 Lambda 函數支援的現有身分提供者。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 連接您的身分提供者 – 您可以建立由 Lambda 函數支援的 API Gateway 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

To choose an authentication method, enable SFTP as one of the protocols selected in Step 1

Cancel

Previous

Next

4. 選擇下一步。
5. 在選擇端點中，執行下列動作：

 Note

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

- a. 針對端點類型，選擇託管的 VPC 來託管伺服器的端點。如需設定 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. 對於啟用 FIPS，保持 FIPS 啟用端點核取方塊清除。

 Note

FTP 伺服器不支援啟用 FIPS 的端點。

- c. 選擇下一步。

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，將檔案儲存和存取為所選通訊協定的物件。
 - 選擇 Amazon EFS，透過選取的通訊協定在 Amazon EFS 檔案系統中存放和存取您的檔案。

選擇下一步。

7. 在設定其他詳細資訊中，執行下列動作：
 - a. 針對記錄，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 [CloudWatch Logs 中建立日誌群組](#)。

- 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，選擇安全政策，其中包含啟用供伺服器使用的密碼編譯演算法。

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，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，否則安全政策仍然未使用。

- d. 對於伺服器主機金鑰，請保留空白。
- e. (選用) 對於標籤，對於索引鍵和值，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，而且您有 10,000 個子目錄。換句話說，Amazon 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。

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

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日訊息 (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給他們的文字訊息，然後在驗證後顯示橫幅文字方塊中，輸入您希望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：啟用此選項可忽略當用戶端嘗試 SETSTAT 在您上傳至 Amazon S3 儲存貯體的檔案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：提供一種機制，可在 FTPS 工作階段的控制和資料連線之間繼續或共用交涉的私密金鑰。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。

在新伺服器的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。

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。

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

在 2021 年 5 月 19 日之後，如果您的帳戶在 2021 年 5 月 19 日之前尚未建立伺服器，您將無法在 `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 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 與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。您可利用 VPC 來控制您的網路設定，例如 IP 地址範圍、子網路、路由表和網路閘道。如需 VPCs 的詳細資訊，請參閱 [什麼是 Amazon VPC ?](#) Amazon VPC 使用者指南中的。

在下一節中，尋找如何建立 VPC 並將其連線至伺服器的指示。概觀如下：

1. 使用 VPC 端點設定伺服器。
2. 使用 VPC 內部的用戶端，透過 VPC 端點連線至您的伺服器。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 外部的用戶端連線至您的伺服器。您可以使用 VPC 安全群組來控制對已驗證使用者的存取，其請求僅來自允許的地址。

 Note

AWS Transfer Family 支援雙堆疊端點，讓您的伺服器同時透過 IPv4 和 IPv6 進行通訊。若要啟用雙堆疊支援，請在建立 VPC 端點時選取啟用 DNS 雙堆疊端點選項。請注意，您的 VPC 和子網路都必須設定為支援 IPv6，才能使用此功能。當您的用戶端需要使用任一通訊協定進行連線時，雙堆疊支援特別有用。

如需雙堆疊 (IPv4 和 IPv6) 伺服器端點的資訊，請參閱 [Transfer Family 伺服器的 IPv6 支援](#)。

主題

- [建立只能在 VPC 內存取的伺服器端點](#)
- [為您的伺服器建立面向網際網路的端點](#)
- [變更伺服器的端點類型](#)
- [停止使用 VPC_ENDPOINT](#)
- [限制 Transfer Family 伺服器的 VPC 端點存取](#)
- [其他聯網功能](#)
- [將 AWS Transfer Family 伺服器端點類型從 VPC_ENDPOINT 更新為 VPC](#)

建立只能在 VPC 內存取的伺服器端點

在下列程序中，您會建立只能存取 VPC 內資源的伺服器端點。

在 VPC 內建立伺服器端點

1. 在 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
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：建立啟用 SFTP 的伺服器](#)。
4. 在選擇身分提供者中，選擇受管服務以存放使用者身分和金鑰 AWS Transfer Family，然後選擇下一步。

此程序使用 服務受管選項。如果您選擇自訂，您可以提供 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. 針對端點類型，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，讓用戶端只能使用端點的私有 IP 地址存取您的端點。

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 VPC 中建立僅供內部存取的伺服器不支援自訂主機名稱。

- c. 對於 VPC，請選擇現有的 VPC ID，或選擇建立 VPC 以建立新的 VPC。
- d. 在可用區域區段中，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 [VPC 的安全群組](#)。若要建立安全群組，請參閱《Amazon Virtual Private Cloud 使用者指南》中的 [建立安全群組](#)。

 Note

您的 VPC 會自動具有預設安全群組。如果您在啟動伺服器時未指定不同的安全群組，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、22000 或任何組合。根據預設，連接埠 22 已設定。若要使用連接埠 2222 或連接埠 22000，請將傳入規則新增至安全群組。針對 類型，選擇自訂 TCP，然後**22000**針對連接埠範圍輸入 **2222**或，針對來源輸入與 SSH 連接埠 22 規則相同的 CIDR 範圍。
- 對於安全群組的傳入規則，設定 FTP 和 FTPS 流量以使用**21**控制通道和資料通道**8192-8200**的連接埠範圍。

 Note

您也可以將連接埠 2223 用於需要 TCP "piggy-back" ACKs用戶端，或 TCP 3 向交握的最終堆疊也包含資料的能力。

某些用戶端軟體可能與連接埠 2223 不相容：例如，需要伺服器在用戶端傳送 SFTP 識別字串之前傳送的用戶端。

VPC > Security Groups > sg-[redacted]-default > Edit inbound rules

Edit inbound rules [Info](#)

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

Inbound rules [Info](#)

Security group rule ID	Type Info
sg-[redacted]	HTTP
sg-[redacted]	RDP
sg-[redacted]	HTTPS
sg-[redacted]	Custom TCP
sg-[redacted]	SSH

[Add rule](#)

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

 Note

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

- g. 選擇下一步。
6. 在設定其他詳細資訊中，執行下列動作：
- a. 針對 CloudWatch 記錄，請選擇下列其中一項，以啟用使用者活動的 Amazon CloudWatch 記錄：
- 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。建立的 IAM 角色稱為 AWSTransferLoggingAccess。
 - 選擇現有的角色，從您的帳戶中選擇現有的 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 `transfer.amazonaws.com` 的信任政策。

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

 Note

- 如果您未指定記錄角色，則無法在 CloudWatch 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，但不選取記錄角色。

- b. 針對密碼編譯演算法選項，選擇安全政策，其中包含啟用供伺服器使用的密碼編譯演算法。

 Note

根據預設，除非您選擇不同的安全政策，否則 TransferSecurityPolicy-2024-01 安全政策會連接到您的伺服器。

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

- c. (選用：本節僅適用於從已啟用 SFTP 的現有伺服器遷移使用者。) 對於伺服器主機金鑰，輸入 RSA、ED25519 或 ECDSA 私有金鑰，用於在用戶端透過 SFTP 連線到伺服器時識別伺服器。
 - d. (選用) 對於標籤，對於索引鍵和值，輸入一或多個標籤做為索引鍵/值對，然後選擇新增標籤。
 - e. 選擇下一步。
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

在您選擇編輯的步驟之後，您將需要檢閱每個步驟。

- 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。

在新伺服器的狀態變更為線上之前，可能需要幾分鐘的時間。此時，您的伺服器可以執行檔案操作，但您必須先建立使用者。如需建立使用者的詳細資訊，請參閱 [管理伺服器端點的使用者](#)。

為您的伺服器建立面向網際網路的端點

在下列程序中，您會建立伺服器端點。只有 VPC 預設安全群組中允許來源 IP 地址的用戶端，才能透過網際網路存取此端點。此外，透過使用彈性 IP 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，允許在其防火牆中存取您的端點。

 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 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
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：建立啟用 SFTP 的伺服器](#)。

4. 在選擇身分提供者中，選擇受管服務以存放使用者身分和金鑰 AWS Transfer Family，然後選擇下一步。

此程序使用 服務受管選項。如果您選擇自訂，您可以提供 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. 針對端點類型，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

選擇面向網際網路時，您可以在每個子網路中選擇現有的彈性 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 AWS 或您擁有。您無法將已經與端點搭配使用的彈性 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 EIP 的主機名稱記錄。如需使用 Route 53 for GovCloud 端點的詳細資訊，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 供應商註冊。然後，您可以輸入主機名稱。
- 無 – 使用伺服器的端點，而不使用自訂主機名稱。伺服器主機名稱的格式為 `server-id.server.transfer.region.amazonaws.com`。

Note

對於 中的客戶 AWS GovCloud (US)，選取無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. 對於 VPC，請選擇現有的 VPC ID 或選擇建立 VPC 以建立新的 VPC。
- e. 在可用區域區段中，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。這是您的用戶端可用來允許存取其防火牆中端點的 IP 地址。

秘訣：您必須為可用區域使用公有子網路，如果想要使用私有子網路，請先設定網際網路閘道。

- 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 [VPC 的安全群組](#)。若要建立安全群組，請參閱《Amazon Virtual Private Cloud 使用者指南》中的 [建立安全群組](#)。

Note

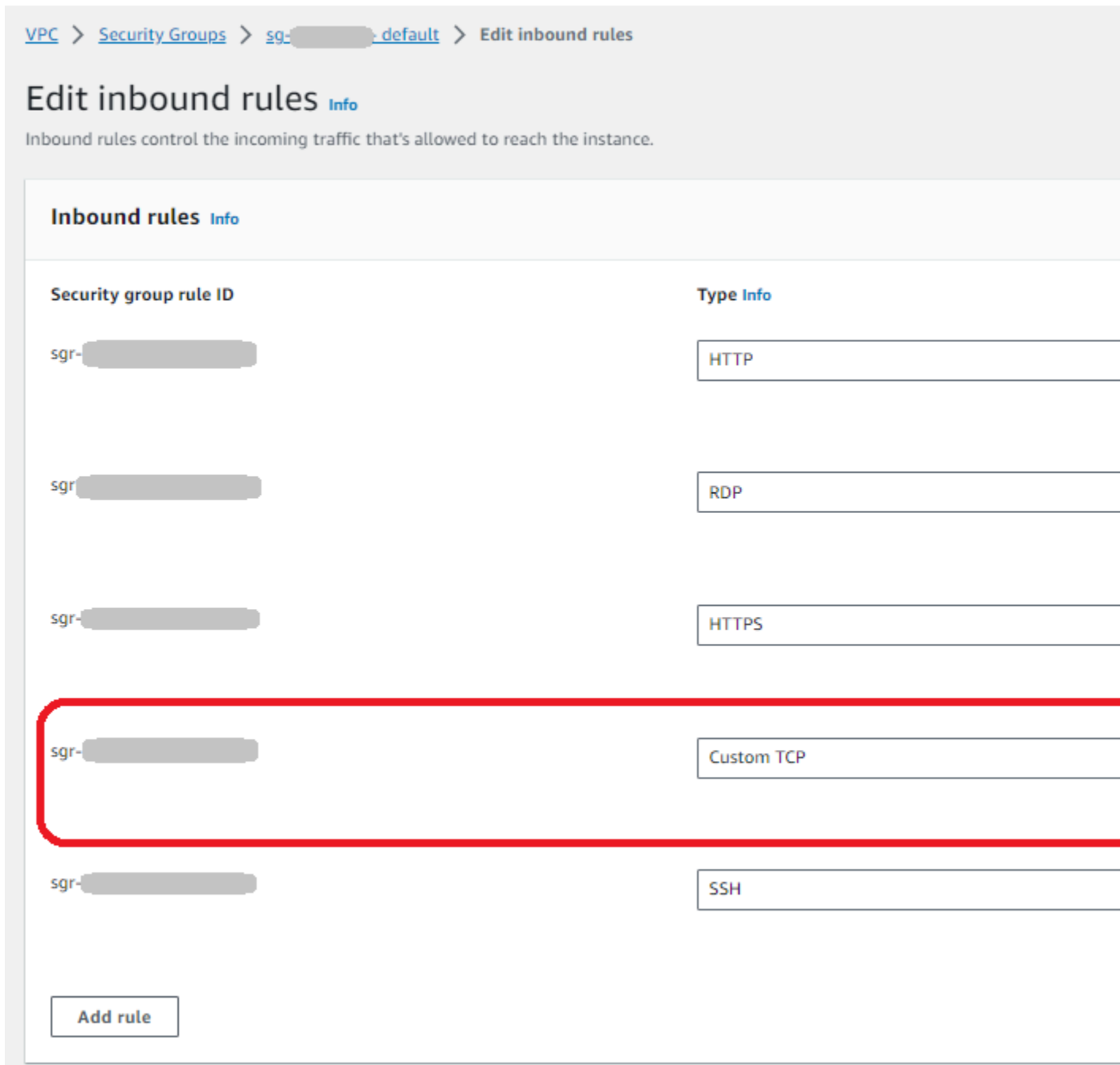
您的 VPC 會自動具有預設安全群組。如果您在啟動伺服器時未指定不同的安全群組，我們會將預設安全群組與您的伺服器建立關聯。

- 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、22000 或任何組合。根據預設，連接埠 22 已設定。若要使用連接埠 2222 或連接埠 22000，請將傳入規則新增至安全群組。針對 類型，選擇自訂 TCP，然後**22000**針對連接埠範圍輸入 **2222**或，針對來源輸入與 SSH 連接埠 22 規則相同的 CIDR 範圍。
- 對於安全群組的傳入規則，設定 FTPS 流量以使用**21**控制頻道和資料頻道**8192-8200**的連接埠範圍。

Note

您也可以將連接埠 2223 用於需要 TCP "piggy-back" ACKs用戶端，或 TCP 3 向交握的最終堆疊也包含資料的能力。

某些用戶端軟體可能與連接埠 2223 不相容：例如，需要伺服器在用戶端傳送 SFTP 識別字串之前傳送的用戶端。



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

 Note

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

h. 選擇下一步。

6. 在設定其他詳細資訊中，執行下列動作：

a. 針對 CloudWatch 記錄，請選擇下列其中一項，以啟用使用者活動的 Amazon CloudWatch 記錄：

- 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。建立的 IAM 角色稱為 AWSTransferLoggingAccess。
- 選擇現有角色，從您的帳戶中選擇現有的 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 `transfer.amazonaws.com` 的信任政策。

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

 Note

- 如果您未指定記錄角色，則無法在 CloudWatch 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，但不選取記錄角色。

b. 針對密碼編譯演算法選項，選擇安全政策，其中包含啟用供伺服器使用的密碼編譯演算法。

 Note

根據預設，除非您選擇不同的安全政策，否則 TransferSecurityPolicy-2024-01 安全政策會連接到您的伺服器。

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

- c. (選用：本節僅適用於從已啟用 SFTP 的現有伺服器遷移使用者。) 對於伺服器主機金鑰，輸入 RSA、ED25519 或 ECDSA 私有金鑰，用於在用戶端透過 SFTP 連線到伺服器時識別伺服器。
- d. (選用) 對於標籤，對於索引鍵和值，輸入一個或多個標籤做為索引鍵/值對，然後選擇新增標籤。
- e. 選擇下一步。
- 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

在您選擇編輯的步驟之後，您將需要檢閱每個步驟。

- 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 VPC 中的伺服器上線時，只能修改子網路，而且只能透過 [UpdateServer](#) API 進行修改。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 中已有伺服器顯示為 VPC_ENDPOINT，建議您將其修改為新的 VPC 端點類型。使用此新端點類型時，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 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
2. 在導覽窗格中，選擇 Servers (伺服器)。
3. 選取您要變更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

繼續下一個步驟之前，請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，以查看狀態變更。

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. 針對編輯端點類型，選擇託管的 VPC。
 - b. 針對存取，選擇下列其中一項：
 - 內部，讓用戶端只能使用端點的私有 IP 地址存取您的端點。
 - 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，您可以在每個子網路中選擇現有的彈性 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 AWS 或您擁有。您無法將已經與端點搭配使用的彈性 IP 地址建立關聯。

- c. (僅適用於面向網際網路的存取選用) 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 供應商註冊。然後，您可以輸入主機名稱。
 - 無 – 使用伺服器的端點，而不使用自訂主機名稱。伺服器主機名稱的格式為 `serverId.server.transfer.regionId.amazonaws.com`。

若要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，請同時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 (<https://console.aws.amazon.com/vpc/> : //) 中建立它們。

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來更新。在伺服器更新完成之前，您無法儲存變更。

f. 選擇儲存。

8. 針對動作，選擇開始並等待伺服器的狀態變更為線上；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到端點。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 已停止為新 AWS 帳戶 EndpointType=VPC_ENDPOINT 使用 建立伺服器的能力。自 2021 年 5 月 19 日起，不擁有端點類型為 VPC_ENDPOINT 之 AWS Transfer Family 伺服器 AWS 的帳戶 VPC_ENDPOINT 將無法透過 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[將您的 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 for 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，而且沒有 PrivateLink 費用。如需詳細資訊，請參閱 [AWS PrivateLink 定價](#)。

此端點類型在功能上等同於先前的端點類型 (VPC_ENDPOINT)。您可以直接將彈性 IP 地址連接到端點，使其面向網際網路，並使用安全群組進行來源 IP 篩選。如需詳細資訊，請參閱[使用 IP 允許清單來保護 AWS Transfer Family 您的 for SFTP 伺服器](#) 部落格文章。

您也可以在此共用 VPC 環境中託管此端點。如需詳細資訊，請參閱 [AWS Transfer Family 現在支援共用服務 VPC 環境](#)。

除了 SFTP 之外，您還可以使用 VPC EndpointType 來啟用 FTPS 和 FTP。我們不打算將這些功能和 FTPS/FTP 支援新增至 EndpointType=VPC_ENDPOINT。我們也已從 AWS Transfer Family 主控台移除此端點類型做為選項。

您可以使用 Transfer Family 主控台、API AWS CLI、SDKs 或 變更伺服器的端點類型 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。我們不再提供它做為主控台上的 AWS Transfer Family 選項。

如果您有其他問題，可以透過 AWS 支援 或您的客戶團隊聯絡我們。

限制 Transfer Family 伺服器的 VPC 端點存取

使用 VPC 端點類型建立 AWS Transfer Family 伺服器時，您的 IAM 使用者和主體需要許可才能建立和刪除 VPC 端點。不過，您組織的安全政策可能會限制這些許可。您可以使用 IAM 政策來允許專為 Transfer Family 建立和刪除 VPC 端點，同時維護其他服務的限制。

 Important

下列 IAM 政策允許使用者僅針對 Transfer Family 伺服器建立和刪除 VPC 端點，同時拒絕其他服務的這些操作：

```
{
  "Effect": "Deny",
  "Action": [
    "ec2:CreateVpcEndpoint",
    "ec2:DeleteVpcEndpoints"
  ],
  "Resource": ["*"],
  "Condition": {
    "ForAnyValue:StringNotLike": {
      "ec2:VpceServiceName": [
        "com.amazonaws.INPUT-YOUR-REGION.transfer.server.*"
      ]
    },
    "StringNotLike": {
      "aws:PrincipalArn": [
        "arn:aws:iam::*:role/INPUT-YOUR-ROLE"
      ]
    }
  }
}
```

```
}
```

將 **INPUT-YOUR-REGION** 取代為您的 AWS 區域（例如，**us-east-1**），並將 **INPUT-YOUR-ROLE** 取代為您要授予這些許可的 IAM 角色。

其他聯網功能

AWS Transfer Family 提供數種進階聯網功能，可在使用 VPC 組態時增強安全性和靈活性：

- 共用 VPC 環境支援 - 您可以在共用 VPC 環境中託管 Transfer Family 伺服器端點。如需詳細資訊，請參閱[搭配 使用共用 VPC VPCs 託管端點 AWS Transfer Family](#)。
- 身分驗證和安全性 - 您可以使用 AWS Web Application Firewall 來保護 Amazon API Gateway 端點。如需詳細資訊，請參閱[AWS Transfer Family 使用 AWS Web Application Firewall 和 Amazon API Gateway 保護](#)。

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

您可以使用 AWS 管理主控台 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 區域和多個帳戶中有伺服器 AWS，您可以使用下一節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 管理主控台](#)
- [使用 更新伺服器端點類型 CloudFormation](#)
- [使用 API 更新伺服器 EndpointType](#)

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 管理主控台。

使用主控台使用 VPC_ENDPOINT 端點類型識別伺服器

1. 在 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
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 區域和多個帳戶中有伺服器 AWS，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 操作。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，則可以使用具有唯讀稽核程式存取權的 IAM 角色來循環通過您的帳戶。

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 管理主控台

1. 在 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
2. 在導覽窗格中，選擇 Servers (伺服器)。
3. 選取您要變更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。您可能必須在伺服器頁面上選擇重新整理，以查看狀態變更。

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. 選擇端點類型的託管 VPC。
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 CloudFormation

本節說明如何使用 CloudFormation 將伺服器的 更新EndpointType 為 VPC。針對您已部署使用的 Transfer Family 伺服器，請使用此程序 CloudFormation。在此範例中，用於部署 Transfer Family 伺服器的原始 CloudFormation 範本如下所示：

```
AWS::Template::FormatVersion: '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

```

範本會隨著下列變更而更新：

- 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 伺服器的端點類型 CloudFormation

1. 使用下列步驟停止您要更新的伺服器。

- a. 在 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
- b. 在導覽窗格中，選擇 Servers (伺服器)。
- c. 選取您要變更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。您可能必須在伺服器頁面上選擇重新整理，以查看狀態變更。

2. 更新 CloudFormation 堆疊

- a. 在 <https://console.aws.amazon.com/cloudformation> 開啟 CloudFormation 主控台。
- b. 選擇用來建立 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會如何影響執行中的資源，然後再實作它們。在此範例中，將修改 Transfer 伺服器資源，並將移除 VPCEndpoint 資源。VPC 端點類型伺服器會代表您建立 VPC 端點，取代原始 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。
- 堆疊更新完成後，請前往 Transfer Family 管理主控台，網址為 <https://console.aws.amazon.com/transfer/>。
 - 重新啟動伺服器。選擇您在其中更新的伺服器 CloudFormation，然後從動作功能表中選擇開始。

使用 API 更新伺服器 EndpointType

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，以及啟動伺服器。

```
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。您可以在使用時，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`。

若要將流量從已註冊的自訂網域重新導向至伺服器端點，您可以使用 Amazon Route 53 或任何網域名稱系統 (DNS) 供應商。Route 53 是 AWS Transfer Family 原生支援的 DNS 服務。

主題

- [使用 Amazon Route 53 做為 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 供應商註冊。然後，您可以輸入主機名稱。
- 無 – 使用伺服器的端點，而不使用自訂主機名稱。

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

如需使用自有網域做為伺服器主機名稱以及 AWS Transfer Family 如何使用 Route 53 的詳細資訊，請參閱下列各節。

使用 Amazon Route 53 做為 DNS 供應商

建立伺服器時，您可以使用 Amazon Route 53 做為 DNS 供應商。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[網域註冊的運作方式](#)。

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，可能會發生三種情況：

1. 如果您是 Route 53 的新手，而且沒有託管區域，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。

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。若您使用替代 DNS 提供者，請確認來自您網域的流量會導向您的 伺服器端點。

若要這樣做，請將您的網域設定為伺服器的端點主機名稱。

- 對於 IPv4 端點，主機名稱在主控台中如下所示：

`serverid.server.transfer.region.amazonaws.com`

- 對於雙堆疊端點，主機名稱在主控台中如下所示：

`serverid.transfer-server.region.on.aws`

Note

如果您的伺服器具有 VPC 端點，則主機名稱的格式與上述格式不同。若要尋找您的 VPC 端點，請在伺服器的詳細資訊頁面上選取 VPC，然後在 VPC 儀表板上選取 VPC 端點 ID。端點是所列項目的第一個 DNS 名稱。

非主控台建立伺服器的自訂主機名稱

當您使用或透過 CLI 建立伺服器時 AWS Cloud Development Kit (AWS CDK) CloudFormation，如果您希望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](#)。

將下列金鑰用於您的自訂主機名稱：

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

若要新增自訂主機名稱，請發出下列 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 託管區域 ID。

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

例如：

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

假設上一個命令的範例值，請執行下列命令來檢視您的標籤：

```
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 上取得。

登入 AWS 管理主控台 並開啟 Route 53 主控台，網址為 <https://console.aws.amazon.com/route53/>。

FTP 和 FTPS Network Load Balancer 考量事項

雖然我們建議避免在 AWS Transfer Family 伺服器前面使用 Network Load Balancer，但如果您的 FTP 或 FTPS 實作需要用戶端通訊路由中的 NLB 或 NAT，請遵循下列建議：

- 對於 NLB，請使用連接埠 21 進行運作狀態檢查，而不是連接埠 8192-8200。
- 對於 AWS Transfer Family 伺服器，請設定來啟用 TLS 工作階段恢復 `TlsSessionResumptionMode = ENFORCED`。

Note

這是建議的模式，因為它提供增強的安全性：

- 要求用戶端對後續連線使用 TLS 工作階段恢復。
- 透過確保一致的加密參數，提供更強大的安全性保證。
- 有助於防止潛在的降級攻擊。
- 保持符合安全標準，同時最佳化效能。

- 如果可能，請遷移至不使用 NLB，以充分利用 AWS Transfer Family 效能和連線限制。

如需 NLB 替代方案的其他指引，請透過 AWS Support 聯絡 AWS Transfer Family 產品管理團隊。如需改善安全狀態的詳細資訊，請參閱部落格文章 [六個改善 AWS Transfer Family 伺服器安全性的秘訣](#)。

中提供了 NLBs 的安全指引 [避免將 NLBs 和 NATs 放在 AWS Transfer Family 伺服器前面](#)。

使用用戶端透過伺服器端點傳輸檔案

您可以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 SFTP 通訊協定的第 3 版。
- OpenSSH (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 (SFTP) 的伺服器。

- 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：

- 不支援 SCP 通訊協定，因為它被視為不安全。您可以使用 OpenSSH scp 命令，如中所述[使用 scp 命令](#)。
- 每個連線的並行多工 SFTP 工作階段數目上限為 10。
- 對於閒置連線，所有通訊協定 (SFTP/FTP/FTPS) 的逾時值為 1800 秒 (30 分鐘)。如果在此期間之後沒有活動，用戶端可能會中斷連線。對於沒有回應的連線：
 - 當用戶端完全沒有回應時，SFTP 會有 300 秒 (5 分鐘) 的逾時。
 - FTPS 和 FTP 有大約 10 分鐘的無回應逾時，由基礎程式庫處理。
- 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[物件金鑰命名準則](#)。
- 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，資料連線的 TLS - PROT C (未受保護) TLS 是預設值，但 AWS Transfer Family FTPS 通訊協定不支援 PROT C。因此，對於 FTPS，您需要發出 PROT P 才能接受您的資料操作。
- 如果您使用 Amazon S3 做為伺服器的儲存體，而且您的用戶端包含使用多個連線進行單一傳輸的選項，請務必停用該選項。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 做為儲存後端，EFS 會支援單一傳輸的多個連線。

以下是 FTP 和 FTPS 的可用命令清單：

可用命令					
ABOR	FEAT	MLST	PASS	RETR	STOR
AUTH	LANG	MKD	PASV	RMD	STOU

可用命令

CDUP	LIST	MODE	PBSZ	RNFR	STRU
CWD	MDTM	NLST	PROT	RNTO	SYST
刪除	MFMT	NOOP	PWD	SIZE	TYPE
EPSV	MLSD	OPTS	結束	STAT	USER

 Note

不支援 APPE。

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

不支援的 SFTP 命令

SSH_FXP_R EADLINK	SSH_FXP_SYMLINK	當請求的檔案為符號連結時，SSH_FXP_STAT	當請求的路徑包含任何符號連結元件時，SSH_FXP_R EALPATH

產生公有/私有金鑰對

您必須先有公有/私有金鑰對可用，才能傳輸檔案。如果您先前尚未產生金鑰對，請參閱 [為服務受管使用者產生 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 OpenSSH](#)
- [使用 WinSCP](#)

- [使用 Cyberduck](#)
- [使用 FileZilla](#)
- [使用 Perl 用戶端](#)
- [使用 LFTP](#)
- [上傳後處理](#)
- [SFTP 訊息](#)

可用的 SFTP/FTPS/FTP 命令

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

Note

資料表提及 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，並以類似資料夾的方式整理資料。此行為說明於《Amazon Simple Storage Service 使用者指南》中的[使用物件中繼資料](#)。

SFTP/FTPS/FTP 命令

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

命令	Amazon S3	Amazon EFS
put	支援	支援
pwd	支援	支援
rename	僅支援 檔案  Note 不支援覆寫現有檔案的重新命名。	支援  Note 不支援覆寫現有檔案或目錄的重新命名。
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 伺服器的端點類型是 VPC，則識別用於傳輸檔案的端點並不簡單。在此情況下，請使用下列程序來尋找您的 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。

Endpoint details Edit

Status Online	Custom hostname -
Endpoint type VPC (vpce- [redacted] 	Endpoint -
VPC vpc- [redacted]	Access Info Internal
FIPS Enabled No	

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。

VPC > Endpoints > vpce-[redacted]

vpce-[redacted] Actions ▼

Details

Endpoint ID vpce-[redacted]	Status Available	Creation time Monday, April 4, 2022 at 10:51:31 EDT	Endpoint type Interface
VPC ID vpc-[redacted] (no-name-specified)	Status message -	Service name com.amazonaws.us-east-2.transfer.server.c-0002	Private DNS names enabled No
DNS record IP type ipv4	IP address type ipv4	DNS names vpce-[redacted] [redacted] [redacted].us-east-2 [redacted] [redacted] [redacted] [redacted].us-east-2	

避免setstat錯誤

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

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

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

使用 OpenSSH

本節包含使用 OpenSSH 從命令列傳輸檔案的說明。

Note

此用戶端僅適用於啟用 SFTP 的伺服器。

主題

- [使用 OpenSSH](#)
- [使用 scp命令](#)

使用 OpenSSH

AWS Transfer Family 使用 OpenSSH 命令列公用程式傳輸檔案

1. 在 Linux、macOS 或 Windows 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，而 *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。您可以將 `-P` 旗標新增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，如果您一律想要使用連接埠 2222 或連接埠 22000，您可以更新 `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的目前目錄中），請在 `sftp` 提示下執行下列命令：

```
put hello.txt
```

類似以下內容的訊息隨即出現，指出檔案傳輸正在進行中或已完成。

```
Uploading hello.txt to /amzn-s3-demo-bucket/home/sftp_user/hello.txt
```

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

 Note

建立伺服器之後，可能需要幾分鐘的時間，伺服器端點主機名稱才能由環境中的 DNS 服務解析。

使用 scp 命令

Transfer Family 不支援 SCP 通訊協定。不過，如果您需要此功能，您可以使用 OpenSSH scp 命令。

透過 SFTP 使用 SCP 的建議是使用 OpenSSH 9.0 版或更新版本。在 OpenSSH 第 9 版及更新版本中，scp 命令預設為使用 SFTP 通訊協定進行檔案傳輸，而非舊版 SCP 通訊協定。

Important

確保您的 Transfer Family 伺服器已設定為使用 S3 最佳化目錄存取。

使用 WinSCP

使用下列說明使用 WinSCP 從命令列傳輸檔案。

Note

如果您使用的是 WinSCP 5.19，則可以使用登入 AWS 資料直接連線至 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 WinSCP 傳輸檔案

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，請針對加密選擇下列其中一項：

- FTP 無加密
 - FTPS 的 TLS/SSL 明確加密
3. 針對 Host name (主機名稱)，輸入您的伺服器端點。伺服器端點位於伺服器詳細資訊頁面上。如需詳細資訊，請參閱[檢視 SFTP、FTPS 和 FTP 伺服器詳細資訊](#)。

如果您的伺服器使用 VPC 端點，請參閱 [尋找您的 Amazon VPC 端點](#)。

4. 針對連接埠號碼，輸入下列項目：

- **22** 適用於 SFTP
- **21** 適用於 FTP/FTPS

5. 針對使用者名稱，輸入您為特定身分提供者建立的使用者名稱。

秘訣：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 for Microsoft Active Directory](#)
- [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 [SSH 私有金鑰檔案](#)，然後從檔案系統選擇 SSH 私有金鑰檔案。

如果 WinSCP 提供將 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網站對話方塊中，選擇確定以完成連線設定。
10. 在登入對話方塊中，選擇工具，然後選擇偏好設定。
11. 在偏好設定對話方塊中，針對轉接，選擇耐久度。

針對啟用傳輸繼續/傳輸到暫時檔案名稱的選項，選擇停用。

Important

如果您啟用此選項，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，然後清除針對單一轉接使用多個連線核取方塊。

秘訣：如果您選擇此選項，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。也可能發生靜音資料損毀。

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 WinSCP 中檔案的屬性。

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，請務必先停用 WinSCP 時間戳記設定（或使用 SetStatOption 中所述的 [避免 setstat 錯誤](#)），再執行檔案傳輸。若要這樣做，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 AUTH TLS) 或 FTP (檔案傳輸通訊協定)。
4. 在伺服器中，輸入您的伺服器端點。伺服器端點位於伺服器詳細資訊頁面上。如需詳細資訊，請參閱 [檢視 SFTP、FTPS 和 FTP 伺服器詳細資訊](#)。

如果您的伺服器使用 VPC 端點，請參閱 [尋找您的 Amazon VPC 端點](#)。

5. 針對連接埠號碼，輸入下列項目：
 - **22** 適用於 SFTP
 - **21** 適用於 FTP/FTPS
6. 針對 Username (使用者名稱)，輸入您在 [管理伺服器端點的使用者](#) 中建立的使用者名稱。
7. 如果選取 SFTP，請針對 SSH 私有金鑰選擇或輸入 SSH 私有金鑰。
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，選擇您要傳輸的檔案，然後將它們拖放到 Amazon S3 目錄（目標）。
- 在 Amazon S3 目錄（來源）中，選擇您要傳輸的檔案，然後將它們拖放到您的本機目錄（目標）。

使用 FileZilla

使用下列指示來使用 FileZilla 傳輸檔案。

設定檔案傳輸的 FileZilla

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，選擇新增網站。
4. 在一般索引標籤上，針對通訊協定選擇通訊協定：SFTP 或 FTP。

如果您選擇 FTP，請針對加密選擇下列其中一項：

- 僅使用純 FTP（不安全）– 適用於 FTP
 - 如果可用，透過 TLS 使用明確的 FTP – 適用於 FTPS
5. 針對主機名稱，輸入您正在使用的通訊協定，後面接著伺服器端點。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](#)。
 - 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`

請務必將####取代為實際的伺服器端點。

如果您的伺服器使用 VPC 端點，請參閱 [尋找您的 Amazon VPC 端點](#)。

6. 針對連接埠號碼，輸入下列項目：
 - **22** 適用於 SFTP
 - **21** 適用於 FTP/FTPS
7. 如果選取 SFTP，請針對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 可能會在 Amazon S3 儲存貯體中寫入部分物件。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 `Net::SFTP::Foreign` perl 用戶端，您必須將 `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。

使用 LFTP

LFTP 是免費的 FTP 用戶端，可讓使用者透過大多數 Linux 機器的命令列界面執行檔案傳輸。

對於大型檔案下載，LFTP 有已知的封包順序錯誤問題，導致檔案傳輸失敗。

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

做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` 且 `x-amz-meta-user-agent-id` 其值為 `username@server-id`。 `username` 是上

傳檔案的 Transfer Family 使用者，`server-id`也是用於上傳的伺服器。您可以使用 Lambda 函數內 S3 物件上的 [HeadObject](#) 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，`RoleSessionName` 會包含在 [S3 事件通知結構](#) 中的請求者欄位中，做為 `[AWS:Role Unique Identifier]/username.sessionid@server-id`。例如，以下是已複製到 S3 儲存貯體之檔案的 S3 存取日誌中請求者範例欄位的內容。S3

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

在上方的申請者欄位中，會顯示名為的 IAM 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) 角色唯一識別符的詳細資訊，請參閱 AWS Identity and Access Management 《[使用者指南](#)》中的[唯一識別符](#)。

SFTP 訊息

本節說明使用 Transfer Family 伺服器時，您在 SFTP 檔案傳輸期間或之後可能收到的用戶端訊息。如需任何 SFTP 事件的詳細資訊，請檢查您的 SFTP 用戶端日誌。您可以使用該資訊對任何錯誤進行故障診斷，或將該資訊轉發給您的網路團隊，以協助他們識別問題。

SFTP 用戶端訊息

活動	Description
AUTH_FAILURE	使用者身分驗證失敗。這可以是自訂身分提供者或服務受管使用者的任何失敗類型。事件中的詳細資訊有助於釐清失敗的根本原因。
CLOSE	表示已開啟的檔案或目錄已成功關閉。
CONNECTED/DISCONNECTED	表示正常連線成功和中斷連線。
CREATE_SYMLINK	已建立符號連結（成功或失敗）。
DELETE	檔案已刪除（成功或失敗）。
ERROR	一般、非預期的錯誤。相關聯的描述包含的資訊可協助您或您的網路管理員識別特定問題。
EXIT_REASON	當意外錯誤導致 SFTP 工作階段終止時發出。與事件相關聯的訊息說明原因。
MKDIR	目錄已建立（成功或失敗）。
OPEN	檔案已開啟進行讀取或寫入（成功或失敗）
PARTIAL_CLOSE	當檔案仍然開啟且未收到 CLOSE 訊息時，用戶端會中斷與伺服器的連線。Transfer Family 會儲存檔案的接收部分（實際上可能是完整檔案），並發出 PARTIAL_CLOSE 事件來提醒客戶此問題。工作流程整合也會收到 onPartialClose 事件，以適當地處理檔案。
RENAME	檔案已重新命名（成功或失敗）
RMDIR	目錄已刪除（成功或失敗）
SETSTAT	檔案的屬性會變更（成功或失敗）。

活動	Description
	 Note 如果您使用 Amazon S3 進行儲存，則 Transfer Family 不支援 SETSTAT。避免setstat錯誤 本節提供如何透過關閉設定來避免SetStat錯誤的詳細資訊。這可避免您收到 fail unsupported error：反之，您會收到 success but do nothing 訊息。
TLS_RESUME_FAILURE	伺服器設定為強制執行 TLS 工作階段恢復，且用戶端不支援它。

管理伺服器端點的使用者

在下列各節中，您可以找到如何使用 AWS Transfer Family AWS Directory Service for Microsoft Active Directory 或自訂身分提供者新增使用者的相關資訊。

每個使用者的屬性中也要存放該使用者的 Secure Shell (SSH) 公有金鑰。金鑰型身分驗證需要這樣做。私有金鑰存放在您使用者的本機電腦上。當您的使用者使用用戶端傳送身分驗證請求到您的伺服器時，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。伺服器接著會成功驗證使用者。

Note

如需具有多個 SSH 金鑰之使用者的自動化部署和管理，請參閱 [Transfer 系列 Terraform 模組](#)。

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 會封鎖從驗證到 SFTP 伺服器長度為 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

每個儲存選項的特性：

- 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 提供。您可以使用主控台內的受限制核取方塊，將使用者鎖定至其主目錄，但無法指定虛擬目錄結構。

邏輯目錄

如果您要為使用者指定邏輯目錄值，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。

AWS Transfer Family 支援在使用 LOGICAL HomeDirectory HomeDirectoryType 值。這適用於回應中提供 HomeDirectoryDetails 的服務受管使用者、Active Directory 存取和自訂身分提供者實作。

 Important

使用 LOGICAL HomeDirectory HomeDirectoryType 時，該值必須映射至其中一個邏輯目錄映射。服務會在使用者建立和更新期間驗證這一點，以防止組態無法運作。

預設行為

根據預設，如果未指定，則 LOGICAL 模式的 HomeDirectory 設定為 "/"。此行為保持不變，並保持與現有使用者定義相容。

- 請務必將您的 HomeDirectory 映射至 項目，而非目標。如需詳細資訊，請參閱[使用邏輯目錄的規則](#)。
- 如需如何建構虛擬目錄的詳細資訊，請參閱 [虛擬目錄結構](#)。

自訂身分提供者考量事項

使用自訂身分提供者時，您現在可以在使用 LOGICAL HomeDirectory HomeDirectoryType。當自訂 IDP 在 LOGICAL 模式中指定 HomeDirectory 時，TestIdentityProvider API 呼叫會產生正確的結果。

HomeDirectory 和 LOGICAL HomeDirectoryType 的自訂 IDP 回應範例：

```
{
  "Role": "arn:aws:iam::123456789012:role/transfer-user-role",
  "HomeDirectoryType": "LOGICAL",
  "HomeDirectory": "/marketing",
  "HomeDirectoryDetails": "[{\"Entry\":\"/\", \"Target\":\"/bucket/home\"}, {\"Entry\":\"/marketing\", \"Target\":\"/marketing-bucket/campaigns\"}]"
}
```

Active Directory 群組配額

AWS Transfer Family 預設限制為每個伺服器 100 個 Active Directory 群組。如果您的使用案例需要超過 100 個群組，請考慮使用自訂身分提供者解決方案，如[簡化 Active Directory 身分驗證與的自訂身分提供者 AWS Transfer Family](#)所述。

此限制適用於使用下列身分提供者的伺服器：

- AWS 適用於 Microsoft Active Directory 的 Directory Service
- AWS 適用於 Entra ID Domain Services 的 Directory Service

如果您需要請求提高服務限制，請參閱 中的[AWS 服務 配額](#)AWS 一般參考。如果您的使用案例需要超過 100 個群組，請考慮使用自訂身分提供者解決方案，如[簡化 Active Directory 身分驗證與的自訂身分提供者 AWS Transfer Family](#)所述。

如需 Active Directory 群組限制的疑難排解資訊，請參閱 [超過 Active Directory 群組限制](#)。

主題

- [使用服務受管使用者](#)
- [使用自訂身分提供者](#)
- [使用 AWS Directory Service for Microsoft Active Directory](#)
- [使用 AWS Directory Service for Entra ID Domain Services](#)

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 服務受管使用者新增至您的伺服器。如需詳細資訊，請參閱[設定 SFTP、FTPS 或 FTP 伺服器端點](#)。

如果您使用服務受管身分類型，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。當您這樣做時，每個使用者名稱在伺服器上都必須是唯一的。

若要以程式設計方式新增服務受管使用者，請參閱 [CreateUser](#) API [的範例](#)。

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詳細資訊，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](#)
- [管理服务受管使用者](#)

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，請遵循本知識中心文章中所述的步驟：[如何將 AWS Transfer Family 伺服器設定為使用另一個 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 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台，然後從導覽窗格中選取伺服器。
2. 在伺服器頁面上，選取要新增使用者的伺服器核取方塊。
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 '@'。使用者名稱開頭不能是連字號 '-'、句點 '.' 或符號 '@'。
5. 針對 Access，選擇您先前建立的 IAM 角色，該角色可讓您存取 Amazon S3 儲存貯體。

您使用[建立 IAM 角色和政策](#)的程序建立此 IAM 角色。該 IAM 角色包含 IAM 政策，可讓您存取 Amazon S3 儲存貯體。它還包含與 AWS Transfer Family 服務的信任關係，在另一個 IAM 政策中定義。若您的使用者需要精細存取控制，請參閱[使用 AWS Transfer Family 和 Amazon S3 增強資料存取控制](#)部落格文章。

6. (選用) 針對政策，選取下列其中一項：
 - 無
 - 現有政策
 - 從 IAM 選取政策：可讓您選擇現有的工作階段政策。選擇檢視以查看包含政策詳細資訊的 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](#)、[為 Amazon S3 儲存貯體建立工作階段政策](#)或[動態許可管理方法](#)。

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

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。在本例中，請確定您的 IAM 角色能夠存取此 root 目錄。

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在該使用者的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

將主目錄指派給使用者，並將使用者限制為該主目錄，就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 金鑰對的說明，請參閱[為服務受管使用者產生 SSH 金鑰](#)。

10. (選用) 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。
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 – 對於下一個步驟，請繼續執行 [使用用戶端透過伺服器端點傳輸檔案](#)。

新增 Amazon EFS 服務受管使用者

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

- 如需 Amazon EFS 檔案擁有權的詳細資訊，請參閱 [Amazon EFS 檔案擁有權](#)。
- 如需為您的 EFS 使用者設定目錄的詳細資訊，請參閱 [為 Transfer 系列設定 Amazon EFS 使用者](#)。

將 Amazon EFS 服務受管使用者新增至您的伺服器

1. 在 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台，然後從導覽窗格中選取伺服器。
2. 在伺服器頁面上，選取要新增使用者的 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 '@'。使用者名稱開頭不能是連字號 '-'、句點 '.' 或符號 '@'。
 - 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，我們建議您為群組 ID 和使用者 ID 輸入 0 的值。這會授予 Amazon EFS 的使用者管理員權限。
 - 對於其他使用者，輸入使用者的 POSIX 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，為每個使用者輸入一或多個額外的 POSIX 群組 IDs，以逗號分隔。
 - d. 針對 Access，選擇符合下列條件的 IAM 角色：
 - 讓使用者只能存取您希望他們存取的 Amazon EFS 資源（檔案系統）。
 - 定義使用者可執行和無法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，以及掛載存取和讀取/寫入許可。例如，以下兩個 AWS 受管政策的組合雖然相當寬鬆，但會為您的使用者授予必要的許可：

- AmazonElasticFileSystemClientFullAccess
- AWSTransferConsoleFullAccess

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

- e. 對於主目錄，請執行下列動作：

- 選擇您要用來存放要用來傳輸資料的 Amazon EFS 檔案系統 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效果：
 - 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) 輸入您要使用者在使用用戶端登入時所在的主目錄路徑。

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 金鑰對的說明，請參閱[為服務受管使用者產生 SSH 金鑰](#)。

6. (選用) 輸入使用者的任何標籤。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。
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。

第一次將 SFTP 傳送到 Transfer Family 伺服器時可能遇到的問題：

- 如果您執行 `sftp` 命令但未出現提示，您可能會遇到下列訊息：

```
Couldn't canonicalize: Permission denied
```

```
Need cwd
```

在此情況下，您必須增加使用者角色的政策許可。您可以新增 AWS 受管政策，例如 `AmazonElasticFileSystemClientFullAccess`。

- 如果您在sftp提示pwd中輸入 以檢視使用者的主目錄，您可能會看到以下訊息，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，請繼續執行 [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 公有金鑰的相關資訊。

- [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](#)

尋找您的使用者清單

1. 在 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
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 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
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，在此頁面上變更使用者的屬性。

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，選擇您先前建立的 IAM 角色，以提供對 Amazon S3 儲存貯體的存取。

您使用[建立 IAM 角色和政策](#)的程序建立此 IAM 角色。該 IAM 角色包含 IAM 政策，可讓您存取 Amazon S3 儲存貯體。它還包含與 AWS Transfer Family 服務的信任關係，在另一個 IAM 政策中定義。

7. （選用）針對政策，選擇下列其中一項：

- 無
- 現有政策
- 從 IAM 選取政策以選擇現有的政策。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的資料 AWS Transfer Family。輸入使用者使用其用戶端登入時所到達home目錄的路徑。

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。在本例中，請確定您的 IAM 角色能夠存取此 root 目錄。

 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在該使用者的 home 目錄。

9. （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時，這應該足以鎖定使用者對指定資料夾的存取。當您需要套用進一步控制時，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 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
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 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
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. 選擇 Add SSH public key (新增 SSH 公有金鑰) 來將新的 SSH 公有金鑰新增至使用者。

 Note

SSH 金鑰僅供啟用 Secure Shell (SSH) 檔案傳輸通訊協定 (SFTP) 的伺服器使用。如需如何產生 SSH 金鑰對的資訊，請參閱 [為服務受管使用者產生 SSH 金鑰](#)。

6. 針對 SSH public key (SSH 公有金鑰)，輸入 SSH 金鑰對的 SSH 公有金鑰部分。

金鑰要先經服務驗證，您才能新增新使用者。SSH 金鑰的格式是 `ssh-rsa string`。若要產生 SSH 金鑰對，請參閱 [為服務受管使用者產生 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 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
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。

使用自訂身分提供者

AWS Transfer Family 為自訂身分提供者提供數個選項，以驗證和授權使用者進行安全的檔案傳輸。以下是主要方法：

- [自訂身分提供者解決方案](#)- 本主題說明 Transfer Family 自訂身分提供者解決方案，使用 GitHub 中託管的工具組。

 Note

對於大多數使用案例，這是建議的選項。具體而言，如果您需要支援超過 100 個 Active Directory 群組，自訂身分提供者解決方案會提供可擴展的替代方案，而不會限制群組。此解決方案在部落格文章中描述：[使用自訂身分提供者簡化 Active Directory 身分驗證 AWS Transfer Family](#)。

- [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 函數來支援 Amazon API Gateway 方法。

您可以使用單一 Amazon API Gateway 方法提供 RESTful 介面。Transfer Family 會呼叫此方法來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 來整合身分提供者，或想要使用 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](#)。

- [動態許可管理方法](#)- 本主題說明使用工作階段政策動態管理使用者許可的方法。

若要驗證您的使用者，您可以使用現有的身分提供者搭配 AWS Transfer Family。您可以使用 AWS Lambda 函數整合您的身分提供者，該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 圖形以取得指標，例如在 AWS Transfer Family 管理主控台中傳輸的檔案數和位元組數，讓您使用集中式儀表板來監控檔案傳輸。

- Transfer Family 提供部落格文章和研討會，引導您建置檔案傳輸解決方案。此解決方案利用 AWS Transfer Family 受管 SFTP/FTPS 端點和 Amazon Cognito 和 DynamoDB 進行使用者管理。

部落格文章可在[使用 Amazon Cognito 做為 AWS Transfer Family 和 Amazon S3 的身分提供者](#)取得。您可以在[此處](#)檢視研討會的詳細資訊。

Note

對於自訂身分提供者，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 '@'。使用者名稱開頭不能是連字號 '-'、句點 '.' 或符號 '@'。

實作自訂身分提供者時，請考慮下列最佳實務：

- 在與 Transfer Family 伺服器相同的 AWS 帳戶和區域中部署解決方案。
- 在設定 IAM 角色和政策時，實作最低權限原則。
- 使用 IP 允許清單和標準化記錄等功能來增強安全性。
- 在部署之前，在非生產環境中徹底測試您的自訂身分提供者。

主題

- [自訂身分提供者解決方案](#)

- [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](#)
- [使用多個身分驗證方法](#)
- [IPv6 支援自訂身分提供者](#)

自訂身分提供者解決方案

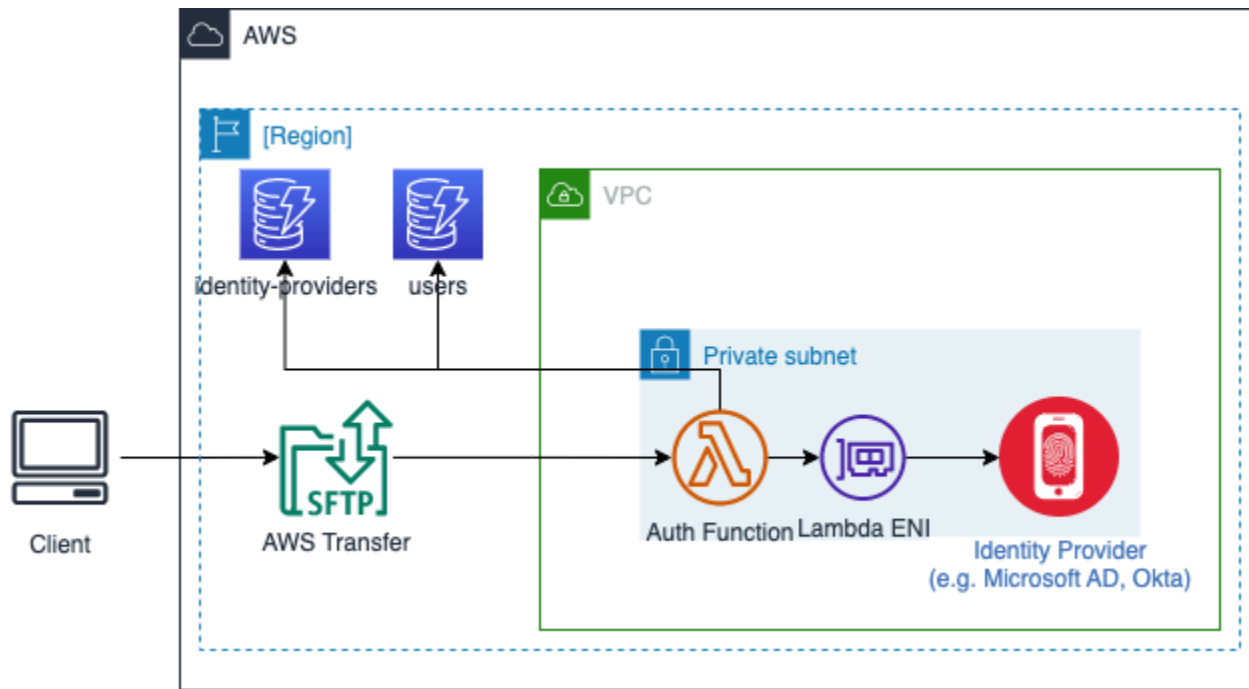
AWS Transfer Family 自訂身分提供者解決方案是一種模組化的自訂身分提供者解決方案，可解決企業在實作服務時有許多常見的身分驗證和授權使用案例。此解決方案為實作具有精細每個使用者工作階段組態的自訂身分提供者提供了可重複使用的基礎，並分隔了身分驗證和授權邏輯，為各種使用案例提供了靈活且easy-to-maintain的基礎。

透過 AWS Transfer Family 自訂身分提供者解決方案，您可以解決常見的企業身分驗證和授權使用案例。此模組化解決方案提供：

- 實作自訂身分提供者的可重複使用基礎
- 精細的每位使用者工作階段組態
- 分開的身分驗證和授權邏輯

自訂身分工具組的實作詳細資訊

解決方案為各種使用案例提供靈活且可維護的基礎。若要開始使用，請檢閱位於 <https://github.com/aws-samples/toolkit-for-aws-transfer-family> 的工具組，然後遵循[入門](#)區段中的部署說明。



Note

如果您之前已使用自訂身分提供者範本和範例，請考慮改用此解決方案。接下來，供應商特定的模組將標準化此解決方案。持續的維護和功能增強功能將套用至此解決方案。

此解決方案包含實作自訂提供者的標準模式，其中包含記錄和存放所需其他工作階段中繼資料的位置等詳細資訊 AWS Transfer Family，例如 `HomeDirectoryDetails` 參數。此解決方案為實作具有精細每個使用者工作階段組態的自訂身分提供者提供了可重複使用的基礎，並將身分提供者身分驗證邏輯與建立傳回 Transfer Family 的組態的可重複使用邏輯分離，以完成身分驗證並建立工作階段的設定。

此解決方案的程式碼和支援資源可在 <https://github.com/aws-samples/toolkit-for-aws-transfer-family> 取得。

工具組包含下列功能：

- 佈建所需資源的 [AWS Serverless Application Model](#) 範本。或者，部署和設定 Amazon API Gateway 以納入 AWS WAF，如使用 [AWS Transfer Family AWS Web Application Firewall](#) 和 [Amazon API Gateway 保護](#) 的部落格文章所述。
- [Amazon DynamoDB](#) 結構描述，用於儲存有關身分提供者的組態中繼資料，包括使用者工作階段設定，例如 `HomeDirectoryDetails`、`Role` 和 `Policy`。
- 模組化方法可讓您在未來將新的身分提供者做為模組新增至解決方案。

- 屬性擷取：選擇性地從支援的身分提供者擷取 IAM 角色和 POSIX 設定檔 (UID 和 GID) 屬性，包括 AD、LDAP 和 Okta。
- 支援使用相同的解決方案部署連接到單一 Transfer Family 伺服器或多個 Transfer Family 伺服器的多個身分提供者。
- 內建 IP 允許清單檢查，例如 IP 允許清單，可選擇性地根據每個使用者或每個身分提供者進行設定。
- 具有可設定日誌層級和追蹤支援的詳細記錄，以協助故障診斷。

開始部署自訂身分提供者解決方案之前，您需要有下列 AWS 資源。

- 具有私有子網路的 Amazon Virtual Private Cloud (VPC)，可透過 NAT 閘道或 DynamoDB 閘道端點進行網際網路連線。
- 執行下列任務的適當 IAM 許可：
 - 部署 custom-idp.yaml CloudFormation 範本、
 - 建立 AWS CodePipeline 專案
 - 建立 AWS CodeBuild 專案
 - 建立 IAM 角色和政策

Important

您必須將解決方案部署到 AWS 區域 包含目標 Transfer Family 伺服器的相同 AWS 帳戶 和 。

支援的身分提供者

下列清單包含自訂身分提供者解決方案支援的身分提供者詳細資訊。

供應商	密碼流程	公有金鑰流程	多重因素	屬性擷取	詳細資訊
Active Directory 和 LDAP	是	是	否	是	使用者驗證可作為公有金鑰驗證流程的一部分執行。
Argon2 (本機雜湊)	是	否	否	否	Argon2 雜湊會存放在「本機」密碼型身

供應商	密碼流程	公有金鑰流程	多重因素	屬性擷取	詳細資訊
					分驗證使用案例的使用者記錄中。
Amazon Cognito	是	否	是*	否	僅限以時間為基礎的一次性密碼 (TOTP) 為基礎的多重要素驗證。 *不支援以 SMS 為基礎的 MFA。
Entra ID (先前為 Azure AD)	是	否	否	否	
Okta	是	是	是*	是	僅限 TOTP 型 MFA。
公有金鑰	否	是	否	否	公有金鑰存放在 DynamoDB 的使用者記錄中。
Secrets Manager	是	是	否	否	

使用 AWS Lambda 整合您的身分提供者

本主題說明如何建立連線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。

對於大多數使用案例，設定自訂身分提供者的建議方法是使用 [自訂身分提供者解決方案](#)。

 Note

在建立使用 Lambda 做為身分提供者的 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。針對選擇身分提供者，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

只有在您將 SFTP 啟用為 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，即 AWS Lambda 使用 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

您必須擁有參考 Transfer Family 伺服器 and Lambda ARNs 的政策。例如，您可以將下列政策與連線至身分提供者的 Lambda 函數搭配使用。政策會以字串形式逸出 JSON。

```
"Policy":
"{\"Version\":\"2012-10-17\",
  \"Id\":\"default\",
  \"Statement\":[
    {\"Sid\":\"AllowTransferInvocation\",
      \"Effect\":\"Allow\",
      \"Principal\":{\"Service\":\"transfer.amazonaws.com\"},
      \"Action\":\"lambda:InvokeFunction\",
      \"Resource\":\"arn:aws:lambda:region:123456789012:function:my-lambda-auth-function\",
      \"Condition\":{\"ArnLike\":{\"AWS:SourceArn\":
        \"arn:aws:transfer:region:123456789012:server/server-id\"}}}}
  ]}"
```

Note

在上述政策範例中，將每個#####取代為您自己的資訊。

事件訊息結構

從 SFTP 伺服器傳送至自訂 IDP 授權方 Lambda 函數的事件訊息結構如下所示。

```
{
  "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，您可以輸入下列命令來連線：

```
sftp bobusa@server_hostname
```

然後，系統會提示您輸入密碼：

```
Enter password:
mysecretpassword
```

您可以從 Lambda 函數內列印傳遞的事件，以從 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 FTPS 的事件結構類似：唯一的區別是這些值用於 protocol 參數，而不是 SFTP。

用於身分驗證的 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

- [有效的 Lambda 值](#)
- [Lambda 函數範例](#)
- [測試您的組態](#)
- [Lambda 函數範本](#)

有效的 Lambda 值

下表說明 Transfer Family 接受用於自訂身分提供者的 Lambda 函數之值的詳細資訊。

Value	Description	必要
Role	指定控制使用者存取 Amazon S3 儲存貯體或 Amazon EFS 檔案系統的 IAM 角色的 Amazon Resource Name (ARN)。連接到此角色的政策會決定在將檔案傳入和傳出 Amazon S3 或 Amazon EFS 檔案系統時，您要提供給使用者的存取層級。IAM 角色也應包含信任關係，允許伺服器在處理您使用者的傳輸請求時，存取您的資源。 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。對檔案系統中的檔案和目錄設定的 POSIX 許可，會決定使用者在 Amazon EFS 檔案系統中傳入和傳出檔案時所取得的存取等級。	Amazon EFS 備份儲存的必要項目
PublicKeys	對此使用者有效的 SSH 公有金鑰值清單。空白清單表示這不是有效的登入。密碼身分驗證期間不得傳回。	選用
Policy	您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 IAM 角色。此政策會將	選用

Value	Description	必要
	使用者存取的範圍縮小到他們 Amazon S3 儲存貯體的部分。如需搭配自訂身分提供者使用工作階段政策的詳細資訊，請參閱本主題中的工作階段政策範例。	
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，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，讓使用者可以看到 Amazon S3 或 Amazon EFS 路徑。	選用
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您的使用者查看，以及如何讓它們可見。您必須指定 Entry 和 Target 對，其中 Entry 顯示如何顯示路徑，而 Target 是實際的 Amazon S3 或 Amazon EFS 路徑。	如果 的值 HomeDirectoryType 為，則為必要 LOGICAL

Value	Description	必要
HomeDirectory	使用者使用 用戶端登入伺服器 的登陸目錄。格式取決於您的 儲存後端： - 對於 Amazon S3： /bucket-name/user-home-directory 範例：/amzn-s3-demo-bucket/users/john - 對於 Amazon EFS： fs-12345/user-home-directory 範例：/fs-faa1a123/users/john  Important 路徑中必須包含儲存貯體名稱或 Amazon EFS 檔案系統 ID。省略此資訊會在檔案傳輸期間導致「找不到檔案」錯誤。	選用

Note

HomeDirectoryDetails 是 JSON 映射的字串表示法。這與相反 PosixProfile，這是實際的 JSON 映射物件，PublicKeys 也是字串的 JSON 陣列。如需特定語言的詳細資訊，請參閱程式碼範例。

⚠ HomeDirectory 格式需求

使用 HomeDirectory 參數時，請務必包含完整的路徑格式：

- 對於 Amazon S3 儲存：一律以 格式包含儲存貯體名稱 /bucket-name/path
- 對於 Amazon EFS 儲存：一律以 格式包含檔案系統 ID /fs-12345/path

「找不到檔案」錯誤的常見原因是從 HomeDirectory 路徑中省略儲存貯體名稱或 EFS 檔案系統 ID。在沒有儲存識別符/的情況下 HomeDirectory 將設定為 將導致身分驗證成功，但檔案操作失敗。

Lambda 函數範例

本節提供一些範例 Lambda 函數，包括 NodeJS 和 Python。

📘 Note

在這些範例中，使用者、角色、POSIX 設定檔、密碼和主目錄詳細資訊都是範例，必須以您的實際值取代。

Logical home directory, NodeJS

下列 NodeJS 範例函數提供具有[邏輯主目錄](#)之使用者的詳細資訊。

```
// GetUserConfig Lambda

exports.handler = (event, context, callback) => {
  console.log("Username:", event.username, "ServerId: ", event.serverId);

  var response;
  // Check if the username presented for authentication is correct. This doesn't
  check the value of the server ID, only that it is provided.
  if (event.serverId !== "" && event.username == 'example-user') {
    var homeDirectoryDetails = [
      {
        Entry: "/",
        Target: "/fs-faa1a123"
      }
    ]
  }
}
```

```

];
response = {
  Role: 'arn:aws:iam::123456789012:role/transfer-access-role', // The user is
authenticated if and only if the Role field is not blank
  PosixProfile: {"Gid": 65534, "Uid": 65534}, // Required for EFS access, but
not needed for S3
  HomeDirectoryDetails: JSON.stringify(homeDirectoryDetails),
  HomeDirectoryType: "LOGICAL",
};

// Check if password is provided
if (!event.password) {
  // If no password provided, return the user's SSH public key
  response['PublicKeys'] = [ "ssh-
rsa abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789" ];
  // Check if password is correct
} else if (event.password !== 'Password1234') {
  // Return HTTP status 200 but with no role in the response to indicate
authentication failure
  response = {};
}
} else {
  // Return HTTP status 200 but with no role in the response to indicate
authentication failure
  response = {};
}
callback(null, response);
};

```

Path-based home directory, NodeJS

下列 NodeJS 範例函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 format depends on your storage backend:
    // For S3: '/bucket-name/user-home-directory' (e.g., '/my-transfer-bucket/
users/john')
    // For EFS: '/fs-12345/user-home-directory' (e.g., '/fs-faa1a123/users/john')
    HomeDirectory: '/my-transfer-bucket/users/example-user' // S3 example -
    replace with your bucket name
    // HomeDirectory: '/fs-faa1a123/users/example-user' // EFS example - uncomment
    for EFS
};

// 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 format depends on your storage backend:
        # For S3: '/bucket-name/user-home-directory' (e.g., '/my-transfer-bucket/
        users/john')
        # For EFS: '/fs-12345/user-home-directory' (e.g., '/fs-faa1a123/users/john')
        'HomeDirectory': '/my-transfer-bucket/users/example-user', # S3 example -
        replace with your bucket name
        # 'HomeDirectory': '/fs-faa1a123/users/example-user', # EFS example -
        uncomment for EFS
        '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，選擇您的新伺服器，選擇動作，然後選擇測試。
3. 輸入您在部署 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，使用者名為 `myuser`，密碼為 `MySuperSecretPassword`。
4. 如果您在部署 CloudFormation 堆疊時設定來源 IP，請選擇伺服器通訊協定並輸入其 IP 地址。

CLI

使用 CLI AWS 測試您的組態

1. 執行 [test-identity-provider](#) 命令。將每個 `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 CloudFormation 堆疊時設定的使用者名稱和密碼。如果您保留預設選項，使用者名為 `myuser`，密碼為 `MySuperSecretPassword`。
4. 如果您在部署 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 `Status Code: 200 HTTP 回應`、空字串 `Message: ""`（否則會包含失敗原因）和 `Response` 欄位。

Note

在下面的回應範例中，`Response` 欄位是「字串」的 JSON 物件（轉換為可在程式內使用的平面 JSON 字串），並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\": \"\"
}
```

Lambda 函數範本

您可以部署使用 Lambda 函數進行身分驗證的 CloudFormation 堆疊。我們提供數個範本，以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啟用 FIPS 的安全政策 CloudFormation，透過 建立啟用 FIPS 的 AWS Transfer Family 伺服器。可用的安全政策說明於 [AWS Transfer Family 伺服器的安全政策](#)

建立用於身分驗證的 CloudFormation 堆疊

1. 在 <https://console.aws.amazon.com/cloudformation> 開啟 CloudFormation 主控台。
2. 遵循AWS CloudFormation 《使用者指南》中的 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，以用於 Transfer Family 中的身分驗證。

- [Classic \(Amazon Cognito\) 堆疊範本](#)

用於建立 AWS Lambda 以用作 中自訂身分提供者的基本範本 AWS Transfer Family。它會對 Amazon Cognito 進行身分驗證，如果使用以公有金鑰為基礎的身分驗證，則會從 Amazon S3 儲存貯體傳回公有金鑰。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 做為身分提供者的基本範本。它會對 格式 AWS Secrets Manager 中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 做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 的基本範本，以及多重要素驗證，做為自訂身分提供者。
- [Azure Active Directory 範本](#)：此堆疊的詳細資訊如[AWS Transfer Family 使用 Azure Active Directory 和 向 驗證 AWS Lambda](#)的部落格文章所述。

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。

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 函數來支援 API Gateway 方法。如果您需要 RESTful API 來整合身分提供者，或想要使用 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。

對於大多數使用案例，設定自訂身分提供者的建議方法是使用 [自訂身分提供者解決方案](#)。

使用 API Gateway 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 Gateway URL。

如果您需要這些其中一項，您可以使用 Lambda 做為身分提供者，無需 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 Gateway 方法進行驗證

您可以建立 API Gateway 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的 API 操作。如需 API Gateway 服務的詳細資訊，請參閱 [API Gateway 開發人員指南](#)。

API Gateway 提供名為 `aws_iam` 的授權方法，它會根據 AWS Identity and Access Management (IAM) 為您提供與內部 AWS 相同的身分驗證。如果您使用 `aws_iam` 身分驗證，只有具有明確許可呼叫 API 的呼叫者才能到達該 API 的 API Gateway 方法。

若要使用 API Gateway 方法做為 Transfer Family 的自訂身分提供者，請為您的 API Gateway 方法啟用 IAM。在此程序中，您會為 IAM 角色提供 Transfer Family 使用閘道的許可。

Note

為了提高安全性，您可以設定 Web 應用程式防火牆。AWS WAF 是一種 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](#)。

⚠ 請勿啟用 API Gateway 快取

將 API Gateway 方法用作 Transfer Family 的自訂身分提供者時，請勿啟用 API Gateway 方法的快取。快取對身分驗證請求不適當且無效，因為：

- 每個身分驗證請求都是唯一的，並且需要即時回應，而不是快取的回應
- 快取沒有好處，因為 Transfer Family 永遠不會將重複或重複的請求傳送至 API Gateway
- 啟用快取會導致 API Gateway 以不相符的資料回應，導致對身分驗證請求的回應無效

使用 API Gateway 方法搭配 Transfer Family 進行自訂身分驗證

1. 建立 CloudFormation 堆疊。若要執行此作業：

Note

堆疊範本已更新為使用 BASE64-encoded密碼：如需詳細資訊，請參閱 [CloudFormation 範本的改善](#)。

- a. 在 <https://console.aws.amazon.com/cloudformation> 開啟 CloudFormation 主控台。
- b. 遵循AWS CloudFormation 《使用者指南》中選取 CloudFormation 堆疊範本中從現有範本部署堆疊的指示。 <https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-using-console-create-stack-template.html>
- c. 使用下列其中一個基本範本來建立 AWS Lambda後端 API Gateway 方法，以做為 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 Secrets Manager 格式的項目進行驗證 `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。如需詳細資訊，請參閱部落格 [postEnable password authentication for AWS Transfer Family using AWS Secrets Manager](#)。

- [Okta 堆疊範本](#)

您的 API Gateway 方法與 Okta 整合，做為 Transfer Family 中的自訂身分提供者。如需詳細資訊，請參閱部落格文章 [使用 Okta 做為身分提供者 AWS Transfer Family](#)。

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，您可以使用 API 方法做為 Transfer Family 中的自訂身分提供者。根據預設，Lambda 函數會使用密碼 `myuser` 來驗證名為的單一使用者 `MySuperSecretPassword`。部署之後，您可以編輯這些登入資料或更新 Lambda 函數程式碼，以執行不同的動作。

 Important

我們建議您編輯預設使用者和密碼登入資料。

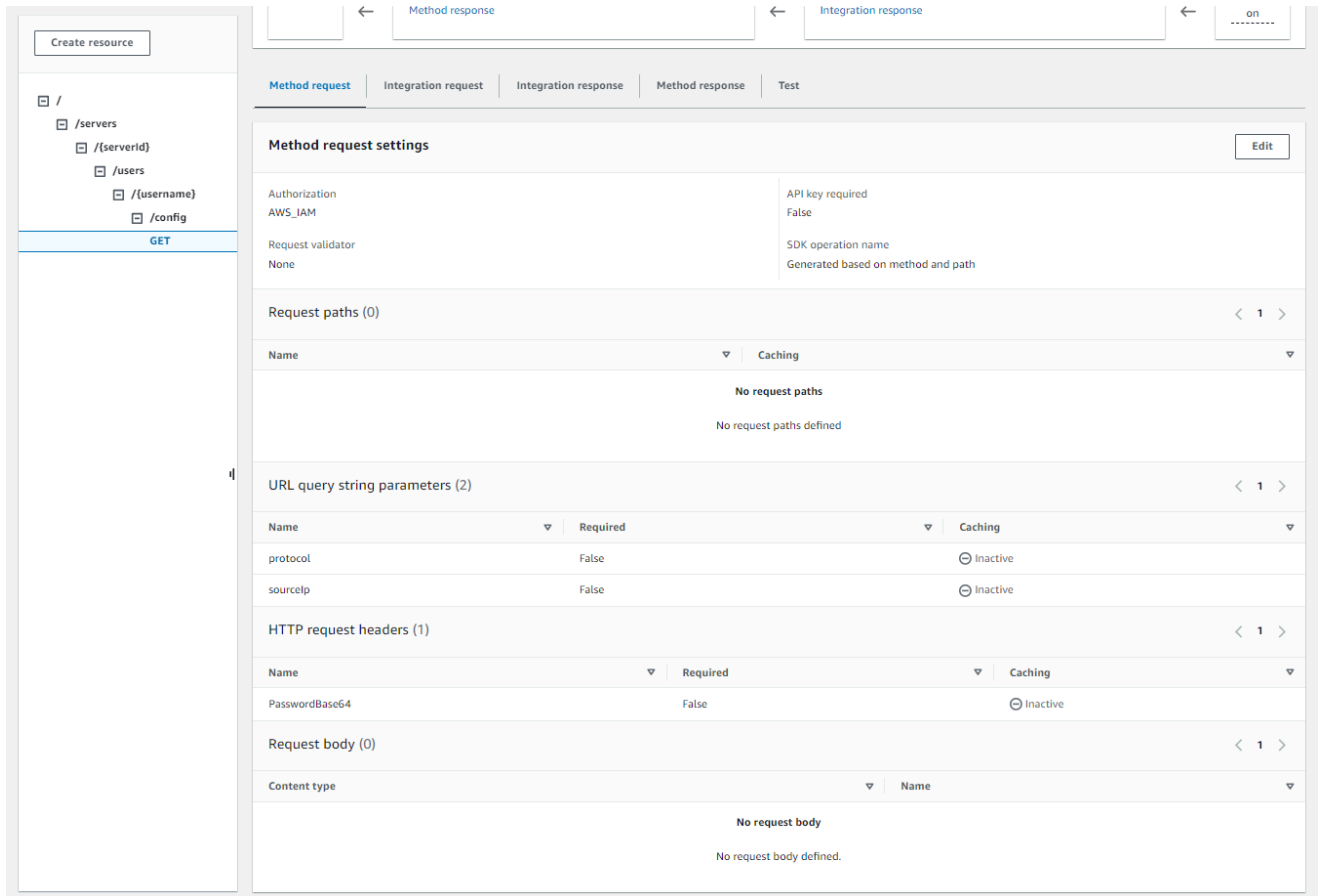
部署堆疊之後，您可以在 CloudFormation 主控台的輸出索引標籤上檢視其詳細資訊。這些詳細資訊包括堆疊的 Amazon Resource Name (ARN)、堆疊建立的 IAM 角色 ARN，以及新開道的 URL。

 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您的 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 Gateway 開發人員指南》](#) 中的 [在 API Gateway 中設定 CloudWatch API 記錄](#)。

2. 檢查您的伺服器的 API Gateway 方法組態。若要執行此作業：

- 在以下網址開啟 API Gateway 主控台：<https://console.aws.amazon.com/apigateway/>。
- 選擇 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，才能查看您的閘道。
- 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 prod，然後選擇部署。

成功部署 API Gateway 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。

API Gateway > APIs > Transfer Custom Identity Provider basic template API > Stages

Stages

Stage actions ▼ Create stage

prod

Stage details info

Edit

Stage name prod	Rate info 10000	Web ACL -
API cache ⊖ Inactive	Burst info 5000	Client certificate -
Invoke URL https://[redacted].execute-api.us-east-1.amazonaws.com/prod		
Active deployment t8agrm on December 12, 2023, 10:49 (UTC-05:00)		

Logs and tracing info

Edit

CloudWatch logs Error and info logs	Detailed metrics ⊖ Inactive	X-Ray tracing ⊖ Inactive
Custom access logging ⊖ Inactive		

Stage variables | Deployment history | Documentation history | Canary | Tags

Stage variables (0/0)

Edit

Find resources

Name	Value
No variables	

No variables associated with the stage.

Manage variables

- 在 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
- 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。
 - 選擇建立伺服器以開啟建立伺服器頁面。針對選擇身分提供者，選擇自訂，然後選取使用 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

Cancel Previous Next

- 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 API Gateway 端點的調用 URL 地址。
- 針對角色，選擇範本建立的 IAM 角色 CloudFormation。此角色允許 Transfer Family 叫用您的 API 閘道方法。

調用角色包含您為步驟 1 中建立的 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](#)。

實作您的 API Gateway 方法

若要為 Transfer Family 建立自訂身分提供者，您的 API Gateway 方法必須實作資源路徑為的單一方法 `/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。

The screenshot displays the AWS API Gateway console interface for configuring a GET method. On the left, a navigation pane shows the resource tree: `/` (root), `/servers`, `/servers/{serverId}`, `/servers/{serverId}/users`, `/servers/{serverId}/users/{username}`, and `/servers/{serverId}/users/{username}/config` (selected). The main area shows the configuration for the `/servers/{serverId}/users/{username}/config - GET - Method execution`. The `ARN` is `arn:aws:execute-api:us-east-1:123456789012:api/*GET/servers/{serverId}/users/{username}/config` and the `Resource ID` is `aw4ihv`. A diagram illustrates the flow: Client → Method request → Integration request → Lambda integration → Integration response → Method response → Client. Below this, the `Method request settings` are shown, including `Authorization: AWS_IAM`, `Request validator: None`, `API key required: False`, and `SDK operation name: Generated based on method and path`. The `Request paths (0)` section is empty. The `URL query string parameters (2)` section lists two parameters: `protocol` and `sourceIp`, both with `Required: False` and `Caching: 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 '@'。使用者名稱開頭不能是連字號 '-'、句點 '.' 或符號 '@'。

如果 Transfer Family 嘗試為您的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來驗證您的使用者。

當您使用身分提供者來驗證和授權最終使用者時，除了驗證其登入資料之外，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，只要您的身分提供者已設定每個通訊協定的特定登入資料，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。

您的 API Gateway 方法應一律傳回 HTTP 狀態碼 200。任何其他 HTTP 狀態碼表示存取 API 時發生錯誤。

Amazon S3 範例回應

回應內文範例是 Amazon S3 的 JSON 文件，格式如下。

```
{
  "Role": "IAM role with configured S3 permissions",
  "PublicKeys": [
    "ssh-rsa public-key1",
    "ssh-rsa public-key2"
  ],
  "Policy": "STS Assume role session policy",
  "HomeDirectory": "/amzn-s3-demo-bucket/path/to/home/directory"
}
```

Note

政策會以字串的形式逸出 JSON。例如：

```
"Policy":
"{
  \"Version\": \"2012-10-17\",
  \"Statement\":
  [
    {\"Condition\":
      {\"StringLike\":
        {\"s3:prefix\":
          [\"user/*\", \"user/\"]}},
      \"Resource\": \"arn:aws:s3:::amzn-s3-demo-bucket\",
      \"Action\": \"s3:ListBucket\",
```

```

    \"Effect\": \"Allow\",
    \"Sid\": \"ListHomeDir\"},
    {\"Resource\": \"arn:aws:s3::*\",
      \"Action\": [\"s3:PutObject\",
        \"s3:GetObject\",
        \"s3:DeleteObjectVersion\",
        \"s3:DeleteObject\",
        \"s3:GetObjectVersion\",
        \"s3:GetObjectACL\",
        \"s3:PutObjectACL\"],
      \"Effect\": \"Allow\",
      \"Sid\": \"HomeDirObjectAccess\"}]
  }"

```

下列範例回應顯示使用者具有邏輯主目錄類型。

```

{
  "Role": "arn:aws:iam::123456789012:role/transfer-access-role-s3",
  "HomeDirectoryType": "LOGICAL",
  "HomeDirectoryDetails": "[{\"Entry\": \"\\\", \"Target\": \"\\\"/amzn-s3-demo-bucket1\\\"}]\"",
  "PublicKeys": [""],
}

```

Amazon EFS 範例回應

回應內文範例是 Amazon EFS 的 JSON 文件，格式如下。

```

{
  "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。執行密碼身分驗證時（當您提供 Password: 標頭時），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。這類回應的範例是空的 JSON 物件。

下列範例回應顯示具有邏輯主目錄類型的使用者。

```
{
  "Role": "arn:aws:iam::123456789012:role/transfer-access-role-efs",
  "HomeDirectoryType": "LOGICAL",
  "HomeDirectoryDetails": "[{\"Entry\": \"\\\"/\\\"\", \"Target\": \"\\\"/faa1a123\\\"\"}]",
  "PublicKeys": [""],
  "PosixProfile": { "Uid": 65534, "Gid": 65534 }
}
```

您可以在 Lambda 函數中包含 JSON 格式的使用者政策。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，請編輯閘道使用的 Lambda 函數。為了協助您滿足應用程式的需求，您可以在 Node.js 中使用下列範例 Lambda 函數。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 Lambda 函數範例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，則只要身分提供者已設定特定通訊協定的登入資料，您就可以這麼做。

對於檔案傳輸通訊協定 (FTP)，我們建議您維護與 Secure Shell (SSH) 檔案傳輸通訊協定 (SFTP) 和透過 SSL 的檔案傳輸通訊協定 (FTPS) 不同的登入資料。我們建議您維護個別的 FTP 登入資料，因為與 SFTP 和 FTPS 不同，FTP 會以純文字傳輸登入資料。透過從 SFTP 或 FTPS 隔離 FTP 憑證，如果共用或公開 FTP 憑證，則使用 SFTP 或 FTPS 的工作負載會保持安全。

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，無論是邏輯或實體。同樣地，我們需要 Lambda 函數結果來傳達所需的使用者實體或邏輯目錄結構。您設定的參數取決於 [HomeDirectoryType](#) 欄位的值。

- HomeDirectoryType 設定為 PATH - 欄位 HomeDirectory 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，我們會設定一個 HomeDirectoryDetails 欄位，提供所需的 Entry/Target 映射，類似於服務受管使用者 [HomeDirectoryDetails](#) 參數中所述的值。

範例函數會列在 [中 Lambda 函數範例](#)。

搭配使用的 Lambda 函數 AWS Secrets Manager

若要使用 AWS Secrets Manager 做為您的身分提供者，您可以在範例 CloudFormation 範本中使用 Lambda 函數。Lambda 函數會使用您的登入資料查詢 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 CloudFormation 範本，請前往 [提供的 Amazon S3 儲存貯 AWS Transfer Family](#) 體。

CloudFormation 範本的改善

已改善已發佈的 CloudFormation 範本的 API Gateway 界面。範本現在搭配 API Gateway 使用 BASE64-encoded 的密碼。您現有的部署會在沒有此增強功能的情況下繼續運作，但不允許使用基本 US-ASCII 字元集以外字元的密碼。

範本中啟用此功能的變更如下：

- 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 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，並確定您有此行：

```
"password":
  "$util.escapeJavaScript($util.base64Decode($input.params('PasswordBase64'))).replaceAll(
    \',\'',\'"\')",
```

- 搜尋 RequestParameters，並確定您有此行：

```
method.request.header.PasswordBase64: false
```

如果您沒有看到更新的行，請編輯您的堆疊。如需如何更新 CloudFormation 堆疊的詳細資訊，請參閱《AWS CloudFormation使用者指南》中的[修改堆疊範本](#)。

使用多個身分驗證方法

Transfer Family 伺服器會在您使用多種身分驗證方法時控制 AND 邏輯。Transfer Family 會將此視為對自訂身分提供者的兩個個別請求：不過，其效果會合併。

這兩個請求都必須以正確的回應成功傳回，才能讓身分驗證完成。Transfer Family 需要兩個回應完成，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。

公有金鑰請求必須具有與身分提供者不同的回應。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。此操作要求在允許使用者完成身分驗證之前都成功。

對於自訂身分提供者選項，您可以指定下列任何選項來驗證身分。

- 密碼 OR 金鑰 – 使用者可以使用其密碼或其金鑰進行身分驗證。這是預設值。
- 僅限密碼 – 使用者必須提供其密碼才能連線。
- 僅限金鑰 – 使用者必須提供其私有金鑰才能連線。
- 密碼和金鑰 – 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存放的公有金鑰不相符，身分驗證會失敗。

IPv6 支援自訂身分提供者

AWS Transfer Family 自訂身分提供者完全支援 IPv6 連線。實作自訂身分提供者時，您的 Lambda 函數可以接收和處理來自 IPv4 和 IPv6 用戶端的身分驗證請求，而不需要任何額外的組態。Lambda 函數會在請求的 `sourceIp` 欄位中接收用戶端的 IP 地址，可以是 IPv4 地址（例如 203.0.113.42）或 IPv6 地址（例如 2001:db8:85a3:8d3:1319:8a2e:370:7348）。您的自訂身分提供者實作應適當處理這兩種地址格式。

Important

如果您的自訂身分提供者執行以 IP 為基礎的驗證或記錄，請確保您的實作正確處理 IPv6 地址格式。IPv6 地址的長度超過 IPv4 地址，並使用不同的表示法格式。

Note

在自訂身分提供者中處理 IPv6 地址時，請確定您使用的是適當的 IPv6 地址剖析函數，而不是簡單的字串比較。IPv6 地址可以以各種正式格式表示（例如 fd00:b600::ec2 或

fd00:b600:0:0:0:0:ec2)。在實作語言中使用適當的 IPv6 地址程式庫或函數，以正確驗證和比較 IPv6 地址。

Example在自訂身分提供者中同時處理 IPv4 和 IPv6 地址

```
def lambda_handler(event, context):
    # Extract the source IP address from the request
    source_ip = event.get('sourceIp', '')

    # Log the client IP address (works for both IPv4 and IPv6)
    print(f"Authentication request from: {source_ip}")

    # Example of IP-based validation that works with both IPv4 and IPv6
    if is_ip_allowed(source_ip):
        # Continue with authentication
        # ...
    else:
        # Reject the authentication request
        return {
            "Role": "",
            "HomeDirectory": "",
            "Status": "DENIED"
        }
```

如需實作自訂身分提供者的詳細資訊，請參閱 [使用 AWS Lambda 整合您的身分提供者](#)。

使用 AWS Directory Service for Microsoft Active Directory

您可以使用 AWS Transfer Family 驗證您的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登入資料或需要自訂授權方。

使用 AWS Managed Microsoft AD，您可以安全地透過 SFTP、FTPS 和 FTP 為存放在 Amazon Simple Storage Service (Amazon S3) 或 Amazon Elastic File System (Amazon EFS) 中的資料提供 Directory Service 使用者和群組存取權。如果您使用 Active Directory 來存放使用者的登入資料，您現在可以更輕鬆地為這些使用者啟用檔案傳輸。

您可以使用 Active Directory 連接器，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

AWS Managed Microsoft AD 用於身分的 AWS Transfer Family 伺服器，無論是在 AWS 雲端或其內部部署網路。AWS 儲存部落格包含一篇文章，詳細說明將 Active Directory 與 Transfer Family 搭配使用的解決方案：[透過的自訂身分提供者簡化 Active Directory 身分驗證 AWS Transfer Family](#)。

 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 為現有的 RADIUS 型 MFA 基礎設施啟用多重要素驗證 (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 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 做為其身分提供者的伺服器。
3. 使用 Active AWS Directory Connector 設定目錄。
4. 從一或多個 Directory Service 群組新增存取權。
5. 雖然並非必要，但我們建議您測試和驗證使用者存取。

主題

- [在您開始使用之前 AWS Directory Service for Microsoft Active Directory](#)
- [使用 Active Directory 領域](#)
- [選擇 AWS Managed Microsoft AD 做為您的身分提供者](#)
- [連線至內部部署 Microsoft Active Directory](#)
- [授予群組的存取權](#)
- [測試使用者](#)
- [刪除群組的伺服器存取權](#)
- [使用 SSH 連線至伺服器（安全殼層）](#)

- [使用樹系和信任 AWS Transfer Family 連接到自我管理的 Active Directory](#)

在您開始使用 之前 AWS Directory Service for Microsoft Active Directory

Note

AWS Transfer Family 預設限制為每個伺服器 100 個 Active Directory 群組。如果您的使用案例需要超過 100 個群組，請考慮使用自訂身分提供者解決方案，如[簡化 Active Directory 身分驗證與的自訂身分提供者 AWS Transfer Family](#)所述。

為您的 AD 群組提供唯一識別符

您必須先為 Microsoft AD 目錄中的每個群組提供唯一識別符 AWS Managed Microsoft AD，才能使用。您可以使用每個群組的安全識別符 (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 Amazon S3 或 Amazon EFS 資源。

使用下列 Windows PowerShell 命令擷取群組的 SID，將 *YourGroupName* 取代為群組的名稱。

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

Note

如果您使用 AWS Directory Service 做為身分提供者，而且如果 `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 Directory Service 許可新增至您的角色

您也需要 Directory Service API 許可才能使用 AWS Directory Service 做為您的身分提供者。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 [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，或兩者都位於信任領域。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，找不到與使用者群組相關聯的存取權。

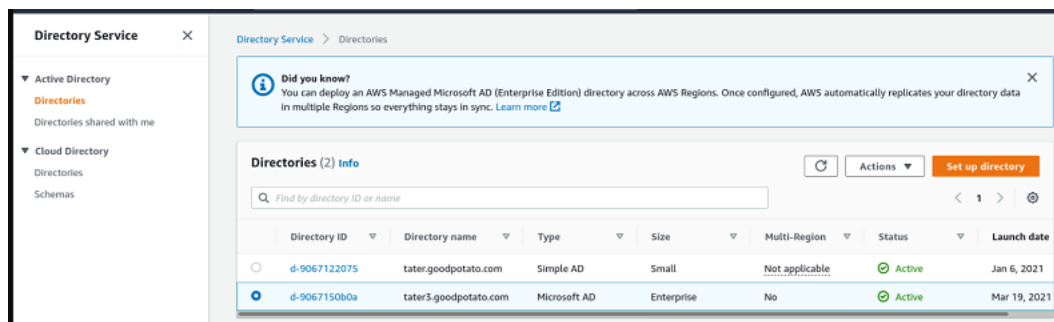
選擇 AWS Managed Microsoft AD 做為您的身分提供者

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

AWS Managed Microsoft AD 搭配 Transfer 系列使用

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

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



2. 在 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台，然後選擇建立伺服器。
3. 在選擇通訊協定頁面上，從清單中選擇一或多個通訊協定。

Note

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

4. 針對選擇身分提供者，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，然後選擇下一步。

Note

- 不支援跨帳戶和共用目錄 AWS Managed Microsoft AD。
- 若要使用 Directory Service 做為您的身分提供者來設定伺服器，您需要新增一些 Directory Service 許可。如需詳細資訊，請參閱[在您的開始使用之前 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：

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

在這些程序中，請繼續執行選擇身分提供者之後的步驟。

 Important

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。

連線至內部部署 Microsoft Active Directory

本節說明如何使用 AD Connector 設定 AWS 目錄

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，選取下一步，然後選取您的 VPC 和子網路。
5. 選取下一步，然後填入欄位，如下所示：
 - 目錄 DNS 名稱：輸入您用於 Microsoft Active Directory 的網域名稱。
 - DNS IP 地址：輸入 Microsoft Active Directory IP 地址。
 - 伺服器帳戶使用者名稱和密碼：輸入要使用之服務帳戶的詳細資訊。
6. 完成畫面以建立目錄服務。

下一個步驟是使用 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，選取您在上一個程序中新增的目錄。

授予 群組的存取權

建立伺服器之後，您必須選擇目錄中的哪些群組應該有權透過已啟用的通訊協定使用 上傳和下載檔案 AWS Transfer Family。您可以透過建立 存取來執行此操作。

 Note

AWS Transfer Family 預設限制為每個伺服器 100 個 Active Directory 群組。如果您的使用案例需要超過 100 個群組，請考慮使用自訂身分提供者解決方案，如[簡化 Active Directory 身分驗證與的自訂身分提供者 AWS Transfer Family](#)所述。

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 是使用者並屬於 groupA，且 groupA 本身包含在 groupB 中。

- 如果您授予對 groupA 的存取權，則會授予 Bob 存取權。
- 如果您將存取權授予 groupB（而不是 groupA），Bob 就無法存取。

授予群組存取權

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

Note

如需如何為您的群組尋找 SID 的資訊，請參閱 [the section called “在您開始使用 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，選擇對應至群組主目錄的 Amazon 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，若要將使用者限制在 /filetest 目錄下自己的資料夾，請在方塊中輸入下列文字。

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

若要進一步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 群組的 SID。

Note

如需如何尋找 SID 的資訊，請參閱 [the section called “在您開始使用 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-' for External Id, '/padbucket3' for Home directory, and 'ADGuy_S3_And_EFS' for Role. 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.

External Id	Home directory	Role
S-	/padbucket3	ADGuy_S3_And_EFS

測試使用者

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

Note

使用者必須剛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）。如果使用者不在群組中，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. 針對身分提供者測試，輸入使用者登入憑證，該使用者位於具有存取權的其中一個群組中。
3. 選擇測試。

您會看到身分提供者測試成功，顯示選取的使用者已獲授予伺服器存取權。

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/MDGuy_SS_And_EFS\", \"policy\": \"null\", \"userNa
  me\": \"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，您會收到下列回應。

```
"Response": "",
"StatusCode": 200,
```

```
"Message": "More than one associated access found for user's groups."
```

刪除群組的伺服器存取權

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 SSH 連線至伺服器（安全殼層）

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

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

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

此格式以搜尋聯合身為目標，限制搜尋潛在的大型 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，即使使用者應該有存取權，身分驗證也可能會失敗。

驗證之後，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 連接到自我管理的 Active Directory

Directory Service 有下列選項可用於連線至自我管理 Active Directory：

- 單向樹系信任（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。

使用信任的網域連線至伺服器時，使用者需要指定信任的網域，例如 `transferuserexample@mycompany.com`。

使用 AWS Directory Service for Entra ID Domain Services

對於只需要 SFTP Transfer 且不想管理網域的客戶，有 Simple Active Directory。或者，想要在全受管服務中受益於 Active Directory 和高可用性的客戶可以使用 AWS Managed Microsoft AD。最後，對於想要利用現有 Active Directory 樹系進行 SFTP Transfer 的客戶，有 Active Directory Connector。

注意下列事項：

- 若要根據 SFTP Transfer 需求利用現有的 Active Directory 樹系，您可以使用 [Active Directory Connector](#)。
- 如果您想要 Active Directory 的優點和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 for Microsoft Active Directory](#)。

本主題說明如何使用 Active Directory Connector 和 [Entra ID \(先前稱為 Azure AD\) Domain Services](#) 來驗證具有 Entra ID 的 SFTP Transfer 使用者。

主題

- [開始使用 AWS Directory Service for Entra ID Domain Services 之前](#)
- [步驟 1：新增 Entra ID 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 Entra ID Domain Services 之前

Note

AWS Transfer Family 預設限制為每個伺服器 100 個 Active Directory 群組。如果您的使用案例需要超過 100 個群組，請考慮使用自訂身分提供者解決方案，如[簡化 Active Directory 身分驗證與的自訂身分提供者 AWS Transfer Family](#)所述。

對於 AWS，您需要下列項目：

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

對於 Microsoft Entra，您需要下列項目：

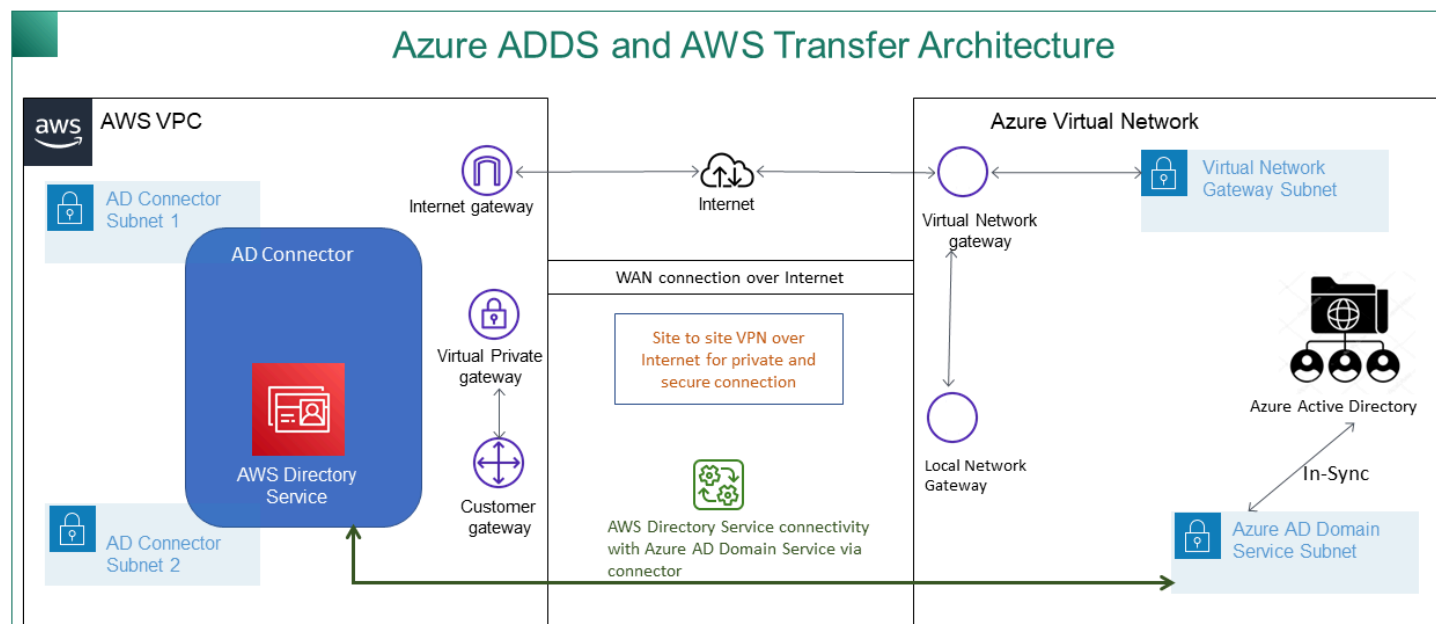
- Entra ID 和 Active Directory 網域服務
- Entra 資源群組
- Entra 虛擬網路
- Amazon VPC 與 Entra 資源群組之間的 VPN 連線

Note

這可以透過原生 IPSEC 通道或使用 VPN 設備。在本主題中，我們會在 Entra Virtual 網路閘道和本機網路閘道之間使用 IPSEC 通道。通道必須設定為允許 Entra Domain Service 端點與存放 AWS VPC 的子網路之間的流量。

- 使用 Microsoft Entra site-to-site連線的客戶閘道和虛擬私有閘道

下圖顯示開始之前所需的組態。



步驟 1：新增 Entra ID 網域服務

根據預設，Entra ID 不支援網域聯結執行個體。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 Entra ID Domain Services。如果您尚未新增 Entra DS，或現有的實作未與您希望 SFTP Transfer 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 Entra ID Domain Services 的詳細資訊，請參閱[教學課程：建立和設定 Microsoft Entra Domain Services 受管網域](#)。

 Note

當您啟用 Entra DS 時，請確定已針對您要連接 SFTP Transfer 伺服器的資源群組和 Entra 網域進行設定。


bob.us

 Azure AD Domain Services

Refresh
Delete

Overview

 Activity log

 Access control (IAM)

 Tags

 Settings

 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

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

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


bobatusa | Profile

 User

Edit
Reset password
Revoke sessions
Delete
Refresh
Got feedback?

Diagnose and solve problems

 Manage

 Profile

 Assigned roles

 Administrative units

 Groups

 Applications

 Licenses

 Devices

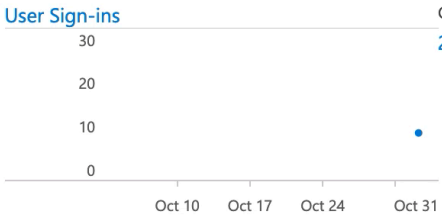
 Azure role assignments

 Authentication methods

bobatusa



bobsmith@xyz.com



Group memberships: 2

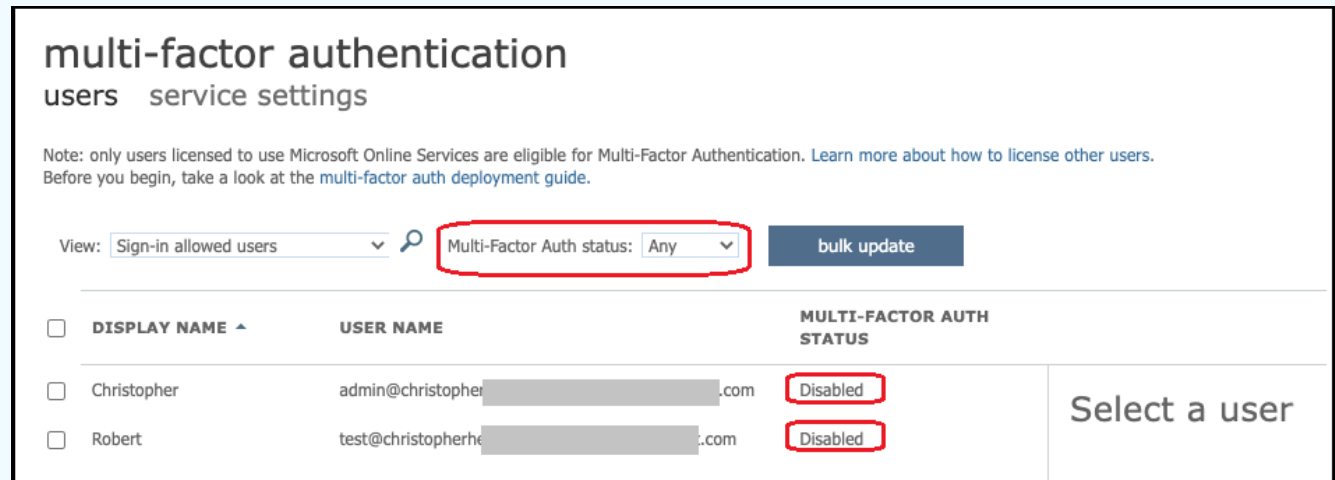
Creation time
 10/6/2021, 1:32:27 AM

Identity

Name	First name	Last name
bobatusa	Bob	Smith
User Principal Name	User type	
bobsmith@xyz.com	Member	

Tip

使用 SFTP 通訊協定的 Transfer Family 伺服器不支援 Entra ID 的多重驗證。Transfer Family 伺服器無法在使用者向 SFTP 進行身分驗證後提供 MFA 字符。嘗試連線之前，請務必停用 MFA。



步驟 3：使用 AD Connector 設定 AWS 目錄

設定 Entra DS 並在 AWS VPC 和 Entra Virtual 網路之間建立具有 IPSEC VPN 通道的服務帳戶之後，您可以從任何 AWS EC2 執行個體 ping Entra DS DNS IP 地址來測試連線。

驗證連線是否作用中後，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，選取下一步，然後選取您的 VPC 和子網路。
5. 選取下一步，然後填入欄位，如下所示：
 - 目錄 DNS 名稱：輸入您用於 Entra DS 的網域名稱。
 - DNS IP 地址：輸入您的 Entra DS IP 地址。
 - 伺服器帳戶使用者名稱和密碼：輸入您在步驟 2：建立服務帳戶中所建立服務帳戶的詳細資訊。
6. 完成畫面以建立目錄服務。

現在目錄狀態應為作用中，且已準備好與 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有權透過已啟用的通訊協定使用上傳和下載檔案 AWS Transfer Family。您可以透過建立存取來執行此操作。

Note

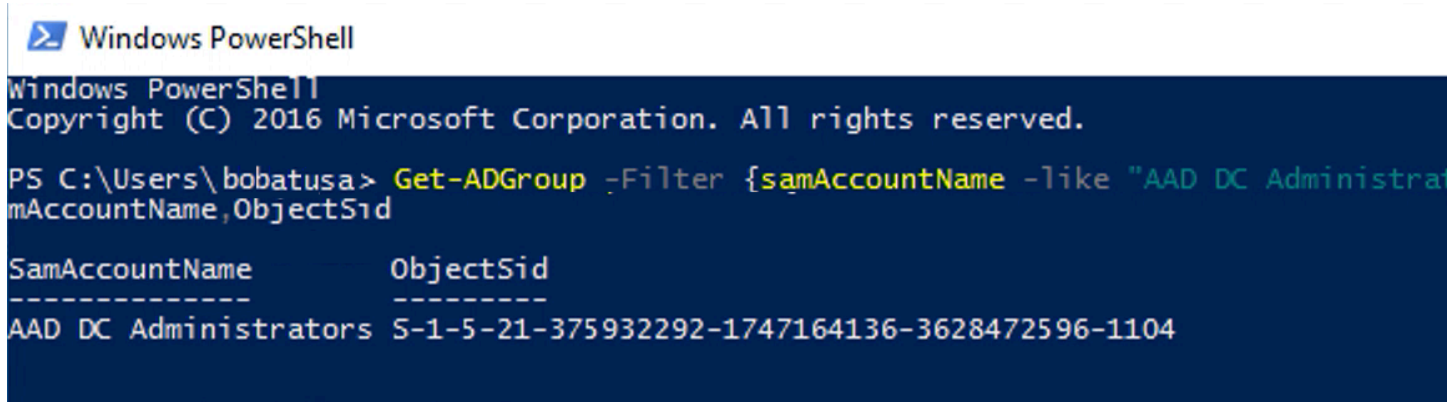
使用者必須直接屬於您要授予存取權的群組。例如，假設 Bob 是使用者並屬於 groupA，且 groupA 本身包含在 groupB 中。

- 如果您授予對 groupA 的存取權，則會授予 Bob 存取權。
- 如果您將存取權授予 groupB（而不是 groupA），Bob 就無法存取。

若要授予存取權，您需要擷取群組的 SID。

使用下列 Windows PowerShell 命令擷取群組的 SID，將 *YourGroupName* 取代為群組的名稱。

```
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 Administrators"} -Properties * | Select SamAccountName, ObjectSid

SamAccountName      ObjectSid
-----
AAD DC Administrators S-1-5-21-375932292-1747164136-3628472596-1104
```

授予 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. 輸入您從先前程序的輸出收到的 SID。
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，選擇對應至群組主目錄的 Amazon 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。使用者必須剛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）。如果使用者不在群組中，或位於多個單一群組中，則不會授予該使用者存取權。

使用邏輯目錄來簡化 Transfer Family 目錄結構

邏輯目錄可簡化您的 AWS Transfer Family 伺服器目錄結構。透過邏輯目錄，您可以使用使用者易用的名稱建立虛擬目錄結構，使用者可在連線至 Amazon S3 儲存貯體或 Amazon EFS 檔案系統時導覽。這可防止使用者查看實際的目錄路徑、儲存貯體名稱和檔案系統名稱。

Note

您應該使用工作階段政策，讓您的最終使用者只能執行您允許他們執行的操作。您應該使用邏輯目錄為最終使用者建立易於使用的虛擬目錄，並抽象化儲存貯體名稱。邏輯目錄映射只允許使用者存取其指定的邏輯路徑和子目錄，並禁止周遊邏輯根的相對路徑。Transfer Family 會驗證每個可能包含相對元素的路徑，並在我們將這些路徑傳遞至 Amazon S3 之前主動阻止這些路徑解析；這可防止您的使用者超越其邏輯映射。即使 Transfer Family 防止最終使用者存取其邏輯目錄以外的目錄，我們也建議您使用唯一角色或工作階段政策，在儲存層級強制執行最低權限。

了解 chroot 和目錄結構

chroot 操作可讓您將使用者的根目錄設定為儲存階層中的任何位置。這會將使用者限制為已設定的主目錄或根目錄，防止存取更高層級的目錄。

請考慮 Amazon S3 使用者僅限於的情況 `amzn-s3-demo-bucket/home/${transfer:UserName}`。如果沒有色彩，有些用戶端可能會允許使用者移至 `/amzn-s3-demo-bucket/home`，需要登出和登入才能返回其適當的目錄。執行 chroot 操作可避免此問題。

您可以跨多個儲存貯體和字首建立自訂目錄結構。如果您的工作流程需要儲存貯體字首本身無法提供的特定目錄配置，這會很有用。您也可以連結到 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，其中您的目錄路徑參考檔案系統中的不同位置。

使用邏輯目錄的規則

本節說明使用邏輯目錄的一些規則和其他考量事項。

映射限制

- 當 Entry 為 時，僅允許一個映射 "/" (不允許重疊路徑)。
- 邏輯目錄支援自訂 IDP 和 AD 使用者最多 2.1 MB 的映射，以及服務受管使用者最多 2,000 個項目。您可以計算映射大小，如下所示：
 1. 以格式寫入典型映射{"Entry":"/*entry-path*","Target":"/*target-path*"}, 其中 *entry-path* 和 *target-path* 是您將使用的實際值。
 2. 計算該字串中的字元，然後新增一個 (1)。
 3. 將該數字乘以您為伺服器擁有的大約映射數量。

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。

目標路徑要求

- 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，請使用 `${transfer:UserName}` 變數。
- 目標可以設定為指向不同的 Amazon S3 儲存貯體或檔案系統，只要相關聯的 IAM 角色具有存取這些儲存位置的必要許可。
- 所有目標必須以正斜線 (/) 開頭，但不能以正斜線結尾。例如，`/amzn-s3-demo-bucket/images` 是正確的，而 `amzn-s3-demo-bucket/images` 和 `/amzn-s3-demo-bucket/images/` 不是正確的。

儲存考量

- Amazon S3 是物件存放區，其中資料夾僅以虛擬概念存在。使用 Amazon S3 儲存體時，Transfer Family 會在 STAT 操作中將字首報告為目錄，即使沒有結尾斜線的零位元組物件。在 STAT 操作中，具有結尾斜線的適當零位元組物件也會報告為目錄。此行為在 [Amazon Simple Storage Service 使用者指南中的使用資料夾在 Amazon S3 主控台中組織物件](#) 中描述。

- 對於需要區分檔案和資料夾的應用程式，請使用 Amazon Elastic File System (Amazon EFS) 作為 Transfer Family 儲存選項。
- 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`。

使用者目錄值

- 指定邏輯目錄值的 參數取決於您的使用者類型：
 - 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`。
- 使用 LOGICAL `HomeDirectoryType` 時，您可以為回應中提供 `HomeDirectory` `HomeDirectoryDetails` 值。如果未指定，`HomeDirectory` 會預設為 `/`。

如需如何實作邏輯目錄的詳細資訊，請參閱 [實作邏輯目錄](#)。

實作邏輯目錄

Important

根目錄需求

- 如果您未使用 Amazon S3 效能最佳化設定，您的根目錄必須在啟動時存在。
- 對於 Amazon S3，這表示建立以正斜線 (/) 結尾的零位元組物件。
- 若要避免此需求，請考慮在建立或更新伺服器時啟用 Amazon S3 效能最佳化。
- 使用 LOGICAL `HomeDirectory` `HomeDirectoryType` 時，該值必須映射至其中一個邏輯目錄映射。服務會在使用者建立和更新期間驗證這一點，以防止組態無法運作。

邏輯主目錄組態

使用 LOGICAL 做為 `HomeDirectoryType` 時，請注意下列事項：

- `HomeDirectory` 值必須對應至其中一個現有的邏輯目錄映射。
- 系統會在使用者建立和更新期間自動驗證此項目。
- 此驗證可防止會導致存取問題的組態。

啟用邏輯目錄

若要為使用者使用邏輯目錄，請將 `HomeDirectoryType` 參數設定為 `LOGICAL`。當您建立新的使用者或更新現有的使用者時，請執行此操作。

```
"HomeDirectoryType": "LOGICAL"
```

chroot 為使用者啟用

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。項目 `/` 代表根資料夾，而目標指定儲存貯體或檔案系統中的實際位置。

Example for Amazon S3

```
[{"Entry": "/", "Target": "/amzn-s3-demo-bucket/jane"}]
```

Example for Amazon EFS

```
[{"Entry": "/", "Target": "/fs-faa1a123/jane"}]
```

您可以使用如上一個範例所示的絕對路徑，也可以使用動態替換搭配的使用者名稱 `${transfer:UserName}`，如下列範例所示。

```
[{"Entry": "/", "Target":  
"/amzn-s3-demo-bucket${transfer:UserName}"}]
```

在上述範例中，使用者已鎖定至其根目錄，且無法在階層中向上移動。

虛擬目錄結構

對於虛擬目錄結構，您可以與 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，只要使用者的 IAM 角色映射具有存取它們的許可。

在下列虛擬結構範例中，當使用者登入 AWS SFTP 時，他們位於具有 `/pics`、`/reporting`、`/doc` 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），否則如果 Amazon S3 目錄尚不存在，使用者或管理員都需要建立目錄。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": "/amzn-s3-demo-bucket1/pics"},
{"Entry": "/doc", "Target": "/amzn-s3-demo-bucket1/anotherpath/docs"},
{"Entry": "/reporting", "Target": "/amzn-s3-demo-bucket2/Q1"},
{"Entry": "/anotherpath/subpath/financials", "Target": "/amzn-s3-demo-bucket2/financials"}]
```

Note

您只能將檔案上傳到您映射的特定資料夾。這表示在先前的範例中，您無法上傳到 /anotherpath 或 anotherpath/subpath 目錄；只有 anotherpath/subpath/financials。您也無法直接映射到這些路徑，因為不允許重疊路徑。

例如，假設您建立下列映射：

```
{
  "Entry": "/pics",
  "Target": "/amzn-s3-demo-bucket/pics"
},
{
  "Entry": "/doc",
  "Target": "/amzn-s3-demo-bucket/mydocs"
},
{
  "Entry": "/temp",
  "Target": "/amzn-s3-demo-bucket2/temporary"
}
```

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，系統會將您放入根目錄 /。如果您嘗試將檔案上傳至該目錄，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 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 \
  --server-id s-11112222333344445 \
  --role arn:aws:iam::1234abcd5678:role/marymajor-role \
  --home-directory-type LOGICAL \
  --home-directory-mappings "[{\"Entry\":\"/pics\", \"Target\":\"/amzn-s3-demo-bucket1/pics\"}, {\"Entry\":\"/doc\", \"Target\":\"/amzn-s3-demo-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 \
  --server-id s-11112222333344445 \
  --role arn:aws:iam::1234abcd5678:role/marymajor-role \
  --home-directory-type LOGICAL \
  --home-directory-mappings "[{\"Entry\":\"/pics\", \"Target\":\"/amzn-s3-demo-bucket1/pics\"}, {\"Entry\":\"/doc\", \"Target\":\"/amzn-s3-demo-bucket2/test/mydocs\"}]"
```

注意下列事項：

- 如果目錄 `/amzn-s3-demo-bucket1/pics` 和 `/amzn-s3-demo-bucket2/test/mydocs` 不存在，使用者（或管理員）需要建立目錄。

Note

如果您已設定最佳化目錄，則 Transfer Family 伺服器會自動建立這些目錄。

- 當 **marymajor** 連線至伺服器並執行 `ls -l` 命令時，Mary 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` 中，她可以新增子目錄。
- Mary 新增至 `pics` 和 `doc` 的檔案分別新增至 Amazon S3 路徑 `/amzn-s3-demo-bucket1/pics` 和 `/amzn-s3-demo-bucket2/test/mydocs`。
- 在此範例中，我們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數個或所有邏輯目錄。

此範例提供邏輯首頁路徑的替代組態。

```
aws transfer create-user \
  --user-name marymajor \
  --server-id s-11112222333344445 \
  --role arn:aws:iam::1234abcd5678:role/marymajor-role \
  --home-directory-type LOGICAL \
  --home-directory /home/marymajor \
  --home-directory-mappings "[{\"Entry\":\"/home/marymajor/pics\", \"Target\":\"/amzn-s3-demo-bucket1/pics\"}, {\"Entry\":\"/home/marymajor/doc\", \"Target\":\"/amzn-s3-demo-bucket2/test/mydocs\"}]" \
  --ssh-public-key-body file://~/.ssh/id_rsa.pub
```

注意下列事項：

- 映射提供通用路徑 `/home/marymajor`，這是兩個邏輯路徑的第一部分。然後，檔案可以新增到 `pics` 和 `doc` 資料夾。
- 如先前範例所示，主目錄 `/home/marymajor` 為唯讀。

設定 Amazon EFS 的邏輯目錄

如果您的 Transfer Family 伺服器使用 Amazon EFS，則必須使用讀取和寫入存取權建立使用者的主目錄，使用者才能在其邏輯主目錄中工作。使用者無法自行建立此目錄，因為他們在其邏輯主目錄 `mkdir` 上缺少 的許可。

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，如下所示：

```
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。若要這樣做，請在 Lambda 函數中，將指定 `HomeDirectoryType` 為 **LOGICAL**，並新增 `HomeDirectoryDetails` 參數的 `Entry` 和 `Target` 值。例如：

```
HomeDirectoryType: "LOGICAL"
HomeDirectoryDetails: "[{"Entry": "\\", \"Target\": \"/amzn-s3-demo-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\\\": \\\"\\\"/amzn-s3-demo-bucket/theRealFolder\\\"\\\"]\\\",
    \"PublicKeys\": \"[ssh-rsa myrsapubkey]\\\"\",
    \"StatusCode\": 200
  }"
```

 Note

只有在您使用 API Gateway 方法做為自訂身分提供者時，才會傳回此 "Url": 行。

使用 Transfer 系列存取 FSx for NetApp ONTAP 檔案系統

內容

- [概觀](#)
- [先決條件](#)
 - [FSx for NetApp ONTAP 要求](#)
 - [所需的 IAM 許可](#)
- [FSx 儲存如何與 Transfer 系列搭配使用](#)
 - [檔案系統使用者身分](#)
- [為 FSx 建立 S3 存取點](#)
 - [存取點命名](#)
 - [建立 FSx for NetApp ONTAP 的存取點](#)
 - [設定檔案系統許可](#)
- [搭配 FSx 使用 S3 存取點別名](#)
 - [關於存取點別名](#)
 - [尋找您的存取點別名](#)
- [設定 FSx 儲存的 Transfer 系列](#)
 - [建立 IAM 角色](#)
- [管理 FSx 儲存體的使用者](#)
 - [建立使用者](#)
 - [設定多個目錄映射](#)
- [設定檔案傳輸用戶端](#)
 - [WinSCP 組態](#)
 - [其他 SFTP 用戶端](#)
- [對 FSx 儲存體進行故障診斷](#)
 - [檔案操作問題](#)

概觀

Transfer Family 透過 S3 存取點支援 Amazon FSx for NetApp ONTAP。Amazon FSx for NetApp ONTAP 是一項全受管服務，提供以 NetApp 熱門 ONTAP 檔案系統建置的高度可靠、可擴展、高效能且功能豐富的檔案儲存。當您使用 FSx 檔案系統設定 Transfer Family 時，您的使用者會使用標準檔案傳輸用戶端連線至 Transfer Family 端點。Transfer Family 會透過連接至 FSx 磁碟區的 S3 存取點路由檔案操作，同時您的資料會保留在 FSx 檔案系統上。若要進一步了解 FSx for NetApp ONTAP，請參閱[什麼是 Amazon FSx for NetApp ONTAP？](#)

此整合可讓您：

- 使用 SFTP、FTPS 或 FTP 通訊協定將檔案傳輸至企業級檔案儲存
- 透過多個通訊協定 (SFTP、NFS、SMB) 存取相同的資料
- 使用快照、備份和資料分層等 FSx 功能

Important

搭配 Transfer Family 使用 FSx 檔案系統時，不支援某些檔案操作，包括重新命名和附加操作。對於上傳操作，檔案大小限制為 5 GB。如需限制的完整清單，請參閱[存取點相容性](#)。

先決條件

使用 Amazon FSx 設定 Transfer Family 之前，您必須符合下列要求。

FSx for NetApp ONTAP 要求

若要將 FSx for NetApp ONTAP 與 Transfer Family 搭配使用，您需要：

- 執行 ONTAP 9.17.1 版或更新版本的 FSx for NetApp ONTAP 檔案系統
- 相同區域中的檔案系統和 S3 存取點 AWS
- 同時擁有檔案系統和存取點的相同 AWS 帳戶

若要進一步了解，請參閱 [Amazon FSx for NetApp ONTAP 入門](#)。

所需的 IAM 許可

您可以使用不同的許可和網路控制來設定每個 S3 存取點，S3 許可和網路控制適用於使用該存取點提出的任何請求。S3 存取點支援 IAM 資源政策，可用來依資源、使用者或其他條件控制存取點的使用。若要讓應用程式或使用者透過存取點存取檔案，存取點和基礎磁碟區都必須允許請求。如需詳細資訊，請參閱 [IAM 存取點政策](#)。

FSx 的 Amazon S3 存取點使用雙層授權模型，結合 IAM 許可與檔案系統層級許可。此方法可確保資料存取請求在 AWS 服務層級和基礎檔案系統層級獲得適當授權。

若要讓應用程式或使用者成功透過存取點存取資料，S3 存取點政策和基礎 FSx 磁碟區都必須允許請求。

若要建立和設定此整合，您需要下列許可：

- `fsx:CreateAndAttachS3AccessPoint`
- `s3:CreateAccessPoint`
- `s3:GetAccessPoint`
- `s3:PutAccessPointPolicy` (如果建立選用存取點政策)

FSx 儲存如何與 Transfer 系列搭配使用

當您使用 FSx 檔案系統設定 Transfer Family 時，下列元件可一起運作以啟用檔案傳輸：

1. 使用者使用 SFTP、FTPS 或 FTP 用戶端連線至 Transfer Family 伺服器。
2. Transfer Family 會使用服務受管身分、自訂身分提供者或來驗證使用者 AWS Directory Service for Microsoft Active Directory。驗證後，Transfer Family 會擔任與使用者相關聯的 IAM 角色。
3. 對於每個檔案操作，Transfer Family 充當標準 S3 API 用戶端，使用使用者的假設 IAM 角色向 S3 存取點提出請求，並根據 S3 存取點政策驗證許可。
4. FSx 檔案系統會驗證與存取點相關聯的檔案系統使用者是否具有執行請求操作的許可。檔案操作接著會在 FSx 磁碟區上執行。

若要讓檔案操作成功，兩個授權層都必須允許請求。

 Note

將 S3 存取點連接至 FSx 磁碟區並不會變更透過 NFS 或 SMB 直接存取磁碟區時的行為。現有的檔案通訊協定存取會繼續保持不變。

檔案系統使用者身分

每個存取點都會使用您在建立存取點時指定的檔案系統使用者身分。此身分會授權透過該存取點提出的所有檔案存取請求。檔案系統使用者是基礎 Amazon FSx 檔案系統上的使用者帳戶。如果檔案系統使用者具有唯讀存取權，則只會授權使用存取點提出的讀取請求，並封鎖寫入請求。如果檔案系統使用者具有讀寫存取權，則會授權對使用存取點建立之連接磁碟區的讀寫請求。

為 FSx 建立 S3 存取點

設定 Transfer Family 之前，您必須建立連接到 FSx 磁碟區的 S3 存取點。S3 存取點是連接至資料來源的具名網路端點，例如儲存貯體或 Amazon FSx for ONTAP 磁碟區。您可以使用 Amazon FSx 主控台、AWS CLI 或 API，建立存取點並將其連接至 FSx for NetApp ONTAP。連接後，您可以使用 S3 物件 API 來存取您的檔案資料。您的資料會繼續駐留於 Amazon FSx 檔案系統，並繼續直接用於您現有的工作負載。您繼續使用所有 FSx for NetApp ONTAP 儲存體管理功能來管理儲存體，包括備份、快照、使用者和群組配額，以及壓縮。

如需詳細資訊，請參閱[建立存取點](#)。

存取點命名

當您命名存取點時，請遵循下列準則：

- 存取點名稱在 AWS 您的帳戶和區域中必須是唯一的。
- 名稱不能以結尾 `-ext-s3alias` (保留給別名)。
- 避免在名稱中包含敏感資訊，因為它們會在 DNS 中發佈。

如需命名規則的完整清單，請參閱[存取點命名規則、限制和限制](#)。

建立 FSx for NetApp ONTAP 的存取點

使用下列程序為 FSx for NetApp ONTAP 磁碟區建立 S3 存取點。

建立存取點（主控台）

1. 在 <https://console.aws.amazon.com/fsx/>：// 開啟 Amazon FSx 主控台。
2. 在導覽窗格中，選擇檔案系統。
3. 選擇 FSx for NetApp ONTAP 檔案系統。
4. 選擇磁碟區索引標籤。
5. 選取您要連接的磁碟區。
6. 針對動作，選擇建立 S3 存取點。
7. 針對存取點名稱，輸入描述性名稱（例如 transfer-family-ap）。
8. 針對檔案系統使用者身分類型，選擇下列其中一項：
 - UNIX 身分 - 適用於具有 UNIX 安全樣式的磁碟區
 - Windows 身分 - 適用於具有 NTFS 安全樣式的磁碟區
9. （選用）對於存取點政策，輸入定義哪些 IAM 主體可以對透過此存取點存取的物件執行哪些操作的 IAM 政策。如需詳細資訊，請參閱[管理存取點存取](#)。
10. 選擇建立。
11. 建立之後，請注意要用於 Transfer Family 組態的存取點別名。

Note

當代表您連接的 SFTP/FTPS 使用者 AWS Transfer Family 存取 S3 資源時，請求來自 AWS Transfer Family 基礎設施，而不是您的 VPC。因此，使用 VPC 網路原始伺服器設定的 S3 存取點將拒絕這些請求。不過，即使您使用設定網際網路來源的存取點，Transfer Family 和存取點之間的所有流量都會保持私有，並透過 AWS 骨幹網路傳輸 - 它不會周遊公有網際網路。

設定檔案系統許可

您指定的檔案系統使用者決定 Transfer Family 使用者可以執行的操作。您必須在 FSx 磁碟區上設定適當的許可。

UNIX 範例：

```
# Create a directory for Transfer Family users
mkdir -p /vol1/transfer-users
```

```
# Set ownership to match the access point user
chown 1001:1001 /vol1/transfer-users

# Set permissions
chmod 755 /vol1/transfer-users
```

Windows 範例：

```
# Create a directory for Transfer Family users
New-Item -Path "D:\vol1\transfer-users" -ItemType Directory

# Set permissions for the file system user associated with the access point
# Replace DOMAIN\TransferUser with your Windows user identity
icacls "D:\vol1\transfer-users" /grant "DOMAIN\TransferUser:(OI)(CI)M" /T

# Verify permissions
icacls "D:\vol1\transfer-users"
```

搭配 FSx 使用 S3 存取點別名

當您搭配 Transfer Family 使用 FSx 檔案系統時，您必須使用 S3 存取點別名。Transfer Family 不支援使用存取點 ARNs 或其他 FSx 儲存的參考方法。

Important

AWS Transfer Family 僅在使用 FSx 檔案系統時支援 S3 存取點別名。您無法使用存取點 ARNs 或 virtual-hosted-style URIs。

Important

存取點必須與磁碟區位於相同的區域。

關於存取點別名

當您建立連接到 FSx 磁碟區的 S3 存取點時，Amazon S3 會自動產生存取點別名。此別名是唯一的識別符，您可以在任何使用 S3 儲存貯體名稱的地方使用。

對於連接到 FSx 磁碟區的存取點，別名使用下列格式：

```
access-point-name-metadata-ext-s3alias
```

別名範例：

```
my-fsx-ap-aqfqprnstn7aefdfbarligizwggyfouse1a-ext-s3alias
```

 Note

-ext-s3alias 字尾會保留給 FSx 存取點別名。您無法在存取點名稱中使用此尾碼。

尋找您的存取點別名

您可以在建立存取點之後找到存取點別名。

尋找存取點別名（主控台）

1. 在 <https://console.aws.amazon.com/fsx/>：// 開啟 Amazon FSx 主控台。
2. 在導覽窗格中，選擇檔案系統。
3. 選擇您的檔案系統。
4. 選擇磁碟區索引標籤，然後選取您為其建立存取點的磁碟區。
5. 移至 S3 存取點詳細資訊欄。
6. 別名會顯示在別名欄中。

尋找存取點別名 (CLI)

使用 `describe-s3-access-point-attachments` 命令。

```
aws fsx describe-s3-access-point-attachments \  
  --filters Name=file-system-id,Values=fs-0123456789abcdef0
```

回應包含別名：

```
{  
  "S3AccessPointAttachments": [  
    {  
      "S3AccessPoint": {
```

```
        "ResourceARN": "arn:aws:s3:us-east-1:111122223333:accesspoint/my-fsx-
ap",
        "Alias": "my-fsx-ap-aqfqprnstn7aefdfbarligizwgyfouse1a-ext-s3alias"
    }
}
]
```

當您設定 Transfer Family 使用者時，請在主目錄映射中使用存取點別名。

主目錄格式：

```
/access-point-alias/path/to/directory
```

範例：

```
/my-fsx-ap-aqfqprnstn7aefdfbarligizwgyfouse1a-ext-s3alias/users/jsmith
```

設定 FSx 儲存的 Transfer 系列

建立 S3 存取點之後，請設定 Transfer Family 伺服器來使用它。

建立 IAM 角色

您必須建立將 Transfer Family 存取權授予 S3 存取點的 IAM 角色。

Important

IAM 政策需要存取點 ARN 格式，而不是別名。在您的 IAM 政策資源陳述式 `arn:aws:s3:region:account-id:accesspoint/access-point-name` 中使用格式。存取點別名（結尾為 `-ext-s3alias`）僅用於主目錄映射。

建立 IAM 角色

1. 前往 <https://console.aws.amazon.com/iam/> 開啟 IAM 主控台。
2. 在導覽窗格中，選擇角色，然後選擇建立角色。
3. 針對信任的實體類型，請選擇 AWS 服務。
4. 針對使用案例，選擇轉接。

5. 選擇下一步。
6. 選擇建立政策並輸入您的政策（請參閱以下範例政策）。
7. 將政策連接至角色，然後選擇建立角色。

IAM 政策範例：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowFileOperations",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetObjectTagging",
        "s3:PutObjectTagging"
      ],
      "Resource": "arn:aws:s3:us-east-2:111122223333:accesspoint/my-fsx-ap/
object/*"
    },
    {
      "Sid": "AllowDirectoryOperations",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws:s3:us-east-2:111122223333:accesspoint/my-fsx-ap"
    }
  ]
}
```

管理 FSx 儲存體的使用者

使用使用 S3 存取點別名的主目錄映射建立 Transfer Family 使用者。

建立使用者

當您為 FSx 儲存體建立使用者時，請在主目錄映射中使用存取點別名。

建立服務受管使用者（主控台）

1. 在 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
2. 在導覽窗格中，選擇 Servers (伺服器)。
3. 選擇您的伺服器。
4. 在使用者區段中，選擇新增使用者。
5. 針對使用者名稱，輸入使用者名稱。
6. 針對角色，選擇您建立的 IAM 角色。
7. 針對主目錄，選擇受限制。
8. 對於主目錄映射，請使用存取點別名新增映射：

```
[{"Entry": "/", "Target": "/my-fsx-ap-aqfqprnstn7aefdfbarligizwgryfouse1a-ext-s3alias/users/jsmith"}]
```

建立使用者 (CLI)

使用 `create-user` 命令。將存取點別名取代為您的別名。

```
aws transfer create-user \  
  --server-id s-0123456789abcdef0 \  
  --user-name jsmith \  
  --role arn:aws:iam::111122223333:role/TransferFamilyFSxRole \  
  --home-directory-type LOGICAL \  
  --home-directory-mappings '[  
    {  
      "Entry": "/",  
      "Target": "/my-fsx-ap-aqfqprnstn7aefdfbarligizwgryfouse1a-ext-s3alias/users/  
jsmith"  
    }  
  ]'
```

設定多個目錄映射

您可以將多個虛擬目錄映射到 FSx 磁碟區上的不同路徑。

範例：個別上傳和下載目錄

```
aws transfer create-user \  
  --server-id s-0123456789abcdef0 \  
  --home-directory-mappings '[  
    {  
      "Entry": "/upload",  
      "Target": "/my-fsx-ap-aqfqprnstn7aefdfbarligizwgryfouse1a-ext-s3alias/users/jsmith/upload"  
    },  
    {  
      "Entry": "/download",  
      "Target": "/my-fsx-ap-aqfqprnstn7aefdfbarligizwgryfouse1a-ext-s3alias/users/jsmith/download"  
    }  
  ]'
```

```
--user-name jsmith \  
--role arn:aws:iam::111122223333:role/TransferFamilyFSxRole \  
--home-directory-type LOGICAL \  
--home-directory-mappings '[  
  {  
    "Entry": "/inbox",  
    "Target": "/my-fsx-ap-aqfqprnstn7aefdfbarligizwggyfouse1a-ext-s3alias/users/  
jsmith/inbox"  
  },  
  {  
    "Entry": "/outbox",  
    "Target": "/my-fsx-ap-aqfqprnstn7aefdfbarligizwggyfouse1a-ext-s3alias/users/  
jsmith/outbox"  
  }  
]'
```

設定檔案傳輸用戶端

搭配 Transfer Family 使用 FSx 檔案系統時，您必須設定檔案傳輸用戶端以停用不支援的功能。

WinSCP 組態

WinSCP 預設使用 S3 FSx 存取點不支援的暫時重新命名功能。

Warning

如果您未在 WinSCP 中停用暫時重新命名功能，檔案上傳將會失敗。

在 WinSCP 中停用暫時重新命名

1. 開啟 WinSCP。
2. 在登入對話方塊中，選擇編輯以修改工作階段設定。
3. 選擇 Advanced (進階)。
4. 在左側導覽中，於 Transfer 下，選擇 Endurance。
5. 針對啟用傳輸繼續/傳輸到暫時檔案名稱，選擇停用。
6. 選擇確定以儲存設定。

或者，您可以停用現有工作階段的此設定：

1. 連線至 Transfer Family 伺服器。
2. 選擇選項，然後選擇偏好設定。
3. 選擇 Transfer，然後選擇 Endurance。
4. 針對啟用傳輸繼續/傳輸到暫時檔案名稱，選擇停用。
5. 選擇確定。

其他 SFTP 用戶端

對於其他 SFTP 用戶端，如果可用，請停用下列功能：

- 暫時檔案上傳（上傳至暫存檔案，然後重新命名）
- 使用暫存檔案繼續傳輸
- 使用重新命名操作的原子上傳
- 上傳的附加模式

如需特定組態步驟，請參閱您的用戶端文件。

對 FSx 儲存體進行故障診斷

本節說明如何識別和解決搭配使用 Transfer Family 與 FSx 檔案系統的常見問題。

檔案操作問題

許可遭拒

如果您收到許可遭拒錯誤：

1. 確認 IAM 角色具有存取點別名的正確許可。您可以直接使用 S3 APIs 進行測試來執行此操作。
2. 檢查存取點政策是否允許 IAM 角色。
3. 確認檔案系統使用者具有目標路徑的許可。
4. 確認主目錄映射使用正確的存取點別名。

使用 WinSCP 上傳失敗

如果使用 WinSCP 上傳失敗，請停用暫時重新命名：

1. 在 WinSCP 中，選擇選項，然後選擇偏好設定。

2. 選擇 Transfer，然後選擇 Endurance。
3. 針對啟用傳輸繼續/傳輸到暫時檔案名稱，選擇停用。

如需詳細資訊，請參閱[the section called “設定檔案傳輸用戶端”](#)。

檔案上傳失敗

如果檔案上傳失敗：

1. 確認檔案大小低於 5 GB。
2. 檢查 FSx 磁碟區是否有足夠的可用儲存空間。
3. 監控 CloudWatch 指標以進行限流。

Transfer Family Web 應用程式

您可以建立 Web 應用程式，以啟用簡單的介面，透過 Web 瀏覽器在 Amazon Simple Storage Service (S3) 之間來回傳輸資料。這不需要您建立或佈建 AWS Transfer Family 伺服器。

在推出 Transfer Family Web 應用程式之前，最終使用者需要使用用戶端、自訂建置或第三方解決方案來存取 Amazon S3 中的資料。這是因為客戶和合作夥伴的嚴格安全要求，以及因為用戶端應用程式對非技術使用者難以操作。

啟動 Web 應用程式後，您現在可以擴展品牌化、安全且高度可用的入口網站，讓您的最終使用者在 Amazon S3 中瀏覽、上傳和下載資料。Web 應用程式原生與 AWS IAM Identity Center 和 Amazon S3 Access Grants 整合。這表示只有經過身分驗證的使用者才能檢視他們獲授權存取的資料。Web 應用程式使用適用於 [Amazon S3 的 Storage Browser](#) 建置，並在全受管產品中提供相同的最終使用者功能，而無需編寫程式碼或託管您自己的應用程式。

如需 AWS 服務與 Transfer Family Web 應用程式搭配使用之其他的詳細資訊，請參閱下列文件：

- [《Amazon Simple Storage Service 使用者指南》中的使用 S3 存取授權管理存取](#)
- [AWS IAM Identity Center 使用者指南](#)
- [Amazon S3 Access Grants 研討會](#)
- [宣布適用於全受管 Amazon S3 檔案傳輸的 AWS Transfer Family Web 應用程式](#)

下列資源可協助您開始使用 Transfer Family Web 應用程式。

- 使用者指南提供設定 Transfer Family Web 應用程式的詳細step-by-step演練，如下所示：[教學課程：設定基本 Transfer Family Web 應用程式](#)
- AWS 入門資源中心在此處提供教學課程：[AWS Transfer Family Web 應用程式入門](#)。
- 檢視 [Web 應用程式入門 AWS Transfer Family](#)。

AWS 區域 適用於 Transfer Family Web 應用程式

AWS Transfer Family Web 應用程式可在所有 Transfer Family 支援的區域中使用，如[AWS 區域表](#)所列，亞太區域（紐西蘭）和除外 AWS European Sovereign Cloud。

提供 Web 應用程式的所有 AWS 區域 都支援 Web 應用程式的 VPC 端點。

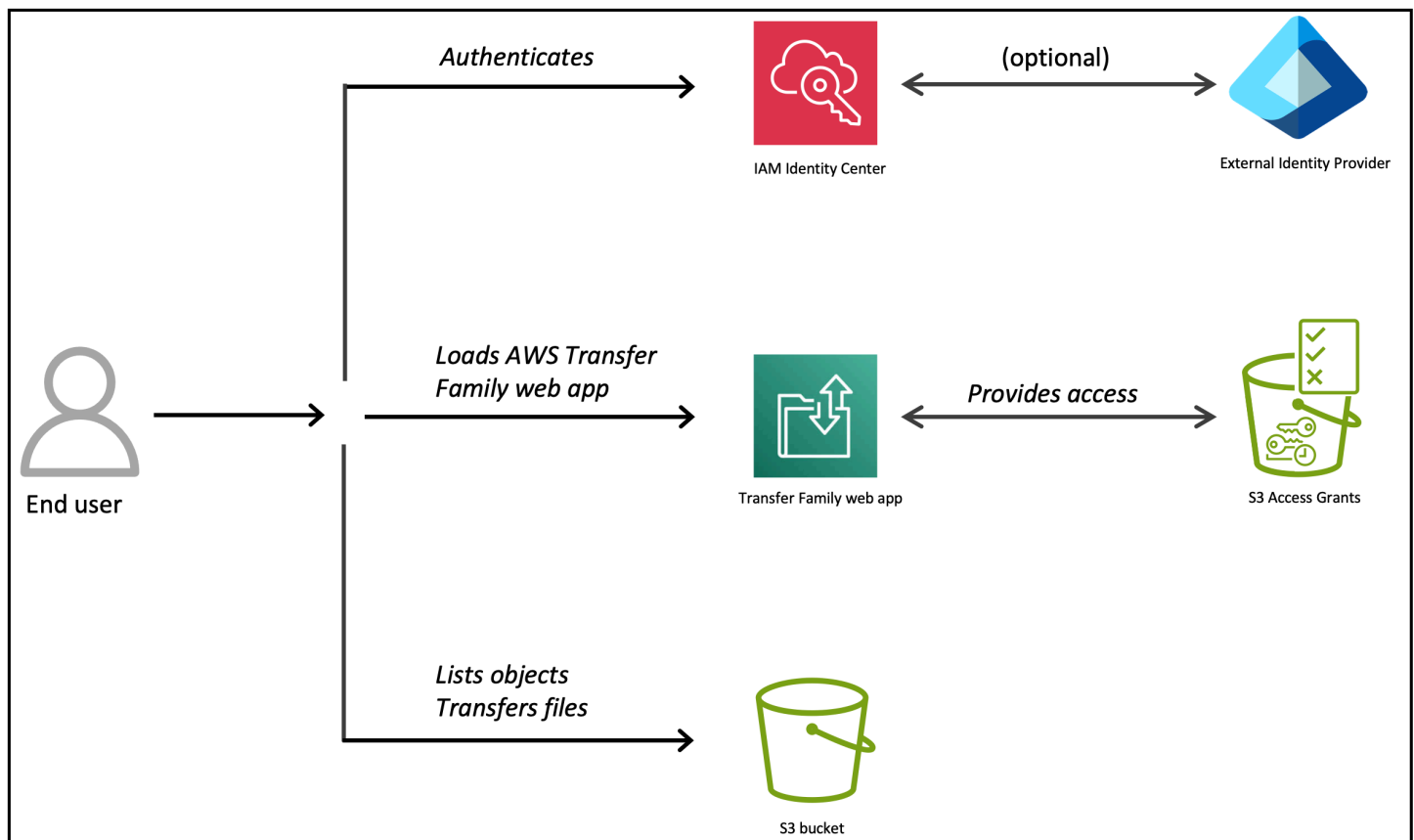
AWS Transfer Family Web 應用程式的瀏覽器相容性

Transfer Family Web 應用程式支援下列瀏覽器。

瀏覽器	版本	相容性
Microsoft Edge	最近 3 個版本	相容
Mozilla Firefox	最近 3 個版本	相容
Google Chrome	最近 3 個版本	相容
Apple Safari	最近 3 個版本	相容

如何建立 Transfer Family Web 應用程式

下圖說明 Transfer Family Web 應用程式架構。



根據圖表，您可以看到 Transfer Family Web 應用程式與下列 互動 AWS 服務：

- Amazon S3 for storage 和 Amazon S3 Access Grants 以取得工作階段登入資料。
- AWS IAM Identity Center 作為聯合身分提供者。
- 如果您為 Web 應用程式設定自訂 URL，Amazon CloudFront。

使用 Web 應用程式時，請注意下列限制。

- 每個查詢的搜尋結果數目上限：10,000
- Transfer Family Web 應用程式使用的 Amazon S3 儲存貯體必須與 Web 應用程式本身位於相同的帳戶中。目前不支援跨帳戶儲存貯體。
- 每個查詢的搜尋廣度上限：10,000 個搜尋的檔案
- 每個檔案的最大上傳大小：160 GB (149 GiB)
- 複製的大小上限：5.36 GB (5 GiB)
- 不支援以點 (.) 開頭或結尾的資料夾名稱

先決條件

在 AWS Identity and Access Management 中，設定必要的角色。貼上我們在說明中提供的程式碼區塊。如需設定必要角色的資訊，請參閱 [設定 Transfer Family Web 應用程式的 IAM 角色](#)。

- 建立身分承載角色。
- 建立 S3 Access Grants 要使用的 IAM 角色。S3 Access Grants 會擔任此 IAM 角色，將臨時憑證提供給已註冊 Amazon S3 位置的承授者。

建立 Transfer Family Web 應用程式的程序

若要建立 Web 應用程式並啟動和執行最終使用者，請執行下列任務：

1. 設定 IAM Identity Center 做為您的聯合身分提供者。在 IAM Identity Center 中執行下列任務。如需設定 IAM Identity Center 的詳細資訊，請參閱 [為 Transfer Family Web 應用程式設定您的身分提供者](#)。
 - a. 如果您還沒有 IAM Identity Center 執行個體，請建立該執行個體。
 - b. 判斷您的身分來源。它可以是預設的 IAM Identity Center 目錄或第三方供應商（例如 Okta）。
 - c. 建立或識別將使用 Web 應用程式的使用者或群組。

- d. 如果您使用身分來源的 IAM Identity Center 目錄，請注意您建立的使用者或群組 IDs。稍後當您使用 S3 Access Grants 建立存取授權時，您需要這些授權。
 2. 在 Amazon S3 中，設定 Amazon S3 Access Grants。如需 S3 存取授權的詳細資訊，請參閱[設定 Transfer Family Web 應用程式的 Amazon S3 Access Grants](#)。
 - 如果您還沒有 S3 Access Grants 執行個體，請建立該執行個體 AWS 區域。
 - 使用 IAM 角色註冊您的位置。
 - 建立存取授權。
 3. 在 Transfer Family 中，執行下列任務。
 - a. 建立 Transfer Family Web 應用程式。如需如何建立 Transfer Family Web 應用程式的詳細資訊，請參閱[設定 Transfer Family Web 應用程式](#)。
-  **Important**

為您的 Web 應用程式使用的所有 Amazon S3 儲存貯體設定跨來源資源共用 (CORS)。如需設定 CORS 的詳細資訊，請參閱[為您的儲存貯體設定跨來源資源共用 \(CORS\)](#)。
- b. 將使用者或群組指派給 Web 應用程式。如需如何指派使用者和群組的詳細資訊，請參閱[將使用者或群組指派或新增至 Transfer Family Web 應用程式](#)。
 - c. （選用）使用自訂 URL 更新 Web 應用程式的存取端點。如需建立自訂 URL 的詳細資訊，請參閱[使用自訂 URL 更新您的存取端點](#)。
 - d. 為您的最終使用者提供存取端點 URL，讓他們可以登入並與您的 Web 應用程式互動。

為 Transfer Family Web 應用程式設定您的身分提供者

下一節說明如何設定您的身分提供者。

若要開始，您必須擁有身分來源。您可以使用 IAM Identity Center 目錄、AWS Directory Service for Microsoft Active Directory 或外部身分提供者。Transfer Family 使用 IAM Identity Center 做為聯合身分提供者，這是存放使用者登入資料並跨多個組織驗證使用者的系統。

如果您不是使用 IAM Identity Center 目錄做為身分來源，請參閱下列主題：

- [管理外部身分提供者](#)
- [連接至 Microsoft AD 目錄](#)

- [IAM Identity Center 的組織和帳戶執行個體](#)
- [IAM Identity Center 身分來源教學課程](#)

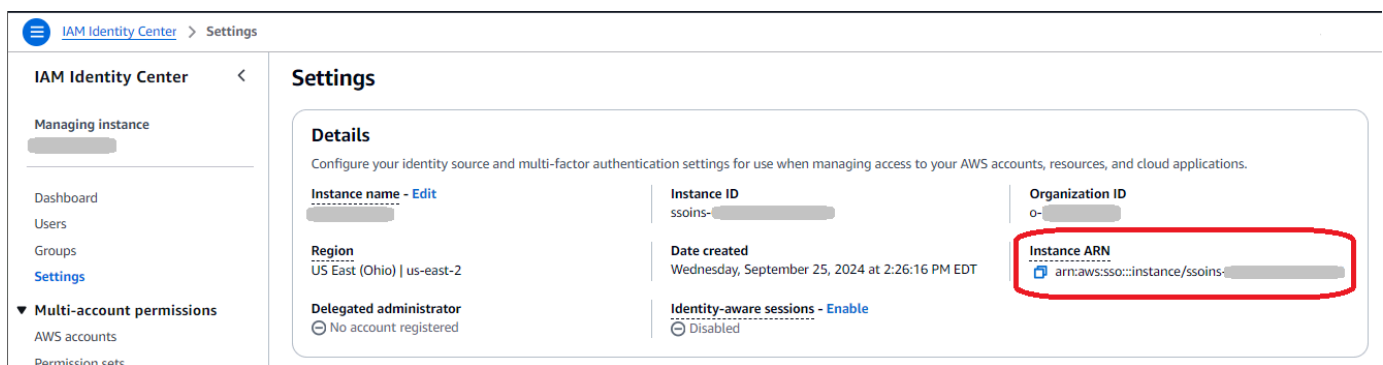
Note

每個執行個體的每個 IAM Identity Center 中只能有一個身分來源 AWS 區域。如需詳細資訊，請參閱 [IAM Identity Center 先決條件和考量事項](#)。

如果您打算使用 IAM Identity Center 目錄做為身分來源，並且想要快速設定，您可以略過本主題，並前往 從精靈 [建立 Transfer Family Web 應用程式](#) 建立 IAM Identity Center 執行個體。

設定 AWS IAM Identity Center 以搭配 Transfer Family Web 應用程式使用

1. 登入 AWS 管理主控台 並在 <https://console.aws.amazon.com/singlesignon/> 開啟 AWS IAM Identity Center 主控台。
2. 您可以建立和使用的帳戶執行個體或的組織執行個體 AWS IAM Identity Center。
 - 如需帳戶執行個體的詳細資訊，請參閱 [建立的帳戶執行個體 AWS IAM Identity Center](#)。透過 IAM Identity Center 的帳戶執行個體，您可以部署支援的 AWS 受管應用程式和 OpenID Connect (OIDC) 型客戶受管應用程式。帳戶執行個體支援在單一 中隔離部署應用程式 AWS 帳戶，利用 IAM Identity Center 人力資源身分和存取入口網站功能。
 - 如需組織執行個體的詳細資訊，請參閱 [IAM Identity Center 的組織執行個體](#)。您可以使用單一組織執行個體集中管理使用者和群組的存取。
3. 在 IAM Identity Center Settings 頁面上，記下您的執行個體 ARN。當您建立 Amazon S3 Access Grant 執行個體時，將需要此值。



4. 建立一或多個使用者和選擇性地群組，以搭配 Transfer Family Web 應用程式使用。如果您使用 IAM Identity Center 目錄做為身分提供者，您也可以直接從 Web 應用程式本身新增使用者。如需詳細資訊，請參閱[將使用者或群組指派或新增至 Transfer Family Web 應用程式](#)。

設定 Transfer Family Web 應用程式的 IAM 角色

您需要兩個角色：一個用於做為 Web 應用程式的身分持有者角色，第二個用於設定存取授權。身分持有者角色是在其工作階段中包含已驗證使用者身分的角色。它用於代表使用者向 S3 Access Grants 提出資料存取請求。

Note

您可以略過建立身分承載角色的程序。如需有關讓 Transfer Family 服務建立身分承載角色的資訊，請參閱 [建立 Transfer Family Web 應用程式](#)。

您可以略過建立存取授權角色的程序。在建立存取授權的程序中，在您註冊 S3 位置的步驟中，選擇建立新角色。

建立身分承載角色

1. 登入 AWS 管理主控台，並在 <https://console.aws.amazon.com/iam/> 開啟 IAM 主控台。
2. 選擇角色，然後選擇建立角色。
3. 選擇自訂信任政策，然後貼上下列程式碼。

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

4. 選擇下一步，然後略過新增許可，然後再次選取下一步。
5. 輸入名稱，例如 `web-app-identity-bearer`。
6. 選擇建立角色以建立身分承載角色。
7. 從清單中選擇您剛建立的角色，然後在許可政策面板中，選擇新增許可 > 建立內嵌政策。
8. 在政策編輯器中，選取 JSON，然後貼上下列程式碼區塊。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetDataAccess",
        "s3:ListCallerAccessGrants",
        "s3:ListAccessGrantsInstances"
      ],
      "Resource": "*"
    }
  ]
}
```

9. 針對政策名稱，輸入 `AllowS3AccessGrants`，然後選取建立政策。

接著，您可以建立 S3 Access Grants 擔任的角色，將臨時憑證提供給承授者。

Note

如果您允許服務為您建立身分持有者角色，該角色會設定混淆代理人保護。因此，其程式碼與此處顯示的內容不同。

建立存取授權角色

1. 登入 AWS 管理主控台，並在 <https://console.aws.amazon.com/iam/> 開啟 IAM 主控台。
2. 選擇角色，然後選擇建立角色。此角色應具有存取中 S3 資料的許可 AWS 區域。
3. 選擇自訂信任政策，然後貼上下列程式碼。

```
{
  "Version": "2012-10-17",
```

```
"Statement": [
  {
    "Effect": "Allow",
    "Principal": {
      "Service": "access-grants.s3.amazonaws.com"
    },
    "Action": [
      "sts:AssumeRole",
      "sts:SetContext"
    ]
  }
]
```

4. 選擇下一步新增最少的政策，如[註冊位置](#)中所述。雖然不建議，但您可以新增 AmazonS3FullAccess 受管政策，這可能過於寬鬆，滿足您的需求。
5. 選擇下一步，然後輸入名稱（例如 access-grants-location）。
6. 選擇建立角色以建立角色。

Note

如果您允許服務為您建立存取授權角色，該角色會設定混淆代理人保護。因此，其程式碼與此處顯示的內容不同。

設定 Transfer Family Web 應用程式

本節說明建立 Transfer Family Web 應用程式的程序。若要指派可以使用的使用者和群組，請參閱 [將使用者或群組指派或新增至 Transfer Family Web 應用程式](#)。

Note

重複這些程序來新增其他 Web 應用程式。您可以重複使用先前建立的 IAM 角色。請務必將新 Web 應用程式的存取端點新增至每個儲存貯體的跨來源資源共用 (CORS) 政策。

建立 Transfer Family Web 應用程式

Note

如果您不是使用身分提供者的 IAM Identity Center 目錄，請勿嘗試建立 Web 應用程式，除非您已設定 IAM Identity Center 並設定第三方身分提供者，如中所述 [為 Transfer Family Web 應用程式設定您的身分提供者](#)。

完成下列步驟以建立 Transfer Family Web 應用程式。

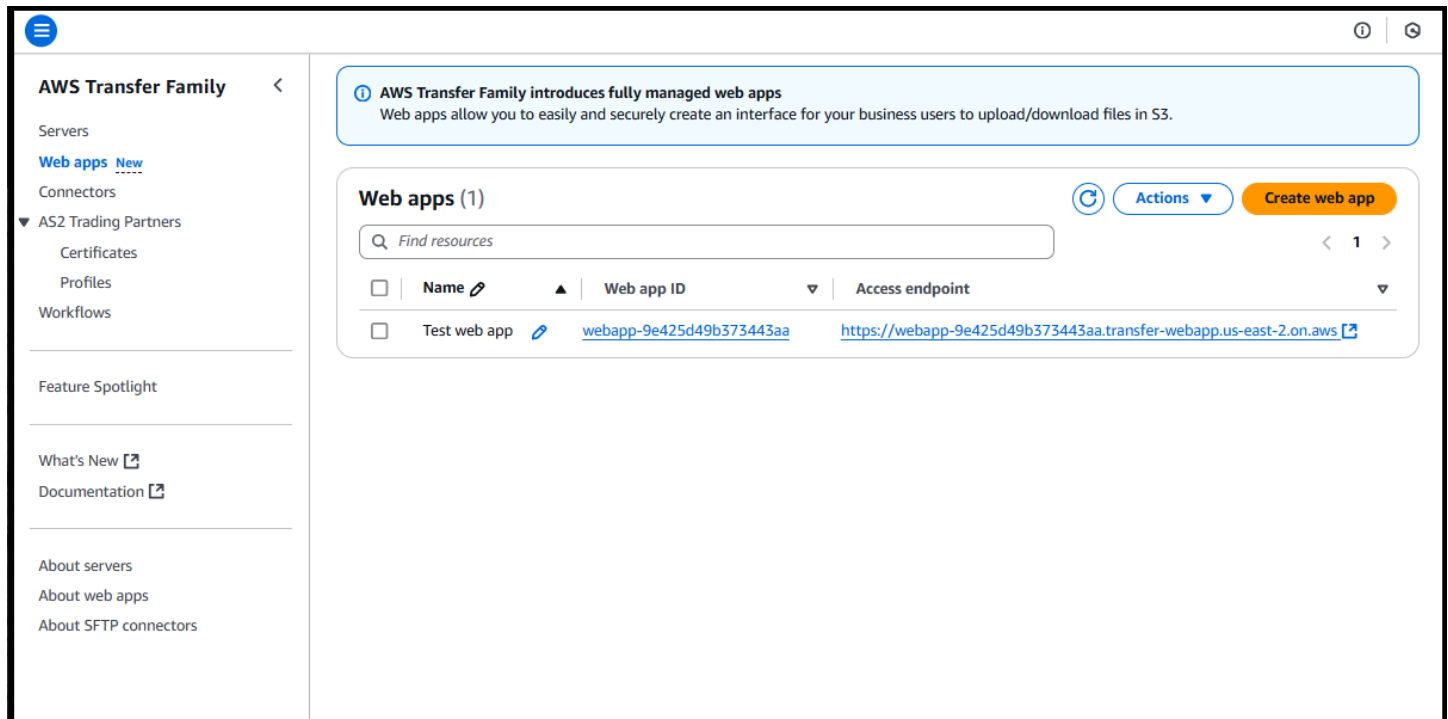
建立 Transfer Family Web 應用程式

1. 登入 AWS 管理主控台 並在 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
2. 在左側導覽窗格中，選擇 Web 應用程式。
3. 選擇建立 Web 應用程式。

對於身分驗證存取，窗格會填入如下。

- 如果您已在 中建立組織或帳戶執行個體 AWS IAM Identity Center，則會看到此訊息：您的 AWS Transfer Family 應用程式已連線至 IAM Identity Center 的帳戶執行個體。
 - 如果您已經有帳戶執行個體，而且是組織執行個體的成員，您可以選擇要連線的執行個體。
 - 如果您還沒有帳戶執行個體，或是組織執行個體中的成員，您會看到建立帳戶執行個體的選項。
4. 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 VPC 中建立 Transfer Family Web 應用程式](#)。
 5. 在許可類型窗格中，您可以使用先前建立的角色，或讓服務為您建立角色。
 - 如果您已建立身分承載角色，請選擇使用現有角色，然後從選取現有角色功能表中選擇您的角色。
 - 若要讓服務為您建立角色，請選擇建立並使用新的服務角色。
 6. 在 Web 應用程式單位窗格中，選擇值。一個 Web 應用程式單元允許來自最多 250 個唯一工作階段的 Web 應用程式活動。建立 Web 應用程式時，您可以根據預期的尖峰工作負載磁碟區佈建所需的單位數量。變更 Web 應用程式單位會影響您的帳單。如需關於定價的資訊，請參閱 [AWS Transfer Family 定價](#)。
 7. 如果您在 中使用 Transfer Family AWS GovCloud (US) Region，您可以在 FIPS Enabled 窗格中選取 FIPS Enabled 端點核取方塊。對於所有其他 AWS 區域，此選項無法使用。

8. (選用) 新增標籤以協助您組織 Web 應用程式。我們建議您新增名為索引鍵的標籤，以及描述性名稱為值的標籤。
9. 選擇下一步。在此畫面上，您可以選擇為您的 Web 應用程式提供標題。如果您未提供標題，則會提供 Transfer Web App 的預設標題。您也可以上傳標誌和 favicon 的影像檔案。
10. 選擇下一步，然後選擇建立 Web 應用程式。



Note

請務必為從 Web 應用程式端點存取的所有儲存貯體設定跨來源資源共用 (CORS) 政策。

IP 定址

Transfer Family Web 應用程式使用雙堆疊端點，同時支援 IPv4 和 IPv6 連線。針對身分驗證，Web 應用程式會使用 AWS IAM Identity Center，這也支援透過雙堆疊端點的 IPv6。

如果您的帳戶在啟動雙堆疊 IAM Identity Center 端點支援時，在區域中有 Web 應用程式，則該帳戶和區域中的所有 Web 應用程式都會繼續使用 IPv4-only 的 IAM Identity Center 端點來回溯相容性。這同時適用於現有和新建立的 Web 應用程式。啟動時沒有 Web 應用程式的帳戶會使用 IAM Identity

Center 雙堆疊端點。如果您需要變更 Web 應用程式使用的 IAM Identity Center 端點，請聯絡 AWS Support。

Note

若要判斷 Web 應用程式使用的端點，請在重新導向至 IAM Identity Center 登入頁面時檢查 URL：

- IPv4-only：[Region].signin.aws.amazon.com
- 雙堆疊：[Region].sso.signin.aws

如果您的組織使用防火牆或網路閘道，允許同時列出現有的 IPv4 和新的雙堆疊 IAM Identity Center 端點，以確保存取不中斷，無論您的 Web 應用程式使用哪個端點。如需允許清單的網域和 URL 端點的完整清單，請參閱《IAM Identity Center 使用者指南》中的[更新防火牆和閘道以允許存取 AWS 入口網站](#)。

對於 VPC 中託管的 Web 應用程式，您可以選擇 VPC 端點的 IP 地址類型：僅限 IPv4 或雙堆疊 (IPv4 和 IPv6)。預設為雙堆疊以實現回溯相容性。如果您的 VPC 是僅限 IPv4 或您不需要 IPv6 連線，請選擇 IPv4。IPv4-only 您可以在建立後更新 Web 應用程式來變更 IP 地址類型。

在 VPC 中建立 Transfer Family Web 應用程式

本節說明在 VPC 中建立 Transfer Family Web 應用程式的程序。您可以在虛擬私有雲端 (VPC) 中託管 Web 應用程式的端點，以用於在 Amazon S3 儲存貯體之間傳輸資料，而無需透過公有網際網路。若要指派可以使用 Web 應用程式的使用者和群組，請參閱[將使用者或群組指派或新增至 Transfer Family Web 應用程式](#)。

Note

若要在使用 Transfer Family Web 應用程式 VPC 端點時確保私有 end-to-end 資料流程，您必須實作三個額外的元件。首先，設定 Amazon S3 Control API 操作的 PrivateLink 端點，這是 Amazon S3 Access Grants API 呼叫的必要項目。其次，使用 PrivateLink Amazon S3 Gateway 端點（適用於 VPC 內的流量）或 Amazon S3 Interface 端點（適用於透過 VPN 或 Direct Connect 來自內部部署網路的流量）來設定 Amazon S3 資料存取的端點。第三，更新儲存貯體政策以僅允許來自這些 VPC 端點的流量，以鎖定您的 Amazon S3 儲存貯體存取。此組合可確保所有資料傳輸都保留在您的私有網路基礎設施中，且絕不會周遊公有網際網路。

建立 Transfer Family Web 應用程式

先決條件

- AWS IAM Identity Center 使用設定的身分提供者進行設定。請參閱 [為 Transfer Family Web 應用程式設定您的身分提供者](#)。
- 已設定 VPC 和網路元件。請參閱[建立 VPC](#)。
- 為 Amazon S3 控制操作設定的 API 端點。請參閱[存取 Amazon S3 介面端點](#)。
- Amazon S3（閘道或界面）設定的 VPC 端點。請參閱 [Amazon S3 的 VPC 端點類型](#)。如果您使用的是介面端點，則必須啟用私有 DNS。如需範例，請參閱[使用 介紹 Amazon S3 的私有 DNS 支援 AWS PrivateLink](#)。

Note

AWS IAM Identity Center 不支援 VPC 端點；所有身分驗證請求都會傳輸公有網際網路。此外，Transfer Family Web 應用程式需要網際網路存取才能載入靜態內容（例如 JavaScript、CSS 和 HTML 檔案）。公有網際網路存取的需求與資料存取不同。您的 VPC 端點可確保透過 VPC 基礎設施路由連線。

建立 Transfer Family Web 應用程式

1. 登入 AWS 管理主控台 並在 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
2. 在左側導覽窗格中，選擇 Web 應用程式。
3. 選擇建立 Web 應用程式。對於身分驗證存取，窗格會填入如下。
 - 如果您已在 中建立組織或帳戶執行個體 AWS IAM Identity Center，則會看到此訊息：您的 AWS Transfer Family 應用程式已連線至 IAM Identity Center 的帳戶執行個體。
 - 如果您已經有帳戶執行個體，而且是組織執行個體的成員，您可以選擇要連線的執行個體。
 - 如果您還沒有帳戶執行個體，或是組織執行個體中的成員，您會看到建立帳戶執行個體的選項。
4. 在端點組態區段中，選擇使用者存取 Web 應用程式的方式：
 - 可公開存取：您可以透過 HTTPS 透過公有存取您的 Web 應用程式端點。此選項不需要任何 VPC 組態，因此設定簡單且適合廣泛公開使用的應用程式。

- VPC 託管：您的 Web 應用程式端點託管在虛擬私有雲端 (VPC) 中 AWS Direct Connect，透過 VPC 網路或 VPN 連接提供私有網路存取。此選項透過網路隔離提供增強的安全性，建議用於內部應用程式。

設定 VPC 託管端點時，您需要指定：

- VPC：選取現有的 VPC 或建立新的 VPC。建立 VPC 按鈕可供使用。
- IP 地址類型：選擇 VPC 端點的 IP 地址類型。為僅限 IPv4 的連線選取 IPv4，或為 IPv4 和 IPv6 連線選取雙堆疊。IPv4-only 預設值為雙堆疊。
- 可用區域：選擇部署端點的可用區域。
- 子網路：選取每個所選可用區域內的子網路。
- 安全群組：選取或建立安全群組，以根據來源 IP 地址控制存取。如果未指定，則會使用 VPC 的預設安全群組。透過 VPC 主控台管理安全群組。設定您的 VPC 安全群組，以允許 TCP 連接埠 443 透過 HTTPS 從網路傳入流量。這是 IAM Identity Center 身分驗證和 Web 應用程式靜態內容載入的必要項目。

Note

無法為 VPC 端點自訂存取端點。若要新增自訂 URL，請使用公有端點。

建立後步驟

- 請務必為從 Web 應用程式端點存取的所有儲存貯體設定跨來源資源共用 (CORS) 政策。請參閱 [跨來源資源共用 \(CORS\) 政策](#)。
- 更新您的儲存貯體政策，僅允許透過 VPC 端點源自 VPC 的流量。請參閱 [限制特定 VPC 端點的存取](#)。
- 指派或新增使用者或群組至 Transfer Family Web 應用程式。請參閱 [將使用者或群組指派或新增至 Transfer Family Web 應用程式](#)。

跨來源資源共用 (CORS) 政策

您必須為 Web 應用程式使用的所有儲存貯體設定跨來源資源共用 (CORS)。如需 CORS 的詳細資訊，請參閱「[為您的儲存貯體設定跨來源資源共用 \(CORS\)](#)」。

⚠ Important

使用下列範例政策之前，請將允許原始伺服器取代為您的存取端點。否則，最終使用者在嘗試存取 Web 應用程式上的位置時，會收到錯誤。

範例政策：

```
[
  {
    "AllowedHeaders": [
      "*"
    ],
    "AllowedMethods": [
      "GET",
      "PUT",
      "POST",
      "DELETE",
      "HEAD"
    ],
    "AllowedOrigins": [
      "https://vpce-1234567-example.vpce-mq.transfer-webapp.us-east-1.on.aws"
    ],
    "ExposeHeaders": [
      "last-modified",
      "content-length",
      "etag",
      "x-amz-version-id",
      "content-type",
      "x-amz-request-id",
      "x-amz-id-2",
      "date",
      "x-amz-cf-id",
      "x-amz-storage-class",
      "access-control-expose-headers"
    ],
    "MaxAgeSeconds": 3000
  }
]
```

限制特定 VPC 端點的存取

下列 Amazon S3 儲存貯體政策範例限制只能從 ID 為 `vpce-1a2b3c4d` 的 VPC 端點存取特定儲存貯體 `amzn-s3-demo-bucket`。如果未使用指定的端點，政策會拒絕所有對儲存貯體的存取。`aws:SourceVpce` 條件會指定端點。`aws:SourceVpce` 條件不需要 VPC 端點資源的 ARN，其只需要 VPC 端點 ID。如需更新儲存貯體政策以僅允許來自 VPC 的流量的詳細資訊，請參閱[使用儲存貯體政策控制來自 VPC 端點的存取](#)。如需在政策中使用條件的詳細資訊，請參閱[使用條件索引鍵的儲存貯體政策範例](#)。作為套用此政策的先決條件，您應該建立 [Amazon S3 VPC 端點](#)。

Important

使用下列範例政策之前，請以適合您使用案例的適當值取代 VPC 端點 ID。否則，您將無法存取儲存貯體。

```
{
  "Version": "2012-10-17",
  "Id": "Policy1415115909152",
  "Statement": [
    {
      "Sid": "Access-to-specific-VPCE-only",
      "Principal": "*",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket",
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:SourceVpce": "vpce-1a2b3c4d"
        }
      }
    }
  ]
}
```

將使用者或群組指派或新增至 Transfer Family Web 應用程式

建立 Transfer Family Web 應用程式後，您可以指派可存取 Web 應用程式的使用者和群組。您可以擷取已在 IAM Identity Center 中建立和存放的使用者，也可以[直接新增使用者](#)（如果您使用 IAM Identity

Center 目錄做為身分提供者)。如果您新增使用者，這些使用者也會新增至您的 IAM Identity Center 執行個體。

注意下列事項：

- 只有在您使用 IAM Identity Center 目錄做為身分來源並具有適當的許可時，才能新增使用者。如果您是組織執行個體的成員，您可能沒有新增使用者的必要許可。

 Note

如果您未將使用者或群組指派給應用程式，則使用者在嘗試登入 Web 應用程式時會收到錯誤。

- 如果您建立新的使用者，您也必須為此使用者建立 S3 存取授權，以便他們可以存取 Web 應用程式上的資料。
- 建立新使用者後，該使用者會收到來自 IAM Identity Center 的加入電子郵件，其中包含如何繼續的指示。

將使用者指派給 Transfer Family Web 應用程式

1. 導覽至您的 Web 應用程式清單，然後選擇您要編輯的清單。
2. 選擇指派使用者和群組。

webapp- [Assign users and groups](#) [Clear customization](#) [Delete](#)

Web app details [Edit](#)

Access endpoint [Info](#)
Share this with your users and add to your CORS policy.
<https://webapp-.transfer-webapp.us-east-2.on.aws>

Web app endpoint
[https://webapp--webapp.us-east-2.on.aws](#)

Web app units [Info](#)
1

Identity provider
[AWS IAM Identity Center](#)

IAM role
[IAM role](#)

Instance ARN
[arn:aws:sso::instance/ssoins-](#)

Users **Groups**

Users (2) [Delete](#)

After you assign users to your web app, set up user permissions to access your S3 data in [S3 Access Grants](#)

< 1 >

☐	Display name	User ID	Username
☐	[link]	[link]	
☐	[link]	[link]	

3. 若要指派您先前在 IAM Identity Center 中建立的使用者，請選取指派現有的使用者和群組。若要建立新的使用者，請跳到步驟 4。
 - a. 出現資訊畫面。選擇 Get started (入門) 以繼續。
 - b. 搜尋使用者。請注意，在您開始輸入搜尋條件之前，不會顯示任何使用者。如果不同，您必須依顯示名稱搜尋，而非使用者名稱。只會傳回完全相符的項目。如果您找不到您的使用者，請導覽至 IAM Identity Center 管理主控台、尋找使用者，然後在此處複製並貼上其顯示名稱。

Assign users and groups

Search: jane

Use "jane"

Users

- Jane Doe
janedoe | janedoe@example.com

Choose to assign users and groups

[Manage users and groups from IAM Identity Center](#)

[Back](#) [Add new users](#) [Done](#)

- c. 選擇要新增的使用者和群組，然後選擇指派。
4. 若要建立新使用者，請選取新增並指派新使用者。
 - a. 出現資訊畫面。選擇 Get started (入門) 以繼續。
 - b. 選擇新增新使用者。
 - c. 在對話方塊中輸入下列使用者詳細資訊：使用者名稱、名字和姓氏，以及電子郵件地址。

Add new users ✕

i Newly-created users are enabled by default. To grant them access to Add User Widget, you must set their password in the IAM Identity Center console. [Manage user passwords in the IAM Identity Center console](#) 🔗 ✕

Username
A username is required for this person to sign in to the AWS access portal. You can't change the username later.

johnstiles

Maximum length of 128 characters. Can only contain alphanumeric characters or any of the following: + = , - @ _

First name **Last name**

John Stiles

Email address **Confirm email address**

johnstiles@example.com johnstiles@example.com

Display name
This is typically the full name of the user (first and last name) and appears in the users list.

John Stiles

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

- d. 選擇下一步，然後選擇新增以新增使用者並關閉對話方塊，或選擇新增使用者以建立其他使用者。

為您的儲存貯體設定跨來源資源共用 (CORS)

您必須為 Web 應用程式使用的所有儲存貯體設定跨來源資源共用 (CORS)。CORS 組態是定義規則的文件，用於識別您允許存取儲存貯體的原始伺服器。如需 CORS 的詳細資訊，請參閱[設定跨來源資源共用 \(CORS\)](#)。

 Important

如果您未設定 CORS，最終使用者在嘗試存取 Web 應用程式上的位置時會收到錯誤。

為您的 Amazon S3 儲存貯體設定跨來源資源共用 (CORS)

1. 登入 AWS 管理主控台，並在 <https://console.aws.amazon.com/s3/>：// 開啟 Amazon S3 主控台。
2. 從左側導覽面板中選擇儲存貯體，然後在搜尋對話方塊中搜尋儲存貯體，然後選擇許可索引標籤。
3. 在跨來源資源共用 (CORS) 中，選擇編輯並貼上下列程式碼。將 *WebAppEndpoint* 取代為 Web 應用程式的實際存取端點。這可以是建立 Web 應用程式時建立的 VPC 託管或公有存取端點，也可以是建立的自訂存取端點。請勿輸入結尾斜線，因為當使用者嘗試登入您的 Web 應用程式時，這樣做會導致錯誤。
 - 不正確的範例：`https://webapp-c7bf3423.transfer-webapp.us-east-2.on.aws/`
 - 正確的範例：
 - `https://webapp-c7bf3423.transfer-webapp.us-east-2.on.aws`
 - `https://vpce-05668789767a-fh45z079.vpce-mq.transfer-webapp.us-east-1.on.aws`

如果您要為多個 Web 應用程式重複使用儲存貯體，請將其端點附加至 AllowedOrigins 清單。

```
[
  {
    "AllowedHeaders": [
      "*"
    ],
    "AllowedMethods": [
      "GET",
      "PUT",
      "POST",
      "DELETE",
      "HEAD"
    ],
    "AllowedOrigins": [
      "https://WebAppEndpoint"
    ],
    "ExposeHeaders": [
```



```
    "last-modified",
    "content-length",
    "etag",
    "x-amz-version-id",
    "content-type",
    "x-amz-request-id",
    "x-amz-id-2",
    "date",
    "x-amz-cf-id",
    "x-amz-storage-class",
    "access-control-expose-headers"
  ],
  "MaxAgeSeconds": 3000
}
```

4. 選擇儲存變更以更新 CORS。

若要測試 CORS 組態，請參閱[測試 CORS](#)。

設定 Transfer Family Web 應用程式的 Amazon S3 Access Grants

本主題說明如何使用 Amazon S3 Access Grants 新增存取授權。此存取授權定義直接存取您公司目錄中的使用者和群組的資料，並根據授權提供 just-in-time、最低權限的臨時憑證。S3 Access Grants 執行個體中的個別授權允許公司目錄中的特定使用者或群組，在 S3 Access Grants 執行個體中註冊的位置內取得存取權。如需詳細資訊，請參閱《Amazon [S3 使用者指南](#)》中的 [S3 Access Grants 概念](#)。

Amazon S3

Note

您無法將 IAM Identity Center 目錄與 Transfer Family Web 應用程式以外的 S3 Access Grants 搭配使用。

您必須指定身分傳播的 Amazon S3 存取授權。Amazon S3 存取授權會存放最終使用者必須存取的資料。當您的最終使用者登入 Transfer Family Web 應用程式時，S3 Access Grants 會將使用者的身分傳遞給信任的應用程式。本節說明如何新增和設定 Amazon S3 存取授權執行個體，以及 Amazon S3 儲存貯體的存取授權。

Note

準備好您的 [IAM Identity Center 執行個體 ARN](#) 和使用使用者或群組 ID，因為您需要它們來完成設定您的存取授權。

使用 Amazon S3 Access Grants 建立授權

1. 登入 AWS 管理主控台，並在 <https://console.aws.amazon.com/s3/>：// 開啟 Amazon S3 主控台。
2. 建立儲存貯體，或記下要與 Web 應用程式搭配使用的現有儲存貯體。如需建立儲存貯體的資訊，請參閱 [Amazon S3 使用者指南](#)。
3. 從左側導覽窗格中，選擇存取授權。
4. 選擇建立 S3 存取授權執行個體，並提供下列資訊。
 - 在### 的區域中選取新增 IAM Identity Center 執行個體 AWS 區域。如果您未使用 IAM Identity Center 做為身分提供者，請清除此方塊。
 - 貼上您的 IAM Identity Center 執行個體 ARN。

[Amazon S3](#) > [Access Grants](#) > Set up Access Grants Instance

- Step 1
- Create S3 Access Grants instance**
- Step 2
- Register S3 Buckets or prefixes as locations
- Step 3
- Create grant
- Step 4
- Review and finish

Create S3 Access Grants instance Info

When you create your S3 Access Grants instance, you can use identities from your corporate directory or you can use IAM users and roles. This Access Grants instance serves as the container for your individual grants.

S3 Access Grants instance Info

AWS Region

You can create one S3 Access Grants instance per AWS Region per account.

US East (Ohio) us-east-2

☒ Add IAM Identity Center instance in US East (Ohio) us-east-2 - optional

You can use an IAM Identity Center instance to specify identities from corporate directories. If you don't have an existing IAM Identity Center instance, you can add one after creating your S3 Access Grants instance.

IAM Identity Center instance ARN

You can find the IAM Identity Center instance ARN in the [IAM Identity Center console](#).

arn:aws:sso::instance/ssoin-

Format: arn:aws:sso::instance/<instanceIdentifier>

選擇 Next (下一步) 繼續。

5. 將 S3 儲存貯體或字首註冊為位置。我們建議您註冊預設位置 `s3://`，並將其映射至 IAM 角色。此預設路徑的位置涵蓋對您帳戶中所有 Amazon S3 儲存貯體 AWS 區域的存取。建立存取授權時，您可以將範圍縮小為預設位置內的儲存貯體、字首或物件。

請提供下列資訊。

- 對於範圍，瀏覽儲存貯體或輸入儲存貯體的名稱，並選擇性地輸入字首。
- 針對 IAM 角色，選擇建立新角色，讓服務建立角色。

或者，您可以自行建立角色，如中所述[設定 Transfer Family Web 應用程式的 IAM 角色](#)，然後在此處輸入其 ARN。

Amazon S3 > Access Grants > US East (N. Virginia) us-east-1: default > Register location

Register location [Info](#)

Registering a location for S3 your S3 Access Grants instance assigns an IAM role the permission to get temporary credentials to access resources within the specified scope.

Location [Info](#)

Location scope [Info](#)

You can't edit the location scope after registering the location.

Scope

[View](#) [Browse S3](#)

Format for all buckets: s3://
Format for bucket: s3://<bucket>
Format for prefix: s3://<bucket>/<prefix-with-path>

Permissions

This IAM role allows S3 Access Grants to access your specified location scope.

Permissions

To ensure the role has proper permissions to access the location scope, consult the [list of permissions](#).

IAM role [Info](#)

This IAM role allows S3 Access Grants to access your specified location scope.

☒ Create new role
☐ Choose from existing IAM roles
☐ Enter IAM role ARN

[Cancel](#) [Register location](#)

選擇 Next (下一步) 繼續。

6. 在建立授予畫面中，提供下列詳細資訊。

- 針對許可，選取讀取和寫入。存取授予許可可以是唯讀或讀取和寫入，但不支援唯讀。
- 針對承授者類型，從 IAM Identity Center 選擇目錄身分。
- 針對目錄身分類型，根據您要立即註冊的類型，選取使用者或群組。
- 在 IAM Identity Center 使用者/群組 ID 中，貼上您的使用者或群組的 ID。此 ID 可在 IAM Identity Center 主控台和使用者和群組資料表中的 Transfer Family Web 應用程式中使用。

Create Grant [Info](#)

Grant [Info](#)

Grant a user or role a specific level of access to your S3 data.

Grant scope

The grant scope is a combination of the location and the subprefix. Choose a registered location or register a new location. To narrow the scope, specify a subprefix. If you use the default "s3://" location, you must specify a subprefix.

Location

s3://test

Location ID [Info](#)

IAM role [Info](#)

[web-app-access-grants](#) [↗](#)

[Browse locations](#)

[Register location](#) [↗](#)

Subprefix - optional [Info](#)

Further scope the grant to a bucket, prefix, or an individual object.

*

Don't include any part of the grant already specified in the location.

Format for bucket: <bucket>/*

Format for prefix: <bucket>/<prefix-with-path>*

Format for object: <bucket>/<prefix-with-path>/<object>

Grant scope [Info](#)

s3://test/*

☐ The grant scope is an object

Permissions and access

Grant a user or role a specific level of access to your S3 data.

 The S3 console can't be used to access the data specified in the grant scope. To access the data, the grantee must do so through the AWS CLI, the application, or other AWS services.

Permissions

☒ Read

☒ Write

Grantee type [Info](#)

☒ Directory identity from IAM Identity Center

☐ IAM principal

Directory identity type [Info](#)

☒ User

☐ Group

IAM Identity Center user ID [Info](#)

The user that you want to grant this level of access to. You can find the ID in the [IAM Identity Center console](#) [↗](#)

Format: a1b2c3d4-5678-90ab-cdef-EXAMPLE1111

► **Application - optional**

選擇下一步。

7. 檢閱畫面上的設定。如果一切正確，請選擇完成以建立存取授權。或者，您可以選擇取消或上一個進行變更。

- Step 1
Create S3 Access Grants instance
- Step 2
Register S3 Buckets or prefixes as locations
- Step 3
Create grant
- Step 4
Review and finish

Review and finish

Step 1 - Create S3 Access Grants instance

S3 Access Grants instance

AWS Region
You can create one S3 Access Grants instance per AWS Region per account.
US East (Ohio) us-east-2

Add IAM Identity Center instance in US East (Ohio) us-east-2 - optional
You can use an IAM Identity Center instance to specify identities from corporate directories. If you don't have an existing IAM Identity Center instance, you can add one after creating your S3 Access Grants instance.
arn:aws:sso:::application/ssoinstance:/apl

Successfully created S3 Access Grants instance
Instance ARN: arn:aws:s3:us-east-2:::access-grants/default

You can grant other accounts access to this S3 Access Grants instance in the [Resource Access Management console](#)

Step 2 - Register S3 buckets or prefixes as locations

Location

Location scope
s3://

IAM role
web-app-beta-access-grants

Successfully registered location
Location ID:

Step 3 - Create grants

Grant

Grant a user or role a specific level of access to your S3 data.

Grant scope
s3:///*

IAM role
web-app-beta-access-grants

Location ID

Permissions and access
Access Type
READWRITE

Grantee type
Directory identity user

Grantee ID

Application - optional
-

Successfully created grant
Grant ARN: arn:aws:s3:us-east-2:::access-grants/default/grant/

Create another grant

Cancel Previous Finish

設定 Amazon S3 存取授權

273

[Amazon S3](#) > [Access Grants](#) > US East (Ohio) us-east-2: default

US East (Ohio) us-east-2: default [Info](#)

[Share Instance](#)[Delete Instance](#)

S3 Access Grants provides scalable access control to data sets in your S3 buckets. To share an S3 Access Grants instance with external accounts by using the AWS Resource Access Manager console, choose Share instance. With S3 Access Grants, you can use identities from your corporate directory or from AWS Identity and Access Management (IAM) to control access. You can create one S3 Access Grants instance per AWS Region per account.

S3 Access Grants instance overview [Info](#)

Amazon Resource Name (ARN)[arn:aws:s3:us-east-2:account-id:access-grants/default](#)**Creation date**

October 25, 2024, 11:50:11 (UTC-04:00)

Account ID

account-id

IAM Identity Center [Info](#)

[Deregister](#)[Add](#)**IAM Identity Center instance ARN**[arn:aws:sso:us-east-2:account-id:application/ssoins-account-id/apl-account-id](#)[Grants](#)[Locations](#)

Grants (1) [Info](#)

[Delete](#)[Create Grant](#)< 1 > [⚙️](#)

	Grant scope ▲	Grant ID ▼	Permission ▼	Grantee type ▼	Grantee ID 🔗 ▼	Creation date ▼	Location ID	Application ARN 🔗 ▼
☐	s3://account-id/*	grant-id	Read, Write	Directory identity user	grantee-id	October 25, 2024, 11:57:30 (UTC-04:00)	location-id	ALL

這會完成 Web 應用程式的設定。您已設定的使用者和群組可以在存取點造訪 Web 應用程式、登入，以及上傳和下載檔案。

使用自訂 URL 更新您的存取端點

使用 Web 應用程式建立的預設存取端點包含服務產生的識別符。若要提供品牌體驗，建議您提供自訂 URL 給使用者，以存取 Transfer Family Web 應用程式。本主題說明如何使用自訂 URL 更新存取端點。

[i](#) Note

無法為 VPC 端點自訂存取端點。若要新增自訂 URL，請使用公有端點。

[i](#) Note

下列程序依賴您使用建議的 [CloudFormation 堆疊範本](#)。您不需要使用範本：您可以直接使用 [CloudFront 主控台](#) 建立分佈。

不過，提供的範本可簡化程序，並讓您更輕鬆地避免設定錯誤。如果您不使用 CloudFormation 範本，請務必遵循下列準則：

- Origin [請求政策](#)應轉送查詢字串和 Cookie 至原始伺服器，且不應轉送Host標頭至原始伺服器。
- [快取政策](#)不應在快取金鑰中包含 Host標頭。

自訂您的 Web 應用程式 URL

1. 使用 Transfer Family 提供的 AWS CloudFormation 範本 [CloudFormation 堆疊範本來建立 CloudFront 分佈](#)。
 - a. 在 <https://console.aws.amazon.com/cloudformation> 開啟 CloudFormation 主控台。
 - b. 選擇建立堆疊並指定下列項目。
 - 在先決條件 - 準備範本區段中，選擇選擇現有範本。
 - 在 Specify template (指定範本) 區段中，選擇 Upload a template file (上傳範本檔案)。
 - 儲存 [CloudFormation 堆疊範本](#) 檔案，然後上傳至此處。
 - c. 選擇下一步，並提供下列資訊。
 - WebAppEndpoint：從您的 Web 應用程式複製值
 - AccessEndpoint：提供您要使用的自訂網域名稱
 - AcmCertificateArn：為存放在 中的公有或私有 SSL/TLS 憑證提供 ARN AWS Certificate Manager
 - d. 完成 CloudFormation 精靈，直到建立新的堆疊。
2. 在 Web 應用程式中，編輯存取端點，將自訂 URL 更新為您要使用的 URL。

Transfer Family > Web apps > webapp- > Edit web app details

Edit web app details

Authentication access [Info](#)

Connect or create an Identity Center instance

Instance ARN

Select your instance ARN

Permission type [Info](#)

Create and use a new service role

Create and use an IAM role to allow the service to access the AWS resource it needs to create your application

Use an existing role

Use an existing IAM role to allow the service to access the AWS resources it needs to create your application

By selecting use existing role, you need to manually create an IAM Role in order for the Transfer Family web application to access your AWS services data. Please select an existing IAM role below or [create a new role in IAM console](#)

Select an existing role

If your newly created role is not showing up in the dropdown list, please try the refresh button on the right

Find your IAM role

Make sure you have attached the trust policy and permission policy to the role you selected.

[learn more about required policies](#)

Access endpoint [Info](#)

Map your own fully qualified domain name to this web app so your end users can use your custom URL, not the service-provided URL to access your web app. Note- you can only complete this step in CloudFront after you have created the web app.

Custom URL

`https://my-custom-url`

[Create a new distribution](#)

3. 建立 DNS 記錄，將自訂網域名稱的流量路由到 CloudFront 分佈。如果您針對區域使用 Route 53，則可以建立 CloudFront 分佈名稱的別名或 CNAME 記錄（例如 xxxx.cloudfront.net）。如需搭配 CloudFront 使用 Amazon Route 53 的詳細資訊，請參閱[設定 Amazon Route 53 將流量路由到 CloudFront 分佈](#)。
4. 將預設存取端點取代為 AllowedOrigins 程式碼區塊中的下列行，以更新您的跨來源資源共用政策：

```
"https://custom-url"
```

您需要針對 Web 應用程式所使用的每個儲存貯體進行此變更。

進行更新後，CORS 政策的 AllowedOrigins 區段應如下所示：

```
"AllowedOrigins": [
  "https://custom-url",
```

每個 Transfer Family Web 應用程式只需要一個 AllowedOrigins 項目。

如需詳細資訊，請參閱[設定 Amazon S3 儲存貯體程序的跨來源資源共用 \(CORS\)](#)。

您現在可以造訪自訂存取端點，並與您的最終使用者共用此連結。

Transfer Family Web 應用程式的 CloudTrail 記錄

CloudTrail 是 AWS 服務，可建立在您的中採取之動作的記錄 AWS 帳戶。它會持續監控並記錄 API 操作，以進行主控台登入、AWS Command Line Interface 命令和 SDK/API 操作等活動。這可讓您記錄誰從何地採取了哪些動作。CloudTrail 透過提供 AWS 環境中所有活動的歷史記錄，協助稽核、存取管理和法規遵循。

對於 Transfer Family Web 應用程式，您可以追蹤身分驗證事件和使用者執行的資料存取操作。若要啟用全方位記錄，您需要：

1. 設定 CloudTrail 記錄用於追蹤身分驗證活動的管理事件。
2. 啟用 Amazon S3 資料事件，以追蹤透過 Web 應用程式執行的檔案操作。

另請參閱

- [IAM Identity Center 的 CloudTrail 使用案例](#)
- [了解 IAM Identity Center 登入事件](#)
- [CloudTrail userIdentity 元素](#)
- [啟用 S3 儲存貯體和物件的 CloudTrail 事件記錄](#)
- [Amazon S3 CloudTrail 事件](#)

啟用 Amazon S3 資料事件

若要追蹤透過 Transfer Family Web 應用程式在 Amazon S3 儲存貯體上執行的檔案操作，您需要啟用這些儲存貯體的資料事件。資料事件提供物件層級 API 活動，對於追蹤 Web 應用程式使用者執行的檔案上傳、下載和其他操作特別有用。

若要為 Transfer Family Web 應用程式啟用 Amazon S3 資料事件：

1. 前往 <https://console.aws.amazon.com/cloudtrail/> 開啟 CloudTrail 主控台。
2. 在導覽窗格中，選擇線索，然後選取現有的線索或建立新的線索。
3. 在進階事件選取器下，選擇編輯。
4. 選擇新增進階事件選取器。
5. 對於第一個欄位選擇器：

- 將欄位設定為 `eventCategory`
 - 將運算子設定為等於
 - 將值設定為 `Data`
6. 針對第二個欄位選擇器，選擇新增欄位和：
- 將欄位設定為 `resources.type`
 - 將運算子設定為等於
 - 將值設定為 `AWS::S3::Object`
7. (選用) 若要僅記錄特定儲存貯體的事件，請選擇新增欄位並新增：
- 將欄位設定為 `resources.ARN`
 - 將運算子設定為從 開始
 - 將值設定為 `arn:aws:s3:::your-bucket-name/`
8. 選擇儲存變更。

或者，您可以使用舊版資料事件組態：

1. 在資料事件下，選擇編輯。
2. 針對資料事件類型，選取 S3 儲存貯體和物件事件。
3. 選擇要記錄資料事件的 Amazon S3 儲存貯體。您可以選取所有目前和未來的 S3 儲存貯體，或指定個別儲存貯體。
4. 選擇記錄讀取事件、寫入事件或兩者。
5. 選擇儲存變更。

啟用資料事件後，您可以在為 CloudTrail 設定的 Amazon S3 儲存貯體中存取這些日誌。日誌包含詳細資訊，例如執行動作的使用者、動作時間戳記、受影響的特定物件，以及協助追蹤透過 Transfer Family Web 應用程式執行之動作 `userId` 的 `onBehalfOf` 欄位。

尋找和檢視您的日誌

有幾種方式可以尋找和檢視 Transfer Family Web 應用程式的 CloudTrail 日誌：

使用 CloudTrail 主控台

檢視最近事件的最快方式：

1. 前往 <https://console.aws.amazon.com/cloudtrail/> 開啟 CloudTrail 主控台。

2. 選擇事件歷史記錄。
3. 依下列條件篩選事件：
 - 事件來源：signin.amazonaws.com適用於 Web 應用程式事件
 - 事件來源：s3.amazonaws.com適用於檔案操作
4. 按一下任何事件以檢視詳細資訊。

在 Amazon S3 中存取日誌

若要存取存放在 Amazon S3 中的完整日誌檔案：

1. 識別 CloudTrail 追蹤的 Amazon S3 儲存貯體：

```
aws cloudtrail describe-trails --query 'trailList[*].[Name,S3BucketName]' --output table
```

2. 導覽至 Amazon S3 中的日誌檔案：

```
aws s3 ls s3://your-cloudtrail-bucket/AWSLogs/account-id/CloudTrail/region/YYYY/MM/DD/
```

3. 下載並搜尋 Web 應用程式 ID 的日誌檔案：

```
aws s3 cp s3://your-cloudtrail-bucket/AWSLogs/account-id/CloudTrail/region/YYYY/MM/DD/ . --recursive
gunzip *.json.gz
grep -l "webapp-1a2b3c4d5e6f7g8h9" *.json
```

使用 AWS CLI 搜尋事件

使用 搜尋特定 Web 應用程式事件 AWS CLI：

```
aws logs filter-log-events \
  --log-group-name /aws/cloudtrail/your-trail-name \
  --filter-pattern "webapp-1a2b3c4d5e6f7g8h9" \
  --start-time $(date -d "1 day ago" +%s)000
```

或搜尋身分驗證事件：

```
aws logs filter-log-events \
```

```
--log-group-name /aws/cloudtrail/your-trail-name \  
--filter-pattern "UserAuthentication" \  
--start-time $(date -d "1 day ago" +%s)000
```

身分驗證日誌範例

CloudTrail 會記錄 Transfer Family Web 應用程式的身分驗證事件，這可協助您追蹤成功和失敗的登入嘗試。這些日誌對於安全監控和合規用途特別有用。

主題

- [登入資料驗證的範例日誌項目](#)
- [登入身分驗證的範例日誌項目](#)
- [ListCallerAccessGrants 的範例日誌項目](#)
- [GetDataAccess 事件的範例日誌項目](#)

登入資料驗證的範例日誌項目

下列範例顯示憑證驗證事件在身分驗證程序期間發生的 CloudTrail 日誌項目。

```
{  
  "eventVersion": "1.09",  
  "userIdentity": {  
    "type": "Unknown",  
    "principalId": "123456789012",  
    "arn": "",  
    "accountId": "123456789012",  
    "accessKeyId": "",  
    "userName": "demo-user-2",  
    "onBehalfOf": {  
      "userId": "f12bb510-a011-702f-10dd-5607e2776dbc",  
      "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/  
d-9a670c546e"  
    },  
    "credentialId": "58138a11-87e5-401d-8f0b-7161c9389112"  
  },  
  "eventTime": "2025-08-08T15:29:30Z",  
  "eventSource": "signin.amazonaws.com",  
  "eventName": "CredentialVerification",  
  "awsRegion": "us-east-2",  
  "sourceIPAddress": "192.0.2.224",
```

```

    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "f304a48b-7b6d-41c8-b136-4f49c91c1f31",
        "CredentialType": "PASSWORD"
    },
    "requestID": "ff936828-4a81-453c-802d-81368b6bca1a",
    "eventID": "70cb7008-493d-42c2-a9eb-38bf168af6a8",
    "readOnly": false,
    "eventType": "AWS ServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "serviceEventDetails": {
        "CredentialVerification": "Success"
    },
    "eventCategory": "Management"
}

```

此事件提供身分驗證程序中登入資料驗證步驟的其他詳細資訊，顯示使用的特定登入資料 ID 和身分驗證工作流程 ID。

登入身分驗證的範例日誌項目

下列範例顯示使用 IAM Identity Center 登入 Web 應用程式期間成功使用者身分驗證事件的 CloudTrail 日誌項目。

```

{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "123456789012",
        "arn": "",
        "accountId": "123456789012",
        "accessKeyId": "",
        "userName": "demo-user-2",
        "onBehalfOf": {
            "userId": "f12bb510-a011-702f-10dd-5607e2776dbc",
            "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/d-9a670c546e"
        },
        "credentialId": "b41f0a02-1635-4d07-a414-aecf9e14b906"
    }
}

```

```

    },
    "eventTime": "2025-08-07T14:09:07Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "UserAuthentication",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "192.0.2.14",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "7a4ef12c-7c4b-4bc3-b5bd-c2469afcc795",
        "LoginTo": "https://example.awsapps.com/start/",
        "CredentialType": "PASSWORD"
    },
    "requestID": "fc91bcf0-ac53-4454-a1a0-fb911eacc095",
    "eventID": "18522007-1e60-4a71-b2b5-150baf504ab3",
    "readOnly": false,
    "eventType": "AWS ServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "serviceEventDetails": {
        "UserAuthentication": "Success"
    },
    "eventCategory": "Management"
}

```

在此範例中，請注意下列重要欄位：

- `eventSource`：顯示 "signin.amazonaws.com"，表示這是 IAM Identity Center 身分驗證事件。
- `userIdentity.onBehalfOf`：包含 Web 應用程式使用者的使用者 ID 和身分存放區 ARN。
- `additionalEventData.LoginTo`：顯示正在存取的 IAM Identity Center 應用程式 URL。
- `additionalEventData.CredentialType`：指出使用的身分驗證方法 (PASSWORD)。
- `serviceEventDetails`：顯示身分驗證結果（成功）。

ListCallerAccessGrants 的範例日誌項目

下列範例顯示 ListCallerAccessGrants 事件的 CloudTrail 日誌項目，當 Transfer Family Web 應用程式查詢使用者的可用存取授權時發生。

```
{
```

```

    "eventVersion": "1.11",
    "userIdentity": {
      "type": "AssumedRole",
      "principalId": "AROEXAMPLEID:aws-transfer",
      "arn": "arn:aws:sts::123456789012:assumed-role/AWS
TransferWebAppIdentityBearer-us-east-2/aws-transfer",
      "accountId": "123456789012",
      "accessKeyId": "ASIAEXAMPLEKEY",
      "sessionContext": {
        "sessionIssuer": {
          "type": "Role",
          "principalId": "AROEXAMPLEID",
          "arn": "arn:aws:iam::123456789012:role/service-role/AWS
TransferWebAppIdentityBearer-us-east-2",
          "accountId": "123456789012",
          "userName": "AWS TransferWebAppIdentityBearer-us-east-2"
        },
        "attributes": {
          "creationDate": "2025-08-08T15:29:34Z",
          "mfaAuthenticated": "false"
        }
      },
      "invokedBy": "transfer.amazonaws.com",
      "onBehalfOf": {
        "userId": "f12bb510-a011-702f-10dd-5607e2776dbc",
        "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/
d-9a670c546e"
      }
    },
    "eventTime": "2025-08-08T15:29:35Z",
    "eventSource": "s3.amazonaws.com",
    "eventName": "ListCallerAccessGrants",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "transfer.amazonaws.com",
    "userAgent": "transfer.amazonaws.com",
    "requestParameters": {
      "Host": "123456789012.s3-control.dualstack.us-east-2.amazonaws.com",
      "allowedByApplication": "true",
      "maxResults": "100"
    },
    "responseElements": null,
    "additionalEventData": {
      "SignatureVersion": "SigV4",
      "CipherSuite": "TLS_AES_128_GCM_SHA256",

```

```

        "bytesTransferredIn": 0,
        "AuthenticationMethod": "AuthHeader",
        "x-amz-id-2": "1g34AaAELn/
fntxwriFVsr41VDl8dp5ygWFasHJFNVq5FDCWYfX0ye7s4tWHEJC8ppI5lLePYLIcw3iTXAgn5Q==",
        "bytesTransferredOut": 462
    },
    "requestID": "48485MTZEDWT0ANT",
    "eventID": "3de5dd60-b7cf-474c-a1ab-631467c1a5c3",
    "readOnly": true,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "AWS:S3::AccessGrantsInstance",
            "ARN": "arn:aws:s3:us-east-2:123456789012:access-grants/default"
        }
    ],
    "eventType": "AWS ApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}

```

在此範例中，請注意下列重要欄位：

- `eventName`：顯示這是 `ListCallerAccessGrants` 事件，可查詢可用的 S3 存取授權。
- `requestParameters.allowedByApplication`：表示查詢會篩選為應用程式允許的授予。
- `requestParameters.maxResults`：顯示回應中傳回的授予數量上限。
- `userIdentity.onBehalfOf`：將請求連結至特定 Web 應用程式使用者。

此事件有助於追蹤 Transfer Family Web 應用程式何時查詢使用者可存取的 S3 資源，提供存取授權探索操作的可見性。

GetDataAccess 事件的範例日誌項目

下列範例顯示 `GetDataAccess` 事件的 CloudTrail 日誌項目，會在 Transfer Family Web 應用程式代表使用者請求 S3 資源的存取許可時發生。

```

{
    "eventVersion": "1.11",
    "userIdentity": {
        "type": "AssumedRole",

```



```

    "principalId": "AROASEQRAEABP7ADWEZA5:aws-transfer",
    "arn": "arn:aws:sts::123456789012:assumed-role/AWSTransferWebAppIdentityBearer-
ap-southeast-1/aws-transfer",
    "accountId": "123456789012",
    "accessKeyId": "ASIAEXAMPLEKEY",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROASEQRAEABP7ADWEZA5",
        "arn": "arn:aws:iam::123456789012:role/service-role/
AWSTransferWebAppIdentityBearer-ap-southeast-1",
        "accountId": "123456789012",
        "userName": "AWSTransferWebAppIdentityBearer-ap-southeast-1"
      },
      "attributes": {
        "creationDate": "2025-05-08T16:09:05Z",
        "mfaAuthenticated": "false"
      }
    },
    "invokedBy": "transfer.amazonaws.com",
    "onBehalfOf": {
      "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/
d-9667b0da7a",
      "userId": "191a35ec-10a1-70c1-e4ab-e2802411e13e"
    }
  },
  "eventTime": "2025-05-08T16:10:25Z",
  "eventSource": "s3.amazonaws.com",
  "eventName": "GetDataAccess",
  "awsRegion": "ap-southeast-1",
  "sourceIPAddress": "transfer.amazonaws.com",
  "userAgent": "transfer.amazonaws.com",
  "requestParameters": {
    "Host": "123456789012.s3-control.dualstack.ap-southeast-1.amazonaws.com",
    "durationSeconds": 900,
    "permission": "READWRITE",
    "target": "s3://amzn-s3-demo-bucket/users/john.doe/documents/*"
  },
  "responseElements": null,
  "additionalEventData": {
    "AuthenticationMethod": "AuthHeader",
    "CipherSuite": "TLS_AES_128_GCM_SHA256",
    "SignatureVersion": "SigV4",
    "bytesTransferredIn": 0,

```

```

        "bytesTransferredOut": 2244,
        "x-amz-id-2": "8ce8sZ0gNwsaj9w1mzagyA
+cs0NjYl8FgEw4FGpE8DARi90aNC0RFWlTYNE7ChqE9RCJrTzMvS+ru7Vz2xXHrkQt/1uQ9exZTZdlhX+/fM="
    },
    "requestID": "BXGSKKQXCWS5RAHB",
    "eventID": "c11db1d1-dfb8-431e-8625-48eba2ebadfe",
    "readOnly": true,
    "resources": [
        {
            "type": "AWS:S3::AccessGrantsInstance",
            "ARN": "arn:aws:s3:ap-southeast-1:123456789012:access-grants/default",
            "accountId": "123456789012"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}

```

在此範例中，請注意下列重要欄位：

- `eventName`：顯示這是一個 `GetDataAccess` 事件，會在 Transfer Family 請求 S3 資源的存取許可時發生。
- `userIdentity.onBehalfOf`：包含身分存放區 ARN 和使用者 ID，將存取請求連結至特定的 Web 應用程式使用者。
- `requestParameters.target`：顯示請求存取的 S3 路徑模式。
- `requestParameters.permission`：指出請求的存取類型 (READWRITE、READWRITE 或 WRITE)。
- `requestParameters.durationSeconds`：顯示存取授權的有效時間長度（通常為 900 秒/15 分鐘）。
- `sourceIPAddress` 和 `userAgent`：兩者都顯示 "transfer.amazonaws.com"，表示這是內部服務請求。

`GetDataAccess` 事件特別適用於追蹤 Transfer Family Web 應用程式使用者何時獲得特定 S3 資源的存取權，協助您監控存取模式並確保適當的授權。

檢視 CloudTrail 日誌項目

有幾種方式可以檢視和分析 Transfer Family Web 應用程式的 CloudTrail 日誌項目：

使用 CloudTrail 主控台

CloudTrail 主控台提供易於使用的界面，用於檢視和篩選日誌項目：

1. 透過 <https://console.aws.amazon.com/cloudtrail/> 開啟 CloudTrail 主控台。
2. 在導覽窗格中，選擇 Event history (事件歷史記錄)。
3. 使用篩選條件選項縮小事件範圍：
 - 將事件來源設定為 `transfer.amazonaws.com`，以僅檢視 Transfer Family 事件。
 - 依事件名稱篩選，以查看特定操作，例如 `UserAuthentication`。
 - 使用時間範圍來專注於特定期間內的事件。
4. 按一下任何事件以檢視其詳細資訊。

在 Amazon S3 中存取日誌

如果您已設定 CloudTrail 追蹤將日誌交付到 Amazon S3 儲存貯體，您可以直接存取原始日誌檔案：

1. 開啟位於 <https://console.aws.amazon.com/s3/> 的 Amazon S3 主控台。
2. 導覽至存放 CloudTrail 日誌的儲存貯體和字首。
3. 日誌會依年、月、日和區域進行組織。導覽至適當的目錄。
4. 下載並開啟 JSON 格式的日誌檔案。

對 Web 應用程式進行故障診斷

Note

這些疑難排解秘訣適用於 Web 應用程式管理員，而非最終使用者。對於最終使用者，如果您遇到任何問題，請聯絡您的 Web 應用程式管理員。以下段落中的所有執行個體都是指 Web 應用程式管理員。

故障診斷網路錯誤

Description

您的最終使用者在載入 Web 應用程式端點時看到網路橫幅網路錯誤。

原因

最常見的問題如下：

- 管理員未指派嘗試登入新應用程式的使用者。
- 管理員未將必要的動作新增至您的 IAM 角色。
- 您會看到指派給使用者的 S3 Access Grants 清單，但 Amazon S3 儲存貯體或儲存貯體的 CORS 未正確設定。

解決方案

- 在 IAM Identity Center 中，請務必將使用者指派給正確的應用程式。或者，如果您已指派群組，請確定嘗試登入的使用者屬於正確的群組。如[將使用者或群組指派或新增至 Transfer Family Web 應用程式](#)中所述。
- 檢查您的角色是否同時包含 sts:AssumeRole 和 動作的自訂信任政策中的必要 sts:SetContext 動作。如[設定 Transfer Family Web 應用程式的 IAM 角色](#)中所述。
- 檢查您的 Web 應用程式使用的所有儲存貯體的 CORS 政策。這會在[為您的 Amazon S3 儲存貯體設定跨來源資源共用 \(CORS\)](#) 中說明。

對未顯示的已設定儲存貯體進行故障診斷

Description

一切似乎都已正確設定，但 Amazon S3 儲存貯體未出現在 Web 應用程式中。

原因

一個可能的原因是 Amazon S3 儲存貯體與 Web 應用程式不在同一個帳戶中。

解決方案

確定 Amazon S3 儲存貯體與 Web 應用程式位於相同的帳戶中。目前不支援跨帳戶儲存貯體。

對自訂 URL 錯誤進行故障診斷

Description

當您的最終使用者登入 Web 應用程式時，會收到錯誤訊息授權失敗：缺少授權碼。

原因

如果您直接使用 CloudFront，而不是提供的 CloudFormation 範本，則可能已將原始伺服器請求政策設定為不轉送查詢字串。

解決方案

更新您的原始伺服器請求政策，將查詢字串和 Cookie 轉送至原始伺服器。

Description

當您的最終使用者嘗試存取 Transfer Family Web 應用程式時，會收到 404 回應。

原因

如果您直接使用 CloudFront，而不是提供的 CloudFormation 範本，則可能已將快取政策錯誤地設定為在快取金鑰中包含 Host 標頭，或將原始伺服器請求政策錯誤地設定為轉送 Host 標頭。

解決方案

- 請確定您的快取政策不包含快取金鑰中的 Host 標頭
- 請確定您的原始伺服器請求政策不會轉送 Host 標頭。

對其他錯誤進行故障診斷

Description

您的最終使用者無法登入，或無法檢視任何儲存貯體或檔案，或您收到另一個錯誤。

原因

可能的原因之一是 IAM Identity Center 執行個體 ARN 不符合授予 ARN 或 Web 應用程式 IAM Identity Center 執行個體 ARN 的值。

解決方案

檢查下列項目，以查看它們是否相符。

- 在 IAM Identity Center 中，導覽至設定並檢視執行個體 ARN。

```
arn:aws:sso:::instance/ssoins-instance-identifier
```

- 在 Amazon S3 中，導覽至存取授權並檢視您的 IAM Identity Center 執行個體 ARN。

```
arn:aws:sso:::account-id:application/ssoins-instance-identifier/apl-1234567890abcdef0
```

- 在 Transfer Family 中，導覽至 Web 應用程式詳細資訊頁面，並檢視其執行個體 ARN。

```
arn:aws:sso:::instance/ssoins-instance-identifier
```

所有三個位置的#####值都必須相同。

Web 應用程式中出現重複的 S3 儲存貯體

Description

使用者會在 Transfer Family Web 應用程式界面中看到多次列出的相同 S3 儲存貯體。

原因

當使用者屬於具有相同 S3 儲存貯體重複授予的多個 Active Directory 群組時，就會發生這種情況。Web 應用程式會列出與使用者 (UID 或 GID) 相關聯的所有最上層授予，無論使用者是否將多個授予指派給相同的儲存貯體位置。

解決方案

若要解決此問題，管理員應該取消重複授予，讓每個使用者都只有一個授予給每個 S3 位置。檢閱 S3 Access Grants 組態，並合併不同 Active Directory 群組中相同儲存貯體的重複授權。

Transfer Family Web 應用程式的最終使用說明

Note

在本主題中，資訊適用於與 Web 應用程式互動的最終使用者。本主題中的所有執行個體都是指最終使用者。

本主題說明如何存取您獲授權使用的 AWS Transfer Family Web 應用程式，並說明如何與其互動。

Web 應用程式配額

使用 Web 應用程式時，請注意下列限制。

- 每個查詢的搜尋結果數目上限：10,000
- Transfer Family Web 應用程式使用的 Amazon S3 儲存貯體必須與 Web 應用程式本身位於相同的帳戶中。目前不支援跨帳戶儲存貯體。
- 每個查詢的搜尋廣度上限：10,000 個搜尋的檔案
- 每個檔案的最大上傳大小：160 GB (149 GiB)
- 複製的大小上限：5.36 GB (5 GiB)
- 不支援以點 (.) 開頭或結尾的資料夾名稱

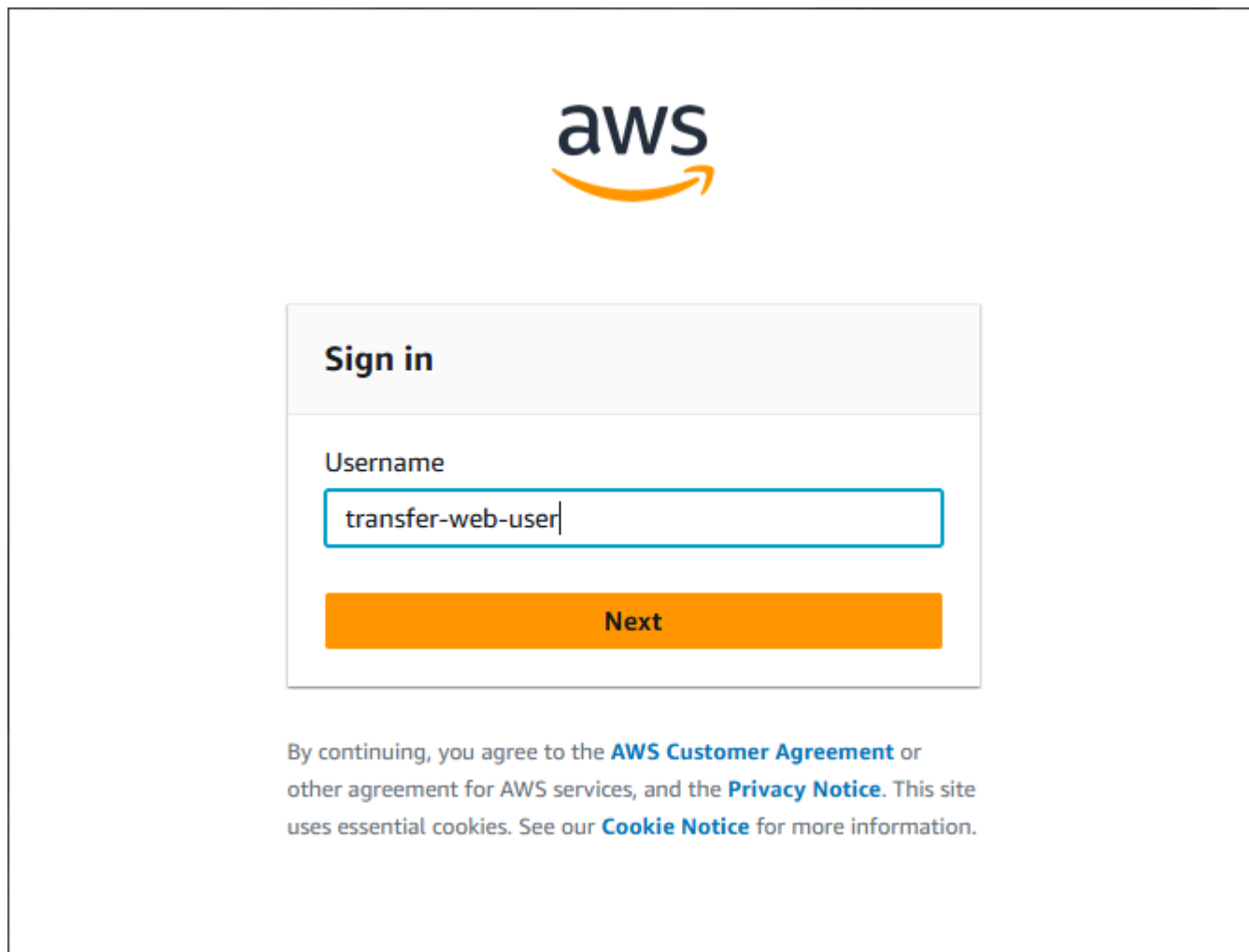
IAM Identity Center 使用者的使用者體驗

如果您的組織使用 IAM Identity Center 來設定其使用者，本節說明使用者體驗。

存取 Transfer Family Web 應用程式

1. 您應該會收到來自 no-reply@login.awsapps.com 的電子郵件，標題為「邀請加入」AWS IAM Identity Center。接受啟用使用者帳戶的邀請。
2. 在訊息中，選擇您的 AWS 存取入口網站 URL 下方的 URL。

這會帶您前往 AWS 登入畫面。



3. 輸入您的登入資料，然後選擇登入。

這會帶您前往 AWS 存取入口網站，其中顯示您的可用應用程式清單。

4. 選擇 Transfer Family Web 應用程式的應用程式。

第三方身分提供者使用者的使用者體驗

如果您的組織未使用 AWS IAM Identity Center 來設定其使用者，您的加入體驗將取決於他們用來設定其最終使用者的身分提供者應用程式。驗證並登入後，您的 Web 應用程式界面會與下一節中所述的相同。

Note

如果使用者屬於多個 Active Directory 群組，而這些群組已授予相同的 Amazon S3 儲存貯體，則該儲存貯體會 Web 應用程式界面中出現多次。這是因為 Web 應用程式會列出與使用者

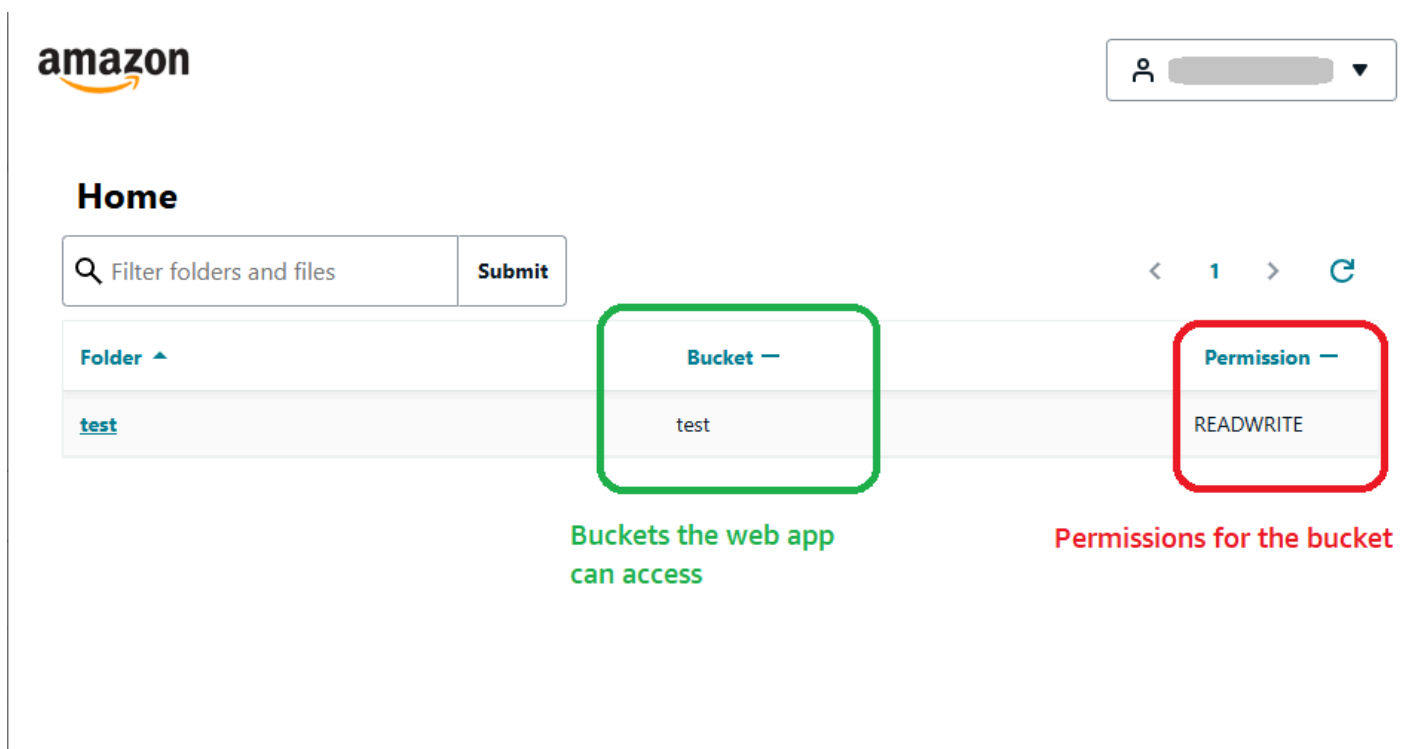
UID 或 GID 相關聯的所有最上層授予，包括對相同儲存貯體的重複授予。為了防止重複的清單，管理員可以合併多個授予，讓每個使用者在每個 Amazon S3 位置只有一個授予。

Transfer Family 最終使用者介面

驗證並登入後，您可以與 Web 應用程式互動。

有四個主要檢視。

- 首頁：您的首頁列出您可以存取的 S3 位置，以及每個位置的許可。S3 位置是 S3 儲存貯體或字首，您可以在使用 S3 Access Grants 時定義。這是使用者的初始檢視，顯示最終使用者可存取的根層級 S3 資源，以及每個 S3 位置的許可。



- 位置詳細資訊：此檢視可讓使用者瀏覽 S3 中的檔案和資料夾，以及上傳或下載檔案
- 位置動作：選擇動作（例如上傳）之後，它會開啟檔案位置的另一個檢視。
- 垂直省略：垂直省略符號圖示會開啟動作功能表。

可用動作

大部分動作都可從動作功能表取得。對於另一個主要動作，下載檔案，您可以在選取檔案後使用下載圖示（目前一次只能下載一個檔案）。

Transfer Web App

Scott

Home / test2 / Testing-01

Testing-01/

☐ Include subfolders

< 1 > ↺ ⋮

☐	Name ▲	Type —	Last Modified —	Size —	
☐	 scott-small.png	png	10/30/2024, 2:28:31 PM	375.4 kB	
☐	 Scott-02.jpg	jpg	10/30/2024, 2:28:30 PM	196.6 kB	
☐	 Scott-badge.jpg	jpg	10/30/2024, 2:28:31 PM	1.3 MB	

Download icon

從資料夾中，使用動作功能表來執行下列任何任務：

- 將一或多個檔案複製到另一個位置。
- 建立資料夾。
- 刪除一或多個檔案。
- 上傳一或多個檔案。
- 上傳整個資料夾（如果有，包括子資料夾）。
- 選取資料夾並導覽至該資料夾。然後，您可以執行任何先前列出的動作。
- 依頁面排序。
- 依每個資料夾和子資料夾的檔案或資料夾名稱進行篩選。

amazon

👤

▼

Home

/

test

test

🔍

Search current folder

Submit

☐ Include subfolders

<

1

>

↺

⋮

Name ▲	Type —	Last Modified —
📁 My First Folder/	Folder	
📁 My Second Folder/	Folder	
📁 Testing-01/	Folder	
📁 Testing-02/	Folder	

📄

Copy files

📁+

Create folder

🗑️

Delete files

📁↑

Upload files

📁+

Upload folder

AWS Transfer Family SFTP 連接器

AWS Transfer Family SFTP 連接器會與遠端 SFTP 伺服器建立連線，以使用 SFTP 通訊協定在 Amazon 儲存體和遠端伺服器之間傳輸檔案。您可以將檔案從 Amazon S3 傳送到外部、合作夥伴擁有的 SFTP 伺服器、從合作夥伴的 SFTP 伺服器擷取檔案到 Amazon S3 或列出、刪除、重新命名或移動遠端伺服器上的檔案。SFTP 連接器支援兩種輸出類型：服務受管（使用 AWS 受管基礎設施）和 VPC（使用 Amazon VPC Lattice 透過 VPC 路由）。使用 SFTP 連接器，您可以在其中建置自動化、事件驅動的檔案傳輸工作流程 AWS。

檢視 [AWS Transfer Family SFTP 連接器](#)，以取得 Transfer Family SFTP 連接器的簡介。

主題

- [建立 SFTP 連接器](#)
- [SFTP 連接器的 VPC 連線能力](#)
- [使用 SFTP 連接器](#)
- [監控 SFTP 連接器](#)
- [管理 SFTP 連接器](#)
- [SFTP 連接器的擴展和配額](#)
- [使用 SFTP 連接器的參考架構](#)

建立 SFTP 連接器

本主題說明如何建立 SFTP 連接器。每個連接器都可以與一個遠端 SFTP 伺服器連線。您可以執行下列高階任務來設定 SFTP 連接器。

Note

如需透過虛擬私有雲端路由流量的 VPC 型連接器，請參閱[使用 VPC 型輸出建立 SFTP 連接器](#)。

1. 將連接器的身分驗證憑證存放在其中 AWS Secrets Manager。
2. 透過指定秘密 ARN、遠端伺服器的 URL 或資源組態 ARN、包含連接器所支援演算法的安全政策，以及其他組態設定，來建立連接器。

3. 建立連接器後，您可以對其進行測試，以確保它可以與遠端 SFTP 伺服器建立連線。

選擇 SFTP 連接器輸出類型

當您建立 SFTP 連接器時，您可以選擇介於「服務受管」和「VPC Lattice」之間的輸出類型。

- **服務受管（預設）**：連接器使用擁有的 NAT 閘道和 IP 地址 AWS Transfer Family，透過公有網際網路路由連線。此服務為您的連接器提供 3 個靜態 IP 地址，這些地址需要在遠端伺服器上允許列出以建立連線。
- **VPC Lattice**：連接器會使用 Amazon VPC Lattice 透過您的 VPC 環境路由流量。在下列情況下，使用 SFTP 連接器的 VPC 連線能力：
 - **私有 SFTP 伺服器**：連線至只能從 VPC 存取的 SFTP 伺服器
 - **內部部署連線**：透過 AWS Direct Connect 或 AWS Virtual Private Network 連線連線至內部部署 SFTP 伺服器
 - **自訂 IP 地址**：向遠端伺服器展示您自己的 NAT 閘道和彈性 IP 地址
 - **集中式安全控制**：透過組織的中央輸入/輸出控制路由檔案傳輸

下列矩陣可協助您為使用案例選擇正確的連接器類型。

SFTP 連接器輸出類型矩陣

功能	輸出類型 = 服務受管	輸出類型 = VPC Lattice
連線至公有託管（可存取網際網路）SFTP 伺服器	支援	支援的 ¹
連線至私有託管（內部部署）SFTP 伺服器	不支援	支援的 ²
連線至私有託管 (VPC 內) SFTP 伺服器	不支援	支援
呈現給遠端 SFTP 伺服器的靜態 IP 地址	透過服務提供的靜態 IP 地址支援	透過客戶擁有的靜態 IP 地址支援
可用的頻寬	每個帳戶 50 MBPS	更高的頻寬，可從客戶擁有的資源閘道和 NAT 閘道取得

功能	輸出類型 = 服務受管	輸出類型 = VPC Lattice
透過客戶擁有的 NAT Gateways 和 Network Firewalls 將流量路由至網際網路	不支援。NAT Gateways 由 Transfer Family 服務擁有和管理。	支援

¹ 在輸出類型 = VPC Lattice 的情況下，使用輸出 VPCs 中的輸出基礎設施 (NAT 閘道) 設定支援連線至公有託管伺服器。

² 在輸出類型 = VPC Lattice 的情況下，支援使用 VPC 中的現有網路連線至私有託管伺服器，例如 AWS Direct Connect 或 VPN。

選擇 IP 定址模式

當您使用服務管理的輸出建立 SFTP 連接器時，您可以選擇兩種 IP 定址模式：

- 僅限 IPv4（預設）：連接器僅使用 IPv4 地址連線至遠端 SFTP 伺服器。這是透過主控台、AWS CLI 或 API 建立連接器時的預設模式。
- 雙堆疊：連接器支援 IPv6 和 IPv4 地址。在雙堆疊模式中，當 DNS 解析傳回 IPv6 結果時，連接器偏好 IPv6，並在僅傳回 IPv4 DNS 結果時使用 IPv4。

Note

IP 定址模式僅適用於具有服務受管輸出類型的連接器。使用 VPC Lattice 輸出的連接器不支援此設定。

主題

- [在 Secrets Manager 中存放 SFTP 連接器的身分驗證憑證](#)
- [使用服務管理的輸出建立 SFTP 連接器](#)
- [使用 VPC 型輸出建立 SFTP 連接器](#)
- [測試 SFTP 連接器](#)

在 Secrets Manager 中存放 SFTP 連接器的身分驗證憑證

您可以使用 Secrets Manager 來存放 SFTP 連接器的使用者登入資料。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 連接器的配額](#)。

Note

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

在 Secrets Manager 中存放 SFTP 連接器的使用者登入資料

1. 登入 AWS 管理主控台 並在 <https://console.aws.amazon.com/secretsmanager/> 開啟 AWS Secrets Manager 主控台。
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. 提供秘密的金鑰/值資訊：您需要提供使用者名稱，以及私有金鑰或密碼。
 - a. 在鍵/值對區段中，選擇鍵/值索引標籤。
 - 金鑰 – 輸入 **Username**。
 - value – 輸入獲授權連接到合作夥伴伺服器的使用者名稱。
 - b. 如果您想要提供金鑰對，請選擇新增資料列，然後在金鑰/值對區段中，選擇金鑰/值索引標籤。
 - 金鑰 – 輸入 **PrivateKey**。
 - value – 貼到您的私有金鑰中。

秘訣：您輸入的私有金鑰資料必須對應至遠端 SFTP 伺服器上為此使用者存放的公有金鑰。

Note

無法使用受複雜密碼保護的私有金鑰搭配 AWS Transfer Family SFTP 連接器進行身分驗證。

如需如何產生公有/私有金鑰對的詳細資訊，請參閱 [在 macOS、Linux 或 Unix 上建立 SSH 金鑰](#)。

- c. 如果您想要提供密碼，請選擇新增資料列，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。
6. 選擇下一步。
7. 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，您可以將秘密命名為 **aws/transfer/connector-1**。
8. 選擇下一步，然後在設定輪換頁面上接受預設值。然後選擇下一步。
9. 在檢閱頁面上，選擇存放以建立和存放秘密。

使用服務管理的輸出建立 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

建立 SFTP 連接器

1. 在 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
2. 在左側導覽窗格中，選擇 SFTP 連接器，然後選擇建立 SFTP 連接器。
3. 在連接器組態區段中，針對輸出類型，選擇服務受管。此選項使用 AWS Transfer Family 受管輸出基礎設施。Transfer Family 服務提供和管理每個 SFTP 連接器的靜態 IP 地址。
4. 在連接器組態區段中，提供下列資訊：

Connector configuration

Egress type [Info](#)
Choose your SFTP connector's egress type: either directly over public internet, or via your VPC environment

☒ **Service managed**
Connect to public endpoints over the internet. The connector will present service-provided static IP addresses to remote server.

☐ **VPC Lattice**
Connect to public or private endpoints through your VPC. The connector will present elastic IP address from your VPC's CIDR range to remote server.

URL
Enter the URL of remote server to which you need to connect using the SFTP connector

URL of the remote (target) SFTP server

Access role [Info](#)
IAM Role for Amazon S3 access and AWS Secrets Manager access

Logging role - optional [Info](#)
IAM role for the connector to push events to your CloudWatch logs

- 針對 URL，輸入遠端 SFTP 伺服器的 URL。此 URL 必須格式化為 `sftp://partner-SFTP-server-url`，例如 `sftp://AnyCompany.com`。

Note

或者，您可以在 URL 中提供連接埠號碼。格式是 `sftp://partner-SFTP-server-url:port-number`。預設連接埠號碼（未指定連接埠時）是連接埠 22。

- 針對存取角色，選擇要使用的 (IAM) 角色的 Amazon Resource Name AWS Identity and Access Management (ARN)。
 - 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，您必須指定秘密的 ARN。ARN 包含秘密名稱，但以六個隨機的英數字元附加名稱。秘密的 ARN 格式如下。

```
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](#)。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListingOfUserFolder",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket"
      ]
    },
    {
      "Sid": "HomeDirObjectAccess",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
    },
    {
      "Sid": "GetConnectorSecretValue",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": "arn:aws:secretsmanager:us-west-2:111122223333: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，如果您想要為多個使用者和秘密重複使用相同的 IAM 角色，則可以儲存工作。例如，下列資源陳述式會授予名稱開頭為 `aws/transfer/` 的所有秘密的許可。

```
"Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/transfer/*"
```

您也可以將包含 SFTP 登入資料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](#)。

5. 完成連接器組態：

- （選用）針對記錄角色，選擇要用於將事件推送至 CloudWatch 日誌之連接器的 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": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource": "arn:aws:logs:*:*:log-group:/aws/transfer/*"
    }
  ]
}
```

6. 在 SFTP 組態區段中，提供下列資訊：

SFTP configuration [Info](#)

Connector credentials [Info](#)
Select a secret from AWS Secrets Manager containing the username and SSH private key, or username and password, to be used to connect to the remote server

aws/transfer/sftp-connector1 ▼

↻

Store a new secret ↗

Trusted host keys - optional [Info](#)
Enter the public portion of the host key(s) that is used to identify the remote server you need to connect to. You can enter the trusted host key(s) now, or add them after creating the connector by using the host key information returned by the TestConnection action.

① Connections to the remote server are established only if it's SSH fingerprint matches one of the provided trusted host key(s).

ssh-rsa AAAAF

Remove

Add trusted host key

Maximum concurrent connections [Info](#)
Select the maximum number of concurrent connections that your connector can create to the remote server

5 ▼

- 對於 Connector 登入資料，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 [在 Secrets Manager 中存放 SFTP 連接器的身分驗證憑證](#)。
- (選用) 您可以選擇在將 TrustedHostKeys 參數保留空白時建立連接器。不過，除非您在連接器的組態中提供此參數，否則連接器將無法透過遠端伺服器傳輸檔案。您可以在建立連接器時輸入信任的主機金鑰，或稍後使用 TestConnection 主控台動作或 API 命令傳回的主機金鑰資訊來更新連接器。也就是說，對於信任的主機金鑰文字方塊，您可以執行下列其中一項操作：
 - 在建立連接器時提供信任的主機金鑰 (信任的主機金鑰)。貼上用來識別外部伺服器的主機金鑰公有部分。您可以選擇新增信任的主機金鑰來新增額外的金鑰，以新增多個金鑰。您可以對 SFTP 伺服器使用 ssh-keyscan 命令來擷取必要的金鑰。如需 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](#)。
 - 建立連接器時，請將信任的主機金鑰 (Trusted Host Key) 文字方塊保留空白，稍後再使用此資訊更新您的連接器。如果您在建立連接器時沒有主機金鑰資訊，現在可以將此參數保留空白，並繼續建立連接器。建立連接器後，請使用新連接器的 ID 在 AWS CLI 中或從連接器的詳細資訊頁面執行 TestConnection 命令。如果成功，TestConnection 將傳回必要的主機金鑰資訊。然後，您可以使用 主控台 (或執行 UpdateConnector AWS CLI 命令) 編輯連接器，並新增執行時傳回的主機金鑰資訊 TestConnection。

⚠ Important

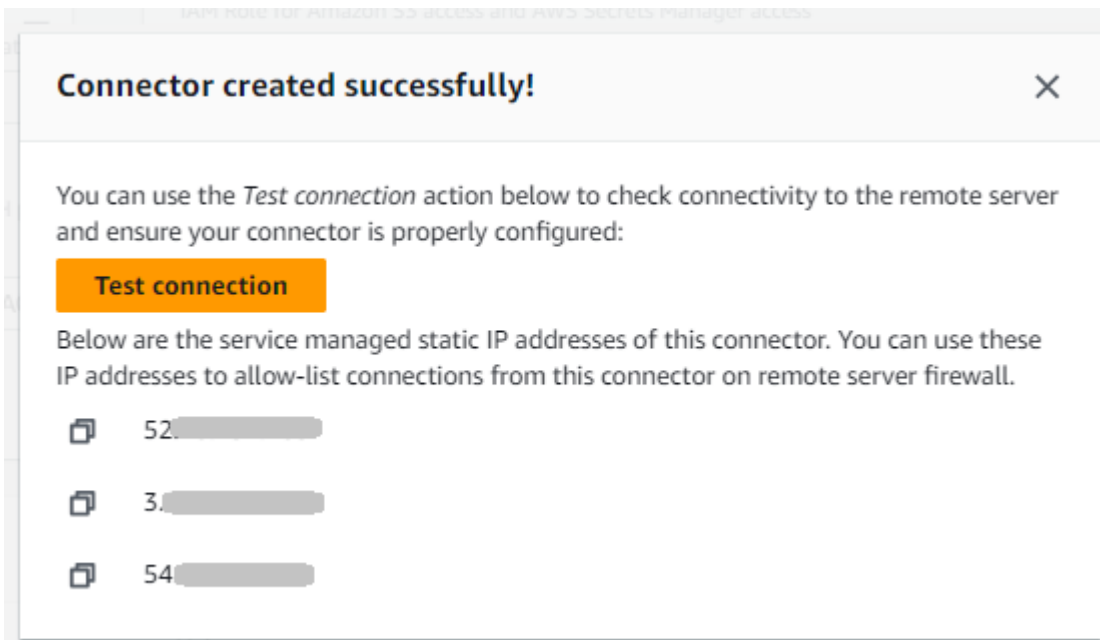
如果您透過執行 `來擷取遠端伺服器的主機金鑰` `TestConnection`，請務必對傳回的金鑰執行 `out-of-band` 驗證。

您必須接受信任的新金鑰，或是使用先前已知的指紋來驗證所呈現的指紋，而此指紋來自您要連線的遠端 SFTP 伺服器擁有者。

- (選用) 對於並行連線數量上限，從下拉式清單中選擇連接器建立到遠端伺服器的並行連線數量。主控台上的預設選擇為 5。

此設定指定您的連接器可以與遠端伺服器同時建立的作用中連線數目。建立並行連線可以透過啟用平行操作來增強連接器效能。

7. 在密碼編譯演算法選項區段中，從安全政策欄位中的下拉式清單中選擇安全政策。安全政策可讓您選取連接器支援的密碼編譯演算法。如需可用安全政策和演算法的詳細資訊，請參閱 [AWS Transfer Family SFTP 連接器的安全政策](#)。
8. (選用) 在標籤區段中，針對索引鍵和值，輸入一或多個標籤做為索引鍵/值對。
9. 確認所有設定後，請選擇建立 SFTP 連接器以建立 SFTP 連接器。如果成功建立連接器，則會出現一個畫面，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。



連接器頁面隨即出現，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。若要使用此命令來建立 SFTP 連接器，您必須提供下列資訊。

- 遠端 SFTP 伺服器的 URL。此 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 (IAM) 角色的 Amazon Resource Name AWS Identity and Access Management (ARN)。
 - 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，您必須指定秘密的 ARN。ARN 包含秘密名稱，但以六個隨機的英數字元附加名稱。秘密的 ARN 格式如下。

```
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](#)。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListingOfUserFolder",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket"
      ]
    }
  ]
}
```

```

    },
    {
      "Sid": "HomeDirObjectAccess",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
    },
    {
      "Sid": "GetConnectorSecretValue",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": "arn:aws:secretsmanager:us-west-2:111122223333: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，如果您想要為多個使用者和秘密重複使用相同的 IAM 角色，則可以儲存工作。例如，下列資源陳述式會授予名稱開頭為 `aws/transfer/` 之所有秘密的許可。

```
"Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/transfer/*"
```

您也可以將包含 SFTP 登入資料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）選擇要用於將事件推送至 CloudWatch 日誌之連接器的 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": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource": "arn:aws:logs:*:*:log-group:/aws/transfer/*"
    }
  ]
}
```

- 提供下列 SFTP 組態資訊。
 - 中 AWS Secrets Manager 包含 SFTP 使用者私有金鑰或密碼之秘密的 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 SFTP 資訊最簡單的方法是將其儲存至檔案。例如，將下列範例文字複製到名為的檔案 `testSFTPConfig.json`。

```
// Listing for testSFTPConfig.json
{
  "UserSecretId": "arn:aws::secretsmanager:us-east-2:123456789012:secret:aws/transfer/example-username-key",
  "TrustedHostKeys": [
    "sftp.example.com ssh-rsa AAAAbbbb...EEEE="
  ]
}
```

- 為您的連接器指定安全政策，輸入安全政策名稱。

Note

SecretId 可以是整個 ARN 或秘密的名稱（上一個清單中的 *example-username-key*）。

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 \  
--security-policy-name security-policy-name \  
--maximum-concurrent-connections integer-from-1-to-5
```

當您描述 VPC 輸出類型連接器時，回應會包含新欄位：

```
{  
  "Connector": {  
    "AccessRole": "arn:aws:iam::123456789012:role/connector-role",  
    "Arn": "arn:aws:transfer:us-east-1:123456789012:connector/  
c-1234567890abcdef0",  
    "ConnectorId": "c-1234567890abcdef0",  
    "Status": "ACTIVE",  
    "EgressConfig": {  
      "VpcLattice": {  
        "ResourceConfigurationArn": "arn:aws:vpc-lattice:us-  
east-1:123456789012:resourceconfiguration/rcfg-12345678",  
        "PortNumber": 22  
      }  
    },  
    "EgressType": "VPC",  
    "ServiceManagedEgressIpAddresses": null,  
    "SftpConfig": {  
      "TrustedHostKeys": [ "ssh-rsa AAAAB3NzaC..." ],  
      "UserSecretId": "aws/transfer/connector-secret"  
    },  
    "Url": "sftp://my.sftp.server.com:22"  
  }  
}
```

請注意，VPC 輸出類型連接器為 `ServiceManagedEgressIpAddresses` null，因為流量會透過 VPC 路由，而非 AWS 受管基礎設施。

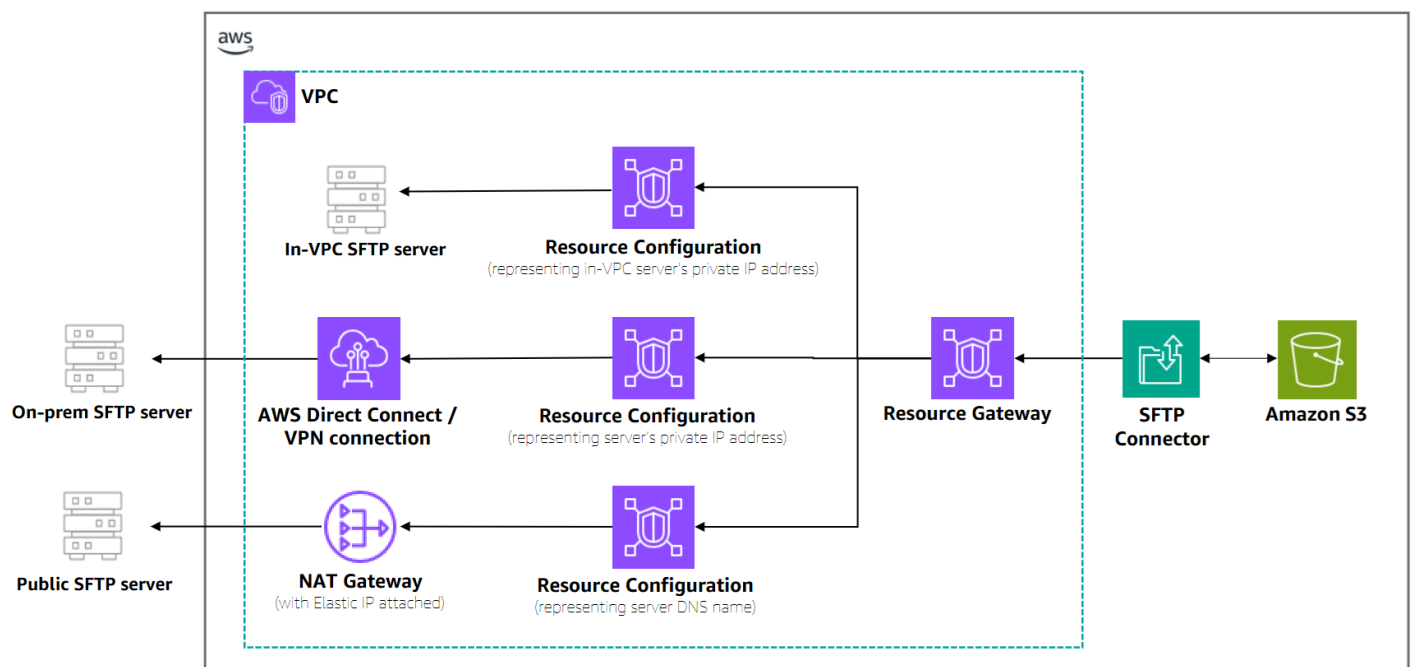
使用 VPC 型輸出建立 SFTP 連接器

本主題提供step-by-step說明。啟用 VPC_LATTICE 的連接器使用 Amazon VPC Lattice 透過虛擬私有雲端路由流量，啟用與私有端點的安全連線，或使用您自己的 NAT 閘道進行網際網路存取。

何時使用 VPC 連線

在下列情況下，使用 SFTP 連接器的 VPC 連線能力：

- 私有 SFTP 伺服器：連線至只能從 VPC 存取的 SFTP 伺服器。
- 內部部署連線：透過 AWS Direct Connect 或 AWS Site-to-Site VPN 連線連線至內部部署 SFTP 伺服器。
- 自訂 IP 地址：使用您自己的 NAT 閘道和彈性 IP 地址，包括 BYOIP 案例。
- 集中式安全控制：透過組織的中央輸入/輸出控制路由檔案傳輸。



啟用 VPC_LATTICE 的 SFTP 連接器的先決條件

在建立已啟用 VPC_LATTICE 的 SFTP 連接器之前，您必須完成下列先決條件：

VPC 型連線的運作方式

VPC Lattice 可讓您安全地與其他 AWS 服務共用 VPC 資源。AWS Transfer Family 使用服務網路來簡化資源共用程序。關鍵元件包括：

- 資源閘道：做為 VPC 的存取點。您可以在至少有兩個可用區域的 VPC 中建立此項目。
- 資源組態：包含您要連線之 SFTP 伺服器的私有 IP 地址或公有 DNS 名稱。

當您建立已啟用 VPC_LATTICE 的連接器時，AWS Transfer Family 會使用轉送存取工作階段 (FAS) 暫時取得您的登入資料，並將您的資源組態與我們的服務網路建立關聯。

必要的設定步驟

1. VPC 基礎設施：確保您已正確設定 VPC，其中包含 SFTP 伺服器連線需求所需的子網路、路由表和安全群組。
2. 資源閘道：使用 VPC Lattice `create-resource-gateway` 命令在 VPC 中建立資源閘道。資源閘道必須與至少兩個可用區域中的子網路相關聯。如需詳細資訊，請參閱《Amazon VPC Lattice 使用者指南》中的[資源閘道](#)。
3. 資源組態：使用 VPC Lattice `create-resource-configuration` 命令建立代表目標 SFTP 伺服器的資源組態。您可以指定下列其中一項：
 - 私有端點的私有 IP 地址
 - 公有端點的公有 DNS 名稱（公有端點不支援 IP 地址）
4. 身分驗證憑證：將 SFTP 使用者憑證存放在 AWS Secrets Manager，如中所述在 [Secrets Manager 中存放 SFTP 連接器的身分驗證憑證](#)。

Important

資源閘道和資源組態必須在相同的 AWS 帳戶中建立。建立資源組態時，您必須先備妥資源閘道。

如需 VPC 資源組態的詳細資訊，請參閱《Amazon VPC Lattice 使用者指南》中的[資源組態](#)。

Note

可使用 Amazon VPC Lattice 資源 AWS 區域的，提供 SFTP 連接器的 VPC 連線能力。如需詳細資訊，請參閱 [VPC Lattice FAQs](#)。可用區域支援因區域而異，資源閘道至少需要兩個可用區域。

建立已啟用 VPC_LATTICE 的 SFTP 連接器

完成先決條件後，您可以使用、AWS 管理主控台或 SDK AWS CLI 建立具有 VPC 連線能力的 SFTP 連接器。AWS SDKs

Console

建立已啟用 VPC_LATTICE 的 SFTP 連接器

1. 在 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
2. 在左側導覽窗格中，選擇 SFTP 連接器，然後選擇建立 SFTP 連接器。
3. 在連接器組態區段中，針對輸出類型，選擇 VPC Lattice。

此選項使用 Amazon VPC Lattice 透過 VPC 路由流量，以進行跨 VPC 資源存取。您可以使用此選項來連線至私有託管伺服器端點、透過 VPC 的安全控制路由流量，或使用您自己的 NAT 閘道和彈性 IP 地址。遠端 SFTP 伺服器的地址表示為 VPC 中的資源組態。如需資源組態的詳細資訊，請參閱《Amazon [VPC Lattice 使用者指南](#)》中的 [VPC 資源的資源組態](#)。

4. 完成連接器組態：
 - 針對存取角色，選擇要使用的 (IAM) 角色的 Amazon Resource Name AWS Identity and Access Management (ARN)。
 - 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，您必須指定秘密的 ARN。ARN 包含秘密名稱，但以六個隨機的英數字元附加名稱。秘密的 ARN 格式如下。

```
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](#)。

```
{  
  "Version": "2012-10-17",
```

```

"Statement": [
  {
    "Sid": "AllowListingOfUserFolder",
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Effect": "Allow",
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket"
    ]
  },
  {
    "Sid": "HomeDirObjectAccess",
    "Effect": "Allow",
    "Action": [
      "s3:PutObject",
      "s3:GetObject",
      "s3:DeleteObject",
      "s3:DeleteObjectVersion",
      "s3:GetObjectVersion",
      "s3:GetObjectACL",
      "s3:PutObjectACL"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
  },
  {
    "Sid": "GetConnectorSecretValue",
    "Effect": "Allow",
    "Action": [
      "secretsmanager:GetSecretValue"
    ],
    "Resource": "arn:aws:secretsmanager:us-  
west-2:111122223333: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，如果您想要為多個使用者和秘密重複使用相同的 IAM 角色，則可以儲存工作。例如，下列資源陳述式會授予名稱開頭為 `aws/transfer/` 之所有秘密的許可 `aws/transfer`。

```
"Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/transfer/*"
```

您也可以將包含 SFTP 登入資料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](#)。

- 針對資源組態 ARN，輸入指向 SFTP 伺服器的 VPC Lattice 資源組態 ARN：

```
arn:aws:vpc-lattice:region:account-id:resourceconfiguration/rcfg-12345678
```

- (選用) 針對記錄角色，選擇要用於將事件推送至 CloudWatch 日誌之連接器的 IAM 角色。

```
{
  "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/*"
    }
  ]
}
```

- 在 SFTP 組態區段中，提供下列資訊：

- 針對 Connector 登入資料，選擇中包含 AWS Secrets Manager SFTP 使用者私有金鑰或密碼的秘密名稱。
- 對於信任的主機金鑰，請將貼到用來識別外部伺服器的主機金鑰公有部分，或保留空白，以便稍後使用 `TestConnection` 命令進行設定。

由於此主機金鑰適用於 VPC_LATTICE 連接器，請移除金鑰中的主機名稱

- (選用) 針對並行連線數上限，選擇連接器建立到遠端伺服器的並行連線數 (預設為 5)。
6. 在密碼編譯演算法選項區段中，從下拉式清單中選擇安全政策。
 7. (選用) 在標籤區段中，將標籤新增為鍵/值對。
 8. 選擇建立 SFTP 連接器以建立已啟用 VPC_LATTICE 的 SFTP 連接器。

在佈建資源關聯PENDING時，將會建立狀態為 的連接器，這通常需要幾分鐘的時間。狀態變更為後ACTIVE，連接器即可使用。

CLI

使用下列命令來建立已啟用 VPC_LATTICE 的 SFTP 連接器：

```
aws transfer create-connector \
  --url "sftp://my.sftp.server.com:22" \
  --access-role arn:aws:iam::123456789012:role/TransferConnectorRole \
  --sftp-config UserSecretId=my-secret-id,TrustedHostKeys="ssh-rsa AAAAB3NzaC..." \
  --egress-config VpcLattice={ResourceConfigurationArn=arn:aws:vpc-lattice:us-east-1:123456789012:resourceconfiguration/rcfg-1234567890abcdef0} \
  --security-policy-name TransferSecurityPolicy-2024-01
```

VPC 連線的金鑰參數為 `--egress-config`，指定定義 SFTP 伺服器目標的資源組態 ARN。

監控 VPC 連接器狀態

啟用 VPC_LATTICE 的連接器具有非同步設定程序。建立後，監控連接器狀態：

- 待定：正在佈建連接器。服務網路佈建正在進行中，通常需要幾分鐘的時間。
- ACTIVE：連接器已準備就緒，可以傳輸檔案。
- ERRORED：連接器無法佈建。檢查錯誤詳細資訊以取得故障診斷資訊。

使用 `describe-connector` 命令檢查連接器狀態：

```
aws transfer describe-connector --connector-id c-1234567890abcdef0
```

在 PENDING 狀態期間，`test-connectionAPI` 將傳回「Connector not available」，直到佈建完成為止。

限制及考量

- 公有端點：透過 VPC 連線至公有端點時，您必須在資源組態中提供 DNS 名稱。不支援公有 IP 地址。
- 區域可用性：VPC 連線可在選取中使用 AWS 區域。不支援跨區域資源共用。
- 可用區域需求：資源閘道必須與至少兩個可用區域中的子網路相關聯。並非所有可用區域在每個區域中都支援 VPC Lattice。
- 連線限制：每個資源最多 350 個連線，TCP 連線的閒置逾時為 350 秒。

成本考量

除了一般服務費用 AWS Transfer Family 之外，沒有額外的費用。不過，客戶可能會因為共用其 Amazon Virtual Private Cloud 資源而產生來自 Amazon VPC Lattice 的額外費用，如果使用自己的 NAT 閘道輸出至網際網路，則會收取 NAT 閘道費用。

如需完整的 AWS Transfer Family 定價資訊，請參閱 [AWS Transfer Family 定價頁面](#)。

SFTP 連接器的 VPC 連線範例

本節提供為各種案例建立具有 VPC 連線能力的 SFTP 連接器的範例。使用這些範例之前，請確定您已完成 VPC 連線文件中所述的 VPC 基礎設施設定。

範例：私有端點連線

此範例示範如何建立 SFTP 連接器，以連接至只能從 VPC 存取的私有 SFTP 伺服器。

先決條件

1. 在 VPC 中建立資源閘道：

```
aws vpc-lattice create-resource-gateway \  
  --name my-private-server-gateway \  
  --vpc-identifier vpc-1234567890abcdef0 \  
  --subnet-ids subnet-1234567890abcdef0 subnet-0987654321fedcba0
```

2. 為您的私有 SFTP 伺服器建立資源組態：

```
aws vpc-lattice create-resource-configuration \  
  --name my-private-server-config \  
  --resource-gateway-identifier rgw-1234567890abcdef0 \
```



```
--resource-configuration-definition ipResource={ipAddress="10.0.1.100"} \  
--port-ranges 22
```

建立已啟用 VPC_LATTICE 的連接器

1. 建立具有 VPC 連線能力的 SFTP 連接器：

```
aws transfer create-connector \  
  --access-role arn:aws:iam::123456789012:role/TransferConnectorRole \  
  --sftp-config UserSecretId=my-private-server-credentials,TrustedHostKeys="ssh-  
rsa AAAAB3NzaC..." \  
  --egress-config VpcLattice={ResourceConfigurationArn=arn:aws:vpc-lattice:us-  
east-1:123456789012:resourceconfiguration/rcfg-1234567890abcdef0,PortNumber=22}
```

2. 監控連接器狀態，直到變成 ACTIVE：

```
aws transfer describe-connector --connector-id c-1234567890abcdef0
```

遠端 SFTP 伺服器將看到來自您 VPC CIDR 範圍內資源閘道 IP 地址的連線。

範例：透過 VPC 的公有端點

此範例說明如何透過 VPC 將連線路由至公有 SFTP 伺服器，以利用集中式安全控制並使用您自己的 NAT Gateway IP 地址。

先決條件

1. 在 VPC 中建立資源閘道（與私有端點範例相同）。
2. 使用公有 SFTP 伺服器 DNS 名稱建立資源組態：

```
aws vpc-lattice create-resource-configuration \  
  --name my-public-server-config \  
  --resource-gateway-identifier rgw-1234567890abcdef0 \  
  --resource-configuration-definition dnsResource={domainName="sftp.example.com"} \  
  \  
  --port-ranges 22
```

Note

對於公有端點，您必須使用 DNS 名稱，而不是 IP 地址。

建立連接器

- 建立 SFTP 連接器：

```
aws transfer create-connector \  
  --access-role arn:aws:iam::123456789012:role/TransferConnectorRole \  
  --sftp-config UserSecretId=my-public-server-credentials,TrustedHostKeys="ssh-  
rsa AAAAB3NzaC..." \  
  --egress-config VpcLattice={ResourceConfigurationArn=arn:aws:vpc-lattice:us-  
east-1:123456789012:resourceconfiguration/rcfg-0987654321fedcba0,PortNumber=22}
```

流量會從連接器流向資源閘道，然後透過 NAT Gateway 流向公有 SFTP 伺服器。遠端伺服器會將 NAT Gateway 的彈性 IP 地址視為來源。

範例：跨帳戶私有端點

此範例說明如何使用資源共用連線到不同 AWS 帳戶中的私有 SFTP 伺服器。

Note

如果您已透過其他機制啟用跨 VPC 資源共用 AWS Transit Gateway，例如，您不需要設定此處所述的資源共用。SFTP 連接器會自動使用現有的路由機制，例如 Transit Gateway 路由表。您只需在建立 SFTP 連接器的相同帳戶中建立資源組態。

帳戶 A（資源提供者）- 共用資源組態

1. 在帳戶 A 中建立資源閘道和資源組態（與先前的範例相同）。
2. 使用 Resource Access Manager 與帳戶 B 共用 AWS 資源組態：

```
aws ram create-resource-share \  
  --name cross-account-sftp-share \  
  --resource-arns arn:aws:vpc-lattice:us-  
east-1:111111111111:resourceconfiguration/rcfg-1234567890abcdef0 \  
  --resource-owner-account-id 111111111111
```

```
--principals 222222222222
```

帳戶 B (資源消費者) - 接受並使用共用

1. 接受資源共享邀請：

```
aws ram accept-resource-share-invitation \  
    --resource-share-invitation-arn arn:aws:ram:us-east-1:111111111111:resource-  
share-invitation/invitation-id
```

2. 在帳戶 B 中建立 SFTP 連接器：

```
aws transfer create-connector \  
    --access-role arn:aws:iam::222222222222:role/TransferConnectorRole \  
    --sftp-config UserSecretId=cross-account-server-  
credentials,TrustedHostKeys="ssh-rsa AAAAB3NzaC..." \  
    --egress-config VpcLattice={ResourceConfigurationArn=arn:aws:vpc-lattice:us-  
east-1:111111111111:resourceconfiguration/rcfg-1234567890abcdef0,PortNumber=22}
```

帳戶 B 中的連接器現在可以透過共用資源組態存取帳戶 A 中的私有 SFTP 伺服器。

常見的疑難排解案例：

以下是建立已啟用 VPC_LATTICE 的連接器時常見問題的解決方案：

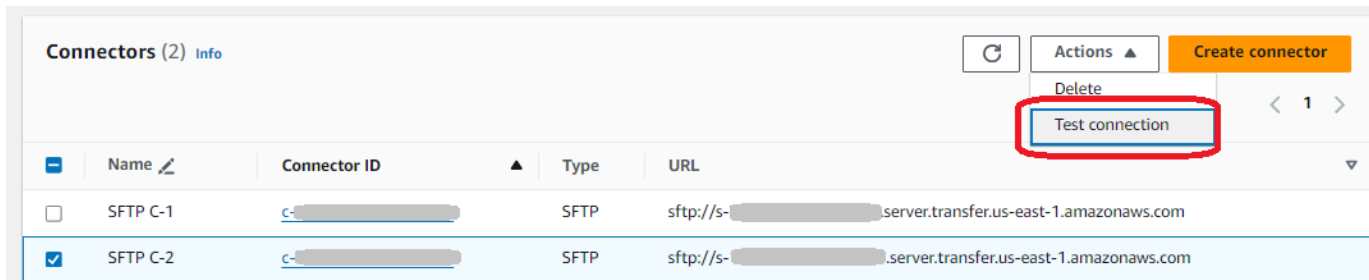
- 連接器卡在待定狀態：檢查您的資源閘道是否為 ACTIVE，並在支援的可用區域中具有子網路。如果連接器仍然卡在 PENDING 狀態，UpdateConnector 請使用您最初使用的相同組態參數來呼叫。這會觸發可能解決問題的新狀態事件。
- 連線逾時：驗證安全群組規則是否允許連接埠 22 上的流量，以及您的 VPC 路由是否正確。
- DNS 解析問題：對於公有端點，請確保您的 VPC 透過 NAT 閘道或網際網路閘道具有網際網路連線能力。
- 跨帳戶存取遭拒：確認資源共用已接受且資源組態 ARN 正確。如果在原始伺服器帳戶建立資源共用時，將適當的許可政策連接到資源組態，則需要這些許可：vpc-lattice:AssociateViaAWSService、vpc-lattice:AssociateViaAWSService-EventsAndStates、vpc-lattice:CreateServiceNetworkResourceAssociation、vpc-lattice:GetResourceConfiguration。

測試 SFTP 連接器

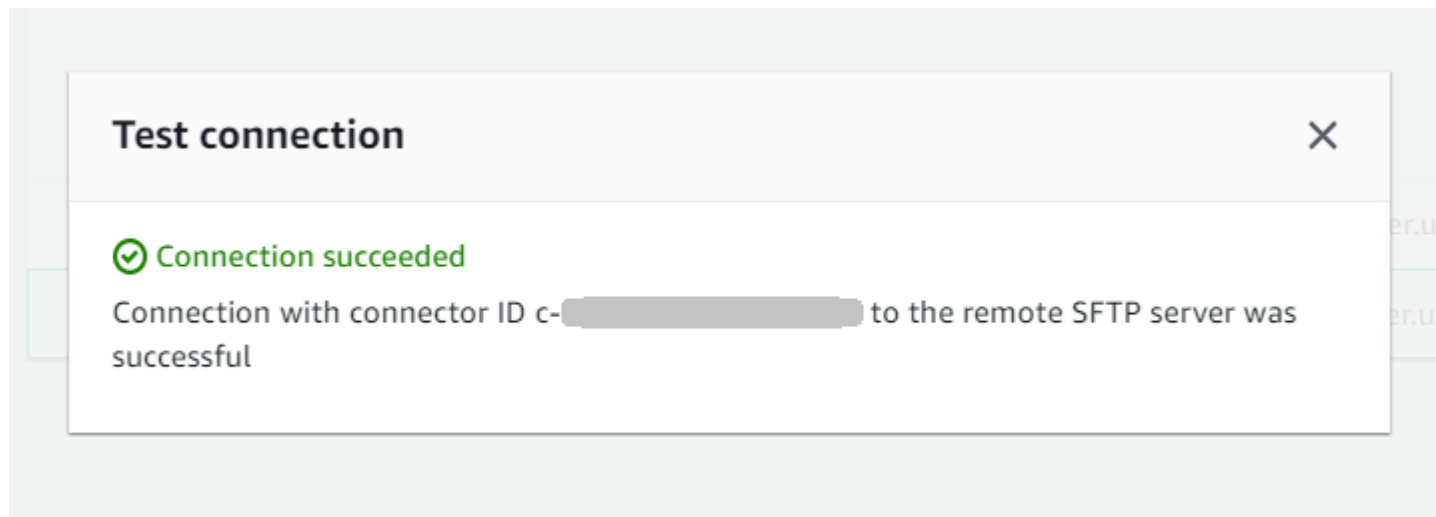
建立 SFTP 連接器後，建議您在嘗試使用新連接器傳輸任何檔案之前進行測試。

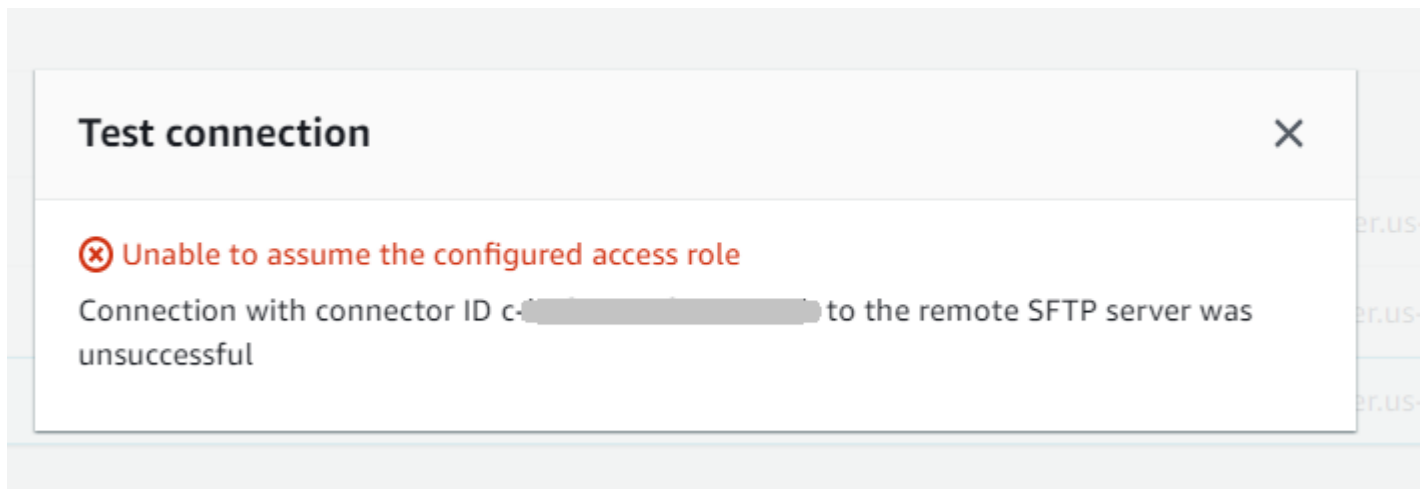
測試 SFTP 連接器

1. 在 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
2. 在左側導覽窗格中，選擇 SFTP 連接器，然後選取連接器。
3. 從動作功能表中，選擇測試連線。



系統會傳回訊息，指出測試通過或失敗。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。

SFTP 連接器的 VPC 連線能力

AWS Transfer Family SFTP 連接器支援使用 Amazon VPC Lattice 透過 VPC 環境連線至遠端 SFTP 伺服器。這可讓您與私有託管的 SFTP 伺服器連線，或透過 VPC 的安全控制路由網際網路流量，並使用您自己的 NAT 閘道和彈性 IP 地址。

輸出類型

SFTP 連接器可以使用兩種輸出類型之一：

- 服務受管（預設）：連接器使用擁有的 NAT 閘道和 IP 地址 AWS Transfer Family，透過公有網際網路路由連線。
- VPC_LATTICE：連接器會使用跨 VPC 資源存取，透過您的 VPC 環境路由流量。

何時使用 VPC 連線

在下列情況下，使用 SFTP 連接器的 VPC 連線能力：

- 私有 SFTP 伺服器：連線至只能從 VPC 存取的 SFTP 伺服器。
- 內部部署連線：透過 AWS Direct Connect 或 AWS Site-to-Site VPN 連線連線至內部部署 SFTP 伺服器。
- 自訂 IP 地址：使用您自己的 NAT 閘道和彈性 IP 地址，包括 BYOIP 案例。

- 集中式安全控制：透過組織的中央輸入/輸出控制路由檔案傳輸。

需求

在建立已啟用 VPC_LATTICE 的 SFTP 連接器之前，您需要：

- VPC 和相關基礎設施（子網路、路由表、安全群組）
- VPC 中的資源閘道（至少兩個可用區域）
- 指定目標 SFTP 伺服器的資源組態

如需詳細的設定說明，請參閱 [建立已啟用 VPC_LATTICE 的 SFTP 連接器](#)。此外，如需範例，請參閱 [SFTP 連接器的 VPC 連線範例](#)。

使用 SFTP 連接器

本主題說明如何使用 SFTP 連接器執行支援的檔案操作。您也可以在此 AWS Transfer Family 主控台上選取連接器的詳細資訊，以尋找執行這些操作的範例命令，網址為 <https://console.aws.amazon.com/transfer/>。

建立 SFTP 連接器之後，您可以使用它在與其相關聯的遠端 SFTP 伺服器上執行下列檔案操作。

- 將檔案從 Amazon S3 傳送至遠端 SFTP 伺服器。
- 從遠端 SFTP 伺服器擷取檔案至 Amazon S3。
- 從遠端 SFTP 伺服器上的目錄列出檔案和子資料夾。
- 刪除、重新命名或移動遠端 SFTP 伺服器上的檔案和目錄。

如需建立連接器的詳細資訊，請參閱 [建立 SFTP 連接器](#)。

主題

- [傳輸檔案](#)
- [列出遠端目錄的內容](#)
- [移動、重新命名或刪除遠端伺服器上的檔案或目錄](#)

傳輸檔案

主題

- [使用 SFTP 連接器傳送和擷取檔案](#)

使用 SFTP 連接器傳送和擷取檔案

若要使用 SFTP 連接器傳送和擷取檔案，您可以使用 [StartFileTransfer](#) API 操作並指定下列參數，這取決於您要傳送檔案（傳出傳輸）或接收檔案（傳入傳輸）。請注意，每個 `StartFileTransfer` 請求可以包含 10 個不同的路徑。

Note

根據預設，SFTP 連接器一次處理一個檔案，依序傳輸檔案。您可以選擇使用支援來自相同使用者的並行工作階段的遠端伺服器建立並行工作階段，並平行處理最多 5 個檔案，以加速傳輸效能。

若要啟用任何連接器的並行連線，您可以在建立或更新連接器時編輯並行連線上限設定。如需詳細資訊，請參閱[使用服務管理的輸出建立 SFTP 連接器](#)。

- 傳出傳輸

- `send-file-paths` 包含從 1 到 10 個來源檔案路徑，讓檔案傳輸到合作夥伴的 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` 是存放檔案的 Amazon S3 位置（儲存貯體和選用字首）。

若要傳送檔案，請指定 `send-file-paths` 和 `remote-directory-path` 參數。您最多可以為 `send-file-paths` 參數指定 10 個檔案。下列範例命令會將 `/amzn-s3-demo-source-bucket/file2.txt` 位於 Amazon S3 儲存體中名為 `/amzn-s3-demo-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 `amzn-s3-demo-source-bucket` 為您自己的儲存貯體。

```
aws transfer start-file-transfer --send-file-paths /amzn-s3-demo-source-bucket/
file1.txt /amzn-s3-demo-source-bucket/file2.txt \
--remote-directory-path /tmp --connector-id c-1111AAAA2222BBBB3 --region us-east-2
```

若要擷取檔案，請指定 `retrieve-file-paths` 和 `local-directory-path` 參數。下列範例會擷取 `/my/remote/file2.txt` 合作夥伴 SFTP 伺服器上的檔案 `/my/remote/file1.txt` 和 `remote/file2.txt`，並將其置於 Amazon S3 位置 `/amzn-s3-demo-bucket/prefix`。若要使用此範例命令，請以您自己的資訊取代 *user input placeholders*。

```
aws transfer start-file-transfer --retrieve-file-paths /my/remote/file1.txt /my/remote/file2.txt \
  --local-directory-path /amzn-s3-demo-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：也就是相對於 SFTP 使用者主目錄的路徑。例如，如果 SFTP 使用者是 `marymajor`，且 SFTP 伺服器上的主目錄是 `/users/marymajor/`，則下列命令會 `/amzn-s3-demo-source-bucket/file1.txt` 傳送至 `/users/marymajor/test-connectors/file1.txt`

```
aws transfer start-file-transfer --send-file-paths /amzn-s3-demo-source-bucket/file1.txt \
  --remote-directory-path test-connectors --connector-id c-2222BBBB3333CCCC4 --region us-east-2
```

列出遠端目錄的內容

從遠端 SFTP 伺服器擷取檔案之前，您可以擷取遠端 SFTP 伺服器上目錄的內容。若要這樣做，您可以使用 [StartDirectoryListing](#) API 操作。

下列範例列出遠端 SFTP 伺服器上資料夾的內容，該 `home` 資料夾在連接器的組態中指定。結果會放入 Amazon S3 位置 `/amzn-s3-demo-bucket/connector-files` 和名為 `AAAA1111BBBB2222C-6666abcd-11aa-22bb-cc33-0000aaaa3333.json` 的檔案。

```
aws transfer start-directory-listing \
  --connector-id c-AAAA1111BBBB2222C \
  --output-directory-path /amzn-s3-demo-bucket/example/connector-files \
  --remote-directory-path /home
```

此 AWS CLI 命令會傳回清單 ID 和包含結果的檔案名稱。

```
{
  "ListingId": "6666abcd-11aa-22bb-cc33-0000aaaa3333",
  "OutputFileName": "c-AAAA1111BBBB2222C-6666abcd-11aa-22bb-cc33-0000aaaa3333.json"
}
```


 Note

輸出檔案的命名慣例為 *connector-ID-listing-ID.json*。

JSON 檔案包含下列資訊：

- `filePath`：遠端檔案的完整路徑，相對於遠端伺服器上 SFTP 連接器的清單請求目錄。
- `modifiedTimestamp`：上次修改檔案的時間，以秒為單位，即國際標準時間 (UTC) 格式。此欄位為選用欄位。如果遠端檔案屬性不包含時間戳記，則會從檔案清單中省略。
- `size`：檔案大小，以位元組為單位。此欄位為選用欄位。如果遠端檔案屬性不包含檔案大小，則會從檔案清單中省略。
- `path`：遠端目錄的完整路徑，相對於遠端伺服器上 SFTP 連接器的清單請求目錄。
- `truncated`：標記，指出清單輸出是否包含遠端目錄中包含的所有項目。如果您的 `truncated` 輸出值為 `true`，您可以增加選用 `max-items` 輸入屬性中提供的值，以便能夠列出更多項目（最大允許清單大小為 200,000 個項目）。

以下是輸出檔案 (*c-AAAA1111BBBB2222C-6666abcd-11aa-22bb-cc33-0000aaaa3333.json*) 內容的範例，其中遠端目錄包含兩個檔案和兩個子目錄（路徑）。

```
{
  "files": [
    {
      "filePath": "/home/what.txt",
      "modifiedTimestamp": "2024-01-30T20:34:54Z",
      "size" : 2323
    },
    {
      "filePath": "/home/how.pgp",
      "modifiedTimestamp": "2024-01-30T20:34:54Z",
      "size" : 4691
    }
  ],
  "paths": [
    {
      "path": "/home/magic"
    },
    {
      "path": "/home/aws"
    }
  ]
}
```

```
    },  
  ],  
  "truncated": "false"  
}
```

移動、重新命名或刪除遠端伺服器上的檔案或目錄

主題

- [移動或重新命名遠端 SFTP 伺服器上的檔案或目錄](#)
- [刪除遠端 SFTP 伺服器上的檔案或目錄](#)

移動或重新命名遠端 SFTP 伺服器上的檔案或目錄

您可以使用 SFTP 連接器來移動或重新命名遠端 SFTP 伺服器上的檔案和目錄。請注意，遠端伺服器需要支援這些操作，才能使用連接器成功處理。

一些常見的使用案例如下所示。

- 遠端伺服器每小時會產生或接收新的檔案，其檔案名稱相同，但時間戳記不同。若要讓主要資料夾保持最新狀態（以便只包含最新的檔案），您可以使用連接器將較舊的檔案移至封存的資料夾。
- 您可以使用連接器列出遠端目錄中的所有檔案，然後將所有檔案傳輸到您的本機儲存體。然後，您可以使用連接器將檔案移至遠端伺服器上的封存資料夾。

您必須對要處理的每個檔案或目錄使用 `StartRemoteMove` 呼叫，因為命令會將單一來源和目的地檔案或目錄做為引數。不過，您可以透過讓連接器使用支援來自相同使用者的並行工作階段的遠端伺服器建立並行工作階段，以及平行移動/重新命名最多 5 個檔案，來加速效能。

下列範例會將遠端 SFTP 伺服器上的檔案從 `/source/folder/sourceFile` 移至 `/destination/targetFile`，並傳回操作的唯一識別符。

```
aws transfer --connector-id c-AAAA1111BBBB2222C start-remote-move \  
  --source-path /source/folder/sourceFile --target-path /destination/targetFile
```

Note

對於移動/重新命名操作，Transfer Family 會使用標準 SFTP `SSH_FXP_RENAME` 命令來執行移動/重新命名操作。

刪除遠端 SFTP 伺服器上的檔案或目錄

您可以使用 SFTP 連接器來刪除遠端 SFTP 伺服器上的檔案或目錄。請注意，遠端伺服器需要支援這些操作，才能使用連接器成功處理。

Note

只有空白目錄才支援遠端目錄的刪除操作。

一些常見的使用案例如下所示。

- 您可以使用連接器從遠端 SFTP 伺服器擷取檔案，將其存放在 Amazon S3 儲存貯體中，然後將其加密。最後，您可以使用連接器來刪除遠端伺服器上未加密的檔案。
- 您可以使用連接器列出遠端目錄中的所有檔案，然後將所有檔案傳輸到您的本機儲存體。然後，您可以使用連接器來刪除您傳輸的所有檔案。您也可以視需要刪除遠端目錄。

您必須對要刪除的每個檔案或目錄使用 `StartRemoteDelete` 呼叫，因為命令會將單一檔案或目錄做為引數。不過，您可以讓連接器使用支援相同使用者並行工作階段的遠端伺服器建立並行工作階段，並平行刪除最多 5 個檔案/目錄，以加速效能。

下列範例會刪除路徑 中遠端 SFTP 伺服器上的檔案 `/delete/folder/deleteFile`，並傳回 操作的唯一識別符。

```
aws transfer start-remote-delete --connector-id c-AAAA1111BBBB2222C \
  --delete-path /delete/folder/deleteFile
```

Note

對於刪除操作，Transfer Family 會使用標準 `SSH_FXP_REMOVE` 命令來刪除檔案，以及 `SSH_FXP_RMDIR` 刪除目錄。

監控 SFTP 連接器

您可以使用下列任何一種方式監控連接器操作的狀態。選擇符合您需求的方法。

使用連接器 API 查詢檔案傳輸請求的狀態

若要追蹤檔案傳輸操作的進度，您可以使用 [ListFileTransferResults](#) API 操作，該操作會傳回特定檔案傳輸操作中每個個別檔案狀態的即時更新和詳細資訊。您可以透過提供其連接器 ID 及其傳輸 ID 來指定檔案傳輸。下列範例會傳回連接器 ID a-1111222233334444 和 transfer-ID 的檔案清單 aa1b2c3d4-5678-90ab-cdef-EXAMPLE11111。

```
aws transfer list-file-transfer-results --connector-id a-1111222233334444 --transfer-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Note

檔案傳輸結果會在您呼叫 ListFileTransferResults API 操作後最多 7 天內提供。

您也可以檢視使用 SFTP 連接器之檔案傳輸請求的日誌和事件。Transfer Family 的 Amazon EventBridge 事件如中所述 [SFTP 連接器事件](#)。如需如何檢視 Transfer Family CloudWatch 日誌項目，請參閱 [檢視 Transfer Family 日誌串流](#)。

在 Amazon EventBridge 中檢視 SFTP 連接器事件

對於 SFTP 連接器執行的每個操作，Transfer Family 會自動產生事件並將其傳送至 Amazon EventBridge 帳戶中的預設事件匯流排。事件包含有關操作的詳細中繼資料，包括操作狀態。您可以在 EventBridge 中訂閱這些事件、對操作狀態等特定事件條件套用篩選條件，並根據狀態自動觸發下游動作。如需 SFTP 連接器操作所產生事件的詳細資訊，請參閱 [SFTP 連接器事件](#)。

在 Amazon CloudWatch 中檢視 SFTP 連接器日誌

所有 SFTP 連接器操作都會在 CloudWatch 中產生詳細日誌。如需 SFTP 連接器產生的日誌項目範例，請參閱 [SFTP 連接器的範例日誌項目](#)。

監控 VPC 輸出類型連接器

VPC 輸出類型連接器提供標準服務受管連接器以外的其他監控功能和考量事項：

連接器狀態監控

VPC_LATTICE 連接器包含其他資訊，可協助您監控佈建和操作狀態：

- EgressType 欄位：顯示 VPC VPC_LATTICE 輸出類型連接器
- EgressConfig 欄位：包含資源組態 ARN 和連接埠資訊

使用 describe-connector API 監控連接器狀態：

```
aws transfer describe-connector --connector-id c-1234567890abcdef0
```

VPC Lattice 成本監控

VPC 輸出類型連接器會產生您應監控的其他 VPC Lattice 費用：

- 資源提供者費用：作為資源提供者，您需要支付 0.006/GB 的資料處理費用（由 VPC Lattice 直接計費）
- 資源消費者費用：AWS Transfer Family 會吸收每 GB 0.01 USD 的資源消費者成本（前 1 PB）
- NAT Gateway 費用：對於透過 VPC 存取的公有端點，可能會收取額外的 NAT Gateway 和資料傳輸費用
- Transfer Family 費用：標準 0.40 USD/GB 的資料處理費用仍適用

透過 AWS Cost and Billing 主控台監控 VPC Lattice 用量和成本，依 VPC Lattice 服務進行篩選。

VPC 連接器的網路監控

監控 VPC 輸出類型連接器的網路活動和效能：

- VPC 流程日誌：啟用 VPC 流程日誌來監控資源閘道和 SFTP 伺服器之間的網路流量模式
- VPC Lattice 存取日誌：VPC Lattice 提供存取日誌，顯示來源/目的地 IP 地址、連線時間和資料傳輸磁碟區
- 安全群組監控：監控安全群組規則和流量模式，以確保適當的網路存取控制
- DNS 解析監控：監控服務網路端點的 DNS 解析時間和失敗

範例 VPC Lattice 存取日誌項目：

```
{
  "eventTimestamp": "2025-01-16T20:59:08.531Z",
  "serviceNetworkArn": "arn:aws:vpc-lattice:us-east-1:123456789012:servicenetwork/sn-1234567890abcdef0",
  "sourceVpcArn": "arn:aws:ec2:us-east-1:123456789012:vpc/vpc-12345678",
```

```
"resourceConfigurationArn": "arn:aws:vpc-lattice:us-east-1:123456789012:resourceconfiguration/rcfg-12345678",
"protocol": "tcp",
"sourceIpPort": "10.0.1.100:33760",
"destinationIpPort": "10.0.2.200:22",
"gatewayIpPort": "10.0.1.150:1769",
"resourceIpPort": "10.0.2.200:22"
}
```

透過監控進行故障診斷

使用監控資料來疑難排解常見的 VPC 連接器問題：

- 等待狀態：監控 DNS 解析進度並等待 ACTIVE 狀態，然後再嘗試傳輸
- 連線逾時：檢查 VPC 流量日誌和安全群組規則是否有連接埠 22 上的流量遭到封鎖
- 傳輸失敗：檢閱 CloudWatch 日誌以取得詳細的錯誤訊息，以及檢閱 VPC Lattice 存取日誌以取得網路層級問題
- 效能問題：監控 VPC Lattice 存取日誌的連線時間和輸送量指標

管理 SFTP 連接器

本主題說明如何檢視和更新 SFTP 連接器。

Note

每個連接器都會自動指派靜態 IP 地址，在連接器的生命週期內保持不變。這可讓您與只接受來自已知 IP 地址之傳入連線的遠端 SFTP 伺服器連線。您的連接器會獲指派一組靜態 IP 地址，由所有連接器在中使用相同的通訊協定 (SFTP 或 AS2) 共用 AWS 帳戶。這些地址並非專屬於您的帳戶。

如果您需要專用且可預測的 IP 地址，請使用以 VPC 為基礎的輸出來設定連接器。如需詳細資訊，請參閱[the section called “使用 VPC 型輸出建立 SFTP 連接器”](#)。

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
```

更新 VPC 連線設定

您可以更新現有連接器的 VPC 連線設定，包括在服務受管和 VPC 輸出類型之間切換，或變更資源組態 ARN。

若要將連接器從服務受管切換到 VPC 輸出：

```
aws transfer update-connector \
  --connector-id connector-id \
  --egress-type VPC \
  --egress-config ResourceConfigurationArn=resource-configuration-arn
```

若要更新已啟用 VPC_LATTICE 連接器的資源組態 ARN：

```
aws transfer update-connector \
  --connector-id connector-id \
  --egress-config ResourceConfigurationArn=new-resource-configuration-arn
```

Note

更新 VPC 連線設定時，連接器狀態會在重新設定程序 PENDING 期間變更為。使用 `describe-connector` 命令監控連接器狀態。

檢視 SFTP 連接器詳細資訊

您可以在主控台找到 AWS Transfer Family 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 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
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。

您可以在連接器詳細資訊頁面上選擇編輯，以變更 SFTP 連接器的屬性。

監控 VPC 連接器狀態

啟用 VPC_LATTICE 的連接器包含其他狀態資訊，可協助您監控佈建程序：

- 狀態：顯示 PENDING、ACTIVE 或 ERRORED
- EgressType：顯示 VPC 或 SERVICE_MANAGED
- EgressConfig：包含 VPC 連接器的資源組態 ARN
- 錯誤：如果連接器處於 ERRORED 狀態，請提供詳細的錯誤資訊

對於 VPC 連接器，ServiceManagedEgressIpAddresses 欄位將為 null，因為流量會改為使用您的 VPC IP 地址。

Note

您可以執行 following AWS Command Line Interface (AWS CLI) 命令，取得大部分此資訊，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 API 參考 [DescribeConnector](#) 中的。

SFTP 連接器的擴展和配額

主題

- [SFTP 連接器的配額](#)
- [擴展 SFTP 連接器](#)

SFTP 連接器的配額

SFTP 連接器有下列配額。

Note

中的 [AWS Transfer Family 端點和配額](#) 會列出更多 SFTP 連接器的服務配額 Amazon Web Services 一般參考。

SFTP 連接器配額

名稱	預設	可調整
每秒測試連線交易數上限 (TPS)	每個帳戶每秒 1 個請求	否
待定檔案傳輸的佇列大小上限	1000	否
檔案大小上限	150 GB (GiB)	否
每個檔案的傳輸時間上限	12 小時	否
每個檔案的請求等待時間上限	12 小時	否
每個帳戶連接器的最大頻寬 (SFTP 和 AS2 連接器都有助於此值)	50 MBps	否
目錄列出操作的項目數量上限	200,000	否

 Note

根據預設，SFTP 連接器一次處理一個檔案，依序傳輸檔案。您可以選擇使用支援來自相同使用者的並行工作階段的遠端伺服器建立並行工作階段，並平行處理最多 5 個檔案，以加速傳輸效能。

若要啟用任何連接器的並行連線，您可以在建立或更新連接器時編輯並行連線上限設定。如需詳細資訊，請參閱[使用服務管理的輸出建立 SFTP 連接器](#)。

為了儲存 SFTP 連接器的登入資料，每個 Secrets Manager 秘密都有相關聯的配額。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

擴展 SFTP 連接器

本節描述如何擴展 AWS Transfer Family SFTP 連接器工作負載的考量。當您想要使用 SFTP 連接器擴展工作負載時，您需要考慮以下三個適用的配額。

- 佇列大小上限。這是指連接器佇列中已請求的待處理操作數目上限。待定操作是指任何先前提交但尚未成功完成的轉移請求，無論是成功還是失敗。

待定請求的最大佇列深度目前設定為每個連接器 1,000 個（如[AWS Transfer Family 服務配額](#)中所定義）。當您在短時間內請求數千個傳輸操作時，您的工作負載可能會超過此服務限制，而且您會收到 `ThrottlingException` 訊息超過待處理請求上限的。如果您的工作負載受限於此配額，請透過 AWS 支援 或您的客戶團隊聯絡 Transfer Family 服務團隊，以討論您的可擴展性需求。

您也可以採取下列其中一個或兩個動作。

- 將您的檔案磁碟區分散到多個連接器。
- 讓您的連接器與遠端伺服器建立並行工作階段，以平行處理來自佇列的多個請求。
- 並行工作階段的數量。根據預設，SFTP 連接器一次傳輸一個檔案，依序從佇列傳輸檔案。

您可以選擇讓連接器平行傳輸多個檔案，以加速傳輸效能。您可以使用支援來自相同使用者的並行工作階段的遠端伺服器建立並行工作階段，並平行處理最多 5 個檔案。當您建立 SFTP 連接器時，請在建立或更新連接器時，為最大並行連線設定選擇最多 5 的值。如需詳細資訊，請參閱[使用服務管理的輸出建立 SFTP 連接器](#)。

- **StartFileTransfer** 請求的速率。您可以請求每秒最多 100 個檔案路徑，以便透過每個 SFTP 連接器進行傳輸。請求的檔案路徑會新增至連接器的佇列以進行處理。無論個別 `StartFileTransfer` 命令中提供的檔案數目為何，您都可以以遞迴方式使用 `StartFileTransfer` 命令來請求每個連接器每秒最多 100 個檔案路徑。

使用 SFTP 連接器的參考架構

本節列出可用於使用 SFTP 連接器設定自動檔案傳輸工作流程的參考資料。您可以使用 Amazon EventBridge 中的 SFTP 連接器事件，在檔案傳輸動作與中的前置和後置處理動作之間協調，以設計您自己的事件驅動架構 AWS。

部落格文章

下列部落格文章提供使用 SFTP 連接器建置 MFT 工作流程的參考架構，包括在使用 SFTP 連接器將檔案傳送到遠端 SFTP 伺服器之前，先使用 PGP [AWS Transfer Family 加密檔案：使用 SFTP 連接器和 PGP 加密來架構安全且合規的受管檔案傳輸](#)。

研討會

- 下列研討會提供實作實驗室，用於設定 SFTP 連接器，以及使用您的連接器從遠端 SFTP 伺服器傳送或擷取檔案：[Transfer Family - SFTP 研討會](#)。
- 以下研討會提供實作實驗室，以建置全自動化和事件驅動的工作流程，涉及將檔案傳輸到外部 SFTP 伺服器或從外部 SFTP 伺服器傳輸到 Amazon S3，以及這些檔案的常見前置和後置處理：[事件驅動的 MFT 研討會](#)。

此影片提供本研討會的逐步解說。

解決方案

AWS Transfer Family 提供下列解決方案：

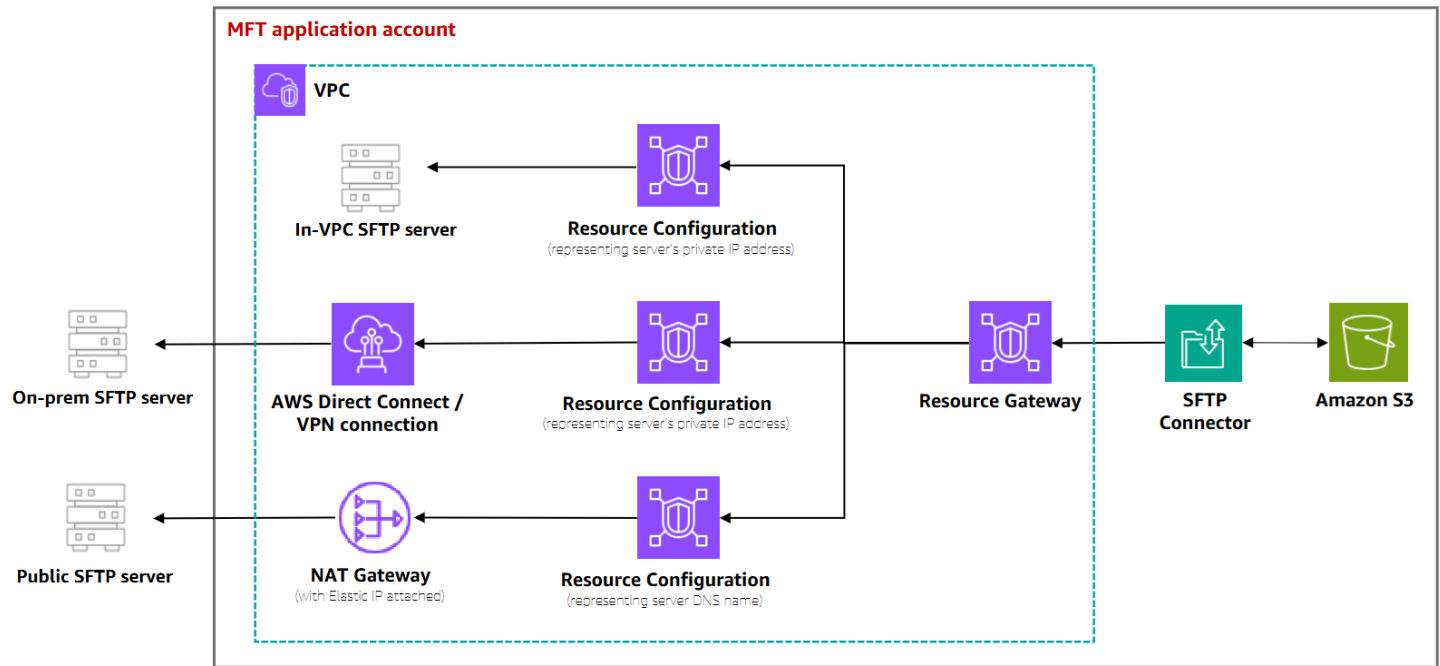
- [檔案傳輸同步解決方案](#)提供參考架構，以自動化使用 SFTP 連接器與本機 Amazon S3 儲存貯體同步遠端 SFTP 目錄的程序，包括整個資料夾結構。它協調列出遠端目錄、偵測變更以及傳輸新檔案或修改檔案的程序。
- [Serverlessland - 使用在遠端 SFTP 伺服器與 S3；之間選擇性檔案傳輸 AWS Transfer Family](#)提供範例模式，用於列出存放在遠端 SFTP 位置上的檔案，以及將選擇性檔案傳輸到 Amazon S3。

VPC 參考架構

下列參考架構顯示部署已啟用 VPC_LATTICE 的 SFTP 連接器的常見模式。這些範例可協助您了解需要在整體 AWS 架構中建立 VPC Lattice 資源的位置。

具有共用輸出基礎設施的單一帳戶

在此架構中，輸出基礎設施 (NAT Gateway、VPN 通道或 Direct Connect) 是在與您 SFTP 連接器相同的帳戶中的 VPC 中設定。所有連接器都可以共用相同的資源閘道和 NAT 閘道。

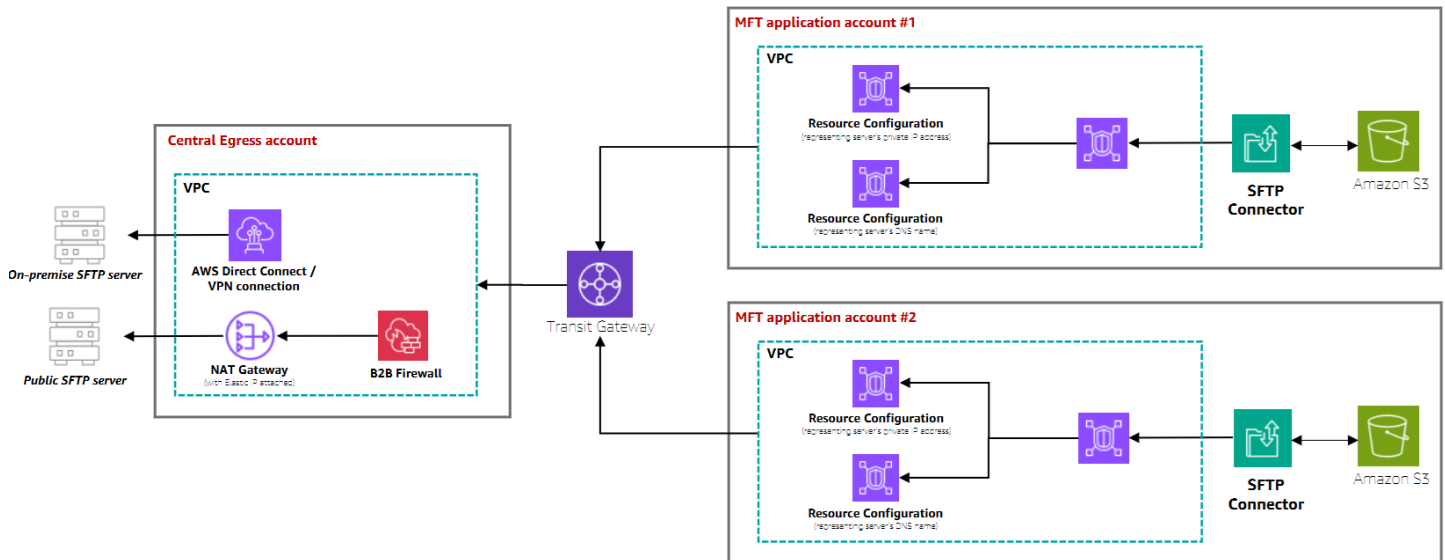


此模式的理想時機如下：

- 所有 SFTP 連接器都在單一 中管理 AWS 帳戶
- 輸出基礎設施是在與 SFTP 連接器位於相同帳戶內的 VPC 中設定

具有集中式輸出基礎設施的跨帳戶

在此架構中，輸出基礎設施 (NAT Gateway、VPN 通道、Direct Connect 或 B2B 防火牆) 是在網路團隊管理的中央輸出帳戶中設定。SFTP 連接器是在由 MFT 管理員團隊管理的 MFT 應用程式帳戶中建立。使用 Transit Gateway 建立跨帳戶聯網，以遵守現有的聯網規則。



此模式的理想時機如下：

- 網路基礎設施由專用帳戶中的個別團隊管理
- 您在建立 SFTP 連接器的帳戶與設定輸出基礎設施的帳戶之間有現有的路由（例如 AWS Transit Gateway）。SFTP 連接器將能夠利用您現有的路由來連接兩個帳戶。
- 需要集中式安全控制和 B2B 防火牆
- 您需要維持聯網和應用程式團隊之間的職責分離

AWS Transfer Family 適用於 AS2 的

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。保護傳輸中的 AS2 承載會使用加密訊息語法 (CMS) 搭配加密和數位簽章，以提供資料保護和對等身分驗證。已簽署的訊息處置通知 (MDN) 回應承載可提供訊息已接收並成功解密的驗證（不可否認）。

AS2 通訊協定對於具有合規要求的工作流程至關重要，這些工作流程依賴於在協定中內建的資料保護和安全性功能。AWS Transfer Family AS2 端點經過 [Drummond 認證](#)，可讓零售、生命科學、製造、金融服務和公用程式等產業的客戶安全地與其業務合作夥伴交易。

當您搭配 Transfer Family 使用 AS2 時，交易的資料可在中 AWS 原生存取：

- 處理、分析和機器學習
- 與企業資源規劃 (ERP) 系統整合
- 與客戶關係管理 (CRM) 系統整合

若要與具有 AS2-enabled 之伺服器的合作夥伴交換檔案，您必須：

- 產生用於加密的公有/私有金鑰對
- 產生公有/私有金鑰對以進行簽署
- 與您的合作夥伴交換公有金鑰

Important

目前不支援 HTTPS AS2 伺服器端點。您必須負責終止 TLS。

Transfer Family 提供您可以參加的研討會，您可以在其中設定啟用 AS2 的 Transfer Family 端點，以及 Transfer Family AS2 連接器。您可以[在這裡](#)檢視此研討會的詳細資訊。

如需在 Transfer Family 中設定 AS2 step-by-step 說明，請參閱以下內容：

1. [匯入 AS2 憑證](#)
2. [建立 AS2 設定檔](#)
3. [建立 AS2 伺服器](#)
4. [建立 AS2 協議](#)

5. 設定 AS2 連接器

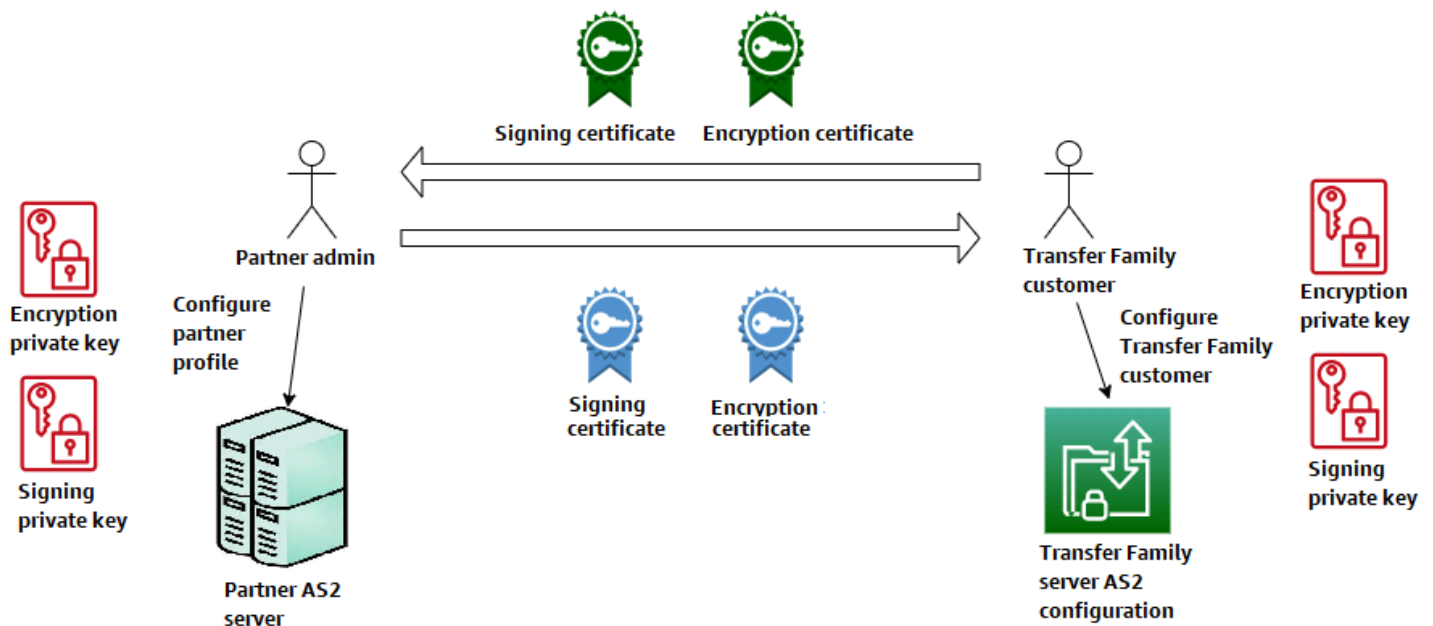
如需完整範例，請參閱 [設定 AS2 組態](#)。

Note

若要顯示 AS2 Terraform 範本的支援，請將拇指向上反應 (#) 新增至 [Transfer Family Terraform 範本功能請求](#)。您也可以新增說明使用案例的註解。

AS2 使用案例

如果您是想要與AS2-enabled之伺服器的合作夥伴交換檔案 AWS Transfer Family 的客戶，則設定中最複雜的部分包括產生一個公有/私有金鑰對以進行加密，以及產生一個用於簽署，以及與合作夥伴交換公有金鑰。



考慮將 AWS Transfer Family 與 AS2 搭配使用的下列變化。

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。
下表中的所有提及 MDN 都會假設已簽署MDNs。

AS2 使用案例

僅限傳入使用案例

- 將加密的 AS2 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：

- 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。
- 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您的合作夥伴設定檔以進行加密。
- 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，您的合作夥伴可以傳送加密的訊息給您，而且您可以解密它們並將其存放在 Amazon S3 儲存貯體中。

- 將加密的 AS2 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（做為新增至合作夥伴設定檔的簽署憑證）。

- 將加密的 AS2 訊息從交易合作夥伴傳輸到 Transfer Family 伺服器，並新增簽署和傳送 MDN 回應。

在此案例中，您仍然只執行傳入傳輸，但現在除了接收已簽署的承載之外，您的交易合作夥伴還希望收到已簽署的 MDN 回應。

- 匯入您的公有和私有簽署金鑰（做為您設定檔的簽署憑證）。
- 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

- 將加密的 AS2 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。在此情況下，您會將交易合作夥伴的公有金鑰匯入其設定檔。

- 將加密的 AS2 訊息從 Transfer Family 伺服器傳輸到交易合作夥伴，並新增簽署。

您仍然只進行對外轉移，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（做為新增至設定檔的簽署憑證）。
 2. 將公有金鑰傳送給您的交易合作夥伴。
- 將加密的 AS2 訊息從 Transfer Family 伺服器傳輸到交易合作夥伴，並新增簽署並傳送 MDN 回應。

您仍然只執行傳出傳輸，但現在除了傳送已簽署的承載之外，還希望從交易合作夥伴收到已簽署的 MDN 回應。

1. 您的交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（做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 and 交易合作夥伴之間雙向傳輸加密的 AS2 訊息。

在此情況下，請執行下列操作：

- 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您的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，而且可以解密它們。您可以將收到的訊息存放在 Amazon S3 儲存貯體中，您的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的 AS2 訊息，並新增簽署。

現在您和您的合作夥伴想要已簽章的訊息。

- 匯入您的簽署私有金鑰（做為新增至設定檔的簽署憑證）。
 - 將公有金鑰傳送給您的交易合作夥伴。
 - 匯入您交易合作夥伴的簽署公有金鑰，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的 AS2 訊息，並新增簽署並傳送 MDN 回應。

現在，您想要交換已簽署的承載，而且您和您的交易合作夥伴都想要 MDN 回應。

- 您的交易合作夥伴會傳送其公有簽署金鑰給您。
- 匯入您交易合作夥伴的公有金鑰（做為您合作夥伴設定檔的簽署憑證）。
- 將您的公有金鑰傳送給您的交易合作夥伴。

AS2 CloudFormation 範本

本主題提供有關 AWS CloudFormation 範本的資訊，您可以用來快速部署 AS2 伺服器和組態 AWS Transfer Family。這些範本會自動化設定程序，並協助您實作 AS2 檔案傳輸的最佳實務。

- 基本 AS2 範本說明於 [使用 範本建立示範 Transfer 系列 AS2 堆疊](#)
- 中說明自訂 HTTP 標頭的 AS2 範本 [自訂 AS2 訊息的 HTTP 標頭](#)。

自訂 AS2 範本

您可以自訂提供的範本，以符合您的特定需求：

1. 從 S3 URL 下載範本。
2. 修改 YAML 程式碼以調整組態，例如：
 - 安全性設定和憑證組態
 - 網路架構和 VPC 設定
 - 儲存選項和檔案處理
 - 監控和通知偏好設定
3. 將修改後的範本上傳至您自己的 S3 儲存貯體。
4. 使用 CloudFormation 主控台或 部署自訂範本 AWS CLI。

Important

自訂範本時，請確定您維護資源之間的相依性，並遵循安全最佳實務。

測試您的 AS2 部署

使用範本部署 AS2 伺服器之後，您可以測試組態：

1. 檢查 CloudFormation 堆疊輸出的範例命令和端點資訊。
2. 使用 AWS CLI 傳送測試檔案：

```
aws s3api put-object --bucket your-bucket-name --key test.txt --body test.txt  
aws transfer start-file-transfer --connector-id your-connector-id --send-file-  
paths /your-bucket-name/test.txt
```

3. 在目的地 S3 儲存貯體中驗證檔案交付。
4. 檢查 CloudWatch 日誌是否有成功的處理和 MDN 回應。

如需更全面的測試，請考慮使用第三方 AS2 用戶端將檔案傳送到 Transfer Family AS2 伺服器。

AS2 範本部署的最佳實務

使用 AS2 CloudFormation 範本時，請遵循下列最佳實務：

安全

使用強式憑證並定期輪換。

實作最低權限的 IAM 政策。

使用安全群組限制網路存取。

可靠性

跨多個可用區域部署。

針對失敗的傳輸實作監控和提醒。

設定失敗傳輸的自動重試。

效能

為您的傳輸磁碟區選擇適當的執行個體類型。

實作 S3 生命週期政策以實現高效的檔案管理。

監控和最佳化網路組態。

成本最佳化

針對可變工作負載使用自動擴展。

實作較舊檔案的 S3 儲存類別。

根據實際用量監控和調整資源。

設定 AS2

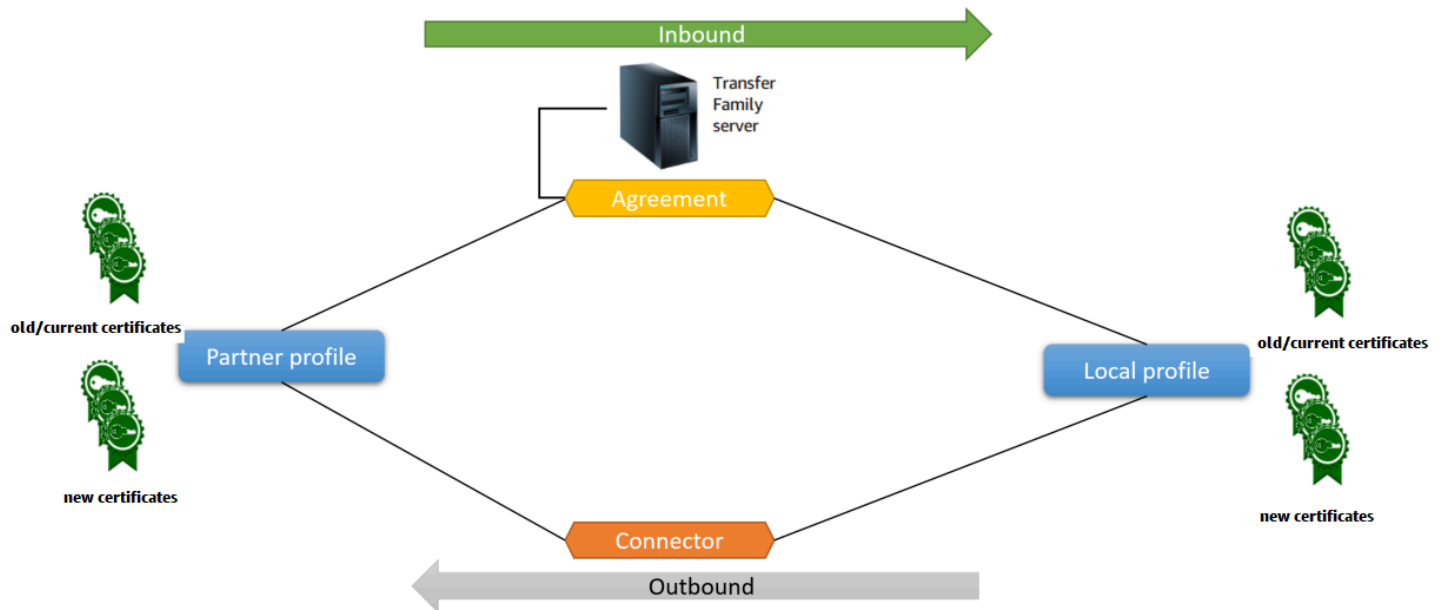
若要建立AS2-enabled的伺服器，您還必須指定下列元件：

- 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。為了定義協議，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 系列 AS2-inbound程序使用協議。

- 憑證 – 公有金鑰 (X.509) 憑證用於 AS2 通訊，以進行訊息加密和驗證。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（啟用 AS2 的 Transfer Family 伺服器）組織或 "party"。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-enabled 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。將檔案傳送到客戶的外部非 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 end-to-end 範例 AS2 組態，請參閱 [設定 AS2 組態](#)。

主題

- [AS2 組態](#)
- [AS2 配額和限制](#)
- [AS2 功能](#)

AS2 組態

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。

簽署、加密、壓縮、MDN

對於傳入和傳出轉接，下列項目為必要或選用：

- 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是 ZLIB）
- 訊息處置通知 (MDN) – 選用

密碼

傳入和傳出傳輸都支援下列密碼：

- AES128_CBC
- AES192_CBC
- AES256_CBC
- 3DES（僅適用於回溯相容性）

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，支援特定類型，如下所示：

- 傳入傳輸 – 同步和非同步
- 傳出傳輸 – 同步和非同步
- 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 上終止 TLS。如[透過 HTTPS 接收 AS2 訊息](#)中所述。

- 傳出傳輸 – 如果您提供 HTTP URL，您還必須指定加密演算法。如果您提供 HTTPS URL，您可以選擇為加密演算法指定 NONE。

AS2 配額和限制

本節討論 AS2 的配額和限制

主題

- [AS2 配額](#)
- [處理秘密的配額](#)
- [已知限制](#)

AS2 配額

AS2 檔案傳輸具有下列配額。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
每個傳出請求的檔案數量上限	10	否
每秒傳出請求的數量上限	100	否
每秒傳入請求的數量上限	100	否
每個帳戶的最大傳出頻寬（傳出 SFTP 和 AS2 請求都有助於此值）	每秒 50 MB	否

處理秘密的配額

AWS Transfer Family AWS Secrets Manager 代表使用基本身分驗證的 AS2 客戶呼叫。此外，Secrets Manager 會呼叫 AWS KMS。

Note

這些配額並非專屬於您使用 Transfer Family 的秘密：它們會與您 中的所有服務共用 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	Description
<code>DescribeSecret</code> 和 <code>GetSecretValue</code> API 請求的合併速率	每個支援的區域：每秒 1 萬個	合併 <code>DescribeSecret</code> 和 <code>GetSecretValue</code> API 操作的每秒交易上限。

對於 AWS KMS，下列配額適用於 `Decrypt`。如需詳細資訊，請參閱[每個 AWS KMS API 操作的請求配額](#)

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

配額名稱	預設值 (每秒請求數)
	- 亞太區域 (東京), ap-northeast-1 - 歐洲 (法蘭克福), eu-central-1 - 歐洲 (倫敦), eu-west-2 - 下列區域中為 50,000 (共用) : - 美國東部 (維吉尼亞北部), us-east-1 - 美國西部 (奧勒岡), us-west-2 - 歐洲 (愛爾蘭), eu-west-1
自訂金鑰存放區請求配額  Note 此配額僅適用於您使用外部金鑰存放區的情況。	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。 - 每個 AWS CloudHSM 金鑰存放區 1,800 個 (共用) - 每個外部金鑰存放區 1800 個 (共用)

已知限制

- 不支援伺服器端 TCP 保持連線。除非用戶端傳送持續連線封包，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 logs 中的作用中協議，訊息必須包含有效的 AS2 標頭。
- 從 AWS Transfer Family for AS2 接收訊息的伺服器必須支援密碼編譯訊息語法 (CMS) 演算法保護屬性，以驗證訊息簽章，如 [RFC 6211](#) 中所定義。某些舊版 IBM Sterling 產品不支援此屬性。
- 重複的訊息 IDs 會產生已處理/警告：重複的文件訊息。
- AS2 憑證的金鑰長度必須至少為 2048 位元，最多為 4096 位元。
- 將 AS2 訊息或非同步 MDNs 傳送至交易合作夥伴的 HTTPS 端點時，訊息或 MDNs 必須使用由公開信任憑證授權單位 (CA) 簽署的有效 SSL 憑證。自我簽署憑證目前僅支援傳出傳輸。
- 端點必須支援 TLS 1.2 版通訊協定和安全政策允許的密碼編譯演算法 (如 [AWS Transfer Family 伺服器的安全政策](#))。
- 目前不支援來自 AS2 1.2 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。

- 您可以將檔案處理工作流程連接至使用 AS2 通訊協定的 Transfer Family 伺服器：不過，AS2 訊息不會執行連接到伺服器的工作流程。

AS2 功能

下表列出使用 AS2 的 Transfer Family 資源可用的功能。

AS2 功能

Transfer Family 為 AS2 提供下列功能。

Feature	Supported by AWS Transfer Family
Drummond 認證	Yes
AWS CloudFormation 支援	Yes
Amazon CloudWatch 指標	Yes
SHA-2 密碼編譯演算法	Yes
Support for Amazon S3	Yes
Support for Amazon EFS	No
Scheduled Messages	Yes ¹
AWS Transfer Family Managed Workflows	No
Certificate Exchange Messaging (CEM)	No
Mutual TLS (mTLS)	No
Support for self-signed certificates	Yes

1. [使用 Amazon EventBridge 排程 AWS Lambda 函數](#) 可用的傳出排程訊息

AS2 傳送和接收功能

下表提供 AWS Transfer Family AS2 傳送和接收功能的清單。

Capability	Inbound: Receiving with server	Outbound: Sending with connector
TLS 加密傳輸 (HTTPS)	是 ¹	Yes
Non-TLS Transport (HTTP)	Yes	是 ²
Synchronous MDN	Yes	Yes
Message Compression	Yes	Yes
Asynchronous MDN	Yes	Yes
Static IP Address	Yes	Yes
Bring Your Own IP Address	Yes	No
Multiple File Attachments	No	No
Basic Authentication	No	Yes
AS2 Restart	Not applicable	No
AS2 Reliability	No	No
Custom Subject per Message	Not applicable	No

1. Network Load Balancer (NLB) 或 Application Load Balancer (ALB) 提供傳入 TLS 加密傳輸
2. 只有在啟用加密時才能使用傳出非 TLS Transport

管理 AS2 憑證

本主題討論如何匯入和管理 AS2 憑證。匯入憑證是 Transfer Family 的 AS2 程序的第一步。

1. 匯入憑證
2. [建立 AS2 設定檔](#)
3. [建立 AS2 伺服器](#)
4. [建立 AS2 協議](#)

5. 設定 AS2 連接器

匯入 AS2 憑證

Transfer Family AS2 程序使用憑證金鑰來加密和簽署傳輸的資訊。合作夥伴可以針對這兩個目的使用相同的金鑰，或針對每個目的使用個別的金鑰。如果您有由可信任第三方託管的常見加密金鑰，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。透過使用單獨的簽署金鑰（您未託管的金鑰），您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。

下列要點詳細說明如何在程序期間使用 AS2 憑證。

- 傳入 AS2
 - 交易合作夥伴會傳送簽署憑證的公有金鑰，而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，而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進行簽署，並匯入憑證的私有金鑰以進行簽署。
 - 如果您使用的是 HTTPS，則可以匯入自我簽署的 Transport Layer Security (TLS) 憑證。

如需如何建立憑證的詳細資訊，請參閱 [the section called “步驟 1：建立 AS2 的憑證”](#)。

此程序說明如何使用 Transfer Family 主控台匯入憑證。如果您想要 AWS CLI 改用，請參閱 [the section called “步驟 2：將憑證匯入為 Transfer Family 憑證資源”](#)。

指定 AS2-enabled 憑證

1. 在 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
2. 在左側導覽窗格的 AS2 交易合作夥伴下，選擇憑證。
3. 選擇 Import certificate (匯入憑證)。

- 在憑證組態區段中，針對憑證描述，輸入憑證易於識別的名稱。請確定您可以透過憑證的描述來識別憑證的用途。此外，選擇憑證的角色。
- 在憑證使用量區段中，選擇此憑證的用途。它可用於加密、簽署或兩者。

秘訣：如果您為用量選擇加密和簽署，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。

- 在憑證內容區段中，提供交易合作夥伴的公有憑證，或本機憑證的公有和私有金鑰。

在憑證內容區段中填入適當的詳細資訊。

- 如果您選擇自我簽署憑證，則不會提供憑證鏈。
 - 將憑證文字及其鏈貼到憑證和憑證鏈欄位中。
 - 如果此憑證是本機憑證，請貼入其私有金鑰。
- 選擇匯入憑證以完成程序，並儲存匯入憑證的詳細資訊。

Note

TLS 憑證只能匯入為合作夥伴的公有憑證。如果您從合作夥伴選取公有憑證，然後選取使用量的 Transport Layer Security (TLS)，您會收到警告。此外，TLS 憑證必須是自我簽署（也就是說，您必須選取自我簽署憑證才能匯入 TLS 憑證）。

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（強制性）。如果您願意，可以為這兩個目的指定單一憑證。

憑證輪換是將舊過期憑證取代為較新憑證的程序。如果協議中的合作夥伴尚未為傳出傳輸設定新憑證，或可能正在傳送在也可能使用較新憑證的期間使用舊憑證簽署或加密的承載，則轉換是一項漸進式轉換，以避免中斷傳輸。新舊憑證都有效的中繼期間稱為寬限期。

X.509 憑證具有 Not Before 和 Not After 日期。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。

憑證過期監控

Transfer Family 會在匯入憑證 `DaysUntilExpiry` 後發佈 Amazon CloudWatch 指標。指標會發出目前日期與憑證 `InactiveDate` 上指定為 的日期之間的天數。指標位於 CloudWatch 指標儀表板的 `Transfer AWS` 命名空間下。

此指標一律會有 `CertificateId` 的指標維度，如果客戶在憑證上提供，則選擇性地包含描述維度。如需 CloudWatch 指標維度的詳細資訊，請參閱 CloudWatch API 參考中的 [維度](#)。

Note

在匯入 Transfer Family 的憑證之後，最多可能需要一整天的時間，才能將此指標傳送到客戶帳戶。

您可以使用此指標來建立 CloudWatch 警示，以便在憑證即將過期時通知您。

傳出憑證選擇會使用傳輸日期之前的值上限做為 `Inactive Date`。傳入程序接受 `Not Before` 和 範圍內的憑證 `Not After`，以及 `Active Date` 和 範圍內的憑證 `Inactive Date`。

憑證輪換範例

下表說明為單一設定檔設定兩個憑證的一種可能方式。

兩個輪換中的憑證

名稱	NOT BEFORE (由憑證授權單位控制)	ACTIVE DATE (由 Transfer Family 設定)	INACTIVE DATE (由 Transfer Family 設定)	NOT AFTER (由憑證授權單位設定)
Cert1 (較舊的憑證)	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 `Not Before` 和 之間的範圍內 `Not After`。

- 我們建議您為每個設定檔設定多個憑證，確保所有憑證的作用中日期範圍都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成非作用中，以及較新的憑證變成作用中時，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。在 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

本主題討論如何建立設定檔以用於 AS2 程序。本機設定檔會定義本機（啟用 AS2 的 Transfer Family 伺服器）組織或 "party"。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。

1. [匯入 AS2 憑證](#)
2. 建立 AS2 設定檔
3. [建立 AS2 伺服器](#)
4. [建立 AS2 協議](#)
5. [設定 AS2 連接器](#)

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。如果您想要改用 AWS CLI，請參閱 [the section called “步驟 3：為您和您的交易合作夥伴建立設定檔”](#)。

建立 AS2 設定檔

1. 在 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
2. 在左側導覽窗格的 AS2 交易合作夥伴下，選擇設定檔，然後選擇建立設定檔。
3. 在設定檔組態區段中，輸入設定檔的 AS2 ID。此值用於 AS2 通訊協定特定的 HTTP 標頭 `as2-fromas2-to`，並識別交易合作夥伴關係，這會決定要使用的憑證等。
4. 在設定檔類型區段中，選擇本機設定檔或合作夥伴設定檔。
5. 在憑證區段中，從下拉式選單中選擇一或多個憑證。

秘訣：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中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](#)。

6. （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。
7. 選擇建立設定檔以完成程序並儲存新的設定檔。

建立 AS2 伺服器

本主題提供使用主控台或 CloudFormation 範本建立 AS2-enabled Transfer Family 伺服器的指示。如需 end-to-end 範例 AS2 組態，請參閱 [設定 AS2 組態](#)。建立 AS2 伺服器之後，您可以將協議新增至伺服器。

1. [匯入 AS2 憑證](#)
2. [建立 AS2 設定檔](#)
3. 建立 AS2 伺服器
4. [建立 AS2 協議](#)
5. [設定 AS2 連接器](#)

主題

- [使用 Transfer Family 主控台建立 AS2 伺服器](#)
- [使用 範本建立示範 Transfer 系列 AS2 堆疊](#)
- [建立 AS2 協議](#)

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 AS2-enabled 的伺服器。如果您想要 AWS CLI 改用，請參閱 [the section called “步驟 4：建立使用 AS2 通訊協定的 Transfer Family 伺服器”](#)。

Note

您可以將檔案處理工作流程連接至使用 AS2 通訊協定的 Transfer Family 伺服器：不過，AS2 訊息不會執行連接到伺服器的工作流程。

建立 AS2-enabled 的伺服器

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

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。反之，您可以透過虛擬私有雲端 (VPC) 安全群組來控制存取。

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

Select a VPC ID ▼ [Refresh](#) [Create a VPC](#)

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

☐ FIPS Enabled endpoint

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

- a. 針對端點類型，選擇託管的 VPC 來託管伺服器的端點。如需設定 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。若要讓 VPC 端點可透過網際網路存取，請在存取下選擇網際網路面向，然後提供彈性 IP 地址。

b. 針對存取，選擇下列其中一個選項：

- 內部 – 選擇此選項可在 VPC 和 VPC 連線環境中提供存取權，例如透過 Direct Connect 或 VPN 的現場部署資料中心。
- 面向網際網路 – 選擇此選項以透過網際網路以及從您的 VPC 和 VPC 連線環境提供存取，例如透過 Direct Connect 或 VPN 的現場部署資料中心。

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，請選擇現有的 VPC 或選擇建立 VPC 以建立新的 VPC。
- d. 對於啟用 FIPS，保持 FIPS 啟用端點核取方塊清除。

Note

AS2 通訊協定不支援啟用 FIPS 的端點。

e. 選擇下一步。

6. 在選擇網域頁面上，選擇 Amazon S3，使用選取的通訊協定將檔案儲存並存取為物件。

選擇下一步。

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 AS2 一起設定，則會套用所有其他詳細資訊設定。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，我們強烈建議進行設定，以便您可以查看訊息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，以確保它們正確無誤。

- 如果您想要編輯任何設定，請選擇您要變更之步驟旁的編輯。

 Note

如果您編輯步驟，我們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。

可能需要幾分鐘的時間，新伺服器的狀態才會變更為線上。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 系列 AS2 堆疊

我們提供獨立的 CloudFormation 範本，以快速建立 AS2-enabled 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。

基本 AS2 伺服器範本會建立下列資源：

- 具有 VPC 端點 AS2-enabled 的 Transfer Family 伺服器
- 具有憑證的本機和合作夥伴 AS2 設定檔
- 設定檔之間的協議
- 檔案儲存的 Amazon S3 儲存貯體
- 必要的 IAM 角色和政策
- CloudWatch 記錄組態

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，因為您需要支付使用此服務的費用。在 Secrets Manager 中刪除這些憑證並不會從 Transfer Family 伺服器中刪除它們。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，建議您使用 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，並建立可在生產中使用的 AWS Lambda 函數。

從 CloudFormation 範本建立 AS2-enabled 的 Transfer Family 伺服器

1. 在 <https://console.aws.amazon.com/cloudformation> 開啟 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，選擇選擇現有範本。
5. 複製此連結 [AS2 示範範本](#)，並將其貼到 Amazon S3 URL 欄位中。
6. 選擇下一步。
7. 在指定堆疊詳細資訊頁面上，為您的堆疊命名，然後指定下列參數：
 - 在 AS2 下，輸入 Local AS2 ID 和 Partner AS2 ID 的值，或 partner 分別接受預設值 local 和。
 - 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

此值採用 CIDR 格式，可指定傳入流量至 AS2 伺服器的 IP 地址。預設值 0.0.0.0/0 會允許所有 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-*amzn-s3-demo-bucket*。
8. 選擇下一步。在設定堆疊選項頁面上，再次選擇下一步。
 9. 檢閱您正在建立之堆疊的詳細資訊，然後選擇建立堆疊。

Note

在頁面底部的功能下，您必須確認 CloudFormation 可能會建立 AWS Identity and Access Management (IAM) 資源。

建立堆疊之後，您可以使用 AWS Command Line Interface ()，將測試 AS2 訊息從合作夥伴伺服器傳送至本機 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 [AWS Command Line Interface](#) 《使用者指南》中的 [安裝或更新最新版本的 AWS CLI](#)。

範例命令具有下列格式：

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key test.txt && aws transfer start-file-transfer --region aws-region --connector-id TransferConnectorId --send-file-paths /amzn-s3-demo-bucket/test.txt
```

 Note

此命令的版本包含堆疊中 *amzn-s3-demo-bucket* 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。

第一個命令會在您的儲存貯體中建立新的空白文字檔案：

```
aws s3api put-object --bucket amzn-s3-demo-bucket --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 /amzn-s3-demo-bucket/test.txt
```

執行命令後，您可以前往 Amazon S3 儲存貯體 (*amzn-s3-demo-bucket*) 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檔案和 MDN 回應的 JSON 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，此資料夾應為空白。
- *server-id/* – 此資料夾會根據 Transfer Family 伺服器 ID 命名。它包含 *from-partner* (此資料夾根據合作夥伴的 AS2 ID 動態命名)，它本身包含 *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。

建立 AS2 協議

協議與 Transfer Family 伺服器相關聯。它們為使用 AS2 通訊協定交換訊息或檔案的交易合作夥伴指定詳細資訊，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 改用，請參閱 [the section called “步驟 5：建立您與合作夥伴之間的協議”](#)。

建立 Transfer Family 伺服器的協議

1. 在 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
2. 在左側導覽窗格中，選擇伺服器，然後選擇使用 AS2 通訊協定的伺服器。

或者，只要您至少有一個使用 AS2 通訊協定的 Transfer Family 伺服器，請選取協議以從 AS2 交易合作夥伴選單接收訊息。AS2 然後，在建立協議畫面中，選取要與本合約建立關聯的 AS2 伺服器。

3. 在伺服器詳細資訊頁面上，向下捲動至協議區段。
4. 選擇新增協議。
5. 填寫協議參數，如下所示：
 - a. 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，設定協議的狀態：作用中（預設為選取）或非作用中。
 - b. 在通訊組態區段中，選擇本機設定檔和合作夥伴設定檔。此外，選擇是否強制執行訊息簽署。
 - 根據預設，啟用強制執行訊息簽署，這表示 Transfer Family 拒絕來自您交易合作夥伴的未簽署訊息。
 - 清除此設定，以允許 Transfer Family 接受來自您交易合作夥伴的未簽署訊息。
 - c. 在收件匣目錄組態區段中，提供下列資訊。
 - 決定是否選取指定個別目錄來存放 AS2 訊息、MDN 檔案和 JSON 狀態檔案。
 - 如果選取此選項，您可以指定承載檔案、失敗檔案、MDN 檔案、狀態檔案和暫存檔案的個別位置。
 - 如果您清除此選項，所有 AS2 檔案都會進入您為基礎目錄指定的位置。
 - 針對 S3 儲存貯體，選擇 Amazon S3 儲存貯體。

- 對於字首，您可以輸入要用於在儲存貯體中存放檔案的字首（資料夾）。

例如，如果您 **amzn-s3-demo-bucket** 為儲存貯體輸入，**incoming** 並為字首輸入，則 AS2 檔案會儲存到 **/amzn-s3-demo-bucket/incoming** 資料夾。

- 針對 AWS IAM 角色，選擇可存取您指定之儲存貯體的角色。
 - 針對保留檔案名稱，選擇是否要保留傳入 AS2 訊息承載的原始檔案名稱。
 - 如果您選取此設定，則當檔案儲存在 Amazon S3 中時，交易合作夥伴提供的檔案名稱會保留。
 - 如果您清除此設定，則 Transfer Family 儲存檔案時，會調整檔案名稱，如 中所述[檔案名稱和位置](#)。
- 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。

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）。

準備好連接器後，您可以將資訊傳輸給交易合作夥伴。每個 AS2 伺服器都會指派三個靜態 IP 地址。AS2 連接器使用這些 IP 地址透過 AS2 傳送非同步 MDNs 給您的交易合作夥伴。

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。

1. [匯入 AS2 憑證](#)
2. [建立 AS2 設定檔](#)
3. [建立 AS2 伺服器](#)
4. [建立 AS2 協議](#)

5. 建立 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 改用，請參閱 [the section called “步驟 6：在您和合作夥伴之間建立連接器”](#)。

建立 AS2 連接器

1. 在 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
2. 在左側導覽窗格中，從 AS2 交易合作夥伴功能表中選擇要傳送訊息的連接器，然後選擇建立 AS2 連接器。
3. 在連接器組態區段中，指定下列資訊：

- URL – 輸入傳出連線的 URL。
- IP 定址模式 – 選擇僅限 IPv4（預設）以僅使用 IPv4 地址，或選擇雙堆疊來支援 IPv6 和 IPv4。在雙堆疊模式中，當 DNS 解析傳回 IPv6 結果時，連接器偏好 IPv6，並在僅傳回 IPv4 DNS 結果時使用 IPv4。
- 存取角色 – 選擇要使用的 (IAM) 角色的 Amazon Resource Name AWS Identity and Access Management (ARN)。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

如果您為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 AWS 受管金鑰中的加密 AWS Secrets Manager，則角色也需要該金鑰的 `kms:Decrypt` 許可。如果您以字首命名秘密 `aws/transfer/`，您可以使用萬用字元 (*) 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 日誌的 IAM 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，以及是否壓縮傳輸的資訊。注意下列事項：
 - Preserve S3 Content-Type 參數預設為啟用。

設定時，Transfer Family 會使用與 S3 中的物件相關聯的 Amazon S3，而不是根據副檔名來映射內容類型。Content-Type 如果您希望服務根據副檔名來映射 AS2 訊息的內容類型，而不是使用 S3 物件中的內容類型，請清除此設定。

- 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，因為它是一種較弱的加密演算法。
- 在與連接器一起傳送的 AS2 訊息中，主旨會用作 subject HTTP 標頭屬性。
- 如果您選擇在沒有加密演算法的情況下建立連接器，則必須指定 HTTPS 做為您的通訊協定。

5. 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登入資料，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。這些登入資料必須符合連線至合作夥伴端點的使用者。

The screenshot shows the 'Basic authentication' section of the AWS Transfer Family console. It includes a checkbox to 'Enable Basic authentication - optional' with a note to select this option for authenticating with a trading partner's host. Below this is the 'Basic authentication credentials' section, where users can choose to 'Create a new secret' (selected) or 'Choose an existing secret'. There are input fields for 'Username' (containing 'test-user') and 'Password' (masked with dots). A blue information box at the bottom states: 'Update the access role associated with your connector to provide AWS Transfer Family with permission to read the secret containing your Basic authentication credentials.'

- 若要使用現有的秘密，請選擇選擇現有的秘密，然後從下拉式功能表中選擇秘密。如需在 Secrets Manager 中建立正確格式秘密的詳細資訊，請參閱 [啟用 AS2 連接器的基本身分驗證](#)。

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

Choose a secret

- aws/transfer/...
SFTP connector...
- aws/transfer/sftp-connector1
Secret key ...
- aws/transfer/c...

or to provide AWS Transfer Family with permission to credentials.

6. 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 AS2 接收您的訊息之後，傳送 MDN 給您。
- 已簽署 MDN – 您可以選擇要求簽署 MDNs。只有在您已選取請求 MDN 時，才能使用此選項。

7. 確認所有設定後，請選擇建立 AS2 連接器以建立連接器。

連接器頁面隨即出現，並將新連接器的 ID 新增至清單。若要檢視連接器的詳細資訊，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
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Type	演算法
	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 HTTPS 時，才能使用基本身分驗證。

若要對連接器使用身分驗證，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，秘密中的登入資料都會與使用此連接器的傳出訊息一起傳送。登入資料必須符合嘗試連線至交易合作夥伴遠端端點的使用者。

下列螢幕擷取畫面顯示已選取啟用基本身分驗證，以及建立已選擇的新秘密。做出這些選擇後，您可以輸入秘密的使用者名稱和密碼。

下列螢幕擷取畫面顯示已選取啟用基本身分驗證，以及選擇所選的現有秘密。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](#)。

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。在任何一種情況下，您的秘密都會存放在 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

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。這些登入資料必須符合連線至合作夥伴端點的使用者。

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.

ⓘ Note

當您在主控台中建立新的秘密時，秘密的名稱遵循此命名慣例：**/aws/transfer/*connector-id***，其中 *connector-id* 是您建立的連接器 ID。當您嘗試在其中尋找秘密時，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。

若要使用現有的秘密，請選擇選擇現有的秘密，然後從下拉式功能表中選擇秘密。如需在 Secrets Manager 中建立正確格式秘密的詳細資訊，請參閱 [在 中建立秘密 AWS Secrets Manager](#)。

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 HTTPS 時，才能使用基本身分驗證。

在 Secrets Manager for AS2 基本身分驗證中存放使用者登入資料

1. 登入 AWS 管理主控台，並在 <https://console.aws.amazon.com/secretsmanager/> 開啟 AWS Secrets Manager 主控台。
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. 在鍵/值對區段中，選擇鍵/值索引標籤。
 - 金鑰 – 輸入 **Username**。
 - value – 輸入獲授權連線至合作夥伴伺服器的使用者名稱。

6. 如果您想要提供密碼，請選擇新增資料列，然後在鍵/值對區段中，選擇鍵/值索引標籤。

選擇新增資料列，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，請選擇新增資料列，然後在金鑰/值對區段中，選擇金鑰/值索引標籤。

- 金鑰 – 輸入 **PrivateKey**。
- value – 輸入使用者的私有金鑰。此值必須以 OpenSSH 格式存放，且必須對應至遠端伺服器中為此使用者存放的公有金鑰。

8. 選擇下一步。

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，您可以將秘密命名為 **aws/transfer/connector-1**。

10. 選擇下一步，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，選擇存放以建立和存放秘密。

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 connector 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 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
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，在連接器的詳細資訊頁面上變更 AS2 連接器的屬性。

C- [redacted]

Delete

Connector configuration Info

Edit

Name

my-as2-connector

URL

<https://www.example.com>

Access role

[redacted]

Logging role

[AWSTransferLoggingAccess](#)

Communication settings Info

AS2-From header

[redacted]

AS2-To header

[redacted]

AS2 configuration Info

Edit

Local profile

[redacted]

Partner profile

[redacted]

Preserve S3 Content-Type

Enabled

Compression

Enabled

Message Subject

[View](#)

Encryption algorithm

AES128_CBC

Signing algorithm

SHA384

MDN configuration Info

Edit

Request MDN

Enabled

Signed MDN

Default to message signing algorithm: SHA384

Synchronization

Enabled

Basic authentication [Info](#)[Edit](#)**Basic authentication**
Enabled**Secret**
aws/transfer/c-**Egress IP details** [Info](#)

Service managed static IP addresses of this connector

 23.23.130.9 44.196.109.11 3.219.16.7**Tags (1)**[Manage tags](#)

Use tags to organize, search, and filter your Connectors. We recommend adding a tag with 'Name' as the key and a unique string as the value to easily identify your Connector.

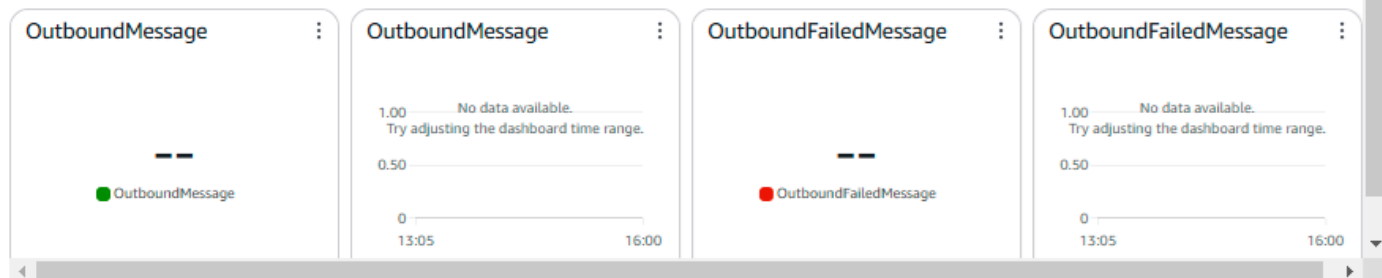
< 1 >

Key	Value
Name	my-as2-connector

AS2 Monitoring

3h 1d 1w

UTC timezone

**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 API 參考[DescribeConnector](#)中的。

傳送和接收 AS2 訊息

本節說明傳送和接收 AS2 訊息的程序。它也提供與 AS2 訊息相關聯的檔案名稱和位置的詳細資訊。

下表列出 AS2 訊息的可用加密演算法，以及何時可以使用它們。

加密演算法	HTTP	HTTPS	備註
AES128_CBC	Yes	Yes	
AES192_CBC	Yes	Yes	
AES256_CBC	Yes	Yes	
DES_EDE3_CBC	Yes	Yes	Only use this algorithm if you must support a legacy client that requires it, as it is a weak encryption algorithm.
NONE	No	Yes	If you are sending messages to a Transfer Family server, you can only select NONE if you are using an Application Load Balancer (ALB).

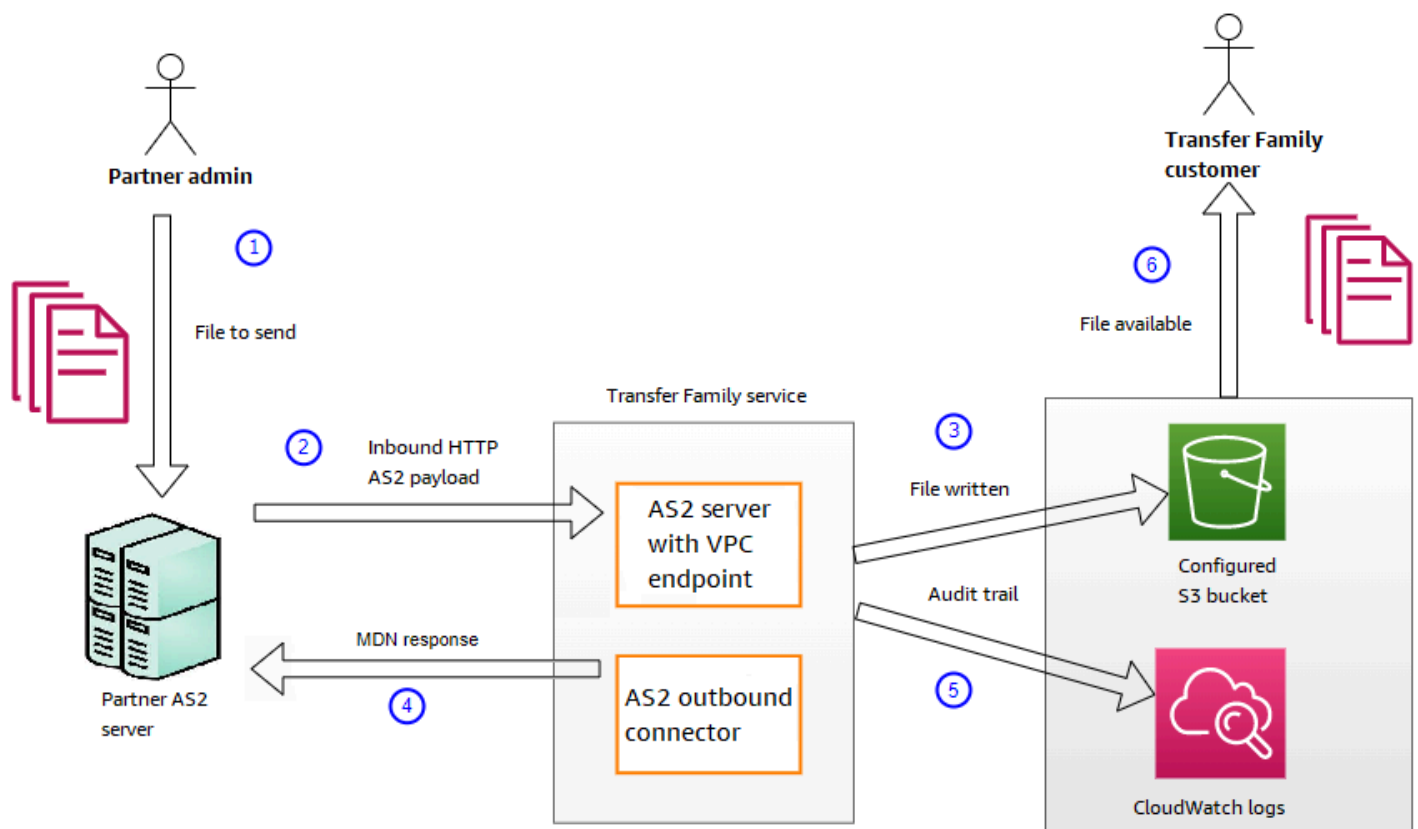
主題

- [接收 AS2 訊息程序](#)
- [透過 HTTPS 傳送和接收 AS2 訊息](#)
- [使用 AS2 連接器傳輸檔案](#)
- [檔案名稱和位置](#)
- [狀態碼](#)
- [範例 JSON 檔案](#)

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 HTTP POST 請求傳送至 Transfer Family 上託管的 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。檔案內容會存放在設定的 Amazon S3 檔案存放區中。
4. 已簽署的 MDN 回應會與 HTTP 回應內嵌傳回，或透過個別 HTTP POST 請求以非同步方式傳回原始伺服器。
5. 稽核線索會寫入 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。



透過 HTTPS 傳送和接收 AS2 訊息

本節說明如何設定 Transfer Family 伺服器，該伺服器使用 AS2 通訊協定透過 HTTPS 傳送和接收訊息。

主題

- [透過 HTTPS 傳送 AS2 訊息](#)

- [透過 HTTPS 接收 AS2 訊息](#)

透過 HTTPS 傳送 AS2 訊息

若要使用 HTTPS 傳送 AS2 訊息，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，選取任何可用的演算法。

Note

若要在不使用加密時傳送訊息至 Transfer Family 伺服器（亦即，您 NONE 為加密演算法選取），您必須使用 Application Load Balancer (ALB)。

- 提供連接器的剩餘值，如中所述[設定 AS2 連接器](#)。

透過 HTTPS 接收 AS2 訊息

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，在 Transfer Family 伺服器 VPC 端點之前終止網路或應用程式負載平衡器上的 TLS。透過此方法，您可以讓傳入的 AS2 訊息使用 HTTPS。

先決條件

- VPC 必須與 AWS 區域 Transfer Family 伺服器位於相同的 中。
- VPC 的子網路必須位於您要使用伺服器的可用區域內。

Note

每個 Transfer Family 伺服器最多可支援三個可用區域。

- 在與伺服器相同的區域中配置最多三個彈性 IP 地址。或者，您可以選擇使用自己的 IP 地址範圍 (BYOIP)。

Note

彈性 IP 地址的數量必須符合您搭配伺服器端點使用的可用區域數量。

您可以設定 Network Load Balance (NLB) 或 Application Load Balancer (ALB)。下表列出每種方法的優缺點。

下表提供當您使用 NLB 與 ALB 終止 TLS 時的功能差異。

功能	Network Load Balancer (NLB)	Application Load Balancer (ALB)
延遲	在網路層操作時降低延遲。	在應用程式層操作時延遲較高。
靜態 IP 支援	可以連接可以是靜態的彈性 IP 地址。	無法連接彈性 IP 地址：提供基礎 IP 地址可以變更的網域。
進階路由	不支援進階路由。	支援進階路由。無需加密即可注入 AS2 所需的 X-Forwarded-Proto 標頭。 此標頭說明於 https://developer.mozilla.org 網站上的 X-Forwarded-Proto 。
TLS/SSL 終止	支援 TLS/SSL 終止	支援 TLS/SSL 終止
交互 TLS (mTLS)	Transfer Family 目前不支援使用 NLB for mTLS	支援 mTLS

Configure NLB

此程序說明如何在 VPC 中設定面向網際網路的網路 Load Balancer (NLB)。

建立 Network Load Balancer 並將伺服器的 VPC 端點定義為負載平衡器的目標

1. 開啟位於 <https://console.aws.amazon.com/ec2/> 的 Amazon Elastic Compute Cloud 主控台。
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：
 - 在名稱中，輸入負載平衡器的描述性名稱。
 - 對於 Scheme (結構描述)，選擇 Internet-facing (面向網際網路)。
 - 針對 IP 地址類型，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，選擇與公有子網路相關聯的可用區域，這些子網路可在與伺服器端點搭配使用的相同 VPC 中使用。
 - 針對每個子網路的 IPv4 地址，選擇您配置的其中一個彈性 IP 地址。
6. 在接聽程式和轉接區段中，輸入下列資訊：
 - 針對通訊協定，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](#)。

建立目標群組之後，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 NLB。
9. (選用，但建議) 開啟 Network Load Balancer 的存取日誌，以維護完整的稽核線索，如 [Network Load Balancer 的存取日誌](#) 中所述。

我們建議您執行此步驟，因為 TLS 連線會在 NLB 終止。因此，Transfer Family 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。

Configure ALB

此程序說明如何在 VPC 中設定 Application Load Balancer (ALB)。

建立 Application Load Balancer 並將伺服器的 VPC 端點定義為負載平衡器的目標

1. 開啟位於 <https://console.aws.amazon.com/ec2/> 的 Amazon Elastic Compute Cloud 主控台。

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 Application Load Balancer (應用程式負載平衡器) 下，選擇 Create (建立)。
4. 在 ALB 主控台中，在連接埠 443 (HTTPS) 上建立新的 HTTP 接聽程式。
5. (選用)。如果您想要設定交互身分驗證 (mTLS)，請設定安全設定和信任存放區。
 - a. 將您的 SSL/TLS 憑證連接至接聽程式。
 - b. 在用戶端憑證處理下，選取相互身分驗證 (mTLS)。
 - c. 選擇使用信任存放區驗證。
 - d. 在進階 mTLS 設定下，透過上傳您的 CA 憑證來選擇或建立信任存放區。
6. 建立新的目標群組，並將 Transfer Family AS2 伺服器端點的私有 IP 地址新增為連接埠 5080 上的目標。如需建立新目標群組的詳細資訊，請參閱 [若要建立目標群組](#)。
7. 設定目標群組的運作狀態檢查，以在連接埠 5080 上使用 HTTP 通訊協定。
8. 建立新的規則，將 HTTPS 流量從接聽程式轉送到目標群組。
9. 設定接聽程式以使用您的 SSL/TLS 憑證。

設定負載平衡器之後，用戶端會透過自訂連接埠接聽程式與負載平衡器通訊。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. 在先前的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。
 - 針對選擇目標類型，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。
 - 對於通訊協定，您的選擇取決於您使用的是 ALB 還是 NLB。
 - 針對 Network Load Balancer (NLB)，選擇 TCP
 - 針對 Application Load Balancer (ALB)，選擇 HTTP
 - 針對連接埠，輸入 **5080**。
 - 針對 IP 地址類型，選擇 IPv4。
 - 針對 VPC，選擇您為 Transfer Family AS2 伺服器建立的 VPC。
3. 在運作狀態檢查區段中，選擇運作狀態檢查通訊協定。
 - 針對 ALB，選擇 HTTP

- 針對 NLB，選擇 TCP
4. 選擇下一步。
 5. 在註冊目標頁面上，輸入下列資訊：
 - 針對網路，請確認已指定您為 Transfer Family AS2 伺服器建立的 VPC。
 - 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，以新增另一列來輸入另一個 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**。
 - 選擇包含為以下待定項目，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，然後返回先前建立 NLB 的程序，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 的 DNS 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。若要疑難排解此問題，請檢查下列項目：

- 確認伺服器[端點相關聯的安全群組](#)允許從負載平衡器上設定的子網路傳入連線。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 透過參考連接器 ID 和檔案路徑來傳送 AS2 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 "/amzn-s3-demo-source-bucket/myfile1.txt" "/amzn-s3-demo-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 IDs、URLs 和 Amazon Resource Name (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 MDN 檔案，確認合作夥伴已成功收到檔案。這些檔案是根據中所述的慣例命名 [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。

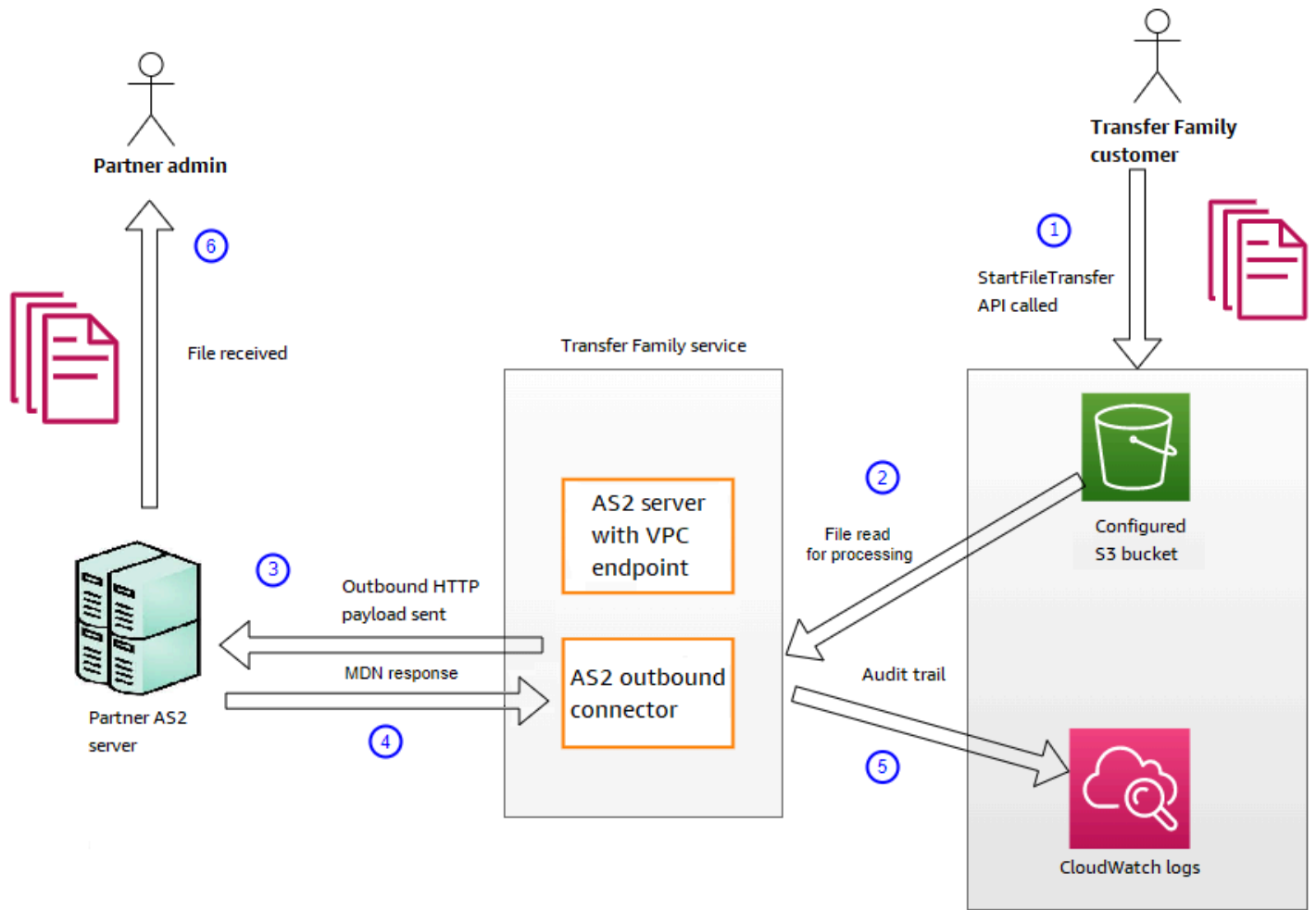
若要檢視 AS2 連接器詳細資訊，請參閱 [檢視 AS2 連接器詳細資訊](#)。如需建立 AS2 連接器的詳細資訊，請參閱 [設定 AS2 連接器](#)。

傳送 AS2 傳出訊息

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 `StartFileTransfer` API 操作。此操作會參考 `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 HTTP POST 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，可與 HTTP 回應（同步或非同步 MDN）內嵌。
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AS2-enabled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 組態](#)。

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。基礎目錄是結合字首的 Amazon S3 儲存貯體名稱，如果有的話。例如 `/amzn-s3-demo-bucket/AS2-folder`。
- 如果成功處理傳入檔案，檔案（和對應的 JSON 檔案）會儲存到 `/processed` 資料夾。例如 `/amzn-s3-demo-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檔案，檔案（和對應的 JSON 檔案）會儲存到 /failed 資料夾。例如 /amzn-s3-demo-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 會在原始副檔名之前附加到檔案名稱。
 - 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 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 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 –

ExampleFileInS3Payload.c4d6b6c7-23ea-4b8c-9ada-0cb811dc8b35@44313c54b0a46a36.

- JSON –

ExampleFileInS3Payload.c4d6b6c7-23ea-4b8c-9ada-0cb811dc8b35@44313c54b0a46a36.

- MDN –

ExampleFileInS3Payload.c4d6b6c7-23ea-4b8c-9ada-0cb811dc8b35@44313c54b0a46a36.

對於傳出傳輸，命名類似，差別在於沒有傳入訊息檔案，而且傳輸訊息的傳輸 ID 也會新增至檔案名稱。StartFileTransfer API 操作（或另一個程序或指令碼呼叫此操作時）會傳回傳輸 ID。

- 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 StartFileTransfer API 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 /amzn-s3-demo-bucket/AS2-folder/
file-to-send.txt
```

如果您執行此命令，則 MDN 和 JSON 檔案會儲存在 /amzn-s3-demo-bucket/AS2-folder/processed（傳輸成功）或 /amzn-s3-demo-bucket/AS2-folder/failed（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.j

- MDN – ExampleFileOutTestOutboundSyncMdn.dedf4601-4e90-4043-

b16b-579af35e0d83.fbe18db8-7361-42ff-8ab6-49ec1e435f34@c9c705f0baaaabaa.dat.m

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 AS2 訊息時，可以記錄到 CloudWatch 日誌的所有狀態碼。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，並顯示在 JSON 檔案中。

Code	Description	處理完成？
處理	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 (已完成)	訊息處理已成功完成。此狀態包括傳送 MDN 以進行傳入訊息或 MDN 驗證傳出訊息的時間。	是
失敗	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_OID to partner YourCompany",
  "requester-file-name": "TestOutboundSyncMdn-9lmCr79hV.dat",
  "as2-from": "MyCompany_OID",
  "connector-id": "c-c21c63ceaaf34d99b",
```

```
{
  "status-code": "COMPLETED",
  "disposition": "automatic-action/MDN-sent-automatically; processed",
  "transfer-size": 3198,
  "mdn-message-id": "OPENAS2-11072022063009+0000-df865189-1450-435b-9b8d-d8bc0cee97fd@PartnerA_OID_MyCompany_OID",
  "mdn-subject": "Message be18db8-7361-42ff-8ab6-49ec1e435f34@c9c705f0baaaabaa has been accepted",
  "as2-to": "PartnerA_OID",
  "transfer-id": "dedf4601-4e90-4043-b16b-579af35e0d83",
  "file-path": "/amzn-s3-demo-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": "/amzn-s3-demo-bucket-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"
}

```

自訂 AS2 訊息的 HTTP 標頭

傳送 AS2 訊息給交易合作夥伴時，您可能需要自訂 HTTP 標頭以符合特定需求，或增強與合作夥伴 AS2 伺服器組態的相容性。此 CloudFormation 範本會建立 基礎設施，為透過 傳送的 AS2 訊息啟用自訂 HTTP 標頭 AWS Transfer Family。它將 Amazon API Gateway 和 Lambda 函數設定為代理，允許動態修改交易合作夥伴的 AS2 伺服器所需的標頭。

使用此範本執行下列動作：

- 將自訂 HTTP 標頭新增至傳出 AS2 訊息
- 使用自訂值覆寫預設標頭值

Important

覆寫預設標頭值時請小心，因為這可能會導致傳送失敗：需要一些 AS2 標頭。

- 確保與具有特定標頭要求的交易合作夥伴相容

範本概觀

範本會建立下列主要元件：

- 處理和轉送 AS2 訊息的 Lambda 函數
- 公開 Lambda 函數的 Amazon API Gateway
- Lambda 函數的 IAM 角色和許可
- HTTPS 支援的條件式資源

範本檔案可在此處取得：[動態 HTTP 標頭範本](#)。

運作方式

1. Amazon API Gateway 接收來自 的傳入 AS2 訊息 AWS Transfer Family。
2. 請求會轉送至 Lambda 函數。
3. Lambda 函數會處理請求，並視需要新增或修改標頭。
4. 修改後的請求接著會轉送至合作夥伴的 AS2 伺服器。
5. 來自合作夥伴伺服器的回應會透過 Lambda 和 Amazon API Gateway 傳回至 AWS Transfer Family。

主要功能

- 動態標頭修改：允許自訂主旨標頭，並新增其他必要的標頭。
- 通訊協定支援：適用於 HTTP 和 HTTPS 通訊協定。

- 彈性組態：允許合作夥伴主機、連接埠和路徑的規格。

實作詳細資訊

範本會實作下列重要元件：

Lambda 功能

解決方案的核心是 Node.js Lambda 函數，可：

- 從 Amazon API Gateway 接收請求
- 根據組態和傳入請求資料修改標頭
- 將修改後的請求轉送至合作夥伴的 AS2 伺服器
- 同時處理 HTTP 和 HTTPS 通訊協定
- 包括錯誤處理和記錄

Amazon API Gateway

HTTP API 設定為：

- 接收傳入的 AS2 訊息
- 將請求路由至 Lambda 函數
- 將回應傳回至 AWS Transfer Family

範本參數

輸入範本參數的資訊，如下所示。請注意，所有這些參數都是字串。

- Environment：此參數用於命名範本建立的資源：無論是用於開發或生產環境。有效值為 dev 和 prod。
- PartnerHost：AS2 合作夥伴伺服器的 IP 地址或主機名稱。
- PartnerPort：AS2 合作夥伴伺服器的連接埠號碼。如果未指定，HTTP 預設為 80，HTTPS 預設為 443。
- PartnerPath：合作夥伴伺服器上 AS2 端點的路徑
- ProtocolType：用於 AS2 通訊的通訊協定：有效值為 HTTP 和 HTTPS。

條件式資源

對於 HTTPS 支援，範本會依條件建立：

- CA 憑證的 Lambda 層
- Lambda 函數中的 HTTPS 特定組態

部署和使用

使用 CloudFormation 範本自訂 AS2 HTTP 標頭

1. 在 <https://console.aws.amazon.com/cloudformation> 開啟 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，選擇選擇現有範本。
5. 複製此連結、[動態 HTTP 標頭範本](#)，並將其貼入 Amazon S3 URL 欄位。
6. 選擇下一步。
7. 將您的資訊填入參數詳細資訊。這些會在 [中](#) 詳細說明 [範本參數](#)。
8. 選擇下一步。在設定堆疊選項頁面上，再次選擇下一步。
9. 檢閱您正在建立之堆疊的詳細資訊，然後選擇建立堆疊。

Note

在頁面底部的功能下，您必須確認 CloudFormation 可能會建立 AWS Identity and Access Management (IAM) 資源。

部署此 CloudFormation 堆疊之後：

1. 請注意堆疊輸出中提供的 Amazon API Gateway 端點 URL。
2. 更新現有的 AWS Transfer Family Connector 以使用此新的 Amazon API Gateway 端點。
3. 解決方案現在將處理 AS2 訊息，並依設定新增或修改標頭。

⚠ Warning

僅修改您的合作夥伴明確預期的主旨標頭或新增標頭。變更其他標頭可能會導致傳輸失敗。

監控 AS2 用量

您可以使用 Amazon CloudWatch 和 監控 AS2 活動 AWS CloudTrail。若要檢視其他 Transfer Family 伺服器指標，請參閱 [AWS Transfer Family 伺服器 Amazon CloudWatch 記錄](#)

AS2 指標

指標	Description
InboundMessage	從交易合作夥伴成功接收的 AS2 訊息總數。 單位：Count 期間：5 分鐘
InboundFailedMessage	未成功從交易合作夥伴收到的 AS2 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：Count 期間：5 分鐘
OutboundMessage	從 Transfer Family 伺服器成功傳送至交易合作夥伴的 AS2 訊息總數。 單位：Count 期間：5 分鐘
OutboundFailedMessage	未成功傳送給交易合作夥伴的 AS2 訊息總數。 也就是說，它們是從 Transfer Family 伺服器傳送，但交易合作夥伴未成功收到。 單位：Count

指標	Description
	期間：5 分鐘
DaysUntilExpiry	憑證過期前的天數，由匯入時憑證上的 InactiveDate 設定決定。 單位：Count 維度：CertificateId 、 Description （如有提供） 期間：1 天 如需詳細資訊，請參閱 AS2 憑證輪換 。

AS2 狀態碼

下表列出當您或合作夥伴傳送 AS2 訊息時，可以記錄到 CloudWatch 日誌的所有狀態碼。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，並顯示在 JSON 檔案中。

Code	Description	處理完成？
處理	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 (已完成)	訊息處理已成功完成。此狀態包括傳送 MDN 以進行傳入訊息或 MDN 驗證傳出訊息的時間。	是

Code	Description	處理完成？
失敗	訊息處理失敗。如需錯誤代碼的清單，請參閱 AS2 錯誤代碼 。	是

AS2 錯誤代碼

下表列出並說明您可能會從 AS2 檔案傳輸收到的錯誤代碼。

AS2 錯誤代碼

Code	錯誤	描述和解析度
ACCESS_DENIED	- 存取遭拒。檢查您的存取角色是否具有必要的許可。 - 無效的檔案路徑 <i>send-file-path</i> - 無法使用 ErrorCode 取得登入資料：###	當處理任何 SendFilePaths 無效的 StartFile Transfer 請求或格式不正確時，便會發生。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。 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。	找不到協議，或協議與非作用中設定檔相關聯。 更新 Transfer Family 伺服器中的協議，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設定檔相關聯。

Code	錯誤	描述和解析度
		更新連接器以包含作用中設定檔。
CREDENTIALS_RETRIEVAL_FAILED	1. 在 Secrets Manager 中找不到秘密。 2. 無法存取 Secrets Manager。 3. 無法在 Secrets Manager 中解密秘密。 4. 由於限流，無法取得秘密值。	對於 AS2 基本身分驗證，秘密必須正確格式化。下列解析度對應於上一欄中列出的錯誤。 1. 確保秘密 ID 正確。 2. 確定存取角色具有讀取秘密的適當許可。存取角色必須提供對 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 。 3. 如果客戶受管金鑰用於秘密，請確保存取角色具有 AWS Key Management Service (AWS KMS) 金鑰的許可。 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。	傳送的檔案已損毀，或壓縮演算法無效。 重新傳送訊息並確認已使用 ZLIB 壓縮，或在未啟用壓縮的情況下重新傳送訊息。

Code	錯誤	描述和解析度
DECRYPT_FAILED	無法解密## <i>ID</i> 。確保合作夥伴擁有正確的公有加密金鑰。	解密失敗。 確認合作夥伴使用有效的憑證傳送承載，並使用有效的加密演算法執行加密。
DECRYPT_FAILED_INVALID_SMIME_FORMAT	無法剖析信封 mimePart。	MIME 承載已損毀或為不支援的 SMIME 格式。 寄件者應確保支援其使用的格式，然後重新傳送承載。
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，並確保其中包含有效的憑證。
DECRYPT_FAILED_UNSUPPORTED_ENCRYPTION_ALG	使用 ID 為 <i>encryption-ID</i> 的不支援演算法請求的 SMIME 承載解密。	遠端寄件者已使用不支援的加密演算法傳送 AS2 承載。 寄件者必須選擇 支援的加密演算法 AWS Transfer Family。
DUPLICATE_MESSAGE	重複或雙重處理的步驟。	承載具有重複的處理步驟。例如，有兩個加密步驟。 使用簽署、壓縮和加密的單一步驟來重新傳送訊息。

Code	錯誤	描述和解析度
ENCRYPT_FAILED_NO_ENCRYPTION_KEY_FOUND	在設定檔中找不到有效的公有加密憑證： <i>local-pro file-ID</i>	Transfer Family 正在嘗試加密傳出訊息，但找不到本機設定檔的加密憑證。 解析選項： • 確保本機設定檔已連接加密的憑證和私有金鑰。 • 確保加密憑證目前處於作用中狀態。
ENCRYPTION_FAILED	無法加密 <i>file-name</i> 。	要傳送的檔案不適用於加密。 確認檔案位於其預期的 AS2 位置，且 AWS Transfer Family 具有讀取檔案的許可。
FILE_SIZE_TOO_LARGE	檔案大小太大。	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	<i>partner-URL</i> 傳回 ID= <i>message-ID</i> 訊息的狀態 400。	與合作夥伴的 AS2 伺服器通訊會傳回非預期的 HTTP 回應碼。 合作夥伴可能可以透過 AS2 伺服器日誌提供更多診斷。
INSUFFICIENT_MESSAGE_SECURITY_UNENCRYPTED	需要加密。	合作夥伴將未加密的訊息傳送至不支援的 Transfer Family。寄件者必須使用加密的承載。
INVALID_ENDPOINT_PROTOCOL	僅支援 HTTP 和 HTTPS。	您必須將 HTTP 或 HTTPS 指定為 AS2 連接器組態中的通訊協定。

Code	錯誤	描述和解析度
INVALID_REQUEST	1. 訊息標頭發生問題。 2. 無法剖析秘密 JSON。 秘密 JSON 不符合預期的格式。 3. 秘密必須是 JSON 字串。 4. 使用者名稱不得包含冒號。 使用者名稱不得包含控制字元。 使用者名稱只能包含 ASCII 字元。 密碼不得包含控制字元。 密碼只能包含 ASCII 字元。	此錯誤有幾個原因。下列解析度對應於上一欄中列出的錯誤。 1. 檢查 as2-from 和 as2-to 欄位。請確定原始訊息 ID 對於 MDN 格式是準確的。此外，請確定訊息 ID 格式未遺漏任何 AS2 標頭。 2. 確保秘密值符合記錄的格式，如中所述啟用 AS2 連接器的基本身分驗證。 3. 確保秘密是以字串形式提供，而不是以二進位形式提供。 4. 對使用者名稱或密碼進行必要的更正。
INVALID_URL_FORMAT	URL 格式無效： <i>URL</i>	當您使用以格式不正確 URL 設定的連接器來傳送傳出訊息時，就會發生這種情況。 確定連接器已設定有效的 HTTP 或 HTTPS URL。
MDN_RESPONSE_INDICATES_AUTHENTICATION_FAILED	不適用	接收者無法驗證寄件者。交易合作夥伴會傳回 MDN 至 Transfer 系列， 其中包含處置修飾詞 錯誤：身分驗證失敗。
MDN_RESPONSE_INDICATES_DECOMPRESSION_FAILED	不適用	當接收者無法解壓縮訊息內容時，就會發生這種情況。交易合作夥伴會傳回 MDN 至 Transfer 系列， 其中包含處置修飾詞 錯誤：解壓縮失敗。

Code	錯誤	描述和解析度
MDN_RESPONSE_INDICATES_DECRYPTION_FAILED	不適用	接收者無法解密訊息內容。 交易合作夥伴會傳回 MDN 至 Transfer 系列， 其中包含處置修飾詞 錯誤：身分驗證失敗。
MDN_RESPONSE_INDICATES_INSUFFICIENT_MESSAGE_SECURITY	不適用	接收者預期訊息會經過簽署或加密，但不會。交易合作夥伴會傳回 MDN 以傳輸系列， 其中包含處置修飾詞 錯誤：insufficient-message-security。 在連接器上啟用簽署和/或加密，以符合交易合作夥伴的期望。
MDN_RESPONSE_INDICATES_INTEGRITY_CHECK_FAILED	不適用	接收者無法驗證內容完整性。 交易合作夥伴傳回 MDN 至 Transfer 系列， 其中包含處置修飾詞 錯誤：integrity-check-failed。
PATH_NOT_FOUND	無法建立目錄 <i>file-path</i> 。找不到父路徑。	Transfer Family 正在嘗試在客戶的 Amazon S3 儲存貯體中建立目錄，但找不到儲存貯體。 請確定StartFile Transfer 命令中提及的每個路徑都包含現有儲存貯體的名稱。

Code	錯誤	描述和解析度
SEND_FILE_NOT_FOUND	找不到檔案路徑 <i>file-path</i> 。	Transfer Family 在傳送檔案操作中找不到檔案。 檢查設定的主目錄和路徑是否有效，以及 Transfer Family 是否具有檔案的讀取許可。
SERVER_NOT_FOUND	找不到與訊息相關聯的伺服器。	Transfer Family 在接收訊息時找不到伺服器。如果在處理傳入訊息期間刪除伺服器，可能會發生這種情況。
SERVER_NOT_ONLINE	伺服器### ID 未上線。	Transfer Family 伺服器離線。 啟動伺服器，以便接收和處理訊息。
SIGNING_FAILED	無法簽署檔案。	要傳送的檔案無法用於簽署，或無法執行簽署。 確認檔案位於其預期的 AS2 位置，且 AWS Transfer Family 具有讀取檔案的許可。
SIGNING_FAILED_NO_SIGNING_KEY_FOUND	找不到設定檔的憑證： <i>local-profile-ID</i> 。	嘗試簽署傳出訊息，但找不到本機設定檔的簽署憑證。 解析選項： • 確保本機設定檔具有憑證和私有金鑰，用於連接簽署。 • 確定簽署憑證目前作用中。

Code	錯誤	描述和解析度
UNABLE_RESOLVE_HOST_TO_IP_ADDRESS	無法將主機名稱解析為 IP 地址。	Transfer Family 無法在 AS2 連接器中設定的公有 DNS 伺服器上執行 DNS 到 IP 地址解析。 更新連接器以指向有效的合作夥伴 URL。
UNABLE_TO_CONNECT_TO_REMOTE_HOST_OR_IP	與端點的連線逾時。	Transfer Family 無法建立與已設定合作夥伴 AS2 伺服器的通訊端連線。 檢查合作夥伴的 AS2 伺服器是否在設定的 IP 地址可用。
UNABLE_TO_RESOLVE_HOSTNAME	無法解析主機名稱####。	Transfer Family 伺服器無法使用公有 DNS 伺服器解析合作夥伴的主機名稱。 檢查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 ## ID 或 MIC 代碼不相符的簽章驗證失敗。	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 演算法是否與相容 AWS Transfer Family。

Code	錯誤	描述和解析度
VERIFICATION_FAILED_NO_MATCHING_KEY_FOUND	- 在設定檔中找不到符合訊息簽章的公有憑證：<i>partner-profile-ID</i>。 - 無法取得不存在設定檔的憑證：<i>partner-profile-ID</i>。 - 在設定檔中找不到有效的憑證：<i>partner-profile-ID</i>。	AWS Transfer Family 正在嘗試驗證所接收訊息的簽章，但合作夥伴設定檔找不到相符的簽署憑證。 解析選項： - 確定合作夥伴設定檔已連接簽署憑證。 - 確保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。

憑證過期監控

AWS Transfer Family 會自動監控 AS2 憑證的過期日期，並發佈 Amazon CloudWatch 指標，協助您追蹤憑證何時即將過期。這可讓您主動管理憑證續約，並避免服務中斷。

DaysUntilExpiry 指標

當您匯入憑證以供 AS2 使用時，Transfer Family 會自動建立名為 `DaysUntilExpiry` 的 CloudWatch 指標。此指標會根據 `InactiveDate` 您在匯入憑證時指定的，追蹤憑證過期之前剩餘的天數。

指標詳細資訊：

- 指標名稱：DaysUntilExpiry
- 命名空間：AWS/Transfer
- 維度：CertificateId (一律存在)、Description (如果在憑證匯入期間提供)
- 單位：計數 (天)
- 頻率：每日發佈

Important

匯入 Transfer Family 憑證後，最多可能需要一整天的時間，才能將此指標傳送到您的帳戶。

當憑證接近其非作用中日期時，指標值每天會減少 1。例如，如果憑證過期前有 30 天，指標會顯示 30 天，第二天會顯示 29 天，以此類推。

憑證監控的最佳實務

設定憑證過期監控時，請遵循下列最佳實務：

- 設定多個提醒閾值：建立不同時段（例如過期前 30 天、14 天和 7 天）的警示，以提供足夠的憑證續約時間。
- 使用適當的統計資料：建立警示時使用 Maximum 統計資料，以確保您擷取最新的指標值。
- 設定適當的警示動作：設定通知來提醒可以續約憑證的適當團隊成員。
- 測試您的提醒：定期測試您的通知系統，以確保提醒正確傳送。
- 記錄您的程序：維護憑證續約程序的文件，以及負責不同憑證的人員。

警示組態範例

以下是不同通知案例的一些警示組態範例：

30 天過期警告

建立警示，當憑證過期前有 30 天或更少時觸發：

- 指標：DaysUntilExpiry
- 統計資料：最大值
- 期間：1 天
- 閾值：30
- 比較：小於或等於閾值
- 缺少資料處理：將缺少的資料視為良好（未違反）

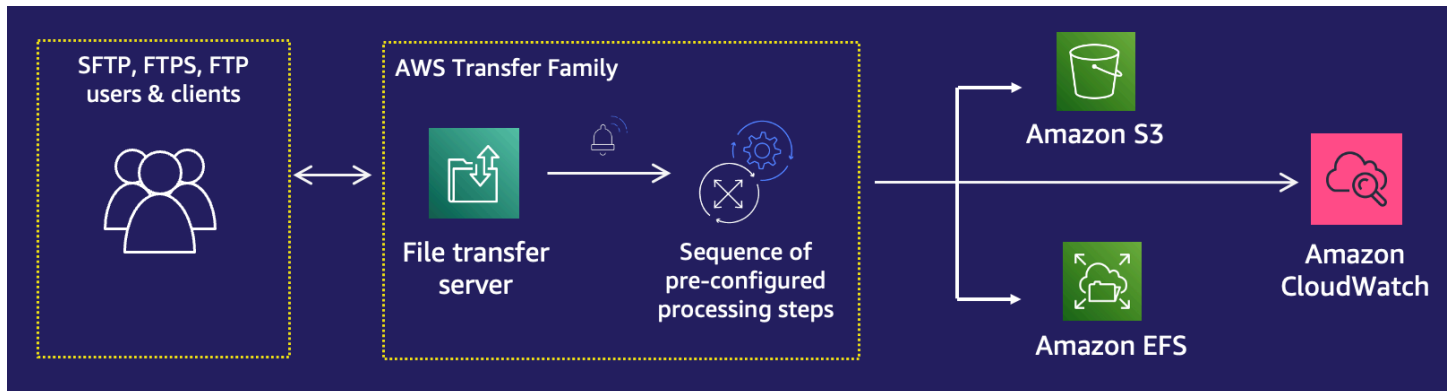
關鍵 7 天過期警告

建立關鍵警示，當憑證過期前有 7 天或更短時間時觸發：

- 指標：DaysUntilExpiry
- 統計資料：最大值
- 期間：1 天
- 閾值：7
- 比較：小於或等於閾值
- 缺少資料處理：將缺少的資料視為良好（未違反）

AWS Transfer Family 受管工作流程

AWS Transfer Family 支援 受管工作流程以進行檔案處理。透過 受管工作流程，您可以在檔案透過 SFTP、FTPS 或 FTP 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，以安全且經濟實惠的方式滿足您的business-to-business (B2B) 檔案交換合規要求。此外，您可以受益於end-to-end稽核和可見性。



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預先處理資料。這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即程式碼 (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歷程。

若要開始使用，請執行下列任務：

1. 設定您的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，供 Transfer Family 用來執行工作流程。如需詳細資訊，請參閱 [工作流程的 IAM 政策](#)。
3. 將工作流程映射到伺服器，以便在檔案送達時，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 伺服器的 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 CloudWatch 對工作流程相關錯誤進行故障診斷](#)。
- Transfer Family 提供部落格文章和研討會，引導您建置檔案傳輸解決方案。此解決方案利用 AWS Transfer Family 受管 SFTP/FTPS 端點和 Amazon Cognito 和 DynamoDB 進行使用者管理。

部落格文章可在[使用 Amazon Cognito 做為 AWS Transfer Family 和 Amazon S3 的身分提供者](#)取得。您可以在[此處](#)檢視研討會的詳細資訊。

- 檢視[AWS Transfer Family 受管工作流程](#)以取得 Transfer Family 工作流程的簡介。
- 以下研討會提供實作實驗室，以建置全自動化和事件驅動的工作流程，涉及將檔案傳輸到外部 SFTP 伺服器或從外部 SFTP 伺服器傳輸到 Amazon S3，以及這些檔案的常見前置和後置處理：[事件驅動的 MFT 研討會](#)。

此影片提供本研討會的逐步解說。

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](#)
- [工作流程的 IAM 政策](#)
- [工作流程的例外狀況處理](#)
- [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 受管工作流程入門的更多說明，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 管理主控台，如本主題所述。為了讓工作流程建立程序盡可能簡單，主控台的大多數區段都可以使用情境說明面板。

工作流程有兩種步驟：

- 名義步驟 – 名義步驟是您想要套用至傳入檔案的檔案處理步驟。如果您選擇多個名目步驟，則每個步驟都會以線性順序處理。
- 例外狀況處理步驟 – 例外狀況處理常式是在任何名目步驟失敗或導致驗證錯誤時 AWS Transfer Family 執行的檔案處理步驟。

建立工作流程

1. 在 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
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。此描述會出現在工作流程頁面上。
5. 在名義步驟區段中，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. 選擇下一步，然後設定步驟的參數。
 - c. 選擇下一步，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. 新增所有必要的名目步驟後，向下捲動至例外處理常式 – 選用區段，然後選擇新增步驟。

Note

為了讓您即時收到失敗的通知，建議您設定例外狀況處理常式，以及在工作流程失敗時執行的步驟。

- 若要設定例外狀況處理常式，請以先前所述的相同方式新增步驟。如果檔案導致任何步驟擲回例外狀況，則會逐一叫用例外狀況處理常式。
- (選用) 向下捲動至標籤區段，並為您的工作流程新增標籤。
- 檢閱組態，然後選擇建立工作流程。

Important

建立工作流程之後，您無法編輯它，因此請務必仔細檢閱組態。

設定和執行工作流程

您必須先將工作流程與 Transfer Family 伺服器建立關聯，才能執行工作流程。

設定 Transfer Family 在上傳的檔案上執行工作流程

- 在 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
- 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其中。如需詳細資訊，請參閱[設定 SFTP、FTPS 或 FTP 伺服器端點](#)。
- 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，將工作流程與所選伺服器建立關聯。

- 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。

- 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[工作流程的 IAM 政策](#)。選擇 Save (儲存)。

The screenshot displays the 'Managed workflows' section of the AWS Transfer Family console. It includes three main configuration areas: 'Workflow for complete file uploads', 'Workflow for partial file uploads', and 'Managed workflows execution role'. Each area has a dropdown menu for selecting a workflow, a refresh button, and a 'Create a new Workflow' link. The 'Managed workflows execution role' section has a dropdown menu and a refresh button.

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]

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，您必須等待大約 10 分鐘，才能執行新的工作流程。Transfer Family 伺服器會快取工作流程詳細資訊，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的 SFTP 工作階段，然後在 10 分鐘的等待期間之後重新登入，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 /amzn-s3-demo-bucket/home/users/bob/doc1.pdf
doc1.pdf                                     100% 5013KB
 601.0KB/s   00:08
sftp> exit
>
```

上傳檔案後，定義的動作會在您的檔案上執行。例如，如果您的工作流程包含複製步驟，檔案會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

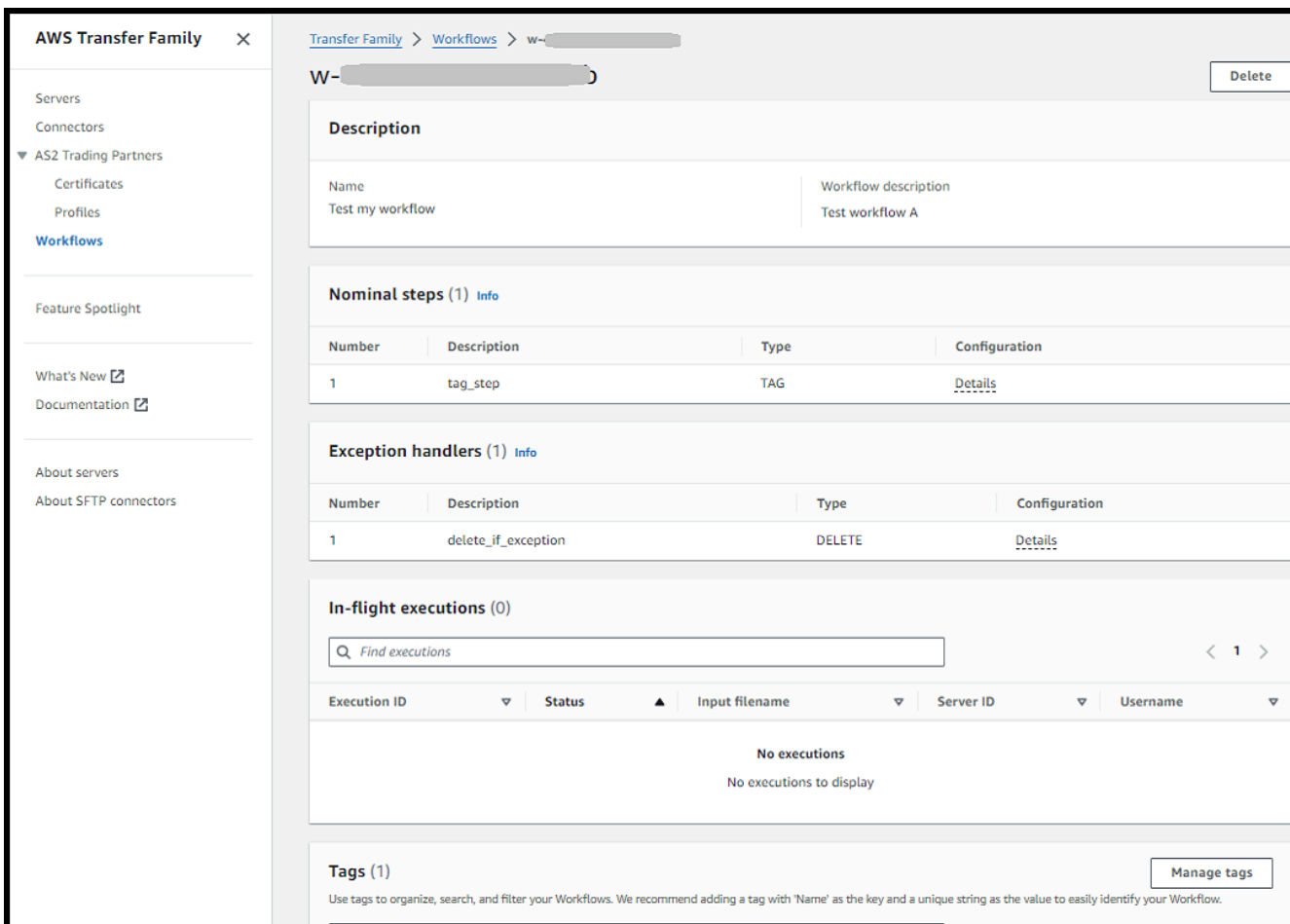
您可以檢視先前建立的工作流程或工作流程執行的詳細資訊。若要檢視這些詳細資訊，您可以使用 主控台或 AWS Command Line Interface (AWS CLI)。

Console

檢視工作流程詳細資訊

1. 在 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
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": "amzn-s3-demo-bucket",
              "Key": "home/shared_files/"
            }
          }
        },
        "OnException": {}
      ],
    }
  }
}
```

如果您的工作流程是建立為 AWS CloudFormation 堆疊的一部分，您可以使用 CloudFormation 主控台 (<https://console.aws.amazon.com/cloudformation> : //) 來管理工作流程。

Transfer Family > Workflows > w-

W-

Delete

This workflow belongs to the AWS CloudFormation stack **stack-transfer-notifications-blog**. [Manage this stack](#) on the CloudFormation console.

Description

Name

Stack-managed

Workflow description

Workflow for blogpost

Nominal steps (4) [Info](#)

Number	Description	Type	Configuration
1	Lambda	CUSTOM	Details
2	CopyFile	COPY	Details
3	TagFileNotified	TAG	Details
4	DeleteOriginalSourceFile	DELETE	Details

使用預先定義的步驟

當您建立工作流程時，您可以選擇新增下列其中一個本主題中討論的預先定義步驟。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副本。目前，您只能搭配 Amazon S3 使用複製檔案步驟。

下列複製檔案步驟會將檔案複製到 *amzn-s3-demo-destination-bucket* 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。您可以使用此功能來製作原始檔案的多個副本，同時保持來源檔案完整，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

您必須提供複製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。是否將金鑰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，且其名稱不會變更。如果最後一個字元是英數字元，您上傳的檔案會重新命名為金鑰值。在這種情況下，如果具有該名稱的檔案已存在，則行為取決於覆寫現有欄位的設定。

- 如果選取覆寫現有檔案，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，且工作流程處理會停止。

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/`，您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 `today test` 資料夾中名為 `test` 的檔案，而每個後續檔案都會覆寫先前的檔案。

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。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特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 `amzn-s3-demo-destination-bucket/richard-roe/processed/` 資料夾。如果使用者 `mary-major` 上傳檔案，則會將其複製到 `amzn-s3-demo-destination-bucket/mary-major/processed/` 資料夾。

Configure parameters

Configure copy parameters

Step name

dynamic-copy

Destination bucket name

amzn-s3-demo-destination-bucket ▼

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 `${transfer:UploadDate}` 做為變數，將檔案複製到目前日期名為 的目的地位置。在下列範例中，如果您在 2022 年 2 月 1 `${transfer:UploadDate}/processed` 日將目的地設定為 `amzn-s3-demo-destination-bucket/2022-02-01/processed/` 資料夾。

Configure copy parameters

Step name

dynamic-copy-date

Destination bucket name

amzn-s3-demo-destination-bucket ▼

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

您也可以結合這兩個變數的功能。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/`。

複製步驟的 IAM 許可

若要允許複製步驟成功，請確定工作流程的執行角色包含下列許可。

```
{
  "Sid": "ListBucket",
  "Effect": "Allow",
  "Action": "s3:ListBucket",
  "Resource": [
    "arn:aws:s3:::amzn-s3-demo-destination-bucket"
  ]
}, {
  "Sid": "HomeDirObjectAccess",
  "Effect": "Allow",
  "Action": [
```

```
    "s3:PutObject",
    "s3:GetObject",
    "s3:DeleteObjectVersion",
    "s3:DeleteObject",
    "s3:GetObjectVersion"
  ],
  "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
}
```

Note

只有在您未選取覆寫現時，才需要 `s3:ListBucket` 許可。此許可會檢查您的儲存貯體，以查看是否有同名的檔案已存在。如果您已選取覆寫現有檔案，則工作流程不需要檢查檔案，而且只能寫入檔案。

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` 針對未進行版本控制的 Amazon S3 檔案新增。
- `s3:GetObjectVersionTagging` 為版本控制的 Amazon S3 檔案新增。

解密檔案

AWS 儲存部落格有一篇文章，說明如何簡單地解密檔案，而無需使用 Transfer Family Managed 工作流程撰寫任何程式碼、[使用 PGP 和 加密和解密檔案 AWS Transfer Family](#)。

支援的對稱加密演算法

對於 PGP 解密，Transfer Family 支援對稱加密演算法，這些演算法用於加密 PGP 檔案中的實際檔案資料。

- 如需支援對稱加密演算法的詳細資訊，請參閱 [PGP 對稱加密演算法](#)。
- 如需有關搭配這些對稱演算法使用的 PGP 金鑰對演算法的資訊，請參閱 [PGP 金鑰對演算法](#)。

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 FTP 上傳到 Amazon Simple Storage Service (Amazon S3) 或 Amazon Elastic File System (Amazon EFS) 的檔案上使用 PGP 解密。

若要使用 PGP 解密，您必須建立和存放用於檔案解密的 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](#)。

如需支援的 PGP 演算法和建議的相關資訊，請參閱 [PGP 加密和解密演算法](#)。

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 以正確的秘密名稱存放在 中。
2. 將您的 PGP 金鑰存放在所需的秘密名稱 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 中的秘密名稱，自動找到要用於解密的正確 PGP 金鑰。

Note

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

3. 使用您的 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，請將 `username@example.com` 取代為您用來建立 PGP 金鑰對的電子郵件地址。`testfile.txt` 將取代為您要加密的檔案名稱。

```
gpg -e -r username@example.com testfile.txt
```

Important

加密檔案以搭配 AWS Transfer Family 工作流程使用時，請務必使用 `-r` 參數來指定非匿名收件人。匿名加密（未指定收件人）可能會導致工作流程中的解密失敗，因為系統無法識別要用於解密的金鑰。此問題的偵錯資訊可在取得[對匿名收件人加密問題進行故障診斷](#)。

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

解密步驟會解密在工作流程中上傳至 Amazon S3 或 Amazon EFS 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 CloudWatch Logs 監控解密工作流程結果，並即時取得每個檔案的稽核日誌。

選擇步驟的 Decrypt 檔案類型後，即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 檔案系統做為解密檔案的目的地。
- 如果您選擇 Amazon S3，則必須提供目的地儲存貯體名稱和目的地金鑰字首。若要依使用者名稱參數化目的地金鑰字首，請在目的地金鑰字首中輸入 `${transfer:UserName}`。同樣地，若要依上傳日期參數化目的地金鑰字首，請在目的地金鑰字首輸入 `${Transfer:UploadDate}`。
- 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，且工作流程處理會停止。

 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能會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.

解密步驟的 IAM 許可

若要允許解密步驟成功，請確定工作流程的執行角色包含下列許可。

```
{
  "Sid": "ListBucket",
  "Effect": "Allow",
  "Action": "s3:ListBucket",
  "Resource": [
    "arn:aws:s3:::amzn-s3-demo-destination-bucket"
  ]
}, {
  "Sid": "HomeDirObjectAccess",
  "Effect": "Allow",
  "Action": [
    "s3:PutObject",
    "s3:GetObject",
    "s3:DeleteObjectVersion",
    "s3:DeleteObject",
    "s3:GetObjectVersion"
  ],
  "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
}, {
  "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 `s3:ListBucket` 許可。此許可會檢查您的儲存貯體，以查看是否有同名的檔案已存在。如果您已選取覆寫現有檔案，則工作流程不需要檢查檔案，而且只能寫入檔案。

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` 針對未進行版本控制的 Amazon S3 檔案新增。
- `s3:GetObjectVersionTagging` 為版本控制的 Amazon S3 檔案新增。

標籤檔案

若要標記傳入檔案以供進一步下游處理，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 伺服器儲存體時，才支援標籤操作。

下列範例標籤步驟會分別指派 `scan_outcome` 和 `clean` 做為標籤索引鍵和值。

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

若要允許標籤步驟成功，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:::amzn-s3-demo-bucket/*"
    ]
}
```

Note

如果您的工作流程包含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` 針對未進行版本控制的 Amazon S3 檔案新增。
- `s3:GetObjectVersionTagging` 為版本控制的 Amazon S3 檔案新增。

刪除檔案

若要從先前的工作流程步驟中刪除已處理的檔案，或刪除最初上傳的檔案，請使用刪除檔案步驟。

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。

- 使用 根據上傳檔案的使用者`${transfer:UserName}`，將檔案複製或解密至目的地。
- 使用 根據目前日期`${transfer:UploadDate}`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

下列範例說明的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。標記傳入檔案之後，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 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
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. 在名義步驟區段中，選擇新增步驟。
 - b. 選擇複製檔案，然後選擇下一步。
 - c. 輸入步驟名稱，然後選取目的地儲存貯體和金鑰字首。

Step 1
Choose step type

Step 2
Configure parameters

Step 3
Review and create

Configure parameters

Configure copy parameters

Step name
copy-step-first-step

Destination bucket name
example-bucket ▼

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.
test/

☐ Overwrite existing

- d. 選擇下一步，然後檢閱步驟的詳細資訊。
 - e. 選擇建立步驟來新增步驟並繼續。
6. 新增第二個步驟（標籤）。
- a. 在名義步驟區段中，選擇新增步驟。
 - b. 選擇標籤檔案，然後選擇下一步。
 - c. 輸入步驟名稱。
 - d. 針對檔案位置，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. 選擇下一步，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. 在名義步驟區段中，選擇新增步驟。
 - b. 選擇刪除檔案，然後選擇下一步。

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. 針對檔案位置，選取刪除原始來源檔案。
 - e. 選擇下一步，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": "amzn-s3-demo-bucket",
          "Key": "test/"
        }
      }
    }
  },
  {
    "Type": "TAG",
    "TagStepDetails": {
      "Name": "TagStep",
      "Tags": [
        {
          "Key": "name",
          "Value": "demo"
        }
      ],
      "SourceFileLocation": "${previous.file}"
    }
  },
  {
    "Type": "DELETE",
    "DeleteStepDetails": {
```



```

        "Name": "DeleteStep",
        "SourceFileLocation": "${original.file}"
    }
}
]

```

第一個步驟會將上傳的檔案複製到新的 Amazon S3 位置。第二個步驟會將標籤（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. 更新現有的伺服器。

Note

此步驟假設您已經有 Transfer Family 伺服器，而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，您可以使用使用自有檔案處理邏輯 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範例 Lambda 函數](#)。如需範例事件（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 函數來呼叫 [SendWorkflowStepState](#) API 操作。會 SendWorkflowStepState 通知工作流程執行，該步驟已完成，包括成功或失敗狀態。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名目步驟。

如果 Lambda 函數失敗或逾時，則步驟會失敗，而您會在 CloudWatch 日誌 StepErrored 中看到。如果 Lambda 函數是名目步驟的一部分，且函數 SendWorkflowStepState 以 Status="FAILURE" 或逾時回應，則流程會繼續執行例外處理常式步驟。在此情況下，工作流程不會繼續執行剩餘的（如果有的話）標稱步驟。如需詳細資訊，請參閱 [工作流程的例外狀況處理](#)。

當您呼叫 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 Lambda ExecutionId 函數執行時傳遞的 WorkflowId 輸入事件中擷取 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 SendWorkflowStepState API 操作，您必須使用 [推出受管工作流程](#) 之後發佈的 AWS SDK 版本。

連續使用多個 Lambda 函數

當您依序使用多個自訂步驟時，檔案位置選項的運作方式會與只使用單一自訂步驟不同。Transfer Family 不支援傳遞 Lambda 處理的檔案，以用作下一個步驟的輸入。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），previous.file 則設定的運作方式也不同。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自訂步驟所使用的相同輸入檔案。來自自訂步驟的已處理檔案不會傳遞至預先定義的步驟。

在自訂處理之後存取檔案

如果您使用 Amazon S3 做為儲存體，而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 `example-file.txt` 的檔案。
- 步驟 2 – 叫用 `example-file.txt` 以某種方式變更的 Lambda 函數。
- 步驟 3 – 嘗試對更新版本的 `example-file.txt` 執行進一步處理。

如果您將步驟 3 `sourceFileLocation` 的設定為 `${original.file}`，步驟 3 會使用在步驟 1 中將檔案上傳至儲存體時來自的原始檔案位置。如果您使用 `${previous.file}` 進行步驟 3，步驟 3 會重複使用步驟 2 用作輸入的檔案位置。

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` 使其不符合原始檔案。

Note

如果您使用 Amazon EFS，則不會發生此行為，因為 Amazon EFS 不會使用實體標籤來識別檔案。

檔案上傳 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": "amzn-s3-demo-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範例 Lambda 函數

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)
    }
```

自訂步驟的 IAM 許可

若要允許呼叫 Lambda 的步驟成功，請確定工作流程的執行角色包含下列許可。

```
{
  "Sid": "Custom",
  "Effect": "Allow",
  "Action": [
    "lambda:InvokeFunction"
  ],
  "Resource": [
    "arn:aws:lambda:region:account-id:function:function-name"
  ]
}
```

工作流程的 IAM 政策

當您將工作流程新增至伺服器時，您必須選取執行角色。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。

本節說明一組可用於執行工作流程的 AWS Identity and Access Management (IAM) 許可。本主題稍後將說明其他範例。

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` 針對未進行版本控制的 Amazon S3 檔案新增。
- `s3:GetObjectVersionTagging` 為版本控制的 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 受管政策新增至 `AWSTransferFullAccess` 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，並將其連接到您的角色。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:::amzn-s3-demo-bucket"
    ]
  },
  {
    "Sid": "AllObjectActions",
    "Effect": "Allow",
    "Action": "s3:*Object",
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket/*"
    ]
  },
  {
    "Sid": "GetObjectVersion",
    "Effect": "Allow",
    "Action": "s3:GetObjectVersion",
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket/*"
    ]
  },
  {
    "Sid": "Custom",
    "Effect": "Allow",
    "Action": [
      "lambda:InvokeFunction"
    ],
    "Resource": [
      "arn:aws:lambda:us-east-1:123456789012:function:function-name"
    ]
  },
  {
    "Sid": "Tag",

```



```

        "Effect": "Allow",
        "Action": [
            "s3:PutObjectTagging",
            "s3:PutObjectVersionTagging"
        ],
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket/*"
        ]
    }
}

```

3. 當您將工作流程新增至伺服器時，請儲存此角色並將其指定為執行角色。

Note

當您建構 IAM 角色時，AWS 建議您盡可能限制對資源的存取工作流程。

工作流程信任關係

工作流程執行角色也需要與 `transfer.amazonaws.com` 建立信任關係。若要建立的信任關係 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人問題。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:::amzn-s3-demo-source-bucket/*"
},
{
    "Sid": "CopyWrite",
    "Effect": "Allow",
    "Action": [
        "s3:PutObject",
        "s3:PutObjectTagging"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
},
{
    "Sid": "CopyList",
    "Effect": "Allow",
    "Action": "s3:ListBucket",
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-source-bucket",
        "arn:aws:s3:::amzn-s3-demo-destination-bucket"
    ]
},
{
    "Sid": "Tag",
    "Effect": "Allow",
    "Action": [
        "s3:PutObjectTagging",
        "s3:PutObjectVersionTagging"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*",
    "Condition": {
        "StringEquals": {
            "s3:RequestObjectTag/Archive": "yes"
        }
    }
},
{
    "Sid": "ListBucket",
    "Effect": "Allow",
    "Action": "s3:ListBucket",
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-destination-bucket"
    ]
},

```

```

    {
      "Sid": "HomeDirObjectAccess",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObjectVersion",
        "s3:DeleteObject",
        "s3:GetObjectVersion"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    },
    {
      "Sid": "Decrypt",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": "arn:aws:secretsmanager:us-east-1:123456789012:secret:aws/transfer/*"
    }
  ]
}

```

範例執行角色：執行 函數並刪除

在此範例中，您有一個叫用 AWS Lambda 函數的工作流程。如果工作流程刪除上傳的檔案，並具有例外處理常式步驟來處理上一個步驟中失敗的工作流程執行，請使用下列 IAM 政策。將每個 *user input placeholder* 替換成您自己的資訊。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Delete",
      "Effect": "Allow",
      "Action": [
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::bucket-name"
    }
  ]
}

```

```
    },  
    {  
      "Sid": "Custom",  
      "Effect": "Allow",  
      "Action": [  
        "lambda:InvokeFunction"  
      ],  
      "Resource": [  
        "arn:aws:lambda:us-east-1:123456789012:function:function-name"  
      ]  
    }  
  ]  
}
```

工作流程的例外狀況處理

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狀況處理步驟。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，假設您已在名目步驟中設定自訂處理，以驗證傳入的檔案。如果檔案驗證失敗，例外狀況處理步驟可以傳送電子郵件給管理員。

下列範例工作流程包含兩個步驟：

- 檢查上傳檔案是否為 CSV 格式的名目步驟
- 例外狀況處理步驟，可傳送電子郵件，以防上傳的檔案不是 CSV 格式，且名目步驟失敗

若要啟動例外狀況處理步驟，名目步驟中的 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

Name
Delete after upload

Workflow description
test-my-workflow

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 CloudWatch AWS 雲端 會即時監控您在 中執行 AWS 的資源和應用程式。您可以使用 Amazon CloudWatch 來收集和追蹤指標，這是您可以為工作流程測量的變數。您可以使用 Amazon CloudWatch 檢視工作流程指標和合併日誌。

工作流程的 CloudWatch 記錄

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 logs

1. 在 <https://console.aws.amazon.com/cloudwatch/> 開啟 Amazon CloudWatch 主控台。
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. 選擇對應至您伺服器的日誌群組。

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。
- 一個用於為您的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 位數英數識別符是虛構的。您在 Amazon CloudWatch 中看到的值不同。

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。

以下是的範例日誌串流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": "amzn-s3-demo-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": "amzn-s3-demo-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"
}
}
```

工作流程的 CloudWatch 指標

AWS Transfer Family 為工作流程提供數個指標。您可以檢視前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 指標如 中所述[使用 Transfer Family 伺服器的 CloudWatch 指標](#)。

從範本建立工作流程

您可以部署從範本建立工作流程和伺服器的 CloudFormation 堆疊。此程序包含您可以用來快速部署工作流程的範例。

建立建立 AWS Transfer Family 工作流程和伺服器的 CloudFormation 堆疊

1. 在 <https://console.aws.amazon.com/cloudformation> 開啟 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"
      }
    ]
  }
}
}
}

```

3. 將下列項目取代為您的實際值。

- 將 *workflow-execution-role-arn* 取代為具有實際工作流程執行角色的 ARN。例如 `arn:aws:transfer:us-east-2:111122223333:workflow/w-1234567890abcdef0`
- `arn:aws:lambda:region:account-id:function:function-name` 將取代為 Lambda 函數的 ARN。例如 `arn:aws:lambda:us-east-2:123456789012:function:example-lambda-idp`。

4. 遵循 AWS CloudFormation 《使用者指南》中的 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。範本會建立新的 AWS Transfer Family SFTP 伺服器，使用服務受管使用者和新的工作流程，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執行此操作。

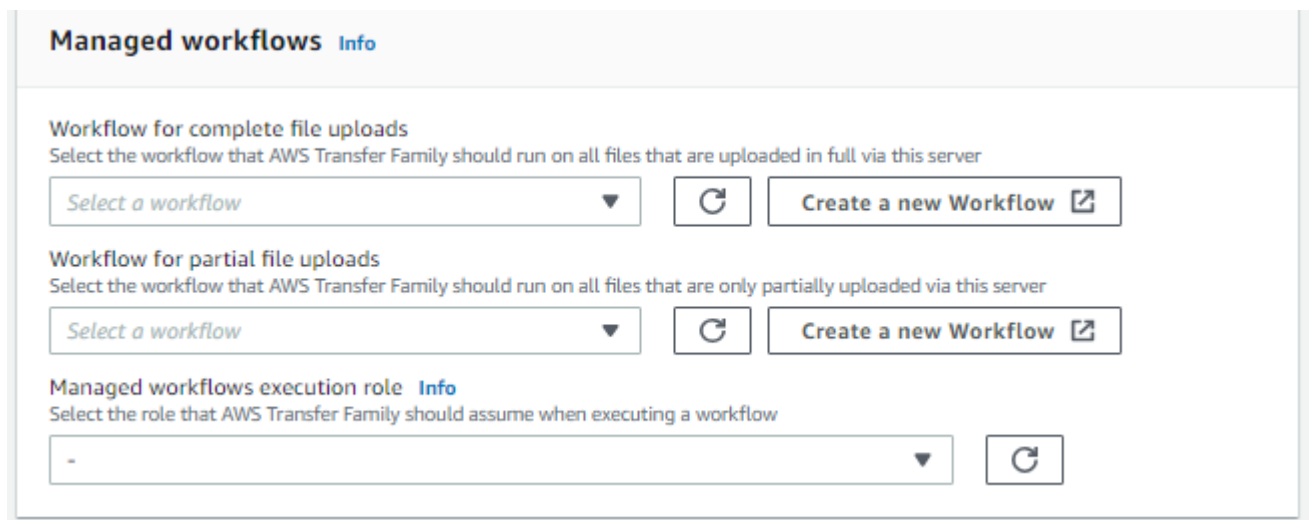
Console

從 Transfer Family 伺服器移除工作流程

1. 在 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
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，請從工作流程清單中選取破折號 (-)，以進行部分檔案上傳。
 - 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，請向上捲動直到看到它，因為它是每個選單中的第一個值。

畫面看起來應該如下所示。



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

Select a workflow ▼  [Create a new Workflow](#) 

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

Select a workflow ▼  [Create a new Workflow](#) 

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

- ▼ 

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 以您伺服器的 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，您可以跨帳戶複製，前提是您的 AWS Identity and Access Management (IAM) 政策已正確設定。
- 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的區域。
- 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。
- 自訂步驟逾時為近似值。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。
- 您可以將檔案處理工作流程連接至使用 AS2 通訊協定的 Transfer Family 伺服器：不過，AS2 訊息不會執行連接到伺服器的工作流程。

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。
- 每個使用者每個 Transfer Family 伺服器最多可以存放 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 且重新填充速率為 1 的 [字符儲存貯](#) 體系統來調節新的執行速率。
- 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，您必須等待大約 10 分鐘，才能執行新的工作流程。Transfer Family 伺服器會快取工作流程詳細資訊，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的 SFTP 工作階段，然後在 10 分鐘的等待期間之後重新登入，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，以及如何為啟用 SFTP 的伺服器變更主機金鑰的相關資訊。

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](#)
- [Transfer Family 伺服器的 IPv6 支援](#)
- [編輯伺服器詳細資訊](#)
- [編輯身分提供者組態](#)
- [管理已啟用 SFTP 的伺服器的主機金鑰](#)
- [在 主控台中監控用量](#)

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 區域中所有伺服器的清單。

尋找存在於 區域中的伺服器清單 AWS

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

如果您在目前區域中有一或多個伺服器 AWS，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 AWS Amazon S3 儲存貯體權限的使用者仍可存取。

Console

使用主控台刪除伺服器

1. 在 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
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刪除，您不會再支付該伺服器的費用。

AWS CLI

使用 CLI 刪除伺服器

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 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
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。對於 AS2 伺服器，請參閱 [檢視 AS2 伺服器詳細資訊](#)。

Protocols

[Edit](#)

Protocols over which clients can connect to your server's endpoint

- SFTP

Identity provider

[Edit](#)

Identity provider type
Service managed

Note

伺服器主機金鑰 描述和日期 匯入值自 2022 年 9 月起為新值。引進這些值以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設定為伺服器的上次修改日期。也就是說，您為遷移的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，可讓您輕鬆地將其識別為已遷移。

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您伺服器的 區域。

Additional details Edit

Log group /aws/transfer/s-	Domain Amazon S3	SetStat option Ignore
Logging role Info -	Login display banner View the display message	TLS session resumption -
Security Policy Info TransferSecurityPolicy-PQ-SSH-Experimental-2023-04	Optimized directories Info ENABLED	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 MDN 輸出 IP 地址。

Protocols Edit

Protocols over which clients can connect to your server's endpoint

- AS2

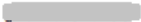
Identity provider Edit

 **AS2 Auth**
Basic authentication is not supported for AS2. Access can be controlled through VPC security groups.

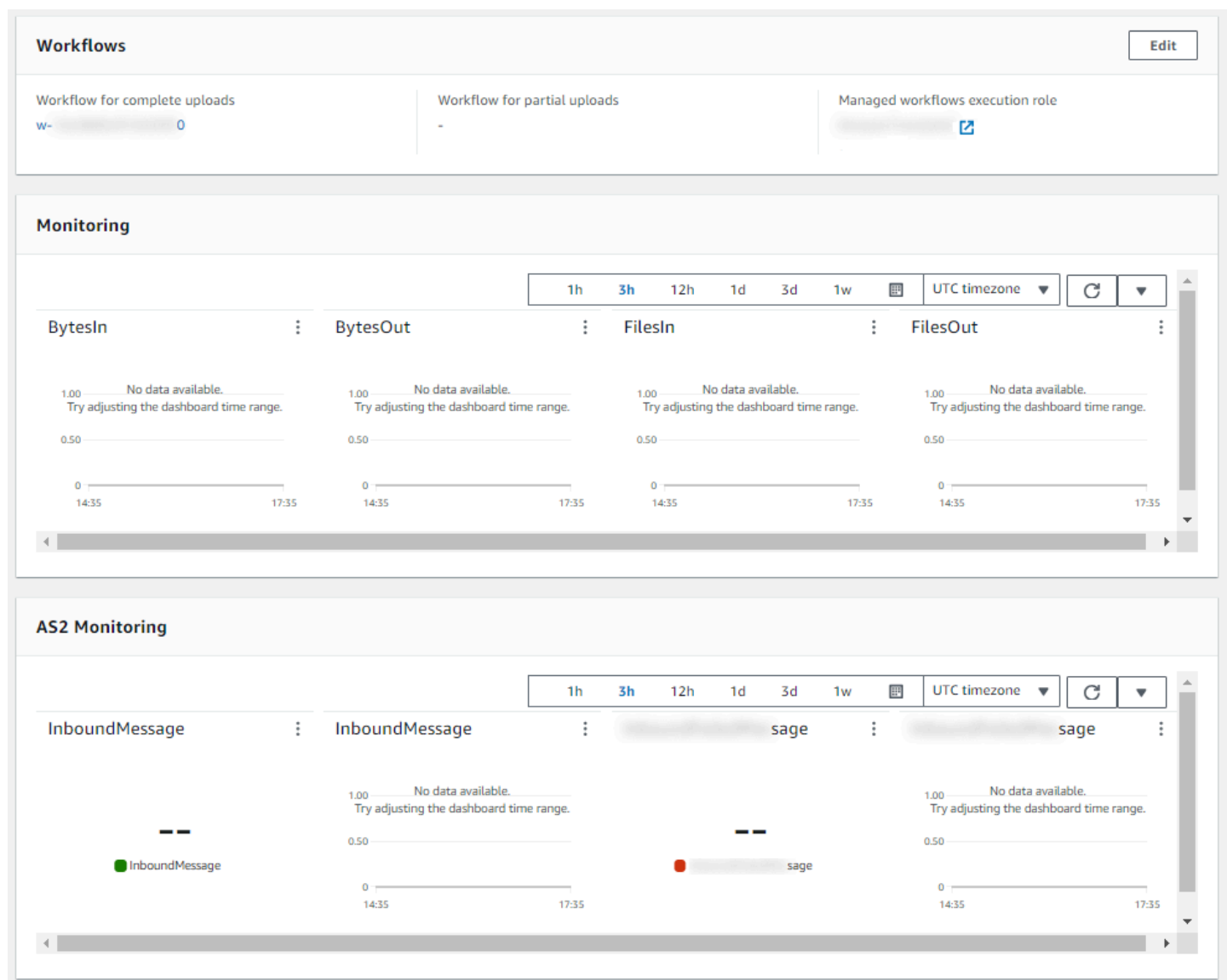
每個 AS2 伺服器都會指派三個靜態 IP 地址。使用這些 IP 地址透過 AS2 傳送非同步 MDNs 給您的交易合作夥伴。

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。



Transfer Family 伺服器的 IPv6 支援

AWS Transfer Family 支援下列資源的雙堆疊 (IPv4 和 IPv6) 端點：

- SFTP 公有端點
- 所有通訊協定的 VPC 內部端點 (SFTP/FTPS/FTP 和 AS2)
- AS2-enabled 的 Transfer Family 伺服器的公有端點，方法是使用 中提供的步驟 [使用 Application Load Balancer 進行雙堆疊 AS2 伺服器連線](#)
- API 端點

透過雙堆疊支援，您的 Transfer Family 端點可以與啟用 IPv4 和 IPv6 的用戶端通訊。這可讓您逐步從 IPv4 轉換到 IPv6 型系統，而不需要一次全部切換、符合 IPv6 合規要求，並不需要昂貴的網路設備來處理 IPv4 和 IPv6 之間的地址轉譯。如需詳細資訊，請參閱 AWS Transfer Family API 參考中的 [DNS 和端點](#)。如需可用端點的完整清單，請參閱 [AWS Transfer Family 端點和配額](#) AWS 一般參考。

IPv6 限制

下列 Transfer Family 資源目前不支援 IPv6：

- VPC-Internet 端點
- VPC_ENDPOINT 端點類型（已棄用）

FTPS 通訊協定支援 PASV 和 EPSV 命令，以請求用於檔案列出、取得和放置操作的開放資料連接埠。不過，PASV 無法使用 IPv6，因為它需要 IPv4-specific 回應。EPSV 會繼續運作，因為它只會傳回連接埠資訊。

若要使用 FTPS，我們建議下列其中一項：

- 將 FTPS 用戶端設定為使用 EPSV
- 使用 IPv4 而非 IPv6

SFTP 同時支援 IPv4 和 IPv6。使用雙堆疊端點時，建議使用 SFTP 而非 FTPS。

設定伺服器的 IPv6

建立新伺服器或更新現有伺服器時，您可以選擇 IP 地址類型：

- IPv4（預設）：為了回溯相容性，伺服器只會接受 IPv4 連線。
- 雙堆疊：伺服器將同時接受 IPv4 和 IPv6 連線。

若要更新現有伺服器的 IP 地址類型：

1. 停止伺服器。
2. 編輯端點詳細資訊。
3. 將 IP 地址類型變更為雙堆疊。
4. 啟動伺服器。

 Note

對於 VPC-Internet 端點，目前不支援雙堆疊模式。

使用 Application Load Balancer 進行雙堆疊 AS2 伺服器連線

您可以使用具有公開端點的 Application Load Balancer 來啟用 AS2 伺服器的雙堆疊 (IPv4 和 IPv6) 連線。這可讓交易合作夥伴使用 IPv4 或 IPv6 連線至 AS2 伺服器。

為您的 AS2 伺服器設定雙堆疊 Application Load Balancer

1. 使用下列設定建立 VPC：
 - 僅 VPC
 - 手動 IPv4 CIDR 輸入
 - Amazon 提供的 IPv6 CIDR 區塊
2. 在不同的可用區域中建立至少兩個子網路：
 - 將 IPv6 CIDRs 新增至子網路
 - 建立子網路時，僅配置 VPC IPv4/IPv6 地址的子集，讓其他子網路的地址可用
3. 建立 VPC 的網際網路閘道。
4. 編輯路由表並新增兩個路由：
 - 一個具有目的地的路由 0.0.0.0/0
 - 一個具有目的地的路由 ::/0
 - 將兩個路由目標設定為您建立的網際網路閘道
5. 在您在步驟 1 中建立的 VPC 中建立 AS2-enabled 的伺服器。請務必將指定 IpAddressType 為 DUALSTACK。

如需如何建立使用 AS2 通訊協定的 Transfer Family 伺服器的詳細資訊，請參閱 [建立 AS2 伺服器](#)。
6. 建立目標群組：
 - 針對指定群組詳細資訊，設定：
 - 目標類型：IP 地址
 - 名稱：輸入名稱

- 協定：HTTP
- 連接埠：5080
- VPC：選取您建立的 VPC
- 通訊協定版本：HTTP1
- 運作狀態檢查：使用預設值
- 對於註冊目標：
 - 輸入 AS2 伺服器的私有 IPv4 地址
 - 選擇包含為以下待定項目

7. 建立 Application Load Balancer：

- 輸入名稱
- 針對結構描述，選擇面向網際網路
- 針對 IP 地址類型，選擇 Dualstack
- 對於網路映射：
 - 選取您建立的 VPC
 - 選取您建立子網路的可用區域
- 針對安全群組，選取允許來自連接埠 80 上任何 IP 地址的傳入 IPv4 和 IPv6 流量的安全群組
- 對於接聽程式和路由：
 - 協定：HTTP
 - 連接埠：80
 - 預設動作：轉送至您建立的目標群組
- 選擇建立負載平衡器

建立 Application Load Balancer 之後，交易合作夥伴可以使用其 DNS 名稱將流量傳送至 AS2 伺服器。此組態可讓您的 AS2 伺服器透過雙堆疊 Application Load Balancer 接受來自 IPv4 和 IPv6 用戶端的連線。

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](#)
- [將您的伺服器置於線上或離線狀態](#)

編輯伺服器的組態

1. 在 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
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，在此頁面上變更伺服器的屬性：

- 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，您現在可以在任何身分提供者類型（服務受管、AWS 目錄服務或自訂身分提供者）之間進行變更。如需變更身分提供者類型的詳細資訊，以及每次轉換所需的資訊，請參閱 [編輯身分提供者組態](#)。
- 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 做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 [管理已啟用 SFTP 的伺服器的主機金鑰](#)。
- 在其他詳細資訊下，您可以編輯下列資訊：
 - 若要變更記錄角色，請參閱 [編輯您的記錄組態](#)。
 - 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 [管理已啟用 SFTP 的伺服器的主機金鑰](#)。
 - 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：啟用此選項可忽略當用戶端嘗試 SETSTAT 在您上傳至 Amazon S3 儲存體的檔案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：提供一種機制，可在 FTPS 工作階段的控制和資料連線之間繼續或共用交涉的私密金鑰。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。

 Note

避免將 Network Load Balancer (NLBs) 或 NAT 閘道放在 AWS Transfer Family 伺服器前面。此組態會增加成本，並可能導致效能問題。如需詳細資訊，請參閱 [避免將 NLBs 和 NATs 放在 AWS Transfer Family 伺服器前面](#)。

- 若要啟動或停止您的伺服器，請參閱 [將您的伺服器置於線上或離線狀態](#)。
- 若要刪除伺服器，請參閱 [刪除伺服器](#)。
- 若要編輯使用者的屬性，請參閱 [管理存取控制](#)。

Protocols

[Edit](#)

Protocols over which clients can connect to your server's endpoint

- SFTP

Identity provider

[Edit](#)

Identity provider type
Service managed

 Note

伺服器主機金鑰 描述和日期 匯入值自 2022 年 9 月起為新值。引進這些值以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設定為伺服器的上次修改日期。也就是說，您為遷移的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，可讓您輕鬆地將其識別為已遷移。

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您伺服器的 區域。

Additional detailsEdit

Log group /aws/transfer/s-	Domain Amazon S3	SetStat option Ignore
Logging role Info -	Login display banner View the display message	TLS session resumption -
Security Policy Info TransferSecurityPolicy-PQ-SSH-Experimental-2023-04	Optimized directories Info ENABLED	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線至伺服器的端點。

編輯通訊協定

1. 在伺服器詳細資訊頁面上，選擇通訊協定旁的編輯。
2. 在編輯通訊協定頁面上，選取或清除通訊協定核取方塊或核取方塊，以新增或移除下列檔案傳輸通訊協定：

- 安全殼層 (SSH) 檔案傳輸通訊協定 (SFTP) – 透過 SSH 傳輸檔案

如需 SFTP 的詳細資訊，請參閱 [建立啟用 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 FTP 的詳細資訊，請參閱 [建立啟用 FTPS 的伺服器](#)。

- 檔案傳輸通訊協定 (FTP) – 未加密的檔案傳輸

如需 FTPS 的詳細資訊，請參閱 [建立啟用 FTP 的伺服器](#)。

Note

如果您只為 SFTP 啟用現有伺服器，並且想要新增 FTPS 和 FTP，則必須確保您擁有與 FTPS 和 FTP 相容的正確身分提供者和端點類型設定。

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，您必須選擇存放在 AWS Certificate Manager (ACM) 中的憑證，當用戶端透過 FTPS 連線到伺服器時，該憑證將用於識別您的伺服器。

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AWS Certificate Manager 《使用者指南》中的[將憑證匯入 ACM](#)。

若要透過私有 IP 地址請求私有憑證以使用 FTPS，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，並包含發行者的相關資訊。

3. 選擇儲存。您將返回伺服器詳細資訊頁面。

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。此外，對於 VPC 端點，您可以編輯可用區域資訊。

編輯伺服器端點詳細資訊

1. 在伺服器詳細資訊頁面上，選擇端點詳細資訊旁的編輯。
2. 您必須先停止伺服器，才能編輯端點類型。然後，在編輯端點組態頁面上，針對端點類型，您可以選擇下列其中一個值：
 - 公有 – 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 VPC 的詳細資訊，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：
 - 無 – 如果您不想使用自訂網域，請選擇無。

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`。

- Amazon Route 53 DNS 別名 – 若要使用在 Route 53 中自動為您建立的 DNS 別名，請選擇此選項。
- 其他 DNS – 若要使用您已在外部 DNS 服務中擁有的主機名稱，請選擇其他 DNS。

選擇 Amazon Route 53 DNS 別名或其他 DNS 會指定要與伺服器端點建立關聯的名稱解析方法。

例如，您的自訂網域可能是 `sftp.inbox.example.com`。自訂主機名稱會使用您提供且 DNS 服務可解析的 DNS 名稱。您可以使用 Route 53 做為 DNS 解析程式，或使用您自己的 DNS 服務提供者。若要了解如何 AWS Transfer Family 使用 Route 53 將流量從自訂網域路由到伺服器端點，請參閱 [使用自訂主機名稱](#)。

Transfer Family > Servers > s-[redacted] > Edit endpoint configuration

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

Select a VPC ID

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

☐ FIPS Enabled endpoint

[Cancel](#) [Save](#)

4. 對於 VPC 端點，您可以在可用區域窗格中變更資訊。
5. 選擇儲存。您將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 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

如果您的端點已啟用 FIPS，則無法將 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，選擇安全政策，其中包含啟用供伺服器使用的密碼編譯演算法。

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

3. 選擇儲存。

您將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 CLI 編輯安全政策

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，包括下列幾行：

```
"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AWS Transfer Family 伺服器的安全政策](#)。

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。

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[工作流程的 IAM 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- [dropdown] [refresh] [Create a new Workflow](#) [external link]

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](#) [external link]

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

[dropdown] [refresh]

3. 選擇儲存。您將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. 選擇儲存。您將返回伺服器詳細資訊頁面。

將您的伺服器置於線上或離線狀態

在 AWS Transfer Family 主控台上，您可以讓伺服器上線或離線。

讓伺服器上線

1. 在 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
2. 在導覽窗格中，選擇 Servers (伺服器)。
3. 選取離線伺服器的核取方塊。
4. 針對 Actions (動作)，選擇 Start (啟動)。

伺服器可能需要幾分鐘的時間才能從離線切換到線上。

Note

當您停止伺服器使其離線時，您目前仍在為該伺服器產生服務費用。若要消除額外的伺服器型費用，請刪除該伺服器。

讓您的伺服器離線

1. 在 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
2. 在導覽窗格中，選擇 Servers (伺服器)。
3. 選取線上伺服器的核取方塊。
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。

編輯身分提供者組態

您可以將伺服器的身分提供者類型從任何類型變更為任何其他類型。可用的身分提供者類型為：

- 服務受管 – 將使用者登入資料存放在服務內
- AWS Directory Service – 使用 AWS Managed Microsoft AD 或 AWS Directory Service for Entra ID Domain Services
- 自訂 – 使用 Lambda 函數或 Amazon API Gateway 與您現有的身分提供者整合

變更身分提供者類型時，您需要根據正在進行的轉換提供特定資訊。下列各節說明每種變更類型的必要資訊。

Important

變更身分提供者時的考量事項：

- 使用者遷移 – 變更身分提供者類型時，不會自動遷移現有的使用者組態。您需要在新的身分提供者系統中設定使用者。

- 測試 – 在生產環境中進行變更之前，請徹底測試新的身分提供者組態。
- 許可 – 在進行變更之前，請確定新的身分提供者已設定必要的 IAM 許可和角色。

變更為服務受管身分提供者

從任何其他身分提供者類型變更為服務受管時，您需要：

- 選取做為身分提供者類型受管的服務
- 在變更完成後直接在 中建立新使用者，因為不會傳輸來自其他身分提供者 AWS Transfer Family 的現有使用者組態

範例：如果您要從自訂身分提供者變更為服務受管，則需要重新建立服務中的所有 AWS Transfer Family 使用者帳戶及其相關聯的許可。

變更為 AWS Directory Service

從任何其他身分提供者類型變更為 AWS Directory Service 時，您需要提供：

- 目錄 – 選取現有的 AWS Managed Microsoft AD 或 AWS Directory Service for Entra ID Domain Services 目錄
- 存取 – 選擇是否限制對特定群組的存取，或允許目錄中所有使用者存取
- 存取角色 – 允許 存取目錄的 AWS Transfer Family IAM 角色

範例：如果您要從服務受管變更為 AWS Directory Service，您可以選擇現有的 d-1234567890 目錄，選擇限制對 TransferUsers 群組的存取，並指定 TransferDirectoryAccessRole IAM 角色。

變更為自訂身分提供者

從任何其他身分提供者類型變更為自訂身分提供者時，您需要在 Lambda 函數或 Amazon API Gateway 之間進行選擇，並提供必要的組態：

使用 Lambda 函數

對於 Lambda 函數整合，請提供：

- 函數 – 選取處理身分驗證的現有 Lambda 函數
- 身分驗證方法（適用於 SFTP 通訊協定）– 選擇密碼、公有金鑰或兩者

範例：如果您要從 AWS Directory Service 變更為自訂 Lambda 身分提供者，您可以選擇您的 `TransferCustomAuth` 函數，然後選擇密碼作為身分驗證方法。

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

[redacted] ▼



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

使用 Amazon API Gateway

對於 Amazon API Gateway 整合，請提供：

- API Gateway URL – 叫用 API Gateway 端點的 URL
- 叫用角色 – 允許 AWS Transfer Family 叫用 API Gateway 的 IAM 角色
- 身分驗證方法（適用於 SFTP 通訊協定）– 選擇密碼、公有金鑰或兩者

範例：如果您要從服務受管變更為 API Gateway，您會提供 URL `https://abcdef123.execute-api.us-east-1.amazonaws.com/prod`、指定 `TransferApiGatewayInvocationRole` IAM 角色，然後選擇公有金鑰做為身分驗證方法。

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

從 Amazon API Gateway 變更為 Lambda 函數

常見的轉換是從 Amazon API Gateway 變更為 Lambda 函數，以進行自訂身分提供者整合。此變更可讓您簡化架構，同時維護相同的身分驗證邏輯。

此轉換的主要考量事項：

- 相同的函數，不同的許可 – 您可以對 API Gateway 和直接 Lambda 整合使用相同的 Lambda 函數，但必須更新資源政策。
- 資源政策要求 – 變更為直接 Lambda 整合時，除了 之外，函數的資源政策還必須授予叫用函數的 `transfer.amazonaws.com` 許可 `apigateway.amazonaws.com`。

若要進行此變更

1. 更新 Lambda 函數的資源政策，`transfer.amazonaws.com` 以允許 叫用函數。
2. 在 AWS Transfer Family 主控台中，將身分提供者從 API Gateway 變更為 Lambda 函數。
3. 選取您現有的 Lambda 函數。
4. 測試組態以確保身分驗證正常運作。

直接 Lambda 整合的資源政策範例：

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Principal": {
      "Service": [
        "transfer.amazonaws.com",
        "apigateway.amazonaws.com"
      ]
    },
    "Action": "lambda:InvokeFunction",
    "Resource": "arn:aws:lambda:us-east-1:123456789012:function:function-name"
  }]
}
```

身分提供者轉換期間的使用者保留

在身分提供者類型之間變更時，會在特定案例中保留現有的使用者組態，以便在發生問題時啟用有效的轉返：

- 服務受管至自訂身分提供者和返回 – 如果您從服務受管變更為自訂身分提供者，然後返回服務受管，則所有使用者都會保留在其上次已知的組態中。
- AWS Directory Service 變更為自訂身分提供者和返回 – 如果您從 AWS Directory Service 變更為自訂身分提供者，然後再變更為 AWS Directory Service，委派存取群組的所有定義都會保留在其上次已知的組態中。

此保留行為可讓您安全地測試自訂身分提供者組態，並復原至先前的設定，而不會遺失使用者存取組態。

變更身分提供者時的重要考量

- 使用者遷移 – 變更身分提供者類型時，不會自動遷移現有的使用者組態。您需要在新的身分提供者系統中設定使用者。
- 測試 – 在生產環境中進行變更之前，請徹底測試新的身分提供者組態。
- 許可 – 在進行變更之前，請確定新的身分提供者已設定必要的 IAM 許可和角色。

管理已啟用 SFTP 的伺服器的主機金鑰

伺服器主機金鑰是 Transfer Family 伺服器用來為發起人提供唯一身分的私有金鑰，並保證它是正確的伺服器。該保證是由發起人known_hosts檔案中存在正確的公有金鑰強制執行。(known_hosts檔案是大多數 SSH 用戶端用來存放您已連線之伺服器的公有金鑰的標準功能。) 您可以針對伺服器執行，擷取對應至伺服器主機金鑰ssh-keyscan的公有金鑰。

Important

意外變更伺服器的主機金鑰可能造成破壞。視 SFTP 用戶端的設定方式而定，它可能會立即失敗，並顯示沒有信任主機金鑰存在的訊息，或出現威脅提示。如果有助於自動化連線的指令碼，它們很可能也會失敗。

根據預設，會為啟用 SFTP 的伺服器 AWS Transfer Family 產生主機金鑰。您可以匯入伺服器主機金鑰來保留主機身分，並避免更新用戶端信任存放區。[何時匯入主機金鑰](#)會列出您可能想要這麼做的幾個原因。如果您不提供主機金鑰，則會為您產生新的金鑰。

AWS Transfer Family 支援多種不同類型的主機金鑰 (RSA、ECDSA 和 ED25519)，可與更廣泛的用戶端主機簽章演算法相容。不同的金鑰類型可啟用特定演算法：RSA 金鑰可啟用 rsa-* 演算法、ECDSA

金鑰可啟用 `ecdsa-*` 演算法，而 ED25519 金鑰可啟用 `ed25519` 演算法。在伺服器建立時間規劃您的金鑰類型，因為在用戶端開始與伺服器互動之後引入其他金鑰類型，可能會對某些用戶端造成干擾，並可能和取代現有的主機金鑰一樣有問題。

若要防止提示使用者再次驗證已啟用 SFTP 伺服器的真實性，請將現場部署伺服器的主機金鑰匯入已啟用 SFTP 的伺服器。這麼做也會防止使用者收到潛在中間人攻擊的警告。

您也可以定期輪換主機金鑰，做為額外的安全措施。如需詳細資訊，請參閱[輪換伺服器主機金鑰](#)。

Note

伺服器主機金鑰由支援 SFTP 通訊協定的伺服器使用。

何時匯入主機金鑰

雖然 AWS Transfer Family 可以自動產生主機金鑰，但匯入您自己的主機金鑰有幾種情況可提供操作優勢：

- 伺服器遷移 - 您正在從現有伺服器遷移至 `known_hosts` 檔案，AWS Transfer Family 並希望避免更新現有用戶端的用戶端信任存放區 (known_hosts 檔案)。
- 災難復原和容錯移轉 - 您擁有多個共用相同公有 DNS 名稱的 AWS Transfer Family 伺服器（例如，一個在美國東部（俄亥俄）和一個在美國西部（奧勒岡））。在兩個伺服器上使用相同的主機金鑰可確保無縫容錯移轉，而不會發生用戶端身分驗證失敗。
- 營運持續性 - 您希望主機金鑰材料未來可與其他伺服器 (AWS Transfer Family 或其他) 搭配使用，以在整個基礎設施中維持一致的伺服器身分。
- 演算法控制 - 您想要透過提供更多主機金鑰演算法來提高用戶端相容性，或者您想要透過僅提供與特定演算法相容的金鑰來控制用戶端可以使用的演算法。

下列主題提供管理伺服器主機金鑰的詳細程序：

- [新增額外的伺服器主機金鑰](#) - 將其他主機金鑰新增至伺服器
- [刪除伺服器主機金鑰](#) - 從伺服器移除主機金鑰
- [輪換伺服器主機金鑰](#) - 輪換主機金鑰以增強安全性
- [其他伺服器主機金鑰資訊](#) - 檢視和管理主機金鑰詳細資訊

新增額外的伺服器主機金鑰

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，有助於在用戶端連線到伺服器時識別伺服器，並改善您的安全性設定檔。例如，如果您的原始金鑰是 RSA 金鑰，您可以新增額外的 ECDSA 金鑰。

Note

SFTP 用戶端將使用符合金鑰演算法之組態中最舊的金鑰進行連線。每個金鑰類型的最舊金鑰 (RSA、ECDSA 或 ED25519) 是該類型伺服器的作用中金鑰。

Transfer Family 伺服器具有多種主機金鑰類型時的安全性備註

如果伺服器有多種類型的主機金鑰，SFTP 用戶端可以依類型指派偏好設定。因此，當伺服器存在 RSA、ECDSA 和 ED25519 主機金鑰時，選擇取決於 類型偏好設定。

現代 SFTP 用戶端在存在時偏好 ECDSA 和 ED25519 主機金鑰。如果您想要在伺服器先前只有 RSA 金鑰時新增 ECDSA 或 ED25519 金鑰，這就變得很重要。新增 ECDSA 或 ED25519 金鑰可能會顯示為用戶端的安全警告。

對於用戶端，金鑰會顯示為已變更，實際上並未變更：除了現有的 RSA 金鑰之外，還新增了新的金鑰。如果您決定新增類型的伺服器主機金鑰，請記住這一點。

新增額外的伺服器主機金鑰

1. 在 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
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 (2)							Actions	Add host key
Find resources							< 1 >	
☐	Name	Host key ID	Fingerprint Info	Description	Key type	Date imported		
☐	Default host key	hostkey-	SHA256:	Default	ssh-rsa	2023-06-30		
☐	ecdsa-521	hostkey-	SHA256:	ECDSA host key	ecdsa-sha2-nistp521	2024-06-13		

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 的伺服器連線到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 ""`（無複雜密碼）。如需如何產生金鑰對的詳細資訊，請參閱 [在 macOS、Linux 或 Unix 上建立 SSH 金鑰](#)。

- （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。
- 選擇 Add key (新增金鑰)。您將返回伺服器詳細資訊頁面。

若要使用 AWS Command Line Interface (AWS CLI) 新增主機金鑰，請使用 [ImportHostKey](#) API 操作並提供新的主機金鑰。如果您建立新的啟用 SFTP 的伺服器，您可以在 [CreateServer](#) API 操作中提供主機金鑰做為參數。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 命令會為指定的啟用 SFTP 的伺服器匯入主機金鑰。

```
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。

刪除伺服器主機金鑰

- 在 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
- 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。
- 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 (2)							Actions	Add host key
Find resources							< 1 >	
☐	Name	Host key ID	Fingerprint	Description	Key type	Date imported		
☐	Default host key	hostkey-	SHA256:	Default	ssh-rsa	2023-06-30		
☐	ecdsa-521	hostkey-	SHA256:	ECDSA host key	ecdsa-sha2-nistp521	2024-06-13		

- 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。
- 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 [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 命令會刪除指定啟用 SFTP 之伺服器的主機金鑰。

```
aws transfer delete-host-key --server-id your-server-id --host-key-id your-host-key-id
```

輪換伺服器主機金鑰

您可以定期輪換伺服器主機金鑰。本主題說明伺服器如何選擇要套用的金鑰，以及輪換這些金鑰的程序。

用戶端如何選擇伺服器主機金鑰

Transfer Family 選擇要套用的伺服器金鑰取決於 SFTP 用戶端的條件，如此處所述。假設有一個較舊的金鑰和一個較新的金鑰。

- SFTP 用戶端沒有該伺服器的先前公有主機金鑰。用戶端第一次連線到伺服器時，會發生下列任一情況：
 - 如果設定連線，用戶端會失敗。
 - 或者，用戶端會選擇第一個符合可用演算法的金鑰，並詢問使用者是否可以信任該金鑰。若是如此，用戶端會自動更新known_hosts檔案（或用戶端用來記錄信任決策的任何本機組態檔案或資源），並輸入該金鑰。
- SFTP 用戶端的known_hosts檔案中有較舊的金鑰。即使存在較新的金鑰，用戶端也偏好使用此金鑰，無論是針對此金鑰的演算法或其他演算法。這是因為用戶端對其known_hosts檔案中的金鑰具有更高層級的信任。
- SFTP 用戶端在其金鑰檔案中具有新的known_hosts金鑰（在任何可用的演算法中）。用戶端會忽略較舊的金鑰，因為它們不受信任並使用新的金鑰。
- SFTP 用戶端的known_hosts檔案中有兩個金鑰。用戶端會依索引選擇符合伺服器所提供可用金鑰清單的第一個金鑰。

Transfer Family 偏好 SFTP 用戶端在其known_hosts檔案中擁有所有金鑰，因為這可在連線至 Transfer Family 伺服器時提供最大的彈性。金鑰輪換是根據同一 Transfer Family 伺服器的known_hosts檔案中可能存在多個項目。

輪換伺服器主機金鑰程序

例如，假設您已將下列一組伺服器主機金鑰新增至 Transfer Family 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
RSA	2020 年 4 月 1 日
ECDSA	2020 年 2 月 1 日
ED25519	2019 年 12 月 1 日
RSA	2019 年 10 月 1 日
ECDSA	2019 年 6 月 1 日
ED25519	2019 年 3 月 1 日

輪換伺服器主機金鑰

1. 新增伺服器主機金鑰。此程序說明於 [新增額外的伺服器主機金鑰](#)。
2. 刪除您先前新增之相同類型之一或多個主機金鑰。此程序說明於 [刪除伺服器主機金鑰](#)。
3. 所有金鑰都可見，並且可以處於作用中狀態，具體取決於先前在 [用戶端如何選擇伺服器主機金鑰](#) 中所述的行為。

其他伺服器主機金鑰資訊

您可以選擇主機金鑰以顯示該金鑰的詳細資訊。

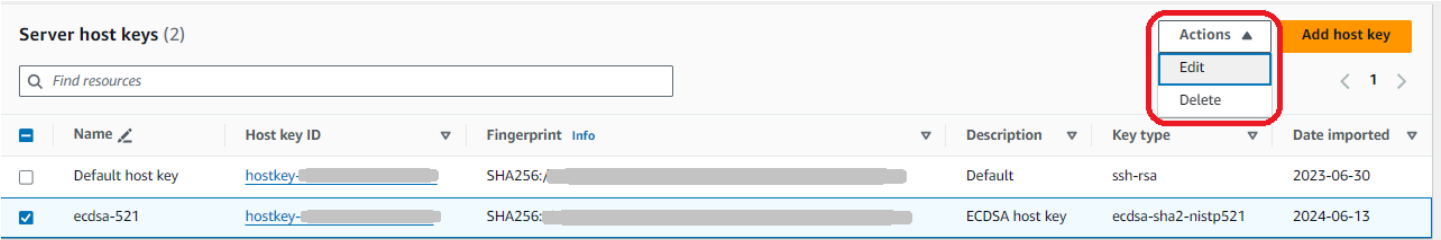
Transfer Family > Servers > s-3fe215d89f074ed2a > Hostkey: hostkey-a6fed60bcb704ea9b

hostkey-a6fed60bcb704ea9b Delete

Host key configuration Edit

Name	ecdsa-521	Key type	ecdsa-sha2-nistp521
Fingerprint	SHA256: [redacted]	Date imported	Thu, 13 Jun 2024 17:08:59 GMT
Description	ECDSA host key	Amazon Resource Name (ARN)	arn:aws:transfer:us-east-1:[redacted]:host-key/s-[redacted]/hostkey-a-[redacted]

您可以刪除主機金鑰，或從伺服器詳細資訊畫面上的動作功能表編輯其描述。選取主機金鑰，然後從功能表中選擇適當的動作。



在 主控台中監控用量

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 Transfer Family 可用的指標。

命名空間	指標	Description
AWS/Transfer	BytesIn	傳輸到伺服器的位元組總數。 報告條件： - 對於 SFTP/FTP/FTPS：在與 Transfer Family 伺服器建立連線時，每 5 分鐘發出一次。如果期間內沒有傳輸任何檔案或位元組，則會發出「0」。 - 對於 AS2：當客戶在其 AS2 伺服器中收到訊息，並在傳入訊息處理完成後立即發出 單位：計數 期間：5 分鐘
	BytesOut	從伺服器傳輸的位元組總數。 報告條件： 對於 SFTP/FTP/FTPS：在與 Transfer Family 伺服器建立連線時，每 5 分鐘發出一次。如果期間內沒有傳輸任何檔案或位元組，則會發出「0」。

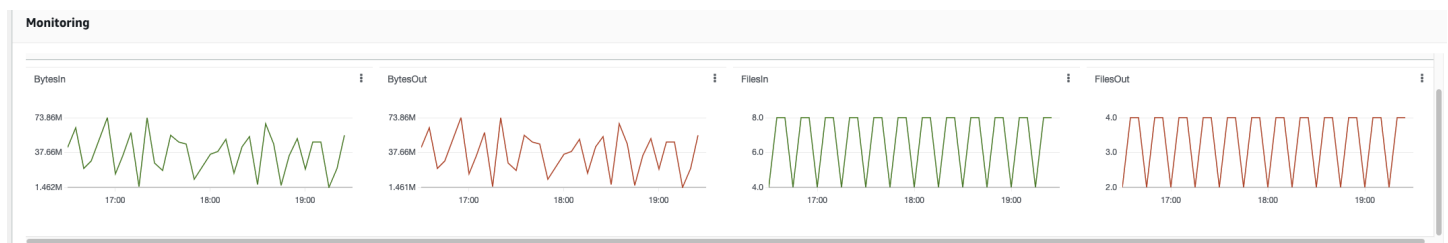
命名空間	指標	Description
		對於 AS2：當客戶StartFileTransfer 從其 AS2 連接器呼叫，並在傳出訊息完成處理後立即發出時。 單位：計數 期間：5 分鐘
	FilesIn	傳輸到伺服器的檔案總數。 對於使用 AS2 通訊協定的伺服器，此指標代表接收的訊息數量。 報告條件： - 對於 SFTP/FTP/FTPS：在與 Transfer Family 伺服器建立連線時，每 5 分鐘發出一次。如果期間內沒有傳輸任何檔案或位元組，則會發出「0」。 - 對於 AS2：當客戶在其 AS2 伺服器中收到訊息，並在傳入訊息完成處理時立即發出。 單位：計數 期間：5 分鐘

命名空間	指標	Description
	FilesOut	從伺服器傳輸的檔案總數。 報告條件： - 對於 SFTP/FTP/FTPS：在與 Transfer Family 伺服器建立連線時，每 5 分鐘發出一個。如果期間內沒有傳輸任何檔案或位元組，則會發出「0」。 - 對於 AS2：當客戶 StartFileTransfer 從其 AS2 連接器呼叫，並在傳出訊息完成處理後立即發出時。 單位：計數 期間：5 分鐘
	InboundMessage	成功從交易合作夥伴接收的 AS2 訊息總數。 報告條件：當客戶在其 AS2 伺服器中收到訊息，並在傳入訊息成功完成處理時立即發出 單位：計數 期間：5 分鐘
	InboundFailedMessage	未成功從交易合作夥伴收到的 AS2 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。 報告條件：當客戶在其 AS2 伺服器中收到訊息，並在傳入訊息處理失敗時立即發出 單位：計數 期間：5 分鐘

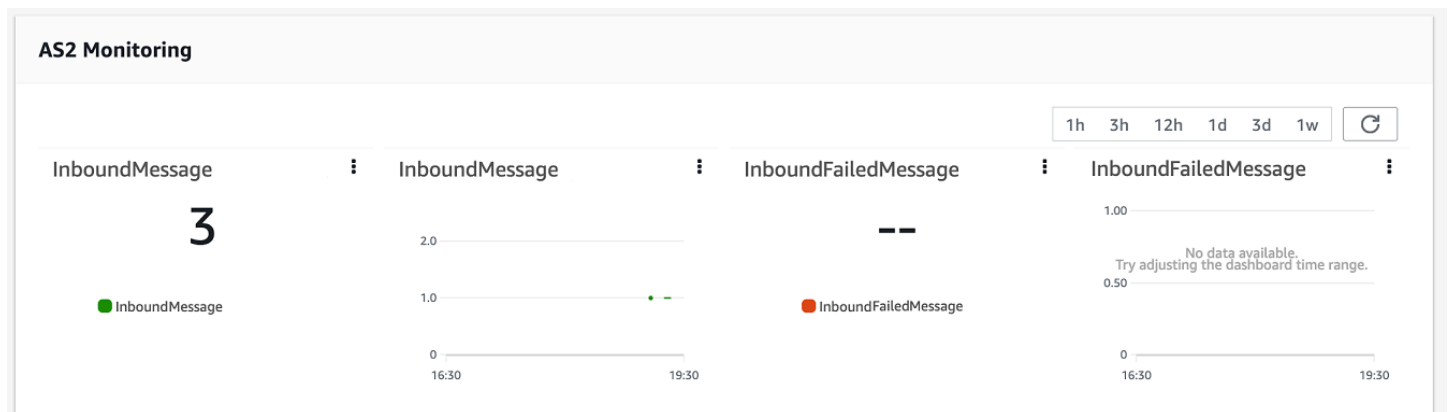
命名空間	指標	Description
	OnUploadExecutionsStarted	在伺服器上啟動的工作流程執行總數。 報告條件：每次執行啟動時觸發 單位：計數 Period：1 分鐘
	OnUploadExecutionsSuccess	在伺服器上成功執行工作流程的總數。 報告條件：每次執行成功完成時觸發 單位：計數 Period：1 分鐘
	OnUploadExecutionsFailed	伺服器上失敗的工作流程執行總數。 報告條件：每次執行未成功完成時觸發 單位：計數 Period：1 分鐘
	OutboundMessage	成功傳送給交易合作夥伴的 AS2 訊息總數。 報告條件：當客戶StartFileTransfer 從 AS2 連接器呼叫，並在外撥訊息成功完成處理時立即發出 單位：計數 期間：5 分鐘

命名空間	指標	Description
	OutboundFailedMessage	未成功傳送給交易合作夥伴的 AS2 訊息總數。 報告條件：當客戶StartFileTransfer 從 AS2 連接器呼叫，並在傳出訊息處理失敗時立即發出 單位：計數 期間：5 分鐘

監控區段包含四個個別圖形。這些圖表顯示傳入的位元組、傳出的位元組、傳入的檔案和傳出的檔案。



對於已啟用 AS2 通訊協定的伺服器，監控資訊下方有一個 AS2 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 CloudWatch 中開啟對應的指標詳細資訊。
- 檢視日誌 – 在 CloudWatch 中開啟對應的日誌群組。

管理存取控制

您可以使用 AWS Identity and Access Management (IAM) 政策來控制使用者對 AWS Transfer Family 資源的存取。IAM 政策是一種陳述式，通常採用 JSON 格式，允許特定層級的資源存取。您可以使用 IAM 政策來定義要讓使用者執行和不執行哪些檔案操作。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 具有與其相關聯的 IAM 政策和信任關係的 IAM 角色。

每個使用者都會獲指派 IAM 角色。AWS Transfer Family 使用的 IAM 角色類型稱為服務角色。當使用者登入您的伺服器時，會 AWS Transfer Family 擔任映射至使用者的 IAM 角色。若要了解如何建立可讓使用者存取 Amazon S3 儲存貯體的 IAM 角色，請參閱《IAM 使用者指南》中的[建立角色以將許可委派給 AWS 服務](#)。

您可以使用 IAM 政策中的特定許可，授予 Amazon S3 物件的唯寫存取權。如需詳細資訊，請參閱[授予僅寫入和列出檔案的能力](#)。

AWS 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[資料保護和加密](#)。此外，您可以在 IAM 使用者指南中查看有關[工作階段政策](#)的詳細資訊。

主題

- [允許讀取和寫入存取 Amazon S3 儲存貯體](#)
- [為 Amazon S3 儲存貯體建立工作階段政策](#)
- [動態許可管理方法](#)

允許讀取和寫入存取 Amazon S3 儲存貯體

本節說明如何建立允許讀取和寫入存取特定 Amazon S3 儲存貯體的 IAM 政策。將具有此 IAM 政策的 IAM 角色指派給您的使用者，可讓該使用者存取指定的 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:::amzn-s3-demo-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:::amzn-s3-demo-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。由於這些是不同的資源，因此會使用不同的 Amazon Resource Name (ARNs) 來指定這些資源。

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

工作階段政策是將使用者限制為 Amazon S3 儲存貯體特定部分的 AWS Identity and Access Management (IAM) 政策。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。

當您需要對 Amazon S3 儲存貯體特定部分的使用者群組提供相同存取權時，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 受管政策中使用上述變數。您也無法在 IAM 角色定義中使用它們做為政策變數。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。

工作階段政策範例

下列程式碼顯示範例工作階段政策。

```
{
  "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結尾斜線，以表示它是目錄。另一方面，如果您設定的使用者HomeDirectory沒有結尾斜線，則應該將其包含在政策中。

在之前的範例政策中，請注意 `transfer:HomeFolder`、`transfer:HomeBucket` 和 `transfer:HomeDirectory` 政策參數的使用方式。這些參數是針對為使用者設定的 HomeDirectory 所設定，如 [HomeDirectory](#) 和 中所述 [實作您的 API Gateway 方法](#)。這些參數具有下列定義：

- `transfer:HomeBucket` 參數會取代為 的第一個元件HomeDirectory。
- `transfer:HomeFolder` 參數會替換為HomeDirectory參數的剩餘部分。
- `transfer:HomeDirectory` 參數已移除正斜線 (/)，因此可以做為Resource陳述式中 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` 已設定為 `/home`。
- `transfer:HomeFolder` 已設定為 `/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" 限制使用者對相同路徑的 `put` 和 `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 儲存貯體的 IAM 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位使用者的存取權。如需詳細資訊，請參閱《IAM 使用者指南》中的 [AssumeRole](#)、[AssumeRoleWithSAML](#) 和 [AssumeRoleWithWebIdentity](#) 的許可。

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)"
```

工作階段政策的巢狀取代

巢狀取代不會在 Transfer Family 工作階段政策中執行。工作階段政策可以使用巢狀變數，例如 `${transfer:HomeDirectory}`。處理政策時，外部變數（例如 `${transfer:HomeDirectory}`）可能會取代為包含另一個變數（例如 `{amzn-s3-demo-bucket:${transfer:UserName}}`）的值。不過，巢狀變數不會進一步以實際使用者名稱（例如 `johndoe`）取代。

這表示在為 Transfer Family 建立工作階段政策時，您需要考慮此行為，並確保相應地設計政策結構和變數用量。巢狀變數可能無法如預期解析，且政策可能不會授予預期的許可。請務必徹底測試和驗證工作階段政策，以確保它們如預期般運作。此行為是實作 Transfer Family 環境的存取控制和許可時的重要考量。

此問題的一個解決方法是在工作階段政策中使用實際的 Amazon S3 儲存貯體名稱。因此，例如，使用 `${transfer:HomeDirectory}` 下列，其中 `amzn-s3-demo-bucket` 是您的實際儲存貯體：`${amzn-s3-demo-bucket/transfer:UserName}`。

動態許可管理方法

了解 Transfer Family 許可架構

AWS Transfer Family 透過工作階段政策支援動態許可管理，可讓您在執行時間限制 IAM 角色的有效許可。此方法適用於服務受管使用者和自訂身分提供者使用者，但只有在將檔案傳輸到 Amazon S3 (而非 Amazon EFS) 時受支援。

每個 AWS Transfer Family 使用者都使用包含下列項目的許可模型來操作：

1. 基本 IAM 角色 - 定義使用者的基本許可
2. 選用工作階段政策 - 在執行時間限制 (範圍縮小) 基本許可

有效許可是基本角色許可和工作階段政策許可的交集。工作階段政策只能限制許可；他們不能授予基本角色允許以外的其他許可。

此架構適用於這兩種使用者類型：

- 服務受管使用者 - 工作階段政策可以直接在使用者設定中設定
- 自訂身分提供者使用者 - 工作階段政策可在身分驗證回應中傳回，或存放在 AWS Secrets Manager

許可管理的兩種方法

為需要唯一存取模式的 Transfer Family 使用者設計許可時，您可以選擇兩種主要方法：

每個使用者一個角色

為每個 Transfer Family 使用者建立個別的 IAM 角色，具有專為該使用者需求量身打造的特定許可。在下列情況下使用此方法：

- 每個使用者都需要非常不同的許可
- 許可管理是由組織中的不同人員處理
- 您需要對個別使用者存取進行精細控制

具有工作階段政策的共用角色

使用具有廣泛許可的單一 IAM 角色 (例如存取包含多個使用者主目錄的整個 Amazon S3 儲存貯體)，並套用工作階段政策，將每位使用者限制為其特定區域。相較於管理每個使用者的個別角色，此方法可大幅降低管理開銷。在下列情況下使用此方法：

- 使用者需要類似類型的存取權，但需要不同的資源（例如，所有使用者都需要讀取/寫入存取權，但每個使用者都只需要自己的資料夾）
- 您想要簡化角色管理，並避免建立數十或數百個個別角色
- 使用者應該只在共用儲存貯體中存取其指定的主目錄
- 在您的組織內集中管理許可

例如，您可以建立一個可存取整個 `s3://company-transfers/` 儲存貯體的角色，然後使用工作階段政策將 `alice` 限制為 `s3://company-transfers/alice/`、`bob` 限制為 `s3://company-transfers/bob/` 等，而不是為使用者「alice」`s3://company-transfers/bob/`、「bob」和「charlie」建立個別角色。

實作工作階段政策

工作階段政策的運作方式是限制指派給使用者的基本 IAM 角色的有效許可。最終許可是角色許可和工作階段政策許可的交集。

您可以透過兩種方式實作動態工作階段政策：

變數替換

在工作階段政策 `${transfer:HomeBucket}` 中使用 Transfer Family 政策變數 `${transfer:Username}`，例如 `${transfer:HomeDirectory}`、和 `${transfer:HomeBucket}`。這些變數會在執行時間自動取代為實際值。如需這些變數的詳細資訊，請參閱 [為 Amazon S3 儲存貯體建立工作階段政策](#)。

動態產生

對於自訂身分提供者，從 Lambda 函數或 API Gateway 方法的身分驗證回應產生 on-the-fly 工作階段政策。此方法可讓您在身分驗證時，根據使用者屬性、群組成員資格或外部資料來源建立高度自訂的政策。

您也可以在中存放預先產生的工作階段政策，AWS Secrets Manager 方法是將名為 `Policy` 的金鑰 `Policy` 與工作階段政策 JSON 作為值。這可讓您跨多個使用者使用相同的廣泛 IAM 角色，同時維護使用者特定的存取控制。

Note

只有往返 Amazon S3 的檔案傳輸才支援工作階段政策。它們不適用於 Amazon EFS 檔案系統。對於 Amazon EFS，許可由 UID/GID 和在檔案系統本身內套用的許可位元管理。

依使用者類型實作

服務受管使用者

對於服務受管使用者，您可以透過 AWS Transfer Family 主控台、API 或 CLI，直接在使用者組態中指定工作階段政策。如需詳細資訊，請參閱[使用服務受管使用者](#)。

自訂身分提供者使用者

對於自訂身分提供者使用者，您可以透過兩種方式提供工作階段政策：

- 透過 `aws-secretsmanager`，AWS Secrets Manager 將名為 `SecretsManagerPolicy` 的金鑰 Policy 與工作階段政策作為值
- 直接在 Lambda 函數回應或 API Gateway 回應中作為身分驗證結果的一部分

如需詳細資訊，請參閱[自訂身分提供者解決方案](#)。

範例：使用工作階段政策簡化角色管理

此範例示範動態許可管理如何大幅降低管理開銷，同時維護安全性。

案例

您的組織有 50 位使用者需要 SFTP 存取權才能傳輸檔案。每個使用者都應該在名為 `company-transfers` 的共用 Amazon S3 儲存貯體中存取自己的資料夾。如果沒有工作階段政策，您需要建立 50 個不同的 IAM 角色。

傳統方法（不含工作階段政策）

- 建立 50 個 IAM 角色：`TransferRole-Alice`、`TransferRole-Charlie`、`TransferRole-Bob`等。
- 每個角色都有只有該使用者的資料夾的特定許可
- 管理許可需要更新個別角色
- 新增使用者需要建立新的角色

動態方法（使用工作階段政策）

- 建立 1 個 IAM 角色：`TransferRole-Shared`具有整個儲存貯體的廣泛許可
- 使用工作階段政策，將每位使用者限制在執行時間的特定資料夾
- 管理許可需要更新一個角色或工作階段政策範本

- 新增使用者不需要新的角色，只需要使用者組態

實作

以下是實作動態方法的方式（使用儲存company-transfers貯體做為以實際 Amazon S3 儲存貯體取代的範例）：

實作動態許可管理

1. 建立一個具有廣泛 Amazon S3 許可的共用 IAM 角色：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource": "arn:aws:s3:::company-transfers/*"
    },
    {
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::company-transfers"
    }
  ]
}
```

2. 建立工作階段政策範本，限制對使用者資料夾的存取：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
```

```
        "s3:DeleteObject"
      ],
      "Resource": "arn:aws:s3:::company-transfers/${transfer:Username}/*"
    },
    {
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::company-transfers",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${transfer:Username}*"
        }
      }
    }
  ]
}
```

3. 使用 設定每個使用者：

- 共用的 IAM 角色
- 套用的工作階段政策如下所示：
 - 服務受管使用者：在建立或修改使用者時，使用 API 或 CLI 透過政策參數套用 JSON（主控台僅提供預先定義的政策選項）
 - 自訂身分提供者使用者：在身分驗證期間將其作為 Lambda 函數回應的一部分傳回，或將其與使用者的憑證一起存放 AWS Secrets Manager 為名為 "Policy" 的金鑰
- 主目錄：/company-transfers/\${transfer:Username}/

AWS CloudTrail 的記錄 AWS Transfer Family

AWS Transfer Family 與 AWS CloudTrail 和 Amazon CloudWatch 整合。CloudTrail 和 CloudWatch 提供不同但互補的目的。

- 本主題涵蓋與 CloudTrail 的整合，CloudTrail 是一項 AWS 服務，可建立在您的 中採取之動作的記錄 AWS 帳戶。它會持續監控並記錄 API 操作，以進行主控台登入、AWS Command Line Interface 命令和 SDK/API 操作等活動。這可讓您記錄誰從何地採取了哪些動作。CloudTrail 透過提供環境中 AWS 所有活動的歷史記錄，協助稽核、存取管理和法規遵循。如需詳細資訊，請參閱 [AWS CloudTrail 使用者指南](#)。
- [AWS Transfer Family 伺服器 Amazon CloudWatch 記錄](#) 涵蓋與 CloudWatch 的整合，CloudWatch 是一種 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 可協助操作任務，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](#)。

追蹤是一種組態，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一或多個日誌專案。一個事件為任何來源提出的單一請求，並包含請求動作、請求的日期和時間、請求參數等資訊。CloudTrail 日誌檔案不是公有 API 操作的排序堆疊追蹤，因此不會以任何特定順序顯示。

若要不持續記錄您 AWS 帳戶中的事件，包括的事件 AWS Transfer Family，請建立追蹤。線索能讓 CloudTrail 將日誌檔案交付至 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。線索會記錄 AWS 分割區中所有區域的事件，並將日誌檔案交付至您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析和處理 CloudTrail 日誌中所收集的事件資料。如需詳細資訊，請參閱下列內容：

- [建立追蹤的概觀](#)
- [CloudTrail 支援的服務和整合](#)
- [設定 CloudTrail 的 Amazon SNS 通知](#)
- [接收多個區域的 CloudTrail 日誌檔案和接收多個帳戶的 CloudTrail 日誌檔案](#)

CloudTrail 會記錄所有 AWS Transfer Family 動作，並記錄在 [Actions](#) 中 [API reference](#)。例如，對 CreateServer、ListUsers 和 StopServer 動作發出的呼叫會在 CloudTrail 記錄檔案中產生專案。

每一筆事件或日誌專案都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 是否使用根登入資料或 AWS Identity and Access Management 使用者登入資料提出請求。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 請求是否由其他 AWS 服務提出。

如需詳細資訊，請參閱 [CloudTrail userIdentity 元素](#)。

如果您建立線索，您可以將 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括的事件 AWS Transfer Family。即使您未設定追蹤，依然可以透過 CloudTrail 主控台內的 Event history (事件歷史記錄) 檢視最新事件。

您可以利用 CloudTrail 所收集的資訊來判斷向 AWS Transfer Family 發出的請求，以及發出請求的 IP 地址、人員、時間和其他詳細資訊。

若要進一步了解 CloudTrail，請參閱 [AWS CloudTrail 《使用者指南》](#)。

主題

- [啟用 AWS CloudTrail 記錄](#)
- [建立伺服器的範例日誌項目](#)
- [資料存取日誌範例](#)

啟用 AWS CloudTrail 記錄

您可以使用 監控 AWS Transfer Family API 操作 AWS CloudTrail。透過監控 API 操作，您可以取得有用的安全性和操作資訊。如果您 [已啟用 Amazon S3 物件層級記錄](#)，RoleSessionName 會包含在請求者欄位中，做為 [AWS:Role Unique Identifier]/username.sessionid@server-id。如需 AWS Identity and Access Management (IAM) 角色唯一識別符的詳細資訊，請參閱 AWS Identity and Access Management 《使用者指南》中的 [唯一識別符](#)。

Important

的長度上限為 RoleSessionName 64 個字元。如果 RoleSessionName 較長，server-id 則會截斷。

啟用 Amazon S3 資料事件

若要追蹤透過在 Amazon S3 儲存貯體 AWS Transfer Family 上執行的檔案操作，您需要啟用這些儲存貯體的資料事件。資料事件提供物件層級 API 活動，對於追蹤 AWS Transfer Family 使用者執行的檔案上傳、下載和其他操作特別有用。

為您的 AWS Transfer Family 伺服器啟用 Amazon S3 資料事件：

1. 前往 <https://console.aws.amazon.com/cloudtrail/> 開啟 CloudTrail 主控台。
2. 在導覽窗格中，選擇線索，然後選取現有的線索或建立新的線索。
3. 在資料事件下，選擇編輯。
4. 針對資料事件類型，選取 S3。
5. 選擇要記錄資料事件的 Amazon S3 儲存貯體。您可以記錄所有儲存貯體的資料事件，或指定個別儲存貯體。
6. 選擇記錄讀取事件、寫入事件或兩者。
7. 選擇儲存變更。

啟用資料事件後，您可以在為 CloudTrail 追蹤設定的 Amazon S3 儲存貯體中存取這些日誌。日誌包含詳細資訊，例如執行動作的使用者、動作時間戳記、受影響的特定物件，以及協助追蹤透過執行之動作 `userId` 的 `onBehalfOf` 欄位 AWS Transfer Family。

建立伺服器的範例日誌項目

下列範例顯示示範 `CreateServer` 動作的 CloudTrail 日誌項目 (JSON 格式)。

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AAAA4FFF5HHHH6NNWWW: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"
}
```

資料存取日誌範例

當您為 CloudTrail 追蹤啟用 Amazon S3 資料事件時，您可以追蹤透過 執行的檔案操作 AWS Transfer Family。這些日誌可協助您監控誰存取了哪些資料、何時及如何存取。

成功存取資料的範例日誌項目

下列範例顯示透過 成功下載檔案操作的 CloudTrail 日誌項目 AWS Transfer Family。

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROEXAMPLEID:TransferSessionUser",
    "arn": "arn:aws:sts::123456789012:assumed-role/TransferS3AccessRole/TransferSessionUser",
    "accountId": "123456789012",
    "accessKeyId": "ASIAEXAMPLEKEY",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROEXAMPLEID",
        "arn": "arn:aws:iam::123456789012:role/TransferS3AccessRole",
        "accountId": "123456789012",
        "userName": "TransferS3AccessRole"
      },
      "attributes": {
        "creationDate": "2025-07-15T16:12:05Z",
        "mfaAuthenticated": "true"
      }
    },
    "invokedBy": "transfer.amazonaws.com"
  },
  "eventTime": "2025-07-15T16:15:22Z",
  "eventSource": "s3.amazonaws.com",
  "eventName": "GetObject",
```

```

"awsRegion": "us-east-1",
"sourceIPAddress": "transfer.amazonaws.com",
"userAgent": "transfer.amazonaws.com",
"requestParameters": {
  "bucketName": "my-transfer-bucket",
  "key": "users/john.doe/reports/quarterly-report-2025-Q2.pdf",
  "Host": "my-transfer-bucket.s3.amazonaws.com",
  "x-amz-request-payer": "requester"
},
"responseElements": null,
"additionalEventData": {
  "SignatureVersion": "SigV4",
  "CipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
  "bytesTransferredIn": 0,
  "bytesTransferredOut": 2458732,
  "x-amz-id-2":
"EXAMPLE123456789+abcdefghijklmnopqrstuvwxyABCDEFGHIJKLMNOPQRSTUVWXYZ="
},
"requestID": "EXAMPLE123456789",
"eventID": "example12-3456-7890-abcd-ef1234567890",
"readOnly": true,
"resources": [
  {
    "type": "AWS::S3::Object",
    "ARN": "arn:aws:s3:::my-transfer-bucket/users/john.doe/reports/quarterly-
report-2025-Q2.pdf"
  },
  {
    "accountId": "123456789012",
    "type": "AWS::S3::Bucket",
    "ARN": "arn:aws:s3:::my-transfer-bucket"
  }
],
"eventType": "AwsApiCall",
"managementEvent": false,
"recipientAccountId": "123456789012",
"eventCategory": "Data",
"requestParameters": {
  "x-amz-onBehalfOf": "john.doe.sessionid@s-abcd1234efgh5678"
}
}

```

在此範例中，請注意下列重要欄位：

- `eventName`：表示已執行的 S3 API 操作 (GetObject 用於檔案下載)。
- `requestParameters.bucketName` 和 `requestParameters.key`：顯示已存取的 S3 物件。
- `additionalEventData.bytesTransferredOut`：以位元組為單位顯示下載檔案的大小。
- `requestParameters.x-amz-onBehalfOf`：包含 AWS Transfer Family 使用者名稱和工作階段 ID，可讓您追蹤哪些 AWS Transfer Family 使用者執行動作。

`x-amz-onBehalfOf` 欄位特別重要，因為它會將 S3 API 呼叫連結回啟動動作的特定 AWS Transfer Family 使用者。此欄位遵循格式 `username.sessionid@server-id`，其中：

- `username` 是 AWS Transfer Family 使用者名稱。
- `sessionid` 是使用者工作階段的唯一識別符。
- `server-id` 是 AWS Transfer Family 伺服器的 ID。

常見的資料存取操作

透過 監控資料存取時 AWS Transfer Family，您通常會在 CloudTrail 日誌中看到下列 S3 API 操作：

AWS Transfer Family 日誌中的常見 S3 操作

S3 API 操作	AWS Transfer Family 動作	Description
GetObject	檔案下載	使用者從伺服器下載檔案
PutObject	檔案上傳	使用者將檔案上傳到伺服器
DeleteObject	檔案刪除	使用者從伺服器刪除檔案
ListObjects 或 ListObjectsv2	目錄清單	目錄中的使用者列出檔案
CopyObject	檔案複製	使用者在伺服器內複製檔案

透過監控 CloudTrail 日誌中的這些操作，您可以追蹤透過 AWS Transfer Family 伺服器執行的所有檔案活動，協助您符合合規要求並偵測未經授權的存取。

AWS Transfer Family 伺服器 Amazon CloudWatch 記錄

Amazon CloudWatch 是一項強大的監控和可觀測性服務，可讓您全面了解 AWS 資源，包括 AWS Transfer Family。

- 即時監控：CloudWatch 會即時監控 Transfer Family 資源和應用程式，讓您追蹤和分析其效能。
- 指標收集：CloudWatch 會為您的資源和應用程式收集和追蹤各種指標，這些是您可以測量和用於分析的變數。
- CloudWatch 首頁：CloudWatch 首頁會自動顯示 Transfer Family 和您使用之 AWS 其他服務的指標，提供監控資料的集中檢視。
- 自訂儀表板：您可以在 CloudWatch 中建立自訂儀表板，以顯示自訂應用程式的特定指標，以及您選擇監控的資源。
- 警示和通知：CloudWatch 可讓您建立警示，以監控指標，並在超過特定閾值時觸發通知或自動化動作。這對於監控 Transfer Family 伺服器中的檔案傳輸活動以及相應地擴展資源非常有用。
- 成本最佳化：您可以使用 CloudWatch 收集的資料來識別未充分利用的資源，並採取動作，例如停止或刪除執行個體，以最佳化您的成本。

整體而言，CloudWatch 中全面的監控功能使其成為管理和最佳化 Transfer Family 基礎設施及其上執行應用程式的重要工具。

Transfer Family Web 應用程式的 CloudWatch 記錄詳細資訊可在 [中取得 Transfer Family Web 應用程式的 CloudTrail 記錄](#)。

Transfer Family 的 CloudWatch 記錄類型

Transfer Family 提供兩種將事件記錄到 CloudWatch 的方式：

- JSON 結構化日誌記錄
- 透過記錄角色記錄

對於 Transfer Family 伺服器，您可以選擇您偏好的記錄機制。對於連接器和工作流程，僅支援記錄角色。

JSON 結構化記錄

對於記錄伺服器事件，建議使用 JSON 結構化記錄。這可提供更全面的日誌格式，以啟用 CloudWatch 日誌查詢。對於這種類型的記錄，建立伺服器（或編輯伺服器記錄組態）之使用者的 IAM 政策必須包含下列許可：

- logs:CreateLogDelivery
- logs>DeleteLogDelivery
- logs:DescribeLogGroups
- logs:DescribeResourcePolicies
- logs:GetLogDelivery
- logs>ListLogDeliveries
- logs:PutResourcePolicy
- logs:UpdateLogDelivery

政策範例如下。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs>DeleteLogDelivery",
        "logs>ListLogDeliveries",
        "logs:PutResourcePolicy",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups"
      ],
      "Resource": "*"
    }
  ]
}
```

如需設定 JSON 結構化記錄的詳細資訊，請參閱 [建立、更新和檢視伺服器的記錄](#)。

記錄角色

若要記錄連接到伺服器的受管工作流程以及連接器的事件，您需要指定記錄角色。若要設定存取，您可以建立以資源為基礎的 IAM 政策和提供該存取資訊的 IAM 角色。以下是 AWS 帳戶可記錄伺服器事件的範例政策。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource": "arn:aws:logs:*:*:log-group:/aws/transfer/*"
    }
  ]
}
```

如需設定記錄角色以記錄工作流程事件的詳細資訊，請參閱 [管理工作流程的記錄](#)。

建立、更新和檢視伺服器的記錄

對於所有 AWS Transfer Family 伺服器，我們提供結構化記錄。建議您對所有新的和現有的 Transfer Family 伺服器使用結構化記錄。使用結構化記錄的優勢包括：

- 以結構化 JSON 格式接收日誌。
- 使用 Amazon CloudWatch Logs Insights 查詢您的日誌，自動探索 JSON 格式欄位。
- 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、視覺化和儀表板，以追蹤用量和效能資料。

若要啟用連接到伺服器的工作流程記錄，您必須使用記錄角色。

 Note

當您新增記錄角色時，記錄群組一律為 `/aws/transfer/your-serverID`，且無法變更。這表示，除非您將結構化伺服器日誌傳送至相同的群組，否則您會記錄到兩個不同的記錄群組。如果您知道要將工作流程與伺服器建立關聯，因此需要新增記錄角色，您可以設定結構化記錄以記錄到預設日誌群組 `/aws/transfer/your-serverID`。若要修改您的記錄群組，請參閱 AWS Transfer Family API 參考中的 [StructuredLogDestinations](#)。

如果您使用 Transfer Family 主控台建立新伺服器，預設會啟用記錄。建立伺服器之後，您可以使用 `UpdateServer` API 操作來變更記錄組態。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 操作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，日誌會傳送到名稱中包含伺服器 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到這個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，除非工作流程連接到伺服器。
- 對於您在主控台中建立的新伺服器，沒有記錄不是一個選項。
- 現有的伺服器可以隨時透過主控台啟用結構化 JSON 記錄。
- 透過主控台啟用結構化 JSON 記錄會停用現有的記錄方法，以免向客戶重複收費。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 記錄，您稍後無法透過主控台將其停用。
- 如果您啟用結構化 JSON 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，且已透過 API 啟用這兩種記錄類型，則無法透過主控台編輯記錄角色。例外情況是，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。

使用 API 或 SDK 建立和編輯伺服器的記錄考量

- 如果您透過 API 建立新伺服器，您可以設定記錄或兩種類型，或選擇不記錄。

- 對於現有的伺服器，可隨時啟用和停用結構化 JSON 記錄。
- 您可以隨時透過 API 變更日誌群組。
- 您可以隨時透過 API 變更記錄角色。

若要啟用結構化記錄，您必須使用下列許可登入 帳戶

- logs:CreateLogDelivery
- logs>DeleteLogDelivery
- logs:DescribeLogGroups
- logs:DescribeResourcePolicies
- logs:GetLogDelivery
- logs:ListLogDeliveries
- logs:PutResourcePolicy
- logs:UpdateLogDelivery

範例政策可在 區段中取得[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

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 [CloudWatch Logs 中建立日誌群組](#)。

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

當您選擇使用結構化 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的 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謹慎傳輸檔案，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。

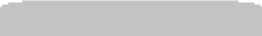
Edit additional details

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.

- 伺服器已啟用結構式 JSON 記錄，也已指定記錄角色。

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

Logging Role [Info](#)
 Select an existing role from your account

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

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 -

- 這兩種記錄類型（記錄角色和結構化 JSON 記錄）都已啟用。

Additional details

Edit

Log group /aws/transfer/s-[redacted]	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-[redacted]	Workflow for partial uploads -	TLS session resumption -
Security Policy Info TransferSecurityPolicy-2020-06	Managed workflows execution role transfer-workflows-[redacted]	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。您可以檢視前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 指標如中所述[使用 Transfer Family 伺服器的 CloudWatch 指標](#)。

檢視工作流程的 Amazon CloudWatch logs

1. 在 <https://console.aws.amazon.com/cloudwatch/> 開啟 Amazon CloudWatch 主控台。
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. 選擇對應至您伺服器的日誌群組。

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。
 - 一個用於為您的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 位數英數識別符是虛構的。您在 Amazon CloudWatch 中看到的值不同。

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 的範例日誌串流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": "amzn-s3-demo-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": "amzn-s3-demo-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，您可以建立以資源為基礎的 IAM 政策和提供該存取資訊的 IAM 角色。

若要啟用 Amazon CloudWatch 記錄，請先建立啟用 CloudWatch 記錄的 IAM 政策。然後，您可以建立 IAM 角色，並將政策連接到該角色。您可以在[建立伺服器](#)或[編輯現有伺服器](#)時執行此操作。如需 CloudWatch 的詳細資訊，請參閱[什麼是 Amazon CloudWatch？](#) [什麼是 Amazon CloudWatch logs？](#) Amazon CloudWatch 使用者指南中的。

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": "*"
}
]
}
```

在上述範例政策中，對於 **Resource**，將 *region-id* 和 取代 **AWS ##** 為您的值。例如
"Resource": "arn:aws::logs:us-east-1:111122223333:log-group:/aws/transfer/*"

然後，您可以建立角色並連接您建立的 CloudWatch Logs 政策。

建立 IAM 角色並連接政策

1. 在導覽窗格中，選擇角色，然後選擇建立角色。

在建立角色頁面上，確定已選擇 AWS 服務。

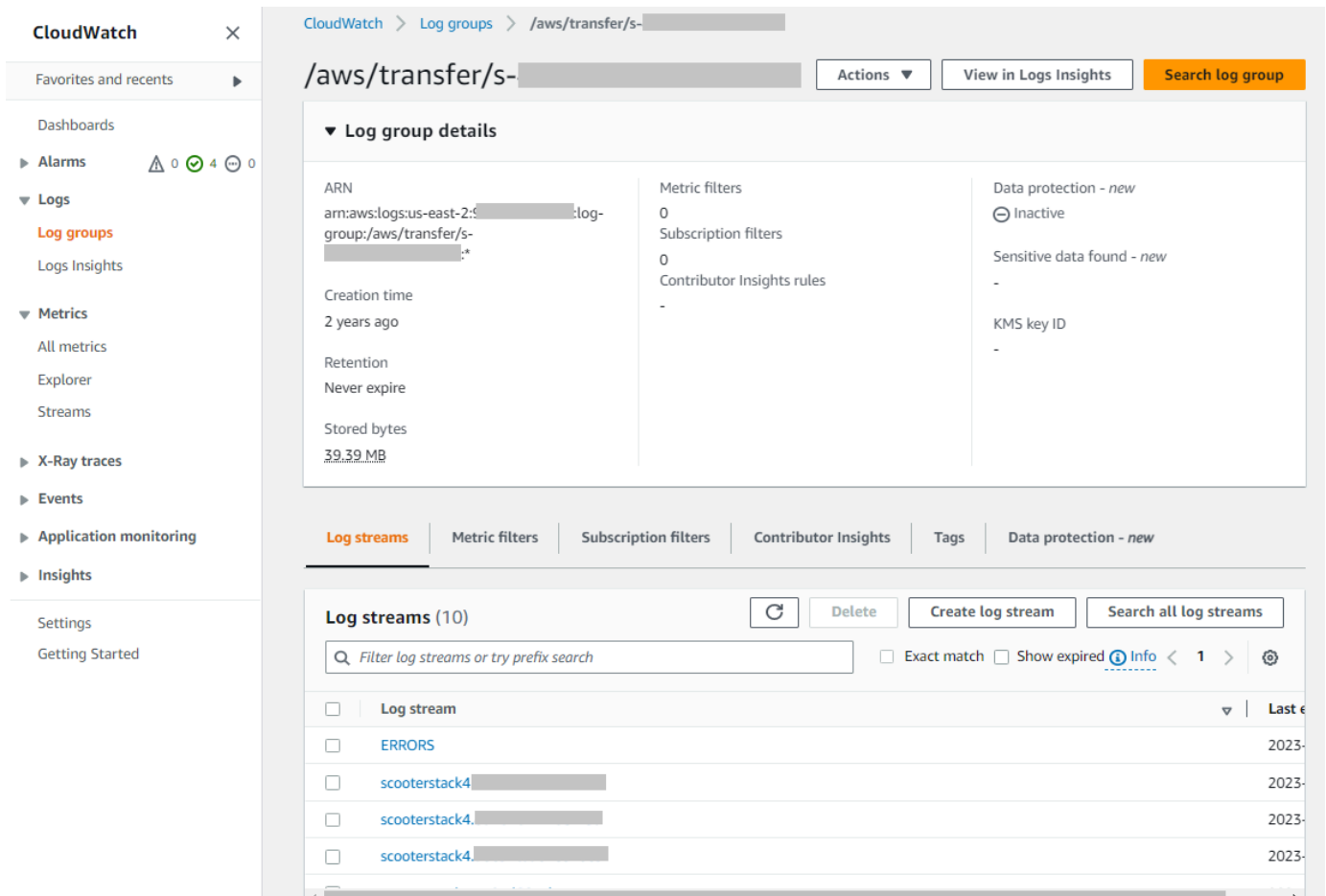
2. 從服務清單選擇 Transfer (傳輸)，然後選擇 Next: Permissions (下一步：許可)。這會在 AWS Transfer Family 和 IAM 角色之間建立信任關係。此外，新增 `aws:SourceAccount` 和 `aws:SourceArn` 條件金鑰，以保護自己免受混淆代理人問題的影響。如需詳細資訊，請參閱下列文件：
 - 與 建立信任關係的程序 AWS Transfer Family：[建立信任關係](#)
 - 混淆代理人問題的描述：[混淆代理人問題](#)
3. 在連接許可政策區段中，尋找並選擇您剛建立的 CloudWatch Logs 政策，然後選擇下一步：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. 隨即顯示所選伺服器的日誌群組。



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 ERRORS 的清單，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範例日誌串流。

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	<code>{"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": ""}}}}</code>
2023-03-21T14:12:02.850-04:00	<code>{</code> <code> "type": "StepStarted",</code> <code> "details": {</code> <code> "input": {</code> <code> "fileLocation": {</code> <code> "backingStore": "S3",</code> <code> "bucket": "",</code> <code> "key": "decrypt-user/test.json.gpg",</code> <code> "versionId": "",</code> <code> "etag": ""</code> <code> },</code> <code> },</code> <code> "stepType": "DECRYPT",</code> <code> "stepName": "decrypt-step"</code> <code> },</code> <code> "workflowId": "w-",</code> <code> "executionId": "",</code> <code> "transferDetails": {</code> <code> "serverId": "s-",</code> <code> "username": "decrypt-user",</code> <code> "sessionId": ""</code> <code> }</code> <code>}</code>
2023-03-21T14:12:03.464-04:00	<code>{"type": "StepCompleted", "details": {"output": {}, "stepType": "DECRYPT", "stepName": "decrypt-step", "workflowId": "w-"}}</code>

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,
});
```

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 操作記錄到 S3 存取日誌

Note

本節不適用於 Transfer Family Web 應用程式。

如果您[使用 Amazon S3 存取日誌來識別代表您的檔案傳輸使用者提出的 S3 請求](#)，RoleSessionName 則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。格式為 [AWS:Role Unique Identifier]/username.sessionid@server-id，且包含在申請者欄位中。例如，以下是已複製到 S3 儲存貯體的檔案的 S3 存取日誌中請求者範例欄位的內容。S3

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

在上方的申請者欄位中，會顯示名為的 IAM 角色IamRoleName。如需 IAM 角色唯一識別符的詳細資訊，請參閱AWS Identity and Access Management 《使用者指南》中的[唯一識別符](#)。

限制混淆代理人問題的範例

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 中，跨服務模擬可能會導致混淆代理人問題。如需詳細資訊，請參閱[預防跨服務混淆代理人](#)。

Note

在下列範例中，將每個#####取代為您自己的資訊。
在這些範例中，如果您的伺服器沒有連接任何工作流程，您可以移除工作流程的 ARN 詳細資訊。

下列範例記錄/呼叫政策允許帳戶中的任何伺服器（和工作流程）擔任該角色。

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

```

    "Sid": "AllowAllServersWithWorkflowAttached",
    "Effect": "Allow",
    "Principal": {
      "Service": "transfer.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "111122223333"
      },
      "ArnLike": {
        "aws:SourceArn": [
          "arn:aws:transfer:us-west-2:111122223333:server/*",
          "arn:aws:transfer:us-west-2:111122223333:workflow/*"
        ]
      }
    }
  }
]
}

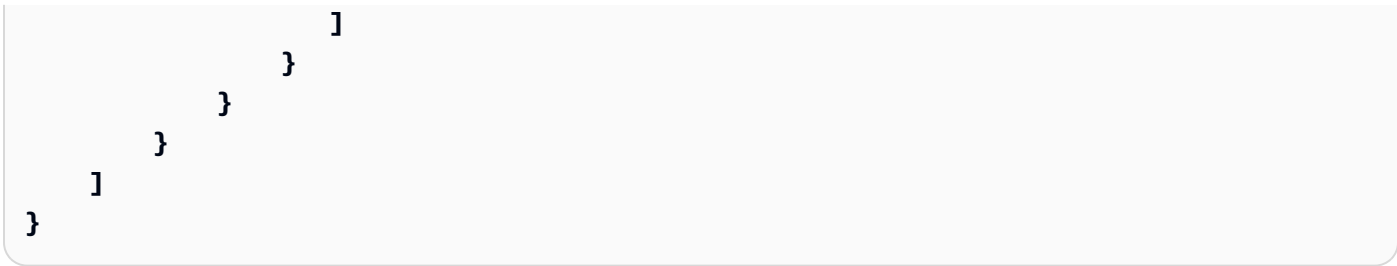
```

下列範例記錄/叫用政策允許特定伺服器（和 workflow）擔任該角色。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSpecificServerWithWorkflowAttached",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333"
        },
        "ArnEquals": {
          "aws:SourceArn": [
            "arn:aws:transfer:us-west-2:111122223333:server/server-id",
            "arn:aws:transfer:us-west-2:111122223333:workflow/workflow-
id"

```

Transfer 系列適用的 CloudWatch 日誌結構

本主題說明 Transfer Family 日誌中填入的欄位：適用於 JSON 結構化日誌項目和舊版日誌項目。

主題

- [Transfer Family 的 JSON 結構化日誌](#)
- [Transfer Family 的舊版日誌](#)

Transfer Family 的 JSON 結構化日誌

下表包含 Transfer Family SFTP/FTP/FTPS 動作的日誌項目欄位詳細資訊，採用新的 JSON 結構化日誌格式。

欄位	Description	範例項目
activity-type	The action by the user	可用的活動類型如下：AUTH_FAIL、CONNECTED、DISCONNECTED、ERROREXIT_REASON、CLOSE、CREATE_SYMLINK、DELETE、MKDIR、OPENPAUSE、RENAME、RMDIR、SETSTIME_FAILURE 。
bytes-in	Number of bytes uploaded by the user	29238420042
bytes-out	Number of bytes downloaded by the user	23094032490328

欄位	Description	範例項目
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	<##>
method	The authentication method	publickey
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	/amzn-s3-demo-bucket/test-file-1.pdf
ssh-public-key	The public key body for the user that is connecting	AAAAC3NzaC1lZDI1NT E5AAAAIA9OY0qV6XYV HaaOiWAcj2spDJVbgj rqDPY4pxd6GnHl

欄位	Description	範例項目
ssh-public-key-fingerprint	列出使用者金鑰時，服務受管使用者在主控台中顯示的公有金鑰指紋。	SHA256:BY3gNMHwTfj d4n2VuT4pTyLOk82zW Zj4KEYEu7y4r/0
 Note 在 主控台中，指紋會以填補字元（如果有的話）顯示：從 0 到 3 等號 (=) 的結尾。在日誌項目中，此填補會從輸出中分割。		
ssh-public-key-type	Type of public key: Transfer Family supports RSA-, ECDSA-, and ED25519-formatted keys	ssh-ed25519
resource-arn	A system-assigned, unique identifier for a specific resource (for example, a server)	arn : aws : transfer : ap-northeast-1 : 12346789012 : server/s-1234567890akeu2js2
role	The IAM role of the user	arn : aws : iam : : 0293883675 : role/testuser-role
session-id	A system-assigned, unique identifier for a single session	9ca9a0e1cec6ad9d
source-ip	Client IP address	18.323.0.129
user	The end user's username	myname192

欄位	Description	範例項目
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 的舊版日誌

下表包含各種 Transfer Family 動作的日誌項目詳細資訊。

Note

這些項目不是新的 JSON 結構化日誌格式。

下表包含各種 Transfer Family 動作的日誌項目詳細資訊，採用新的 JSON 結構化日誌格式。

Action	Amazon CloudWatch Logs 中的對應日誌
身分驗證失敗	ERRORS AUTH_FAILURE Method=publickey User=lhr Message="RSA SHA256 : Lfz3R2nmLY4raK+b7Rb1rSvUIbAE+a+Hxg0c7l1JIZ0" SourceIP=3.8.172.211
COPY/TAG/DELETE/DECRYPT 工作流程	<pre>{ "type": "StepStarted", "details": { "input": { "fileLocation": { "backingStore": "EFS", "filesystemId": "fs-12345678", "path": "/lhr/regex.py" } }, "stepType": "TAG", "stepName": "successful_tag_step", "workflowId": "w-1111aaaaa2222bb3", "executionId": "81234abcd-1234-efgh-5678-ijklmnopqr90", "transferDetails": { "serverId": "s-1234abcd557", "userId": "user", "sessionId": "1234567890" } } }</pre>

Action	Amazon CloudWatch Logs 中的對應日誌
自訂步驟工作流程	<pre>{ "type": "CustomStepInvoked", "details": { "output": { "token": "MzM4Mjg5YWUtYT EzMy00YjIzLWI3OGMtYzU4OGI2ZjQyMzE5" } , "stepType": "CUSTOM", "stepName": "efs- s3_copy_2", "workflowId": "w-9283e49 d33297c3f7", "executionId": "1234abcd-1234- efgh-5678-ijklmnop90", "transferDetails": { "1"- serverId": "1"1"sessionId1234567890</pre>
刪除	<pre>lhr.33a8fb495ffb383b DELETE 路徑=/bucket/ user/123.jpg</pre>
下載	<pre>lhr.33a8fb495ffb383b OPEN Path=/bucket/user/ 123.jpg Mode=READ llhr.33a8fb495ffb383b CLOSE 路徑=/bucket/ user/123.jpg BytesOut=3618546</pre>
登入/登出	<pre>user.914984e553bcd6b6 CONNECTED SourceIP=1.22.111.222 User=lhr HomeDir=L OGICAL Client=SSH-2.0-OpenSSH_7.4 Role=arn : aws : : iam : : 123456789012 : role/sftp-s3-access user.914984e553bcd6b6 DISCONNECTED</pre>
重新命名	<pre>lhr.33a8fb495ffb383b RENAME 路徑=/bucket/ user/lambo.png NewPath=/bucket/user/ferrari.png</pre>

Action	Amazon CloudWatch Logs 中的對應日誌
工作流程錯誤日誌範例	<pre>{"type": "StepErrored", "details": {"errorType": "BAD_REQUEST", "errorMessage": "Cannot tag Efs file", "stepType": "TAG", "stepName": "successful_tag_step"}, "workflowId": "w-1234abcd5678efghi", "executionId": "81234abcd-1234-efgh-5678-ijklmnopqr90", "transferDetails": {"serverId": "s-1234abcd5678efghi", "username": "l ldefchr": "1234567890ssessionId"}}</pre>
Symlinks	<pre>lhr.eb49cf7b8651e6d5 CREATE_SYMLINK LinkPath=/fs-12345678/lhr/pqr.jpg TargetPath=abc.jpg</pre>
上傳	<pre>lhr.33a8fb495ffb383b OPEN Path=/bucket/user/123.jpg Mode=CREATE TRUNCATE WRITE lhr.33a8fb495ffb383b CLOSE 路徑=/bucket/user/123.jpg BytesIn=3618546</pre>

Action	Amazon CloudWatch Logs 中的對應日誌
工作流程	<pre>{ "type": "ExecutionStarted", "details": { "input": { "initialFileLocation": { "backingStore": "EFS", "filesystemId": "fs-12345678", "path": "/lhr/regex.py" } }, "workflowId": "w-1111aaaa2222bbb3", "executionId": "1234abcd-1234-efgh-5678-ijklmno", "transferDetails": { "serverId": "s-zz-zz111aaa2223", "username": "lhr", "sessionId": "1234567890" } } }</pre> <pre>{ "type": "StepStarted", "details": { "input": { "fileLocation": { "backingStore": "EFS", "filesystemId": "fs-12345678", "path": "/lhr/regex.py" } }, "stepType": "CUSTOM", "stepName": "efs-s3_copy_2", "workflowId": "w-9283e49d3297c3f7", "executionId": "1234abcd-1234-efgh-5678-ijklmno", "transferDetails": { "serverId": "s-189db45d2", "sessionId": "1234567890" } } }</pre>

CloudWatch 日誌項目範例

本主題提供範例日誌項目。

主題

- [轉移工作階段日誌項目範例](#)
- [SFTP 連接器的範例日誌項目](#)
- [VPC Lattice 連接器的範例日誌項目](#)
- [金鑰交換演算法失敗的範例日誌項目](#)

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 伺服器的 SFTP 使用者。

```
{
  "role": "arn:aws:iam::500655546075:role/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": "/test/log-me",
  "ssh-public-key":
"AAAAC3NzaC1lZDI1NTE5AAAAIA90Y0qV6XYVHaa0iWAcj2spDJVbgjrqpDPY4pxd6GnH1",
  "ssh-public-key-fingerprint": "SHA256:BY3gNMHwTfjd4n2VuT4pTyL0k82zWZj4KEYEu7y4r/0",
  "ssh-public-key-type": "ssh-ed25519",
  "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": "/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 工作階段的連線。

```
{
  "path": "/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"
}
```

Note

可用的活動類型如

下：AUTH_FAILURE、CONNECTED、DISCONNECTED、ERROR_EXIT_REASON、CLOSE、CREATE_SYM

SFTP 連接器的範例日誌項目

本節包含成功和失敗傳輸的範例日誌。日誌會產生到名為 `/aws/transfer/connector-id` 的日誌群組，其中 *connector-id* 是 SFTP 連接器的識別符。當您執行 `StartFileTransfer` 或 `StartDirectoryListing` 命令時，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:account-id:connector/connector-id",
  "local-directory-path": "/connectors-localbucket",
  "bytes": 514,
  "egress-type": "SERVICE_MANAGED"
}
```

此日誌項目適用於逾時的傳輸，因此無法成功完成。

```
{
  "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:account-id:connector/connector-id",
  "local-directory-path": "/connectors-localbucket",
  "egress-type": "SERVICE_MANAGED"
}
```

此日誌項目適用於成功的 SEND 操作。

```
{
  "operation": "SEND",
  "timestamp": "2024-04-24T18:16:12.513207284Z",
  "connector-id": "connector-id",
  "transfer-id": "transfer-id",
  "file-transfer-id": "transfer-id/file-transfer-id",
  "url": "sftp://server-id.server.transfer.us-east-1.amazonaws.com",
  "file-path": "/amzn-s3-demo-bucket/my-test-folder/connector-metrics-us-east-1-2024-01-02.csv",
  "status-code": "COMPLETED",
  "start-time": "2024-04-24T18:16:12.295235884Z",
  "end-time": "2024-04-24T18:16:12.461840732Z",
  "account-id": "255443218509",
  "connector-arn": "arn:aws:transfer:us-east-1:account-id:connector/connector-id",
  "bytes": 275,
  "egress-type": "SERVICE_MANAGED"
}
```

先前日誌範例中某些索引鍵欄位的描述。

- `timestamp` 代表日誌新增至 CloudWatch 的時間。 `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 操作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，`file-transfer-id` 的初始部分與 `transfer-id` 相同。

VPC Lattice 連接器的範例日誌項目

本節包含 VPC Lattice 連接器的範例日誌。對於 VPC Lattice 連接器，日誌包含提供連接器組態和網路設定相關資訊的其他欄位。

此日誌項目適用於成功完成的 VPC Lattice 連接器 SEND 操作。

```
{
  "operation": "SEND",
  "timestamp": "2025-09-05T14:20:19.577192454Z",
  "connector-id": "connector-id",
  "transfer-id": "transfer-id",
  "file-transfer-id": "transfer-id/file-transfer-id",
  "file-path": ""/amzn-s3-demo-bucket/my-test-folder/connector-vpc-lattice-us-east-1-2025-03-22.csv"",
  "status-code": "COMPLETED",
  "start-time": "2025-09-05T14:20:19.434072509Z",
  "end-time": "2025-09-05T14:20:19.481453346Z",
  "account-id": "account-id",
  "connector-arn": "arn:aws:transfer:us-east-1:account-id:connector/connector-id",
  "remote-directory-path": "/test-bucket/test-folder/",
  "bytes": 262,
  "egress-type": "VPC_LATTICE",
  "vpc-lattice-resource-configuration-arn": "arn:aws:vpc-lattice:us-east-1:account-id:resourceconfiguration/resource-configuration-arn-id",
  "vpc-lattice-port-number": 22
}
```

VPC Lattice 連接器日誌包含下列其他欄位：

- `egress-type` - 連接器的輸出組態類型
- `vpc-lattice-resource-configuration-arn` - 定義目標 SFTP 伺服器位置的 VPC Lattice 資源組態 ARN
- `vpc-lattice-port-number` - 透過 VPC Lattice 連線至 SFTP 伺服器的連接埠號碼

金鑰交換演算法失敗的範例日誌項目

本節包含金鑰交換演算法 (KEX) 失敗的範例日誌。這些是結構化日誌之 ERRORS 日誌串流中的範例。

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 KEX 不相符的範例。

```
{
  "activity-type": "KEX_FAILURE",
  "source-ip": "999.999.999.999",
  "resource-arn": "arn:aws:transfer:us-east-1:999999999999:server/
s-999999999999999999",
  "message": "no matching key exchange method found",
  "kex": "diffie-hellman-group1-sha1,diffie-hellman-group14-sha1,diffie-hellman-
group14-sha256"
}
```

使用 Transfer Family 伺服器的 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，請參閱在 [主控台中監控用量](#)

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 CloudWatch 的一組按時間排序的資料點。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	Description
AWS/Transfer	BytesIn	傳輸到伺服器的位元組總數。 報告條件： - 對於 SFTP/FTP/FTPS：在與 Transfer Family 伺服器建立連線時，每 5 分鐘發出一個。如果期間內沒有傳輸任何檔案或位元組，則會發出「0」。 - 對於 AS2：當客戶在其 AS2 伺服器中收到訊息，並在傳入訊息處理完成後立即發出 單位：計數 期間：5 分鐘
	BytesOut	從伺服器傳輸的位元組總數。 報告條件： - 對於 SFTP/FTP/FTPS：在與 Transfer Family 伺服器建立連線時，每 5 分鐘發出一個。如果期間內沒有傳輸任何檔案或位元組，則會發出「0」。 - 對於 AS2：當客戶 StartFileTransfer 從其 AS2 連接器呼叫，並在傳出訊息完成處理後立即發出時。 單位：計數 期間：5 分鐘
	FilesIn	傳輸到伺服器的檔案總數。

命名空間	指標	Description
		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。 報告條件： - 對於 SFTP/FTP/FTPS：在與 Transfer Family 伺服器建立連線時，每 5 分鐘發出一個。如果期間內沒有傳輸任何檔案或位元組，則會發出「0」。 - 對於 AS2：當客戶在其 AS2 伺服器中收到訊息，並在傳入訊息處理完成時立即發出。 單位：計數 期間：5 分鐘
	FilesOut	從伺服器傳輸的檔案總數。 報告條件： - 對於 SFTP/FTP/FTPS：在與 Transfer Family 伺服器建立連線時，每 5 分鐘發出一個。如果期間內沒有傳輸任何檔案或位元組，則會發出「0」。 - 對於 AS2：當客戶 StartFileTransfer 從其 AS2 連接器呼叫，並在傳出訊息完成處理後立即發出時。 單位：計數 期間：5 分鐘
	InboundMessage	從交易合作夥伴成功接收的 AS2 訊息總數。 報告條件：當客戶在其 AS2 伺服器中收到訊息，並在傳入訊息成功完成處理時立即發出 單位：計數 期間：5 分鐘

命名空間	指標	Description
	InboundFailedMessage	未成功從交易合作夥伴收到的 AS2 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。 報告條件：當客戶在其 AS2 伺服器中收到訊息，並在傳入訊息處理失敗時立即發出 單位：計數 期間：5 分鐘
	OnUploadExecutionsStarted	在伺服器上啟動的工作流程執行總數。 報告條件：每次執行啟動時觸發 單位：計數 Period：1 分鐘
	OnUploadExecutionsSuccess	在伺服器上成功執行工作流程的總數。 報告條件：每次執行成功完成時觸發 單位：計數 Period：1 分鐘
	OnUploadExecutionsFailed	伺服器上失敗的工作流程執行總數。 報告條件：每次執行未成功完成時觸發 單位：計數 Period：1 分鐘

命名空間	指標	Description
	OutboundMessage	成功傳送給交易合作夥伴的 AS2 訊息總數。 報告條件：當客戶StartFileTransfer 從 AS2 連接器呼叫，並在外撥訊息成功完成處理時立即發出 單位：計數 期間：5 分鐘
	OutboundFailedMessage	未成功傳送給交易合作夥伴的 AS2 訊息總數。 報告條件：當客戶StartFileTransfer 從 AS2 連接器呼叫，並在傳出訊息處理失敗時立即發出 單位：計數 期間：5 分鐘

Transfer 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	Description
ServerId	伺服器的唯一 ID。
ConnectorId	連接器的唯一 ID。用於 AS2、用於 OutboundMessage 和 OutboundFailedMessage

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](#) 來設定各種交付管道。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、[聊天應用程式中的 Amazon Q Developer](#) 聊天通知或 [AWS Console Mobile Application](#) 推送通知。您也可以可以在[主控台通知中心](#)查看通知。使用者通知支援彙總，可減少您在特定事件期間收到的通知數量。

如需詳細資訊，請參閱[使用 AWS Transfer Family 受管工作流程的自訂檔案交付通知](#)部落格文章，以及[什麼是 AWS 使用者通知？](#) AWS 使用者通知 《使用者指南》中的。

使用查詢篩選日誌項目

您可以使用 CloudWatch 查詢來篩選和識別 Transfer Family 的日誌項目。本節包含一些範例。

1. 登入 AWS 管理主控台，並在 <https://console.aws.amazon.com/cloudwatch/> 開啟 CloudWatch 主控台。
2. 您可以建立查詢或規則。
 - 若要建立 Logs Insights 查詢，請從左側導覽面板中選擇 Logs Insights，然後輸入查詢的詳細資訊。
 - 若要建立 Contributor Insights 規則，請從左側導覽面板中選擇 Insights > Contributor Insights，然後輸入規則的詳細資訊。
3. 執行您建立的查詢或規則。

檢視最佳身分驗證失敗參與者

在您的結構化日誌中，身分驗證失敗日誌項目如下所示：

```
{
  "method":"password",
  "activity-type":"AUTH_FAILURE",
  "source-ip":"999.999.999.999",
  "resource-arn":"arn:aws:transfer:us-east-1:999999999999:server/s-0123456789abcdef",
  "message":"Invalid user name or password",
  "user":"exampleUser"
}
```

執行下列查詢，以檢視身分驗證失敗的主要參與者。

```
filter @logStream = 'ERRORS'
| filter `activity-type` = 'AUTH_FAILURE'
| stats count() as AuthFailures by user, method
```

```
| sort by AuthFailures desc
| limit 10
```

您可以建立 CloudWatch Contributors Insights 規則來檢視身分驗證失敗，而不是使用 CloudWatch Logs Insights CloudWatch。建立類似下列的規則。

```
{
  "AggregateOn": "Count",
  "Contribution": {
    "Filters": [
      {
        "Match": "$.activity-type",
        "In": [
          "AUTH_FAILURE"
        ]
      }
    ],
    "Keys": [
      "$.user"
    ]
  },
  "LogFormat": "JSON",
  "Schema": {
    "Name": "CloudWatchLogRule",
    "Version": 1
  },
  "LogGroupARNs": [
    "arn:aws:logs:us-east-1:999999999999:log-group:/customer/structured_logs"
  ]
}
```

檢視開啟檔案的日誌項目

在您的結構化日誌中，檔案讀取日誌項目看起來類似如下：

```
{
  "mode": "READ",
  "path": "/fs-0df669c89d9bf7f45/avtester/example",
  "activity-type": "OPEN",
  "resource-arn": "arn:aws:transfer:us-east-1:999999999999:server/s-0123456789abcdef",
  "session-id": "0049cd844c7536c06a89"
}
```

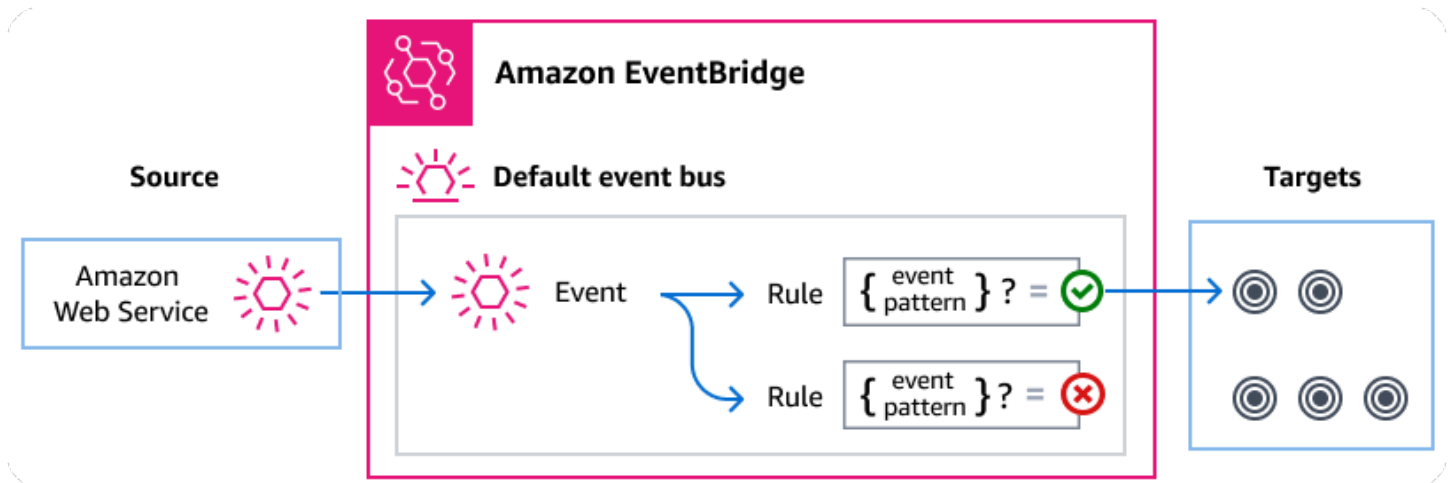
執行下列查詢，以檢視表示檔案已開啟的日誌項目。

```
filter `activity-type` = 'OPEN'  
| display @timestamp, @logStream, `session-id`, mode, path
```

使用 管理 Transfer Family 事件 Amazon EventBridge

Amazon EventBridge 是一種無伺服器服務，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。事件驅動型架構是一種透過發出和回應事件來建置鬆耦合軟體系統的方式。事件代表資源或環境中的變更。

如同許多 AWS 服務，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，以在事件到達時評估事件。每項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或持久性交付至指定的目標（請注意，某些事件可能會不按順序交付）。這些交付層級說明於 Amazon EventBridge Events Reference 中[AWS 服務事件的交付層級](#)。

- SFTP、FTPS 和 FTP 伺服器的伺服器層級事件會盡最大努力交付。
- SFTP 連接器事件會以持久的方式交付。
- AS2 事件會以持久的方式交付。

以下事件是由 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

下表列出 SFTP、FTPS 和 FTP 伺服器的事件，依事件類型組織。

檔案上傳和下載事件

事件詳細資訊類型	說明
FTP 伺服器檔案下載已完成	已成功下載 FTP 通訊協定的檔案。
FTP 伺服器檔案下載失敗	FTP 通訊協定嘗試下載檔案失敗。
FTP 伺服器檔案上傳已完成	已成功上傳 FTP 通訊協定的檔案。
FTP 伺服器檔案上傳失敗	FTP 通訊協定嘗試上傳檔案失敗。
FTPS 伺服器檔案下載已完成	已成功下載 FTPS 通訊協定的檔案。
FTPS 伺服器檔案下載失敗	FTPS 通訊協定嘗試下載檔案失敗。
FTPS 伺服器檔案上傳已完成	已成功上傳 FTPS 通訊協定的檔案。
FTPS 伺服器檔案上傳失敗	FTPS 通訊協定嘗試上傳檔案失敗。
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	SFTP 通訊協定嘗試下載檔案失敗。
SFTP 伺服器檔案上傳已完成	SFTP 通訊協定的檔案已成功上傳。

事件詳細資訊類型	說明
SFTP 伺服器檔案上傳失敗	SFTP 通訊協定的上傳檔案嘗試失敗。

其他檔案操作事件

事件詳細資訊類型	說明
FTP 伺服器目錄建立已完成	已成功為 FTP 通訊協定建立目錄。
FTP 伺服器目錄建立失敗	FTP 通訊協定嘗試建立目錄失敗。
FTP 伺服器目錄刪除已完成	已成功刪除 FTP 通訊協定的目錄。
FTP 伺服器目錄刪除失敗	FTP 通訊協定嘗試刪除目錄失敗。
FTP 伺服器檔案刪除已完成	已成功刪除 FTP 通訊協定的檔案。
FTP 伺服器檔案刪除失敗	FTP 通訊協定嘗試刪除檔案失敗。
FTP 伺服器檔案重新命名已完成	已成功重新命名 FTP 通訊協定的檔案。
FTP 伺服器檔案重新命名失敗	嘗試重新命名 FTP 通訊協定的檔案失敗。
FTPS 伺服器目錄建立已完成	已成功為 FTPS 通訊協定建立目錄。
FTPS 伺服器目錄建立失敗	FTPS 通訊協定嘗試建立目錄失敗。
FTPS 伺服器目錄刪除已完成	已成功刪除 FTPS 通訊協定的目錄。
FTPS 伺服器目錄刪除失敗	FTPS 通訊協定嘗試刪除目錄失敗。
FTPS 伺服器檔案刪除已完成	已成功刪除 FTPS 通訊協定的檔案。
FTPS 伺服器檔案刪除失敗	FTPS 通訊協定嘗試刪除檔案失敗。
FTPS 伺服器檔案重新命名已完成	已成功重新命名 FTPS 通訊協定的檔案。

事件詳細資訊類型	說明
FTPS 伺服器檔案重新命名失敗	FTPS 通訊協定嘗試重新命名檔案失敗。
SFTP 伺服器目錄建立已完成	已成功為 SFTP 通訊協定建立目錄。
SFTP 伺服器目錄建立失敗	SFTP 通訊協定嘗試建立目錄失敗。
已完成 SFTP 伺服器目錄刪除	SFTP 通訊協定的目錄已成功刪除。
SFTP 伺服器目錄刪除失敗	嘗試刪除 SFTP 通訊協定的目錄失敗。
SFTP 伺服器檔案刪除已完成	SFTP 通訊協定的檔案已成功刪除。
SFTP 伺服器檔案刪除失敗	嘗試刪除 SFTP 通訊協定的檔案失敗。
SFTP 伺服器檔案重新命名已完成	SFTP 通訊協定的檔案已成功重新命名。
SFTP 伺服器檔案重新命名失敗	嘗試重新命名 SFTP 通訊協定的檔案失敗。

SFTP 連接器事件

Note

這些事件會以耐久的層級交付至 EventBridge，如 Amazon EventBridge Events Reference 中[AWS 服務事件的交付層級](#)所述。

事件詳細資訊類型	說明
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	說明
SFTP 連接器檔案擷取失敗	從遠端 SFTP 伺服器到連接器的檔案傳輸失敗。
SFTP 連接器目錄清單已完成	開始檔案目錄，列出已成功完成的呼叫。
SFTP 連接器目錄清單失敗	失敗的啟動檔案目錄清單。
SFTP 連接器遠端移動已完成	檔案或目錄已在遠端伺服器上成功移動或重新命名。
SFTP 連接器遠端移動失敗	檔案或目錄無法在遠端伺服器上移動或重新命名。
SFTP 連接器遠端刪除已完成	檔案或目錄已成功在遠端伺服器上刪除。
SFTP 連接器遠端刪除失敗	檔案或目錄無法在遠端伺服器上刪除。

AS2 事件

Note

這些事件會以耐久的層級交付至 EventBridge，如 Amazon EventBridge Events Reference 中[AWS 服務事件的交付層級](#)所述。

事件詳細資訊類型	說明
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	AS2 訊息的承載已成功傳送。
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 AS2 訊息的訊息處置通知。
AS2 MDN 接收失敗	尚未收到 AS2 訊息的訊息處置通知。
AS2 MDN 傳送已完成	AS2 訊息的訊息處置通知已成功傳送。

事件詳細資訊類型	說明
AS2 MDN 傳送失敗	AS2 訊息的訊息處置通知無法傳送。

使用 EventBridge 規則傳送 Transfer Family 事件

如果您希望 EventBridge 預設事件匯流排將 Transfer Family 事件傳送至目標，您必須建立規則，其中包含符合所需 Transfer Family 事件中資料的事件模式。

在 Amazon EventBridge 中擷取 AWS Transfer Family 事件

1. 登入 AWS 管理主控台，並在 <https://console.aws.amazon.com/events/> 開啟 Amazon EventBridge 主控台。
2. 在導覽窗格中，選擇規則，然後選擇建立規則。
3. 輸入規則的描述性名稱，然後選擇性地輸入描述。
4. 針對規則類型，選取具有事件模式的規則，然後選擇下一步。
5. 在事件來源區段中，選取AWS事件或 EventBridge 合作夥伴事件。
6. 在建立方法區段中，選擇使用模式表單。
7. 在事件模式區段中，提供下列資訊。
 - a. 在事件來源欄位中，選擇 AWS 服務。
 - b. 針對AWS服務，選擇轉接。
 - c. 針對事件類型，選擇您要觸發規則的 Transfer Family 事件類型。

根據您的事件類型選擇，您可能會看到事件類型規格 1 區段。

- d. 如果您看到事件類型規格 1 區段，請選取您要擷取的特定事件（或選取任何事件以擷取所選事件類型的所有事件）。
 - e. （選用）使用事件模式編輯器來指定事件詳細資訊的篩選條件。
 - f. 選擇下一步。
8. 從選取目標中可用的選項中選擇目標。從下列可用的目標中進行選擇。
 - AWS 服務。熱門選項是用於無伺服器運算的 Lambda 函數、用於訊息處理的 Amazon SQS 佇列、用於通知的 Amazon SNS 主題，以及 AWS Step Functions 用於協調工作流程。
 - EventBridge API 目的地。如果您想要將事件傳送至外部的 HTTP 端點 AWS，您可以使用 API 目的地做為目標。

- EventBridge 事件匯流排。您可以將事件傳送至相同帳戶和區域中的另一個事件匯流排，或不同帳戶或區域中的事件匯流排。

如需建立事件匯流排規則的完整說明，請參閱《Amazon EventBridge 使用者指南》中的[建立對事件做出反應的規則](#)。

如需選取目標的說明，請參閱《Amazon EventBridge 使用者指南》中的[選取目標](#)。

9. 為您的目標設定任何其他選項，然後選擇下一步。
10. (選用) 將標籤新增至規則，然後選擇下一步。
11. 在檢閱和建立畫面中，如果一切看起來都不錯，請選擇建立規則。

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` 屬性，其中包含要比對的事件類型陣列。
- (選用) `detail` 屬性，其中包含要比對的任何其他事件資料。

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：

```
{
  "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](#)。

在 中測試 Transfer Family 事件的事件模式 EventBridge

您可以使用 EventBridge 沙盒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 不需要任何其他許可即可將事件交付至 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。

- 如需事件匯流排如何運作的詳細資訊，請參閱[Amazon EventBridge 事件匯流排](#)。

- 如需事件結構的資訊，請參閱[事件](#)。
- 如需建構事件模式 EventBridge 以讓 在比對事件與規則時使用的資訊，請參閱[事件模式](#)。
- 如需建立規則以指定哪些事件 EventBridge 程序的詳細資訊，請參閱[規則](#)。
- 如需如何指定傳送 EventBridge 相符事件的服務或其他目的地的資訊，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做為事件來源 AWS 的服務、產生事件的時間、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。下列參考定義各種 Transfer Family 事件的詳細資訊欄位。

當您使用 EventBridge 選取和管理 Transfer Family 事件時，請考慮下列事項：

- 來自 的所有事件的 source 欄位 Transfer Family 都設定為 `aws.transfer`。
- detail-type 欄位指定事件類型。

例如 FTP Server File Download Completed。

- detail 欄位包含該特定事件的特定資料。

如需有關建構事件模式以讓規則符合 Transfer Family 事件的資訊，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 伺服器目錄建立已完成
- FTP 伺服器目錄建立失敗
- FTP 伺服器目錄刪除已完成
- FTP 伺服器目錄刪除失敗
- FTP 伺服器檔案刪除已完成
- FTP 伺服器檔案刪除失敗
- FTP 伺服器檔案下載已完成
- FTP 伺服器檔案下載失敗
- FTP 伺服器檔案重新命名已完成
- FTP 伺服器檔案重新命名失敗
- FTP 伺服器檔案上傳已完成
- FTP 伺服器檔案上傳失敗
- FTPS 伺服器目錄建立已完成
- FTPS 伺服器目錄建立失敗
- FTPS 伺服器目錄刪除已完成
- FTPS 伺服器目錄刪除失敗
- FTPS 伺服器檔案刪除已完成
- FTPS 伺服器檔案刪除失敗
- FTPS 伺服器檔案下載已完成
- FTPS 伺服器檔案下載失敗
- FTPS 伺服器檔案重新命名已完成
- FTPS 伺服器檔案重新命名失敗
- FTPS 伺服器檔案上傳已完成
- FTPS 伺服器檔案上傳失敗
- SFTP 伺服器目錄建立已完成
- SFTP 伺服器目錄建立失敗
- SFTP 伺服器目錄刪除已完成
- SFTP 伺服器目錄刪除失敗
- 已完成 SFTP 伺服器檔案刪除
- SFTP 伺服器檔案刪除失敗

- SFTP 伺服器檔案下載已完成
- SFTP 伺服器檔案下載失敗
- SFTP 伺服器檔案重新命名已完成
- SFTP 伺服器檔案重新命名失敗
- SFTP 伺服器檔案上傳已完成
- SFTP 伺服器檔案上傳失敗

以下包含 `source` 和 `detail-type` 欄位，因為它們包含 Transfer Family 事件的特定值。如需所有事件中包含的其他中繼資料欄位的定義，請參閱 Amazon EventBridge 《使用者指南》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",
    "original-file-path" : "string",
    "renamed-file-path" : "string",
    "directory-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 SFTP、FTPS 或 FTP 伺服器事件名稱。

source

識別產生事件的服務。對於 Transfer Family 事件，此值為 `aws.transfer`。

detail

包含事件相關資訊的 JSON 物件。產生事件的服務會決定此欄位的內容。

對於此事件，資料包含下列項目：

failure-code

轉移失敗原因的類別。數值: `PARTIAL_UPLOAD` | `PARTIAL_DOWNLOAD` | `UNKNOWN_ERROR`

status-code

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，則為傳輸失敗原因的詳細資訊。

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

正在傳輸、刪除或以其他方式操作之檔案的路徑。

original-file-path

對於檔案重新命名事件，在重新命名之前檔案的原始路徑。

`renamed-file-path`

對於檔案重新命名事件，是重新命名後檔案的新路徑。

`directory-path`

對於目錄建立和刪除事件，則為目錄的路徑。

`server-id`

Transfer Family 伺服器的唯一 ID。

`username`

正在執行傳輸的使用者。

`session-id`

傳輸工作階段的唯一識別符。

`start-timestamp`

為了成功傳輸，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 伺服器檔案上傳完成範例事件

下列範例顯示在 FTP 伺服器上成功完成上傳的事件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": "/amzn-s3-demo-bucket/test/1mb_file",
    "server-id": "s-1111aaaa2222bbbb3",
    "username": "test",
    "session-id": "event-ID",
    "start-timestamp": "2024-01-29T16:31:42.462088327Z"
  }
}

```

Example SFTP 伺服器檔案刪除已完成的範例事件

下列範例顯示 SFTP 伺服器上檔案已成功刪除的事件。

```

{

```

```
{
  "version": "0",
  "id": "event-ID",
  "detail-type": "SFTP Server File Delete Completed",
  "source": "aws.transfer",
  "account": "958412138249",
  "time": "2025-05-15T14:30:27Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:transfer:us-east-1:958412138249:server/s-1234abcd5678efghi"
  ],
  "detail": {
    "status-code": "COMPLETED",
    "protocol": "SFTP",
    "client-ip": "IP-address",
    "end-timestamp": "2025-05-15T14:30:27.749749117Z",
    "file-path": "/fs-1234abcd5678efghi/user0/test-file-to-delete.txt",
    "server-id": "s-1234abcd5678efghi",
    "username": "test",
    "session-id": "session-ID",
    "start-timestamp": "2025-05-15T14:30:26.706282454Z"
  }
}
```

Example SFTP 伺服器檔案重新命名已完成範例事件

下列範例顯示在 SFTP 伺服器上成功重新命名檔案的事件。

```
{
  "version": "0",
  "id": "event-ID",
  "detail-type": "SFTP Server File Rename Completed",
  "source": "aws.transfer",
  "account": "958412138249",
  "time": "2025-05-15T15:45:12Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:transfer:us-east-1:958412138249:server/s-1234abcd5678efghi"
  ],
  "detail": {
    "status-code": "COMPLETED",
    "protocol": "SFTP",
    "client-ip": "IP-address",
    "end-timestamp": "2025-05-15T15:45:12.749749117Z",
    "original-file-path": "/fs-1234abcd5678efghi/user0/old-filename.txt",

```

```
    "renamed-file-path": "/fs-1234abcd5678efghi/user0/new-filename.txt",
    "server-id": "s-1234abcd5678efghi",
    "username": "test",
    "session-id": "session-ID",
    "start-timestamp": "2025-05-15T15:45:11.706282454Z"
  }
}
```

Example SFTP 伺服器目錄建立已完成的範例事件

下列範例顯示在 SFTP 伺服器上成功建立目錄的事件。

```
{
  "version": "0",
  "id": "event-ID",
  "detail-type": "SFTP Server Directory Create Completed",
  "source": "aws.transfer",
  "account": "958412138249",
  "time": "2025-05-15T16:20:05Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:transfer:us-east-1:958412138249:server/s-1234abcd5678efghi"
  ],
  "detail": {
    "status-code": "COMPLETED",
    "protocol": "SFTP",
    "client-ip": "IP-address",
    "end-timestamp": "2025-05-15T16:20:05.749749117Z",
    "directory-path": "/fs-1234abcd5678efghi/user0/new-directory",
    "server-id": "s-1234abcd5678efghi",
    "username": "test",
    "session-id": "session-ID",
    "start-timestamp": "2025-05-15T16:20:04.706282454Z"
  }
}
```

SFTP 連接器事件

Note

這些事件會以耐久的層級交付至 EventBridge，如 Amazon EventBridge Events Reference 中[AWS 服務事件的交付層級](#)所述。

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
- SFTP 連接器目錄清單已完成
- SFTP 連接器目錄清單失敗
- SFTP 連接器遠端移動已完成
- SFTP 連接器遠端移動失敗
- 已完成 SFTP 連接器遠端刪除
- SFTP 連接器遠端刪除失敗

以下包含 `source` 和 `detail-type` 欄位，因為它們包含 Transfer Family 事件的特定值。如需所有事件中包含的其他中繼資料欄位的定義，請參閱 Amazon EventBridge 《使用者指南》中的 [事件結構參考](#)。

```
{
  . . . ,
  "detail-type": "string",
  "source": "aws.transfer",
  . . . ,
  "detail": {
    "operation" : "string",
    "max-items" : "number",
    "connector-id" : "string",
    "output-directory-path" : "string",
    "listing-id" : "string",
    "transfer-id" : "string",
    "file-transfer-id" : "string",
    "url" : "string",
    "file-path" : "string",
    "status-code" : "string",
    "failure-code" : "string",
    "failure-message" : "string",
    "start-timestamp" : "string",
    "end-timestamp" : "string",
    "local-directory-path" : "string",
```

```

    "remote-directory-path" : "string"
    "item-count" : "number"
    "truncated" : "boolean"
    "bytes" : "number",
    "egress-type" : "string",
    "vpc-lattice-resource-configuration-arn" : "string",
    "vpc-lattice-port-number" : "number",
    "local-file-location" : {
      "domain" : "string",
      "bucket" : "string",
      "key" : "string"
    },
    "output-file-location" : {
      "domain" : "string",
      "bucket" : "string",
      "key" : "string"
    }
  }
}

```

detail-type

識別事件的類型。

對於此事件，值是先前列出的其中一個 SFTP 連接器事件名稱。

source

識別產生事件的服務。對於 Transfer Family 事件，此值為 `aws.transfer`。

detail

包含事件相關資訊的 JSON 物件。產生事件的服務會決定此欄位的內容。

對於此事件，資料包含下列項目：

max-items

要傳回的目錄/檔案名稱數目上限。

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。

output-directory-path

Amazon S3 中儲存檔案/目錄清單結果的路徑（儲存貯體和字首）。

listing-id

StartDirectoryListing API 操作的唯一識別符。此識別符可用來檢查 CloudWatch 日誌，以查看列出請求的狀態。

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符。

url

合作夥伴 AS2 或 SFTP 端點的 URL。

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，則為傳輸失敗的原因代碼。值：ASSUME_ROLE_ERROR | UNSUPPORTED_OPERATION_ERROR | CONNECTION_ERROR | READ_FILE_ERROR | WRITE_FILE_ERROR | TIMEOUT_ERROR | LIST_DIRECTORY_ERROR | SEND_FILE_NOT_FOUND | RETRIEVE_FILE_NOT_FOUND | DIRECTORY_NOT_FOUND | FILE_NOT_FOUND | PATH_NOT_FOUND | RENAME_ERROR | DELETE_ERROR | INTERNAL_ERROR | UNKNOWN_ERROR。

failure-message

對於失敗的傳輸，則為傳輸失敗原因的詳細資訊。

start-timestamp

為了成功傳輸，檔案處理開始時的時間戳記。

end-timestamp

為了成功傳輸，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 SFTP 伺服器上指定預設目錄。若是如此，此欄位為空白。

item-count

為列出請求傳回的項目（目錄和檔案）數量。

truncated

清單輸出是否包含遠端目錄中包含的所有項目。

bytes

要傳輸的位元組數。失敗傳輸的值為 0。

egress-type

連接器的輸出組態類型。值：SERVICE_MANAGED或 VPC_LATTICE。

vpc-lattice-resource-configuration-arn

定義目標 SFTP 伺服器位置的 VPC_LATTICE 資源組態 ARN。服務受管連接器的此欄位為 null。

vpc-lattice-port-number

透過 VPC_LATTICE 連線至 SFTP 伺服器的連接埠號碼。

local-file-location

此參數包含 AWS 儲存檔案位置的詳細資訊。

domain

正在使用的儲存體。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。

output-file-location

此參數包含儲存體中 AWS 目錄清單結果存放位置的詳細資訊。

domain

正在使用的儲存體。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的範例事件

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": "/amzn-s3-demo-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": "amzn-s3-demo-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 連接器成功從遠端 SFTP 伺服器擷取檔案的事件。

```

{
  "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": "/amzn-s3-demo-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": "amzn-s3-demo-bucket",
      "key": "testfile.txt"
    }
  }
}

```

Example SFTP 連接器目錄列出已完成的範例事件

下列範例顯示 事件，其中列出呼叫的啟動目錄從遠端 SFTP 伺服器擷取清單檔案。

```
{
  "version": "0",
  "id": "event-ID",
  "detail-type": "SFTP Connector Directory Listing Completed",
  "source": "aws.transfer",
  "account": "123456789012",
  "time": "2024-01-24T18:28:08Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:transfer:us-east-1:123456789012:connector/c-f1111aaaa2222bbbb3"
  ],
  "detail": {
    "max-items": 10000,
    "connector-id": "c-fc68000012345aa18",
    "output-directory-path": "/amzn-s3-demo-bucket/example/file-listing-output",
    "listing-id": "123456-23aa-7980-abc1-1a2b3c4d5e",
    "url": "sftp://s-21a23456789012a.server.transfer.us-east-1.amazonaws.com",

    "status-code": "COMPLETED",
    "remote-directory-path": "/home",
    "item-count": 10000,
    "truncated": true,
    "start-timestamp": "2024-01-24T18:28:07.632388Z",
    "end-timestamp": "2024-01-24T18:28:07.774898Z",
    "output-file-location": {
      "domain": "S3",
      "bucket": "amzn-s3-demo-bucket",
      "key": "c-fc1ab90fd0d047e7a-70987273-49nn-4006-bab1-1a7290cc412ba.json"
    }
  }
}
```

AS2 事件

Note

這些事件會以耐久的層級交付至 EventBridge，如 Amazon EventBridge Events Reference 中[AWS 服務事件的交付層級](#)所述。

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

以下包含 `source` 和 `detail-type` 欄位，因為它們包含 Transfer Family 事件的特定值。如需所有事件中包含的其他中繼資料欄位的定義，請參閱 Amazon EventBridge 《使用者指南》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，該值是先前列出的其中一個 AS2 事件。

source

識別產生事件的服務。對於 Transfer Family 事件，此值為 `aws.transfer`。

detail

包含事件相關資訊的 JSON 物件。產生事件的服務會決定此欄位的內容。

s3-attributes

識別要傳輸之檔案的 Amazon S3 儲存貯體和金鑰。對於 MDN 事件，它也會識別 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

對於已完成或失敗的傳輸，則為 JSON 檔案的容器。

json-key

對於 COMPLETED 或 FAILED 傳輸，指定給 Amazon S3 中 JSON 檔案的名稱。

mdn-bucket

對於 MDN 事件，則為 MDN 檔案的容器。

mdn-key

對於 MDN 事件，為 Amazon S3 中 MDN 檔案指派的名稱。

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，則為處置的類別。

bytes

訊息中的位元組數。

as2-from

正在傳送訊息的 AS2 交易合作夥伴。

as2-message-id

要傳輸之 AS2 訊息的唯一識別符。

as2-to

接收訊息的 AS2 交易合作夥伴。

connector-id

對於從 Transfer Family 伺服器傳送至交易合作夥伴的 AS2 訊息，這是使用之 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，為 AS2 協議的唯一識別符。

`server-id`

對於伺服器事件，唯一的 ID 僅適用於 Transfer Family 伺服器。

`requester-file-name`

對於承載事件，在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`

為了成功傳輸，檔案處理開始時的時間戳記。

`end-timestamp`

為了成功傳輸，檔案處理完成時的時間戳記。

`status-code`

對應至 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，則為傳輸失敗原因的類別。

`failure-message`

對於失敗的傳輸，則為傳輸失敗原因的詳細資訊。

`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": "amzn-s3-demo-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": "amzn-s3-demo-bucket1",
      "file-key": "/as2Integ/TestOutboundWrongCert.dat",
      "file-bucket": "amzn-s3-demo-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

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

安全性是 AWS 與您之間共同責任。[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 AWS 服務 是否在特定合規計劃範圍內，請參閱[AWS 服務 合規計劃範圍內](#)然後選擇您感興趣的合規計劃。如需一般資訊，請參閱[AWS 合規計劃](#)。

您可以使用 下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱[下載報告 in AWS Artifact](#)

您使用 時的合規責任 AWS 服務 取決於資料的機密性、您公司的合規目標，以及適用的法律和法規。如需使用 時合規責任的詳細資訊 AWS 服務，請參閱 [AWS 安全文件](#)。

本文件可協助您了解如何在使用 時套用共同責任模型 AWS Transfer Family。下列主題說明如何設定 AWS Transfer Family 以符合您的安全與合規目標。您也會了解如何使用其他 AWS 服務來協助您監控和保護 AWS Transfer Family 資源。

我們提供一個研討會，提供規範性指導和實作實驗室，說明如何在 上建置可擴展且安全的檔案傳輸架構，AWS 而不需要修改現有的應用程式或管理伺服器基礎設施。您可以[在這裡](#)檢視此研討會的詳細資訊。

主題

- [VPC 連線安全性優點](#)
- [AWS Transfer Family 伺服器的安全政策](#)
- [AWS Transfer Family SFTP 連接器的安全政策](#)
- [搭配 使用混合式後量子金鑰交換 AWS Transfer Family](#)
- [資料保護和加密](#)
- [管理 Transfer 系列中的 SSH 和 PGP 金鑰](#)
- [的身分和存取管理 AWS Transfer Family](#)
- [的合規驗證 AWS Transfer Family](#)
- [中的彈性 AWS Transfer Family](#)
- [在 VPC 和 AWS Transfer Family APIs之間建立私有連線](#)
- [中的基礎設施安全性 AWS Transfer Family](#)
- [新增 Web 應用程式防火牆](#)

- [預防跨服務混淆代理人](#)
- [AWS AWS Transfer Family 的 受管政策](#)

VPC 連線安全性優點

具有 VPC 輸出類型的 SFTP 連接器透過跨 VPC 資源存取提供增強的安全優勢：

- 網路隔離：所有流量都會保留在您的 VPC 環境中，為私有端點連線提供與公有網際網路的完整網路隔離。
- 來源 IP 控制：遠端 SFTP 伺服器只會看到 VPC CIDR 範圍的 IP 地址，讓您完全控制用於連線的來源 IP 地址。
- 私有端點存取：使用私有 IP 地址直接連線至 VPC 中的 SFTP 伺服器，消除公有網際網路的暴露。
- 混合連線：透過已建立的 VPN 或 Direct Connect 連線安全地存取內部部署 SFTP 伺服器，無需額外的網際網路暴露。
- VPC 安全控制：利用現有的 VPC 安全群組、NACLs 和路由政策來控制和監控 SFTP 連接器流量。

VPC Lattice 安全模型

SFTP 連接器的 VPC 連線使用 AWS VPC Lattice 與服務網路，以提供安全的多租戶存取：

- 預防混淆代理人：身分驗證和授權檢查可確保連接器只能存取其設定的特定資源，防止未經授權的跨租用戶存取。
- IPv6-only 服務網路：使用 IPv6 定址以避免潛在的 IP 地址衝突，並增強安全隔離。
- 轉送存取工作階段 (FAS)：暫時憑證處理不需要長期憑證儲存或手動資源共用。
- 資源層級存取控制：每個連接器都與特定資源組態相關聯，以確保對個別 SFTP 伺服器的精細存取控制。

VPC 連線的安全最佳實務

使用 VPC 輸出類型連接器時，請遵循下列安全最佳實務：

- 安全群組：設定安全群組，僅允許必要資源之間的 SFTP 流量（連接埠 22）。將來源和目的地 IP 範圍限制在所需的最低範圍內。
- 資源閘道置放：盡可能在私有子網路中部署資源閘道，並確保它們至少跨越兩個可用區域，以實現高可用性。

- 網路監控：使用 VPC 流程日誌和 Amazon CloudWatch 來監控網路流量模式並偵測異常活動。
- 存取記錄：啟用連接器記錄以追蹤檔案傳輸活動，並維護稽核追蹤以符合合規要求。
- 資源組態管理：定期檢閱和更新資源組態，以確保它們指向正確的 SFTP 伺服器，並使用適當的網路設定。

AWS Transfer Family 伺服器的安全政策

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)、密碼套件、內容加密密碼和雜湊演算法）。

AWS Transfer Family 支援使用混合金鑰交換演算法的後量子安全政策，結合傳統密碼編譯方法與後量子演算法，以針對未來的量子運算威脅提供增強的安全性。如需詳細資訊，請參閱[搭配使用混合式後量子金鑰交換 AWS Transfer Family](#)。

如需支援的加密演算法清單，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[管理 Transfer 系列中的 SSH 和 PGP 金鑰](#)。

Note

從 2025 年開始，所有新的 AWS Transfer Family 安全政策都包含使用混合金鑰交換演算法的量子後密碼編譯支援。如需量子後安全性的詳細資訊，請參閱[搭配使用混合式後量子金鑰交換 AWS Transfer Family](#)。

Note

我們強烈建議將您的伺服器更新為最新的安全政策。

- TransferSecurityPolicy-2024-01 是使用主控台、API 或 CLI 建立伺服器時連接到伺服器的預設安全政策。
- 如果您使用 CloudFormation 建立 Transfer Family 伺服器並接受預設安全政策，則會指派伺服器 TransferSecurityPolicy-2018-11。

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，該政策可能會有所變更。若要變更伺服器的安全政策，請參閱[編輯安全政策](#)。

 Note

較早的後量子政策 (TransferSecurityPolicy-PQ-SSH-Experimental-2023-04 和 TransferSecurityPolicy-PQ-SSH-FIPS-Experimental-2023-04) 已棄用。我們建議您改用新的政策。

如需 Transfer Family 中安全性的詳細資訊，請參閱下列部落格文章：

- [改善 AWS Transfer Family 伺服器安全性的六個秘訣](#)
- [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](#)
- [安全政策詳細資訊](#)

密碼編譯演算法

對於主機金鑰，我們支援下列演算法：

- rsa-sha2-256
- rsa-sha2-512
- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384
- ecdsa-sha2-nistp521
- ssh-ed25519

此外，下列安全政策允許 ssh-rsa：

- TransferSecurityPolicy-2018-11
- TransferSecurityPolicy-2020-06
- TransferSecurityPolicy-FIPS-2020-06
- TransferSecurityPolicy-FIPS-2023-05
- TransferSecurityPolicy-FIPS-2024-01

 Note

請務必了解 RSA 金鑰類型 - 一律 `ssh-rsa`- 和 RSA 主機金鑰演算法 - 之間的區別，這可以是任何支援的演算法。

以下是每個安全政策支援的加密演算法清單。

 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 伺服器不使用加密，因此請勿使用任何這些演算法。
- AS2 伺服器僅在 `ContentEncryptionCiphers` 和 `HashAlgorithms` 區段中使用演算法。這些區段定義用於加密和簽署檔案內容的演算法。
- FIPS-2024-05 和 FIPS-2024-01 安全政策完全相同，但 FIPS-2024-05 不支援 `ssh-rsa` 演算法。
- Transfer Family 已推出新的限制政策，以密切平行現有的政策：
 - `TransferSecurityPolicy-Restricted-2018-11` 和 `TransferSecurityPolicy-2018-11` 安全政策完全相同，但受限制政策不支援 `chacha20-poly1305@openssh.com` 加密。
 - `TransferSecurityPolicy-Restricted-2020-06` 和 `TransferSecurityPolicy-2020-06` 安全政策完全相同，但限制政策不支援 `chacha20-poly1305@openssh.com` 加密。

*在下表中，`chacha20-poly1305@openssh.com` 密碼僅包含在非限制政策中，

安全 政策	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS
	curity-2025-03	curity-2025-03	curity-2025-03	curity-2025-03	curity-2025-03	curity-2025-03	curity-2025-03	curity-2025-03	curity-2025-03	curity-2025-03	curity-2025-03	curity-2025-03
	Policy-2025-03	Policy-2025-03	Policy-2025-03	Policy-2025-03	Policy-2025-03	Policy-2025-03	Policy-2025-03	Policy-2025-03	Policy-2025-03	Policy-2025-03	Policy-2025-03	Policy-2025-03
	-03	FIPS	SshA	AS2R	-01	FIPS	-05	FIPS	-03	-06	FIPS	-11
		-2025-03	ditCom	stricted		-2024-01/		-2023-05		和	-2020-06	和
			iant-2025-02	2025-07		TransferS				TransferS		TransferS
						curityPo				curityPo		curityPo
						licy-				licy-		licy-
						FIPS				Rest		Rest
						-2024-05				stricted-20		stricted-20
										20-06		18-11
SshCiphers												
aes128-ctr	◆	◆	◆	◆	◆					◆	◆	◆
aes128-gcm@openssh.com	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
aes192-ctr	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
aes256-ctr	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
aes256-gcm@openssh.com	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
chacha20-poly1305@openssh.com										◆ *		◆ *

安全 政策	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS
	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo
	licy-2025	licy-2025	licy-2025	licy-2025	licy-2024	licy-2024	licy-2023	licy-2023	licy-2022	licy-2020	licy-2020	licy-2018
	-03	FIPS	SshA	AS2R	-01	FIPS	-05	FIPS	-03	-06	FIPS	-11
		-2025-08	ditCom	restricted		-2024-01/		-2023-05		和	-2020-06	和
			iant-2025	2025-07		TransferS				TransferS		TransferS
			-02			ecurityPo				ecurityPo		ecurityPo
						licy-				licy-		licy-
						FIPS				Rest		Rest
						-2024-05				ricted-20		ricted-20
										20-06		18-11
SshKexs												
mlkem768x	◆			◆								
25519-sha256												
mlkem768n	◆			◆								
istp256-s												
ha256												
mlkem1024	◆			◆								
nistp384-sha384												
curve25519-sha256		◆	◆	◆		◆		◆				◆
curve25519-sha256@libssh.org		◆	◆	◆		◆		◆				◆

安全 政策	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-03
	FIPS	SshA	AS2R	-01	FIPS	-05	FIPS	-03	-06	FIPS	-11	
		-2025-08	ditComes	stricted		-2024-01/	-2023-05		和	-2020-06	和	
			iant-2025-07	-02		TransferS			TransferS	ecurityPo	TransferS	ecurityPo
						ecurityPo			ecurityPo		ecurityPo	
						licy-			licy-		licy-	
						FIPS			Rest		Rest	
						-2024-05			ricted-20		ricted-20	
									20-06		18-11	
diffie- he llman- gro up14- sha1											◆	
diffie- he llman- gro up14- sha2 56									◆	◆	◆	
diffie- he llman- gro up16- sha5 12	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆

安全 政策	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS
	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo
	licy-2025	licy-2025	licy-2025	licy-2025	licy-2024	licy-2024	licy-2023	licy-2023	licy-2022	licy-2020	licy-2020	licy-2018
	-03	FIPS	SshA	AS2R	-01	FIPS	-05	FIPS	-03	-06	FIPS	-11
		-2025-08	ditCom	stricted		-2024-01/		-2023-05		和	-2020-06	和
			iant-2025	2025-07		TransferS				TransferS		TransferS
			-02			ecurityPo				ecurityPo		ecurityPo
						licy-				licy-		licy-
						FIPS				Rest		Rest
						-2024-05				ricted-20		ricted-20
										20-06		18-11
diffie- he llman- gro up18- sha5 12	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
diffie- he llman- gro up- exchan ge- sha256	◆	◆	◆	◆	◆		◆	◆	◆	◆	◆	◆
ecdh- sha2 - nistp256	◆	◆		◆	◆	◆				◆	◆	◆

安全 政策	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS
	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo
	licy-2025	licy-	licy-	licy-	licy-2024	licy-	licy-2023	licy-	licy-2022	licy-2020	licy-	licy-2018
	-03	FIPS	SshA	AS2R	-01	FIPS	-05	FIPS	-03	-06	FIPS	-11
		-2025-08	ditCom	restricted		-2024-01/		-2023-05		和	-2020-06	和
			iant-2025	2025-07		TransferS				TransferS		TransferS
			-02			ecurityPo				ecurityPo		ecurityPo
						licy-				licy-		licy-
						FIPS				Rest		Rest
						-2024-05				ricted-20		ricted-20
										20-06		18-11
ecdh-	◆	◆		◆	◆	◆				◆	◆	◆
sha2												
-												
nistp384												
ecdh-	◆	◆		◆	◆	◆				◆	◆	◆
sha2												
-												
nistp521												
SshMacs												
hmac-												◆
sha1												
hmac-												◆
sha1												
-												
etm@open												
ssh.com												
hmac-								◆	◆	◆	◆	
sha2												
-256												

安全 政策	TransferS ecurityPo licy-2025- -03	TransferS ecurityPo licy- FIPS -2025-08	TransferS ecurityPo licy- SshA -2025-08	TransferS ecurityPo licy- AS2R -2025-07	TransferS ecurityPo licy- -01 Restricted -2025-07	TransferS ecurityPo licy- FIPS -2024-01/ TransferS ecurityPo licy- FIPS -2024-05	TransferS ecurityPo licy- -05 FIPS -2023-05	TransferS ecurityPo licy- -03 FIPS -2023-05	TransferS ecurityPo licy- -06 和 TransferS ecurityPo licy- Rest ricted-20 20-06	TransferS ecurityPo licy- FIPS -2020-06 和	TransferS ecurityPo licy- -11 TransferS ecurityPo licy- Rest ricted-20 18-11
hmac- sha2 -256- etm@ openssh.c om	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
hmac- sha2 -512								◆	◆	◆	◆
hmac- sha2 -512- etm@ openssh.c om	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
umac-128- etm@opens sh.com									◆		◆
umac-128@ openssh.c om									◆		◆

安全 政策	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS
	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo
	licy-2025-	licy-2025-	licy-2025-	licy-2025-	licy-2024-	licy-2024-	licy-2023-	licy-2023-	licy-2022-	licy-2020-	licy-2018-	
	-03	FIPS	SshA	AS2R	-01	FIPS	-05	FIPS	-03	-06	FIPS	-11
		-2025-08	ditCom	restricted		-2024-01/		-2023-05		和	-2020-06	和
			iant-2025-	2025-07		TransferS				TransferS		TransferS
			-02			ecurityPo				ecurityPo		ecurityPo
						licy-				licy-		licy-
						FIPS				Rest		Rest
						-2024-05				ricted-20		ricted-20
										20-06		18-11
umac-64-												◆
e												
tm@openss												
h.com												
umac-64@o												◆
penssh.co												
m												
ContentEncryptionCiphers												
aes256-	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
cbc												
aes192-	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
cbc												
aes128-	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
cbc												
3des-	◆	◆	◆		◆	◆	◆	◆	◆	◆	◆	◆
cbc												
HashAlgorithms												
sha256	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆

安全 政策	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-03-FIPS	TransferSecurityPolicy-2025-03-SshA	TransferSecurityPolicy-2025-03-AS2R	TransferSecurityPolicy-2025-01	TransferSecurityPolicy-2024-01-FIPS	TransferSecurityPolicy-2023-05-FIPS	TransferSecurityPolicy-2023-03-FIPS	TransferSecurityPolicy-2023-06和	TransferSecurityPolicy-2020-06-FIPS	TransferSecurityPolicy-2018-11和
			TransferSecurityPolicy-2025-07-ditComes	TransferSecurityPolicy-2025-07-Restricted		TransferSecurityPolicy-2024-05-FIPS			TransferSecurityPolicy-2020-06-Restricted	TransferSecurityPolicy-2018-11-Restricted	
sha384	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
sha512	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
sha1	◆	◆	◆		◆	◆	◆	◆	◆	◆	◆
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	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS	TransferS
	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo	ecurityPo
	licy-2025	licy-2025	licy-2025	licy-2025	licy-2024	licy-2024	licy-2023	licy-2023	licy-2022	licy-2020	licy-2020	licy-2018
	-03	FIPS	SshA	AS2R	-01	FIPS	-05	FIPS	-03	-06	FIPS	-11
		-2025-08	ditCom	stricted		-2024-01/		-2023-05		和	-2020-06	和
			iant-2025	2025-07		TransferS				TransferS		TransferS
			-02			ecurityPo				ecurityPo		ecurityPo
						licy-				licy-		licy-
						FIPS				Rest		Rest
						-2024-05				ricted-20		ricted-20
										20-06		18-11
TLS_ECDHE	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
_ECDSA_WITH												
TH_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												

安全政策	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-08	TransferSecurityPolicy-2025-09	TransferSecurityPolicy-2025-10	TransferSecurityPolicy-2025-11	TransferSecurityPolicy-2025-12	TransferSecurityPolicy-2026-01	TransferSecurityPolicy-2026-02	TransferSecurityPolicy-2026-03	TransferSecurityPolicy-2026-04	TransferSecurityPolicy-2026-05	TransferSecurityPolicy-2026-06	TransferSecurityPolicy-2026-07	TransferSecurityPolicy-2026-08	TransferSecurityPolicy-2026-09	TransferSecurityPolicy-2026-10	TransferSecurityPolicy-2026-11	TransferSecurityPolicy-2026-12
	FIPS-2025-08	SshA	AS2R	-01	FIPS-2024-01	-05	FIPS-2023-05	-03	-06	FIPS-2020-06	-11							
		ComRestricted-2025-02			TransferSecurityPolicy-2024-05				和	TransferSecurityPolicy-2020-06	和							
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆							
TLS_RSA_WITH_AES_128_CBC_SHA256																	◆	
TLS_RSA_WITH_AES_128_CBC_SHA256																	◆	

安全政策詳細資訊

下列各節包含每個安全政策的 JSON 表示法。

TransferSecurityPolicy-2025-03

以下顯示 TransferSecurityPolicy-2025-03 安全政策。

```
{
  "SecurityPolicy": {
```

```
"Fips": false,
"SecurityPolicyName": "TransferSecurityPolicy-2025-03",
"SshCiphers": [
    "aes256-gcm@openssh.com",
    "aes128-gcm@openssh.com",
    "aes128-ctr",
    "aes256-ctr",
    "aes192-ctr"
],
"SshKexs": [
    "mlkem768x25519-sha256",
    "mlkem768nistp256-sha256",
    "mlkem1024nistp384-sha384",
    "ecdh-sha2-nistp256",
    "ecdh-sha2-nistp384",
    "ecdh-sha2-nistp521",
    "curve25519-sha256",
    "curve25519-sha256@libssh.org",
    "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"
],
"ContentEncryptionCiphers": [
    "aes256-cbc",
    "aes192-cbc",
    "aes128-cbc",
    "3des-cbc"
],
"HashAlgorithms": [
    "sha256",
    "sha384",
    "sha512",
    "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"
    ],
    "Type": "SERVER",
    "Protocols": [
        "SFTP",
        "FTPS"
    ]
}
}

```

TransferSecurityPolicy-FIPS-2025-03

以下顯示 TransferSecurityPolicy-FIPS-2025-03 安全政策。

```

{
  "SecurityPolicy": {
    "Fips": true,
    "SecurityPolicyName": "TransferSecurityPolicy-FIPS-2025-03",
    "SshCiphers": [
      "aes256-gcm@openssh.com",
      "aes128-gcm@openssh.com",
      "aes256-ctr",
      "aes192-ctr",
      "aes128-ctr"
    ],
    "SshKexs": [
      "mlkem768x25519-sha256",
      "mlkem768nistp256-sha256",
      "mlkem1024nistp384-sha384",
      "ecdh-sha2-nistp256",
      "ecdh-sha2-nistp384",
      "ecdh-sha2-nistp521",
      "diffie-hellman-group-exchange-sha256",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512"
    ],
    "SshMacs": [
      "hmac-sha2-512-etm@openssh.com",
      "hmac-sha2-256-etm@openssh.com"
    ],
    "ContentEncryptionCiphers": [

```

```

        "aes256-cbc",
        "aes192-cbc",
        "aes128-cbc",
        "3des-cbc"
    ],
    "HashAlgorithms": [
        "sha256",
        "sha384",
        "sha512",
        "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"
    ],
    "Type": "SERVER",
    "Protocols": [
        "SFTP",
        "FTPS"
    ]
}

```

TransferSecurityPolicy-AS2Restricted-2025-07

此安全政策專為需要透過排除傳統密碼編譯演算法增強安全性的 AS2 檔案傳輸而設計。它支援現代 AES 加密和 SHA-2 雜湊演算法，同時移除對較弱演算法的支援，例如 3DES 和 SHA-1。

Note

此安全政策與 TransferSecurityPolicy-2025-03 相同，但它不支援 3DES（在 ContentEncryptionCiphers 中）且不支援 SHA1（在 HashAlgorithms 中）。它包含 2025 年 3 月的所有演算法，包括量子後密碼編譯演算法 (mlkem* KEXs)。

```
{
```

```
"SecurityPolicy": {
  "Fips": false,
  "SecurityPolicyName": "TransferSecurityPolicy-AS2Restricted-2025-07",
  "SshCiphers": [
    "aes256-gcm@openssh.com",
    "aes128-gcm@openssh.com",
    "aes128-ctr",
    "aes256-ctr",
    "aes192-ctr"
  ],
  "SshKexs": [
    "mlkem768x25519-sha256",
    "mlkem768nistp256-sha256",
    "mlkem1024nistp384-sha384",
    "ecdh-sha2-nistp256",
    "ecdh-sha2-nistp384",
    "ecdh-sha2-nistp521",
    "curve25519-sha256",
    "curve25519-sha256@libssh.org",
    "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"
  ],
  "ContentEncryptionCiphers": [
    "aes256-cbc",
    "aes192-cbc",
    "aes128-cbc"
  ],
  "HashAlgorithms": [
    "sha256",
    "sha384",
    "sha512"
  ],
  "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"
    ],
    "Type": "SERVER",
    "Protocols": [
        "SFTP",
        "FTPS"
    ]
}
}

```

TransferSecurityPolicy-SshAuditCompliant-2025-02

以下顯示 TransferSecurityPolicy-SshAuditCompliant-2025-02 安全政策。

Note

此安全政策的設計是以 ssh-audit 工具提供的建議為依據，且 100% 符合該工具。

```

{
  "SecurityPolicy": {
    "Fips": false,
    "Protocols": [
      "SFTP",
      "FTPS"
    ],
    "SecurityPolicyName": "TransferSecurityPolicy-SshAuditCompliant-2025-02",
    "SshCiphers": [
      "aes128-gcm@openssh.com",
      "aes256-gcm@openssh.com",
      "aes128-ctr",
      "aes256-ctr",
      "aes192-ctr"
    ],
    "SshKexs": [
      "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"
    ],
    "ContentEncryptionCiphers": [
      "aes256-cbc",
      "aes192-cbc",
      "aes128-cbc",
      "3des-cbc"
    ],
    "HashAlgorithms": [
      "sha256",
      "sha384",
      "sha512",
      "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"
    ],
    "Type": "SERVER"
  }
}

```

TransferSecurityPolicy-2024-01

以下顯示 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-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"
    ],
    "ContentEncryptionCiphers": [
        "aes256-cbc",
        "aes192-cbc",
        "aes128-cbc",
        "3des-cbc"
    ],
    "HashAlgorithms": [
        "sha256",
        "sha384",
        "sha512",
        "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"
    ]
}
}
```

TransferSecurityPolicy-FIPS-2024-01/TransferSecurityPolicy-FIPS-2024-05

以下顯示 TransferSecurityPolicy-FIPS-2024-01 和 TransferSecurityPolicy-FIPS-2024-05 安全政策。

Note

FIPS 服務端點和 TransferSecurityPolicy-FIPS-2024-01 和 TransferSecurityPolicy-FIPS-2024-05 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](#)。

這兩個安全政策的唯一區別是 TransferSecurityPolicy-FIPS-2024-01 支援ssh-rsa演算法，而 TransferSecurityPolicy-FIPS-2024-05 則不支援。

```
{
  "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-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"
    ],
    "ContentEncryptionCiphers": [
      "aes256-cbc",
      "aes192-cbc",
      "aes128-cbc",
      "3des-cbc"
    ],
  },
}
```

```

    "HashAlgorithms": [
        "sha256",
        "sha384",
        "sha512",
        "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"
    ]
}

```

TransferSecurityPolicy-2023-05

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"
    ]
  }
}

```



```

    ],
    "ContentEncryptionCiphers": [
        "aes256-cbc",
        "aes192-cbc",
        "aes128-cbc",
        "3des-cbc"
    ],
    "HashAlgorithms": [
        "sha256",
        "sha384",
        "sha512",
        "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"
    ]
}

```

TransferSecurityPolicy-FIPS-2023-05

如需的 FIPS 認證詳細資訊 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"
],
"ContentEncryptionCiphers": [
    "aes256-cbc",
    "aes192-cbc",
    "aes128-cbc",
    "3des-cbc"
],
"HashAlgorithms": [
    "sha256",
    "sha384",
    "sha512",
    "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"
]
}
```

TransferSecurityPolicy-2022-03

以下顯示 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"
    ],
    "ContentEncryptionCiphers": [
      "aes256-cbc",
      "aes192-cbc",
      "aes128-cbc",
      "3des-cbc"
    ],
    "HashAlgorithms": [
      "sha256",
      "sha384",
      "sha512",
      "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"
  ]
}
}

```

TransferSecurityPolicy-2020-06 和 TransferSecurityPolicy-Restricted-2020-06

以下顯示 TransferSecurityPolicy-2020-06 安全政策。

Note

TransferSecurityPolicy-Restricted-2020-06 和 TransferSecurityPolicy-2020-06 安全政策完全相同，但限制政策不支援chacha20-poly1305@openssh.com加密。

```

{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2020-06",
    "SshCiphers": [
      "chacha20-poly1305@openssh.com", //Not included in TransferSecurityPolicy-
Restricted-2020-06
      "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"
  ],
  "ContentEncryptionCiphers": [
    "aes256-cbc",
    "aes192-cbc",
    "aes128-cbc",
    "3des-cbc"
  ],
  "HashAlgorithms": [
    "sha256",
    "sha384",
    "sha512",
    "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"
  ]
}
}

```

TransferSecurityPolicy-FIPS-2020-06

如需的 FIPS 認證詳細資訊 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-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"
    ],
    "ContentEncryptionCiphers": [
      "aes256-cbc",
      "aes192-cbc",
      "aes128-cbc",
      "3des-cbc"
    ],
    "HashAlgorithms": [
      "sha256",
      "sha384",
      "sha512",
      "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"
  ]
}
}

```

TransferSecurityPolicy-2018-11 和 TransferSecurityPolicy-Restricted-2018-11

以下顯示 TransferSecurityPolicy-2018-11 安全政策。

Note

TransferSecurityPolicy-Restricted-2018-11 和 TransferSecurityPolicy-2018-11 安全政策完全相同，但受限制政策不支援chacha20-poly1305@openssh.com加密。

```

{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2018-11",
    "SshCiphers": [
      "chacha20-poly1305@openssh.com", //Not included in TransferSecurityPolicy-
Restricted-2018-11
      "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"
],
"ContentEncryptionCiphers": [
  "aes256-cbc",
  "aes192-cbc",
  "aes128-cbc",
  "3des-cbc"
],
"HashAlgorithms": [
  "sha256",
  "sha384",
  "sha512",
  "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"
]
}
}
```


AWS Transfer Family SFTP 連接器的安全政策

中的 SFTP 連接器安全政策 AWS Transfer Family 可讓您限制與 SFTP 連接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）。以下是每個 SFTP 連接器安全政策支援的加密演算法清單。

Note

TransferSFTPConnectorSecurityPolicy-2024-03 是套用至 SFTP 連接器的預設安全政策。

您可以變更連接器的安全政策。從 Transfer Family 左側導覽窗格中選取連接器，然後選取連接器。然後在 Sftp 組態區段中選取編輯。在密碼編譯演算法選項區段中，從安全政策欄位中的下拉式清單中選擇任何可用的安全政策。

密碼編譯演算法

對於主機金鑰，SFTP 連接器支援 Transfer Family 伺服器支援的所有演算法，但 ed25519 除外：

- rsa-sha2-256
- rsa-sha2-512
- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384
- ecdsa-sha2-nistp521

此外，對於主機金鑰，我們支援 ssh-rsa，但僅適用於 TransferSFTPConnectorSecurityPolicy-2023-07。

對於身分驗證，SFTP 連接器支援下列金鑰類型：

- ssh-rsa
- ecdsa

SFTP 連接器安全政策詳細資訊

下表顯示每個 SFTP 連接器安全政策支援的特定密碼編譯演算法。

安全政策	TransferSFTPConnectorSecurityPolicy-FIPS-2024-10	TransferSFTPConnectorSecurityPolicy-2024-03	TransferSFTPConnectorSecurityPolicy-2023-07
Ciphers			
aes128-ctr			◆
aes128-gcm@openssh.com	◆	◆	◆
aes192-ctr		◆	◆
aes256-ctr		◆	◆
aes256-gcm@openssh.com	◆	◆	◆
Kexs			
curve25519-sha256		◆	◆
curve25519-sha256@libssh.org		◆	◆
diffie-hellman-group14-sha1			◆
diffie-hellman-group16-sha512		◆	◆
diffie-hellman-group18-sha512		◆	◆
diffie-hellman-group-exchange-sha256		◆	◆
ecdh-sha2-nistp256	◆		
ecdh-sha2-nistp384	◆		

安全政策	TransferSFTPConnectorSecurityPolicy-FIPS-2024-10	TransferSFTPConnectorSecurityPolicy-2024-03	TransferSFTPConnectorSecurityPolicy-2023-07
ecdh-sha2-nistp521	◆		
Macs			
hmac-sha2-512-etm@openssh.com		◆	◆
hmac-sha2-256-etm@openssh.com		◆	◆
hmac-sha2-512	◆	◆	◆
hmac-sha2-256	◆	◆	◆
hmac-sha1			◆
hmac-sha1-96			◆
Host Key Algorithms			
rsa-sha2-256	◆	◆	◆
rsa-sha2-512	◆	◆	◆
ecdsa-sha2-nistp256	◆	◆	◆
ecdsa-sha2-nistp384		◆	◆
ecdsa-sha2-nistp521		◆	◆
ssh-rsa			◆

搭配 使用混合式後量子金鑰交換 AWS Transfer Family

Transfer Family 支援 Secure Shell (SSH) 通訊協定的混合式後量子金鑰建立選項。需要建立後量子金鑰，因為已經可以記錄網路流量，並儲存它以供量子電腦未來解密，這稱為 store-now-harvest-later 攻擊。

當您連線到 Transfer Family 時，您可以使用此選項，以安全地傳入和傳出 Amazon Simple Storage Service (Amazon S3) 儲存體或 Amazon Elastic File System (Amazon EFS) 的檔案。SSH 中的後量子混合金鑰建立引入後量子金鑰建立機制，它與傳統金鑰交換演算法搭配使用。使用傳統密碼套件建立的 SSH 金鑰可安全防範目前技術的暴力破解攻擊。不過，未來出現大規模量子運算之後，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 正與密碼編譯社群參與開發量子抗性或後量子演算法。我們已在 Transfer Family 中實作混合式後量子金鑰交換密碼套件，結合傳統元素和後量子元素。

這些混合密碼套件可用於大多數 AWS 區域的生產工作負載。不過，由於混合式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 連線上測試它們。

在後量子密碼編譯安全部落格文章中進一步了解[後量子密碼編譯](#)。

內容

- [關於 SSH 中的後量子混合金鑰交換](#)
- [後量子混合金鑰建立如何在 Transfer 系列中運作](#)
 - [為什麼選擇 ML-KEM？](#)
 - [量子後混合 SSH 金鑰交換和密碼編譯要求 \(FIPS 140\)](#)
- [在 Transfer Family 中測試後量子混合金鑰交換](#)
 - [在 SFTP 端點上啟用後量子混合金鑰交換](#)
 - [設定支援後量子混合金鑰交換的 SFTP 用戶端](#)
 - [在 SFTP 中確認後量子混合金鑰交換](#)

關於 SSH 中的後量子混合金鑰交換

Transfer Family 支援後量子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 ML-KEM。ML-KEM 是一種後量子公有金鑰加密和金鑰建立演算法，由[國家標準技術研究所 \(NIST\)](#) 指定為第一個標準後量子金鑰協議演算法。

用戶端和伺服器仍會執行 ECDH 金鑰交換。此外，伺服器會將後量子共用密封裝至用戶端的後量子 KEM 公有金鑰，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保證與建議的後量子金鑰交換的安全性，以協助確保只要 ECDH 或後量子共用秘密無法中斷，交握都會受到保護。

後量子混合金鑰建立如何在 Transfer 系列中運作

AWS 最近宣布支援 SFTP 檔案傳輸中的後量子金鑰交換 AWS Transfer Family。Transfer Family 使用 SFTP 和其他通訊協定，安全地將business-to-business檔案傳輸擴展至 AWS 儲存服務。SFTP 是透過 SSH 執行之檔案傳輸通訊協定 (FTP) 的更安全版本。Transfer Family 的後量子金鑰交換支援提高透過 SFTP 傳輸資料的安全標準。

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 ML-KEM-768 和 ML-KEM-1024，以及透過 P256、P384 或 Curve25519 曲線的 ECDH。下列對應的 SSH 金鑰交換方法在[後量子混合 SSH 金鑰交換草案](#)中指定。

- mlkem768nistp256-sha256
- mlkem1024nistp384-sha384
- mlkem768x25519-sha256

為什麼選擇 ML-KEM？

AWS 致力於支援標準化、可互通的演算法。ML-KEM 是唯一經過 [NIST 後量子密碼編譯專案標準化和核准的後量子](#) 金鑰交換演算法。標準內文已將 ML-KEM 整合到通訊協定中。在某些 AWS API 端點中 AWS，已在 TLS 中支援 ML-KEM。

作為此承諾的一部分，AWS 已向 IETF 提交了量子後密碼編譯的草案提案，該提案結合了 ML-KEM 和 NIST 核准的曲線，例如 P256 for SSH。為了協助增強客戶的安全性，SFTP 和 SSH 中的後量子金鑰交換 AWS 實作遵循該草案。我們計劃支援未來的更新，直到 IETF 採用我們的提案並成為標準。

新的金鑰交換方法（列於第節[後量子混合金鑰建立如何在 Transfer 系列中運作](#)）可能會隨著草稿朝向標準化發展而變更。

Note

目前，TLS 中的後量子演算法支援可用於後量子混合金鑰交換 AWS KMS (請參閱[搭配使用混合後量子 TLS AWS KMS](#))AWS Certificate Manager、和 AWS Secrets Manager API 端點。

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 使用 FIPS 140 認證的開放原始碼密碼編譯程式庫 AWS-LC，在 SSH 中提供 AWS FIPS 核准的密碼編譯。TransferSecurityPolicy-FIPS-2025-03 in Transfer Family 中支援的後量子混合金鑰交換方法是根據 [NIST 的 SP 800-56Cr2 \(第 2 節\)](#) 核准的 FIPS。德國聯邦資訊安全辦公室 ([BSI](#)) 和法國的 Agence nationale de la sécurité des systèmes d'information ([ANSSI](#)) 也建議採用這種後量子混合金鑰交換方法。

在 Transfer Family 中測試後量子混合金鑰交換

本節說明您測試後量子混合金鑰交換所採取的步驟。

1. [在 SFTP 端點上啟用後量子混合金鑰交換](#)。
2. 遵循上述草案規格中的指引，使用支援量子後混合金鑰交換的 SFTP 用戶端 (例如 [設定支援後量子混合金鑰交換的 SFTP 用戶端](#))。
3. 使用 Transfer Family 伺服器傳輸檔案。
4. [在 SFTP 中確認後量子混合金鑰交換](#)。

在 SFTP 端點上啟用後量子混合金鑰交換

您可以在 Transfer Family 中建立新的 SFTP 伺服器端點時選擇 SSH 政策，或在現有的 SFTP 端點中編輯密碼編譯演算法選項。下列快照顯示 AWS 管理主控台 您更新 SSH 政策的 範例。

Cryptographic algorithm options Info

Security Policy

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

TransferSecurityPolicy-PQ-SSH-Experimental-2023-04 ▲

TransferSecurityPolicy-2018-11	
TransferSecurityPolicy-2020-06	
TransferSecurityPolicy-2022-03	
TransferSecurityPolicy-2023-05	
TransferSecurityPolicy-2024-01	
TransferSecurityPolicy-2025-03	✓
TransferSecurityPolicy-Restricted-2018-11	
TransferSecurityPolicy-Restricted-2020-06	



to it. Additi

支援後量子金鑰交換的 SSH 政策名稱為 TransferSecurityPolicy-2025-03 和 TransferSecurityPolicy-FIPS-2025-03。如需 Transfer Family 政策的詳細資訊，請參閱 [AWS Transfer Family 伺服器的安全政策](#)。

設定支援後量子混合金鑰交換的 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 中實驗後量子 SFTP。在本機系統上安裝要測試的最新 OpenSSH 用戶端（例如 9.9 版）。

Note

請確定您的用戶端支援先前列出的一或多個 ML-KEM 演算法。您可以執行此命令來檢視 OpenSSH 版本的支援演算法：`ssh -Q kex`。

您可以使用後量子混合金鑰交換方法，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 -v -o \
```

```
KexAlgorithms=mlkem768x25519-sha256 \  
-i username_private_key_PEM_file \  
username@server-id.server.transfer.region-id.amazonaws.com
```

在上一個命令中，將下列項目取代為您自己的資訊：

- 使用 SFTP 使用者的私有金鑰 PEM 編碼檔案取代 *username_private_key_PEM_file*
- 將#####取代為 SFTP 使用者名稱
- 將 *server-id* 取代為 Transfer Family 伺服器 ID
- 將 *region-id* 取代為 Transfer Family 伺服器所在的實際區域

在 SFTP 中確認後量子混合金鑰交換

若要確認在 SFTP 到 Transfer Family 的 SSH 連線期間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 OpenSSH 9.9 用戶端，輸出看起來應該類似以下內容（為了簡潔起見而省略不相關的資訊）：

```
% sftp -o KexAlgorithms=mlkem768x25519-sha256 -v -o IdentitiesOnly=yes -  
i username_private_key_PEM_file username@s-1111aaaa2222bbbb3.server.transfer.us-  
west-2.amazonaws.com  
OpenSSH_9.9p2, OpenSSL 3.4.1 11 Feb 2025  
debug1: Reading configuration data /Users/username/.ssh/config  
debug1: /Users/username/.ssh/config line 146: Applying options for *  
debug1: Reading configuration data /Users/username/.ssh/bastions-config  
debug1: Reading configuration data /opt/homebrew/etc/ssh/ssh_config  
debug1: Connecting to s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com  
[xxx.yyy.zzz.nnn] port 22.  
debug1: Connection established.  
[...]  
debug1: Local version string SSH-2.0-OpenSSH_9.9  
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 /Users/username/.ssh/known_hosts2: No such file or  
directory  
[...]  
debug1: SSH2_MSG_KEXINIT sent  
debug1: SSH2_MSG_KEXINIT received  
debug1: kex: algorithm: mlkem768x25519-sha256  
debug1: kex: host key algorithm: ssh-ed25519
```



```
debug1: kex: server->client cipher: aes128-ctr MAC: hmac-sha2-256-etm@openssh.com
compression: none
debug1: kex: client->server cipher: aes128-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:Ic1Ti0cdDmFdStj06rfU0cmmNccwAha/ASH2unr6zX0
[...]
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 s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com
([xxx.yyy.zzz.nnn]:22) using "publickey".
debug1: channel 0: new session [client-session] (inactive timeout: 0)
[...]
Connected to s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com.
sftp>
```

輸出顯示使用後量子混合mlkem768x25519-sha256方法進行用戶端交涉，並成功建立 SFTP 工作階段。

資料保護和加密

AWS [共同責任模型](#)適用於 AWS Transfer Family (Transfer 系列) 中的資料保護。如此模型所述，AWS 負責保護執行所有 AWS 雲端的全球基礎設施。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[資料隱私權常見問答集](#)。如需歐洲資料保護的相關資訊，請參閱安全部落格上的[AWS 共同責任模型和 GDPR](#) AWS 部落格文章。

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

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源通訊。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。

- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Simple Storage Service (Amazon Simple Storage Service (Amazon S3)) 的個人資料。
- 如果您在透過命令列介面或 API 存取 AWS 時，需要 FIPS 140-2 驗證的加密模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的詳細資訊，請參閱[聯邦資訊處理標準 \(FIPS\) 140-2 概觀](#)。

我們強烈建議您絕對不要將客戶帳戶號碼等敏感的識別資訊，放在自由格式的欄位中，例如名稱欄位。這包括當您使用 Transfer Family 或使用主控台、API AWS CLI 或 AWS SDKs 的其他 AWS 服務時。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，都可能被選入診斷日誌中。當您提供外部伺服器的 URL 時，請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

相反地，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。只有獲得授權的人員才能存取此資料。

Transfer 系列中的資料加密

AWS Transfer Family 會使用您為 Amazon S3 儲存貯體設定的預設加密選項來加密您的資料。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。透過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-KMS) 來加密物件。如需有關伺服器端加密的資訊，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。

在 中允許加密 AWS Transfer Family

1. 為您的 Amazon S3 儲存貯體啟用預設加密。如需說明，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，以授予必要的 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，授予使用 AWS Transfer Family 搭配已啟用 AWS KMS 加密的 Amazon S3 儲存貯體時所需的最低許可。如果您使用的是 ，請在使用者 IAM 角色政策和工作階段政策中包含此範例政策。

```
{
  "Sid": "Stmt1544140969635",
  "Action": [
```

```
"kms:Decrypt",
"kms:Encrypt",
"kms:GenerateDataKey",
"kms:GetPublicKey",
"kms:ListKeyPolicies"
],
"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 KMS 金鑰 ID 相同。AWS KMS 金鑰政策中必須允許根角色或用於使用者的 IAM 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[在 AWS KMS 中使用金鑰政策](#)。

AWS Transfer Family 靜態加密

由於 AWS Transfer Family 是檔案傳輸服務，因此不會管理您的靜態儲存資料。AWS Transfer Family 支援的儲存服務和系統負責保護該狀態下的資料。不過，有一些服務相關資料會 AWS Transfer Family 管理靜態。

加密的內容為何？

唯一 AWS Transfer Family 處理靜態資料與操作檔案傳輸伺服器和處理傳輸所需的詳細資訊相關。會在 Amazon DynamoDB 中使用完整靜態加密來 AWS Transfer Family 存放下列資料：

- 伺服器組態（例如，伺服器設定、通訊協定組態和端點詳細資訊）。
- 使用者身分驗證資料，包括 SSH 公有金鑰和使用者中繼資料。
- 工作流程執行詳細資訊和步驟組態。
- 第三方系統的連接器組態和身分驗證登入資料。這些登入資料會使用 AWS Transfer Family 受管加密金鑰進行加密。

金鑰管理

您無法管理 AWS Transfer Family 用來在 DynamoDB 中存放與執行伺服器和處理傳輸相關資訊的加密金鑰。此資訊包含您的伺服器組態、使用者身分驗證資料、工作流程詳細資訊和連接器登入資料。

哪些項目未加密？

雖然 AWS Transfer Family 無法控制儲存資料的靜態加密方式，但仍建議使用其支援的最高安全性來設定儲存位置。例如，您可以使用 Amazon S3 受管加密金鑰 (SSE-S3) 或 AWS KMS 金鑰 (SSE-KMS) 來加密物件。

進一步了解 AWS 儲存服務如何加密靜態資料：

- [Amazon S3](#)
- [Amazon EFS](#)

管理 Transfer 系列中的 SSH 和 PGP 金鑰

在本節中，您可以找到 SSH 金鑰的相關資訊，包括如何產生金鑰以及如何輪換金鑰。如需使用 Transfer Family 搭配 AWS Lambda 來管理金鑰的詳細資訊，請參閱部落格文章[使用 AWS Transfer Family 和 啟用使用者自助式金鑰管理 AWS Lambda](#)。如需具有多個 SSH 金鑰之使用者的自動化部署和管理，請參閱 [Transfer 系列 Terraform 模組](#)。

Note

AWS Transfer Family 接受 RSA、ECDSA 和 ED25519 金鑰進行 SSH 身分驗證。

本節也涵蓋如何產生和管理 Pretty Good Privacy (PGP) 金鑰。

如需所有支援的加密和金鑰演算法的完整概觀，包括不同使用案例的建議，請參閱 [加密和金鑰演算法概觀](#)。

加密和金鑰演算法概觀

AWS Transfer Family 支援不同類型的演算法用於不同的用途。了解要用於特定使用案例的演算法，有助於確保安全且相容的檔案傳輸。

演算法快速參考

使用案例	建議的演算法	符合 FIPS 規範	備註
SSH/SFTP 身分驗證	RSA (rsa-sha2-256/512)、ECDSA 或 ED25519	RSA：是，ECD	與所有 SSH 用戶端和伺服器相容

使用案例	建議的演算法	符合 FIPS 規範	備註
		SA : 是 , ED25519 : 否	
PGP 金鑰產生	RSA 或 ECC (NIST)	是	對於工作流程解密
PGP 檔案加密	AES-256	是	由 PGP 軟體決定

SSH 身分驗證演算法

這些演算法用於用戶端和 AWS Transfer Family 伺服器之間的 SSH/SFTP 身分驗證。為使用者身分驗證或伺服器主機金鑰產生 SSH 金鑰對時，請選擇其中一項。

RSA (建議)

與所有 SSH 用戶端和伺服器相容，且符合 FIPS 規範。搭配 SHA-2 雜湊使用 可增強安全性：

- `rsa-sha2-256` - 建議大多數使用案例使用
- `rsa-sha2-512` - 更高的安全選項

ED25519

現代化且高效率。具有強大安全性的較小金鑰大小：

- `ssh-ed25519` - 快速且安全，但不符合 FIPS

ECDSA

橢圓曲線選項。安全與效能的良好平衡：

- `ecdsa-sha2-nistp256` - 標準曲線
- `ecdsa-sha2-nistp384` - 更高的安全曲線
- `ecdsa-sha2-nistp521` - 最高安全性曲線

Note

我們支援`ssh-rsa`舊版安全政策的 SHA1。如需詳細資訊，請參閱[密碼編譯演算法](#)。

選擇正確的 SSH 演算法

- 對於大多數使用者：搭配 `rsa-sha2-256` 或 使用 RSA `rsa-sha2-512`
- 針對 FIPS 合規：使用 RSA 或 ECDSA 演算法
- 對於現代環境：ED25519 提供卓越的安全性和效能

PGP 加密和解密演算法

PGP (Pretty Good Privacy) 使用兩種類型的演算法，共同加密和解密工作流程中的檔案：

1. 金鑰對演算法 - 用來產生加密和數位簽章的公有/私有金鑰對
2. 對稱演算法 - 用於加密實際檔案資料（金鑰對演算法加密對稱金鑰）

PGP 金鑰對演算法

為工作流程解密產生 PGP 金鑰對時，請選擇下列其中一種演算法：

RSA（建議）

建議大多數使用者使用。廣泛支援、建立良好且符合 FIPS 規範。在安全性和相容性之間取得良好的平衡。

ECC（橢圓曲線密碼編譯）

比具有較小金鑰大小的 RSA 更有效率，同時維持強大的安全性：

- NIST 曲線 - 廣泛支援且符合 FIPS 標準曲線
- BrainPool 曲線 - 特定合規要求的替代曲線
- Curve25519 - 現代高效能曲線提供強大的安全性和高效率的運算

ElGamal

舊版演算法。支援與舊版系統相容。使用 RSA 或 ECC 進行新實作。

如需產生 PGP 金鑰的詳細說明，請參閱 [產生 PGP 金鑰](#)。

PGP 對稱加密演算法

這些演算法會加密您的實際檔案資料。使用的演算法取決於 PGP 軟體如何建立 PGP 檔案：

FIPS 相容演算法（建議用於受管制的環境）

- AES-128、AES-192、AES-256 - 進階加密標準（建議）
- 3DES - 三重資料加密標準（舊版，盡可能使用 AES）

其他支援的演算法

- IDEA、CAST5、Blowfish、DES、TwoFish、CAMELLIA-128、CAMELLIA-192、CAMELLIA-256

Note

您不 AWS Transfer Family 在使用工作流程時直接選擇對稱演算法 - 由用來建立加密檔案的 PGP 軟體決定。不過，您可以將 PGP 軟體設定為偏好符合 FIPS 的演算法，例如 AES-256。

如需支援的對稱演算法的詳細資訊，請參閱 [支援的對稱加密演算法](#)。

為服務受管使用者產生 SSH 金鑰

您可以設定伺服器，以使用服務受管身分驗證方法對使用者進行身分驗證，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至伺服器。伺服器會使用此金鑰做為標準金鑰型身分驗證程序的一部分。每個使用者都可以針對個別伺服器上的檔案擁有多個公有 SSH 金鑰。如需每個使用者可存放的金鑰數量限制，請參閱中的 [AWS Transfer Family 端點和配額](#) Amazon Web Services 一般參考。

做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對使用者進行身分驗證，或者 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 for Microsoft Active Directory](#)。

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，且該方法無法在建立伺服器之後變更。

主題

- [在 macOS、Linux 或 Unix 上建立 SSH 金鑰](#)
- [在 Microsoft Windows 上建立 SSH 金鑰](#)
- [將 SSH2 金鑰轉換為 SSH 公有金鑰格式](#)

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。

Note

在下列範例中，我們不會指定密碼短語：在此情況下，工具會要求您輸入密碼短語，然後重複它進行驗證。建立密碼短語可為您的私有金鑰提供更好的保護，也可能改善整體系統安全性。

您無法復原密碼短語：如果您忘記密碼短語，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）來指定空密碼短語，因為 Transfer Family 伺服器無法在啟動時請求密碼。

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-formatted 的金鑰。根據您要產生的金鑰對類型選擇適當的命令。

秘訣：*key_name* 將取代為 SSH 金鑰對檔案的實際名稱。

- 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 的位元大小為 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
```

以下顯示 `ssh-keygen` 輸出的範例。

```
ssh-keygen -t rsa -b 4096 -f key_name
Generating public/private rsa key pair.
```



```

Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in key_name.
Your public key has been saved in key_name.pub.
The key fingerprint is:
SHA256:8tDDwPmanTFcEzjTwPGETVW0GW1nVz+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]-----+

```

秘訣：執行上述ssh-keygen命令時，它會將公有和私有金鑰建立為目前目錄中的檔案。

您的 SSH 金鑰對現在已準備好可供使用。請遵循步驟 3 和 4，為您的服務受管使用者存放 SSH 公有金鑰。這些使用者會在 Transfer Family 伺服器端點上傳檔案時使用金鑰。

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 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台，然後從導覽窗格中選取伺服器。
 - b. 在伺服器頁面上，選取包含您要更新之使用者之伺服器的伺服器 ID。
 - c. 選取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 'User configuration' with an 'Edit' button. It is divided into two columns: 'Role' (with a 'Role' link) and 'Policy' (with a 'View' button). Below these are 'Posix Profile' and 'Home directory' sections. The 'Posix Profile' section shows 'User ID' as 2001, 'Group ID' as 2001, and 'Secondary Group IDs' as an empty array. The 'Home directory' section shows a path like '/fs-[redacted]/[redacted]' and a 'Restricted' checkbox. Below this is the 'SSH public keys (1)' section, which includes a 'Delete' button, an 'Add SSH public key' button, and a table of existing keys. The table has 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	Policy View
Posix Profile	Home directory
User ID 2001	/fs-[redacted]/[redacted]
Group ID 2001	Restricted
Secondary Group IDs -	

SSH public keys (1) [Delete](#) [Add SSH public key](#)

☐	Date imported	Fingerprint
☐	6/14/2022, 12:53:34 PM	SHA256-[redacted]

- 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 section is 'SSH public keys'. It contains a heading 'SSH public key' with an 'Info' link, followed by the instruction 'Paste the contents of SSH public key'. Below this is a large text input field with a placeholder 'Enter SSH public key'. At the bottom right are 'Cancel' and 'Add key' buttons.

Transfer Family > Servers > s-[server icon] > OneUser > Add key

Add key

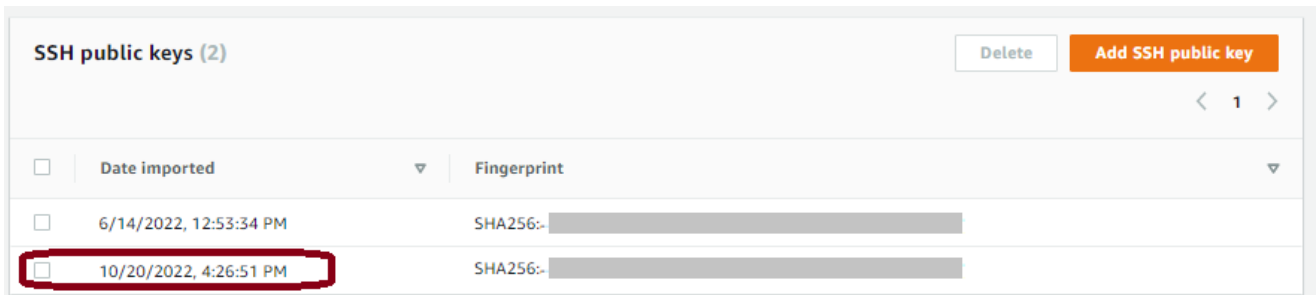
SSH public keys

SSH public key [Info](#)
Paste the contents of SSH public key

Enter SSH public key

[Cancel](#) [Add key](#)

新金鑰會列在 SSH 公有金鑰窗格中。



SSH public keys (2)		Delete	Add SSH public key
☐	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 包含 OpenSSH 作為內建功能，您可以使用它在 Linux 或 macOS 上產生相同格式的 SSH 金鑰。或者，您可以使用第三方工具，例如 PuTTY 的金鑰產生器 (PuTTYgen)。

使用 Windows 內建 OpenSSH

根據預設，Windows 的最近版本包括 OpenSSH。您可以使用與 macOS/Linux 章節所述的相同 `ssh-keygen` 命令：

1. 開啟 Windows PowerShell 或命令提示字元。
2. 根據您要產生的金鑰類型執行下列其中一個命令：

- 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：

```
ssh-keygen -t ecdsa -b 521 -f key_name
```

- 若要產生 ED25519 金鑰對：

```
ssh-keygen -t ed25519 -f key_name
```

3. 請依照與 macOS/Linux 區段相同的步驟，將公有金鑰上傳至其中 AWS Transfer Family。

使用 PuTTYgen (第三方工具)

某些適用於 Windows 的第三方 SSH 用戶端，例如 PuTTY，使用不同的金鑰格式。PuTTY 使用私有金鑰的 PPK 格式。如果您使用的是 PuTTY 或 WinSCP 等相關工具，您可以使用 PuTTYgen 以此格式建立金鑰。

Note

如果您使用非 .ppk 格式的私有金鑰檔案呈現 WinSCP，該用戶端會為您提供將金鑰轉換為 .ppk 格式的。

如需使用 PuTTYgen 建立 SSH 金鑰的教學課程，請參閱 [SSH.com : // 網站](https://www.ssh.com/)。

將 SSH2 金鑰轉換為 SSH 公有金鑰格式

AWS Transfer Family 僅接受 SSH 格式的公有金鑰。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 -----
```

SSH 公有金鑰的格式如下：

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAA...
```

執行下列命令，將 SSH2-formatted 的公有金鑰轉換為 SSH 格式的公有金鑰。將 *ssh2-key* 取代為您的 SSH2 金鑰名稱，將 *ssh-key* 取代為您的 SSH 金鑰名稱。

```
ssh-keygen -i -f ssh2-key.pub > ssh-key.pub
```

輪換 SSH 金鑰

為了安全起見，我們建議輪換 SSH 金鑰的最佳實務。通常，此輪換會指定為安全政策的一部分，並以某種自動化方式實作。根據安全性層級，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，存放 SSH 登入資料一段時間，並設定不會對使用者造成過度負擔的間隔，會更為常見。常見的間隔是三個月。

Note

如需使用基礎設施做為程式碼的自動 SSH 金鑰輪換，請參閱 [Transfer 系列 Terraform 模組](#)。

執行 SSH 金鑰輪換的方法有兩種：

- 在主控台上，您可以上傳新的 SSH 公有金鑰，並刪除現有的 SSH 公有金鑰。
- 您可以使用 API 更新現有的使用者，方法是使用 [DeleteSshPublicKey](#) API 刪除使用者的 Secure Shell (SSH) 公有金鑰，並使用 [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輪換

1. 在 <https://console.aws.amazon.com/transfer/> 開啟 AWS Transfer Family 主控台。
2. 導覽至伺服器頁面。
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，選取您要輪換其 SSH 公有金鑰之使用者的核取方塊，然後選擇動作，然後選擇新增金鑰以查看新增金鑰頁面。

或

選擇使用者名稱以查看使用者詳細資訊頁面，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，金鑰開頭為 `ecdsa-sha2-nistp256`、`ecdsa-sha2-nistp384` 或 `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. 輸入字詞 確認刪除操作delete，然後選擇刪除。

API

使用 API 執行金鑰輪換

1. 在 macOS、Linux 或 Unix 作業系統上，開啟命令終端機。
2. 輸入下列命令，擷取您要刪除的 SSH 金鑰。若要使用此命令，請將 *serverID* 取代為 Transfer Family 伺服器的伺服器 ID，並將 取代*username*為您的使用者名稱。

```
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。您稍後需要在此程序中輸入此值。

```
"SshPublicKeys": [ { "SshPublicKeyBody": "public-key", "SshPublicKeyId":  
  "keyID",  
  "DateImported": 1621969331.072 } ],
```

3. 接著，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，請將 *serverID* 取代為 Transfer Family 伺服器的伺服器 ID、將 取代*username*為使用者名稱，並將 取代*public-key*為新公有金鑰的指紋。

```
aws transfer import-ssh-public-key --server-id='serverID' --user-name='username'  
  --ssh-public-key-body='public-key'
```

如果命令成功，則不會傳回任何輸出。

4. 最後，執行下列命令來刪除舊金鑰。若要使用此命令，請將 *serverID* 取代為 Transfer Family 伺服器的伺服器 ID、將 取代*username*為使用者名稱，並將 取代*keyID-from-step-2*為您在此程序的步驟 2 中複製的金鑰 ID 值

```
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 PGP 金鑰

您可以搭配 Transfer Family 使用工作流程處理的檔案，使用 Pretty Good Privacy (PGP) 解密。若要在工作流程步驟中使用解密，請提供 PGP 金鑰。如需 PGP 金鑰演算法的詳細資訊，包括建議和 FIPS 合規，請參閱 [PGP 金鑰對演算法](#)。

AWS 儲存部落格有一篇文章，說明如何簡單地解密檔案，而無需使用 Transfer Family Managed 工作流程撰寫任何程式碼、[使用 PGP 和 加密和解密檔案 AWS Transfer Family](#)。

您用來產生 PGP 金鑰的運算子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，請使用您的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/> : // 下載所需的內容。

安裝 PGP 金鑰產生器軟體之後，您可以執行 `gpg --full-gen-key` 或 `gpg --gen-key` 命令來產生金鑰對。

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`。當系統提示要建立的金鑰類型時，請選擇 RSA 或 ECC。如果您選擇 ECC，您可以從 中選擇橢圓曲線 Curve25519 的 NISTBrainPool 和 。

有用的 **gpg** 子命令

以下是一些適用於 的實用于命令 `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之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` – 此命令會針對產生金鑰時所使用的 *user-name*，匯出金鑰的公有金鑰部分。

管理 PGP 金鑰

若要管理您的 PGP 金鑰，請使用 AWS Secrets Manager。

Note

您的秘密名稱包含 Transfer Family 伺服器 ID。這表示在存放 PGP 金鑰資訊之前，您應該已識別或建立伺服器 AWS Secrets Manager。

如果您想要為所有使用者使用一個金鑰和複雜密碼，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 *user-name* 符合執行工作流程之使用者的金鑰，Transfer Family 會使用此預設金鑰。

您可以為特定使用者建立金鑰。在此情況下，秘密名稱的格式為 `aws/transfer/server-id/user-name`，其中 *user-name* 符合執行 Transfer Family 伺服器工作流程的使用者。

Note

每個使用者每個 Transfer Family 伺服器最多可存放 3 個 PGP 私有金鑰。

設定 PGP 金鑰以搭配解密使用

1. 根據您正在使用的 GPG 版本，執行下列其中一個命令來產生 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**，則可以 **Curve25519** 為橢圓曲線選擇 **NISTBrainPool1** 或 **Curve25519**。如果您 `gpg --gen-key` 改為執行 `gpg --full-gen-key`，您可以建立使用 ECC Curve 25519 加密演算法的金鑰對。

- 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，您必須提供密碼短語和電子郵件地址。請務必記下這些值。當您在此程序 AWS Secrets Manager 稍後的 中輸入金鑰的詳細資訊時，必須提供密碼短語。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 *private.pgp* 取代為儲存私有金鑰區塊的檔案名稱，並將 *marymajor@example.com* 取代為您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 PGP 金鑰。
 - a. 登入 AWS 管理主控台 並在 <https://console.aws.amazon.com/secretsmanager/> 開啟 AWS Secrets Manager 主控台。
 - 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

您必須完全輸入 **PGPPrivateKey** 字串：請勿在字元之前或之間新增任何空格。

- value – 將私有金鑰的文字貼到值欄位中。您可以在先前在此程序中匯出金鑰時指定的檔案中（例如 *private.pgp*），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. 選取新增資料列，然後在鍵/值對區段中，選擇鍵/值索引標籤。

- 金鑰 – 輸入 **PGPPassphrase**。

Note

您必須完全輸入**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短語。

Choose secret type

Secret type [Info](#)

☐ Credentials for Amazon RDS database
 ☐ Credentials for Amazon DocumentDB database
 ☐ Credentials for Amazon Redshift cluster
 ☒ 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.

aws/secretsmanager [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，請新增兩個新資料列，並為金鑰輸入 **PGPPassphrase2** **PGPPrivateKey2**和，然後貼上另一個私有金鑰和密碼片語。若要新增第三個集合，索引鍵值必須為 **PGPPrivateKey3**和 **PGPPassphrase3**。

g. 選擇下一步。

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，也就是任何 Transfer Family 使用者都可以使用的金鑰，請輸入 **aws/transfer/*server-id*/epgp-default**。*server-id* 將取代為包含具有解密步驟之工作流程的伺服器 ID。
- 如果您要建立要供特定 Transfer Family 使用者使用的金鑰，請輸入 **aws/transfer/*server-id*/*user-name***。*server-id* 將取代為包含具有解密步驟之工作流程的伺服器 ID，並將取代 *user-name* 為執行工作流程的使用者名稱。*user-name* 存放在 Transfer Family 伺服器正在使用的身分提供者中。
 - 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。
 - 在檢閱頁面上，選擇存放以建立和存放秘密。

下列螢幕擷取畫面顯示特定 Transfer Family 伺服器 **marymajor** 的使用者詳細資訊。此範例顯示三個金鑰及其對應的密碼短語。

The screenshot displays the AWS Secrets Manager console for a secret named `/aws/transfer/s-[redacted]/marymajor`. The secret is encrypted using `aws/secretsmanager`. The secret description states: "Contains the PGP secret keys and corresponding passphrases to use for user marymajor on Transfer Family server s-[redacted]".

The 'Secret value' section shows a table with columns 'Secret key' and 'Secret value'.

Secret key	Secret value
PGPPrivateKey	-----BEGIN PGP PRIVATE KEY BLOCK----- [redacted]
PGPPassphrase	mypassphrase
PGPPrivateKey2	-----BEGIN PGP PRIVATE KEY BLOCK----- [redacted]
PGPPassphrase2	mypassphrase2
PGPPrivateKey3	-----BEGIN PGP PRIVATE KEY BLOCK----- [redacted]
PGPPassphrase3	mypassphrase3

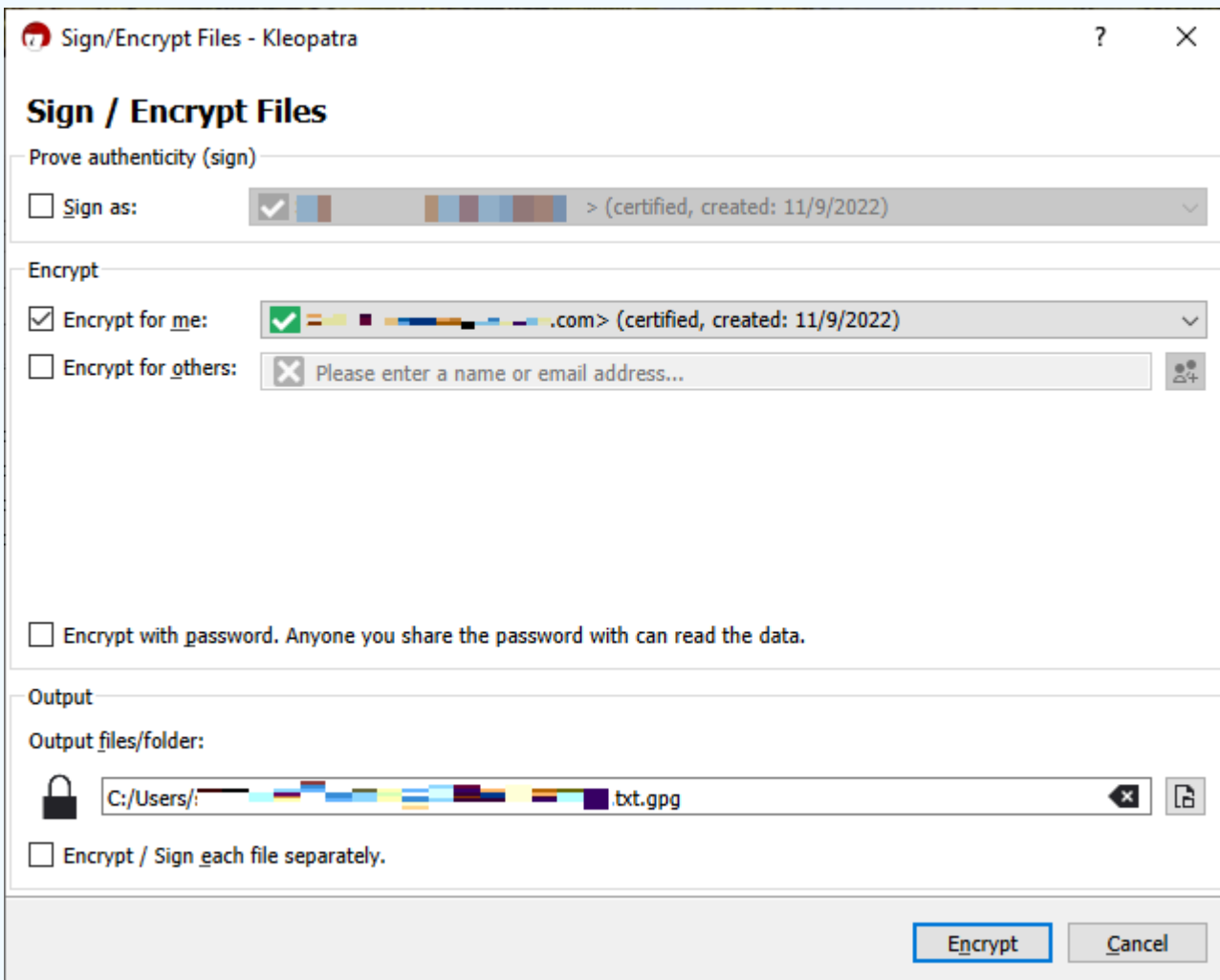
支援的 PGP 用戶端

下列用戶端已使用 Transfer Family 進行測試，可用於產生 PGP 金鑰，以及加密您想要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：我們目前不支援加密檔案的簽署。



The screenshot shows the 'Sign / Encrypt Files' dialog in Kleopatra. It has three main sections: 'Prove authenticity (sign)', 'Encrypt', and 'Output'. In the 'Prove authenticity' section, the 'Sign as:' dropdown is set to a specific identity. In the 'Encrypt' section, 'Encrypt for me:' is checked and set to the same identity, while 'Encrypt for others:' is unchecked. In the 'Output' section, the 'Output files/folder:' field shows a path ending in '.txt.gpg'. The 'Encrypt / Sign each file separately' checkbox is unchecked. At the bottom right, there are 'Encrypt' and 'Cancel' buttons.

如果您簽署加密的檔案並嘗試使用解密工作流程將其上傳至 Transfer Family 伺服器，您會收到下列錯誤：

Encrypted file with signed message unsupported

- 主要 GnuPG 版本：2.4、2.3、2.2、2.0 和 1.4。

請注意，其他 PGP 用戶端也可以運作，但只有此處提及的用戶端已經過 Transfer Family 測試。

的身分和存取管理 AWS Transfer Family

AWS Identity and Access Management (IAM) 是 AWS 服務，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員可控制誰可以進行驗證（登入）和授權（具有許可）來使用 AWS Transfer Family 資源。IAM 是您可以免費使用 AWS 服務的。

主題

- [目標對象](#)
- [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 身分和存取進行故障診斷](#)
- [組織控管的 IAM 條件索引鍵](#)

目標對象

使用方式 AWS Identity and Access Management (IAM) 會根據您的角色而有所不同：

- 服務使用者 — 若無法存取某些功能，請向管理員申請所需許可 (請參閱 [對 AWS Transfer Family 身分和存取進行故障診斷](#))
- 服務管理員 — 負責設定使用者存取權並提交相關許可請求 (請參閱 [AWS Transfer Family 如何使用 IAM](#))
- IAM 管理員 — 撰寫政策以管理存取控制 (請參閱 [AWS Transfer Family 身分型政策範例](#))

使用身分驗證

身分驗證是您 AWS 使用身分憑證登入的方式。您必須以 AWS 帳戶根使用者、IAM 使用者或擔任 IAM 角色身分進行身分驗證。

您可以使用身分來源的登入資料，例如 AWS IAM Identity Center (IAM Identity Center)、單一登入身分驗證或 Google/Facebook 登入資料，以聯合身分的形式登入。如需有關登入的詳細資訊，請參閱《AWS 登入 使用者指南》中的[如何登入您的 AWS 帳戶](#)。

對於程式設計存取，AWS 提供 SDK 和 CLI 以密碼編譯方式簽署請求。如需詳細資訊，請參閱《IAM 使用者指南》中的 [API 請求的AWS 第 4 版簽署程序](#)。

AWS 帳戶根使用者

當您建立時 AWS 帳戶，您會從一個名為 AWS 帳戶 theroot 使用者的登入身分開始，該身分具有對所有 AWS 服務和資源的完整存取權。強烈建議不要使用根使用者來執行日常任務。有關需要根使用者憑證的任務，請參閱《IAM 使用者指南》中的[需要根使用者憑證的任務](#)。

聯合身分

最佳實務是要求人類使用者使用聯合身分提供者，以 AWS 服務使用臨時憑證存取。

聯合身分是您企業目錄、Web 身分提供者的使用者，或使用來自身分來源的 AWS 服務憑證存取 Directory Service。聯合身分會擔任角色，而該角色會提供臨時憑證。

若需集中化管理存取權限，建議使用 AWS IAM Identity Center。如需詳細資訊，請參閱 AWS IAM Identity Center 使用者指南中的[什麼是 IAM Identity Center？](#)。

IAM 使用者和群組

IAM 使用者https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html是一種身分具備單人或應用程式的特定許可權。建議以臨時憑證取代具備長期憑證的 IAM 使用者。如需詳細資訊，請參閱《IAM 使用者指南》中的[要求人類使用者使用聯合身分提供者來 AWS 使用臨時憑證存取](#)。

[IAM 群組](#)會指定 IAM 使用者集合，使管理大量使用者的許可權更加輕鬆。如需詳細資訊，請參閱《IAM 使用者指南》中的[IAM 使用者的使用案例](#)。

IAM 角色

IAM 角色https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html的身分具有特定許可權，其可以提供臨時憑證。您可以透過[從使用者切換到 IAM 角色（主控台）](#)或呼叫 AWS CLI 或 AWS API 操作來擔任角色。如需詳細資訊，請參閱《IAM 使用者指南》中的[擔任角色的方法](#)。

IAM 角色適用於聯合身分使用者存取、臨時 IAM 使用者許可、跨帳戶存取權與跨服務存取，以及在 Amazon EC2 執行的應用程式。如需詳細資訊，請參閱《IAM 使用者指南》中的[IAM 中的快帳戶資源存取](#)。

使用政策管理存取權

您可以透過建立政策並將其連接到身分或資源 AWS 來控制 AWS 中的存取。政策定義與身分或資源相關聯的許可。當委託人提出請求時 AWS，會評估這些政策。大多數政策會以 JSON 文件 AWS 的形式存放在 中。如需進一步了解 JSON 政策文件，請參閱《IAM 使用者指南》中的 [JSON 政策概觀](#)。

管理員會使用政策，透過定義哪些主體可在哪些條件下對哪些資源執行動作，以指定可存取的範圍。

預設情況下，使用者和角色沒有許可。IAM 管理員會建立 IAM 政策並將其新增至角色，供使用者後續擔任。IAM 政策定義動作的許可，無論採用何種方式執行。

身分型政策

身分型政策是附加至身分 (使用者、使用者群組或角色) 的 JSON 許可政策文件。這類政策控制身分可對哪些資源執行哪些動作，以及適用的條件。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的[透過客戶管理政策定義自訂 IAM 許可](#)。

身分型政策可分為內嵌政策 (直接內嵌於單一身分) 與受管政策 (可附加至多個身分的獨立政策)。如需了解如何在受管政策及內嵌政策之間做選擇，請參閱《IAM 使用者指南》中的[在受管政策與內嵌政策之間選擇](#)。

資源型政策

資源型政策是附加到資源的 JSON 政策文件。範例包括 IAM 角色信任政策與 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。您必須在資源型政策中[指定主體](#)。

資源型政策是位於該服務中的內嵌政策。您無法在資源型政策中使用來自 IAM 的 AWS 受管政策。

存取控制清單 (ACL)

存取控制清單 (ACL) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

Amazon S3 AWS WAF 和 Amazon VPC 是支援 ACLs 的服務範例。如需進一步了解 ACL，請參閱《Amazon Simple Storage Service 開發人員指南》中的[存取控制清單 \(ACL\) 概觀](#)。

其他政策類型

AWS 支援其他政策類型，可設定更多常見政策類型授予的最大許可：

- 許可界限 — 設定身分型政策可授與 IAM 實體的最大許可。如需詳細資訊，請參閱《IAM 使用者指南》中的 [IAM 實體許可界限](#)。
- 服務控制政策 (SCP) — 為 AWS Organizations 中的組織或組織單位指定最大許可。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的 [服務控制政策](#)。
- 資源控制政策 (RCP) — 設定您帳戶中資源可用許可的上限。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的 [資源控制政策 \(RCP\)](#)。
- 工作階段政策 — 在以程式設計方式為角色或聯合身分使用者建立臨時工作階段時，以參數形式傳遞的進階政策。如需詳細資訊，請參《IAM 使用者指南》中的 [工作階段政策](#)。

多種政策類型

當多種類型的政策適用於請求時，產生的許可會更複雜而無法理解。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

在您使用 AWS Identity and Access Management (IAM) 來管理對的存取之前 AWS Transfer Family，您應該了解可使用哪些 IAM 功能 AWS Transfer Family。若要全面了解 AWS Transfer Family 和其他 AWS 服務如何與 IAM 搭配使用，請參閱《[AWS IAM 使用者指南](#)》中的與 IAM 搭配使用的 [服務](#)。

主題

- [AWS Transfer Family 身分型政策](#)
- [AWS Transfer Family 資源型政策](#)
- [以 AWS Transfer Family 標籤為基礎的授權](#)
- [AWS Transfer Family IAM 角色](#)

AWS Transfer Family 身分型政策

使用 IAM 身分類型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下會允許或拒絕動作。AWS Transfer Family 支援特定動作、資源及條件索引鍵。若要了解您在 JSON 政策中使用的所有元素，請參閱 AWS Identity and Access Management 《使用者指南》中的 [IAM JSON 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 元素描述您可以用來允許或拒絕政策中存取的動作。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，使用 Transfer Family CreateServer API 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》中的 [定義的動作 AWS Transfer Family](#)。

Resources

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Resource JSON 政策元素可指定要套用動作的物件。最佳實務是使用其 [Amazon Resource Name \(ARN\)](#) 來指定資源。若動作不支援資源層級許可，使用萬用字元 (*) 表示該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 ARNs 格式的詳細資訊，請參閱服務授權參考中的 [Amazon Resource Name \(ARNs\)](#)，或 IAM [使用者指南中的 IAM ARNs](#)。

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項資源，請使用逗號分隔 ARN。

```
"Resource": [  
    "resource1",  
    "resource2"  
]
```

若要查看 AWS Transfer Family 資源清單，請參閱《服務授權參考》中的 [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 元素會根據定義的條件，指定陳述式的執行時機。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，也支援使用一些全域條件金鑰。若要查看 AWS Transfer Family 條件索引鍵的清單，請參閱《服務授權參考》中的 [的條件索引鍵 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](#)。如需 VPC 端點特定的 IAM 政策，請參閱 [限制 Transfer Family 伺服器的 VPC 端點存取](#)。

AWS Transfer Family 資源型政策

以資源為基礎的政策是 JSON 政策文件，指定指定委託人可以在 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。資源型政策可讓您依資源將使用許可授予至其他帳戶。您也可以使用資源型政策，允許 AWS 服務存取您的 Amazon S3 #####。

若要啟用跨帳戶存取，您可以指定在其他帳戶內的所有帳戶或 IAM 實體，作為[資源型政策的委託人](#)。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當委託人和資源位於不同的 AWS 帳戶中時，您還必須授予委託人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 角色與以資源為基礎的政策有何不同](#)。

Amazon S3 服務僅支援一種資源型政策，稱為儲存#體政策，連接到儲存##。此政策定義哪些主體實體（帳戶、使用者、角色和聯合身分使用者）可以對物件執行動作。

範例

若要檢視以 AWS Transfer Family 資源為基礎的政策範例，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，或在請求中將標籤傳遞至其中 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 使用臨時登入資料 AWS Transfer Family

您可以搭配聯合使用暫時憑證、擔任 IAM 角色，或是擔任跨帳戶角色。您可以透過呼叫 [AssumeRole](#) 或 [GetFederationToken](#) 等 AWS STS API 操作來取得臨時安全登入資料。

AWS Transfer Family 支援使用臨時登入資料。

AWS Transfer Family 身分型政策範例

根據預設，IAM 使用者和角色不具備建立或修改 AWS Transfer Family 資源的許可。他們也無法使用 AWS 管理主控台 AWS CLI 或 AWS API 執行任務。IAM 管理員必須建立 IAM 政策，授予使用者和角色在指定資源上執行特定 API 作業的所需許可。管理員接著必須將這些政策連接至需要這些許可的 IAM 使用者或群組。

若要了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱 AWS Identity and Access Management 《使用者指南》中的 [在 JSON 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

身分型政策會判斷您帳戶中的某個人員是否可以建立、存取或刪除 AWS Transfer Family 資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用將許可授予許多常見使用案例的 AWS 受管政策。它們可在您的 中使用 AWS 帳戶。我們建議您定義特定於使用案例 AWS 的客戶受管政策，以進一步減少許可。如需更多資訊，請參閱《IAM 使用者指南》中的 [AWS 受管政策](#) 或 [任務職能的 AWS 受管政策](#)。
- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱《IAM 使用者指南》中的 [IAM 中的政策和許可](#)。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。如果透過特定 例如 使用服務動作 AWS 服務，您也可以使用條件來授予其存取權 CloudFormation。如需詳細資訊，請參閱《IAM 使用者指南》中的 [IAM JSON 政策元素：條件](#)。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您撰寫安全且實用的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的 [使用 IAM Access Analyzer 驗證政策](#)。

- 需要多重要素驗證 (MFA) – 如果您的案例需要 IAM 使用者或 中的根使用者 AWS 帳戶，請開啟 MFA 以提高安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的[透過 MFA 的安全 API 存取](#)。

如需 IAM 中最佳實務的相關資訊，請參閱《IAM 使用者指南》中的 [IAM 安全最佳實務](#)。

使用 AWS Transfer Family 主控台

若要存取 AWS Transfer Family 主控台，您必須擁有一組最低許可。這些許可必須允許您列出和檢視 AWS 帳戶中 AWS Transfer Family 資源的詳細資訊。如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (IAM 使用者或角色) 而言，主控台就無法如預期運作。如需詳細資訊，請參閱 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 AWS API 進行呼叫的使用者，您不需要允許最低主控台許可。反之，只需允許存取符合您嘗試執行之 API 操作的動作就可以了。

允許使用者檢視他們自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視附加到他們使用者身分的內嵌及受管政策。此政策包含在主控台或使用 或 AWS CLI AWS API 以程式設計方式完成此動作的許可。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsForUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",
```

```

        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
    ],
    "Resource": "*"
}
]
}

```

AWS Transfer Family 標籤型政策範例

以下是如何根據標籤控制 AWS Transfer Family 資源存取的範例。

使用標籤控制對 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](#)》中的 [AWS 一般參考](#)。

在 AWS Transfer Family 中，資源可以有標籤，而某些動作可以包含標籤。建立 IAM 政策時，可使用標籤條件索引鍵來控制以下項目：

- 哪些使用者可以根據 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。您可以建立 IAM 政策，根據請求中提供的標籤（請求標籤）來允許或拒絕操作。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，資源標籤適用於已存在於資源上的標籤，當您將標籤新增至資源或從中移除標籤時，請求標籤適用於。

如需標籤條件索引鍵的完整語法和語意，請參閱《IAM 使用者指南》中的[使用資源標籤控制 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《[API Gateway 開發人員指南](#)》中的[使用 IAM 許可控制對 API 的存取](#)。

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以金鑰 和值 標記，則下列範例政策會拒絕 DescribeServer、TagResourceUntagResourceStartServerStopServer、stage 和 DescribeUser操作prod。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "transfer:TagResource",
        "transfer:UntagResource",
        "transfer:StartServer",
        "transfer:StopServer",
        "transfer:DescribeServer",
        "transfer:DescribeUser"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/stage": "prod"
        }
      }
    }
  ]
}
```

範例 2：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以 金鑰和 值 標記，則下列範例政策允許 TagResource UntagResourceDescribeServer、StartServerStopServer、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：根據請求標籤拒絕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索引鍵沒有值，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索引鍵包含除 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 `costcenter` 的金鑰和 1、2 或 3 的值。

```

{
  "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 身分和存取進行故障診斷

使用以下資訊來協助您診斷和修正使用 AWS Transfer Family 和 IAM 時可能遇到的常見問題。

主題

- [我無權在 中執行動作 AWS Transfer Family](#)
- [我未獲得執行 iam:PassRole 的授權](#)
- [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 管理主控台 告訴您無權執行 動作，則必須聯絡您的管理員尋求協助。您的管理員是為您提供簽署憑證的人員。

以下範例錯誤會在 mateojackson IAM 使用者嘗試使用主控台檢視 *widget* 的詳細資訊，但卻沒有 `transfer:GetWidget` 許可時發生。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
transfer:GetWidget on resource: my-example-widget
```

在此情況下，Mateo 會請求管理員更新他的政策，允許他使用 *my-example-widget* 動作存取 `transfer::GetWidget` 資源。

我未獲得執行 iam:PassRole 的授權

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 服務可讓您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

名為 marymajor 的 IAM 使用者嘗試使用主控台在 AWS Transfer Family 中執行動作時，發生下列範例錯誤。但是，動作要求服務具備服務角色授予的許可。Mary 沒有將角色傳遞給服務的許可。

```
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。

下列範例政策包含傳遞角色的許可 AWS Transfer Family。**123456789012** 將取代為您的 AWS 帳戶 ID，並將 **MyTransferRole** 取代為您的實際 IAM 角色名稱。

```
{
  "Version": "2012-10-17",
  "Statement": [
    { "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::123456789012:role/MyTransferRole",
      "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。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

如需進一步了解，請參閱以下內容：

- 若要了解 是否 AWS Transfer Family 支援這些功能，請參閱 [AWS Transfer Family 如何使用 IAM](#)。
- 若要了解如何在您擁有 AWS 帳戶 的 資源之間提供存取權，請參閱 [《IAM 使用者指南》中的在您擁有 AWS 帳戶 的另一個 IAM 使用者中提供存取權](#)。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱 [《IAM 使用者指南》中的將存取權提供給第三方 AWS 帳戶 擁有](#)。
- 如需了解如何透過聯合身分提供存取權，請參閱 [《IAM 使用者指南》中的將存取權提供給在外部進行身分驗證的使用者 \(聯合身分\)](#)。
- 如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱 [《IAM 使用者指南》中的 IAM 中的跨帳戶資源存取](#)。

組織控管的 IAM 條件索引鍵

AWS Transfer Family 提供 IAM 條件金鑰，可讓您限制任何 IAM 政策中的資源組態。這些條件金鑰可用於連接到使用者或角色的身分型政策，或用於組織控管的服務控制政策 (SCPs)。

服務控制政策是適用於整個 AWS 組織的 IAM 政策，可為多個帳戶提供預防性護欄。在 SCPs 中使用時，這些條件金鑰有助於在整個組織範圍內強制執行安全與合規要求。

另請參閱

- [Transfer 系列的動作、資源和條件索引鍵](#)
- [服務控制政策 \(SCP\)](#)
- 檢視[此影片](#)，說明如何使用服務控制政策強制執行預防性護欄

可用的條件索引鍵

AWS Transfer Family 支援下列條件金鑰，可用於 IAM 政策：

`transfer:RequestServerEndpointType`

根據端點類型 (PUBLIC、VPC、VPC_ENDPOINT) 限制伺服器建立和更新。通常用於防止公開端點。

`transfer:RequestServerProtocols`

根據支援的通訊協定 (SFTP、FTPS、FTP、AS2) 限制伺服器建立和更新。

`transfer:RequestServerDomain`

根據網域類型 (S3、EFS) 限制伺服器建立。

`transfer:RequestConnectorProtocol`

根據通訊協定 (AS2、SFTP) 限制連接器的建立。

支援的動作

條件索引鍵可套用至下列 AWS Transfer Family 動作：

- `CreateServer`：支援 `RequestServerEndpointType`、`RequestServerProtocols` 和 `RequestServerDomain` 條件索引鍵
- `UpdateServer`：支援 `RequestServerEndpointType` 和 `RequestServerProtocols` 條件索引鍵
- `CreateConnector`：支援 `RequestConnectorProtocol` 條件金鑰

範例 SCP 政策

下列範例 SCP 可防止整個組織的公有 AWS Transfer Family 伺服器建立：

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "DenyPublicTransferServers",
    "Effect": "Deny",
    "Action": ["transfer:CreateServer", "transfer:UpdateServer"],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "transfer:RequestServerEndpointType": "PUBLIC"
      }
    }
  }]
}
```

```
}  
    }  
  }  
}
```

的合規驗證 AWS Transfer Family

在多個合規計畫 AWS Transfer Family 中，第三方稽核人員會評估的安全與 AWS 合規。這些包括 SOC、PCI、HIPAA 等。如需完整清單，請參閱[AWS 合規計畫範圍內的服務](#)。

如需特定合規計畫範圍內 AWS 的服務清單，請參閱[AWS 合規計畫範圍內的服務](#)。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](#)。

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

- [安全與合規快速入門指南](#) – 這些部署指南討論架構考量，並提供部署以安全與合規為中心之基準環境的步驟 AWS。
- [HIPAA 安全與合規架構白皮書](#) – 此白皮書說明公司如何使用 AWS 來建立符合 HIPAA 規範的應用程式。
- [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符合內部實務、產業準則和法規的程度。
- [AWS Security Hub CSPM](#) – AWS 此服務提供內安全狀態的完整檢視 AWS，協助您檢查是否符合安全產業標準和最佳實務。

中的彈性 AWS Transfer Family

AWS 全球基礎設施是以 AWS 區域和可用區域為基礎建置。AWS 區域提供多個實體分隔和隔離的可用區域，這些可用區域以低延遲、高輸送量和高備援聯網連接。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、備援機群支援您的連線和傳輸請求。

對於所有 Transfer Family 端點：

- 可用區域層級備援內建於 服務中。
- 每個 AZ 都有備援機群。
- 此備援會自動提供。

Note

對於虛擬私有雲端 (VPC) 中的端點，可以提供單一子網路。不過，我們建議您在 VPC 內的多個可用區域中建立端點，以降低在可用區域中斷期間服務中斷的風險。

另請參閱

- 如需如何在 VPC 中建立 Transfer Family 伺服器的詳細資訊，請參閱 [在虛擬私有雲端中建立伺服器](#)。
- 如需 AWS 區域 和可用區域的詳細資訊，請參閱 [AWS 全球基礎設施](#)。
- 如需如何使用延遲型路由來建置 以獲得更高備援並將網路延遲降至最低的範例，請參閱部落格文章 [將 AWS Transfer Family 伺服器的網路延遲降至最低](#)。

在 VPC 和 AWS Transfer Family APIs 之間建立私有連線

您可以透過建立採用 [AWS PrivateLink](#) 技術的介面 VPC 端點，在 VPC 和 AWS Transfer Family APIs 之間建立私有連線。您可以像在 VPC 中一樣存取 AWS Transfer Family APIs，無需使用網際網路閘道、NAT 裝置、VPN 連接或 AWS Direct Connect 連接。VPC 中的執行個體不需要公有 IP 地址，即能與 AWS Transfer Family API 通訊。

我們會在您為介面端點啟用的每個子網中建立端點網路介面。如需詳細資訊，請參閱《[AWS PrivateLink 指南](#)》中的[透過 PrivateLink 存取 AWS 服務](#)。AWS PrivateLink 在您為 AWS Transfer Family APIs 設定介面 VPC 端點之前，請檢閱 AWS PrivateLink 指南中的[考量事項](#)。

使用 VPC 端點政策控制存取

根據預設，允許透過端點完整存取 AWS Transfer Family APIs。您可以使用 VPC 端點政策控制對介面端點的存取。您可以將端點政策連接至控制 API AWS Transfer Family APIs VPC 端點。此政策會指定下列資訊：

- 可執行動作的委託人。

- 可執行的動作。
- 可以對其執行動作的資源。

如需詳細資訊，請參閱 Amazon VPC 使用者指南中的[使用 VPC 端點控制對服務的存取](#)。

以下是 AWS Transfer Family APIs 端點政策的範例。連接至端點時，此政策會授予所有資源上所有 AWS Transfer Family APIs 動作的存取權，但已標記索引鍵 `Environment` 和值 `Test` 的資源除外。

```
{
  "Statement": [{
    "Effect": "Deny",
    "Action": "transfer:StartFileTransfer",
    "Principal": "*",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/Environment": "Test"
      }
    }
  }, {
    "Effect": "Allow",
    "Action": "transfer:*",
    "Principal": "*",
    "Resource": "*"
  }]
}
```

建立介面 VPC 端點 AWS Transfer Family APIs

您可以使用 Amazon VPC 主控台或 AWS 命令列界面 (CLI) 來建立適用於 AWS Transfer Family APIs 的 VPC 端點 AWS CLI。如需詳細資訊，請參閱 AWS PrivateLink 指南中的[建立 VPC 端點](#)。

使用下列其中一個服務名稱建立 VPC 端點 AWS Transfer Family APIs：

- `com.amazonaws.region.transfer`
- `com.amazonaws.region.transfer-fips` — 建立符合聯邦資訊處理標準 (FIPS) 出版物 140-3 美國政府標準的介面 VPC 端點。

如果您為端點啟用私有 DNS，您可以使用區域的預設 DNS 名稱向 AWS Transfer Family APIs 提出 API 請求，例如 `transfer.us-east-1.amazonaws.com`。

中的基礎設施安全性 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 AWS 安全服務和 如何 AWS 保護基礎設施的相關資訊，請參閱[AWS 雲端安全](#)。若要使用基礎設施安全的最佳實務設計您的 AWS 環境，請參閱安全支柱 AWS Well-Architected Framework 中的[基礎設施保護](#)。

您可以使用 AWS 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 並建議使用 TLS 1.3。
- 具備完美轉送私密(PFS)的密碼套件，例如 DHE (Ephemeral Diffie-Hellman)或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。現代系統(如 Java 7 和更新版本)大多會支援這些模式。

避免將 NLBs和 NATs放在 AWS Transfer Family 伺服器前面

Note

使用 FTP 和 FTPS 通訊協定設定的伺服器只允許使用 VPC 的組態：沒有可用於 FTP/FTPS 的公有端點。

許多客戶設定 Network Load Balancer (NLB) 將流量路由到其 AWS Transfer Family 伺服器。他們通常會這麼做，因為他們在 AWS 提供方法從 VPC 內部和網際網路存取伺服器，或支援網際網路上的 FTP。此組態不僅會增加客戶的成本，還可能導致其他問題，我們將在本節中說明。

當用戶端從公司防火牆後方的客戶私有網路連線時，NAT 閘道是強制性元件。不過，您應該知道，當許多用戶端位於相同的 NAT 閘道之後，這可能會影響效能和連線限制。如果從用戶端到 FTP 或 FTPS 伺服器的通訊路徑中有 NLB 或 NAT，則伺服器無法準確識別用戶端的 IP 地址，因為只會 AWS Transfer Family 看到 NLB 或 NAT 的 IP 地址。

如果您使用的是 NLB 後方 Transfer Family 伺服器的組態，建議您移至 VPC 端點並使用彈性 IP 地址，而不是使用 NLB。使用 NAT 閘道時，請注意以下所述的連線限制。

如果您使用的是 FTPS 通訊協定，此組態不僅會降低您稽核誰存取伺服器的能力，也會影響效能。AWS Transfer Family 會使用來源 IP 地址將您的連線分片到資料平面。對於 FTPS，這表示與 10,000 個同時連線不同，通訊路由上具有 NLB 或 NAT 閘道的 Transfer Family 伺服器僅限於 300 個同時連線。

雖然我們建議避免在 AWS Transfer Family 伺服器前面使用 Network Load Balancer，但如果您的 FTP 或 FTPS 實作需要用戶端通訊路由中的 NLB 或 NAT，請遵循下列建議：

- 對於 NLB，請使用連接埠 21 進行運作狀態檢查，而不是連接埠 8192-8200。
- 對於 AWS Transfer Family 伺服器，請設定來啟用 TLS 工作階段恢復 `TlsSessionResumptionMode = ENFORCED`。

Note

這是建議的模式，因為它提供增強的安全性：

- 要求用戶端對後續連線使用 TLS 工作階段恢復。
- 透過確保一致的加密參數，提供更強大的安全性保證。
- 有助於防止潛在的降級攻擊。
- 保持符合安全標準，同時最佳化效能。

- 如果可能，請遷移至不使用 NLB，以充分利用 AWS Transfer Family 效能和連線限制。

如需 NLB 替代方案的其他指引，請透過 AWS Support 聯絡 AWS Transfer Family 產品管理團隊。如需改善安全狀態的詳細資訊，請參閱部落格文章 [六個改善 AWS Transfer Family 伺服器安全性的秘訣](#)。

VPC 連線基礎設施安全性

具有 VPC 輸出類型的 SFTP 連接器透過網路隔離和私有連線提供增強的基礎設施安全性：

網路隔離的優點

- 私有網路流量：私有 SFTP 伺服器的所有連接器流量都會保留在您的 VPC 中，絕不會周遊公有網際網路。
- 控制輸出：對於透過 VPC 存取的公有端點，流量會透過 NAT 閘道路由，讓您控制輸出 IP 地址和網路政策。
- VPC 安全控制：利用現有的 VPC 安全群組、網路 ACLs 和路由表來控制連接器網路存取。
- 混合連線：透過已建立的 VPN 或 Direct Connect 連線存取內部部署 SFTP 伺服器，無需額外的網際網路暴露。

資源閘道安全性考量事項

資源閘道提供跨 VPC 資源存取的安全輸入點：

- 異地同步備份部署：資源閘道需要至少兩個可用區域中的子網路，以實現高可用性和容錯能力。
- 安全群組控制：設定安全群組以限制只能從授權來源存取 SFTP 連接埠（通常是連接埠 22）。
- 私有子網路置放：連線至私有 SFTP 伺服器以維持網路隔離時，在私有子網路中部署資源閘道。
- 連線限制：每個資源閘道支援最多 350 個並行連線，以及 TCP 連線的 350 秒閒置逾時。

新增 Web 應用程式防火牆

AWS WAF 是一種 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. 在以下網址開啟 API Gateway 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，選擇您要與此階段建立關聯的 Web ACL。
 - 如果您需要的 Web ACL 不存在，則需要執行下列動作來建立一個：
 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 ACL 的名稱。
 4. 在規則中，選擇新增規則，然後選擇新增我自己的規則和規則群組。
 5. 針對規則類型，選擇 IP 集以識別 IP 地址的特定清單。
 6. 在規則中，輸入規則的名稱。
 7. 針對 IP 集，選擇現有的 IP 集。若要建立 IP 集，請參閱[建立 IP 集](#)。

8. 若要使用 IP 地址做為原始地址，請在 標頭中選擇 IP 地址。
 9. 針對標頭欄位名稱，輸入 SourceIP。
 10. 針對標頭內的位置，選擇第一個 IP 地址。
 11. 對於遺失 IP 地址的備用，根據您希望如何處理標頭中的無效（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. 針對不符合任何規則之請求的預設 Web ACL 動作，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。

如需使用 AWS Web 應用程式防火牆保護 Transfer Family 安全的資訊，請參閱 AWS 儲存部落格中的[使用 AWS 應用程式防火牆和 Amazon API Gateway 保護 Transfer Family](#)。

預防跨服務混淆代理人

混淆代理人問題屬於安全性議題，其中沒有執行動作許可的實體可以強制具有更多許可的實體執行該動作。在中 AWS，跨服務模擬可能會導致混淆代理人問題。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。可以操縱呼叫服務，以使用其許可來對其他客戶的資源採取不應具有存取許可的方式。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》中的混淆代理人問題](#)。

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 對資源具有的許可。如果同時使用全域條件內容金鑰，則在相同政策陳述式中使用 `aws:SourceAccount` 值和 `aws:SourceArn` 值中的帳戶時，必須使用相同的帳戶 ID。

防範混淆代理人問題的最有效方法是精確使用您允許的資源 Amazon Resource Name (ARN) 資源。如果您要指定多個資源，請將 `aws:SourceArn` 全域內容條件金鑰與萬用字元 (*) 用於 ARN 的未知部分。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 ARN 的內容中擔任此角色。
- 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，存取角色會使用協議的 Amazon Resource Name (ARN)。對於傳出 AS2 傳輸，存取角色會使用連接器的 ARN。
- 調用角色 – 與 Amazon API Gateway 搭配使用，做為伺服器的自訂身分提供者。Transfer Family 會在 Transfer Family 伺服器 ARN 的內容中擔任此角色。
- 記錄角色 – 用來將項目記錄到 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 ARN 的內容中擔任此角色。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 ARN 的內容中擔任此角色。

如需詳細資訊，請參閱「IAM 使用者指南」中的 [IAM 中的政策和許可](#)。

 Note

在下列範例中，將每個#####取代為您自己的資訊。

 Note

在我們的範例中，我們同時使用 ArnLike 和 ArnEquals。它們的功能相同，因此您可以在建構政策時使用。Transfer Family 文件會在條件包含萬用字元 ArnLike 時使用，ArnEquals 並指出完全相符的條件。

AWS Transfer Family 使用者角色跨服務混淆代理人預防

下列範例政策允許帳戶中任何伺服器的任何使用者擔任該角色。

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

```

    "Principal": {
      "Service": "transfer.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      },
      "ArnLike": {
        "aws:SourceArn": "arn:aws:transfer:us-east-1:123456789012:user/"
      }
    }
  }
]
}

```

下列範例政策允許特定伺服器的任何使用者擔任該角色。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:transfer:us-east-1:123456789012:user/server-id"
        }
      }
    }
  ]
}

```

下列範例政策允許特定伺服器的特定使用者擔任該角色。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:transfer:us-east-1:123456789012:user/server-id/user-name"
        }
      }
    }
  ]
}
```

AWS Transfer 系列工作流程角色跨服務混淆代理人預防

下列範例政策允許 帳戶中的任何工作流程擔任該角色。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333"
        }
      }
    }
  ]
}
```

```

        "ArnLike": {
            "aws:SourceArn": "arn:aws:transfer:us-west-2:111122223333:workflow/*"
        }
    }
}
]
}

```

下列範例政策允許特定工作流程擔任該角色。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:transfer:us-west-2:111122223333:workflow/workflow-id"
        }
      }
    }
  ]
}

```

AWS Transfer 系列連接器角色跨服務混淆代理人預防

下列範例政策允許 帳戶中的任何連接器擔任該角色。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {

```

```

        "Sid": "",
        "Effect": "Allow",
        "Principal": {
            "Service": "transfer.amazonaws.com"
        },
        "Action": "sts:AssumeRole",
        "Condition": {
            "StringEquals": {
                "aws:SourceAccount": "123456789012"
            },
            "ArnLike": {
                "aws:SourceArn": "arn:aws:transfer:us-east-1:123456789012:connector/*"
            }
        }
    }
]
}

```

下列範例政策允許特定連接器擔任該角色。

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Service": "transfer.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:transfer:us-east-1:123456789012:connector/connector-id"
                }
            }
        }
    ]
}

```


AWS Transfer 系列記錄和調用角色跨服務混淆代理人預防

Note

下列範例可用於記錄和調用角色。

在這些範例中，如果您的伺服器沒有連接任何工作流程，您可以移除工作流程的 ARN 詳細資訊。

下列範例記錄/呼叫政策允許帳戶中的任何伺服器（和工作流程）擔任該角色。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAllServersWithWorkflowAttached",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333"
        },
        "ArnLike": {
          "aws:SourceArn": [
            "arn:aws:transfer:us-west-2:111122223333:server/*",
            "arn:aws:transfer:us-west-2:111122223333:workflow/*"
          ]
        }
      }
    }
  ]
}
```

下列範例記錄/叫用政策允許特定伺服器（和工作流程）擔任該角色。

```
{
```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "AllowSpecificServerWithWorkflowAttached",
    "Effect": "Allow",
    "Principal": {
      "Service": "transfer.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "111122223333"
      },
      "ArnEquals": {
        "aws:SourceArn": [
          "arn:aws:transfer:us-west-2:111122223333:server/server-id",
          "arn:aws:transfer:us-west-2:111122223333:workflow/workflow-id"
        ]
      }
    }
  }
]
}

```

AWS AWS Transfer Family 的 受管政策

若要新增許可給使用者、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 受管政策的更多相關資訊，請參閱「IAM 使用者指南」中的 [AWS 受管政策](#)。如需所有 AWS 受管政策的詳細清單，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 受管政策移除許可，因此政策更新不會破壞您現有的許可。

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。當服務啟動新功能時，會為新操作和資源 AWS 新增唯讀許可。如需任務職能政策的清單和說明，請參閱 IAM 使用者指南中 [有關任務職能的 AWS 受管政策](#)。

AWS 受管政策：AWSTransferConsoleFullAccess

此AWSTransferConsoleFullAccess政策透過 AWS 管理主控台提供 Transfer Family 的完整存取權。如需詳細資訊，請參閱 [AWS Transfer Family 的服務連結角色](#)。

AWS 受管政策：AWSTransferFullAccess

此AWSTransferFullAccess政策提供 Transfer Family 服務的完整存取權。如需詳細資訊，請參閱 [AWS Transfer Family 的服務連結角色](#)。

AWS 受管政策：AWSTransferLoggingAccess

此AWSTransferLoggingAccess政策授予 AWS Transfer Family 建立日誌串流和群組的完整存取權，並將日誌事件放入您的帳戶。如需詳細資訊，請參閱 [AWS Transfer Family 的服務連結角色](#)。

AWS 受管政策：AWSTransferReadOnlyAccess

此AWSTransferReadOnlyAccess政策提供 Transfer Family 服務的唯讀存取權。如需詳細資訊，請參閱 [AWS Transfer Family 的服務連結角色](#)。

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 AWS 受管政策更新的詳細資訊。如需有關此頁面變更的自動提醒，請訂閱 [的文件歷史記錄 AWS Transfer Family](#) 頁面的 RSS 摘要。

變更	描述	日期
文件更新	新增每個 Transfer Family 受管政策的區段。	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 開始追蹤其 AWS 受管政策的變更。	2021 年 6 月 15 日

Transfer 系列 Terraform 模組

[HashiCorp Terraform](#) 是使用 HashiCorp 組態語言 (HCL) 開發的開放原始碼基礎設施即程式碼 (IaC) 引擎。Terraform 提供一致的命令列界面 (CLI) 工作流程，搭配後端基礎設施的 AWS Transfer Family，可以管理數百個雲端服務，並將雲端 APIs 編譯為宣告式組態檔案。

您可以使用 Terraform 安全地部署 AWS Transfer Family SFTP 伺服器 and SFTP 連接器，以及相關聯的相依性和自訂。如需包含 Terraform 程式碼以建立執行 AWS Transfer Family 所需資源的儲存庫，請參閱 GitHub 上的 [Terraform Transfer Family 模組](#) 原始程式碼。

Note

Terraform 的 AWS Transfer Family 模組是社群支援的工作。它們不是 AWS 服務的一部分。最佳支援由 AWS Storage 社群提供。

SFTP 伺服器

此自動化為您提供可自訂的 Terraform 模組和 end-to-end 範例，以建立 SFTP 端點 (PUBLIC 或 VPC 端點類型)、與 Amazon CloudWatch 整合以用於記錄和監控、管理端點存取的使用者身分，以及設定 IAM 角色以存取存放檔案的 Amazon S3 儲存貯體。模組支援每個使用者多個 SSH 公有金鑰（最多 50 個金鑰），以增強安全性和金鑰輪換功能。

SFTP 連接器

AWS Transfer Family Terraform 模組現在支援部署 SFTP 連接器，以在 Amazon S3 和遠端 SFTP 伺服器之間傳輸檔案。SFTP 連接器提供全受管和低程式碼功能，可在 Amazon S3 和遠端 SFTP 伺服器之間複製檔案。

您現在可以使用 Terraform，以程式設計方式在單一部署中佈建 SFTP 連接器、相關聯的相依性和自訂。模組也提供 end-to-end 範例，以根據排程或事件觸發來自動化檔案傳輸工作流程。使用 Terraform 進行部署不需要耗時且容易出錯的手動組態，並為您提供快速、可重複且安全的部署選項來擴展。

AS2

若要顯示 AS2 Terraform 範本的支援，請將拇指向上反應 (#) 新增至 [Transfer Family Terraform 範本功能請求](#)。您也可以新增說明使用案例的註解。

B2B 資料交換

AWS B2B 資料交換 會自動在 JSON 和 XML 資料格式之間轉換、驗證和產生電子資料交換 (EDI) 文件。若要顯示 B2B Data Interchange 的 Terraform 範本支援，請將拇指向上反應 (#) 新增至[功能請求](#)。您也可以新增說明使用案例的註解。

故障診斷 AWS Transfer Family

本章提供您在使用時可能遇到的常見問題的疑難排解資訊 AWS Transfer Family。每個區段都著重於特定的功能領域，以協助您快速找到問題的解決方案。

- 如需 Transfer Family 中 IAM 的問題，請參閱 [對 AWS Transfer Family 身分和存取進行故障診斷](#)。
- 如需 Transfer Family Web 應用程式的問題，請參閱 [對 Web 應用程式進行故障診斷](#)。

主題

- [對身分驗證問題進行故障診斷](#)
- [疑難排解 SFTP 連接器問題](#)
- [疑難排解 SFTP 連線和傳輸問題](#)
- [對自訂身分提供者問題進行故障診斷](#)
- [對工作流程問題進行故障診斷](#)
- [故障診斷 EFS 問題](#)
- [對儲存和加密問題進行故障診斷](#)
- [對監控和警示問題進行故障診斷](#)
- [對跨區域傳輸問題進行故障診斷](#)
- [故障診斷 Terraform 部署問題](#)
- [針對 Web Application Firewall 整合問題進行故障診斷](#)
- [對服務受管使用者問題進行故障診斷](#)
- [疑難排解 AS2 問題](#)

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

- [身分驗證失敗 - SSH/SFTP](#)
- [Managed AD 不相符領域問題](#)
- [超過 Active Directory 群組限制](#)

- [其他身分驗證問題](#)
- [對 Amazon API Gateway 問題進行故障診斷](#)
- [對測試您的身分提供者進行故障診斷](#)
- [Web 應用程式中的重複 Amazon S3 儲存貯體](#)

身分驗證失敗 - 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，您會收到類似以下的訊息：

```
Received disconnect from 3.130.115.105 port 22:2: Too many authentication failures
Authentication failed.
```

Note

如果您使用 API Gateway 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。兩者都必須位於預設領域，或兩者都必須位於信任領域。

原因

如果使用者及其群組不相符，則 Transfer Family 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（預設或信任）的群組。

超過 Active Directory 群組限制

Description

嘗試將更多 Active Directory 群組新增至 AWS Transfer Family 伺服器時，您會收到錯誤，指出已達到允許的群組數量上限。

原因

AWS Transfer Family 預設限制為每個伺服器 100 個 Active Directory 群組。

解決方案

以下是兩種可能的解決方案：

- 合併您的 Active Directory 群組，以減少所需的總數。
- 如果您的使用案例需要超過 100 個群組，請考慮使用自訂身分提供者解決方案，如[透過自訂身分提供者簡化 Active Directory 身分驗證 AWS Transfer Family](#)中所述。

其他身分驗證問題

Description

您會收到身分驗證錯誤，而且其他故障診斷都無法運作

原因

您可能已指定邏輯目錄的目標，其中包含正斜線或結尾斜線 (/)。

解決方案

更新您的邏輯目錄目標，以確保其開頭為斜線，且不包含結尾斜線。例如，`/amzn-s3-demo-bucket/images` 是可接受的，但 `amzn-s3-demo-bucket/images` 和 `/amzn-s3-demo-bucket/images/` 是不可接受的。

對 Amazon API Gateway 問題進行故障診斷

本節說明下列 API Gateway 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。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) 無效所致。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，角色 ARN 只是預留位置，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 ARN 取代為具有伺服器存取許可的實際角色。

更新角色

1. 在 <https://console.aws.amazon.com/cloudformation> 開啟 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，然後選擇下一步。
5. 將 UserRoleArn 取代為具有足夠許可的角色 ARN，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. 選擇下一步，然後再次選擇下一步。在檢閱##頁面上，選取我確認 AWS CloudFormation 可能會建立 IAM 資源，然後選擇更新堆疊。

連線已關閉

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

請確定伺服器的記錄角色與 Transfer Family 具有信任關係。如需詳細資訊，請參閱[建立信任關係](#)。

對測試您的身分提供者進行故障診斷

Description

如果您使用 主控台或 TestIdentityProvider API 操作測試身分提供者，則 Response 欄位為空白。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

請務必為使用者使用正確的登入資料，並視需要更新使用者名稱或密碼。

Web 應用程式中的重複 Amazon S3 儲存貯體

Description

相同的 Amazon S3 儲存貯體會在 Transfer Family Web 應用程式界面中出現多次。

原因

當使用者屬於具有授予相同 Amazon S3 儲存貯體的多個 Active Directory 群組時，就會發生這種情況。Web 應用程式會列出與使用者 UID 或 GID 相關聯的所有最上層授予，包括對相同儲存貯體位置的重複授予。

解決方案

為了防止重複的清單，請合併授予，讓每個使用者在每個 Amazon S3 位置只有一個授予。檢閱您的 Amazon S3 Access Grants 組態，並移除不同 Active Directory 群組中相同儲存貯體的備援授權。

疑難排解 SFTP 連接器問題

本節說明 SFTP 連接器問題的可能解決方案。

主題

- [針對為您的 SFTP 連接器新增受信任主機金鑰進行故障診斷](#)
- [金鑰交涉失敗](#)

- [SFTP 連接器限流](#)
- [最佳化 SFTP 連接器效能](#)
- [故障診斷 VPC 連線問題](#)
- [其他 SFTP 連接器問題](#)

針對為您的 SFTP 連接器新增受信任主機金鑰進行故障診斷

Description

當您建立或編輯 SFTP 連接器，並新增信任的主機金鑰時，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

當您將金鑰貼入文字欄位時，請刪除金鑰的註解部分。例如，假設您的金鑰看起來類似以下內容：

```
ssh-rsa AAAA...== marymajor@dev-dsk-marymajor-1d-c1234567.us-east-1.amazon.com
```

移除==字元後面的文字，並只貼到 和包含 的索引鍵部分==。

```
ssh-rsa AAAA...==
```

金鑰交換失敗

Description

您收到金鑰交換交涉失敗的錯誤。例如：

```
Key exchange negotiation failed due to incompatible host key algorithms.  
Client offered: [ecdsa-sha2-nistp256, ecdsa-sha2-nistp384,  
ecdsa-sha2-nistp521, rsa-sha2-512, rsa-sha2-256] Server offered: [ssh-rsa]
```

原因

此錯誤是因為伺服器支援的主機金鑰演算法與連接器支援的主機金鑰演算法之間沒有重疊。

解決方案

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 [AWS Transfer Family SFTP 連接器的安全政策](#)。

SFTP 連接器限流

Description

使用 SFTP 連接器進行檔案傳輸時，您遇到以下錯誤：

```
{"type": "ExecutionThrottled", "details": {}, "connectorId": "c-1234567890abcdef0"}
```

或者，您注意到檔案傳輸在大量操作期間發生延遲或間歇性失敗。

原因

SFTP 連接器具有限制並行檔案傳輸和 API 操作數量的服務配額。超過這些限制時，會發生限流以保護服務並確保所有客戶的公平使用。

解決方案

若要解決 SFTP 連接器問題，請嘗試下列解決方案：

1. 在應用程式中實作指數退避和重試邏輯。例如，建立 函數來自動重試失敗的操作，並在嘗試之間增加等待時間。
2. 在應用程式中實作速率限制：
 - 限制並行傳輸的數量。
 - 在批次傳輸之間新增延遲。
3. 根據服務配額監控您的用量：
 - 使用 CloudWatch 指標來追蹤 API 用量。
 - 設定警示以在接近配額限制時通知您。
4. 如需擴展 SFTP 連接器的選項，請參閱[擴展 SFTP 連接器](#)。
5. 如果限流持續存在並影響您的業務營運，請透過 Service Quotas 主控台請求增加配額。

最佳化 SFTP 連接器效能

Description

您的 SFTP 連接器傳輸速度比預期慢，或者效能不一致。

原因

SFTP 連接器效能可能會受到各種因素的影響，包括網路條件、檔案大小、遠端伺服器組態和並行傳輸限制。

解決方案

若要最佳化 SFTP 連接器效能：

- 設定遠端 SFTP 伺服器以取得最佳效能：
 - 增加每個工作階段的工作階段和傳輸上限
 - 最佳化高延遲連線的 TCP 視窗大小
 - 如果兩端都支援，請使用壓縮
- 將 Transfer Family 連接器放置在遠端 SFTP 伺服器附近的區域，以考慮網路最佳化。
- 實作監控策略來識別效能瓶頸：
 - 監控網路輸送量和延遲
 - 分析慢速傳輸中模式的日誌

故障診斷 VPC 連線問題

本節說明啟用 VPC_LATTICE 的 SFTP 連接器常見問題的解決方案。

連接器卡在待定狀態

Description

啟用 VPC_LATTICE 的 SFTP 連接器會長時間處於 PENDING 狀態（超過 10 分鐘）。

原因

這可能是因為 DNS 解析延遲、資源閘道組態問題或 VPC Lattice 服務網路關聯問題而發生。

解決方案

聯絡 AWS 支援 [聯絡 AWS](#)。以協助分析問題的根本原因。您也可以嘗試以下解決方法。

1. 確認您的資源閘道處於 ACTIVE 狀態：

```
aws vpc-lattice get-resource-gateway --resource-gateway-  
identifier rgw-1234567890abcdef0
```

2. 檢查您的資源組態是否已正確設定並處於作用中狀態：

```
aws vpc-lattice get-resource-configuration --resource-configuration-  
identifier rcfg-1234567890abcdef0
```

3. 確保您的 Resource Gateway 在至少兩個支援 VPC Lattice 的可用區域中具有子網路。
4. 如果問題仍然存在，請刪除並重新建立具有相同組態的連接器。

連接器處於 ERRORED 狀態

Description

啟用 VPC_LATTICE 的 SFTP 連接器會顯示ERRORED狀態與錯誤詳細資訊。

原因

常見原因包括資源組態 ARN 無效、VPC 子網路中 IP 地址不足，或跨區域資源共用嘗試。

解決方案

1. 使用 檢查錯誤詳細資訊describe-connector：

```
aws transfer describe-connector --connector-id c-1234567890abcdef0
```

2. 驗證資源組態 ARN 是否正確，且位於與連接器相同的區域。
3. 確保您的 VPC 子網路有足夠的可用 IP 地址供資源閘道使用。
4. 檢查您的資源組態目標 (IP 地址或 DNS 名稱) 是否可從 VPC 連線。

不支援公有 IP 地址錯誤

Description

嘗試使用公有 IP 地址建立資源組態時，您會收到錯誤：ValidationException: IP address x.x.x.x is not in allowed ranges.

原因

公有端點的資源組態必須使用 DNS 名稱，而不是 IP 地址。

解決方案

建立資源組態時，請使用 SFTP 伺服器的公有 DNS 名稱，而非其 IP 地址：

```
aws vpc-lattice create-resource-configuration \  
  --name my-public-server-config \  
  --resource-gateway-identifier rgw-1234567890abcdef0 \  
  --resource-configuration-definition dnsResource={domainName="my.sftp.server.com"} \  
  --port-ranges 22
```

不支援可用區域錯誤

Description

您在建立資源閘道時收到錯誤：Subnet subnet-xxx is not valid because it is not in a supported Availability Zone.

原因

並非所有可用區域都支援 VPC Lattice 跨 VPC 資源存取。錯誤訊息會列出您所在區域的支援 AZs。

解決方案

1. 在錯誤訊息中列出的支援可用區域中建立子網路。
2. 更新您的 Resource Gateway 以僅使用來自支援 AZs 子網路。
3. 確保在不同支援的 AZs 中至少有兩個子網路。

使用 VPC_LATTICE 連接器的連線逾時

Description

透過 VPC 連接器的檔案傳輸會逾時或間歇性失敗。

原因

VPC Lattice 具有連線限制（每個資源 350 個連線）和閒置逾時（TCP 為 350 秒）。

解決方案

1. 監控並行連線，以保持每個資源的 350 個連線限制內。
2. 在您的應用程式中實作連線集區和重複使用。
3. 在 SFTP 用戶端應用程式中設定適當的逾時值（少於 350 秒）。
4. 請考慮為相同目標建立多個資源組態，以分配負載。

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，而且在 API 呼叫後只會傳回連接器 ID。

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 `TestConnection` API 命令測試您的連接器。
- 檢視連接器的 CloudWatch 日誌：請參閱[SFTP 連接器的範例日誌項目](#)。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。

疑難排解 SFTP 連線和傳輸問題

本節說明 SFTP 連線和檔案傳輸問題的可能解決方案。

主題

- [疑難排解 SFTP 連線問題](#)
- [疑難排解 SFTP 用戶端問題](#)
- [對檔案上傳問題進行故障診斷](#)
- [故障診斷 VPC 輸出類型 SFTP 連接器問題](#)

疑難排解 SFTP 連線問題

Description

您的 SFTP 用戶端無法啟動連線。此問題可能會持續或間歇發生。例如，您可能會在 SFTP 用戶端偵錯日誌中看到下列一系列事件：

```
sftp -vvv username@1.1.1.1
.....
debug1: Local version string .....
kex_exchange_identification: read: Connection reset by peer
Connection reset by 1.1.1.1 port 22
Connection closed.
```

原因

有一種邊緣案例，即零位元組 TCP ACK（不含資料的 ACK），也稱為三向交握，會遭到捨棄或延遲。

解決方案

作為解決方法，Transfer Family 提供了使用不同組態來解決此問題的解決方案，但可能會導致與較舊用戶端的相容性問題。因此，此解決方案僅適用於連接埠 2223。

在 VPC ([在虛擬私有雲端中建立伺服器](#)) 中建立 Transfer Family 伺服器的程序中，當您指定安全群組時，請將 SSH 流量設定為使用連接埠 2223。

疑難排解 SFTP 用戶端問題

SFTP 用戶端訊息如中所述[SFTP 訊息](#)。疑難排解 SFTP 用戶端問題的最佳方法是檢查 SFTP 用戶端日誌，並視需要聯絡您的網路管理員。

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，您會收到下列錯誤訊息：AWS Transfer 不支援隨機存取寫入 S3 物件。

原因

當您使用 Amazon S3 做為伺服器的儲存體時，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 做為儲存體，請停用用戶端軟體提及使用多個連線進行單一傳輸的任何選項。

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 FTP 和 SFTP 傳輸問題，這些傳輸會在檔案名稱中包含某些字元，例如跛行符號、重音字母或某些指令碼，例如中文或阿拉伯文。

原因

雖然 FTP 和 SFTP 通訊協定可以允許用戶端交涉檔案名稱的字元編碼，但 Amazon S3 和 Amazon EFS 不允許。反之，它們需要 UTF-8 字元編碼。因此，某些字元無法正確轉譯。

解決方案

若要解決此問題，請檢閱您的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。

故障診斷 VPC 輸出類型 SFTP 連接器問題

如果您遇到 VPC 輸出類型 SFTP 連接器的問題，請檢查下列項目：

連接器狀態為待定

Description

您的 VPC 輸出類型連接器在建立後會保持待定狀態幾分鐘，且 TestConnection 會傳回「Connector not available」。

原因

建立後，VPC 連接器的 DNS 解析可能需要幾分鐘才能完成。

解決方案

等待連接器狀態變為 ACTIVE，然後再嘗試檔案傳輸。這是 VPC 輸出類型連接器的正常行為。

連線逾時。

Description

嘗試連線至 SFTP 伺服器時，您的 VPC 輸出類型連接器逾時。

原因

安全群組可能不允許資源閘道子網路和目標 SFTP 伺服器之間連接埠 22 上的流量。

解決方案

確認安全群組允許資源閘道子網路與目標 SFTP 伺服器之間的連接埠 22 上的流量。

資源組態錯誤

Description

由於資源組態問題，您的 VPC 輸出類型連接器無法連線。

原因

資源組態可能指向不正確的 IP 地址或 DNS 名稱，或者資源閘道可能與您的 SFTP 伺服器不在相同的 VPC 中（適用於私有端點）。

解決方案

確保您的資源組態指向正確的 IP 地址或 DNS 名稱，且資源閘道與您的 SFTP 伺服器位於相同的 VPC 中（適用於私有端點）。如需詳細資訊，請參閱《Amazon VPC Lattice 使用者指南》中的[資源組態](#)。

公有端點問題

Description

您的 VPC 輸出類型連接器無法連線至公有 SFTP 端點。

原因

對於公有端點，您必須在資源組態中使用 DNS 名稱（而非 IP 地址），而且 VPC 必須具有 NAT 閘道才能進行傳出網際網路存取。

解決方案

請確定您在資源組態中使用 DNS 名稱，而不是 IP 地址。確認您的 VPC 具有用於傳出網際網路存取的 NAT 閘道。

可用區域問題

Description

由於可用區域限制，您無法建立資源閘道。

原因

資源閘道需要至少 2 個可用區域中的子網路，但並非所有 AZs 都支援 VPC Lattice。

解決方案

檢查您區域中 VPC Lattice 支援的可用區域，並確保您在至少 2 個支援的 AZs 中有子網路。

對自訂身分提供者問題進行故障診斷

本節說明與 Transfer Family 的自訂身分提供者相關問題的可能解決方案。

主題

- [故障診斷 API Gateway 整合錯誤](#)
- [故障診斷 Lambda 函數逾時](#)
- [對一致的 Lambda 逾時問題進行故障診斷](#)
- [故障診斷例外KeyError狀況](#)

故障診斷 API Gateway 整合錯誤

Description

使用者無法透過 Transfer Family 伺服器進行身分驗證，在測試您的身分提供者時，您會看到錯誤，例如：

```
{
  "Response": "",
  "StatusCode": 500,
  "Message": "Internal server error"
}
```

原因

API Gateway 整合錯誤可能的原因如下：

- API Gateway 組態不正確
- 未正確處理 Lambda 函數錯誤
- API Gateway 和 Lambda 之間的許可問題
- 來自 Lambda 函數的格式不正確的回應

解決方案

若要疑難排解 API Gateway 整合錯誤：

1. 如需詳細的錯誤資訊，請檢查您的 Lambda 函數日誌：

- 在 CloudWatch 主控台中，導覽至日誌群組 > /aws/lambda/your-function-name
- 尋找指出根本原因的錯誤訊息或堆疊追蹤

2. 確認您的 Lambda 函數傳回格式正確的回應：

```
{
  "Role": "arn:aws:iam::123456789012:role/TransferUserRole",
  "HomeDirectory": "/mybucket/home/username"
}
```

3. 啟用 API Gateway 的詳細 CloudWatch 記錄：

- 在 API Gateway 主控台中，選取您的 API，然後選擇階段
- 選取您的階段並在日誌/追蹤下，啟用 CloudWatch Logs
- 將日誌層級設定為 ERROR 或 INFO

4. 直接測試您的 API Gateway 端點：

```
curl -X POST https://your-api-id.execute-api.region.amazonaws.com/prod/servers/your-server-id/users/username/config \
  -H "Content-Type: application/json" \
  -d '{"Password": "password"}
```

5. 驗證 API Gateway 和 Lambda 之間的許可：

- 確保 API Gateway 具有叫用 Lambda 函數的許可
- 檢查 Lambda 函數的執行角色是否具有必要的許可

故障診斷 Lambda 函數逾時

Description

當使用者嘗試使用自訂身分提供者與您的 Transfer Family 伺服器進行身分驗證時，他們會經歷長時間延遲，然後發生身分驗證失敗。在 Lambda 日誌中，您會看到逾時錯誤。

原因

用於自訂身分提供者的 Lambda 函數預設逾時為 3 秒。如果您的身分驗證邏輯需要比此逾時更長的時間（例如，在查詢外部資料庫或對第三方身分提供者進行 API 呼叫時），函數將會逾時，且身分驗證將會失敗。

解決方案

若要解決 Lambda 逾時問題：

1. 增加 Lambda 函數逾時：
 - 在 Lambda 主控台中，導覽至您的函數，然後選取組態索引標籤
 - 在一般組態下，按一下編輯
 - 增加逾時值（驗證函數建議最多 15 秒）
2. 最佳化您的 Lambda 函數程式碼：
 - 使用資料庫查詢的連線集區
 - 實作經常存取資料的快取
 - 最小化身分驗證期間的外部 API 呼叫
3. 考慮使用 Lambda 佈建並行來消除冷啟動：

```
aws lambda put-provisioned-concurrency-config \  
  --function-name my-authentication-function \  
  --qualifier prod \  
  --provisioned-concurrent-executions 5
```

4. 使用 CloudWatch 指標監控 Lambda 效能，並設定持續時間閾值的警示

對一致的 Lambda 逾時問題進行故障診斷

Description

使用 Lambda 函數進行身分驗證時，使用者會遇到一致的逾時。

原因

Lambda 無法連線到用於驗證的對應 AWS 服務（例如 DynamoDB、Secrets Manager 或其他身分提供者）。

解決方案

確認子網路可以連接 AWS 服務。或者，如果連線到網際網路身分提供者（例如 Okta），請確認 Lambda 函數的子網路可以透過 NAT Gateway 連線到網際網路。

故障診斷例外 **KeyError** 狀況

Description

在 Transfer Family 日誌項目中，您會注意到「KeyError」例外狀況。

原因

最可能的原因是使用者或 `identity_provider` 記錄格式不正確或缺少必要欄位。

解決方案

檢閱位於 ERRORS 日誌群組中的 `/aws/transfer/your-server-id` 日誌以取得線索。

對工作流程問題進行故障診斷

本節說明受管工作流程問題的可能解決方案。

主題

- [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 CloudWatch 對工作流程相關錯誤進行故障診斷](#)
- [對工作流程複製錯誤進行故障診斷](#)

使用 Amazon CloudWatch 對工作流程相關錯誤進行故障診斷

Description

如果您的工作流程發生問題，您可以使用 Amazon CloudWatch 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 系列會向 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 Logs 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)。<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。此錯誤會通知您發生錯誤的步驟，並提供錯誤訊息。在此特定範例中，步驟設定為標記檔案；不過，不支援在 Amazon EFS 檔案系統中標記檔案，因此步驟會產生錯誤。

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，而且如果該步驟無法執行，則整體工作流程會失敗。

執行調節

如果工作流程以比系統可支援的更快的速度觸發，則會調節執行。此日誌訊息指出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速率，請聯絡 AWS 支援 聯絡。 [AWS](#)

啟動工作流程時的服務失敗

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，您必須等待大約 10 分鐘，才能執行新的工作流程。Transfer Family 伺服器會快取工作流程詳細資訊，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的 SFTP 工作階段，然後在 10 分鐘的等待期間之後重新登入，以查看變更。

對工作流程複製錯誤進行故障診斷

Description

如果您執行的工作流程包含複製上傳檔案的步驟，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

本節說明下列加密工作流程問題的可能解決方案。

主題

- [對匿名收件人加密問題進行故障診斷](#)
- [已簽章加密檔案的故障診斷錯誤](#)
- [FIPS 演算法的故障診斷錯誤](#)

對匿名收件人加密問題進行故障診斷

Description

您的解密工作流程在處理特定加密檔案時失敗，但適用於其他檔案。

原因

檔案可能已加密，但未指定收件人（匿名加密），讓工作流程難以判斷要用於解密的金鑰。

解決方案

一律使用 `-r` 參數加密具有非匿名收件人的檔案。例如：

```
gpg -e -r user@example.com --openpgp file.txt
```

若要檢查檔案是否以特定收件人或匿名方式加密，請使用 `--list-packets` 命令：

```
gpg --list-packets file.txt.gpg
```

此命令會顯示 GPG 加密檔案的封包結構，而不解密其內容。尋找包含收件人資訊的輸出，例如：

```
:pubkey enc packet: version 3, algo 1, keyid 1A2B3C4D5E6F7G8H
```

如果您看到 keyid 資訊，檔案會針對特定收件人加密。如果缺少此資訊，檔案可能已匿名加密，這可能會導致 Transfer Family 工作流程中的解密失敗。

您也可以使用此命令來驗證：

- 使用哪些加密演算法
- 壓縮方法（如果有的話）
- 建立時間戳記

若要檢視 GPG 安裝支援的加密演算法清單，請使用：

```
gpg --version
```

此資訊可協助您確保使用的加密演算法與 Transfer Family 工作流程相容，尤其是需要 FIPS 合規時。

已簽章加密檔案的故障診斷錯誤

Description

您的解密工作流程失敗，您會收到下列錯誤：

```
"Encrypted file with signed message unsupported"
```

原因

Transfer Family 目前不支援簽署加密的檔案。

解決方案

在 PGP 用戶端中，如果有簽署加密檔案的選項，請務必清除選取項目，因為 Transfer Family 目前不支援簽署加密檔案。

FIPS 演算法的故障診斷錯誤

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 區塊加密模式）來加密檔案：這會導致工作流程失敗。

解決方案

您必須編輯用來加密檔案的 GPG 金鑰，然後重新加密它們。下列程序說明您必須採取的步驟。

編輯 PGP 金鑰

1. 識別執行時必須編輯的金鑰 `gpg --list-keys`

這會傳回金鑰清單。每個金鑰的詳細資訊如下：

```

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. 出現 gpg> 提示時，輸入 showpref。會傳回下列詳細資訊：

```
[ultimate] (1). Mary Major <marymajor@example.com>
  Cipher: AES256, AES192, AES, 3DES
  AEAD: OCB
  Digest: SHA512, SHA384, SHA256, SHA224, SHA1
  Compression: ZLIB, BZIP2, ZIP, Uncompressed
  Features: MDC, AEAD, Keyserver no-modify
```

請注意，會列出儲存在金鑰上的偏好演算法。

5. 我們希望編輯金鑰以保留 OCB 以外的所有演算法。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，然後在出現確認變更的提示時輸入您的密碼。
7. 儲存變更。

```
gpg> save
```

重新執行解密工作流程之前，您必須使用編輯的金鑰重新加密檔案。

故障診斷 EFS 問題

本節說明 Amazon EFS 儲存相關問題的可能解決方案。

主題

- [對 Amazon EFS 問題進行故障診斷](#)

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

- [Amazon EFS 服務受管使用者疑難排解](#)
- [故障診斷遺失的 POSIX 設定檔](#)
- [使用 Amazon EFS 對邏輯目錄進行故障診斷](#)

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 AWS 受管政策，例如 `AmazonElasticFileSystemClientFullAccess`。

故障診斷遺失的 POSIX 設定檔

Description

如果您為伺服器使用 Amazon EFS 儲存體，而且您使用自訂身分提供者，則必須提供 AWS Lambda 函數 POSIX 設定檔。

原因

其中一個可能的原因是，我們用來建立 AWS Lambda 後端 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

請務必為 PosixProfile 參數提供 Transfer Family 的 JSON 元素。

例如，如果您使用的是 Python，您可以在剖析 PosixProfile 參數的位置新增以下行：

```
if PosixProfile:
    response_data["PosixProfile"] = json.loads(PosixProfile)
```

或者，在 JavaScript 中，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 0 或更高：

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

這些程式碼範例會將 PosixProfile 參數以 JSON 物件的形式傳送至 Transfer Family，而不是以字串的形式傳送。

此外，在 AWS Secrets Manager 中，您必須存放 PosixProfile 參數，如下所示。將 *your-uid* 和 *your-gid* 為您 GID 和 UID 的實際值。

```
{"Uid": your-uid, "Gid": your-gid, "SecondaryGids": []}
```

使用 Amazon EFS 對邏輯目錄進行故障診斷

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，如下所示：

```
sftp> ls
remote readdir ("/"): No such file or directory
```


原因

如果您的 Transfer Family 伺服器使用 Amazon EFS，則必須使用讀取和寫入存取權建立使用者的主目錄，使用者才能在其邏輯主目錄中工作。使用者無法自行建立此目錄，因為他們在其邏輯主目錄 `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。

對儲存和加密問題進行故障診斷

本節說明儲存和加密問題的可能解決方案。

主題

- [對加密 Amazon S3 儲存貯體的政策進行故障診斷](#)
- [對 `ResourceNotFound` 例外狀況進行故障診斷](#)

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至伺服器，您會收到錯誤 `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

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，才能授予必要的 AWS Key Management Service (AWS KMS) 許可。如需詳細資訊，請參閱[資料保護和加密](#)。

對ResourceNotFoundException例外狀況進行故障診斷

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的資源，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，您會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

將區域參數新增至您的 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
```

對監控和警示問題進行故障診斷

本節提供有關對 的監控和警示問題進行故障診斷的資訊 AWS Transfer Family，包括遺失或不完整的 CloudWatch 指標和遺失的 EventBridge 事件。

主題

- [對遺失或不完整的 CloudWatch 指標進行故障診斷](#)
- [故障診斷遺失的 EventBridge 事件](#)

對遺失或不完整的 CloudWatch 指標進行故障診斷

Description

Transfer Family 伺服器的 CloudWatch 指標遺失、不完整或未如預期更新。

原因

遺漏或不完整的指標可能由幾個因素造成：

- 記錄組態問題
- 未在預期時間範圍內產生指標的低活動層級
- 檢視維度或時間範圍不正確的指標

解決方案

若要解決 CloudWatch 指標遺失或不完整的問題：

1. 確定已為您的 Transfer Familyserver 正確設定記錄：
 - 在 Transfer Family 主控台中，檢查是否已在伺服器詳細資訊 > 其他詳細資訊 > 記錄角色下啟用記錄。
 - 記錄角色非常具有必要的許可和信任關係。
2. 在 CloudWatch 主控台中檢視指標時：
 - 使用正確的維度，例如伺服器層級指標的 ServerId
 - 調整時間範圍以確保涵蓋活動期間
 - 檢查您是否位於正確的 AWS 區域
3. 在 Transfer Family 伺服器上產生測試活動，以確保產生指標。

故障診斷遺失的 EventBridge 事件

Description

您已設定 Amazon EventBridge 規則來擷取 Transfer Family 事件，但事件未交付至目標目的地或觸發預期的動作。

原因

遺失 EventBridge 事件的原因可能是：

- 設定不正確的事件模式
- 事件目標的許可問題
- 服務限制或限流

- 事件因伺服器組態而未產生

解決方案

若要對遺失的 EventBridge 事件進行故障診斷：

1. 確認您的事件模式格式正確，以符合 Transfer Family 事件：

```
{
  "source": ["aws.transfer"],
  "detail-type": ["Transfer State Change"],
  "detail": {
    "serverId": ["s-1234567890abcdef0"]
  }
}
```

2. 檢查您的事件目標是否具有必要的許可：

- 對於 Lambda 目標，確保 Lambda 函數的資源政策允許 EventBridge 調用它
- 對於 SQS 目標，確認佇列政策允許 EventBridge 傳送訊息
- 對於 SNS 目標，確認主題政策允許 EventBridge 發佈至該目標

3. 透過產生範例事件來測試您的規則：

- 使用 EventBridge 主控台建立符合您模式的測試事件
- 在應產生事件的 Transfer Family 伺服器上執行動作

4. 啟用 EventBridge 規則指標來監控規則叫用和失敗：

```
aws events put-rule --name "TransferStateChangeRule" --event-pattern '{...}' --state
ENABLED --metrics-enabled
```

5. 檢查 CloudWatch Logs 是否有任何與事件交付失敗相關的錯誤訊息

對跨區域傳輸問題進行故障診斷

本節說明在 之間傳輸檔案相關問題的可能解決方案 AWS 區域。

主題

- [對跨區域傳輸許可問題進行故障診斷](#)
- [對跨區域傳輸效能問題進行故障診斷](#)

對跨區域傳輸許可問題進行故障診斷

Description

嘗試使用 Transfer Family 工作流程在不同區域中的 Amazon S3 儲存貯體之間傳輸檔案時，您遇到以下錯誤：

```
{
  "type": "StepErrored",
  "details": {
    "errorType": "BAD_REQUEST",
    "errorMessage": "Access Denied (Service: Amazon S3; Status Code: 403; Error Code: AccessDenied)",
    "stepType": "COPY",
    "stepName": "cross_region_copy"
  }
}
```

原因

跨區域傳輸需要來源和目的地儲存貯體的特定 IAM 許可。Transfer Family 伺服器或工作流程使用的 IAM 角色可能沒有足夠的許可來存取其他區域中的儲存貯體。

解決方案

若要解決跨區域轉移許可問題：

1. 確保您的 IAM 角色具有來源和目的地儲存貯體的許可：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": "arn:aws:s3:::source-bucket-name/*"
    },
    {
      "Effect": "Allow",
```

```

    "Action": [
      "s3:PutObject",
      "s3:PutObjectAcl"
    ],
    "Resource": "arn:aws:s3:::destination-bucket-name/*"
  }
]
}

```

2. 如果使用 KMS 加密，請同時新增來源和目的地 KMS 金鑰的許可：

```

{
  "Effect": "Allow",
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
  "Resource": [
    "arn:aws:kms:source-region:account-id:key/source-key-id",
    "arn:aws:kms:destination-region:account-id:key/destination-key-id"
  ]
}

```

3. 確認兩個區域中的儲存貯體政策都允許從 Transfer Family 伺服器的 IAM 角色存取

4. 對於跨帳戶轉移，請確保已設定適當的跨帳戶許可

對跨區域傳輸效能問題進行故障診斷

Description

跨區域傳輸明顯比預期慢，或在大型檔案傳輸期間逾時。

原因

跨區域傳輸本質上涉及更高的延遲，並可能受到網路條件、檔案大小和服務限制的影響。大型檔案或大量小型檔案可能會效能降低。

解決方案

若要改善跨區域傳輸效能：

- 對於大型檔案，請考慮使用 Amazon S3 Transfer Acceleration：

```
aws s3 cp --source-region us-east-1 --region us-west-2 \  
s3://source-bucket/large-file.zip s3://destination-bucket/large-file.zip \  
--acl bucket-owner-full-control --s3-accelerate
```

- 對於多個小型檔案，請在傳輸之前將它們批次在一起：
 - 使用壓縮來合併多個檔案
 - 使用 Amazon S3 批次操作進行大規模傳輸
- 考慮使用 Transfer Family SFTP 連接器搭配適用於大型傳輸的適當逾時設定
- 對於經常性傳輸，請考慮使用 Amazon S3 跨區域複寫 (CRR) 複寫資料，而不是隨機操作傳輸
- 使用 Amazon CloudWatch 指標監控傳輸效能，以識別瓶頸

故障診斷 Terraform 部署問題

本節說明使用 Terraform 部署 Transfer Family 資源相關問題的可能解決方案。如需 Transfer Family 的 Terraform 模組一般資訊，請參閱 [Transfer 系列 Terraform 模組](#)。

主題

- [故障診斷 Terraform 資源建立失敗](#)
- [故障診斷 Terraform 狀態管理問題](#)

故障診斷 Terraform 資源建立失敗

Description

嘗試使用 Terraform 建立 Transfer Family 資源時，您遇到以下錯誤：

```
Error: error creating Transfer Server: InvalidRequestException: The request is not  
valid.  
Error: error creating Transfer User: InvalidRequestException: Unable to create the user  
because the server endpoint type is incompatible with the home directory type.
```

原因

這些錯誤通常是由於不相容的組態參數或 Terraform 組態中缺少相依性所造成。常見原因包括：

- 不相容的端點類型和儲存組態

- 缺少必要的 IAM 角色或政策
- 不正確的安全政策規格
- VPC 端點組態問題

解決方案

若要解決 Terraform 部署問題：

- 確保您的 Terraform 組態使用相容的參數組合：
 - 對於公有端點，請確定您使用 Amazon S3 進行儲存。
 - 對於 VPC 端點，驗證適當的 VPC 和安全群組組態。
- 搭配 `depends_on` 屬性使用明確相依性，以確保以正確的順序建立資源。
- 確認所有 IAM 角色都具有必要的信任關係和許可。
- 使用最新版本的 Terraform AWS 供應商，以確保與所有 Transfer Family 功能的相容性。
- 對於複雜的部署和簡單的使用案例，請考慮使用 GitHub 上提供的官方 Transfer Family Terraform 模組，網址為 <https://github.com/aws-ia/terraform-aws-transfer-family>。這些模組提供廣泛的範例，涵蓋簡單且複雜的客戶使用案例、遵循 AWS 最佳實務，並可為需要基礎設施即程式碼 (IaC) 組態協助的客戶簡化部署。

故障診斷 Terraform 狀態管理問題

Description

在 Terraform 之外變更 Transfer Family 資源（透過主控台或 AWS CLI）之後，您會在執行 `terraform plan` 或 `terraform apply` 時遇到狀態偏離。

原因

Terraform 會維護狀態檔案，以追蹤其管理的資源。在 Terraform 之外進行變更時，狀態檔案會與實際資源不同步，導致後續 Terraform 操作期間發生錯誤或意外行為。

解決方案

若要解決 Transfer Family 資源的 Terraform 狀態管理問題：

1. 使用 `terraform import` 在 Terraform 管理下引入現有資源：

```
terraform import <transfer_family_server.example> s-<server-id>
```



```
terraform import <transfer_family_server.example> s-<server-id>/username
```

2. 使用 `terraform refresh` 更新具有目前真實世界基礎設施的狀態檔案
3. 對於無法匯入或存在複雜狀態問題的資源，請考慮使用 `terraform state rm` 中移除它們，然後使用 Terraform 重新建立它們
4. 實作政策，僅透過 Terraform 管理 Transfer Family 資源，以防止未來狀態偏離
5. 使用遠端狀態儲存搭配鎖定功能，以防止在團隊中工作時同時進行修改

針對 Web Application Firewall 整合問題進行故障診斷

本節說明 AWS WAF 與 Transfer Family 整合相關問題的可能解決方案。

主題

- [對封鎖合法流量的 WAF 進行故障診斷](#)
- [對與自訂身分提供者的 WAF 整合進行故障診斷](#)

對封鎖合法流量的 WAF 進行故障診斷

Description

AWS WAF 使用 Transfer Family 端點設定 後，合法使用者無法連線或遇到間歇性連線失敗。您可能會在日誌中看到 HTTP 403（禁止）回應。

原因

您的 AWS WAF 規則可能過於嚴格或設定不正確，導致誤判封鎖合法流量。常見原因包括：

- 不小心封鎖公司網路或 VPNs IP 型規則
- 對於正常流量模式而言，閾值太低的速率型規則
- 對您的使用案例過於積極的受管規則群組

解決方案

若要解決誤判問題：

1. 啟用 AWS WAF 記錄以識別觸發區塊的規則。如需說明，請參閱[記錄 AWS WAF Web ACL 流量](#)。
2. 檢閱您的日誌以識別封鎖請求中的模式。

3. 透過下列方式調整您的規則：

- 將 IP 地址或範圍新增至允許清單
- 提高以速率為基礎的規則的速率限制
- 將特定規則設定為計數模式，而不是將封鎖模式設定為無需封鎖即可監控
- 使用規則群組排除為特定規則建立例外狀況

4. 在完全部署之前，使用合法流量的代表性範例測試更新的組態。

對與自訂身分提供者的 WAF 整合進行故障診斷

Description

AWS WAF 使用使用自訂身分提供者的 Transfer Family 伺服器設定 之後，身分驗證會失敗，或使用者遇到間歇性身分驗證問題。

原因

搭配 API Gateway 使用自訂身分提供者時，AWS WAF 規則可能會干擾 Transfer Family 與您的身分提供者之間的 API 呼叫。可能會發生這種情況，因為 AWS WAF 正在根據其規則集檢查並可能封鎖 API 流量。

解決方案

若要解決 AWS WAF 和自訂身分提供者的問題：

- 請確定您的 AWS WAF 組態包含自訂身分提供者使用的 API Gateway 端點例外狀況。
- 將 Transfer Family 服務主體 (transfer.amazonaws.com) 新增至 AWS WAF 規則中的允許清單。
- 如果使用受管規則群組，請檢閱它們是否有可能影響 API 身分驗證流程的規則，並考慮停用這些特定規則。
- 直接使用 TestIdentityProvider API 操作測試您的身分提供者，以驗證其是否正常運作，而不會 AWS WAF 造成干擾。

對服務受管使用者問題進行故障診斷

本節說明服務受管使用者問題的可能解決方案。

主題

- [對服務受管使用者進行故障診斷](#)

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

- [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](#)

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金鑰內文的 PGP 金鑰，且 AWS Transfer Family 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 在此處提供轉換工具：<https://manpages.ubuntu.com/manpages/jammy/en/man1/openpgp2ssh.1.html>

新增 SSH 公有金鑰故障診斷失敗

Description

當您嘗試為服務受管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-formatted 的公有金鑰，AWS Transfer Family 且不支援服務受管使用者的 SSH2-formatted 公有金鑰。

解決方案

您需要將金鑰轉換為 OpenSSH 格式。此程序說明於 [將 SSH2 金鑰轉換為 SSH 公有金鑰格式](#)。

疑難排解 AS2 問題

本節說明 AS2 傳輸問題的可能解決方案。

主題

- [疑難排解 AS2 問題](#)
- [AS2 憑證問題](#)
- [AS2 MDN 接收問題](#)
- [憑證過期監控問題](#)

疑難排解 AS2 問題

[AS2 錯誤代碼](#)、啟用適用性聲明 2 (AS2) 之伺服器的訊息和疑難排解秘訣，請參閱本指南的 AS2 失敗代碼一節。

AS2 憑證問題

Description

您在 AS2 傳輸時遇到憑證相關錯誤。

原因

常見原因包括憑證過期、憑證格式不正確或憑證鏈不相符。

解決方案

嘗試下列解決方案：

- 確認您的憑證未過期
- 確保憑證的格式正確 (PEM for AWS Transfer Family)
- 檢查憑證鏈是否完整且有效
- 確認簽署和加密憑證在交易合作夥伴之間相符
- 在過期之前充分輪換憑證，以避免中斷

AS2 MDN 接收問題

Description

您未收到 AS2 傳輸的預期訊息處置通知 (MDNs)。

原因

由於網路連線問題、不正確的端點組態或 MDN 格式不相符，可能會發生 MDN 問題。

解決方案

請考慮以下解決方案：

- 確認 MDN URL 已正確設定且可存取
- 檢查 AS2 伺服器與 MDN 端點之間的網路連線
- 確定兩個交易合作夥伴都設定為相同的 MDN 類型（同步或非同步）
- 檢閱 AS2 日誌是否有任何與 MDN 處理相關的錯誤
- 如果使用同步 MDNs，請確認已正確設定逾時

憑證過期監控問題

本節提供與憑證過期監控和 DaysUntilExpiry 指標相關的常見問題的解決方案。

DaysUntilExpiry 指標未顯示

問題：匯入憑證後，在 Amazon CloudWatch 中看不到 DaysUntilExpiry 指標。

解決方案：

- 匯入憑證後，請等待最多 24 小時。Transfer Family 最多可能需要一整天的時間，才能將指標傳送到您的帳戶。
- 請確定您在 CloudWatch 的 AWS/Transfer 命名空間下尋找的是正確的 AWS 區域。

憑證過期警示未觸發

問題：憑證過期的 CloudWatch 警示未如預期觸發。

解決方案：

- 確認警示已設定 Maximum 統計資料和 1 天的期間。
- 檢查閾值比較是否設定為 Less than or equal to 所需的天數。
- 確定 Treat missing data as good (not breaching) 已在警示組態中選取。
- 確認警示維度符合您憑證的 CertificateId 和描述（如果提供）。
- 檢查警示動作 (SNS 主題、電子郵件通知) 是否已正確設定並處於作用中狀態。

AWS Transfer Family API 參考

Transfer Family 的完整 API 參考指南可在 [AWS Transfer Family API 參考](#) 中取得。

AWS Transfer Family 是一種安全傳輸服務，可讓您透過下列通訊協定，將檔案傳入和傳出 Amazon Simple Storage Service (Amazon S3) 儲存體：

- 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)

伺服器、使用者和角色都由其 Amazon Resource Name (ARN) 識別。您可以將索引鍵/值對的標籤指派給具有 ARN 的實體。標籤是中繼資料，可用於分組或搜尋這些實體。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採用格式 `arn:aws:transfer:region:account-id:server/server-id`。

伺服器 ARN 的範例為 `arn:aws:transfer:us-east-1:123456789012:server/s-01234567890abcdef`。

- 針對使用者，ARN 採用 `arn:aws:transfer:region:account-id:user/server-id/username` 的形式。

例如，`arn:aws:transfer:us-east-1:123456789012:user/s-01234567890abcdef/user1`。

使用中的 DNS 項目（端點）如下所示：

- API 端點採用 `transfer.region.amazonaws.com` 的形式。

- 伺服器端點採用 `server-id.server.transfer.region.amazonaws.com` 的形式。

此 API 界面參考 AWS Transfer Family 包含您可以用來管理的程式設計界面的文件 AWS Transfer Family。參考結構如下：

- 如需 API 動作的字母清單，請參閱 [Actions](#)。
- 如需資料類型的字母清單，請參閱 [Types](#)。
- 如需常用查詢參數的清單，請參閱 [常用參數](#)。
- 如需錯誤碼的說明，請參閱 [常見錯誤](#)。

Tip

您可以搭配任何 API 呼叫使用 `--generate-cli-skeleton` 參數來產生和顯示參數範本，而不是實際執行命令。然後，您可以使用產生的範本來自訂和使用 做為稍後命令的輸入。如需詳細資訊，請參閱 [產生和使用參數骨架檔案](#)。

提出 API 請求

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、身分驗證的請求簽署和錯誤處理。如需 Transfer Family 可用區域和端點的相關資訊，請參閱《》中的 [AWS Transfer Family 端點和配額](#)。AWS 一般參考

Note

使用 Transfer Family 開發應用程式時，您也可以使用 AWS SDKs。適用於 Java、.NET 和 PHP AWS SDKs 包裝基礎 Transfer 系列 API，簡化您的程式設計任務。如需下載 SDK 程式庫的資訊，請參閱 [範例程式碼程式庫](#)。

Transfer Family 必要請求標頭

本節說明您必須隨每個 POST 請求傳送至 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](#) 操作中使用的標頭。


```
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}
```

以下是必須包含在 Transfer Family 的 POST 請求中的標頭。以下以 "x-amz" 開頭的標頭是特定的 AWS。所有其他列出的標頭都是 HTTP 交易中使用的常見標頭。

Transfer Family 請求輸入和簽署

所有請求輸入都必須作為請求內文中 JSON 承載的一部分傳送。對於所有請求欄位都是選用的動作，例如 `ListServers`，您仍然需要在請求內文中提供空的 JSON 物件，例如 `{}`。Transfer Family 承載請求/回應的結構記錄在現有的 API 參考中，例如 [DescribeServer](#)。

Transfer Family 支援使用 AWS Signature 第 4 版進行身分驗證。如需詳細資訊，請參閱[簽署 AWS API 請求](#)。

錯誤回應

當發生錯誤時，回應標頭資訊會包含：

- Content-Type: 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

有些例外狀況使用 `message`，其他例外狀況則使用 `Message`。您可以檢查介面的程式碼，以判斷適當的案例。或者，您可以測試每個選項以查看哪些有效。

類型：字串

Resource

叫用錯誤的資源。例如，如果您嘗試建立已存在的使用者，`Resource`即為現有使用者的使用者名稱。

類型：字串

ResourceType

叫用錯誤的資源類型。例如，如果您嘗試建立已存在的使用者，則 `ResourceType`為 `User`。

類型：字串

RetryAfterSeconds

重試命令之前要等待的秒數。

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 內文。

```
{
  "__type": "ResourceNotFoundException",
  "Message": "Unknown server",
  "Resource": "s-11112222333344444",
  "ResourceType": "Server"
}
```

如果執行 API 導致限流發生，則會傳回下列 JSON 內文。

```
{
  "__type": "ThrottlingException",
  "RetryAfterSeconds": "1"
}
```

如果您使用 `CreateServer` API，而且您沒有足夠的許可來建立 Transfer Family 伺服器，則會傳回下列 JSON 內文。

```
{
  "__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 內文。

```
{
  "__type": "ResourceExistsException",
  "Message": "User already exists",
  "Resource": "Alejandro-Rosalez",
  "ResourceType": "User"
}
```

可用程式庫

AWS 為偏好使用特定語言 APIs 而非命令列工具和查詢 API 建置應用程式的軟體開發人員提供程式庫、範例程式碼、教學課程和其他資源。這些程式庫提供基本函數（不包含在 APIs 中），例如請求身分驗證、請求重試和錯誤處理，以便更輕鬆地開始使用。請參閱[要建置的工具 AWS](#)

如需所有語言的程式庫和範本程式碼，請參閱[範本程式碼和程式庫](#)。

身分提供者

AWS Transfer Family 支援多種身分提供者類型來驗證和管理使用者。每個伺服器只能使用一種身分驗證方法，該方法必須在建立伺服器時選取。

服務受管

使用 `SERVICE_MANAGED` 身分驗證方法時，使用者登入資料會存放在其中並進行管理 AWS Transfer Family。使用者會使用與伺服器上使用者名稱相關聯的 SSH 公有金鑰進行身分驗證。

每個使用者可以在服務中存放一或多個 SSH 公有金鑰。當用戶端請求檔案操作時，它會提供使用者名稱和 SSH 私有金鑰，這會根據儲存的公有金鑰進行驗證。

Directory Service

`AWS_DIRECTORY_SERVICE` 身分驗證方法可讓您與 AWS Directory Service for Microsoft Active Directory (AWS Directory Service for Microsoft Active Directory) 整合。

此選項可讓您透過現有的 Active Directory 群組管理使用者身分驗證和存取。使用者可以使用其 Active Directory 登入資料進行身分驗證。

預設限制為每部伺服器 100 個 Active Directory 群組，透過增加服務限制，最多可增加至 150 個群組。

Lambda

`AWS_LAMBDA` 身分驗證方法可讓您使用連線至自訂身分提供者 AWS Lambda。

此選項提供與現有的身分管理系統整合的彈性。Lambda 函數負責驗證使用者並傳回適當的存取政策。

自訂 (API Gateway)

`API_GATEWAY` 身分驗證方法（在主控台中顯示為自訂）可讓您使用同時提供使用者身分驗證和存取控制的自訂身分驗證方法。

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。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。

對於所有身分驗證方法，會指派政策給使用者，以定義他們對 Amazon S3 儲存貯體或 Amazon Elastic File System 檔案系統的存取。伺服器會透過 IAM 角色與 `AssumeRole` 動作繼承使用者的信任關係，允許其代表使用者執行檔案操作。

命名慣例

AWS Transfer Family 針對資源識別符和 Amazon Resource Name (ARNs) 使用標準化格式。使用 API 時，AWS Transfer Family 了解這些慣例非常重要。

ID 格式

下列慣例是以 AWS Transfer Family ID 格式觀察到的：

伺服器 IDs

ServerId 值採用 s-01234567890abcdef 的形式。

SSH 公IDs

SshPublicKeyId 值採用 key-01234567890abcdef 的形式。

連接器 IDs

ConnectorId 值採用 c-01234567890abcdef 的形式。

工作流程 IDs

WorkflowId 值採用 w-01234567890abcdef 的形式。

設定檔 IDs

ProfileId 值採用 p-01234567890abcdef 的形式。

WebApp IDs

WebAppId 值採用 webapp-01234567890abcdef 的形式。

ARN 格式

Amazon Resource Name (ARN) 格式採用下列格式：

伺服器 ARNs

對於 伺服器，ARNs採用格式 `arn:aws:transfer:region:account-id:server/server-id`。

範例：`arn:aws:transfer:us-east-1:123456789012:server/s-01234567890abcdef`。

使用者 ARNs

針對使用者，ARN 採用 `arn:aws:transfer:region:account-id:user/server-id/username` 的形式。

範例：`arn:aws:transfer:us-east-1:123456789012:user/s-01234567890abcdef/user1`。

連接器 ARNs

對於連接器，ARNs 採用形式 `arn:aws:transfer:region:account-id:connector/connector-id`。

範例：`arn:aws:transfer:us-east-1:123456789012:connector/c-01234567890abcdef`。

工作流程 ARNs

對於工作流程，ARNs 採用格式 `arn:aws:transfer:region:account-id:workflow/workflow-id`。

範例：`arn:aws:transfer:us-east-1:123456789012:workflow/w-01234567890abcdef`。

WebApp ARNs

對於 Web 應用程式，ARNs 採用形式 `arn:aws:transfer:region:account-id:webapp/webapp-id`。

範例：`arn:aws:transfer:us-east-1:123456789012:webapp/webapp-01234567890abcdef`。

您可以使用 ARN 將鍵值對的標籤指派給實體。標籤是中繼資料，可用於分組或搜尋這些實體。舉例來說，標籤在會計用途方面就非常有用。

DNS 和端點

AWS Transfer Family 針對 API 端點和伺服器端點使用標準化 DNS 命名慣例。了解這些端點對於設定用戶端和進行 API 呼叫至關重要。

API 端點

API 端點用於進行 API 呼叫以管理 AWS Transfer Family 資源。這些端點採用下列形式：

標準 API 端點

標準 API 端點採用 形式 `transfer.region.amazonaws.com`。

範例：`transfer.us-east-1.amazonaws.com`

雙堆疊 API 端點

AWS Transfer Family 提供可使用 IPv4 或 IPv6 請求存取的雙堆疊 API 端點：

- `https://transfer.region-code.api.aws`
- `https://transfer-fips.region-code.api.aws`

伺服器端點

檔案傳輸用戶端會使用伺服器端點來連線至 AWS Transfer Family 伺服器。這些端點採用下列形式：

標準伺服器端點

標準伺服器端點採用 形式 `server-id.server.transfer.region.amazonaws.com`。

範例：`s-01234567890abcdef.server.transfer.us-east-1.amazonaws.com`

自訂主機名稱

您也可以為 AWS Transfer Family 伺服器設定自訂主機名稱。自訂主機名稱可用來為您的使用者提供更易於使用或品牌化的體驗。

若要使用自訂主機名稱，您必須：

1. 擁有網域名稱
2. 提供有效的憑證
3. 設定 DNS 記錄以指向您的 AWS Transfer Family 伺服器

如需依 AWS 區域列出的 AWS Transfer Family 端點完整清單，請參閱 中的 [AWS Transfer Family 端點和配額](#) AWS 一般參考。

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
- 文件最近更新時間：2025 年 11 月 19 日

變更	描述	Date
Transfer Family Web 應用程式的 VPC 端點支援	AWS Transfer Family Web 應用程式現在支援 VPC 託管端點，可讓您在虛擬私有雲端中託管 Web 應用程式端點，以便在不周遊公有網際網路的情況下往返 Amazon S3 進行私有資料傳輸。如需詳細資訊，請參閱 在 VPC 中建立 Transfer Family Web 應用程式 。	2025 年 11 月 19 日
IPv6 支援	AWS Transfer Family 現在支援 SFTP 公有端點的雙堆疊 (IPv4 和 IPv6) 端點、SFTP/FTPS/FTP/AS2 的 VPC 內部端點、SFTP 和 AS2 連接器，以及 API 端點。如需詳細資訊，請參閱 Transfer Family 伺服器的 IPv6 支援 。	2025 年 6 月 30 日
SFTP 連接器使用者體驗的增強功能	• 能夠為連接器自助同時連線設定 • 能夠以 OpenSSH 格式提供 SSH 私有金鑰，用於驗證連線 • 能夠使用其 SFTP 連接器探索遠端伺服器的公有主機金鑰	2025 年 4 月 9 日

變更	描述	Date
	如需詳細資訊，請參閱 使用服務管理的輸出建立 SFTP 連接器 。	
讓 SFTP 連接器能夠在遠端 SFTP 伺服器上刪除、重新命名和移動檔案	您現在可以在從遠端伺服器複製來源檔案之後，透過刪除、重新命名或將來源檔案移至封存位置，來組織存放在遠端 SFTP 伺服器上的檔案。 如需詳細資訊，請參閱移動或重新命名遠端 SFTP 伺服器上的檔案或目錄。	2025 年 4 月 7 日
支援 AWS Transfer Family Web 應用程式	AWS Transfer Family Web 應用程式是新的資源，客戶可以使用它來建立簡單的界面，以透過 Web 瀏覽器存取 Amazon S3 中的資料。如需詳細資訊，請參閱 Transfer Family Web 應用程式 。	2024 年 12 月 1 日
將 API 參考移至單獨的指南	為了改善客戶體驗，API 參考現在與 使用者指南分開發佈。如需個別 API 參考，請參閱 歡迎使用 AWS Transfer Family API 。	2024 年 7 月 31 日
可讓 SFTP 連接器列出遠端檔案和目錄	Transfer Family 新增了讓客戶使用 SFTP 連接器來列出儲存在遠端 SFTP 伺服器中的檔案的能力。如需詳細資訊，請參閱 列出遠端目錄的內容	2024 年 4 月 23 日

變更	描述	Date
能夠搭配 AS2 訊息交換使用交易合作夥伴的自我簽署 TLS 憑證	AWS Transfer Family 已新增匯入和使用貿易合作夥伴的公有自我簽署 TLS 憑證，以透過 HTTPS 將適用性聲明 2 (AS2) 訊息傳送到其伺服器的選項。	2024 年 4 月 12 日
新增 SFTP 連接器的安全政策	AWS Transfer Family 已新增與 SFTP 連接器搭配使用的安全政策。如需詳細資訊，請參閱 AWS Transfer Family SFTP 連接器的安全政策 。	2024 年 4 月 5 日
與 Amazon EventBridge 整合	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一律是最新的安全政策。如需詳細資訊，請參閱 AWS Transfer Family 伺服器的安全政策 。	2024 年 2 月 5 日
支援 SFTP 連接器和 AS2 的靜態 IP 地址	Transfer Family 現在提供 SFTP 連接器和 AS2 的靜態 IP 地址。這可讓透過 IP 允許清單控制項保護的遠端 SFTP 伺服器連線。針對 AS2，我們會為 AS2 伺服器的非同步 MDN 回應引進靜態 IP 地址。	2024 年 1 月 16 日

變更	描述	Date
使用者指南已重新組織，以更接近最新版本的 AWS Transfer Family。	Transfer Family 自指南起已新增多項功能，因此需要重組指南。	2024 年 1 月 3 日
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為檔案。如需詳細資訊，請參閱 使用邏輯目錄的規則 。 建立或更新使用 Amazon S3 進行儲存的伺服器時，您現在可以最佳化列出 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) 端點的 SFTP 伺服器替代連接埠	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 。	2023 年 7 月 25 日
支援 AS2 基本身分驗證	Transfer Family 現在支援使用適用性聲明 2 (AS2) 通訊協定的伺服器使用基本驗證。如需詳細資訊，請參閱 AS2 連接器的基本身分驗證 。	2023 年 6 月 30 日

變更	描述	Date
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、將日誌串流分組為自訂日誌群組，以及跨通訊協定執行常見的日誌查詢。如需詳細資訊，請參閱 AWS Transfer Family 伺服器 Amazon CloudWatch 記錄 。	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處理的檔案支援 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 FTP 上傳到 Amazon Simple Storage Service (Amazon S3) 或 Amazon Elastic File System (Amazon EFS) 的檔案上使用 PGP 解密。如需詳細資訊，請參閱 產生 PGP 金鑰 及 在工作流程中使用 PGP 解密 。	2022 年 12 月 21 日
使用 Transfer Family 伺服器對適用性聲明 2 (AS2) 檔案傳輸通訊協定的完全受管支援	您可以建立使用 AS2 通訊協定的伺服器，在 AWS 環境內部或外部的交易合作夥伴之間傳送和接收資訊。如需詳細資訊，請參閱 設定 AS2 。	2022 年 7 月 25 日

變更	描述	Date
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 建立啟用 SFTP 的伺服器 、 建立啟用 FTPS 的伺服器 或 建立啟用 FTP 的伺服器 。	2022 年 2 月 17 日
支援 AWS Lambda 做為身分提供者	您現在可以 AWS Lambda 搭配 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 來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 來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 for Microsoft Active Directory 。	2021 年 5 月 24 日

變更	描述	Date
新的 AWS 區域	AWS Transfer Family 現已在非洲（開普敦）區域提供。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 現可於亞太區域（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 EFS) 的檔案傳輸。Amazon EFS 是一種簡單、可擴展、全受管的彈性 NFS 檔案系統。如需詳細資訊，請參閱 設定 Amazon EFS 檔案系統 。	2021 年 1 月 6 日
的支援 AWS WAF	Transfer Family 現在支援 AWS WAF 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 VPC 中的伺服器。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	Date
新的 AWS 區域	Transfer Family 現已在 AWS GovCloud (US) 區域中提供。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 的詳細資訊，請參閱 AWS GovCloud (US) 《使用者指南AWS Transfer Family》 中的。	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到您的伺服器	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 AWS Transfer Family 伺服器的安全政策 。	2020 年 8 月 12 日
支援聯邦資訊處理標準 (FIPS) 端點	啟用 FIPS 的端點現在可在北美洲使用 AWS 區域。如需可用的區域，請參閱 AWS Transfer Family 端點和配額 AWS 一般參考。若要為啟用 SFTP 的伺服器端點啟用 FIPS，請參閱 建立啟用 SFTP 的伺服器 。若要為啟用 FTPS 的伺服器端點啟用 FIPS，請參閱 建立啟用 FTPS 的伺服器 。若要為啟用 FTP 的伺服器端點啟用 FIPS，請參閱 建立啟用 FTP 的伺服器 。	2020 年 8 月 12 日

變更	描述	Date
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在符號 (@) 和句點 (.) 包含，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 logging 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 建立啟用 SFTP 的伺服器 、 建立啟用 FTPS 的伺服器 或 建立啟用 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 地址做為授權因素的支援，可讓您在授權透過安全檔案傳輸通訊協定 (SFTP)、透過 SSL 的檔案傳輸通訊協定 (FTPS) 或檔案傳輸通訊協定 (FTP) 進行存取時套用額外的安全層。如需詳細資訊，請參閱 使用自訂身分提供者 。	2020 年 6 月 9 日
AWS Transfer for SFTP 現在已推出 AWS Transfer Family，並新增對 FTP 和 FTPS 的支援。	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 (SFTP) 支援之外，使用者可以在中透過 SSL (FTPS) 和純文字 FTP 型工作流程移動、執行 AWS、保護和整合 FTP。	2020 年 4 月 23 日

變更	描述	Date
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 VPC 中使用	您現在可以在 VPC 中建立伺服器。您可以使用伺服器透過用戶端在 Amazon S3 儲存貯體之間傳輸資料，而無需透過公有網際網路。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
第一個版本的已 AWS Transfer Family 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

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。