



NetApp Copy and Sync文檔

NetApp Copy and Sync

NetApp
December 16, 2025

目錄

NetApp Copy and Sync文檔	1
發行說明	2
NetApp Copy and Sync的新功能	2
2025年10月6日	2
2025年2月2日	2
2024年10月27日	2
2024年9月16日	2
2024年8月11日	2
2024年7月14日	3
2024年6月2日	3
2024年4月8日	3
2024年2月11日	3
2023年11月26日	3
2023年9月3日	4
2023年8月6日	4
2023年7月9日	4
2023年6月11日	5
2023年5月8日	5
2023年4月2日	6
2023年3月7日	6
2023年2月5日	6
2023年1月3日	7
2022年12月11日	7
2022年10月30日	7
2022年9月4日	8
2022年7月31日	9
2022年7月3日	10
2022年6月6日	11
2022年5月1日	12
2022年4月3日	13
2022年3月3日	13
2022年2月6日	14
2022年1月2日	15
2021年11月28日	17
2021年10月31日	18
2021年10月4日	18
2021年9月2日	18
2021年8月1日	18
2021年7月7日	20

2021年6月7日	20
2021年5月2日	21
2021年4月11日	21
NetApp Copy and Sync的限制	22
開始	23
了解NetApp Copy and Sync	23
NetApp Console	23
NetApp Copy and Sync的工作原理	23
支援的儲存類型	24
成本	24
NetApp Copy and Sync快速入門	25
NetApp Copy and Sync中支援的同步關係	26
在NetApp Copy and Sync中準備來源和目標	33
聯網	33
目標目錄	33
讀取目錄的權限	33
Amazon S3 儲存桶需求	34
Azure Blob 儲存需求	35
Azure 資料湖儲存體 Gen2	36
Azure NetApp Files需求	36
盒子要求	37
Google Cloud Storage 儲存桶需求	37
Google 雲端硬碟	38
NFS 伺服器要求	38
ONTAP 需求	39
ONTAP S3 儲存需求	39
SMB 伺服器要求	39
NetApp Copy and Sync的網路概述	40
數據代理位置	40
網路需求	41
網路端點	41
登入NetApp Copy and Sync	43
安裝數據代理	43
在 AWS 中為NetApp Copy and Sync建立新的資料代理	43
在 Azure 中為NetApp Copy and Sync建立新的資料代理	47
在 Google Cloud 中為NetApp Copy and Sync建立新的資料代理	52
在 Linux 主機上安裝用於NetApp Copy and Sync的資料代理	57
使用NetApp Copy and Sync	61
在來源和目標之間同步數據	61
準備資料代理以在NetApp Copy and Sync中的物件儲存之間同步數據	61
在NetApp Copy and Sync中建立同步關係	61

在NetApp Copy and Sync中從 SMB 共用複製 ACL	69
使用NetApp Copy and Sync中的資料傳輸加密同步 NFS 數據	71
設定資料代理組以在NetApp Copy and Sync中使用外部 HashiCorp Vault	75
NetApp Copy and Sync免費試用期結束後，支付同步關係費用	80
從 AWS 訂閱	80
從 Azure 訂閱	81
從NetApp購買許可證並將其添加到複製和同步	81
更新許可證	82
在NetApp Copy and Sync中管理同步關係	82
立即執行資料同步	82
加速同步效能	83
更新憑證	83
設定通知	84
變更同步關係的設定	85
刪除關係	88
在NetApp Copy and Sync中管理資料代理組	89
數據經紀人團體如何運作	89
安全建議	89
將新的資料代理程式新增至群組	90
編輯群組名稱	91
設定統一配置	91
在群組之間移動資料代理	92
更新代理程式配置	93
查看數據代理的配置	93
解決數據代理問題	94
從群組中刪除資料代理	95
刪除資料代理組	96
建立和檢視報告以調整NetApp Copy and Sync中的配置	96
建立報告	96
下載報告	98
查看報告錯誤	99
刪除報告	99
卸載NetApp Copy and Sync的資料代理	99
NetApp Copy and SyncAPI	101
開始	101
使用列表 API	102
API 參考	104
概念	105
NetApp Copy and Sync許可概述	105
市場訂閱	105
NetApp的許可證	105

NetApp Copy and Sync中的資料隱私	106
NetApp Copy and Sync技術常見問題解答	106
入門	106
支持的來源和目標	107
聯網	108
資料同步	109
安全	109
權限	110
物件儲存元數據	110
表現	111
刪除內容	112
故障排除	112
數據經紀人深度探究	112
知識和支持	114
註冊以獲得支持	114
支援註冊概述	114
註冊NetApp Console以取得NetApp支持	114
關聯 NSS 憑證以獲得Cloud Volumes ONTAP支持	116
獲取協助	117
獲取雲端提供者文件服務的支持	117
使用自助選項	117
向NetApp支援建立案例	118
管理您的支援案例（預覽）	120
法律聲明	123
版權	123
商標	123
專利	123
隱私權政策	123
開源	123

NetApp Copy and Sync文檔

發行說明

NetApp Copy and Sync的新功能

了解NetApp Copy and Sync的新功能。

2025年10月6日

BlueXP copy and sync現已更名**NetApp Copy and Sync**

BlueXP copy and sync已重新命名為NetApp Copy and Sync。

BlueXP現在是**NetApp Console**

NetApp Console建立在增強和重組的BlueXP基礎之上，可在企業級內部和雲端環境中集中管理NetApp儲存和NetApp Data Services，提供即時洞察、更快的工作流程和簡化的管理，並且高度安全且合規。

有關更改的詳細信息，請參閱"[NetApp Console發行說明](#)"。

2025年2月2日

新的作業系統支援數據代理

資料代理現在支援執行 Red Hat Enterprise 9.4、Ubuntu 23.04 和 Ubuntu 24.04 的主機。

["查看 Linux 主機需求"](#)。

2024年10月27日

錯誤修復

我們更新了NetApp Copy and Sync和資料代理程式以修復一些錯誤。新的資料代理版本是 1.0.56。

2024年9月16日

錯誤修復

我們更新了NetApp Copy and Sync和資料代理程式以修復一些錯誤。新的資料代理版本是 1.0.55。

2024年8月11日

錯誤修復

我們更新了NetApp Copy and Sync和資料代理程式以修復一些錯誤。新的資料代理版本是 1.0.54。

2024年7月14日

錯誤修復

我們更新了複製和同步以及資料代理程式以修復一些錯誤。新的資料代理版本是 1.0.53。

2024年6月2日

錯誤修復

NetApp Copy and Sync已更新，修復了一些錯誤。資料代理也進行了更新以應用安全性更新。新的資料代理版本是 1.0.52。

2024年4月8日

支援 RHEL 8.9

運行 Red Hat Enterprise Linux 8.9 的主機現在支援資料代理程式。

["查看 Linux 主機需求"](#)。

2024年2月11日

透過正規表示式過濾目錄

使用者現在可以選擇使用正規表示式過濾目錄。

["了解有關*排除目錄*功能的更多資訊。"](#)

2023年11月26日

Azure Blob 的冷儲存類別支援

建立同步關係時，冷儲存 Azure Blob 層現在可用。

["了解有關建立同步關係的更多資訊。"](#)

AWS 資料代理支援特拉維夫地區

在 AWS 中建立資料代理時，特拉維夫現在是受支援的區域。

["了解有關在 AWS 中建立資料代理的更多信息"](#)。

更新資料代理程式的節點版本

所有新的資料代理現在都將使用節點版本 21.2.0。與此更新不相容的資料代理程式（例如 CentOS 7.0 和 Ubuntu Server 18.0）將不再與NetApp Copy and Sync一起使用。

2023年9月3日

透過正規表示式排除文件

使用者現在可以選擇使用正規表示式排除檔案。

["了解有關*排除檔案副檔名*功能的更多資訊。"](#)

建立 **Azure** 資料代理程式時新增 **S3** 金鑰

使用者現在可以在建立 Azure 資料代理程式時新增 AWS S3 存取金鑰和金鑰。

["了解有關在 Azure 中建立資料代理程式的更多資訊。"](#)

2023年8月6日

建立資料代理程式時使用現有的 **Azure** 安全性群組

使用者現在可以選擇在建立資料代理時使用現有的 Azure 安全性群組。

建立資料代理程式時使用的服務帳戶必須具有以下權限：

- “Microsoft.Network/networkSecurityGroups/securityRules/讀取”
- “Microsoft.Network/networkSecurityGroups/讀取”

["了解有關在 Azure 中建立資料代理程式的更多資訊。"](#)

同步到 **Google** 儲存空間時加密數據

使用者現在可以選擇在以 Google 儲存桶為目標建立同步關係時指定客戶管理的加密金鑰。您可以手動輸入密鑰或從單一區域的密鑰清單中選擇。

建立資料代理程式時使用的服務帳戶必須具有以下權限：

- cloudkms.cryptoKeys.列表
- cloudkms.keyRings.列表

["了解有關 Google Cloud Storage 儲存桶要求的更多資訊。"](#)

2023年7月9日

一次刪除多個同步關係

用戶現在可以在 UI 中一次刪除多個同步關係。

["了解有關刪除同步關係的更多資訊。"](#)

僅複製 **ACL**

使用者現在擁有在 CIF 和 NFS 關係中複製 ACL 資訊的附加選項。建立或管理同步關係時，您可以僅複製文

件、僅複製 ACL 資訊或複製文件和 ACL 資訊。

["了解有關複製 ACL 的更多資訊。"](#)

已更新至 Node.js 20

複製和同步已更新至 Node.js 20。所有可用的資料代理都將被更新。無法安裝與此更新不相容的作業系統，且不相容的現有系統可能會遇到效能問題。

2023年6月11日

支援按分鐘自動中止

現在可以使用「同步逾時」功能在十五分鐘後中止尚未完成的活動同步。

["了解有關同步超時設定的更多信息"](#)。

複製存取時間元數據

在包含檔案系統的關係中，*物件複製*功能現在複製存取時間元資料。

["了解有關“複製對象”設定的更多信息"](#)。

2023年5月8日

硬連結功能

使用者現在可以為涉及不安全的 NFS 到 NFS 關係的同步添加硬連結。

["了解有關文件類型設定的詳細信息"](#)。

能夠在安全 NFS 關係中為資料代理程式新增使用者證書

使用者現在可以在建立安全 NFS 關係時為目標資料代理程式設定自己的憑證。他們需要設定伺服器名稱並提供私鑰和憑證 ID。此功能適用於所有資料代理程式。

延長最近修改文件的排除期限

用戶現在可以排除在計劃同步之前 365 天內修改的文件。

["了解有關“最近修改的文件”設定的更多信息"](#)。

透過關係 ID 過濾 UI 中的關係

使用 RESTful API 的使用者現在可以使用關係 ID 來過濾關係。

["了解有關使用 RESTful API 與NetApp Copy and Sync 的更多信息"](#)。

["了解有關排除目錄設定的更多信息"](#)。

2023年4月2日

Azure Data Lake Storage Gen2 關係的額外支持

現在，您可以使用下列內容建立與 Azure Data Lake Storage Gen2 作為來源和目標的同步關係：

- Azure NetApp Files
- 適用於ONTAP 的Amazon FSx
- Cloud Volumes ONTAP
- 本地ONTAP

["詳細了解支援的同步關係"](#)。

按下完整路徑過濾目錄

除了按名稱過濾目錄之外，現在您還可以按完整路徑過濾目錄。

["了解有關排除目錄設定的更多信息"](#)。

2023年3月7日

AWS 資料代理程式的 EBS 加密

現在您可以使用您帳戶中的 KMS 金鑰加密 AWS 資料代理磁碟區。

["了解有關在 AWS 中建立資料代理的更多信息"](#)。

2023年2月5日

對 Azure Data Lake Storage Gen2、ONTAP S3 儲存和 NFS 的額外支持

Cloud Sync現在支援ONTAP S3 儲存和 NFS 的附加同步關係：

- ONTAP S3 儲存到 NFS
- NFS 到ONTAP S3 存儲

Cloud Sync也額外支援 Azure Data Lake Storage Gen2 作為來源和目標：

- NFS 伺服器
- SMB 伺服器
- ONTAP S3 存儲
- StorageGRID
- IBM 雲端物件儲存

["詳細了解支援的同步關係"](#)。

升級至 **Amazon Web Services** 資料代理作業系統

AWS 資料代理程式的作業系統已升級至 Amazon Linux 2022。

["了解有關 AWS 中資料代理執行個體的更多信息"](#)。

2023年1月3日

在 **UI** 上顯示資料代理程式本機配置

現在有一個*顯示配置*選項，可讓使用者在 UI 上查看每個資料代理程式的本機設定。

["了解有關管理資料代理組的更多信息"](#)。

升級到 **Azure** 和 **Google Cloud** 資料代理作業系統

Azure 和 Google Cloud 中的資料代理作業系統已升級至 Rocky Linux 9.0。

["了解有關 Azure 中的資料代理執行個體的更多信息"](#)。

["詳細了解 Google Cloud 中的資料代理程式實例"](#)。

2022年12月11日

按名稱過濾目錄

現在可以使用新的「排除目錄名稱」設定來同步關係。使用者可以從同步中過濾掉最多 15 個目錄名稱。預設情況下，.copy-offload、.snapshot、~snapshot 目錄被排除。

["了解有關排除目錄名稱設定的更多信息"](#)。

額外的 **Amazon S3** 和 **ONTAP S3** 儲存支持

Cloud Sync現在支援 AWS S3 和ONTAP S3 儲存的附加同步關係：

- AWS S3 到ONTAP S3 存儲
- ONTAP S3 儲存到 AWS S3

["詳細了解支援的同步關係"](#)。

2022年10月30日

從 **Microsoft Azure** 持續同步

現在支援使用 Azure 資料代理程式從來源 Azure 儲存體桶到雲端儲存的連續同步設定。

初始資料同步後，Cloud Sync會監聽來源 Azure 儲存體桶上的更改，並在發生任何變更時持續將其同步至目標。從 Azure 儲存桶同步至 Azure Blob 儲存體、CIFS、Google Cloud Storage、IBM Cloud Object Storage、NFS 和StorageGRID時，此設定可用。

Azure 資料代理程式需要自訂角色和下列權限才能使用此設定：

```
'Microsoft.Storage/storageAccounts/read',  
'Microsoft.EventGrid/systemTopics/eventSubscriptions/write',  
'Microsoft.EventGrid/systemTopics/eventSubscriptions/read',  
'Microsoft.EventGrid/systemTopics/eventSubscriptions/delete',  
'Microsoft.EventGrid/systemTopics/eventSubscriptions/getFullUrl/action',  
'Microsoft.EventGrid/systemTopics/eventSubscriptions/getDeliveryAttributes  
/action',  
'Microsoft.EventGrid/systemTopics/read',  
'Microsoft.EventGrid/systemTopics/write',  
'Microsoft.EventGrid/systemTopics/delete',  
'Microsoft.EventGrid/eventSubscriptions/write',  
'Microsoft.Storage/storageAccounts/write'
```

["了解有關“連續同步”設定的更多信息"](#)。

2022年9月4日

額外的 **Google Drive** 支持

- Cloud Sync現在支援 Google Drive 的附加同步關係：
 - Google Drive 到 NFS 伺服器
 - Google Drive 到 SMB 伺服器
- 您也可以產生包含 Google Drive 在內的同步關係的報告。

["了解有關報告的更多信息"](#)。

持續同步增強

現在您可以在以下類型的同步關係上啟用連續同步設定：

- S3 儲存桶到 NFS 伺服器
- Google Cloud Storage 到 NFS 伺服器

["了解有關“連續同步”設定的更多信息"](#)。

電子郵件通知

現在您可以透過電子郵件接收Cloud Sync通知。

為了透過電子郵件接收通知，您需要在同步關係上啟用*通知*設置，然後在NetApp Console中配置警報和通知設定。

["了解如何設定通知"](#)。

2022年7月31日

Google 雲端硬碟

現在您可以將資料從 NFS 伺服器或 SMB 伺服器同步到 Google Drive。「我的雲端硬碟」和「共享雲端硬碟」都支援作為目標。

在建立包含 Google Drive 的同步關係之前，您需要設定具有所需權限和私密金鑰的服務帳戶。["詳細了解 Google Drive 要求"](#)。

["查看支援的同步關係列表"](#)。

其他 Azure Data Lake 支持

Cloud Sync現在支援 Azure Data Lake Storage Gen2 的其他同步關係：

- Amazon S3 到 Azure Data Lake Storage Gen2
- IBM Cloud Object Storage 到 Azure Data Lake Storage Gen2
- StorageGRID到 Azure Data Lake Storage Gen2

["查看支援的同步關係列表"](#)。

建立同步關係的新方法

我們新增了直接從NetApp控制台的系統頁面設定同步關係的其他方法。

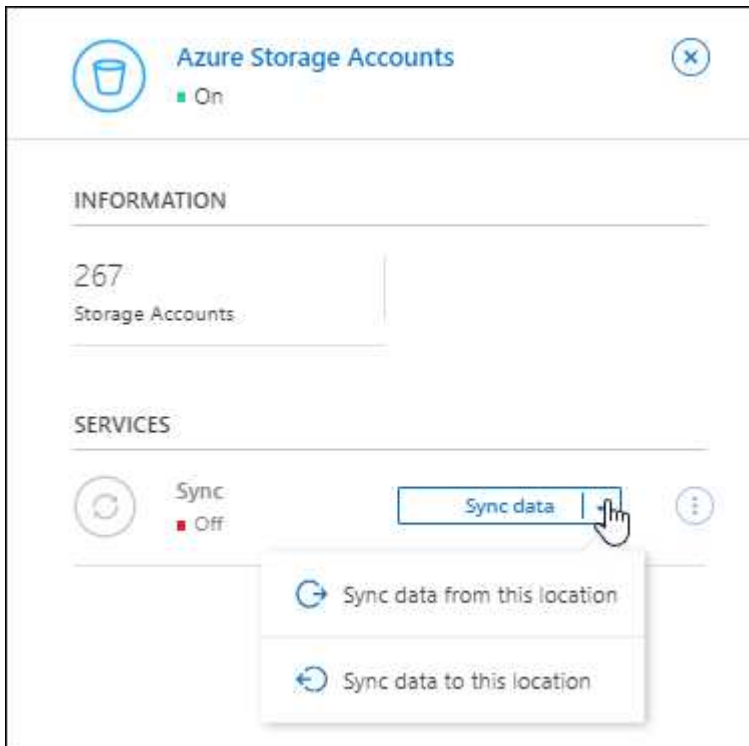
拖放

現在您可以透過將一個系統拖曳到另一個系統上來從系統頁面設定同步關係。



右側面板設定

現在，您可以透過從系統頁面選擇系統，然後從右側面板選擇同步選項來為 Azure Blob 儲存體或 Google Cloud Storage 設定同步關係。



2022年7月3日

支援 **Azure Data Lake Storage Gen2**

現在您可以將資料從 NFS 伺服器或 SMB 伺服器同步到 Azure Data Lake Storage Gen2。

建立包含 Azure Data Lake 的同步關係時，您需要向Cloud Sync提供儲存帳戶連接字串。它必須是常規連接字串，而不是共用存取簽章（SAS）。

["查看支援的同步關係列表"](#)。

從 **Google Cloud Storage** 持續同步

現在支援從來源 Google Cloud Storage 儲存桶到雲端儲存目標的連續同步設定。

初始資料同步後，Cloud Sync會監聽來源 Google Cloud Storage 儲存桶上的變化，並在發生任何變更時持續將其同步到目標。從 Google Cloud Storage 儲存桶同步到 S3、Google Cloud Storage、Azure Blob 儲存、StorageGRID或 IBM Storage 時，此設定可用。

與您的資料代理程式關聯的服務帳戶需要以下權限才能使用此設定：

```
- pubsub.subscriptions.consume
- pubsub.subscriptions.create
- pubsub.subscriptions.delete
- pubsub.subscriptions.list
- pubsub.topics.attachSubscription
- pubsub.topics.create
- pubsub.topics.delete
- pubsub.topics.list
- pubsub.topics.setIamPolicy
- storage.buckets.update
```

["了解有關“連續同步”設定的更多信息"](#)。

新的 **Google Cloud** 區域支持

以下 Google Cloud 區域現在支援Cloud Sync資料代理：

- 哥倫布 (us-east5)
- 達拉斯 (us-south1)
- 馬德里（歐洲西南1）
- 米蘭 (europe-west8)
- 巴黎 (europe-west9)

新的 **Google Cloud** 機器類型

Google Cloud 中資料代理程式的預設機器類型現在是 n2-standard-4。

2022年6月6日

持續同步

新設定可讓您將變更從來源 S3 儲存桶持續同步到目標。

初始資料同步後，Cloud Sync會監聽來源 S3 儲存桶上的變化，並在發生任何變更時持續同步到目標。無需按照預定的時間間隔重新掃描來源。此設定僅在從 S3 儲存桶同步到 S3、Google Cloud Storage、Azure Blob 儲存、StorageGRID或 IBM Storage 時可用。

請注意，與您的資料代理程式關聯的 IAM 角色需要以下權限才能使用此設定：

```
"s3:GetBucketNotification",
"s3:PutBucketNotification"
```

這些權限會自動新增到您建立的任何新資料代理程式。

["了解有關“連續同步”設定的更多信息"](#)。

顯示所有ONTAP卷

當您建立同步關係時，Cloud Sync現在會顯示來源Cloud Volumes ONTAP系統、本機ONTAP叢集或 FSx for ONTAP檔案系統上的所有磁碟區。

以前，Cloud Sync只會顯示與所選協定相符的磁碟區。現在所有磁碟區都會顯示，但任何與所選協定不符或沒有共用或匯出的磁碟區都會顯示為灰色且不可選擇。

將標籤複製到 Azure Blob

當您建立以 Azure Blob 為目標的同步關係時，Cloud Sync現在允許您將標籤複製到 Azure Blob 容器：

- 在*設定*頁面上，您可以使用*物件複製*設定將標籤從來源複製到 Azure Blob 容器。這是對複製元資料的補充。
- 在 **Tags/Metadata** 頁面上，您可以指定要在複製到 Azure Blob 容器的物件上設定的 Blob 索引標籤。以前，您只能指定關係元資料。

當 Azure Blob 是目標且來源是 Azure Blob 或 S3 相容端點（S3、StorageGRID或 IBM Cloud Object Storage）時，支援這些選項。

2022年5月1日

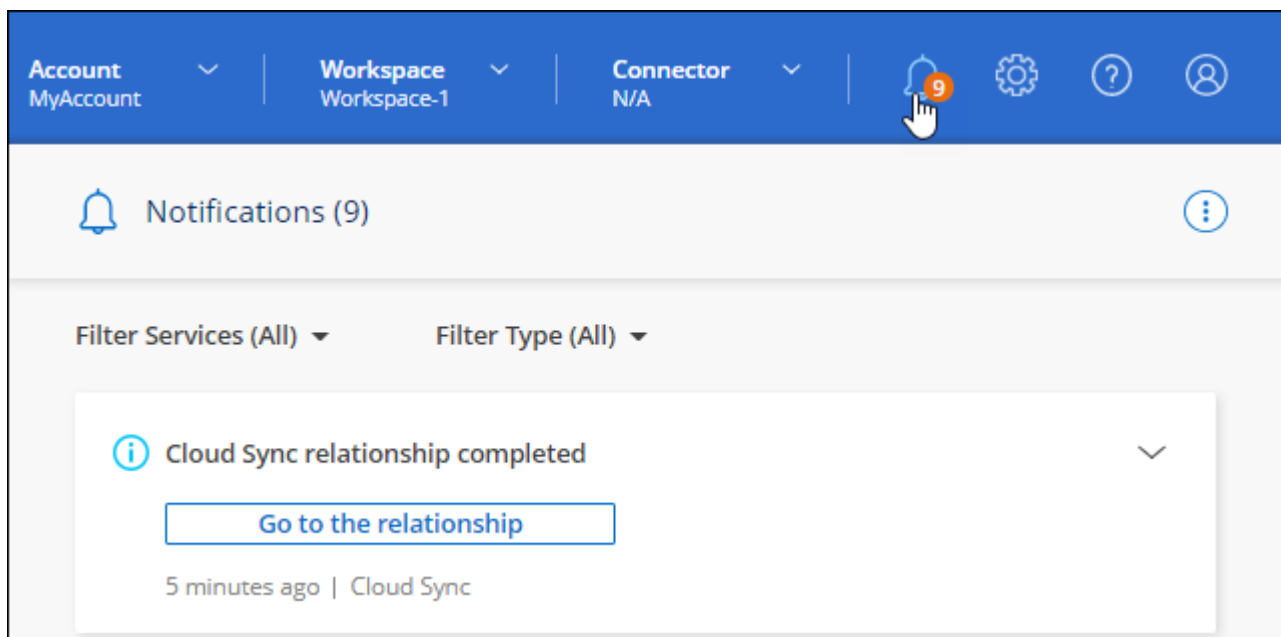
同步逾時

現在可以使用新的*同步逾時*設定來同步關係。此設定可讓您定義如果同步在指定的小時數或天數內未完成，Cloud Sync是否應取消資料同步。

["了解有關更改同步關係設定的詳細信息"](#)。

通知

現在可以使用新的*通知*設定來同步關係。此設定可讓您選擇是否在NetApp控制台的通知中心接收Cloud Sync通知。您可以啟用資料同步成功、資料同步失敗和資料同步取消的通知。



["了解有關更改同步關係設定的詳細信息"](#)。

2022年4月3日

資料代理組增強功能

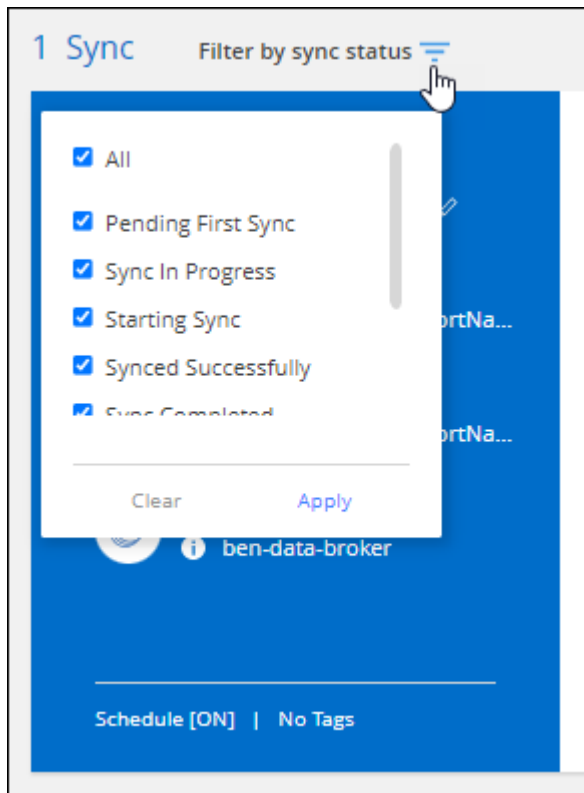
我們對資料代理組進行了幾項增強：

- 現在您可以將資料代理程式移至新的或現有的群組。
- 現在您可以更新資料代理的代理程式配置。
- 最後，您也可以刪除資料代理組。

["了解如何管理資料經紀人群組"](#)。

儀表板過濾器

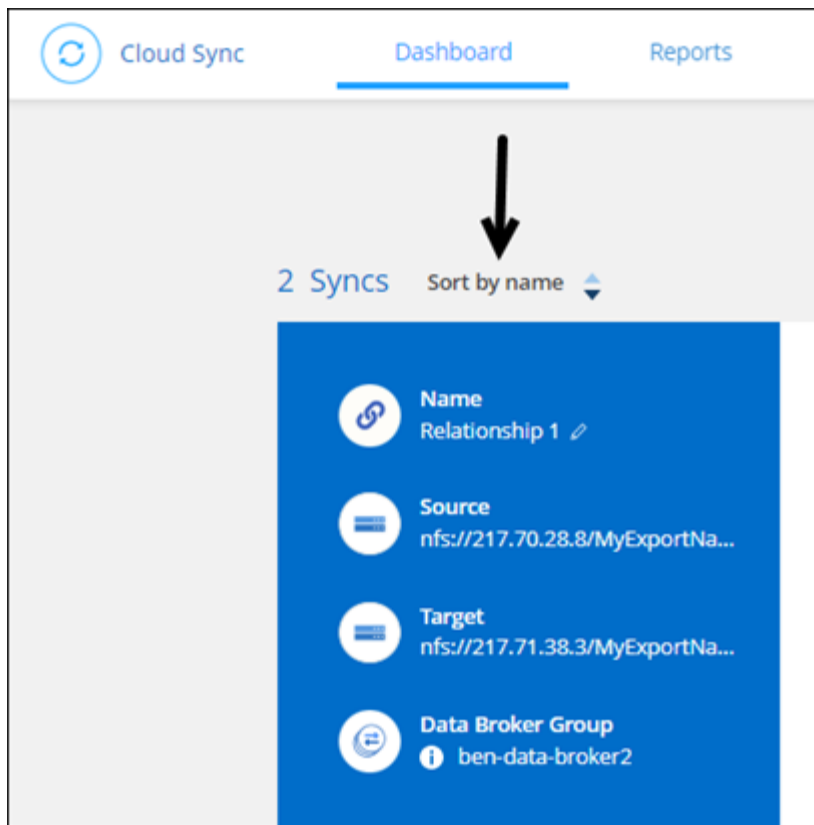
現在您可以過濾同步儀表板的內容，以便更輕鬆地找到符合特定狀態的同步關係。例如，您可以篩選狀態為失敗的同步關係



2022年3月3日

在儀表板中排序

現在您可以按同步關係名稱對儀表板進行排序。



增強數據感知集成

在先前的版本中，我們引入了Cloud Sync與 Cloud Data Sense 的整合。在此更新中，我們透過更輕鬆地建立同步關係來增強整合。從 Cloud Data Sense 啟動資料同步後，所有來源資訊都包含在一個步驟中，只需要您輸入一些關鍵詳細資訊。

Selected Data Sense Source				
Azure NetApp Files	/cifs1 Source	1.1.1.1 Host	cifs Working Environment	\\1.1.1.1\\cifs1 Volume

A few more things before we continue

Define SMB Credentials:

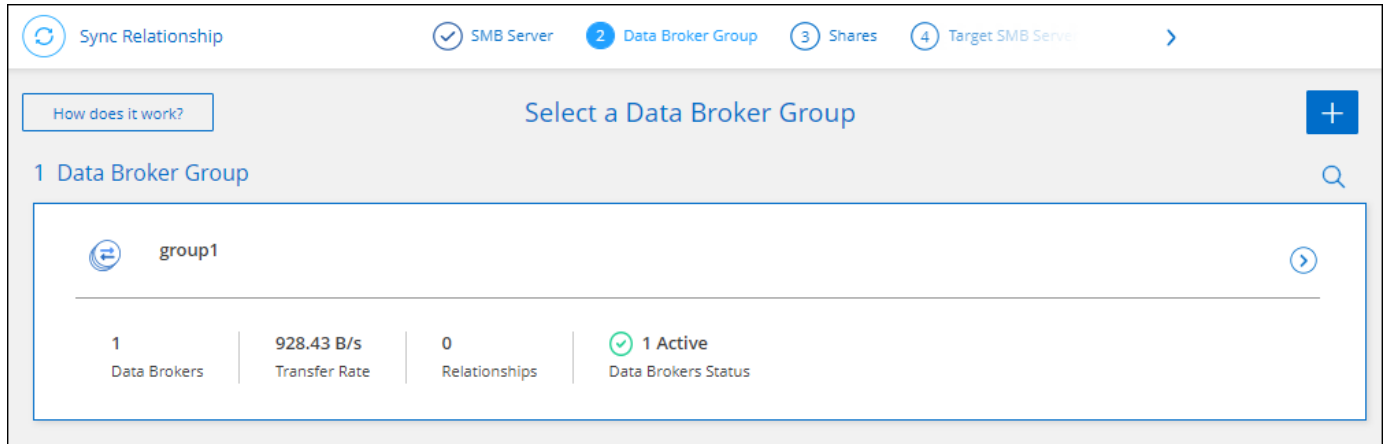
User Name	Password	Domain (Optional)

2022年2月6日

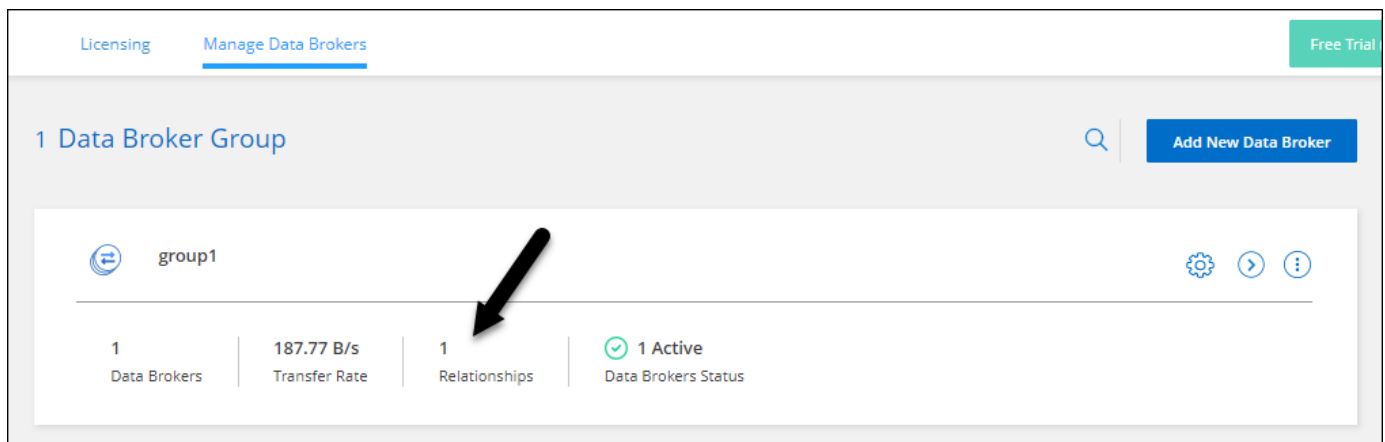
增強數據經紀人群體

我們透過強調資料經紀人_群體_來改變您與資料經紀人互動的方式。

例如，當您建立新的同步關係時，您可以選擇與該關係一起使用的資料代理程式_群組_，而不是特定的資料代理。



在*管理資料代理*標籤中，我們也顯示資料代理群組正在管理的同步關係的數量。



下載 **PDF** 報告

您現在可以下載報告的 PDF。

["了解有關報告的更多信息"](#)。

2022年1月2日

新的 **Box** 同步關係

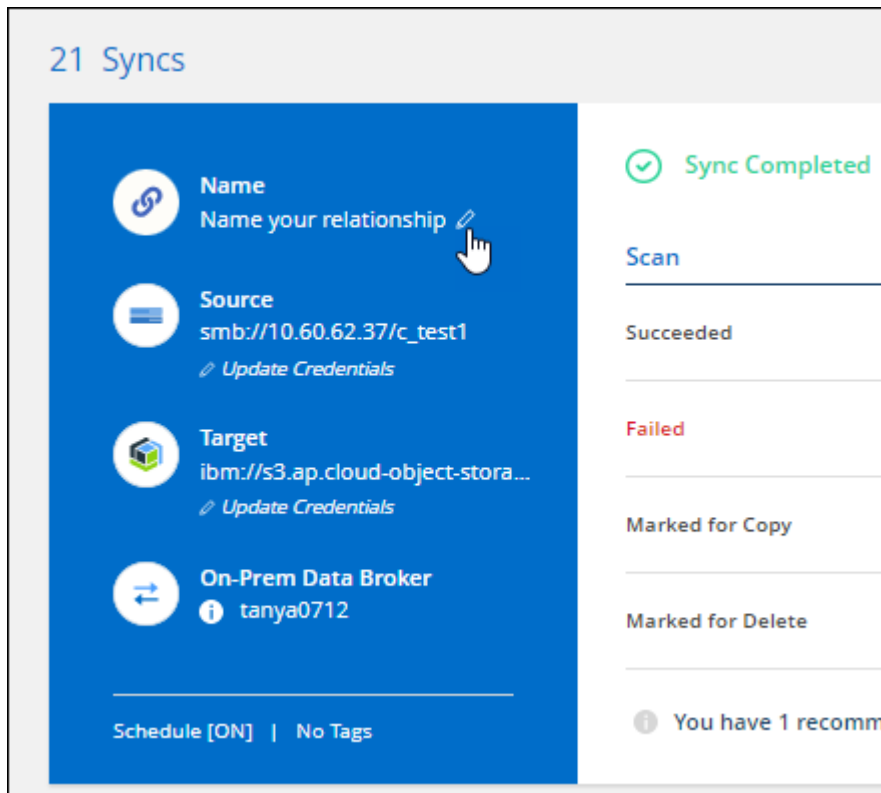
支援兩種新的同步關係：

- Box 到 Azure NetApp Files
- Box 到 Amazon FSx for ONTAP

["查看支援的同步關係列表"](#)。

關係名稱

現在您可以為每個同步關係提供一個有意義的名稱，以便更輕鬆地識別每個關係的目的。您可以在建立關係時以及之後的任何時間新增名稱。



S3 私有連結

當您與 Amazon S3 同步資料時，您可以選擇是否使用 S3 私有連結。當資料代理將資料從來源複製到目標時，它會透過私有連結。

請注意，與您的資料代理程式關聯的 IAM 角色需要以下權限才能使用此功能：

```
"ec2:DescribeVpcEndpoints"
```

此權限會自動新增至您建立的任何新資料代理程式。

冰川即時檢索

當 Amazon S3 是同步關係中的目標時，您現在可以選擇 *Glacier Instant Retrieval* 儲存類別。

從物件儲存到 SMB 共享的 ACL

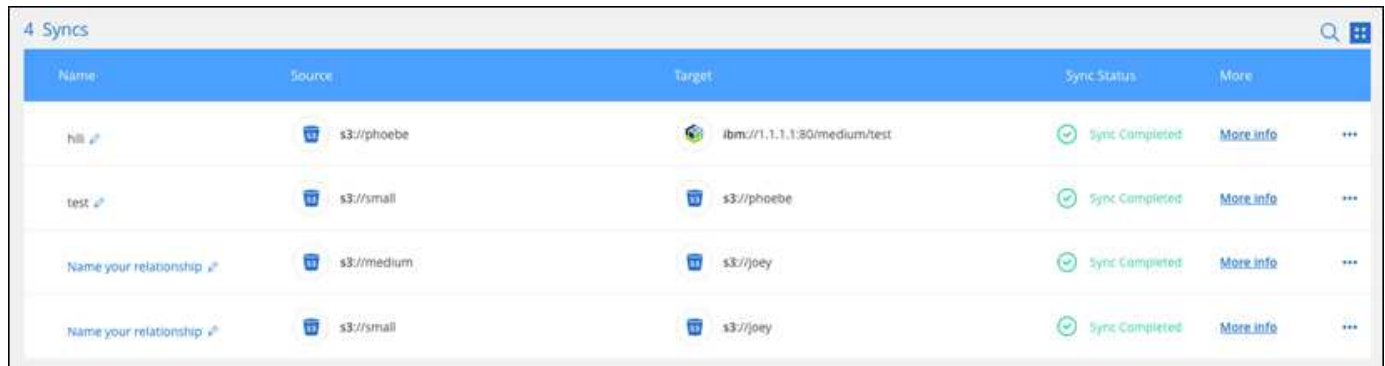
Cloud Sync 現在支援將 ACL 從物件儲存複製到 SMB 共用。以前，我們僅支援將 ACL 從 SMB 共用複製到物件儲存。

SFTP 到 S3

使用者介面現在支援創建從 SFTP 到 Amazon S3 的同步關係。此同步關係以前僅由 API 支援。

表格視圖增強

我們重新設計了儀表板上的表格視圖，以便於使用。如果您選擇*更多資訊*，Cloud Sync會過濾儀表板以向您顯示有關該特定關係的更多資訊。



Name	Source	Target	Sync Status	More
hll	s3://phoebe	ibmc/r1.1.1.1:80/medium/test	Sync Completed	More info
test	s3://small	s3://phoebe	Sync Completed	More info
Name your relationship	s3://medium	s3://joey	Sync Completed	More info
Name your relationship	s3://small	s3://joey	Sync Completed	More info

支持雅加達地區

Cloud Sync現在支援在 AWS 亞太地區（雅加達）區域部署資料代理程式。

2021年11月28日

從 SMB 到物件儲存的 ACL

現在，在設定從來源 SMB 共用到物件儲存（ONTAP S3 除外）的同步關係時，Cloud Sync可以複製存取控制清單 (ACL)。

Cloud Sync不支援將 ACL 從物件儲存複製到 SMB 共用。

["了解如何從 SMB 共用複製 ACL"。](#)

更新許可證

現在您可以更新已延長的Cloud Sync許可證。

如果您延長了從NetApp購買的Cloud Sync許可證，則可以再次新增該許可證以刷新到期日。

["了解如何更新許可證"。](#)

更新 Box 憑證

現在您可以更新現有同步關係的 Box 憑證。

["了解如何更新憑證"。](#)

2021年10月31日

箱體支撐

Box 支援現已在Cloud Sync使用者介面中作為預覽提供。

Box 可以是幾種同步關係中的來源或目標。["查看支援的同步關係列表"](#)。

建立日期設定

當 SMB 伺服器作為來源時，名為「建立日期」的新同步關係設定可讓您同步在特定日期之後、特定日期之前或特定時間範圍之間建立的檔案。

["詳細了解Cloud Sync設定"](#)。

2021年10月4日

附加 Box 支援

Cloud Sync現在支援以下同步關係 ["盒子"](#)使用Cloud Sync API 時：

- Amazon S3 到 Box
- IBM 雲端物件儲存到 Box
- StorageGRID到 Box
- 盒子到 NFS 伺服器
- 盒子到 SMB 伺服器

["了解如何使用 API 設定同步關係"](#)。

SFTP 路徑報告

您現在可以["建立報告"](#)用於 SFTP 路徑。

2021年9月2日

支援 FSx for ONTAP

現在您可以將資料同步到Amazon FSx for ONTAP 檔案系統或從 Amazon FSx for ONTAP檔案系統同步資料。

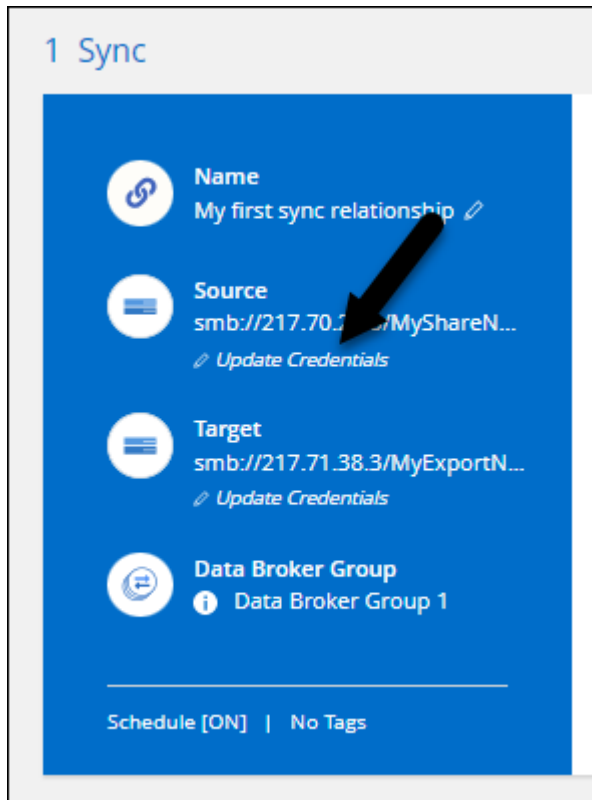
- ["了解Amazon FSx for ONTAP"](#)
- ["查看支援的同步關係"](#)
- ["了解如何為Amazon FSx for ONTAP建立同步關係"](#)

2021年8月1日

更新憑證

現在，Cloud Sync可讓您使用現有同步關係中的來源或目標的最新憑證來更新資料代理程式。

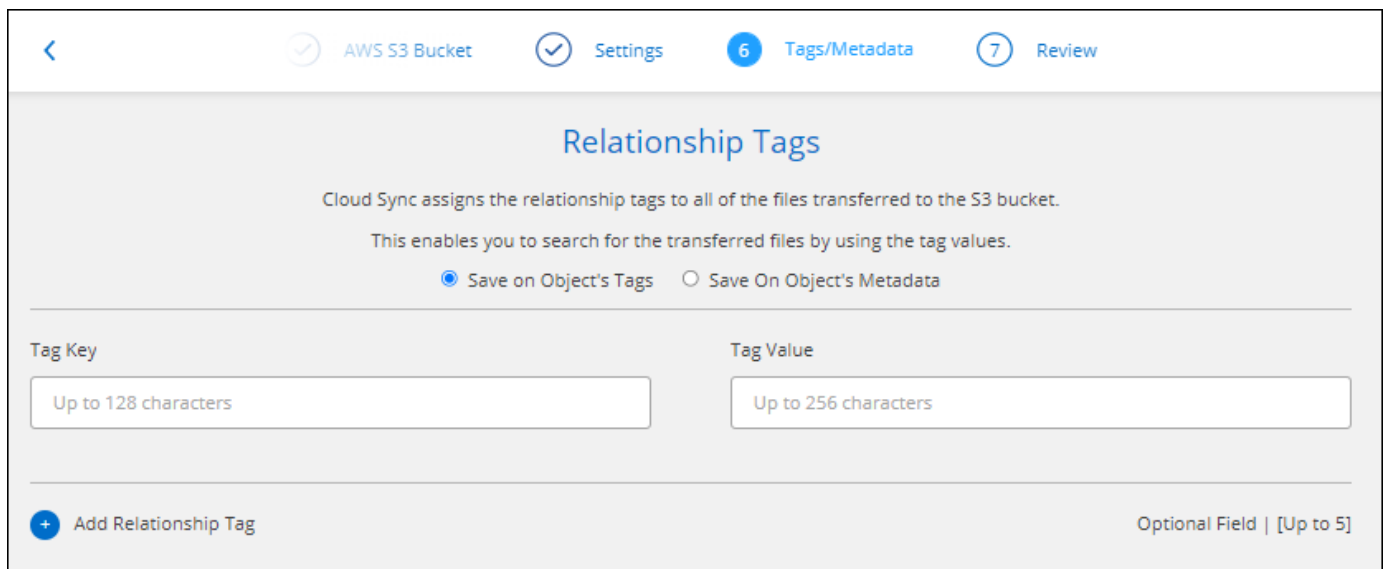
如果您的安全性原則要求您定期更新憑證，則此增強功能可以提供協助。["了解如何更新憑證"](#)。



物件儲存目標的標籤

建立同步關係時，現在可以為同步關係中的物件儲存目標新增標籤。

Amazon S3、Azure Blob、Google Cloud Storage、IBM Cloud Object Storage 和StorageGRID支援新增標籤。



支援 **Box**

Cloud Sync現在支援 "**盒子**"作為使用Cloud Sync API 時與 Amazon S3、StorageGRID和 IBM Cloud Object Storage 同步關係中的來源。

["了解如何使用 API 設定同步關係"](#)。

Google Cloud 中資料代理程式的公用 IP

在 Google Cloud 中部署資料代理程式時，現在可以選擇為虛擬機器執行個體啟用或停用公用 IP 位址。

["了解如何在 Google Cloud 中部署資料代理"](#)。

Azure NetApp Files的雙協定磁碟區

當您為Azure NetApp Files選擇來源磁碟區或目標磁碟區時，無論您為同步關係選擇哪種協議，Cloud Sync現在都會顯示雙協定磁碟區。

2021年7月7日

ONTAP S3 儲存與 **Google Cloud Storage**

Cloud Sync現在支援從使用者介面同步ONTAP S3 儲存和 Google Cloud Storage 儲存桶之間的關係。

["查看支援的同步關係列表"](#)。

對像元資料標籤

當您建立同步關係並啟用設定時，Cloud Sync現在可以基於物件的儲存之間複製物件元資料和標籤。

["了解有關"複製對象"設定的更多信息"](#)。

支援 **HashiCorp Vault**

現在您可以設定資料代理，透過使用 Google Cloud 服務帳戶進行身份驗證來存取來自外部 HashiCorp Vault 的憑證。

["了解有關使用 HashiCorp Vault 和數據代理的更多信息"](#)。

定義 **S3** 儲存桶的標籤或元數據

在設定與 Amazon S3 儲存桶的同步關係時，同步關係精靈現在可讓您定義要在目標 S3 儲存桶中的物件上儲存的標籤或元資料。

標記選項以前是同步關係設定的一部分。

2021年6月7日

Google Cloud 中的儲存類別

當 Google Cloud Storage 儲存桶成為同步關係中的目標時，您現在可以選擇要使用的儲存類別。Cloud Sync支

援以下儲存類別：

- 標準
- 近線
- 涼線
- 檔案

2021年5月2日

報告中的錯誤

現在您可以查看報告中發現的錯誤，並且可以刪除最後一份報告或所有報告。

["了解有關建立和查看報告以調整配置的更多信息"](#)。

比較屬性

現在每個同步關係都可以使用新的*比較*設定。

此進階設定可讓您選擇Cloud Sync在確定檔案或目錄是否已變更並應再次同步時是否應比較某些屬性。

["了解有關更改同步關係設定的詳細信息"](#)。

2021年4月11日

獨立Cloud Sync服務已停用

獨立的Cloud Sync服務已退役。現在您可以直接從NetApp Console存取Cloud Sync，其中所有相同的功能和功能均可使用。

登入NetApp Console後，您可以切換到頂部的「同步」標籤並查看您的關係，就像以前一樣。

不同項目中的 **Google Cloud** 儲存桶

設定同步關係時，如果您向資料代理程式的服務帳戶提供所需的權限，則可以從不同項目中的 Google Cloud 儲存桶中進行選擇。

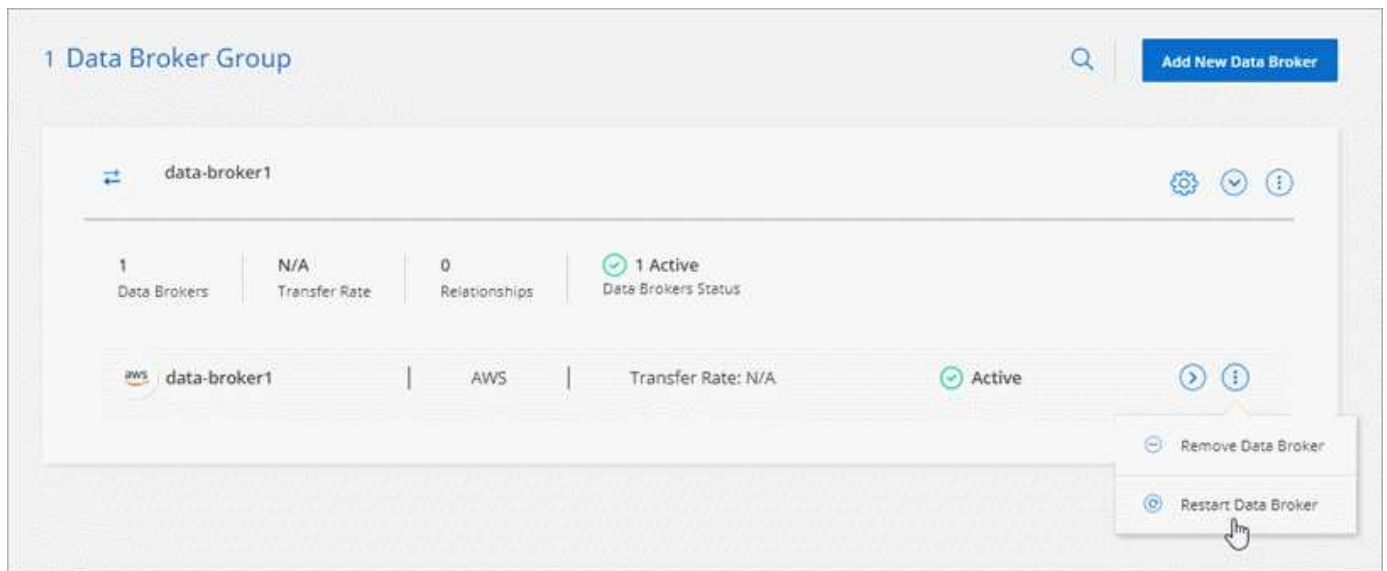
["了解如何設定服務帳戶"](#)。

Google Cloud Storage 與 **S3** 之間的元數據

Cloud Sync現在可以在 Google Cloud Storage 和 S3 供應商（AWS S3、StorageGRID和 IBM Cloud Object Storage）之間複製元資料。

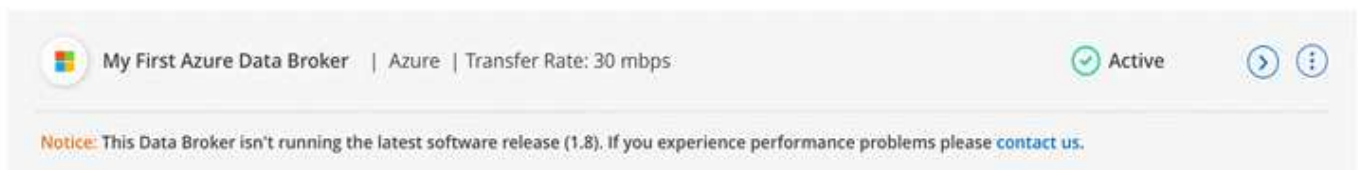
重啟數據代理

現在您可以從Cloud Sync重新啟動資料代理程式。



未運行最新版本時的消息

Cloud Sync現在可以識別資料代理何時未執行最新軟體版本。此訊息可協助確保您獲得最新的功能和功能。



NetApp Copy and Sync的限制

已知限制標識了該產品的此版本不支援或無法與其正確互通的平台、裝置或功能。仔細審查這些限制。

以下區域不支援NetApp Copy and Sync：

- AWS 政府區域
- Azure 政府區域
- 中國

開始

了解NetApp Copy and Sync

NetApp Copy and Sync提供了一種簡單、安全且自動化的方式，可將您的資料遷移到雲端或本地的任何目標。無論它是基於文件的 NAS 資料集（NFS 或 SMB）、Amazon Simple Storage Service (S3) 物件格式、NetApp StorageGRID設備或任何其他雲端提供者物件存儲，Copy and Sync 都可以為您轉換和移動它。

NetApp Console

可透過NetApp Console存取NetApp Copy and Sync。

NetApp Console提供企業級跨本機和雲端環境的NetApp儲存和資料服務的集中管理。需要控制台才能存取和使用NetApp資料服務。作為管理介面，它使您能夠從一個介面管理許多儲存資源。控制台管理員可以控制企業內所有系統的儲存和服務的存取。

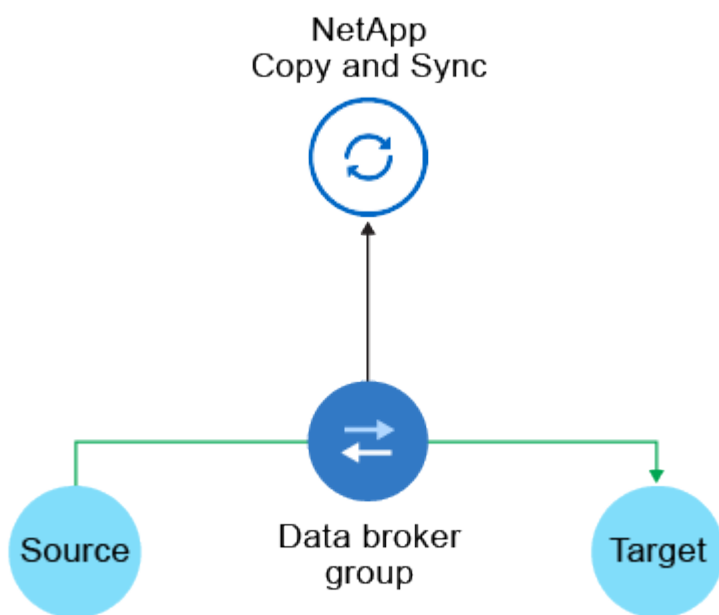
您不需要許可證或訂閱即可開始使用NetApp Console，並且只有當您需要在雲端部署控制台代理程式以確保與儲存系統或NetApp資料服務的連線時才需要付費。但是，一些可從控制台存取的NetApp資料服務是需要授權或基於訂閱的。

詳細了解 "[NetApp Console](#)"。

NetApp Copy and Sync的工作原理

NetApp Copy and Sync是一個軟體即服務 (SaaS) 平台，由資料代理群組、可透過NetApp Console存取的基於雲端的介面以及來源和目標組成。

下圖顯示了 Copy 和 Sync 元件之間的關係：



NetApp資料代理軟體將資料從來源同步到目標（這稱為_同步關係_）。您可以在 AWS、Azure、Google Cloud

Platform 或您的本機上執行資料代理程式。由一個或多個資料代理組成的資料代理群組需要透過連接埠 443 建立出站互聯網連接，以便它可以與複製和同步進行通訊並聯繫其他一些服務和儲存庫。["查看端點列表"](#)。

初始複製後，「複製和同步」會根據您設定的計劃同步任何變更的資料。

支援的儲存類型

複製和同步支援以下儲存類型：

- 任何 NFS 伺服器
- 任何 SMB 伺服器
- 亞馬遜 EFS
- 適用於ONTAP 的Amazon FSx
- 亞馬遜 S3
- Azure Blob
- Azure 資料湖儲存體 Gen2
- Azure NetApp Files
- Box（可預覽）
- Cloud Volumes ONTAP
- Google 雲端儲存
- Google 雲端硬碟
- IBM 雲端物件儲存
- 本地ONTAP集群
- ONTAP S3 存儲
- SFTP（僅使用 API）
- StorageGRID

["查看支援的同步關係"](#)。

成本

使用複製和同步涉及兩種類型的成本：資源費用和服務費用。

資源費用

資源費用與在雲端中運行一個或多個資料代理程式的運算和儲存成本有關。

服務費

14 天免費試用期結束後，有兩種方式可以支付同步關係的費用。第一個選項是從 AWS 或 Azure 訂閱，這樣您就可以按小時或按年付費。第二種選擇是直接從NetApp購買許可證。

["了解許可的工作原理"](#)。

NetApp Copy and Sync快速入門

開始使用NetApp Copy and Sync包含幾個步驟。

1

登入並設定NetApp Console

您應該已經開始使用NetApp Console，其中包括登入、設定帳戶以及可能部署控制台代理程式和建立系統。

如果您想要為以下任何一項建立同步關係，那麼您首先需要建立或發現一個系統：

- 適用於ONTAP 的Amazon FSx
- Azure NetApp Files
- Cloud Volumes ONTAP
- 本地ONTAP集群

Cloud Volumes ONTAP、本機ONTAP叢集和Amazon FSx for ONTAP都需要控制台代理程式。

- ["了解如何開始使用NetApp Console"](#)
- ["了解有關控制台代理的更多信息"](#)

2

準備源和目標

驗證您的來源和目標是否受支援並已設定。最重要的要求是驗證資料代理組與來源位置和目標位置之間的連線。

- ["查看支援的關係"](#)
- ["準備源和目標"](#)

3

為NetApp資料代理程式準備位置

NetApp資料代理軟體將資料從來源同步到目標（這稱為_同步關係_）。您可以在 AWS、Azure、Google Cloud Platform 或您的本機上執行資料代理程式。由一個或多個資料代理組成的資料代理組需要透過連接埠 443 建立出站互聯網連接，以便與NetApp Copy and Sync並聯繫其他一些服務和儲存庫。["查看端點列表"](#)。

當您建立同步關係時，NetApp Copy and Sync會引導您完成安裝過程，此時您可以在雲端部署資料代理程式或為您自己的 Linux 主機下載安裝腳本。

- ["檢查 AWS 安裝"](#)
- ["查看 Azure 安裝Review Azure installation"](#)
- ["檢查 Google Cloud 安裝"](#)
- ["檢查 Linux 主機安裝"](#)

4

建立您的第一個同步關係

登入 ["NetApp Console"](#)，選擇*同步*，然後拖曳來源和目標的選擇。按照提示完成設定。["了解更多"](#)。

從 AWS 或 Azure 訂閱，按使用量付費或按年付費。或直接從NetApp購買許可證。只需前往NetApp Copy and Sync中的「許可證設定」頁面進行設定。["了解更多"](#)。

NetApp Copy and Sync中支援的同步關係

NetApp Copy and Sync可讓您將資料從來源同步到目標。這稱為同步關係。在開始之前您應該了解所支援的關係。

來源位置	支援的目標位置
亞馬遜 EFS	• 亞馬遜 EFS • 適用於ONTAP 的Amazon FSx • 亞馬遜 S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Google 雲端儲存 • IBM 雲端物件儲存 • NFS 伺服器 • 本地ONTAP集群（NFS 或 SMB） • SMB 伺服器 • StorageGRID
適用於ONTAP 的Amazon FSx	• 亞馬遜 EFS • 適用於ONTAP 的Amazon FSx • 亞馬遜 S3 • Azure Blob • Azure 資料湖儲存體 Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Google 雲端儲存 • IBM 雲端物件儲存 • NFS 伺服器 • 本地ONTAP集群（NFS 或 SMB） • SMB 伺服器 • StorageGRID

來源位置	支援的目標位置
亞馬遜 S3	• 亞馬遜 EFS • 適用於ONTAP 的Amazon FSx • 亞馬遜 S3 • Azure Blob • Azure 資料湖儲存體 Gen2 • Azure NetApp Files • 盒子¹ • Cloud Volumes ONTAP • Google 雲端儲存 • IBM 雲端物件儲存 • NFS 伺服器 • 本地ONTAP集群（NFS 或 SMB） • ONTAP S3 存儲 • SMB 伺服器 • StorageGRID
Azure Blob	• 亞馬遜 EFS • 適用於ONTAP 的Amazon FSx • 亞馬遜 S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Google 雲端儲存 • IBM 雲端物件儲存 • NFS 伺服器 • 本地ONTAP集群（NFS 或 SMB） • SMB 伺服器 • StorageGRID

來源位置	支援的目標位置
Azure 資料湖儲存體 Gen2	• Azure NetApp Files • Cloud Volumes ONTAP • 適用於ONTAP的 FSx • IBM 雲端物件儲存 • NFS 伺服器 • 本地ONTAP • ONTAP S3 存儲 • SMB 伺服器 • StorageGRID
Azure NetApp Files	• 亞馬遜 EFS • 適用於ONTAP 的Amazon FSx • 亞馬遜 S3 • Azure Blob • Azure 資料湖儲存體 Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Google 雲端儲存 • IBM 雲端物件儲存 • NFS 伺服器 • 本地ONTAP集群（NFS 或 SMB） • SMB 伺服器 • StorageGRID
盒子 ¹	• 適用於ONTAP 的Amazon FSx • 亞馬遜 S3 • Azure NetApp Files • Cloud Volumes ONTAP • IBM 雲端物件儲存 • NFS 伺服器 • SMB 伺服器 • StorageGRID

來源位置	支援的目標位置
Cloud Volumes ONTAP	• 亞馬遜 EFS • 適用於ONTAP 的Amazon FSx • 亞馬遜 S3 • Azure Blob • Azure 資料湖儲存體 Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Google 雲端儲存 • IBM 雲端物件儲存 • NFS 伺服器 • 本地ONTAP集群（NFS 或 SMB） • SMB 伺服器 • StorageGRID
Google 雲端儲存	• 亞馬遜 EFS • 適用於ONTAP 的Amazon FSx • 亞馬遜 S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Google 雲端儲存 • IBM 雲端物件儲存 • NFS 伺服器 • 本地ONTAP集群（NFS 或 SMB） • ONTAP S3 存儲 • SMB 伺服器 • StorageGRID
Google 雲端硬碟	• NFS 伺服器 • SMB 伺服器

來源位置	支援的目標位置
IBM 雲端物件儲存	• 亞馬遜 EFS • 適用於ONTAP 的Amazon FSx • 亞馬遜 S3 • Azure Blob • Azure 資料湖儲存體 Gen2 • Azure NetApp Files • 盒子¹ • Cloud Volumes ONTAP • Google 雲端儲存 • IBM 雲端物件儲存 • NFS 伺服器 • 本地ONTAP集群（NFS 或 SMB） • SMB 伺服器 • StorageGRID
NFS 伺服器	• 亞馬遜 EFS • 適用於ONTAP 的Amazon FSx • 亞馬遜 S3 • Azure Blob • Azure 資料湖儲存體 Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Google 雲端儲存 • Google 雲端硬碟 • IBM 雲端物件儲存 • NFS 伺服器 • 本地ONTAP集群（NFS 或 SMB） • ONTAP S3 存儲 • SMB 伺服器 • StorageGRID

來源位置	支援的目標位置
本地ONTAP集群（NFS 或 SMB）	• 亞馬遜 EFS • 適用於ONTAP 的Amazon FSx • 亞馬遜 S3 • Azure Blob • Azure 資料湖儲存體 Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Google 雲端儲存 • IBM 雲端物件儲存 • NFS 伺服器 • 本地ONTAP集群（NFS 或 SMB） • SMB 伺服器 • StorageGRID
ONTAP S3 存儲	• 亞馬遜 S3 • Azure 資料湖儲存體 Gen2 • Google 雲端儲存 • NFS 伺服器 • SMB 伺服器 • StorageGRID • ONTAP S3 存儲
SFTP ²	S3

來源位置	支援的目標位置
SMB 伺服器	• 亞馬遜 EFS • 適用於ONTAP 的Amazon FSx • 亞馬遜 S3 • Azure Blob • Azure 資料湖儲存體 Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Google 雲端儲存 • Google 雲端硬碟 • IBM 雲端物件儲存 • NFS 伺服器 • 本地ONTAP集群（NFS 或 SMB） • ONTAP S3 存儲 • SMB 伺服器 • StorageGRID
StorageGRID	• 亞馬遜 EFS • 適用於ONTAP 的Amazon FSx • 亞馬遜 S3 • Azure Blob • Azure 資料湖儲存體 Gen2 • Azure NetApp Files • 盒子¹ • Cloud Volumes ONTAP • Google 雲端儲存 • IBM 雲端物件儲存 • NFS 伺服器 • 本地ONTAP集群（NFS 或 SMB） • ONTAP S3 存儲 • SMB 伺服器 • StorageGRID

筆記：

1. Box 支援目前可作為預覽使用。

2. 僅透過使用複製和同步 API 支援與此來源/目標的同步關係。
3. 當 Blob 容器是目標時，您可以選擇特定的 Azure Blob 儲存層：
 - 熱儲存
 - 冷藏
4. 當 Amazon S3 是目標時，您可以選擇特定的 S3 儲存類別：
 - 標準（這是預設類別）
 - 智能分層
 - 標準-不頻繁訪問
 - 單區-不頻繁訪問
 - 冰川深度檔案
 - 冰川彈性檢索
 - 冰川即時檢索
5. 當 Google Cloud Storage 儲存桶是目標時，您可以選擇特定的儲存類別：
 - 標準
 - 近線
 - 涼線
 - 檔案

在NetApp Copy and Sync中準備來源和目標

驗證您的來源和目標是否符合NetApp Copy and Sync中的以下要求。

聯網

- 來源和目標必須與資料代理組有網路連線。

例如，如果 NFS 伺服器位於您的資料中心，而資料代理程式位於 AWS 中，那麼您需要從您的網路到 VPC 的網路連線（VPN 或 Direct Connect）。

- NetApp建議設定來源、目標和資料代理程式以使用網路時間協定 (NTP) 服務。三個組件之間的時間差不應超過5分鐘。

目標目錄

當您建立同步關係時，「複製和同步」可讓您選擇現有的目標目錄，然後可以選擇在該目錄內建立新資料夾。因此請確保您的首選目標目錄已經存在。

讀取目錄的權限

為了顯示來源或目標中的每個目錄或資料夾，「複製和同步」需要對該目錄或資料夾的讀取權限。

NFS

必須在來源/目標上使用檔案和目錄的 uid/gid 定義權限。

物件儲存

- 對於 AWS 和 Google Cloud，資料代理程式必須具有列出物件權限（如果您遵循資料代理安裝步驟，則預設提供這些權限）。
- 對於 Azure、StorageGRID 和 IBM，設定同步關係時輸入的憑證必須具有列出物件權限。

中小企業

設定同步關係時輸入的 SMB 憑證必須具有列出資料夾權限。



資料代理程式預設忽略以下目錄：`.snapshot`、`~snapshot`、`.copy-offload`



使用複製和同步將 SMB 資料複製到 Cloud Volumes ONTAP 時，來源系統中的檔案和資料夾擁有權不會保留。造成這種行為的原因是 Copy and Sync 使用了 Linux SMB 用戶端，並將所有權分配給用於驗證傳輸的使用者或服務帳戶。雖然可以保留存取控制列表，但所有權和稽核資訊可能與來源系統不同。這是預期行為。

Amazon S3 儲存桶需求

確保您的 Amazon S3 儲存桶符合以下要求。

Amazon S3 支援的資料代理位置

包含 S3 儲存的同步關係需要在 AWS 或您的場所部署資料代理程式。無論哪種情況，複製和同步都會提示您在安裝期間將資料代理程式與 AWS 帳戶關聯。

- ["了解如何部署 AWS 資料代理"](#)
- ["了解如何在 Linux 主機上安裝資料代理"](#)

支援的 AWS 區域

除中國地區外，所有地區均受支援。

其他 AWS 帳戶中的 S3 儲存桶所需的權限

設定同步關係時，您可以指定位於與資料代理程式無關的 AWS 帳戶中的 S3 儲存桶。

["此 JSON 檔案中包含的權限"](#)必須應用於該 S3 儲存桶，以便資料代理程式可以存取它。這些權限使數據代理能夠將數據複製到儲存桶或從儲存桶中複製數據，並列出儲存桶中的物件。

請注意 JSON 檔案中包含的權限的以下幾點：

1. `<BucketName>` 是位於與資料代理程式無關的 AWS 帳戶中的儲存桶的名稱。
2. `<RoleARN>` 應替換為以下之一：
 - 如果在 Linux 主機上手動安裝了資料代理，則 `RoleARN` 應該是您在部署資料代理時為其提供 AWS 憑證的 AWS 使用者的 ARN。

- 如果使用 CloudFormation 範本在 AWS 中部署了資料代理，則 *RoleARN* 應該是該範本建立的 IAM 角色的 ARN。

您可以透過前往 EC2 控制台、選擇資料代理實例，然後從描述標籤中選擇 IAM 角色來找到角色 ARN。然後，您應該會在 IAM 控制台中看到包含角色 ARN 的「摘要」頁面。

Summary

[Delete role](#)

Role ARN `arn:aws:iam::142281742600:role/tanyaBroker0304-DataBrokerIamRole-1VMHWXMW3AQ05` 

Role description [Edit](#)

Azure Blob 儲存需求

確保您的 Azure Blob 儲存體符合以下需求。

Azure Blob 支援的資料代理程式位置

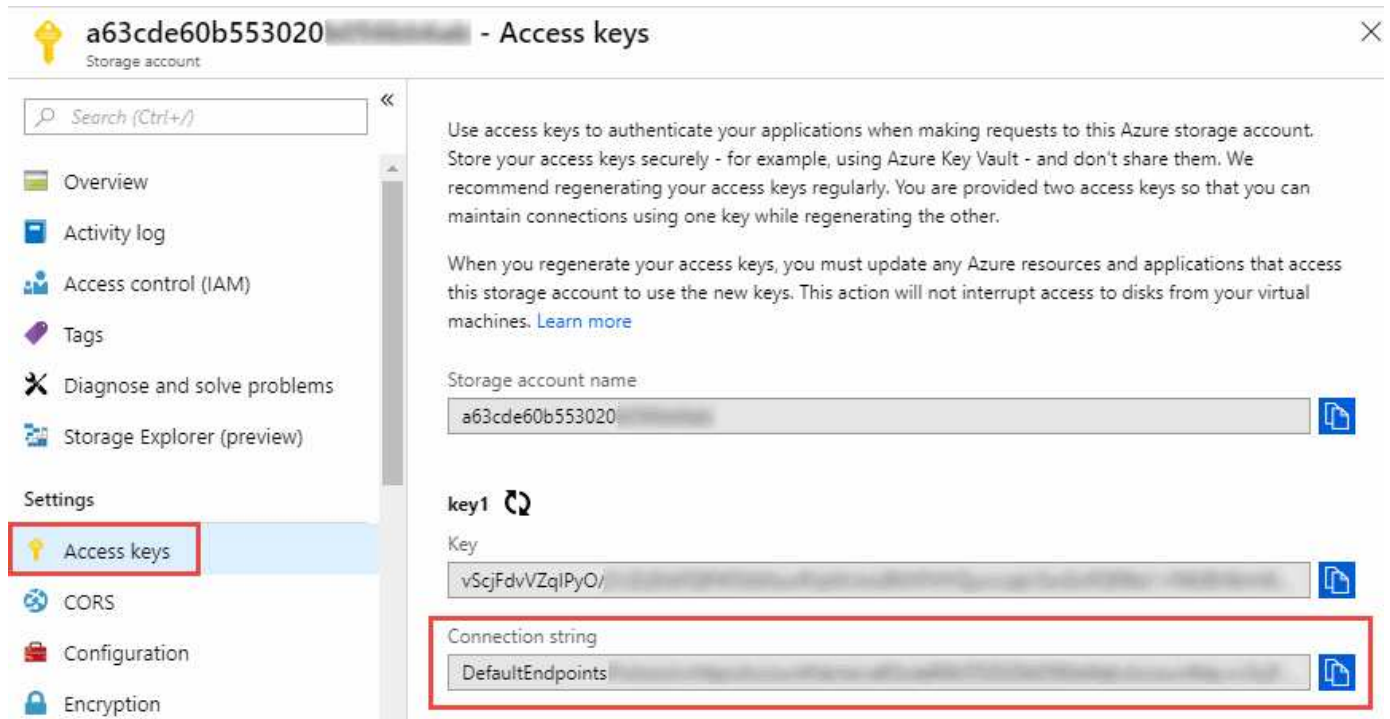
當同步關係包含 Azure Blob 儲存體時，資料代理程式可以駐留在任何位置。

支援的 Azure 區域

除中國、美國政府和美國國防部地區外，所有地區均受支持。

包含 Azure Blob 和 NFS/SMB 的關係的连接字串

在 Azure Blob 容器和 NFS 或 SMB 伺服器之間建立同步關係時，需要為複製和同步提供儲存帳戶连接字串：



a63cde60b553020 - Access keys

Storage account

Search (Ctrl+/)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Storage Explorer (preview)
- Settings
 - Access keys**
 - CORS
 - Configuration
 - Encryption

Use access keys to authenticate your applications when making requests to this Azure storage account. Store your access keys securely - for example, using Azure Key Vault - and don't share them. We recommend regenerating your access keys regularly. You are provided two access keys so that you can maintain connections using one key while regenerating the other.

When you regenerate your access keys, you must update any Azure resources and applications that access this storage account to use the new keys. This action will not interrupt access to disks from your virtual machines. [Learn more](#)

Storage account name: a63cde60b553020

key1

Key: vScjFdvVZqIPyO/

Connection string: DefaultEndpoints

如果要在兩個 Azure Blob 容器之間同步數據，則连接字串必須包含 "共享存取簽名" (SAS)。您也可以選擇在 Blob 容器和 NFS 或 SMB 伺服器之間同步時使用 SAS。

SAS 必須允許存取 Blob 服務和所有資源類型（服務、容器和物件）。SAS 也必須包含以下權限：

- 對於來源 Blob 容器：讀取和列出
- 對於目標 Blob 容器：讀取、寫入、列出、新增和創建

Storage account: a63cde60b553020 - Shared access signature

Search (Ctrl+/)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Storage Explorer (preview)

Settings

Access keys

CORS

Configuration

Encryption

Shared access signature

Firewalls and virtual networks

Advanced Threat Protection (pr...

Properties

Locks

Allowed services ⓘ

☒ Blob ☐ File ☐ Queue ☐ Table

Allowed resource types ⓘ

☒ Service ☒ Container ☒ Object

Allowed permissions ⓘ

☒ Read ☒ Write ☒ Delete ☒ List ☒ Add ☒ Create ☐ Update ☐ Process

Start and expiry date/time ⓘ

Start

2018-10-23 10:07:32 AM

End

2019-10-23 6:07:32 PM

(UTC-04:00) --- Current Time Zone ---

Allowed IP addresses ⓘ

for example, 168.1.5.65 or 168.1.5.65-168.1.5.70

Allowed protocols ⓘ

☒ HTTPS only ☐ HTTPS and HTTP

Signing key ⓘ

key1

Generate SAS and connection string



如果您選擇實作包含 Azure Blob 容器的連續同步關係，則可以使用常規連接字串或 SAS 連接字串。如果使用 SAS 連接字串，則不得將其設定為在不久的將來過期。

Azure 資料湖儲存體 Gen2

建立包含 Azure Data Lake 的同步關係時，需要為複製和同步提供儲存帳戶連接字串。它必須是常規連接字串，而不是共用存取簽章（SAS）。

Azure NetApp Files需求

在與 Azure NetApp Files 同步資料時，請使用 Premium 或 Ultra 服務等級。如果磁碟服務等級為標準，您可能會遇到故障和效能問題。



如果您需要協助確定正確的服務級別，請諮詢解決方案架構師。卷大小和卷層決定了您可以獲得的吞吐量。

["詳細了解Azure NetApp Files服務等級與吞吐量"](#)。

盒子要求

- 要建立包含 Box 的同步關係，您需要提供以下憑證：
 - 客戶端 ID
 - 客戶端機密
 - 私鑰
 - 公鑰ID
 - 密碼
 - 企業 ID
- 如果您建立從 Amazon S3 到 Box 的同步關係，則必須使用具有統一配置的資料代理群組，其中下列設定設為 1：
 - 掃描器並發
 - 掃描器進程限制
 - 轉帳並發
 - 轉移者進程限制

["了解如何為資料代理組定義統一配置"](#)。

Google Cloud Storage 儲存桶需求

確保您的 Google Cloud Storage 儲存桶符合以下要求。

Google Cloud Storage 支援的資料代理位置

包含 Google Cloud Storage 的同步關係需要在 Google Cloud 或您的場所部署資料代理程式。當您建立同步關係時，複製和同步會引導您完成資料代理安裝程序。

- ["了解如何部署 Google Cloud 資料代理"](#)
- ["了解如何在 Linux 主機上安裝資料代理"](#)

支援的 Google Cloud 區域

支援所有地區。

其他 Google Cloud 專案中儲存桶的權限

設定同步關係時，如果您向資料代理程式的服務帳戶提供所需的權限，則可以從不同項目中的 Google Cloud 儲存桶中進行選擇。["了解如何設定服務帳戶"](#)。

SnapMirror目標的權限

如果同步關係的來源是SnapMirror目標（唯讀），則「讀取/列出」權限足以將資料從來源同步到目標。

加密 Google Cloud 儲存桶

您可以使用客戶管理的 KMS 金鑰或預設的 Google 管理金鑰加密目標 Google Cloud 儲存桶。如果儲存桶已新增了 KMS 加密，它將覆蓋預設的 Google 管理加密。

若要新增客戶管理的 KMS 金鑰，您需要使用具有 "正確的權限"，且 key 必須與 bucket 位於同一區域。

Google 雲端硬碟

當您設定包含 Google Drive 的同步關係時，您需要提供以下資訊：

- 有權存取您要同步資料的 Google Drive 位置的使用者的電子郵件地址
- 有權存取 Google Drive 的 Google Cloud 服務帳戶的電子郵件地址
- 服務帳戶的私鑰

若要設定服務帳戶，請依照 Google 文件中的說明進行操作：

- "[建立服務帳戶和憑證](#)"
- "[將網域範圍的權限委託給您的服務帳戶](#)"

編輯 OAuth 範圍欄位時，輸入以下範圍：

- \ <https://www.googleapis.com/auth/drive>
- \ <https://www.googleapis.com/auth/drive.file>

NFS 伺服器要求

- NFS 伺服器可以是NetApp系統，也可以是非NetApp系統。
- 文件伺服器必須允許資料代理主機透過所需連接埠存取匯出。
 - 111 TCP/UDP
 - 2049 TCP/UDP
 - 5555 TCP/UDP
- 支援 NFS 版本 3、4.0、4.1 和 4.2。

必須在伺服器上啟用所需的版本。

- 如果要從ONTAP系統同步 NFS 數據，請確保已啟用對 SVM 的 NFS 匯出清單的存取權（`vserver nfs modify -vserver svm_name -showmount enabled`）。



從ONTAP 9.2 開始，showmount 的預設設定為 *enabled*。

ONTAP 需求

如果同步關係包含 Cloud Volumes ONTAP 或本機 ONTAP 集群，並且您選擇了 NFSv4 或更高版本，則需要在 ONTAP 系統上啟用 NFSv4 ACL。這是複製 ACL 所必需的。

ONTAP S3 儲存需求

當你設定包含以下內容的同步關係時 **"ONTAP S3 存儲"**，您需要提供以下資訊：

- 連接到 ONTAP S3 的 LIF 的 IP 位址
- ONTAP 配置使用的存取金鑰和金鑰

SMB 伺服器要求

- SMB 伺服器可以是 NetApp 系統，也可以是非 NetApp 系統。
- 您需要向複製和同步提供在 SMB 伺服器上具有權限的憑證。
 - 對於來源 SMB 伺服器，需要以下權限：列出和讀取。
- 備份操作員群組的成員受到來源 SMB 伺服器的支援。
- 對於目標 SMB 伺服器，需要以下權限：列出、讀取和寫入。
- 文件伺服器必須允許資料代理主機透過所需連接埠存取匯出。
 - 139 TCP
 - 445 TCP
 - 137-138 UDP
- 支援 SMB 版本 1.0、2.0、2.1、3.0 和 3.11。
- 授予「管理員」群組對來源資料夾和目標資料夾的「完全控制」權限。

如果您不授予此權限，則資料代理程式可能沒有足夠的權限來取得檔案或目錄的 ACL。如果發生這種情況，您將收到以下錯誤：“getxattr 錯誤 95”

隱藏目錄和檔案的 SMB 限制

在 SMB 伺服器之間同步資料時，SMB 限制會影響隱藏目錄和檔案。如果來源 SMB 伺服器上的任何目錄或檔案透過 Windows 隱藏，則隱藏屬性不會複製到目標 SMB 伺服器。

由於不區分大小寫限制導致的 SMB 同步行為

SMB 協定不區分大小寫，這意味著大寫字母和小寫字母被視為相同。如果同步關係包括 SMB 伺服器且目標上已存在數據，則此行為可能導致檔案覆寫和目錄複製錯誤。

例如，假設來源上有一個名為“a”的文件，目標上有一個名為“A”的文件。當複製和同步將名為“a”的檔案複製到目標時，檔案“A”將被來源中的檔案“a”覆蓋。

對於目錄，假設來源上有一個名為「b」的目錄，目標上有一個名為「B」的目錄。當「複製和同步」嘗試將名為「b」的目錄複製到目標時，「複製和同步」會收到一條錯誤訊息，提示該目錄已存在。因此，複製和同步總是無法複製名為“b”的目錄。

避免此限制的最佳方法是確保將資料同步到空目錄。

NetApp Copy and Sync的網路概述

NetApp Copy and Sync的網路包括資料代理群組與來源位置和目標位置之間的連接，以及透過連接埠 443 來自資料代理程式的出站網路連接。

數據代理位置

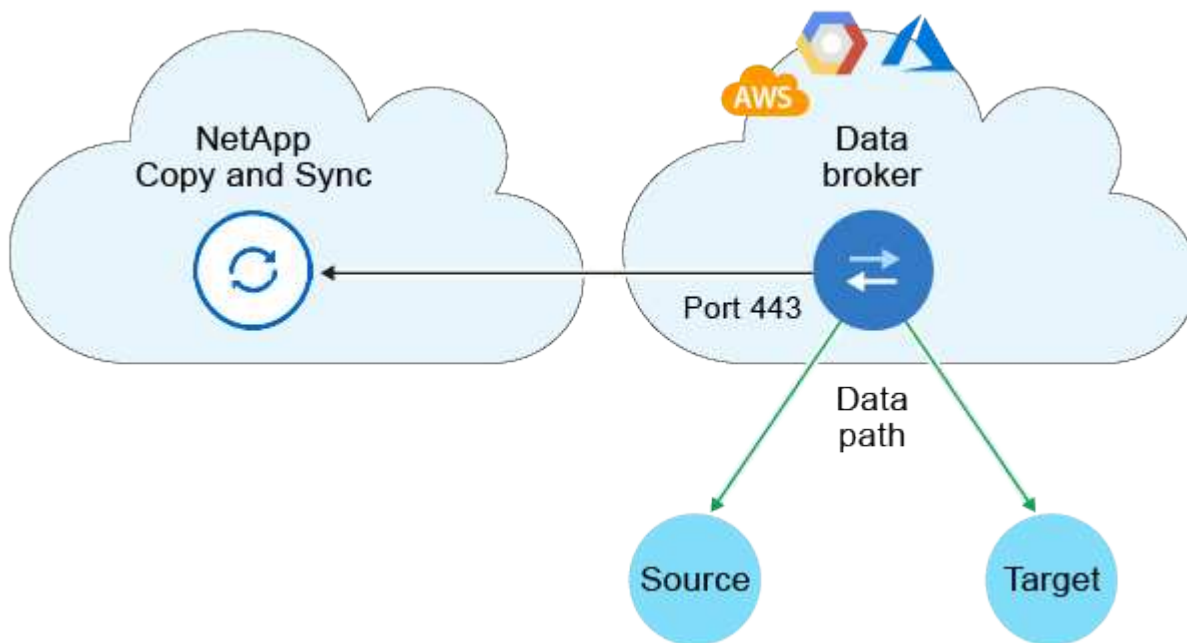
資料代理組由安裝在雲端或您的場所的一個或多個資料代理程式組成。

雲端數據代理

下圖顯示了在 AWS、Google Cloud 或 Azure 雲端中執行的資料代理程式。只要與資料代理有連接，來源和目標就可以位於任何位置。例如，您可能有一個從資料中心到雲端提供者的 VPN 連線。

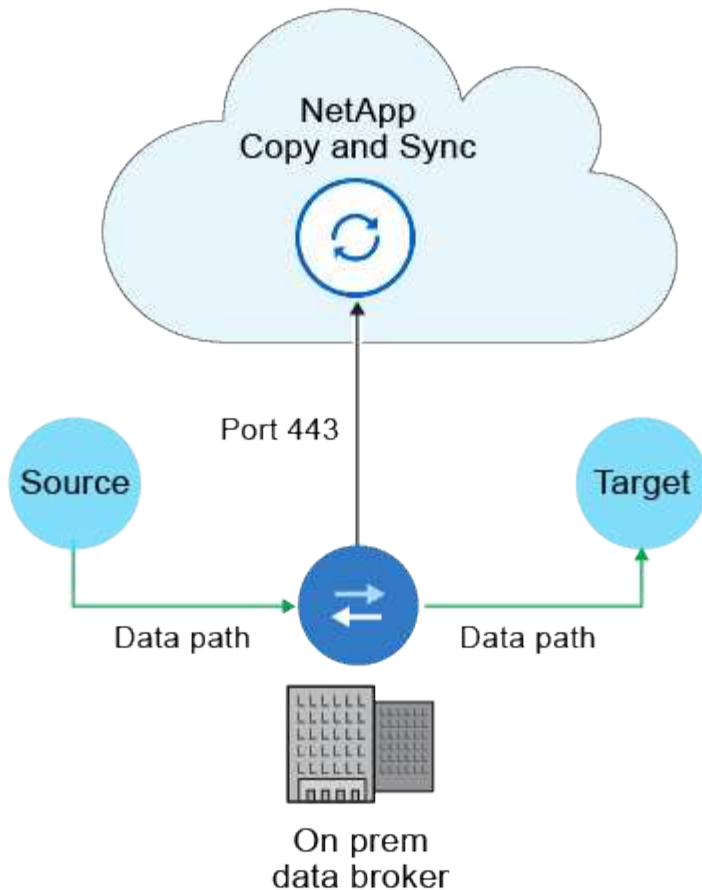


當 Copy and Sync 在 AWS、Azure 或 Google Cloud 中部署資料代理程式時，它會建立一個安全群組來啟用所需的出站通訊。



您所在地的數據代理

下圖顯示了在資料中心內部運行的資料代理程式。同樣，只要與資料代理有連接，來源和目標就可以位於任何位置。



網路需求

- 來源和目標必須與資料代理組有網路連線。

例如，如果 NFS 伺服器位於您的資料中心，而資料代理程式位於 AWS 中，那麼您需要從您的網路到 VPC 的網路連線（VPN 或 Direct Connect）。

- 資料代理需要出站互聯網連接，以便它可以透過連接埠 443 輪詢複製和同步任務。
- NetApp建議設定來源、目標和資料代理程式以使用網路時間協定 (NTP) 服務。三個組件之間的時間差不應超過5分鐘。

網路端點

NetApp資料代理程式需要透過連接埠 443 進行出站互聯網訪問，以便與 Copy 和 Sync 進行通信並聯繫其他一些服務和儲存庫。您的本機網頁瀏覽器也需要存取端點才能執行某些操作。如果您需要限制出站連接，請在為出站流量設定防火牆時參考下列端點清單。

數據代理端點

資料代理聯絡以下端點：

端點	目的
https://olcentgbl.trafficmanager.net	聯絡儲存庫以更新資料代理主機的 CentOS 軟體包。只有在您在 CentOS 主機上手動安裝資料代理程式時才會聯絡此端點。

端點	目的
\ https://rpm.nodesource.com \ https://registry.npmjs.org \ https://nodejs.org :	聯絡儲存庫以更新 Node.js、npm 和開發中使用的其他第三方套件。
\ https://tgz.pm2.io	存取用於更新 PM2 的儲存庫，PM2 是用於監控複製和同步的第三方套件。
\ https://sqs.us-east-1.amazonaws.com \ https://kinesis.us-east-1.amazonaws.com	聯絡複製和同步用於操作（排隊文件、註冊操作以及向資料代理傳遞更新）的 AWS 服務。
\ "請參閱 AWS 文件以取得 S3 端點清單"	當同步關係包含 S3 儲存桶時聯絡 Amazon S3。
\ https://s3.amazonaws.com/	當您從複製和同步下載資料代理程式日誌時，資料代理程式會壓縮其日誌目錄並將日誌上傳到 us-east-1 區域中預先定義的 S3 儲存桶。
\ https://storage.googleapis.com/	當同步關係使用 GCP 儲存桶時聯絡 Google Cloud。
https://storage-account.blob.core.windows.net如果使用 Azure Data Lake Gen2 ： https://storage-account.dfs.core.windows.net[]其中 storage-account 是使用者的來源儲存帳戶。	開啟到使用者 Azure 儲存帳戶位址的代理程式。
\ https://cf.cloudsync.netapp.com \ https://repo.cloudsync.netapp.com	聯繫複製和同步。
\ https://support.netapp.com	使用 BYOL 授權進行同步關係時聯絡NetApp支援。
https://fedoraproject.org	在安裝和更新期間在資料代理虛擬機器上安裝 7z。需要 7z 來將AutoSupport訊息傳送給NetApp技術支援。
\ https://sts.amazonaws.com \ https://sts.us-east-1.amazonaws.com	當資料代理部署在 AWS 中或部署在您的場所並提供 AWS 憑證時，請驗證 AWS 憑證。資料代理程式在部署、更新和重新啟動時聯絡此端點。
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com	當您使用分類來選擇新同步關係的來源檔案時，請聯絡NetApp Data Classification。
\ https://pubsub.googleapis.com	如果從 Google 儲存帳戶建立連續同步關係。

端點	目的
<pre>https://storage-account.queue.core.windows.net\ https://management.azure.com/subscriptions/ \${subscriptionId}/resourceGroups/\${resourceGroup}/providers/Microsoft.EventGrid/*</pre> 其中 <code>storage-account</code> 是使用者的來源儲存帳戶，<code>subscriptionid</code> 是來源訂閱 ID，<code>resourceGroup</code> 是來源資源組。	如果從 Azure 儲存體帳戶建立連續同步關係。

Web 瀏覽器端點

您的 Web 瀏覽器需要存取以下端點來下載日誌以進行故障排除：

logs.cloudsync.netapp.com:443

登入 NetApp Copy and Sync

使用 NetApp Console 登入 NetApp Copy and Sync。

若要登入控制台，您可以使用您的 NetApp 支援網站憑證，也可以使用您的電子郵件和密碼註冊 NetApp 雲端登入。 [了解有關登入的更多信息](#)。

NetApp Copy and Sync 使用身分存取管理來控制每個使用者對特定操作的存取權限。

必要的 **NetApp Console** 角色 組織管理員角色。 [了解 NetApp Console 存取角色](#)。

步驟

1. 開啟 Web 瀏覽器並前往 ["NetApp Console"](#)。

出現 NetApp Console 登入頁面。
2. 登入控制台。
3. 從控制台左側導覽中，選擇 ***移動性*>*複製和同步***。

安裝數據代理

在 **AWS** 中為 **NetApp Copy and Sync** 建立新的資料代理

為 NetApp Copy and Sync 建立新的資料代理程式群組時，請選擇 Amazon Web Services

在 VPC 中的新 EC2 執行個體上部署資料代理程式軟體。NetApp Copy and Sync將引導您完成安裝過程，但此頁面上重複了要求和步驟，以協助您為安裝準備工作。

您也可以選擇在雲端或本機的現有 Linux 主機上安裝資料代理程式。["了解更多"](#)。

支援的 AWS 區域

除中國地區外，所有地區均受支援。

Root權限

資料代理軟體在 Linux 主機上自動以 root 身分執行。以 root 身分運行是資料代理操作的必要條件。例如，掛載共享。

網路需求

- 資料代理需要出站互聯網連接，以便它可以透過連接埠 443 輪詢複製和同步任務。

當 Copy and Sync 在 AWS 中部署資料代理程式時，它會建立一個安全性群組來啟用所需的出站通訊。請注意，您可以在安裝過程中設定資料代理程式以使用代理伺服器。

如果需要限制出站連接，請參閱["資料代理聯繫的端點列表"](#)。

- NetApp建議設定來源、目標和資料代理程式以使用網路時間協定 (NTP) 服務。三個組件之間的時間差不應超過5分鐘。

在 AWS 中部署資料代理程式所需的權限

用於部署資料代理程式的 AWS 使用者帳戶必須具有下列權限：["NetApp提供的政策"](#)。

將您自己的 IAM 角色與 AWS 資料代理程式結合使用的要求

當 Copy and Sync 部署資料代理程式時，它會為資料代理程式實例建立一個 IAM 角色。如果您願意，您可以使用自己的 IAM 角色部署資料代理程式。如果您的組織有嚴格的安全策略，您可以使用此選項。

IAM 角色必須符合以下要求：

- 必須允許 EC2 服務作為受信任實體承擔 IAM 角色。
- ["此 JSON 檔案中定義的權限"](#)必須附加到 IAM 角色，以便資料代理可以正常運作。

請依照下列步驟在部署資料代理程式時指定 IAM 角色。

建立資料代理

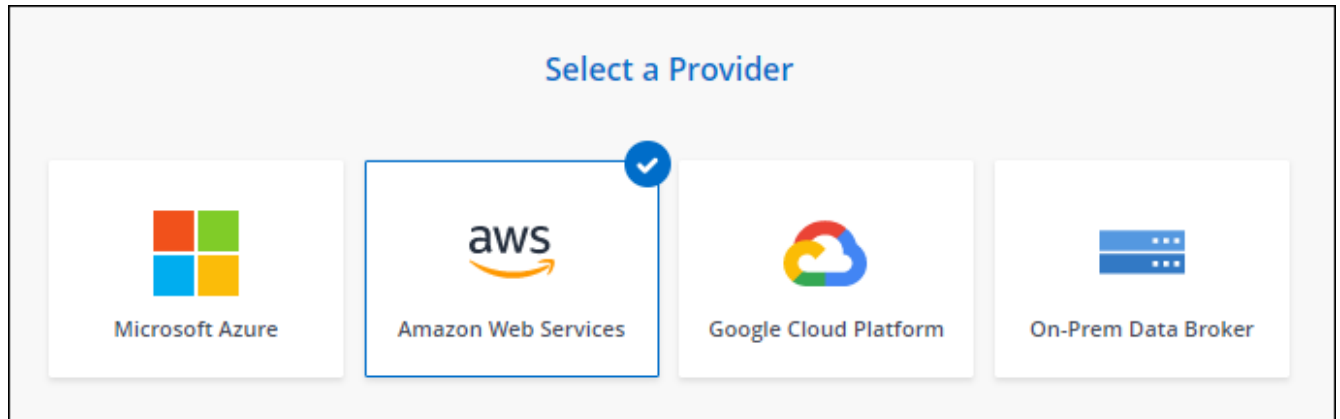
有幾種方法可以建立新的資料代理。這些步驟描述如何在建立同步關係時在 AWS 中安裝資料代理程式。

步驟

1. ["登入以複製和同步"](#)。
2. 選擇*建立新同步*。
3. 在*定義同步關係*頁面上，選擇來源和目標，然後選擇*繼續*。

完成這些步驟，直到到達*資料經紀人群組*頁面。

4. 在*資料代理組*頁面上，選擇*建立資料代理*，然後選擇*Amazon Web Services*。



5. 輸入資料代理的名稱並選擇*繼續*。
6. 輸入 AWS 存取金鑰，以便 Copy and Sync 可以代表您在 AWS 中建立資料代理程式。

密鑰不會被保存或用於任何其他目的。

如果您不想提供存取金鑰，請選擇頁面底部的連結以使用 CloudFormation 範本。當您使用此選項時，您不需要提供憑證，因為您直接登入 AWS。

以下影片展示如何使用 CloudFormation 範本啟動資料代理實例：

[從 AWS CloudFormation 範本啟動資料代理](#)

7. 如果您輸入了 AWS 存取金鑰，請選擇執行個體的位置、選擇金鑰對、選擇是否啟用公用 IP 位址並選擇現有的 IAM 角色，或將欄位留空，以便複製並同步為您建立角色。您也可以選擇使用 KMS 金鑰加密您的資料代理程式。

如果您選擇自己的 IAM 角色，[您需要提供所需的權限](#)。

Basic Settings

Location

VPC

Select VPC ▼

Subnet

Select Subnet ▼

Connectivity

Key Pair

Select Key Pair ▼

Enable Public IP?

☒ Enable ☐ Disable

IAM Role (optional)

IAM Role (optional) ⓘ

KMS Key for EBS volume (optional)

Select KMS Key for EBS Encryption ▼

8. 如果 VPC 中的網際網路存取需要代理，請指定代理設定。
9. 資料代理可用後，在複製和同步中選擇*繼續*。

下圖顯示了 AWS 中成功部署的執行個體：

✓ NFS Server
2 Data Broker Group
 3 Directories
 4 Target NFS Server
 >

Select a Data Broker Group

1 Data Broker Group 🔍

ben-data-broker ➔

1	N/A	0	✓ 1 Active
Data Brokers	Transfer Rate	Relationships	Data Brokers Status

10. 完成精靈中的頁面以建立新的同步關係。

結果

您已在 AWS 中部署了資料代理並建立了新的同步關係。您可以將此資料代理組與其他同步關係一起使用。

有關資料代理實例的詳細信息

複製和同步使用下列配置在 AWS 中建立資料代理程式。

Node.js 相容性

v21.2.0

實例類型

如果該區域可用，則使用 m5n.xlarge，否則使用 m5.xlarge

虛擬 CPU

4

記憶體

16GB

作業系統

亞馬遜Linux 2023

磁碟大小和類型

10 GB GP2 固態硬碟

在 **Azure** 中為**NetApp Copy and Sync**建立新的資料代理

為NetApp Copy and Sync建立新的資料代理程式群組時，請選擇 Microsoft Azure 在 VNet 中的新虛擬機器上部署資料代理程式軟體。NetApp Copy and Sync將引導您完成安裝過程，但此頁面上重複了要求和步驟，以協助您為安裝準備工作。

您也可以選擇在雲端或本機的現有 Linux 主機上安裝資料代理程式。["了解更多"](#)。

支援的 **Azure** 區域

除中國、美國政府和美國國防部地區外，所有地區均受支持。

Root權限

資料代理軟體在 Linux 主機上自動以 root 身分執行。以 root 身分運行是資料代理操作的必要條件。例如，掛載共享。

網路需求

- 資料代理需要出站互聯網連接，以便它可以透過連接埠 443 輪詢複製和同步服務的任務。

當 Copy and Sync 在 Azure 中部署資料代理程式時，它會建立一個安全性群組來啟用所需的出站通訊。

如果需要限制出站連接，請參閱["資料代理聯繫的端點列表"](#)。

- NetApp建議設定來源、目標和資料代理程式以使用網路時間協定 (NTP) 服務。三個組件之間的時間差不應超過5分鐘。

在 **Azure** 中部署資料代理程式所需的權限

確保用於部署資料代理程式的 Azure 使用者帳戶具有以下權限：

```
{
  "Name": "Azure Data Broker",
  "Actions": [
    "Microsoft.Resources/subscriptions/read",

    "Microsoft.Resources/deployments/operationstatuses/read",
    "Microsoft.Resources/subscriptions/locations/read",
    "Microsoft.Network/networkInterfaces/read",
    "Microsoft.Network/virtualNetworks/subnets/read",

    "Microsoft.Resources/subscriptions/resourceGroups/write",

    "Microsoft.Resources/subscriptions/resourceGroups/delete",
    "Microsoft.Resources/deployments/write",
    "Microsoft.Resources/deployments/validate/action",

    "Microsoft.Resources/deployments/operationStatuses/read",
    "Microsoft.Resources/deployments/cancel/action",
    "Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Compute/disks/delete",
    "Microsoft.Network/networkInterfaces/delete",
    "Microsoft.Network/publicIPAddresses/delete",

    "Microsoft.Network/networkSecurityGroups/securityRules/delete",

    "Microsoft.Resources/subscriptions/resourceGroups/write",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Network/networkSecurityGroups/write",
    "Microsoft.Network/networkSecurityGroups/join/action",
    "Microsoft.Compute/disks/write",
    "Microsoft.Network/networkInterfaces/write",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Network/publicIPAddresses/write",
    "Microsoft.Compute/virtualMachines/write",
    "Microsoft.Compute/virtualMachines/extensions/write",
    "Microsoft.Resources/deployments/read",
    "Microsoft.Network/networkSecurityGroups/read",
    "Microsoft.Network/publicIPAddresses/read",

    "Microsoft.Network/virtualNetworks/subnets/join/action",
    "Microsoft.Network/publicIPAddresses/join/action",
```

```

        "Microsoft.Network/networkInterfaces/join/action",
        "Microsoft.Storage/storageAccounts/read",

"Microsoft.EventGrid/systemTopics/eventSubscriptions/write",

"Microsoft.EventGrid/systemTopics/eventSubscriptions/read",

"Microsoft.EventGrid/systemTopics/eventSubscriptions/delete",

"Microsoft.EventGrid/systemTopics/eventSubscriptions/getFullUrl/action",

"Microsoft.EventGrid/systemTopics/eventSubscriptions/getDeliveryAttributes
/action",
        "Microsoft.EventGrid/systemTopics/read",
        "Microsoft.EventGrid/systemTopics/write",
        "Microsoft.EventGrid/systemTopics/delete",
        "Microsoft.EventGrid/eventSubscriptions/write",
        "Microsoft.Storage/storageAccounts/write"

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/read"

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/write"

"Microsoft.Network/networkSecurityGroups/securityRules/read",
        "Microsoft.Network/networkSecurityGroups/read",

```

```

    ],
    "NotActions": [],
    "AssignableScopes": [],
    "Description": "Azure Data Broker",
    "IsCustom": "true"
}

```

筆記：

1. 僅當您計劃啟用 ["連續同步設定"](#)從 Azure 到另一個雲端儲存位置的同步關係：
 - "Microsoft.Storage/storageAccounts/read"，
 - "Microsoft.EventGrid/systemTopics/eventSubscriptions/write"，
 - "Microsoft.EventGrid/systemTopics/eventSubscriptions/read"，
 - 'Microsoft.EventGrid/systemTopics/eventSubscriptions/delete'，

- 'Microsoft.EventGrid/systemTopics/eventSubscriptions/getFullUrl/action' ,
- “Microsoft.EventGrid/systemTopics/eventSubscriptions/getDeliveryAttributes/action” ,
- “Microsoft.EventGrid/systemTopics/讀取” ,
- “Microsoft.EventGrid/systemTopics/write” ,
- “Microsoft.EventGrid/systemTopics/刪除” ,
- “Microsoft.EventGrid/eventSubscriptions/write” ,
- “Microsoft.Storage/storageAccounts/write”

此外，如果您打算在 Azure 中實現連續同步，則必須將可指派範圍設定為訂閱範圍而不是資源組範圍。

2. 只有當您計劃為資料代理程式建立選擇自己的安全性時才需要以下權限：

- “Microsoft.Network/networkSecurityGroups/securityRules/讀取”
- “Microsoft.Network/networkSecurityGroups/讀取”

身份驗證方法

部署資料代理程式時，您需要為虛擬機器選擇一種身份驗證方法：密碼或 SSH 公鑰-私鑰對。

有關建立金鑰對的協助，請參閱 ["Azure 文件：在 Azure 中為 Linux VM 建立並使用 SSH 公鑰-私鑰對"](#)。

建立資料代理

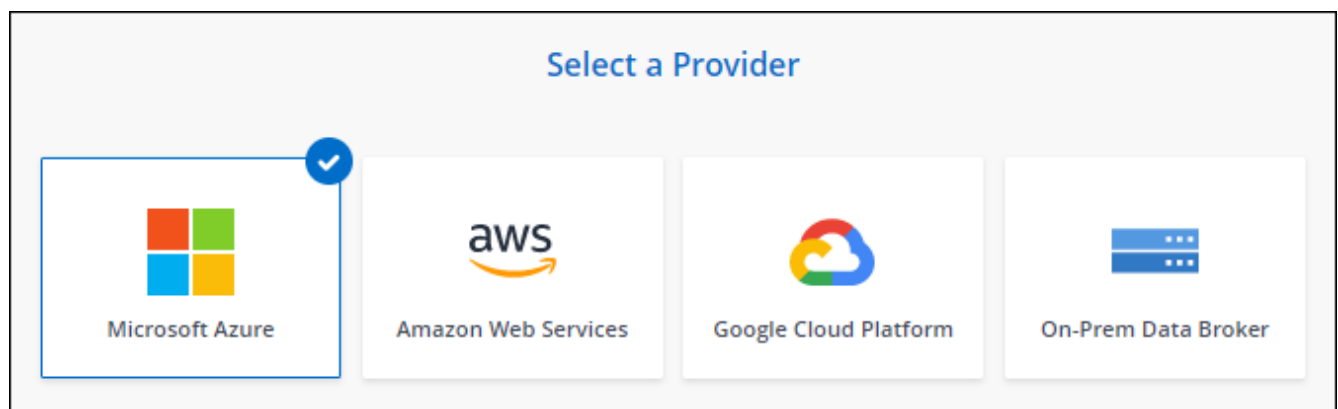
有幾種方法可以建立新的資料代理。這些步驟描述了在建立同步關係時如何在 Azure 中安裝資料代理程式。

步驟

1. ["登入以複製和同步"](#) 。
2. 選擇*建立新同步*。
3. 在*定義同步關係*頁面上，選擇來源和目標，然後選擇*繼續*。

完成這些步驟，直到到達*資料經紀人群組*頁面。

4. 在“資料代理程式群組”頁面上，選擇“建立資料代理程式”，然後選擇“Microsoft Azure”。



5. 輸入資料代理的名稱並選擇*繼續*。

6. 如果出現提示，請登入您的 Microsoft 帳戶。如果沒有提示，請選擇「登入 Azure」。

該表單由 Microsoft 擁有並託管。您的憑證未提供給 NetApp。

7. 選擇資料代理的位置並輸入有關虛擬機器的基本詳細資訊。



如果您打算實現持續同步關係，則必須為資料代理程式指派自訂角色。這也可以在建立代理後手動完成。

8. 如果 VNet 中的 Internet 存取需要代理，請指定代理設定。

9. 選擇*繼續*。如果您想要為資料代理程式新增 S3 權限，請輸入您的 AWS 存取和金鑰。

10. 選擇*繼續*並保持頁面打開，直到部署完成。

該過程可能需要長達 7 分鐘。

11. 在複製和同步中，一旦資料代理可用，請選擇*繼續*。

12. 完成精靈中的頁面以建立新的同步關係。

結果

您已在 Azure 中部署了資料代理程式並建立了新的同步關係。您可以將此資料代理與其他同步關係一起使用。

收到需要管理員同意的訊息嗎？

如果 Microsoft 通知您需要管理員批准，因為複製和同步需要代表您存取組織中的資源的權限，那麼您有兩個選擇：

1. 請您的 AD 管理員為您提供以下權限：

在 Azure 中，前往 管理中心 > **Azure AD** > 使用者和群組 > 使用者設定 並啟用 使用者可以同意應用程式代表他們存取公司資料。

2. 請求您的 AD 管理員代表您同意使用下列 URL（這是管理員同意端點） **CloudSync-AzureDataBrokerCreator**：

\ [https://login.microsoftonline.com/ {在此填寫您的租戶 ID}/v2.0/adminconsent?client_id=8ee4ca3a-bafa-4831-97cc-5a38923cab85&redirect_uri= https://cloudsync.netapp.com&scope=https://management.azure.com/user_impersonationhttps://graph.microsoft.com/User.Read](https://login.microsoftonline.com/{在此填寫您的租戶 ID}/v2.0/adminconsent?client_id=8ee4ca3a-bafa-4831-97cc-5a38923cab85&redirect_uri=https://cloudsync.netapp.com&scope=https://management.azure.com/user_impersonationhttps://graph.microsoft.com/User.Read)

如URL所示，我們的應用程式URL是\ <https://cloudsync.netapp.com>，應用程式用戶端ID是8ee4ca3a-bafa-4831-97cc-5a38923cab85。

有關數據代理虛擬機的詳細信息

複製和同步使用以下配置在 Azure 中建立資料代理程式。

Node.js 相容性

v21.2.0

VM 類型

標準 DS4 v2

虛擬 CPU

8

記憶體

28GB

作業系統

Rocky Linux 9.0

磁碟大小和類型

64 GB 高級固態硬碟

在 Google Cloud 中為NetApp Copy and Sync建立新的資料代理

為NetApp Copy and Sync建立新的資料代理群組時，請選擇 Google Cloud Platform 在 Google Cloud VPC 中的新虛擬機器實例上部署資料代理軟體。 NetApp Copy and Sync將引導您完成安裝過程，但此頁面上重複了要求和步驟，以協助您為安裝準備工作。

您也可以選擇在雲端或本機的現有 Linux 主機上安裝資料代理程式。["了解更多"](#)。

支援的 Google Cloud 區域

支援所有地區。

Root 權限

資料代理軟體在 Linux 主機上自動以 root 身分執行。以 root 身分運行是資料代理操作的必要條件。例如，掛載共享。

網路需求

- 資料代理需要出站互聯網連接，以便它可以透過連接埠 443 輪詢複製和同步任務。

當 Copy and Sync 在 Google Cloud 中部署資料代理程式時，它會建立一個安全性群組來啟用所需的出站通訊。

如果需要限制出站連接，請參閱["資料代理聯繫的端點列表"](#)。

- NetApp 建議設定來源、目標和資料代理程式以使用網路時間協定 (NTP) 服務。三個組件之間的時間差不應超過 5 分鐘。

在 Google Cloud 中部署資料代理程式所需的權限

確保部署資料代理程式的 Google Cloud 使用者俱有以下權限：

```
- compute.networks.list
- compute.regions.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.operations.get
- iam.serviceAccounts.list
```

服務帳戶所需的權限

部署資料代理程式時，您需要選擇具有下列權限的服務帳戶：

```
- logging.logEntries.create
- resourceManager.projects.get
- storage.buckets.get
- storage.buckets.list
- storage.objects.create
- storage.objects.delete
- storage.objects.get
- storage.objects.getIamPolicy
- storage.objects.list
- storage.objects.setIamPolicy
- storage.objects.update
- iam.serviceAccounts.signJwt
- pubsub.subscriptions.consume
- pubsub.subscriptions.create
- pubsub.subscriptions.delete
- pubsub.subscriptions.list
- pubsub.topics.attachSubscription
- pubsub.topics.create
- pubsub.topics.delete
- pubsub.topics.list
- pubsub.topics.setIamPolicy
- storage.buckets.update
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
```

筆記：

1. 僅當您計劃設定資料代理程式以使用外部 HashiCorp 保險庫時才需要「iam.serviceAccounts.signJwt」權限。
2. 只有當您計劃在從 Google Cloud Storage 到另一個雲端儲存位置的同步關係上啟用連續同步設定時，才需要「pubsub.*」和「storage.buckets.update」權限。["了解有關持續同步選項的更多信息"](#)。
3. 只有當您計劃在目標 Google Cloud Storage 儲存桶上使用客戶管理的 KMS 金鑰時，才需要「cloudkms.cryptoKeys.list」和「cloudkms.keyRings.list」權限。

建立資料代理

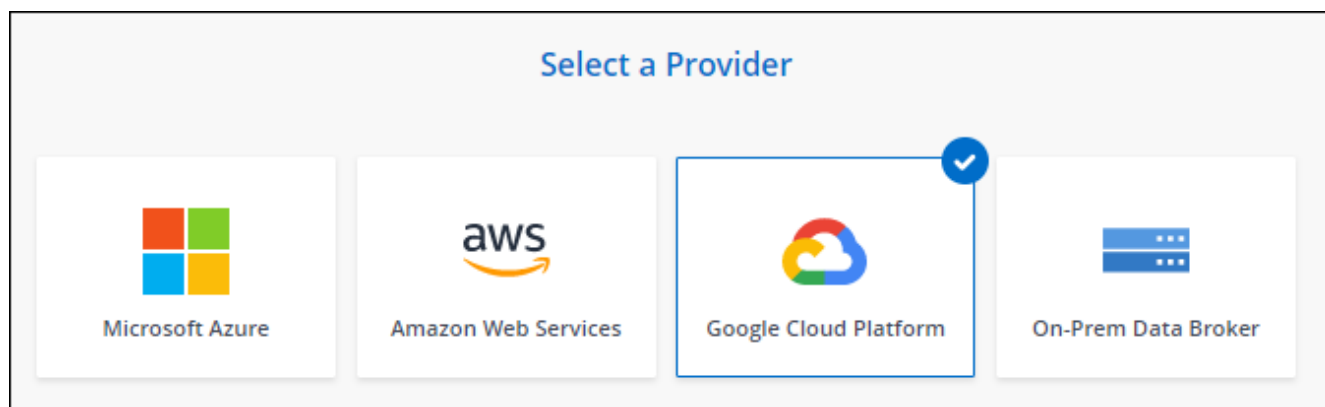
有幾種方法可以建立新的資料代理。以下步驟描述了在建立同步關係時如何在 Google Cloud 中安裝資料代理程式。

步驟

1. ["登入以複製和同步"](#)。
2. 選擇*建立新同步*。
3. 在*定義同步關係*頁面上，選擇來源和目標，然後選擇*繼續*。

完成這些步驟，直到到達*資料經紀人群組*頁面。

4. 在*資料經紀人群組*頁面上，選擇*建立資料經紀人*，然後選擇*Google Cloud Platform*。



5. 輸入資料代理的名稱並選擇*繼續*。
6. 如果出現提示，請使用您的 Google 帳號登入。

該表單由 Google 擁有並託管。您的憑證未提供給NetApp。

7. 選擇一個項目和服務帳戶，然後選擇資料代理的位置，包括是否要啟用或停用公用 IP 位址。

如果您沒有啟用公用 IP 位址，那麼您需要在下一個步驟中定義代理伺服器。

The screenshot shows a 'Basic Settings' form with two columns. The left column is titled 'Project' and contains three sections: 'Project' with a dropdown menu showing 'OCCM-Dev', 'Service Account' with a dropdown menu showing 'test', and a text prompt 'Select a Service Account that includes these permissions' with a link. The right column is titled 'Location' and contains four sections: 'Region' with a dropdown menu showing 'us-west1', 'Zone' with a dropdown menu showing 'us-west1-a', 'VPC' with a dropdown menu showing 'default', and 'Public IP' with a dropdown menu showing 'Enable'.

8. 如果 VPC 中的網際網路存取需要代理，請指定代理設定。

如果需要代理程式才能存取互聯網，則代理必須位於 Google Cloud 中並使用與資料代理相同的服務帳戶。

9. 一旦資料代理可用，請在複製和同步中選擇*繼續*。

該實例大約需要 5 到 10 分鐘才能部署。您可以從複製和同步中監控進度，當實例可用時會自動刷新。

10. 完成精靈中的頁面以建立新的同步關係。

結果

您已在 Google Cloud 中部署了資料代理並建立了新的同步關係。您可以將此資料代理與其他同步關係一起使用。

提供在其他 Google Cloud 專案中使用儲存桶的權限

當您建立同步關係並選擇 Google Cloud Storage 作為來源或目標時，複製和同步可讓您從資料代理程式的服務帳戶有權使用的儲存桶中進行選擇。預設情況下，這包括與資料代理服務帳戶位於相同專案中的儲存桶。但是如果您提供所需的權限，您可以從其他項目中選擇儲存桶。

步驟

1. 開啟 Google Cloud Platform 控制台並載入 Cloud Storage 服務。
2. 選擇您想要用作同步關係中的來源或目標的儲存桶的名稱。
3. 選擇*權限*。
4. 選擇“新增”。
5. 輸入資料代理的服務帳戶的名稱。
6. 選擇提供以下功能的角色與上面顯示的權限相同。
7. 選擇*儲存*。

結果

當您設定同步關係時，現在可以選擇該儲存桶作為同步關係中的來源或目標。

有關資料代理虛擬機器實例的詳細信息

複製和同步使用以下配置在 Google Cloud 中建立資料代理程式。

Node.js 相容性

v21.2.0

機器類型

n2-標準-4

虛擬 CPU

4

記憶體

15GB

作業系統

Rocky Linux 9.0

磁碟大小和類型

20 GB 硬碟 pd-標準

在 Linux 主機上安裝用於NetApp Copy and Sync的資料代理

為NetApp Copy and Sync建立新的資料代理群組時，請選擇 On-Prem Data Broker 選項在本機 Linux 主機或雲端中的現有 Linux 主機上安裝資料代理軟體。NetApp Copy and Sync 將引導您完成安裝過程，但此頁面上重複了要求和步驟，以協助您為安裝準備工作。

Linux 主機需求

- Node.js 相容性：v21.2.0
- 作業系統:
 - CentOS 8.0 和 8.5
 - CentOS Stream 不受支援。
 - Red Hat Enterprise Linux 8.5、8.8、8.9 與 9.4
 - Rocky Linux 9
 - Ubuntu Server 20.04 LTS、23.04 LTS 和 24.04 LTS
 - SUSE Linux Enterprise Server 15 SP1

命令 `yum update` 在安裝資料代理之前必須在主機上執行。

Red Hat Enterprise Linux 系統必須在 Red Hat 訂閱管理中註冊。如果未註冊，系統將無法存取儲存庫來在安裝期間更新所需的第三方軟體。

- 記憶體：16 GB
- **CPU**：4核心
- 可用磁碟空間：10 GB
- **SELinux**：我們建議您在主機上停用 SELinux。

SELinux 強制執行阻止資料代理軟體更新的策略，並且可以阻止資料代理程式聯繫正常運作所需的端點。

Root權限

資料代理軟體在 Linux 主機上自動以 root 身分執行。以 root 身分運行是資料代理操作的必要條件。例如，掛載共享。

網路需求

- Linux 主機必須與來源和目標建立連線。

- 檔案伺服器必須允許 Linux 主機存取導出。
- Linux 主機上必須開啟連接埠 443 才能向 AWS 發送出站流量（資料代理程式不斷與 Amazon SQS 服務通訊）。
- NetApp建議設定來源、目標和資料代理程式以使用網路時間協定 (NTP) 服務。三個組件之間的時間差不應超過5分鐘。

啟用對 **AWS** 的訪問

如果您打算使用包含 S3 儲存桶的同步關係的資料代理，那麼您應該準備好 Linux 主機以供 AWS 存取。安裝資料代理程式時，您需要為具有程式存取權限和特定權限的 AWS 使用者提供 AWS 金鑰。

步驟

1. 使用建立 IAM 策略 ["NetApp提供的政策"](#)

["查看 AWS 說明"](#)

2. 建立具有編程存取權限的 IAM 使用者。

["查看 AWS 說明"](#)

請務必複製 AWS 金鑰，因為您需要在安裝資料代理軟體時指定它們。

啟用對 **Google Cloud** 的訪問

如果您打算使用包含 Google Cloud Storage 儲存桶的同步關係的資料代理，那麼您應該準備 Linux 主機以供 Google Cloud 存取。安裝資料代理程式時，您需要為具有特定權限的服務帳戶提供金鑰。

步驟

1. 如果您還沒有 Google Cloud 服務帳戶，請建立一個具有儲存管理員權限的 Google Cloud 服務帳戶。
2. 建立以 JSON 格式儲存的服務帳戶金鑰。

["查看 Google Cloud 說明"](#)

該檔案至少應包含以下屬性："project_id"、"private_key"和"client_email"



當您建立金鑰時，檔案就會產生並下載到您的機器上。

3. 將 JSON 檔案儲存到 Linux 主機。

啟用對 **Microsoft Azure** 的訪問

透過在同步關係精靈中提供儲存帳戶和連接字串來定義每個關係對 Azure 的存取。

安裝數據代理

建立同步關係時，您可以在 Linux 主機上安裝資料代理程式。

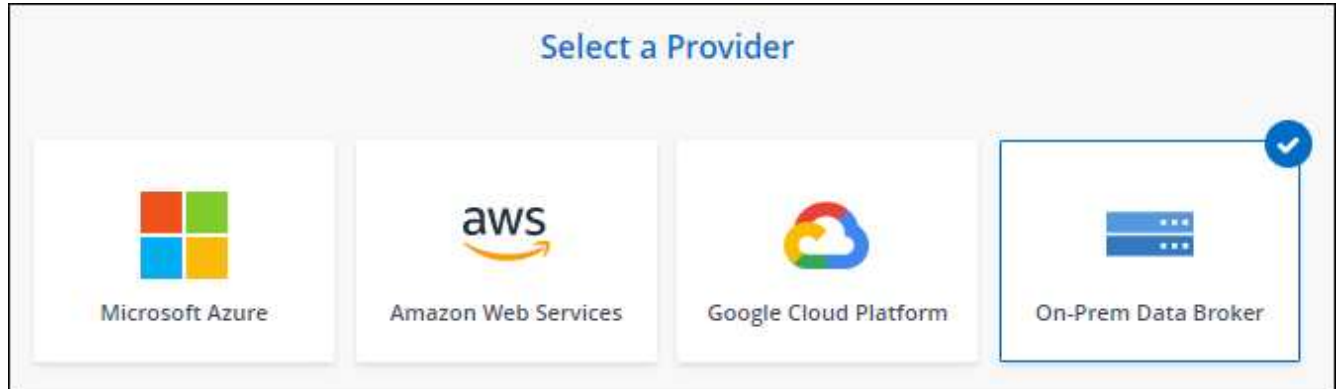
步驟

1. ["登入以複製和同步"](#)。

2. 選擇*建立新同步*。
3. 在*定義同步關係*頁面上，選擇來源和目標，然後選擇*繼續*。

完成這些步驟，直到到達*資料經紀人群組*頁面。

4. 在*資料代理群組*頁面上，選擇*建立資料代理*，然後選擇*本機資料代理*。



儘管該選項標記為 **On-Prem Data Broker**，但它適用於您所在地或雲端中的 Linux 主機。

5. 輸入資料代理的名稱並選擇*繼續*。

說明頁面很快就會載入。您需要遵循這些說明 - 它們包含下載安裝程式的唯一連結。

6. 在說明頁面上：
 - a. 選擇是否啟用對 **AWS**、**Google Cloud** 或兩者的存取。
 - b. 選擇安裝選項：無代理、使用代理伺服器*或*使用具有驗證的代理伺服器。



該用戶必須是本機用戶。不支援網域用戶。

- c. 使用命令下載並安裝資料代理程式。

以下步驟提供了有關每個可能的安裝選項的詳細資訊。按照說明頁面根據您的安裝選項取得準確的命令。

- d. 下載安裝程式：

- 無代理：

```
curl <URI> -o data_broker_installer.sh
```

- 使用代理伺服器：

```
curl <URI> -o data_broker_installer.sh -x <proxy_host>:<proxy_port>
```

- 使用帶有身份驗證的代理伺服器：

```
curl <URI> -o data_broker_installer.sh -x  
<proxy_username>:<proxy_password>@<proxy_host>:<proxy_port>
```

URI

複製和同步會在說明頁面上顯示安裝檔案的 URI，當您依照指示部署 On-Prem 資料代理程式時，該 URI 會載入。該 URI 不會在此重複，因為連結是動態產生的並且只能使用一次。[請依照以下步驟從複製和同步中取得 URI](#)。

e. 切換到超級用戶，使安裝程式可執行並安裝軟體：



下面列出的每個命令都包含 AWS 存取和 Google Cloud 存取的參數。按照說明頁面根據您的安裝選項取得準確的命令。

▪ 無代理配置：

```
sudo -s
chmod +x data_broker_installer.sh
./data_broker_installer.sh -a <aws_access_key> -s <aws_secret_key> -g
<absolute_path_to_the_json_file>
```

▪ 代理配置：

```
sudo -s
chmod +x data_broker_installer.sh
./data_broker_installer.sh -a <aws_access_key> -s <aws_secret_key> -g
<absolute_path_to_the_json_file> -h <proxy_host> -p <proxy_port>
```

▪ 帶有身份驗證的代理配置：

```
sudo -s
chmod +x data_broker_installer.sh
./data_broker_installer.sh -a <aws_access_key> -s <aws_secret_key> -g
<absolute_path_to_the_json_file> -h <proxy_host> -p <proxy_port> -u
<proxy_username> -w <proxy_password>
```

AWS 金鑰

這些是您應該為使用者準備的密鑰[請依照以下步驟](#)。AWS 金鑰儲存在資料代理程式上，該代理程式在您的本機或雲端網路中執行。NetApp 不使用資料代理程式以外的金鑰。

JSON 文件

這是包含您應該準備好的服務帳戶金鑰的 JSON 文件[請依照以下步驟](#)。

7. 一旦資料代理可用，請在複製和同步中選擇*繼續*。
8. 完成精靈中的頁面以建立新的同步關係。

使用NetApp Copy and Sync

在來源和目標之間同步數據

準備資料代理以在NetApp Copy and Sync中的物件儲存之間同步數據

如果您打算在NetApp Copy and Sync中將資料從物件儲存同步到物件儲存（例如，從 Amazon S3 同步到 Azure Blob），則需要在建立同步關係之前準備資料代理程式群組。

關於此任務

為了準備資料代理組，您需要修改掃描器的配置。如果不修改配置，您可能會注意到此同步關係的效能問題。

開始之前

用於將資料從物件儲存同步到物件儲存的資料代理群組應該只管理這些類型的同步關係。如果資料代理組管理不同類型的同步關係（例如，NFS 到 NFS 或物件儲存到 SMB），則這些同步關係的效能可能會受到負面影響。

步驟

1. ["登入以複製和同步"](#)。
2. 從複製和同步中，選擇*管理資料代理*。
3. 選擇 
4. 更新掃描器配置：
 - a. 將*掃描器並發性*更改為*1*。
 - b. 將*掃描器進程限制*變更為*1*。
5. 選擇*統一配置*。

結果

複製和同步更新資料代理組的配置。

下一步是什麼？

現在您可以使用剛剛配置的資料代理程式組建立物件儲存之間的同步關係。

在NetApp Copy and Sync中建立同步關係

當您建立同步關係時，NetApp Copy and Sync會將檔案從來源複製到目標。初始複製後，複製和同步每 24 小時同步一次任何更改的資料。

在建立某些類型的同步關係之前，您首先需要在NetApp Console中建立一個系統。

為特定類型的系統建立同步關係

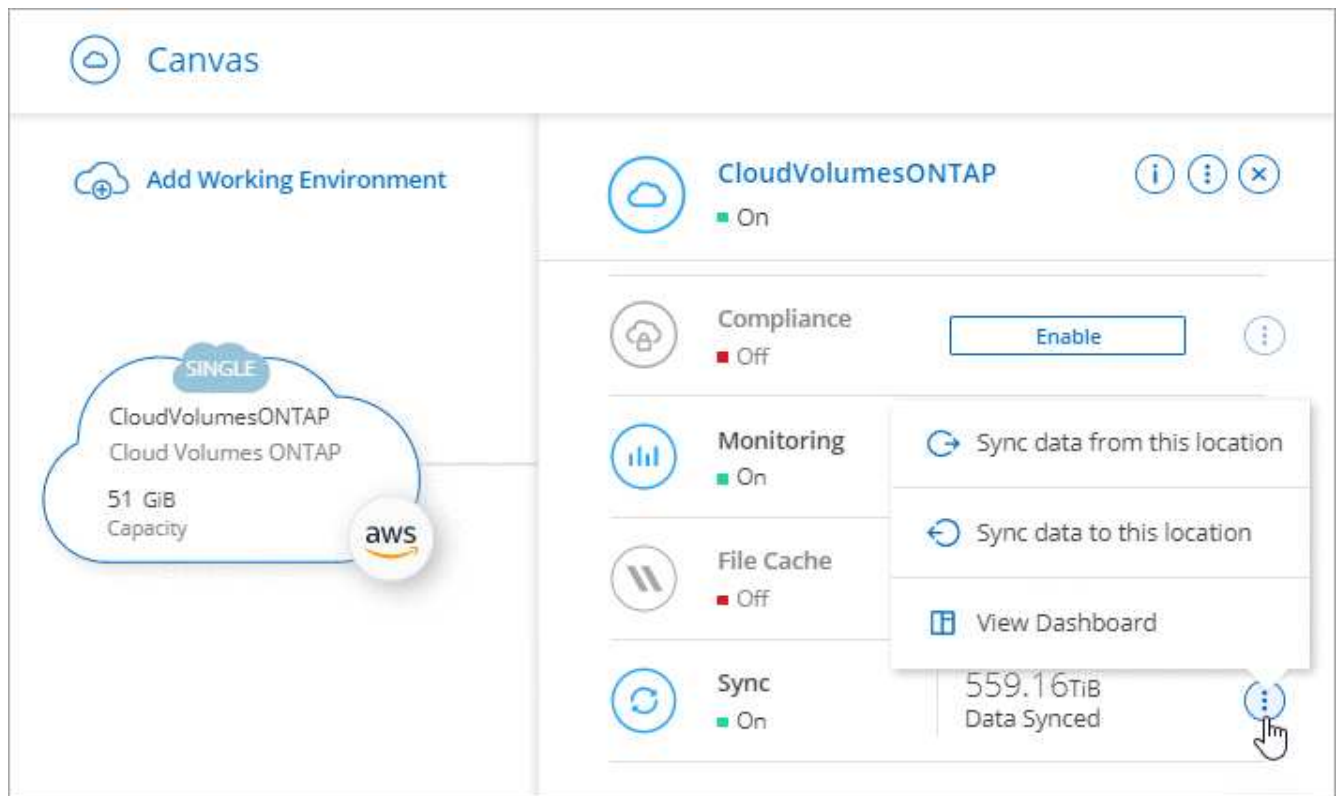
如果您想要為以下任何一項建立同步關係，那麼您首先需要建立或發現系統：

- 適用於ONTAP 的Amazon FSx

- Azure NetApp Files
- Cloud Volumes ONTAP
- 本地ONTAP集群

步驟

1. "登入以複製和同步"。
2. 創建或發現系統。
 - "建立Amazon FSx for ONTAP系統"
 - "設定和發現Azure NetApp Files"
 - "在 AWS 中啟動Cloud Volumes ONTAP"
 - "在 Azure 中啟動Cloud Volumes ONTAP"
 - "在 Google Cloud 啟動Cloud Volumes ONTAP"
 - "新增現有的Cloud Volumes ONTAP系統"
 - "發現ONTAP集群"
3. 選擇*系統頁面*。
4. 選擇與上面列出的任何類型相符的系統。
5. 選擇同步旁邊的操作選單。



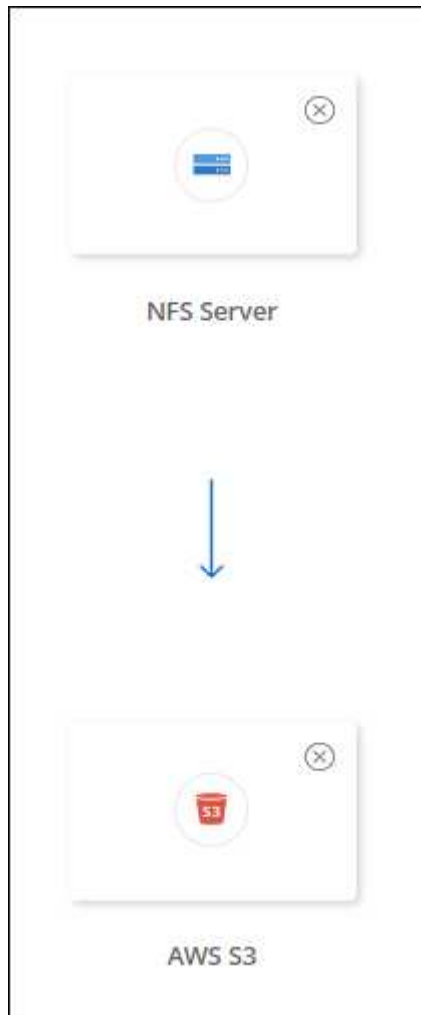
6. 選擇*從此位置同步資料*或*同步資料到此位置*，然後依照指示設定同步關係。

建立其他類型的同步關係

使用這些步驟將資料同步至或同步自除Amazon FSx for ONTAP、 Azure NetApp Files、 Cloud Volumes ONTAP或本機ONTAP叢集之外的支援的儲存類型。以下步驟提供了一個範例，展示如何設定從 NFS 伺服器到 S3 儲存桶的同步關係。

1. 在NetApp Console中，選擇 同步。
2. 在*定義同步關係*頁面上，選擇來源和目標。

以下步驟提供如何建立從 NFS 伺服器到 S3 儲存桶的同步關係的範例。



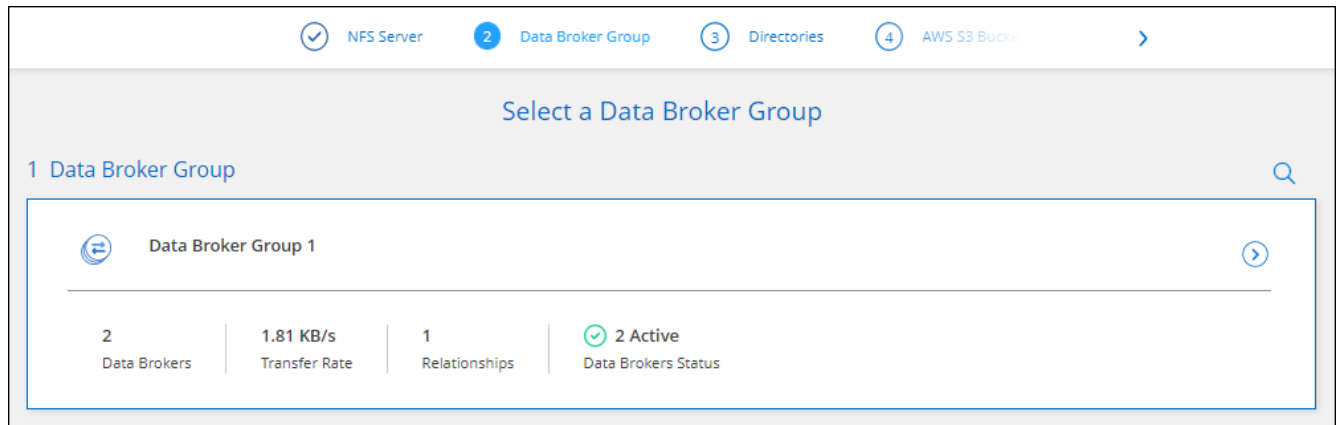
3. 在 **NFS** 伺服器 頁面上，輸入要同步到 AWS 的 NFS 伺服器的 IP 位址或完全限定網域名稱。
4. 在*資料代理群組*頁面上，依照指示在 AWS、Azure 或 Google Cloud Platform 中建立資料代理虛擬機，或在現有的 Linux 主機上安裝資料代理軟體。

欲了解更多詳情，請參閱以下頁面：

- ["在 AWS 中建立資料代理"](#)
- ["在 Azure 中建立資料代理"](#)
- ["在 Google Cloud 中建立資料代理"](#)

◦ "在 Linux 主機上安裝資料代理"

5. 安裝資料代理程式後，選擇*繼續*。



6. 在*目錄*頁面上，選擇頂級目錄或子目錄。

如果複製和同步無法擷取匯出，請選擇*手動新增導出*並輸入 NFS 導出的名稱。



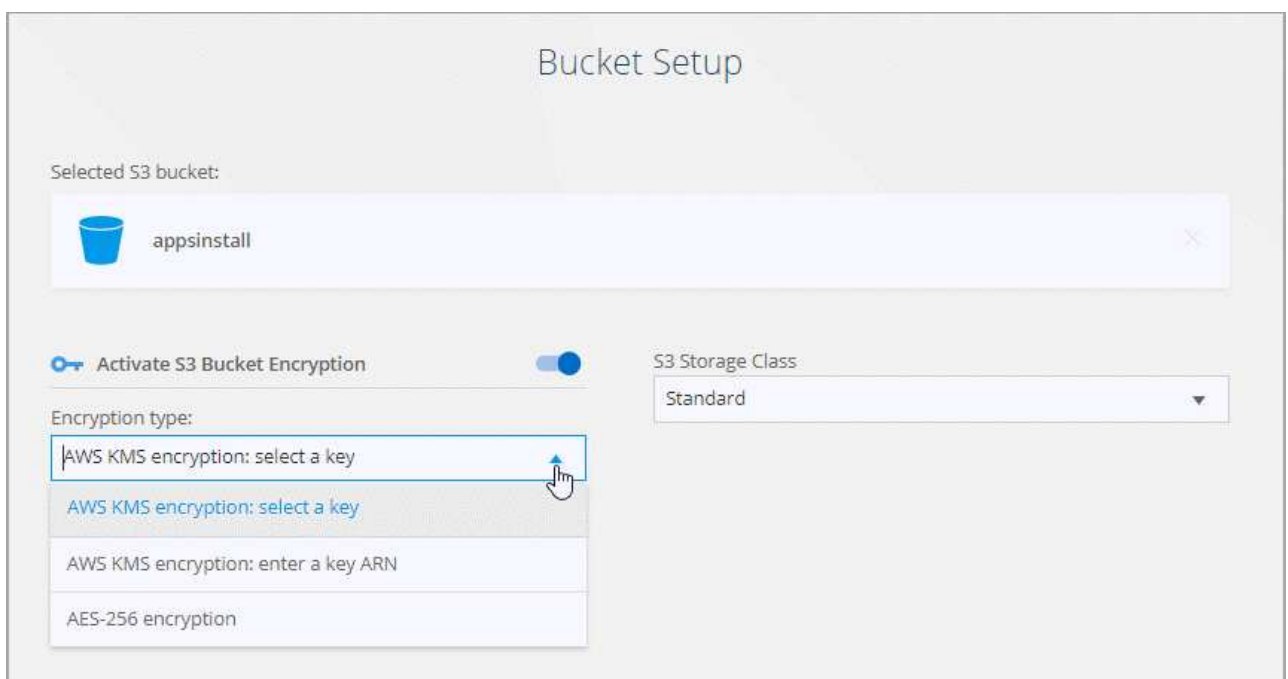
如果您想要同步 NFS 伺服器上的多個目錄，則必須在完成後建立額外的同步關係。

7. 在 **AWS S3 Bucket** 頁面上，選擇一個儲存桶：

- 向下鑽取以選擇儲存桶內的現有資料夾或選擇您在儲存桶內建立的新資料夾。
- 選擇「新增至清單」以選擇與您的 AWS 帳戶不關聯的 S3 儲存桶。"[必須對 S3 儲存桶應用特定權限](#)"。

8. 在*Bucket Setup*頁面上，設定儲存桶：

- 選擇是否啟用 S3 儲存桶加密，然後選擇 AWS KMS 金鑰、輸入 KMS 金鑰的 ARN 或選擇 AES-256 加密。
- 選擇 S3 儲存類別。"[查看支援的儲存類別](#)"。



9. 在「設定」頁面上，定義如何在目標位置同步和維護來源檔案和資料夾：

行程

選擇未來同步的重複計畫或關閉同步計畫。您可以安排每 1 分鐘同步一次資料。

同步逾時

定義如果同步在指定的分鐘數、小時數或天數內未完成，複製和同步是否應取消資料同步。

通知

使您能夠選擇是否在NetApp控制台的Notification中心接收複製和同步通知。您可以啟用資料同步成功、資料同步失敗和資料同步取消的通知。

重試

定義複製和同步在跳過檔案之前應重試同步檔案的次數。

連續同步

初始資料同步後，複製和同步會監聽來源 S3 儲存桶或 Google Cloud Storage 儲存桶上的變化，並在發生任何變更時持續同步到目標。無需按照預定的時間間隔重新掃描來源。

此設定僅在建立同步關係時以及將資料從 S3 儲存桶或 Google Cloud Storage 同步至 Azure Blob 儲存體、CIFS、Google Cloud Storage、IBM Cloud Object Storage、NFS、S3 和StorageGRID *或*從 Azure Blob 儲存體同步到 Azure Blob 儲存體、CIFS、Google Cloud Storage、StorageGRID

如果啟用此設置，它將影響以下其他功能：

- 同步計劃已停用。
- 以下設定恢復為其預設值：同步逾時、最近修改的檔案和修改日期。
- 如果 S3 是來源，則按大小過濾將僅在複製事件（而不是刪除事件）時有效。
- 關係創建後，只能加速或刪除關係。您不能中止同步、修改設定或查看報告。

可以與外部儲存桶建立連續同步關係。為此，請按照下列步驟操作：

- 前往外部儲存桶專案的 Google Cloud 控制台。
- 前往*雲端儲存>設定>雲端儲存服務帳戶*。
- 更新 local.json 檔案：

```
{
  "protocols": {
    "gcp": {
      "storage-account-email": <storage account email>
    }
  }
}
```

- 重新啟動資料代理：

- A. `sudo pm2 停止所有`
- B. `sudo pm2 啟動所有`
- v. 與相關外部儲存桶建立持續同步關係。



用於與外部儲存桶建立連續同步關係的資料代理程式將無法與其專案中的儲存桶建立另一個連續同步關係。

比較依據

選擇在確定檔案或目錄是否已變更並應再次同步時，複製和同步是否應比較某些屬性。

即使您取消選取這些屬性，「複製和同步」仍會透過檢查路徑、檔案大小和檔案名稱將來源與目標進行比較。如果有任何變化，那麼它會同步這些檔案和目錄。

您可以透過比較以下屬性來選擇啟用或停用複製和同步：

- **mtime**：檔案的最後修改時間。此屬性對於目錄無效。
- **uid**、**gid** 和 **mode**：Linux 的權限標誌。

物件複製

啟用此選項可複製物件儲存元資料和標籤。如果使用者變更了來源上的元數據，則「複製和同步」會在下一次同步中複製該對象，但如果使用者變更了來源上的標籤（而不是資料本身），則「複製和同步」不會在下一次同步中複製該物件。

建立關係後，您無法編輯此選項。

以 Azure Blob 或 S3 相容端點（S3、StorageGRID 或 IBM Cloud Object Storage）為目標的同步關係支援複製標籤。

以下任意端點之間的「雲端到雲端」關係支援複製元資料：

- AWS S3
- Azure Blob
- Google 雲端儲存
- IBM 雲端物件儲存
- StorageGRID

最近修改的文件

選擇排除在預定同步之前最近修改的檔案。

刪除來源文件

在「複製和同步」將檔案複製到目標位置後，選擇從來源位置刪除檔案。此選項存在資料遺失的風險，因為來源檔案在複製後會被刪除。

如果啟用此選項，您還需要變更資料代理程式上的 `local.json` 檔案中的參數。開啟檔案並進行以下更新：

```
{
  "workers":{
    "transferrer":{
      "delete-on-source": true
    }
  }
}
```

更新 local.json 檔案後，您應該重新啟動：`pm2 restart all`。

刪除目標文件

如果檔案已從來源位置刪除，則選擇從目標位置刪除檔案。預設設定是從不從目標位置刪除檔案。

文件類型

定義每次同步中要包含的檔案類型：檔案、目錄、符號連結和硬連結。



硬連結僅適用於不安全的 NFS 到 NFS 關係。使用者將被限制為一個掃描器進程和一個掃描器並發，並且掃描必須從根目錄運行。

排除檔案副檔名

透過輸入檔案副檔名並按下 **Enter** 來指定要從同步中排除的正規表示式或檔案副檔名。例如，鍵入 `log` 或 `.log` 來排除 `*.log` 檔案。多個擴展名不需要分隔符號。以下影片提供了一個簡短的演示：

排除同步關係的檔案副檔名



Regex 或正規表示式與通配符或 glob 表達式不同。此功能*僅*適用於正規表示式。

排除目錄

透過輸入其名稱或目錄完整路徑並按 **Enter**，指定最多 15 個要從同步中排除的正規表示式或目錄。預設情況下，`.copy-offload`、`.snapshot`、`~snapshot` 目錄被排除。



Regex 或正規表示式與通配符或 glob 表達式不同。此功能*僅*適用於正規表示式。

文件大小

選擇同步所有文件，無論其大小，或僅同步特定大小範圍內的文件。

修改日期

選擇所有文件，無論其最後修改日期為何，選擇在特定日期之後、特定日期之前或某個時間範圍內修改的文件。

建立日期

當 SMB 伺服器作為來源時，此設定可讓您同步在特定日期之後、特定日期之前或特定時間範圍之間建立的檔案。

ACL——存取控制列表

透過在建立關係時或建立關係後啟用設置，從 SMB 伺服器僅複製 ACL、僅複製檔案或複製 ACL 和檔案。

10. 在「標籤/元資料」頁面上，選擇是否將鍵值對儲存為傳輸到 S3 儲存桶的所有檔案的標籤，或是否為所有檔案指派元資料鍵值對。

The screenshot shows the 'Relationship Tags' configuration page for an AWS S3 Bucket. The page has a breadcrumb trail: < AWS S3 Bucket > Settings > 6 Tags/Metadata > 7 Review. The main heading is 'Relationship Tags'. Below it, a message states: 'Cloud Sync assigns the relationship tags to all of the files transferred to the S3 bucket. This enables you to search for the transferred files by using the tag values.' There are two radio buttons: 'Save on Object's Tags' (selected) and 'Save On Object's Metadata'. Below this, there are two input fields: 'Tag Key' with a placeholder 'Up to 128 characters' and 'Tag Value' with a placeholder 'Up to 256 characters'. At the bottom left is a button '+ Add Relationship Tag' and at the bottom right is the text 'Optional Field | [Up to 5]'.



將資料同步至StorageGRID和 IBM Cloud Object Storage 時，此功能同樣可用。對於 Azure 和 Google Cloud Storage，只有元資料選項可用。

11. 查看同步關係的詳細信息，然後選擇*建立關係*。

結果

複製和同步開始在來源和目標之間同步資料。同步統計資料包括同步所花費的時間、是否停止以及複製、掃描或刪除的檔案數量。然後您可以管理您的 ["同步關係"](#)，["管理您的數據經紀人"](#)，或者 ["建立報告以優化您的效能和配置"](#)。

從NetApp Data Classification建立同步關係

複製和同步與NetApp Data Classification。在NetApp Data Classification中，您可以選擇要使用複製和同步同步到目標位置的來源檔案。

從NetApp Data Classification啟動資料同步後，所有來源資訊都包含在一個步驟中，只需要您輸入一些關鍵詳細資訊。然後，選擇新同步關係的目標位置。

"了解如何從NetApp Data Classification啟動同步關係"。

在NetApp Copy and Sync中從 SMB 共用複製 ACL

NetApp Copy and Sync可以在 SMB 共用之間以及 SMB 共用和物件儲存之間複製存取控制清單 (ACL) (ONTAP S3 除外)。如果需要，您也可以選擇使用 robocopy 手動保留 SMB 共用之間的 ACL。

選擇

- [設定複製和同步以自動複製 ACL](#)
- [在 SMB 共用之間手動複製 ACL](#)

設定複製和同步以複製 ACL

透過在建立關係時或建立關係後啟用設置，在 SMB 共用之間以及 SMB 共用和物件儲存之間複製 ACL。

開始之前

此功能適用於任何類型的資料代理：AWS、Azure、Google Cloud Platform 或本機資料代理程式。本地資料代理可以運行"[任何支援的作業系統](#)"。

建立新關係的步驟

1. ["登入以複製和同步"](#)。
2. 從複製和同步中，選擇*建立新同步*。
3. 將 SMB 伺服器或物件儲存拖放為來源，將 SMB 伺服器或物件儲存拖放為目標，然後選擇*繼續*。
4. 在 **SMB 伺服器** 頁面上：
 - a. 輸入新的 SMB 伺服器或選擇現有伺服器並選擇*繼續*。
 - b. 輸入 SMB 伺服器的憑證。
 - c. 選擇*僅複製檔案*、*僅複製 ACL*或*複製檔案和 ACL，然後選擇*繼續*。

Select an SMB Source

SMB Server Version : 2.1

Selected SMB Server:

210.10.10.10 [Change Server](#)

Define SMB Credentials:

User Name: user1 Password: Password Domain (Optional):

ACL - Access Control List

Copy only files

Notice: Copying ACLs can affect sync performance. You can change this setting after you create the relationship.

Attention: If the sync relationship includes Cloud Volumes ONTAP or an on-prem ONTAP cluster and you selected NFSv4 or later, then you'll need to enable NFSv4 ACLs on the ONTAP system. This is required to copy the ACLs.

5. 請依照其餘提示建立同步關係。

將 ACL 從 SMB 複製到物件儲存時，您可以選擇將 ACL 複製到物件的標籤或物件的元數據，具體取決於目標。對於 Azure 和 Google Cloud Storage，只有元資料選項可用。

以下螢幕截圖顯示了您可以做出此選擇的步驟範例。

< AWS S3 Bucket Settings **6 Tags/Metadata** 7 Review

Relationship Metadata

Cloud Sync assigns the relationship metadata to all of the files transferred to the S3 bucket.

☐ Save on Object's Tags ☒ Save On Object's Metadata

Metadata Key: Up to 128 characters Metadata Value: Up to 256 characters

+ Add Relationship Metadata Optional Field | [Up to 5]

現有關係的步驟

1. 將滑鼠懸停在同步關係上並選擇操作選單。
2. 選擇“設定”。

3. 選擇*僅複製檔案*、僅複製 **ACL***或*複製檔案和 **ACL**，然後選擇*繼續*。
4. 選擇“儲存設定”。



複製和同步功能會保留 SMB ACL（權限），但不會複製檔案或資料夾的所有權。所有權不包含在中小企業存取控制清單 (ACL) 轉移作業中。

結果

同步資料時，複製和同步會保留來源和目標之間的 ACL。

在 SMB 共用之間手動複製 ACL

您可以使用 Windows robocopy 指令手動保留 SMB 共用之間的 ACL。



如果您除了需要保留存取控制清單 (ACL) 之外，還需要保留所有權（擁有者和群組），則可以使用下列方法：`robocopy` 命令。使用 `/copyall` 標記副本 ACL、所有權和審計資訊。

步驟

1. 確定對兩個 SMB 共用都具有完全存取權限的 Windows 主機。
2. 如果任一端點需要驗證，請使用 **net use** 指令從 Windows 主機連線到端點。

在使用 robocopy 之前，必須執行此步驟。

3. 從複製和同步中，在來源和目標 SMB 共享之間建立新的關係或同步現有關係。
4. 資料同步完成後，從 Windows 主機執行以下命令來同步 ACL 和所有權：

```
robocopy /E /COPY:SOU /secfix [source] [target] /w:0 /r:0 /XD ~snapshots  
/UNILOG:"[logfilepath]
```

source 和 *target* 都應該使用 UNC 格式指定。例如：\\<伺服器>\<共享>\<路徑>

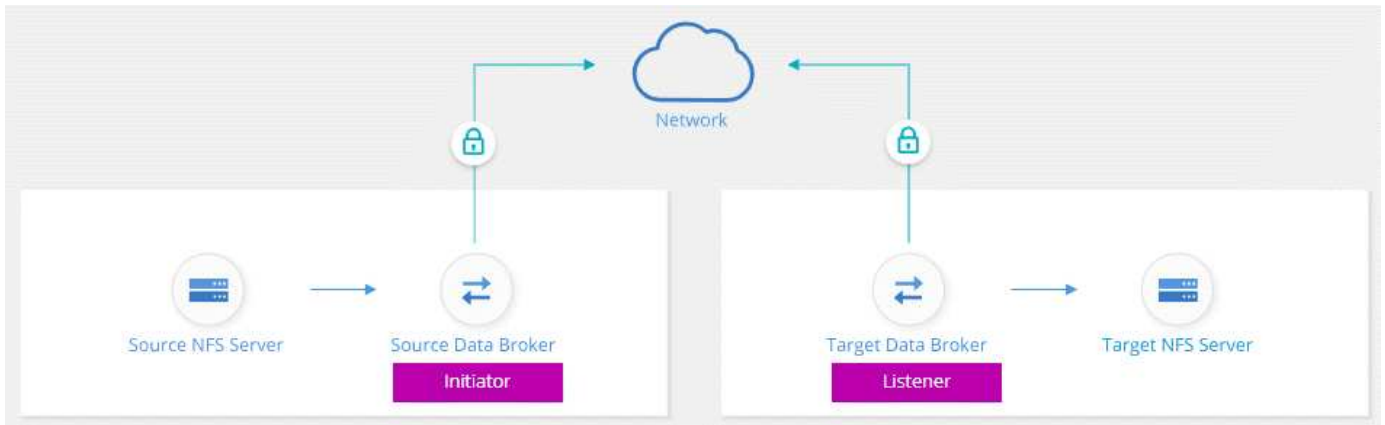
使用NetApp Copy and Sync中的資料傳輸加密同步 NFS 數據

如果您的企業有嚴格的安全策略，您可以使用NetApp Copy and Sync中的資料傳輸加密來同步 NFS 資料。此功能支援從一個 NFS 伺服器到另一個 NFS 伺服器以及從Azure NetApp Files到Azure NetApp Files。

例如，您可能希望在位於不同網路中的兩個 NFS 伺服器之間同步資料。或者您可能需要跨子網路或區域安全地傳輸Azure NetApp Files上的資料。

資料傳輸加密的工作原理

當 NFS 資料在兩個資料代理之間透過網路傳送時，資料傳輸加密會對其進行加密。下圖顯示了兩個 NFS 伺服器和兩個資料代理之間的關係：



一個資料代理充當_發起者_。當需要同步資料時，它會向另一個資料代理程式（即_監聽器_）發送連線請求。此資料代理程式在連接埠 443 上監聽請求。如果需要，您可以使用其他端口，但請務必檢查該端口未被其他服務使用。

例如，如果您將資料從本機 NFS 伺服器同步到基於雲端的 NFS 伺服器，則可以選擇哪個資料代理程式偵聽連線請求以及哪個資料代理程式傳送連線請求。

動態加密的工作原理如下：

1. 建立同步關係後，發起者將與其他資料代理建立加密連線。
2. 來源資料代理程式使用 TLS 1.3 加密來自來源的資料。
3. 然後，它透過網路將資料傳送到目標資料代理。
4. 目標資料代理程式在將資料傳送給目標之前對其進行解密。
5. 初始複製後，複製和同步每 24 小時同步一次任何更改的資料。如果有資料需要同步，則該程序從發起者與其他資料代理程式建立加密連線開始。

如果您希望更頻繁地同步數據，"[您可以在建立關係後變更時間表](#)"。

支援的 NFS 版本

- 對於 NFS 伺服器，NFS 版本 3、4.0、4.1 和 4.2 支援資料傳輸加密。
- 對於 Azure NetApp Files，NFS 版本 3 和 4.1 支援資料傳輸加密。

代理伺服器限制

如果您建立加密同步關係，加密資料將透過 HTTPS 傳送，並且無法透過代理伺服器路由。

入門所需

請確保具備以下條件：

- 兩個 NFS 伺服器"[源和目標要求](#)"或兩個子網路或區域中的 Azure NetApp Files。
- 伺服器的 IP 位址或完全限定網域名稱。
- 兩個資料代理的網路位置。

您可以選擇現有的資料代理，但它必須充當發起者。監聽器資料代理程式必須是新的資料代理程式。

如果要使用現有的資料代理組，則該組必須只有一個資料代理程式。加密同步關係不支援群組中的多個資料代理程式。

如果您尚未部署資料代理，請查看資料代理要求。由於您有嚴格的安全策略，請務必檢查網路要求，其中包括來自連接埠 443 的出站流量和["網路端點"](#)數據經紀人聯繫的。

- ["檢查 AWS 安裝"](#)
- ["查看 Azure 安裝Review Azure installation"](#)
- ["檢查 Google Cloud 安裝"](#)
- ["檢查 Linux 主機安裝"](#)

使用數據傳輸加密同步 **NFS** 數據

在兩個 NFS 伺服器之間或 Azure NetApp Files 之間建立新的同步關係，啟用動態加密選項，然後依照指示操作。

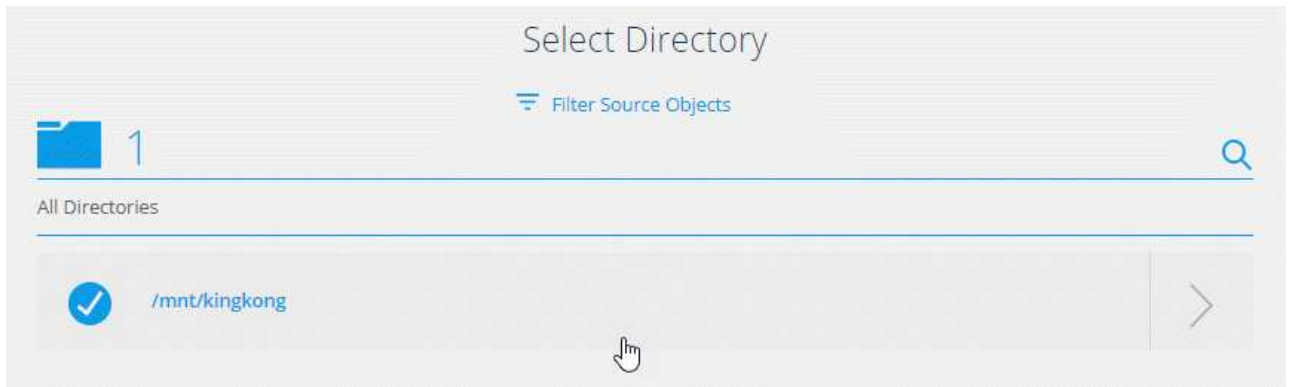
步驟

1. ["登入以複製和同步"](#)。
2. 選擇*建立新同步*。
3. 將 **NFS** 伺服器 拖曳到來源位置和目標位置，或將 * Azure NetApp Files* 拖曳到來源位置和目標位置，然後選擇 是 以啟用資料傳輸加密。
4. 依照提示建立關係：
 - a. **NFS** 伺服器/* Azure NetApp Files*：選擇 NFS 版本，然後指定新的 NFS 來源或選擇現有伺服器。
 - b. 定義資料代理功能：定義哪個資料代理程式在連接埠上監聽連線請求以及哪個資料代理程式啟動連線。根據您的網路要求做出選擇。
 - c. 資料代理：依照提示新增新的來源資料代理程式或選擇現有的資料代理程式。

請注意以下事項：

- 如果要使用現有的資料代理組，則該組必須只有一個資料代理程式。加密同步關係不支援群組中的多個資料代理程式。
- 如果來源資料代理程式充當監聽器，那麼它必須是一個新的資料代理。
- 如果您需要新的資料代理，Copy and Sync 會提示您安裝說明。您可以在雲端部署資料代理，也可以為您自己的 Linux 主機下載安裝腳本。
- d. 目錄：透過選擇所有目錄或向下鑽取並選擇子目錄來選擇要同步的目錄。

選擇「過濾來源物件」來修改定義如何在目標位置同步和維護來源檔案和資料夾的設定。

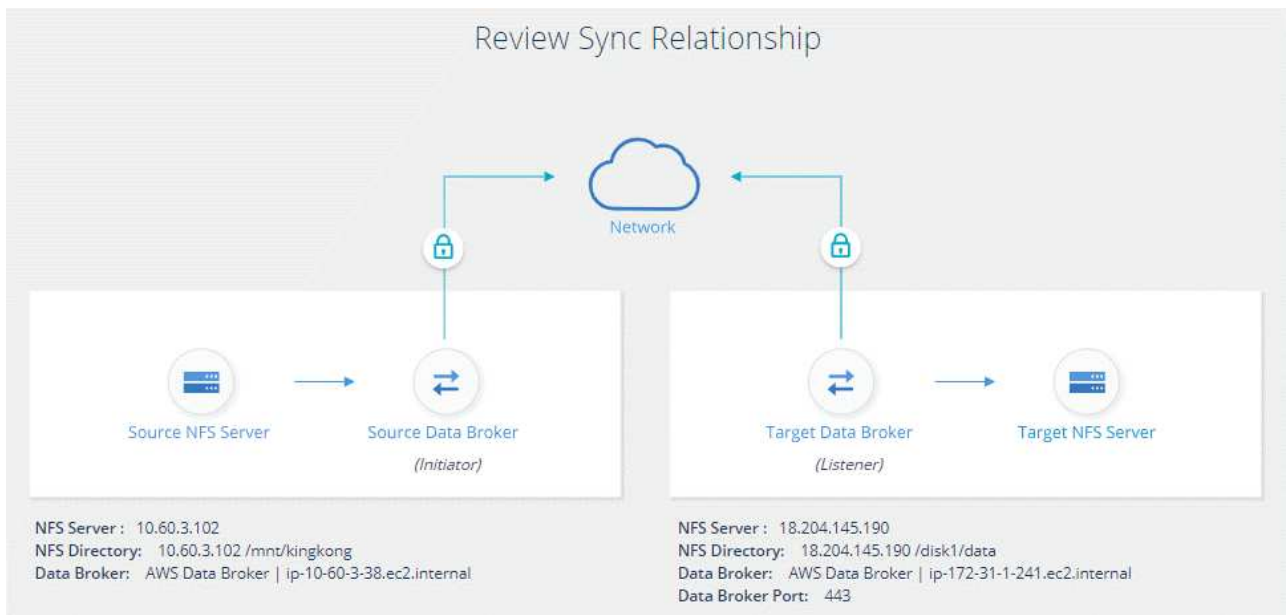


- e. 目標 **NFS** 伺服器/目標**Azure NetApp Files**：選擇 NFS 版本，然後輸入新的 NFS 目標或選擇現有伺服器。
- f. 目標資料代理：依照指示新增新的來源資料代理程式或選擇現有的資料代理程式。

如果目標資料代理程式充當監聽器，那麼它必須是一個新的資料代理。

以下是目標資料代理程式作為監聽器時的提示範例。注意指定連接埠的選項。

- a. 目標目錄：選擇頂級目錄，或向下鑽取以選擇現有子目錄或在匯出中建立新資料夾。
- b. 設定：定義如何在目標位置同步和維護來源檔案和資料夾。
- c. 審核：審核同步關係的詳細信息，然後選擇*建立關係*。



結果

複製和同步開始建立新的同步關係。完成後，選擇*在儀表中查看*以查看有關新關係的詳細資訊。

設定資料代理組以在NetApp Copy and Sync中使用外部 HashiCorp Vault

當您建立需要 Amazon S3、Azure 或 Google Cloud 憑證的同步關係時，您需要透過NetApp Copy and Sync使用者介面或 API 指定這些憑證。另一種方法是設定資料代理群組以直接從外部 HashiCorp Vault 存取憑證（或_秘密_）。

此功能透過複製和同步 API 支持，同步關係需要 Amazon S3、Azure 或 Google Cloud 憑證。

1

準備保管庫

透過設定 URL 來準備保險庫以向資料代理群組提供憑證。保險庫中秘密的 URL 必須以 *Creds* 結尾。

2

準備數據經紀人組

透過修改群組中每個資料代理程式的本機設定文件，準備資料代理群組從外部保險庫取得憑證。

3

使用 API 建立同步關係

現在一切都已設定完畢，您可以發送 API 呼叫來建立使用您的保險庫取得機密的同步關係。

準備保管庫

您需要提供複製和同步到您的保險庫中的秘密的 URL。透過設定這些 URL 來準備保管庫。您需要為您計劃建立的同步關係中的每個來源和目標設定憑證的 URL。

URL 必須如下設定：

/<path>/<requestid>/<endpoint-protocol>Creds

小路

秘密的前綴路徑。這可以是任何對您來說唯一的值。

請求 ID

您需要產生的請求 ID。建立同步關係時，您需要在 API POST 請求的其中一個標頭中提供 ID。

端點協定

定義如下的協定之一 "在 [post relationship v2 文件中](#)"：S3、AZURE 或 GCP（每個都必須大寫）。

信用

URL 必須以 *Creds* 結尾。

範例

以下範例顯示了機密的 URL。

來源憑證的完整 URL 和路徑範例

\ <http://example.vault.com:8200/my-path/all-secrets/hb312vdasr2/S3Creds>

如您在範例中看到的，前綴路徑是 */my-path/all-secrets/*，請求 ID 是 *hb312vdasr2*，來源端點是 S3。

目標憑證的完整 URL 和路徑範例

\ <http://example.vault.com:8200/my-path/all-secrets/n32hcbnejk2/AZURECreds>

前綴路徑為 */my-path/all-secrets/*，請求 ID 為 *n32hcbnejk2*，目標端點為 Azure。

準備數據經紀人組

透過修改群組中每個資料代理程式的本機設定文件，準備資料代理群組從外部保險庫取得憑證。

步驟

1. 透過 SSH 連線到群組中的資料代理程式。
2. 編輯位於 */opt/netapp/databroker/config* 中的 *local.json* 檔案。
3. 將啟用設為 **true** 並設定 *external-integrations.hashicorp* 下的設定參數欄位如下：

已啟用

- 有效值：true/false
- 類型：布林值
- 預設值：false
- 正確：資料經紀人從您自己的外部 HashiCorp Vault 取得機密
- 錯誤：資料代理將憑證儲存在其本機保管庫中

網址

- 類型：字串

- 值：外部保管庫的 URL

小路

- 類型：字串
- 值：使用您的憑證作為金鑰的前綴路徑

拒絕未經授權

- 確定是否希望資料代理拒絕未經授權的外部保管庫
- 類型：布林值
- 預設值：false

授權方法

- 資料代理應使用的身份驗證方法，用於從外部保管庫存取憑證
- 類型：字串
- 有效值：“aws-iam” / “role-app” / “gcp-iam”

角色名稱

- 類型：字串
- 您的角色名稱（如果您使用 aws-iam 或 gcp-iam）

Secretid 和 rootid

- 類型：字串（如果您使用 app-role）

命名空間

- 類型：字串
- 您的命名空間（如果需要，請輸入 X-Vault-Namespace 標頭）

4. 對群組中的任何其他資料代理重複這些步驟。

aws-role 身份驗證範例

```
{
  "external-integrations": {
    "hashicorp": {
      "enabled": true,
      "url": "https://example.vault.com:8200",
      "path": "my-path/all-secrets",
      "reject-unauthorized": false,
      "auth-method": "aws-role",
      "aws-role": {
        "role-name": "my-role"
      }
    }
  }
}
```

gcp-iam 身份驗證範例

```
{
  "external-integrations": {
    "hashicorp": {
      "enabled": true,
      "url": "http://ip-10-20-30-55.ec2.internal:8200",
      "path": "v1/secret",
      "namespace": "",
      "reject-unauthorized": true,
      "auth-method": "gcp-iam",
      "aws-iam": {
        "role-name": ""
      },
      "app-role": {
        "root_id": "",
        "secret_id": ""
      },
      "gcp-iam": {
        "role-name": "my-iam-role"
      }
    }
  }
}
```

使用 **gcp-iam** 身份驗證時設定權限

如果您使用 *gcp-iam* 驗證方法，則資料代理必須具有下列 GCP 權限：

```
- iam.serviceAccounts.signJwt
```

"[詳細了解資料代理的 GCP 權限要求](#)"。

使用保管庫中的機密建立新的同步關係

現在一切都已設定完畢，您可以發送 API 呼叫來建立使用您的保險庫取得機密的同步關係。

使用複製和同步 REST API 發布關係。

```
Headers:  
Authorization: Bearer <user-token>  
Content-Type: application/json  
x-account-id: <accountid>  
x-netapp-external-request-id-src: request ID as part of path for source  
credentials  
x-netapp-external-request-id-trg: request ID as part of path for target  
credentials  
Body: post relationship v2 body
```

- 若要取得使用者令牌和您的NetApp Console帳號 ID，"[請參閱文件中的此頁面](#)"。
- 為了在戀愛後擁有好身材，"[參考 relationships-v2 API 呼叫](#)"。

例子

POST 請求範例：

```
url: https://api.cloudsync.netapp.com/api/relationships-v2
headers:
"x-account-id": "CS-SasdW"
"x-netapp-external-request-id-src": "hb312vdasr2"
"Content-Type": "application/json"
"Authorization": "Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ik..."
Body:
{
  "dataBrokerId": "5e6e111d578dtyuu1555sa60",
  "source": {
    "protocol": "s3",
    "s3": {
      "provider": "sgws",
      "host": "1.1.1.1",
      "port": "443",
      "bucket": "my-source"
    }
  },
  "target": {
    "protocol": "s3",
    "s3": {
      "bucket": "my-target-bucket"
    }
  }
}
```

NetApp Copy and Sync免費試用期結束後，支付同步關係費用

NetApp Copy and Sync 的14 天免費試用期結束後，有兩種方式可以支付同步關係的費用。第一個選項是從 AWS 或 Azure 訂閱，按使用量付費或按年付費。第二種選擇是直接從NetApp購買許可證。

您可以從 AWS Marketplace 或 Azure Marketplace 訂閱。您不能同時訂閱兩者。

您可以選擇透過市場訂閱使用NetApp的授權。例如，如果您有 25 個同步關係，則可以使用授權支付前 20 個同步關係的費用，然後使用剩餘的 5 個同步關係從 AWS 或 Azure 按使用量付費。

["詳細了解許可證的運作方式"](#)。

如果您在免費試用期結束後沒有立即付款，您將無法建立任何其他關係。現有的關係不會被刪除，但在您訂閱或輸入許可證之前，您不能對其進行任何更改。

授權應透過NetApp Copy and Sync或適用網站進行管理，而非透過NetApp Console訂閱進行管理。

從 AWS 訂閱

AWS 可讓您按使用量付費或按年付費。

即用即付的步驟

1. 從NetApp Console導覽功能表中，選擇 **Mobility > Copy and Sync**。
2. 選擇*許可*。
3. 選擇 **AWS**。
4. 選擇*訂閱*，然後選擇*繼續*。
5. 從 AWS Marketplace 訂閱，然後重新登入 Copy and Sync 完成註冊。

以下影片展示了這個過程：

[從 AWS Marketplace 訂閱複製和同步](#)

每年付款的步驟

1. "[前往 AWS Marketplace 頁面](#)"。
2. 選擇*繼續訂閱*。
3. 選擇您的合約選項，然後選擇*建立合約*。

從 Azure 訂閱

Azure 可讓您按使用量付費或按年付費。

你需要什麼

在相關訂閱中具有貢獻者或擁有者權限的 Azure 使用者帳戶。

步驟

1. 從NetApp Console導覽功能表中，選擇 **Mobility > Copy and Sync**。
2. 選擇*許可*。
3. 選擇“**Azure**”。
4. 選擇*訂閱*，然後選擇*繼續*。
5. 在 Azure 入口網站中，選擇“建立”，選擇您的選項，然後選擇“訂閱”。

選擇「每月」按小時付費，或選擇「每年」預付一年的費用。

6. 部署完成後，在通知彈出視窗中選擇 SaaS 資源的名稱。
7. 選擇“配置帳戶”返回“複製和同步”。

以下影片展示了這個過程：

[從 Azure 市場訂閱複製和同步](#)

從NetApp購買許可證並將其添加到複製和同步

要預先支付同步關係的費用，您必須購買一個或多個許可證並將其添加到複製和同步中。

你需要什麼

您需要許可證的序號以及與該許可證關聯的NetApp支援網站帳戶的使用者名稱和密碼。

步驟

1. 透過 [聯絡NetApp](#) 購買授權。
2. "登入以複製和同步"。
3. 選擇*許可*。
4. 選擇*新增許可證*並新增所需資訊：
 - a. 輸入序號。
 - b. 選擇與您要新增的許可證關聯的NetApp支援網站帳戶：
 - 如果您的帳戶已新增至NetApp Console，請從下拉清單中選擇它。
 - 如果您的帳戶尚未新增，請選擇*新增 NSS 憑證*，輸入使用者名稱和密碼，選擇*註冊*，然後從下拉清單中選擇它。
 - c. 選擇“新增”。

更新許可證

如果您延長了從NetApp購買的複製和同步許可證，則新的到期日期將不會在複製和同步中自動更新。您需要重新新增許可證以刷新到期日期。許可證應透過複製和同步或適用的網站進行管理，而不是透過NetApp Console訂閱進行管理。

步驟

1. 從NetApp Console導覽功能表中，選擇 **Mobility > Copy and Sync**。
2. 選擇*許可*。
3. 選擇*新增許可證*並新增所需資訊：
 - a. 輸入序號。
 - b. 選擇與您要新增的許可證關聯的NetApp支援網站帳戶。
 - c. 選擇“新增”。

結果

複製和同步會使用新的到期日更新現有許可證。

在NetApp Copy and Sync中管理同步關係

您可以隨時透過立即同步資料、變更計劃等來管理NetApp Copy and Sync中的同步關係。

立即執行資料同步

您無需等待下一次預定的同步，而是可以立即在來源和目標之間同步資料。

步驟

1. "登入以複製和同步"。
- 2.

從“儀表板”導航到同步關係並選擇 

3. 選擇*立即同步*，然後選擇*同步*確認。

結果

複製和同步啟動關係的資料同步過程。

加速同步效能

透過為管理關係的群組添加額外的資料代理來加速同步關係的效能。附加資料代理必須是_新_資料代理。

工作原理

如果資料代理組管理其他同步關係，那麼您新增至該組的新資料代理程式也會加速這些同步關係的效能。

例如，假設您有三種關係：

- 關係 1 由資料經紀人組 A 管理
- 關係 2 由資料經紀人組 B 管理
- 關係 3 由資料經紀人組 A 管理

您想要加速關係 1 的效能，因此您為資料代理組 A 新增一個新的資料代理程式。由於群組 A 也管理同步關係 3，因此關係的同步效能也會自動加速。

步驟

1. 確保關係中至少有一個現有資料代理處於線上狀態。
2. 從“儀表板”導航到同步關係並選擇 
3. 選擇*加速*。
4. 依照提示建立一個新的資料代理程式。

結果

複製和同步將新的資料代理程式新增到群組中。下一次資料同步的效能應該會加快。

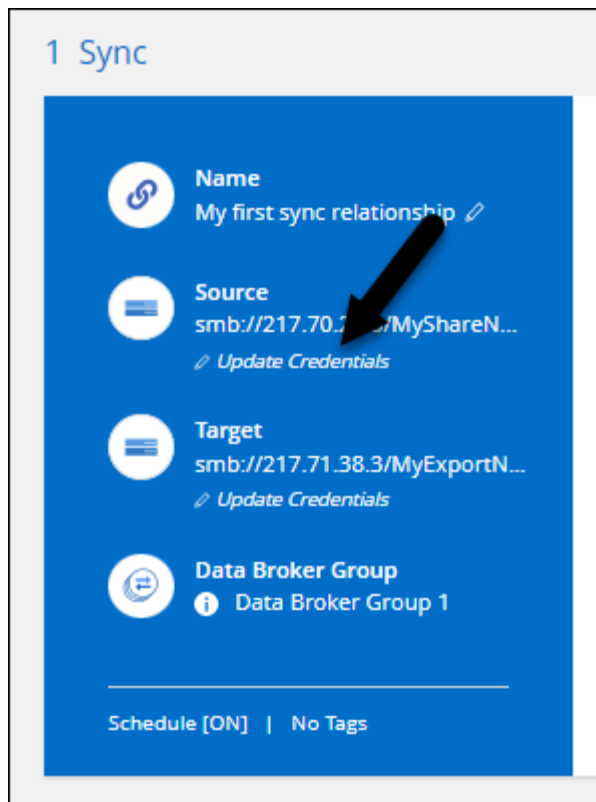
更新憑證

您可以使用現有同步關係中的來源或目標的最新憑證更新資料代理程式。如果您的安全性原則要求您定期更新憑證，則更新憑證會有所幫助。

任何複製和同步需要憑證的來源或目標都支援更新憑證：Azure Blob、Box、IBM Cloud Object Storage、StorageGRID、ONTAP S3 Storage、SFTP 和 SMB 伺服器。

步驟

1. 從*同步儀表板*，前往需要憑證的同步關係，然後選擇*更新憑證*。



2. 輸入憑證並選擇*更新*。

關於 SMB 伺服器的注意事項：如果網域是新的，那麼您需要在更新憑證時指定它。如果網域名稱沒有改變，則無需再次輸入。

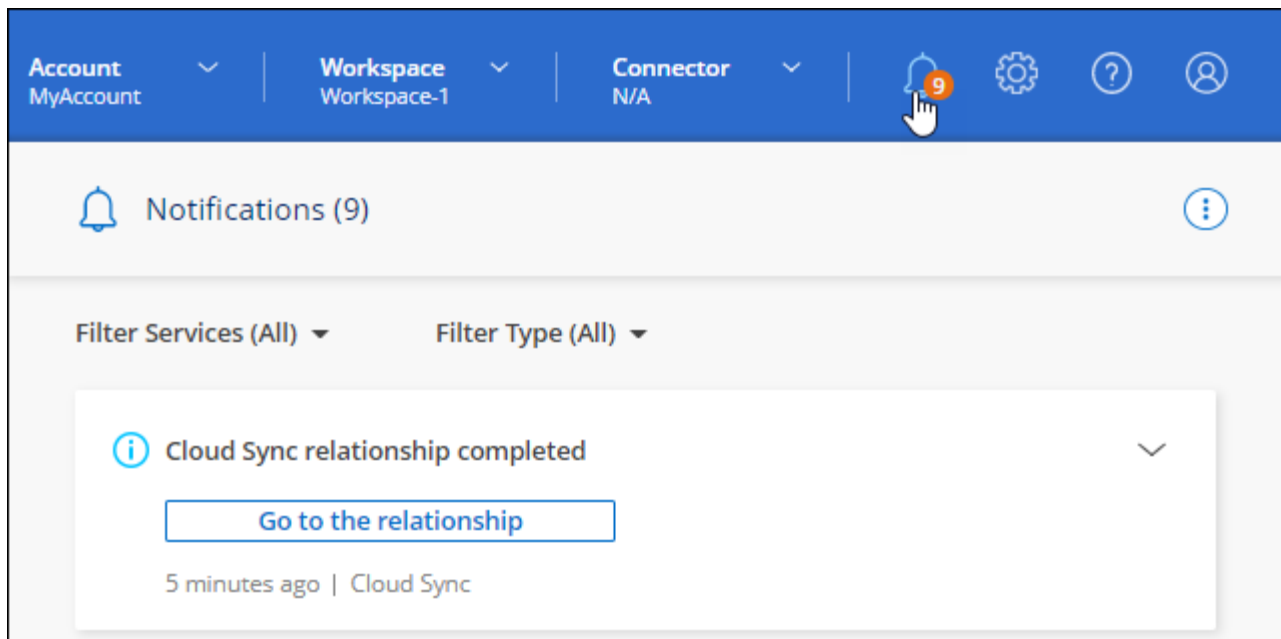
如果您在建立同步關係時輸入了網域，但在更新憑證時未輸入新網域，則複製和同步將繼續使用您提供的原始網域。

結果

複製和同步會更新資料代理程式上的憑證。資料代理開始使用更新後的憑證進行資料同步可能需要 10 分鐘。

設定通知

每個同步關係的*通知*設定可讓您選擇是否在NetApp控制台的通知中心接收複製和同步通知。您可以啟用資料同步成功、資料同步失敗和資料同步取消的通知。



此外，您也可以透過電子郵件接收通知。

步驟

1. 修改同步關係的設定：
 - a. 從“儀表板”導航到同步關係並選擇 .
 - b. 選擇“設定”。
 - c. 啟用*通知*。
 - d. 選擇“儲存設定”。
2. 如果您想透過電子郵件接收通知，請設定警報和通知設定：
 - a. 選擇*設定 > 警報和通知設定*。
 - b. 選擇一個或多個使用者並選擇*訊息*通知類型。
 - c. 選擇*應用*。

結果

如果您配置了該選項，您現在將在NetApp控制台的通知中心收到複製和同步通知，並透過電子郵件發送一些通知。

變更同步關係的設定

修改定義如何在目標位置同步和維護來源檔案和資料夾的設定。

1. 從“儀表板”導航到同步關係並選擇 .
2. 選擇“設定”。
3. 修改任何設定。

General

Schedule	ON Every 1 Day	▼
Retries	Retry 3 times before skipping file	▼

Files and Directories

Compare By	The following attributes (and size): uid, gid, mode, mtime	▼
Recently Modified Files	Exclude files that are modified up to 30 Seconds before a scheduled sync	▼
Delete Files On Source	Never delete files from the source location	▼
Delete Files On Target	Never delete files from the target location	▼
File Types	Include All: Files, Directories, Symbolic Links	▼
Exclude File Extensions	None	▼
File Size	All	▼
Date Modified	All	▼
Date Created	All	▼
ACL - Access Control List	Inactive	▼

Reset to defaults

以下是每個設定的簡要說明：

行程

選擇未來同步的重複計畫或關閉同步計畫。您可以安排每 1 分鐘同步一次資料。

同步逾時

定義如果同步在指定的分鐘數、小時數或天數內未完成，複製和同步是否應取消資料同步。

通知

使您能夠選擇是否在NetApp控制台的通知中心接收複製和同步通知。您可以啟用資料同步成功、資料同步失敗和資料同步取消的通知。

如果您想接收以下通知

重試

定義複製和同步在跳過檔案之前應重試同步檔案的次數。

比較依據

選擇在確定檔案或目錄是否已變更並應再次同步時，複製和同步是否應比較某些屬性。

即使您取消選取這些屬性，「複製和同步」仍會透過檢查路徑、檔案大小和檔案名稱將來源與目標進行比較。如果有任何變化，那麼它會同步這些檔案和目錄。

您可以透過比較以下屬性來選擇啟用或停用複製和同步：

- **mtime**：檔案的最後修改時間。此屬性對於目錄無效。
- **uid**、**gid** 和 **mode**：Linux 的權限標誌。

物件複製

建立關係後，您無法編輯此選項。

最近修改的文件

選擇排除在預定同步之前最近修改的檔案。

刪除來源文件

在「複製和同步」將檔案複製到目標位置後，選擇從來源位置刪除檔案。此選項存在資料遺失的風險，因為來源檔案在複製後會被刪除。

如果啟用此選項，您還需要變更資料代理程式上的 local.json 檔案中的參數。開啟檔案並進行以下更新：

```
{
  "workers": {
    "transferrer": {
      "delete-on-source": true
    }
  }
}
```

更新 local.json 檔案後，您應該重新啟動：`pm2 restart all`。

刪除目標文件

如果檔案已從來源位置刪除，則選擇從目標位置刪除檔案。預設設定是從不從目標位置刪除檔案。

文件類型

定義每次同步中要包含的檔案類型：檔案、目錄、符號連結和硬連結。



硬連結僅適用於不安全的 NFS 到 NFS 關係。使用者將被限制為一個掃描器進程和一個掃描器並發，並且掃描必須從根目錄運行。

排除檔案副檔名

透過輸入檔案副檔名並按下 **Enter** 來指定要從同步中排除的正規表示式或檔案副檔名。例如，鍵入 *log* 或 *.log* 來排除 *.log 檔案。多個擴展名不需要分隔符號。以下影片提供了一個簡短的演示：

排除同步關係的檔案副檔名



Regex 或正規表示式與通配符或 glob 表達式不同。此功能*僅*適用於正規表示式。

排除目錄

透過輸入其名稱或目錄完整路徑並按 **Enter**，指定最多 15 個要從同步中排除的正規表示式或目錄。預設情況下，.copy-offload、.snapshot、~snapshot 目錄被排除。



Regex 或正規表示式與通配符或 glob 表達式不同。此功能*僅*適用於正規表示式。

文件大小

選擇同步所有文件，無論其大小，或僅同步特定大小範圍內的文件。

修改日期

選擇所有文件，無論其最後修改日期為何，選擇在特定日期之後、特定日期之前或某個時間範圍內修改的文件。

建立日期

當 SMB 伺服器作為來源時，此設定可讓您同步在特定日期之後、特定日期之前或特定時間範圍之間建立的檔案。

ACL——存取控制列表

透過在建立關係時或建立關係後啟用設置，從 SMB 伺服器僅複製 ACL、僅複製檔案或複製 ACL 和檔案。

4. 選擇“儲存設定”。

結果

複製和同步會使用新設定修改同步關係。

刪除關係

如果您不再需要在來源和目標之間同步數據，您可以刪除同步關係。此操作不會刪除資料代理組（或單一資料代理實例），也不會從目標中刪除資料。

選項 1：刪除單一同步關係

步驟

1. 從“儀表板”導航到同步關係並選擇 .
2. 選擇*刪除*，然後再次選擇*刪除*進行確認。

結果

複製並同步會刪除同步關係。

選項 2：刪除多個同步關係

步驟

1. 從“儀表板”導航至“建立新同步”按鈕並選擇 。
2. 選擇要刪除的同步關係，選擇*刪除*，然後再次選擇*刪除*進行確認。

結果

複製並同步會刪除同步關係。

在NetApp Copy and Sync中管理資料代理組

NetApp Copy and Sync中的資料代理群組將資料從來源位置同步到目標位置。對於您建立的每個同步關係，群組中至少需要一個資料代理。透過為群組新增新的資料代理程式、查看有關群組的資訊等方式來管理資料代理群組。

數據經紀人團體如何運作

資料代理組可以包括一個或多個資料代理程式。將資料代理分組在一起可以幫助提高同步關係的效能。

群組可以管理多個關係

資料代理組可以同時管理一個或多個同步關係。

例如，假設您有三種關係：

- 關係 1 由資料經紀人組 A 管理
- 關係 2 由資料經紀人組 B 管理
- 關係 3 由資料經紀人組 A 管理

您想要加速關係 1 的效能，因此您為資料代理組 A 新增一個新的資料代理程式。由於群組 A 也管理同步關係 3，因此關係的同步效能也會自動加速。

一個群組中的資料代理數量

在許多情況下，單一資料代理程式可以滿足同步關係的效能要求。如果沒有，您可以透過向群組中新增額外的資料代理程式來加速同步效能。但您應該先檢查可能影響同步效能的其他因素。["詳細了解如何決定何時需要多個資料代理"](#)。

安全建議

為了確保資料代理機器的安全，NetApp建議採取以下措施：

- SSH 不應允許 X11 轉發
- SSH 不應允許 TCP 連線轉送
- SSH 不應允許隧道
- SSH 不應接受客戶端環境變量

這些安全建議有助於防止未經授權連接到資料代理機器。

將新的資料代理程式新增至群組

建立新的資料代理有多種方法：

- 建立新的同步關係時
["了解如何在建立同步關係時建立新的資料代理"](#)。
- 在“管理資料代理”頁面中選擇“新增資料代理”，這將在新群組中建立資料代理
- 從「管理資料代理」頁面，在現有群組中建立新的資料代理

開始之前

- 您無法將資料代理程式新增至管理加密同步關係的群組。
- 如果您想在現有群組中建立資料代理，則該資料代理必須是本機資料代理或相同類型的資料代理。

例如，如果某個群組包含 AWS 資料代理，那麼您可以在該群組中建立 AWS 資料代理或本機資料代理。您無法建立 Azure 資料代理程式或 Google Cloud 資料代理，因為它們不是相同的資料代理類型。

在新群組中建立資料代理的步驟

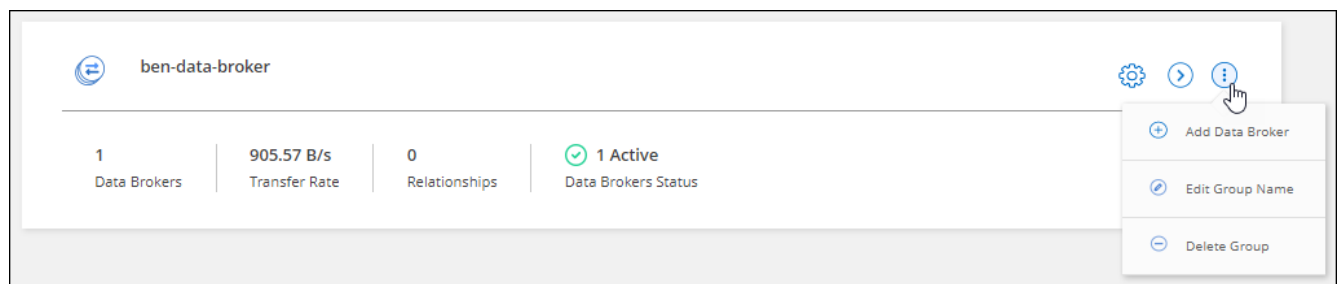
1. ["登入以複製和同步"](#)。
2. 選擇*同步>管理資料代理*。
3. 選擇*新增資料代理*。
4. 依照提示建立資料代理。

如需協助，請參閱以下頁面：

- ["在 AWS 中建立資料代理"](#)
- ["在 Azure 中建立資料代理"](#)
- ["在 Google Cloud 中建立資料代理"](#)
- ["在 Linux 主機上安裝資料代理"](#)

在現有群組中建立資料代理的步驟

1. ["登入以複製和同步"](#)。
2. 選擇*同步>管理資料代理*。
3. 選擇操作選單並選擇*新增資料代理*。



4. 依照提示在群組中建立資料代理程式。

如需協助，請參閱以下頁面：

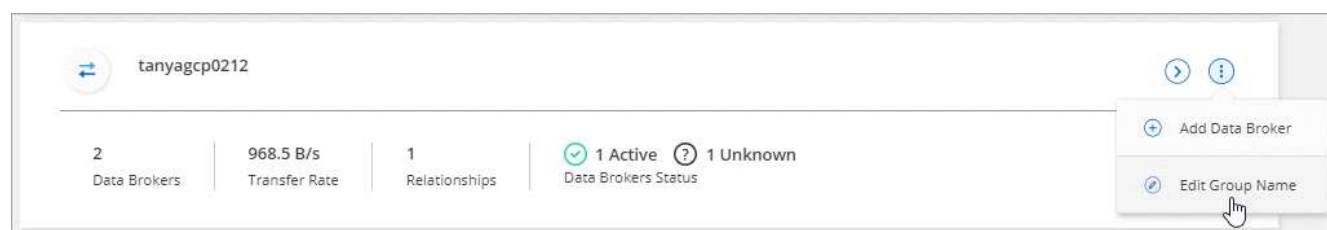
- ["在 AWS 中建立資料代理"](#)
- ["在 Azure 中建立資料代理"](#)
- ["在 Google Cloud 中建立資料代理"](#)
- ["在 Linux 主機上安裝資料代理"](#)

編輯群組名稱

隨時更改資料代理組的名稱。

步驟

1. ["登入以複製和同步"](#)。
2. 選擇*同步>管理資料代理*。
3. 選擇操作選單並選擇*編輯群組名稱*。



4. 輸入新名稱並選擇*儲存*。

結果

複製和同步更新資料代理組的名稱。

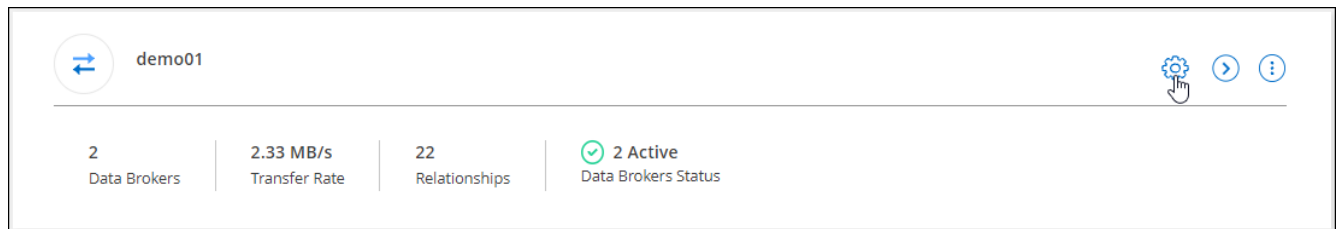
設定統一配置

如果同步關係在同步過程中遇到錯誤，統一資料代理群組的同時可以幫助減少同步錯誤的數量。請注意，變更群組配置可能會減慢傳輸速度，從而影響效能。

我們不建議您自行變更配置。您應該諮詢NetApp以了解何時更改配置以及如何更改。

步驟

1. ["登入以複製和同步"](#)。
2. 選擇*管理資料代理*。
3. 選擇資料代理組的設定圖示。



4. 根據需要變更設置，然後選擇*統一配置*。

請注意以下事項：

- 您可以選擇要變更的設定—您不需要一次更改所有四個設定。
- 將新配置傳送到資料代理程式後，資料代理程式會自動重新啟動並使用新配置。
- 此變更可能需要一分鐘才能生效並在複製和同步介面中可見。
- 如果資料代理沒有運行，它的配置將不會改變，因為複製和同步無法與其通訊。資料代理重啟後配置將會改變。
- 設定統一配置後，任何新的資料代理程式都將自動使用新配置。

在群組之間移動資料代理

如果您需要加速目標資料代理組的效能，請將資料代理從一個組移至另一個組。

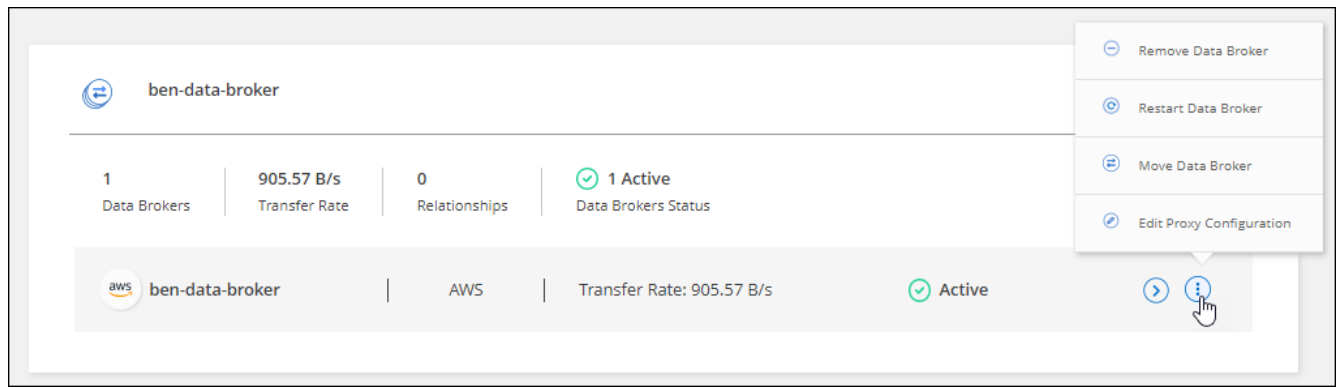
例如，如果資料代理不再管理同步關係，您可以輕鬆地將其移至管理同步關係的另一個群組。

限制

- 如果資料代理群組正在管理同步關係，且群組中只有一個資料代理，那麼您無法將該資料代理移至另一個群組。
- 您無法將資料代理移至管理加密同步關係的群組或從該群組移出。
- 您無法移動目前正在部署的資料代理程式。

步驟

1. "登入以複製和同步"。
2. 選擇*同步>管理資料代理*。
3. 選擇  擴展組中資料經紀人的清單。
4. 選擇資料代理程式的操作選單並選擇*移動資料代理*。



5. 建立一個新的資料代理組或選擇一個現有的資料代理組。

6. 選擇*移動*。

結果

複製和同步將資料代理移至新的或現有的資料代理組。如果前一組中沒有其他資料代理，則複製和同步會將其刪除。

更新代理程式配置

透過新增有關新代理程式配置的詳細資訊或編輯現有代理程式配置來更新資料代理程式的代理程式配置。

步驟

1. "登入以複製和同步"。
2. 選擇*同步>管理資料代理*。
3. 選擇  擴展組中資料經紀人的清單。
4. 選擇資料代理程式的操作選單並選擇*編輯代理程式配置*。
5. 指定有關代理的詳細資訊：主機名稱、連接埠號碼、使用者名稱和密碼。
6. 選擇*更新*。

結果

複製和同步更新資料代理程式以使用代理配置進行網際網路存取。

查看數據代理的配置

您可能想要查看有關資料代理的詳細信息，以識別其主機名稱、IP 位址、可用 CPU 和 RAM 等資訊。

複製和同步提供有關資料代理的以下詳細資訊：

- 基本資訊：實例ID、主機名稱等。
- 網路：區域、網路、子網路、私有IP等。
- 軟體：Linux發行版、資料代理版本等。
- 硬體：CPU 和 RAM
- 配置：資料代理程式的兩種主要進程－掃描器和傳輸器的詳細信息



掃描器掃描來源和目標並決定應該複製什麼。轉讓人進行實際的複製。NetApp人員可能會使用這些設定詳細資訊來建議可以優化效能的操作。

步驟

1. "登入以複製和同步"。
2. 選擇*同步>管理資料代理*。
3. 選擇  擴展組中資料經紀人的清單。
4. 選擇  查看有關資料代理的詳細資訊。

 tanyagcp0212  

2
Data Brokers

968.5 B/s
Transfer Rate

1
Relationships

 1 Active  1 Unknown
Data Brokers Status

 tanyagcp0212

GCP

Transfer Rate: 968.5 B/s

 Active  

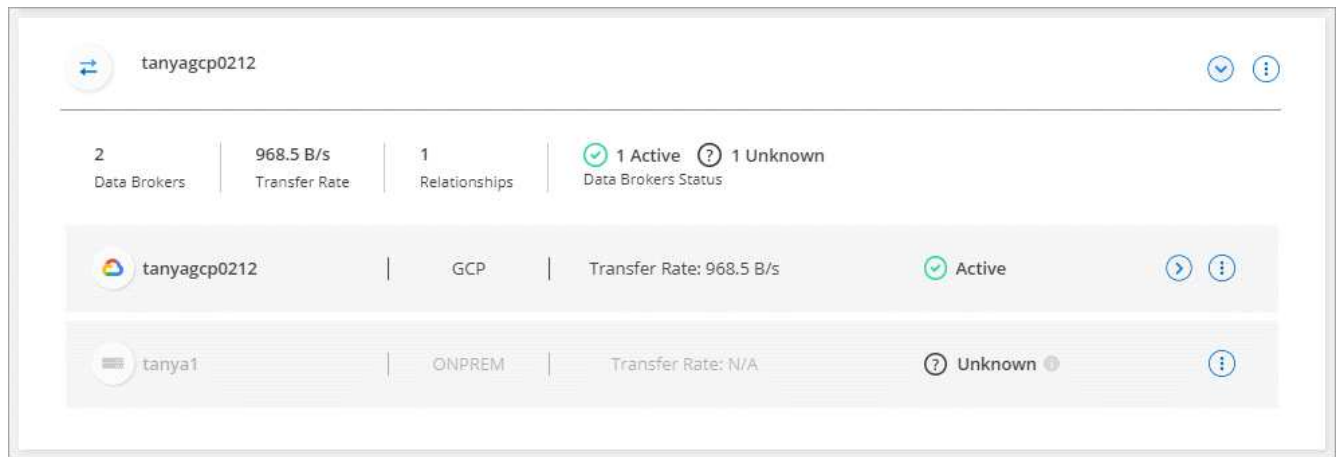
Information	5fc766b3d3e3664b9e116... Broker ID	288871247573080556 Instance ID	tanyagcp0212-mnx-data-... Host Name	cloudsync-dev-214020 Project Id
Network	us-east1-b Region	default Network	255.255.240.0 Subnet	10.142.0.37 Private IP
Software	linux Linux Distribution & Version	1.5.4 Vault Version	14.15.1 Node Version	1.3.0.18650-73f960d-integ Data Broker Version
Hardware	4 Available CPUs	62.22 MB Available RAM		
Configuration	50 Scanner Concurrency	4 Scanner CPUs	50 Transferrer Concurrency	4 Transferrer CPUs

解決數據代理問題

複製和同步顯示每個資料代理的狀態，可以幫助您解決問題。

步驟

1. "登入以複製和同步"。
2. 識別任何狀態為「未知」或「失敗」的資料代理。



3. 將滑鼠懸停在 ⓘ 圖示查看失敗原因。
4. 糾正問題。

例如，如果資料代理處於離線狀態，您可能需要重新啟動它；如果初始部署失敗，您可能需要刪除資料代理。

從群組中刪除資料代理

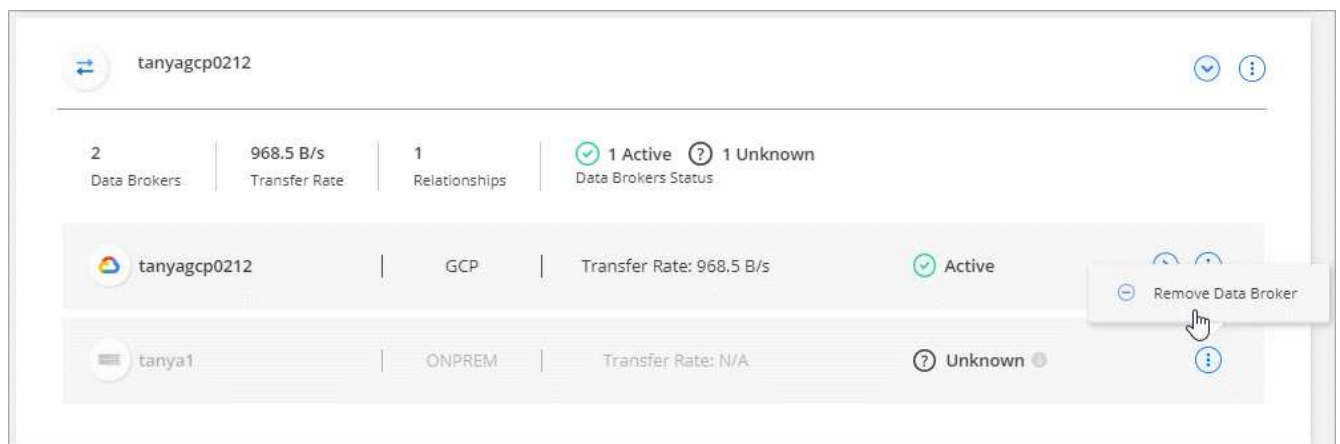
如果不再需要資料代理程式或初始部署失敗，您可以從群組中刪除該資料代理程式。此操作僅從複製和同步的記錄中刪除資料代理程式。您需要手動刪除資料代理和任何其他雲端資源。

您應該知道的事情

- 當您從群組中刪除最後一個資料代理程式時，複製和同步會刪除該群組。
- 如果存在使用該群組的關係，則您無法從該群組中刪除最後一個資料代理程式。

步驟

1. "登入以複製和同步"。
2. 選擇*同步>管理資料代理*。
3. 選擇 ⓘ 擴展組中資料經紀人的清單。
4. 選擇資料代理程式的操作選單並選擇*刪除資料代理*。



5. 選擇*刪除資料代理*。

結果

複製和同步會從群組中刪除資料代理程式。

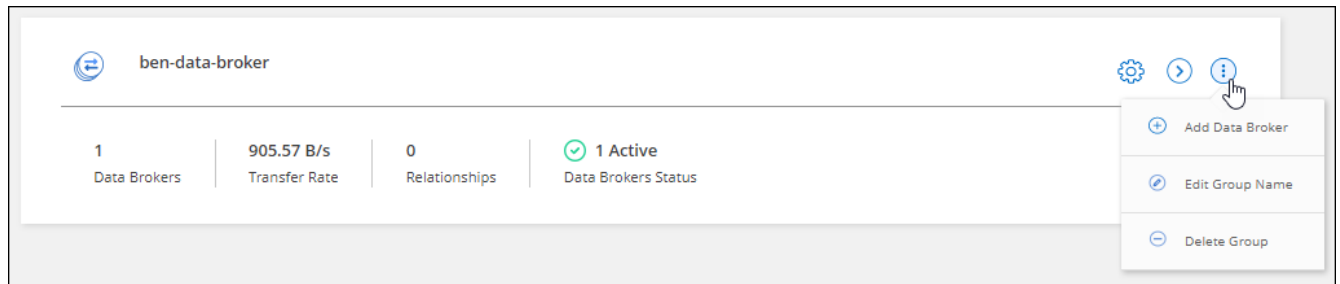
刪除資料代理組

如果資料代理組不再管理任何同步關係，您可以刪除該群組，這將從複製和同步中刪除所有資料代理程式。

Copy and Sync 刪除的資料代理程式僅從 Copy and Sync 的記錄中刪除。您需要從雲端提供者手動刪除資料代理執行個體和任何其他雲端資源。

步驟

1. "登入以複製和同步"。
2. 選擇*同步>管理資料代理*。
3. 選擇操作選單並選擇*刪除群組*。



4. 為了確認，請輸入群組名稱並選擇*刪除群組*。

結果

複製和同步會刪除資料代理並刪除該群組。

建立和檢視報告以調整NetApp Copy and Sync中的配置

在NetApp Copy and Sync中建立和查看報告以獲取信息，您可以在NetApp人員的幫助下使用這些資訊來調整資料代理的配置並提高效率。

每份報告都提供有關同步關係中路徑的詳細資訊。它將包括有多少個目錄、檔案和符號連結、檔案大小的分佈、目錄的深度和寬度、修改時間和存取時間。這與同步靜態資料不同，後者可在 "[成功創建並完成同步](#)"。

建立報告

每次建立報告時，「複製和同步」都會掃描路徑，然後將詳細資訊編譯成報告。

步驟

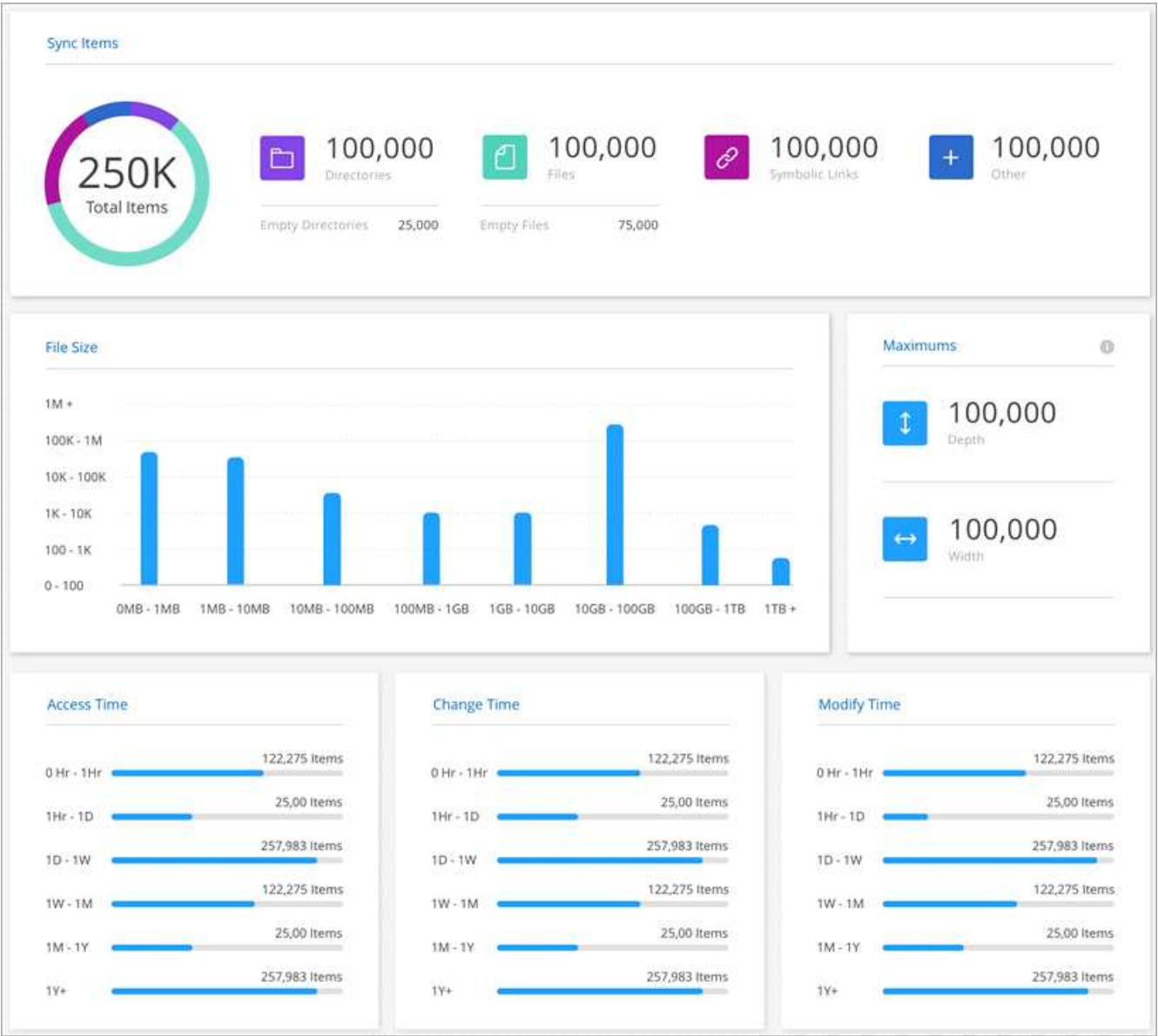
1. "登入以複製和同步"。
2. 選擇*同步 > 報告*。

每個同步關係中的路徑（來源或目標）顯示在一個表格中。

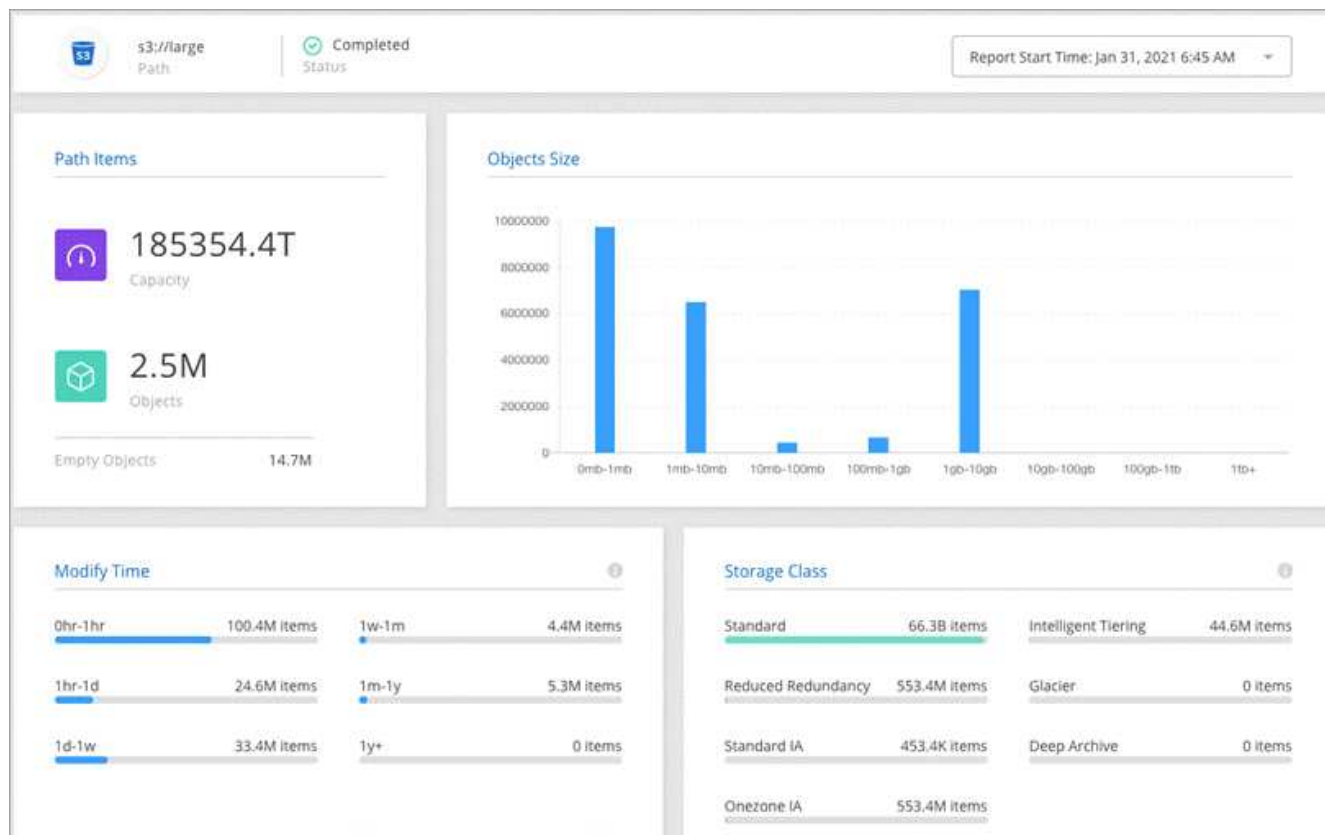
3. 在*報告操作*列中，前往特定路徑並選擇*建立*，或選擇操作選單並選擇*新建*。

4. 報告準備好後，選擇操作選單並選擇*查看*。

這是檔案系統路徑的範例報告。



這是物件儲存的範例報表。

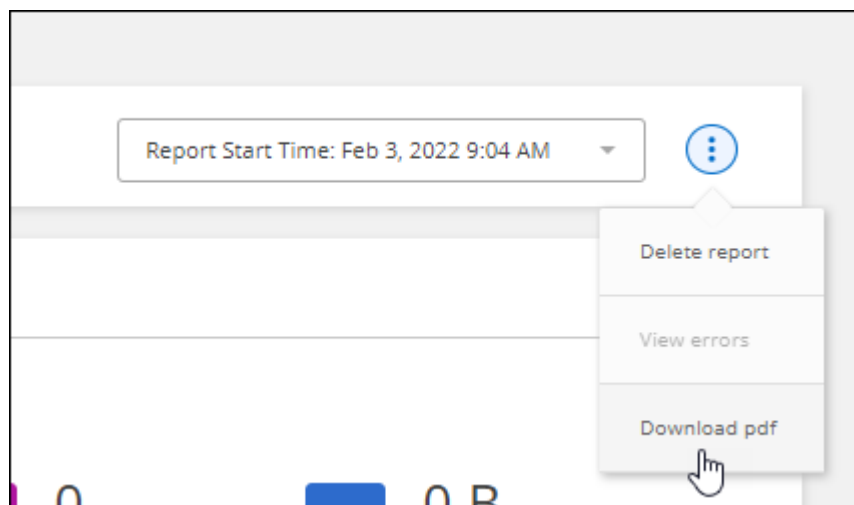


下載報告

您可以下載 PDF 格式的報告，以便離線檢視或分享。

步驟

1. "登入以複製和同步"。
2. 選擇*同步 > 報告*。
3. 在*報告操作*列中，選擇操作選單並選擇*查看*。
4. 在報告的右上角，選擇操作選單並選擇*下載 pdf*。



查看報告錯誤

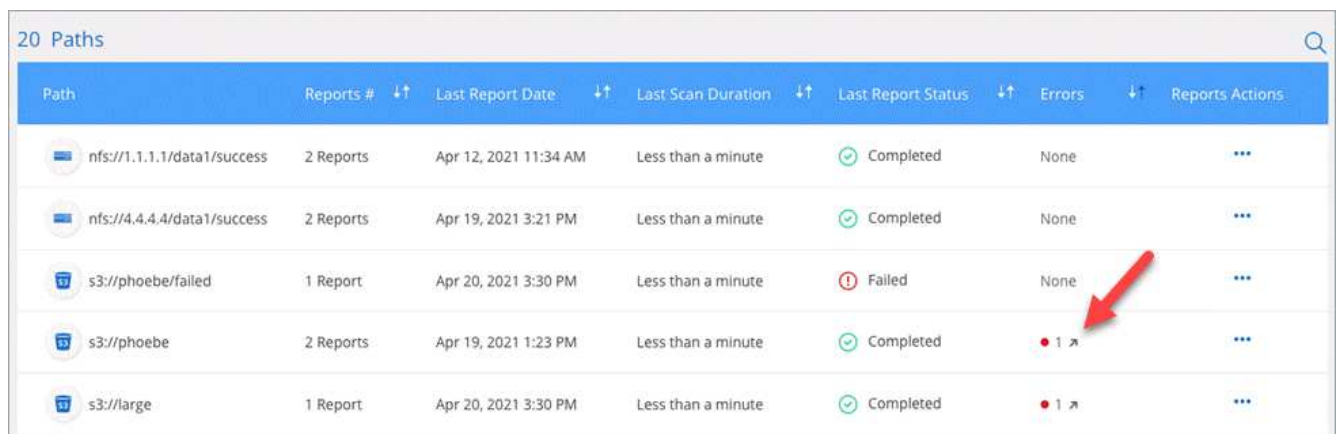
路徑表標識最新報告中是否有任何錯誤。錯誤標識了複製和同步在掃描路徑時遇到的問題。

例如，報告可能包含權限被拒絕的錯誤。此類錯誤會影響複製和同步掃描整個文件和目錄的能力。

查看錯誤清單後，您可以解決問題並再次執行報告。

步驟

1. "登入以複製和同步"。
2. 選擇*同步 > 報告*。
3. 在「錯誤」欄位中，標識報告中是否有任何錯誤。
4. 如果有錯誤，請選擇錯誤數量旁邊的箭頭。



Path	Reports #	Last Report Date	Last Scan Duration	Last Report Status	Errors	Reports Actions
nfs://1.1.1.1/data1/success	2 Reports	Apr 12, 2021 11:34 AM	Less than a minute	Completed	None	...
nfs://4.4.4.4/data1/success	2 Reports	Apr 19, 2021 3:21 PM	Less than a minute	Completed	None	...
s3://phoebe/failed	1 Report	Apr 20, 2021 3:30 PM	Less than a minute	Failed	None	...
s3://phoebe	2 Reports	Apr 19, 2021 1:23 PM	Less than a minute	Completed	1	...
s3://large	1 Report	Apr 20, 2021 3:30 PM	Less than a minute	Completed	1	...

5. 使用錯誤中的資訊來修正問題。

解決問題後，下次執行報告時就不會再出現該錯誤。

刪除報告

如果報告包含您已修復的錯誤，或報告與您已刪除的同步關係相關，您可以刪除該報告。

步驟

1. 選擇*同步 > 報告*。
2. 在*報告操作*列中，選擇路徑的操作選單，然後選擇*刪除最後一份報告*或*刪除所有報告*。
3. 確認您要刪除該報告或這些報告。

卸載NetApp Copy and Sync的資料代理

如有需要，請執行卸載腳本以刪除資料代理程式以及安裝資料代理程式時為NetApp Copy and Sync建立的軟體包和目錄。

步驟

1. 登入資料代理主機。

2. 更改資料代理目錄： /opt/netapp/databroker

3. 運行以下命令：

```
chmod +x uninstaller-DataBroker.sh  
./uninstaller-DataBroker.sh
```

4. 按“y”確認卸載。

NetApp Copy and SyncAPI

可透過 Web UI 使用的NetApp Copy and Sync功能也可透過 RESTful API 使用。

開始

要開始使用複製和同步 API，您需要取得使用者令牌和NetApp Console帳戶 ID。進行 API 呼叫時，您需要將令牌和帳戶 ID 新增至授權標頭。

步驟

1. 從NetApp Console取得使用者令牌。

```
POST https://netapp-cloud-account.auth0.com/oauth/token
Header: Content-Type: application/json
Body:
{
  "username": "<user_email>",
  "scope": "profile",
  "audience": "https://api.cloud.netapp.com",
  "client_id": "UaVhOIXMWQs5i1WdDxauXe5Mqkb34NJQ",
  "grant_type": "password",
  "password": "<user_password>"
}
```



如果您使用的是沒有客戶端 ID 的個人電子郵件帳戶，則可以使用預設用戶端 ID 「QC3AgHk6qdbmC7Yyr82ApBwaaJLwRrNO」。

2. 取得您的NetApp Console帳戶 ID。

```
GET https://api.cloudsync.netapp.com/api/accounts
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
```

此 API 將傳回以下回應：

```
[
  {
    "accountId": "account-JeL97Ry3",
    "name": "Test"
  }
]
```

3. 在每個 API 呼叫的授權標頭中新增使用者令牌和帳戶 ID。

例子

以下範例展示了在 Microsoft Azure 中建立資料代理程式的 API 呼叫。您只需將 <user_token> 和 <accountId> 替換為您在前面步驟中獲得的令牌和 ID。

```
POST https://api.cloudsync.netapp.com/api/data-brokers
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
Body: { "name": "databroker1", "type": "AZURE" }
```

下一步是什麼？

NetApp Console 中的使用者令牌有一個到期日期。若要刷新令牌，您需要再次呼叫步驟 1 中的 API。

API 回應包含一個「expires_in」字段，用於說明令牌何時過期。

使用列表 API

List API 是非同步 API，因此結果不會立即傳回（例如：GET /data-brokers/{id}/list-nfs-export-folders 和 GET /data-brokers/{id}/list-s3-buckets）。來自伺服器的唯一回應是 HTTP 狀態 202。要獲得實際結果，您必須使用 GET /messages/client API。

步驟

1. 呼叫您想要使用的清單 API。
2. 使用 GET /messages/client API 查看操作結果。
3. 使用相同的 API，並在其後附加您剛剛收到的 ID：GET
http://api.cloudsync.netapp.com/api/messages/client?last=<id_from_step_2>

請注意，每次調用 GET /messages/client API。

例子

當你撥打 'list-s3-buckets' API，結果不會立即回傳：

```
GET http://api.cloudsync.netapp.com/api/data-brokers/<data-broker-id>/list-s3-buckets
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
```

結果是 HTTP 狀態代碼 202，這表示訊息已被接受，但尚未處理。

要取得操作的結果，需要使用下列 API：

```
GET http://api.cloudsync.netapp.com/api/messages/client
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
```

結果是一個包含一個 ID 欄位的物件的陣列。ID 欄位代表伺服器傳送的最後一則訊息。例如：

```
[
  {
    "header": {
      "requestId": "init",
      "clientId": "init",
      "agentId": "init"
    },
    "payload": {
      "init": {}
    },
    "id": "5801"
  }
]
```

現在，您可以使用剛剛收到的 ID 進行以下 API 呼叫：

```
GET
http://api.cloudsync.netapp.com/api/messages/client?last=<id_from_step_2>
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
```

結果是一組訊息。每個訊息內部都有一個有效負載對象，它由操作名稱（作為鍵）及其結果（作為值）組成。例如：

```
[
  {
    "payload": {
      "list-s3-buckets": [
        {
          "tags": [
            {
              "Value": "100$",
              "Key": "price"
            }
          ],
          "region": {
            "displayName": "US West (Oregon)",
            "name": "us-west-2"
          },
          "name": "small"
        }
      ]
    },
    "header": {
      "requestId": "f687ac55-2f0c-40e3-9fa6-57fb8c4094a3",
      "clientId": "5beb032f548e6e35f4ed1ba9",
      "agentId": "5bed61f4489fb04e34a9aac6"
    },
    "id": "5802"
  }
]
```

API 參考

每個複製和同步 API 的文檔可從 <https://api.cloudsync.netapp.com/docs>。

概念

NetApp Copy and Sync許可概述

14 天免費試用期結束後，您可以透過兩種方式支付NetApp Copy and Sync關係的費用。第一個選項是從 AWS 或 Azure 訂閱按使用量付費或按年付費。第二種選擇是直接從NetApp購買許可證。

授權應透過NetApp Copy and Sync或適用網站進行管理，而非透過NetApp Console進行管理。

市場訂閱

訂閱 AWS 或 Azure 的複製和同步服務可讓您按小時付費或按年付費。["您可以透過 AWS 或 Azure 訂閱"](#)，取決於您想要在哪裡付款。



Copy and Sync 僅支援來自 **AWS** 和 **Azure** 的 Marketplace 訂閱。Copy and Sync 不支援 Google Cloud Marketplace 訂閱。

按小時訂閱

透過按小時付費訂閱，您將根據創建的同步關係數量按小時付費。

- ["查看 Azure 中的定價"](#)
- ["查看 AWS 中的按使用量付費定價"](#)

年度訂閱

年度訂閱可提供 20 個同步關係的許可證，您需要預付。如果您的同步關係超過 20 個並且已透過 AWS 訂閱，則您需要按小時支付額外的關係費用。

["查看 AWS 中的年度定價"](#)

NetApp的許可證

預先支付同步關係費用的另一種方式是直接從NetApp購買授權。每個許可證允許您創建最多 20 個同步關係。

您可以將這些授權與 AWS 或 Azure 訂閱一起使用。例如，如果您有 25 個同步關係，則可以使用授權支付前 20 個同步關係的費用，然後使用剩餘的 5 個同步關係從 AWS 或 Azure 按使用量付費。

["了解如何購買許可證並將其新增至NetApp Copy and Sync"](#)。

授權條款

購買自帶授權 (BYOL) 進行複製和同步的客戶應該了解與授權權利相關的限制。

- 客戶有權利用 BYOL 許可證，有效期限自交付之日起不超過一年。
- 客戶有權利用 BYOL 授權在來源和目標之間建立總共不超過 20 個單獨連線（每個連線稱為「同步關係」）。

- 無論客戶是否已達到 20 個同步關係的限制，客戶的權利都將在一年許可期限結束時到期。
- 如果客戶選擇續訂其許可證，則與先前的許可證授予相關的未使用的同步關係將不會延續到許可證續約。

NetApp Copy and Sync中的資料隱私

NetApp無法存取您在使用NetApp Copy and Sync時提供的任何憑證。憑證直接儲存在位於您的網路中的資料代理機器上。

根據您選擇的配置，當您建立新的關係時，「複製和同步」可能會提示您輸入憑證。例如，在設定包含 SMB 伺服器的關係時，或在 AWS 中部署資料代理程式時。

這些憑證始終直接保存到資料代理本身。資料代理程式駐留在您網路中的一台機器上，無論它是在本機還是在您的雲端帳戶中。這些憑證永遠不會提供給NetApp。

憑證使用 HashiCorp Vault 在資料代理機器上進行本機加密。

NetApp Copy and Sync技術常見問題解答

如果您只是想快速找到問題的答案，此常見問題解答可以為您提供協助。

入門

以下問題與開始使用NetApp Copy and Sync有關。

NetApp Copy and Sync如何運作？

複製並同步使用NetApp資料代理軟體將資料從來源同步到目標（這稱為_同步關係_）。

資料代理組控制來源和目標之間的同步關係。設定同步關係後，複製和同步會分析您的來源系統並將其分解為多個複製流以推送到您選擇的目標資料。

初始複製後，「複製和同步」會根據您設定的計劃同步任何變更的資料。

14 天免費試用如何進行？

當您註冊 Copy and Sync 時，14 天的免費試用期就開始了。您無需為 14 天內建立的複製和同步關係支付NetApp費用。但是，您部署的任何資料代理程式的所有資源費用仍然適用。

複製和同步的費用是多少？

使用複製和同步有兩種類型的成本：服務費和資源費。

服務費

對於按使用量付費的定價，複製和同步服務費用按小時計算，取決於您創建的同步關係的數量。

- ["查看 AWS 中的按使用量付費定價"](#)
- ["查看 AWS 中的年度定價"](#)

- ["查看 Azure 中的定價"](#)

您也可以透過NetApp代表取得複製和同步授權。每個許可證可支援 12 個月的 20 個同步關係。

["了解有關許可證的更多信息"](#)。



對於Azure NetApp Files來說，複製和同步關係是免費的。

資源費用

資源費用與在雲端中運行資料代理程式的運算和儲存成本有關。

複製和同步如何計費以及如何管理我的訂閱？

14 天免費試用期結束後，您可以透過兩種方式支付同步關係費用。第一個選項是從 AWS 或 Azure 訂閱，這樣您就可以按使用量付費或按年付費。第二種選擇是直接從NetApp購買許可證。在每種情況下，您的訂閱都將透過您的供應商市場進行管理，而不是透過複製和同步使用者介面進行管理。

我可以在雲端外使用複製和同步嗎？

是的，您可以在非雲端架構中使用複製和同步。來源和目標可以駐留在本地，資料代理軟體也可以駐留在本地。

請注意有關在雲端外使用複製和同步的以下要點：

- 數據經紀人團體需要網路連線才能與複製和同步進行通訊。
- 如果您不直接從NetApp購買許可證，則需要一個 AWS 或 Azure 帳戶來進行 PAYGO Copy and Sync 計費。

如何存取複製和同步？

可以從NetApp Console進行複製和同步。從控制台左側導覽中，選擇*移動性*>*複製和同步*。

什麼是數據經紀人團體？

每個數據經紀人都屬於數據經紀人組。將資料代理分組在一起有助於提高同步關係的效能。

支持的來源和目標

以下問題與同步關係中支援的來源和目標有關。

複製和同步支援哪些來源和目標？

複製和同步支援多種不同類型的同步關係。["查看完整列表"](#)。

複製和同步支援哪些版本的 **NFS** 和 **SMB**？

複製和同步支援 NFS 版本 3 及更高版本以及 SMB 版本 1 及更高版本。

["詳細了解同步要求"](#)。

當以 **Amazon S3** 為目標時，資料可以分層到特定的 **S3** 儲存類別嗎？

是的，當 AWS S3 是目標時，您可以選擇特定的 S3 儲存類別：

- 標準（這是預設類別）
- 智能分層
- 標準-不頻繁訪問
- 單區-不頻繁訪問
- 冰川深度檔案
- 冰川彈性檢索
- 冰川即時檢索

Azure Blob 儲存體的儲存層怎麼樣？

當 Blob 容器是目標時，您可以選擇特定的 Azure Blob 儲存層：

- 熱儲存
- 冷藏

您是否支援 **Google Cloud** 儲存層？

是的，當 Google Cloud Storage 儲存桶是目標時，您可以選擇特定的儲存類別：

- 標準
- 近線
- 涼線
- 檔案

聯網

以下問題與複製和同步的網路要求有關。

複製和同步的網路要求是什麼？

複製和同步環境要求資料代理組透過所選協定或物件儲存 API（Amazon S3、Azure Blob、IBM Cloud Object Storage）與來源和目標連接。

此外，資料代理群組需要透過連接埠 443 建立出站互聯網連接，以便與複製和同步進行通訊並聯繫其他一些服務和儲存庫。

欲了解更多詳情，["審查網路要求"](#)。

我可以將代理伺服器與資料代理一起使用嗎？

是的。

複製和同步支援有或沒有基本驗證的代理伺服器。如果在部署資料代理程式時指定代理伺服器，則來自資料代理

程式的所有 HTTP 和 HTTPS 流量都將透過代理程式路由。請注意，非 HTTP 流量（例如 NFS 或 SMB）不能透過代理伺服器路由。

唯一的代理伺服器限制是使用具有 NFS 或 Azure NetApp Files 同步關係的動態資料加密時。加密資料透過 HTTPS 傳送，無法透過代理伺服器路由。

資料同步

以下問題與資料同步的工作原理有關。

同步發生的頻率是多少？

預設計劃設定為每日同步。初始同步後，您可以：

- 將同步計劃修改為所需的天數、小時數或分鐘數
- 停用同步計劃
- 刪除同步計劃（不會遺失任何資料；只會刪除同步關係）

最小同步計劃是多少？

您可以安排每 1 分鐘同步一次資料。

當檔案同步失敗時，資料代理組是否會重試？或者它超時了嗎？

當單一檔案傳輸失敗時，資料代理組不會逾時。相反，資料代理組在跳過該檔案之前會重試 3 次。重試值可以在同步關係的設定中配置。

["了解如何變更同步關係的設置"](#)。

如果我有一個非常大的資料集怎麼辦？

如果單一目錄包含 600,000 個或更多文件，["聯絡我們"](#)以便我們可以幫助您配置資料代理組來處理有效負載。我們可能需要向資料代理組添加額外的記憶體。

請注意，掛載點中的檔案總數沒有限制。對於包含 600,000 個或更多檔案的大型目錄，無論其在層次結構中的層級（頂級目錄或子目錄）如何，都需要額外的記憶體。

安全

以下問題與安全有關。

複製和同步安全嗎？

是的。所有複製和同步網路連線均使用 ["亞馬遜簡單佇列服務 \(SQS\)"](#)。

資料代理組與 Amazon S3、Azure Blob、Google Cloud Storage 和 IBM Cloud Object Storage 之間的所有通訊均透過 HTTPS 協定完成。

如果您將複製和同步功能與本機（來源或目標）系統一起使用，則建議使用以下幾個連線選項：

- AWS Direct Connect、Azure ExpressRoute 或 Google Cloud Interconnect 連接，非互聯網路由（且只能與您指定的雲端網路通訊）
- 本地網關設備與雲端網路之間的 VPN 連接
- 為了使用 S3 儲存桶、Azure Blob 儲存體或 Google Cloud Storage 進行額外的安全資料傳輸，可以建立 Amazon Private S3 Endpoint、Azure Virtual Network 服務端點或 Private Google Access。

這些方法中的任何一種都會在您的本機 NAS 伺服器和複製和同步資料代理群組之間建立安全連線。

複製和同步是否加密資料？

- 複製和同步支援來源和目標 NFS 伺服器之間的資料傳輸加密。["了解更多"](#)。
- 對於 SMB，複製和同步支援您在伺服器端加密的 SMB 3.0 和 3.11 資料。複製和同步將加密資料從來源複製到目標，資料在目標中保持加密狀態。

複製和同步本身無法加密 SMB 資料。

- 當 Amazon S3 儲存桶是同步關係中的目標時，您可以選擇使用 AWS KMS 加密或 AES-256 加密來啟用資料加密。
- 當 Google 儲存桶是同步關係中的目標時，您可以選擇使用預設的 Google 管理的加密金鑰還是您自己的 KMS 金鑰。

權限

以下問題與資料權限有關。

SMB 資料權限是否同步到目標位置？

您可以設定複製和同步以保留來源 SMB 共用和目標 SMB 共用之間以及從來源 SMB 共用到物件儲存（ONTAP S3 除外）的存取控制清單 (ACL)。



複製和同步不支援將 ACL 從物件儲存複製到 SMB 共用。

["了解如何在 SMB 共用之間複製 ACL"](#)。



Copy Sync 會複製 SMB ACL（權限），但不會複製檔案或資料夾的擁有權。SMB ACL 複製作業不包含所有權屬性。如果在 SMB 共用之間複製資料時需要保留所有權，請使用 `robocopy` 手動複製安全資訊。例如，`/copyall` 標記副本 ACL、所有者和審計資料。

NFS 資料權限是否同步到目標位置？

複製和同步會自動在 NFS 伺服器之間複製 NFS 權限，如下所示：

- NFS 版本 3：複製和同步複製權限和使用者群組擁有者。
- NFS 版本 4：複製和同步複製 ACL。

物件儲存元數據

哪些類型的同步關係可以保留物件儲存元資料？

複製和同步將物件儲存元資料從來源複製到目標，以實現以下類型的同步關係：

- 亞馬遜 S3 → 亞馬遜 S3 ¹
- Amazon S3 → StorageGRID
- StorageGRID → Amazon S3
- StorageGRID → StorageGRID
- StorageGRID → Google 雲端存儲
- Google 雲端儲存 → StorageGRID ¹
- Google 雲端儲存 → IBM 雲端物件儲存 ¹
- Google 雲端儲存 → Amazon S3 ¹
- 亞馬遜 S3 → 谷歌雲端存儲
- IBM 雲端物件儲存 → Google 雲端存儲
- StorageGRID → IBM 雲端物件存儲
- IBM 雲端物件儲存 → StorageGRID
- IBM 雲端物件儲存 → IBM 雲端物件存儲

¹ 對於這些同步關係，您需要["建立同步關係時啟用「物件複製」設置"](#)。

在以 **NFS** 或 **SMB** 為來源的同步過程中，會複製哪些類型的元資料？

預設會複製使用者 ID、修改時間、存取時間和 GID 等元資料。使用者可以在建立同步關係時將其標記為必需，從而選擇從 CIF 複製 ACL。

表現

以下問題與複製和同步效能有關。

同步關係的進度指示器代表什麼？

同步關係顯示資料代理組網路適配器的吞吐量。如果您使用多個資料代理來加速同步效能，那麼吞吐量就是所有流量的總和。此吞吐量每 20 秒刷新一次。

我遇到了效能問題。我們可以限制並發傳輸的數量嗎？

如果您有非常大的檔案（每個檔案有多個 TiB），則完成傳輸過程可能需要很長時間，並且效能可能會受到影響。

限制並發傳輸的數量可能會有所幫助。["聯絡我們尋求協助"](#)。

為什麼我的**Azure NetApp Files**效能低？

當您將資料同步至Azure NetApp Files或從 Azure NetApp Files 同步資料時，如果磁碟服務等級為標準，則可能會遇到故障和效能問題。

將服務等級變更為 Premium 或 Ultra 以增強同步效能。

["詳細了解 Azure NetApp Files 服務等級與吞吐量"](#)。

一個集團需要多少個數據經紀人？

當您建立新的關係時，您會從群組中的單一資料代理程式開始（除非您選擇了屬於加速同步關係的現有資料代理程式）。在許多情況下，單一資料代理程式可以滿足同步關係的效能要求。如果沒有，您可以透過向群組中新增額外的資料代理程式來加速同步效能。但您應該先檢查可能影響同步效能的其他因素。

多種因素會影響資料傳輸效能。整體同步效能可能會受到網路頻寬、延遲和網路拓撲以及資料代理 VM 規格和儲存系統效能的影響。例如，一個群組中的單一資料代理程式可以達到 100 MB/s，而目標上的磁碟吞吐量可能只允許 64 MB/s。結果，數據經紀商集團不斷嘗試複製數據，但目標無法滿足數據經紀商集團的表現。

因此，請務必檢查網路效能和目標磁碟吞吐量。

然後，您可以考慮透過在群組中新增額外的資料代理來分擔該關係的負載，從而加速同步效能。["了解如何加速同步效能"](#)。

刪除內容

以下問題與從來源和目標刪除同步關係和資料有關。

如果我刪除複製和同步關係會發生什麼？

刪除關係將停止所有未來的資料同步並終止付款。同步到目標的任何資料都保持原樣。

如果我從來源伺服器中刪除某些內容會發生什麼？它也從目標中移除了嗎？

預設情況下，如果您具有活動的同步關係，則在來源伺服器上刪除的項目不會在下次同步期間從目標伺服器上刪除。但是每個關係的同步設定中都有一個選項，您可以在其中定義如果從來源中刪除了文件，則複製和同步將刪除目標位置中的文件。

["了解如何變更同步關係的設置"](#)。

如果我從目標中刪除某些內容會發生什麼？它也從我的來源中刪除了嗎？

如果從目標中刪除某個項目，則它不會從來源中刪除。這種關係是單向的—從源頭到目標。在下一個同步週期中，「複製和同步」會將來源與目標進行比較，識別出該項目缺失，然後「複製和同步」會再次將其從來源複製到目標。

故障排除

["NetApp 知識庫：複製與同步常見問題：支援與故障排除"](#)

數據經紀人深度探究

以下問題與數據經紀人有關。

您能解釋一下數據代理的架構嗎？

當然。以下是最重要的幾點：

- 資料代理程式是在 Linux 主機上執行的 node.js 應用程式。
- Copy and Sync 如下部署資料代理程式：
 - AWS：來自 AWS CloudFormation 模板
 - Azure：來自 Azure 資源管理器
 - Google：來自 Google Cloud Deployment Manager
 - 如果使用自己的Linux主機，則需要手動安裝軟體
- 數據代理軟體會自動升級到最新版本。
- 資料代理程式使用 AWS SQS 作為可靠、安全的通訊管道並用於控制和監控。SQS 也提供了持久層。
- 您可以為群組中新增額外的資料代理程式以提高傳輸速度並增加高可用性。如果一個資料代理發生故障，則服務具有彈性。

知識和支持

註冊以獲得支持

需要進行支援註冊才能獲得針對NetApp Console及其儲存解決方案和資料服務的技術支援。還需要支援註冊才能啟用Cloud Volumes ONTAP系統的關鍵工作流程。

註冊支援並不能使NetApp獲得雲端提供者文件服務的支援。有關雲端提供者文件服務、其基礎設施或使用該服務的任何解決方案的技術支持，請參閱該產品文件中的「取得協助」。

- ["適用於ONTAP 的Amazon FSx"](#)
- ["Azure NetApp Files"](#)
- ["Google Cloud NetApp Volumes"](#)

支援註冊概述

啟動支持權利的註冊方式有兩種：

- 註冊您的NetApp Console帳戶序號（您的 20 位元 960xxxxxxxx 序號位於控制台中的「支援資源」頁面上）。

這可作為控制台內任何服務的單一支援訂閱 ID。每個控制台帳戶都必須註冊。

- 在您的雲端供應商市場中註冊與訂閱相關的Cloud Volumes ONTAP序號（這些是 20 位元 909201xxxxxxxx 序號）。

這些序號通常稱為_PAYGO 序號_，由NetApp Console在Cloud Volumes ONTAP部署時產生。

註冊兩種類型的序號可以實現開立支援票和自動產生案例等功能。透過將NetApp支援網站 (NSS) 帳戶新增至控制台即可完成註冊，如下所述。

註冊NetApp Console以取得NetApp支持

要註冊支援並啟動支援權利，您的NetApp Console帳戶中的一名使用者必須將NetApp支援網站帳戶與其控制台登入名稱關聯。如何註冊NetApp支援取決於您是否已經擁有NetApp支援網站 (NSS) 帳號。

擁有 NSS 帳戶的現有客戶

如果您是擁有 NSS 帳戶的NetApp客戶，只需透過控制台註冊即可獲得支援。

步驟

1. 選擇“管理”>“憑證”。
2. 選擇*使用者憑證*。
3. 選擇*新增 NSS 憑證*並依照NetApp支援網站 (NSS) 驗證提示進行操作。
4. 若要確認註冊過程是否成功，請選擇「幫助」圖標，然後選擇「支援」。

*資源*頁面應顯示您的控制台帳戶已註冊以獲得支援。

請注意，如果其他控制台使用者尚未將NetApp支援網站帳戶與其登入名稱關聯，他們將看不到相同的支援註冊狀態。但是，這並不意味著您的帳戶沒有註冊支援。只要組織中的一名使用者遵循了這些步驟，您的帳戶就已註冊。

現有客戶但沒有 NSS 帳戶

如果您是現有的NetApp客戶，擁有現有授權和序號但沒有 NSS 帳戶，則需要建立 NSS 帳戶並將其與您的控制台登入關聯。

步驟

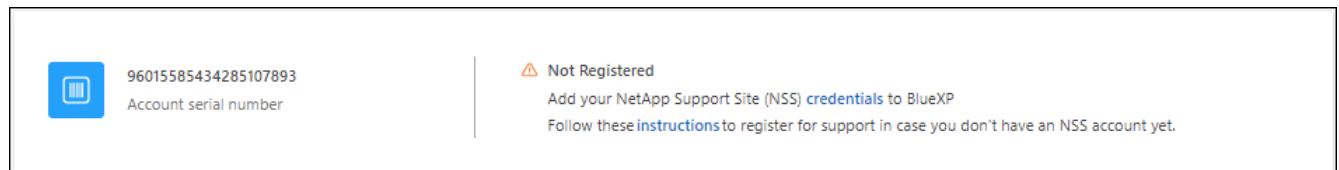
1. 透過完成以下操作建立NetApp支援網站帳戶 "[NetApp支援網站使用者註冊表](#)"
 - a. 請務必選擇適當的使用者級別，通常為* NetApp客戶/最終使用者*。
 - b. 請務必複製上面用於序號欄位的控制台帳戶序號（960xxxx）。這將加快帳戶處理速度。
2. 完成以下步驟，將您的新 NSS 帳戶與您的控制台登入名稱關聯。[擁有 NSS 帳戶的現有客戶](#)。

NetApp全新產品

如果您是NetApp新使用者且沒有 NSS 帳戶，請依照下列步驟操作。

步驟

1. 在控制台的右上角，選擇「幫助」圖標，然後選擇「支援」。
2. 從支援註冊頁面找到您的帳戶 ID 序號。



3. 導航至 "[NetApp 的支援註冊網站](#)"並選擇*我不是註冊的NetApp客戶*。
4. 填寫必填欄位（帶有紅色星號的欄位）。
5. 在*產品線*欄位中，選擇*雲端管理員*，然後選擇適用的計費提供者。
6. 從上面的步驟 2 複製您的帳戶序號，完成安全性檢查，然後確認您已閱讀 NetApp 的全球資料隱私政策。

一封電子郵件會立即發送到提供的郵箱以完成此安全交易。如果幾分鐘內沒有收到驗證電子郵件，請務必檢查您的垃圾郵件資料夾。

7. 從電子郵件中確認操作。

確認向NetApp提交您的請求並建議您建立NetApp支援網站帳戶。

8. 透過完成以下操作建立NetApp支援網站帳戶 "[NetApp支援網站使用者註冊表](#)"
 - a. 請務必選擇適當的使用者級別，通常為* NetApp客戶/最終使用者*。
 - b. 請務必複製上面用於序號欄位的帳戶序號（960xxxx）。這將加快處理速度。

完成後

NetApp應該在過程中與您聯繫。這是針對新用戶的一次性入職培訓。

擁有NetApp支援網站帳號後，請依照下列步驟將該帳號與您的控制台登入關聯擁有 NSS 帳戶的現有客戶。

關聯 NSS 憑證以獲得Cloud Volumes ONTAP支持

需要將NetApp支援網站憑證與您的控制台帳戶關聯，才能為Cloud Volumes ONTAP啟用以下關鍵工作流程：

- 註冊即用即付Cloud Volumes ONTAP系統以獲得支持

需要提供您的 NSS 帳戶才能啟動對您的系統的支援並獲得NetApp技術支援資源的存取權限。

- 自帶授權 (BYOL) 時部署Cloud Volumes ONTAP

需要提供您的 NSS 帳戶，以便控制台可以上傳您的許可證金鑰並啟用您購買的期限的訂閱。這包括期限續訂的自動更新。

- 將Cloud Volumes ONTAP軟體升級至最新版本

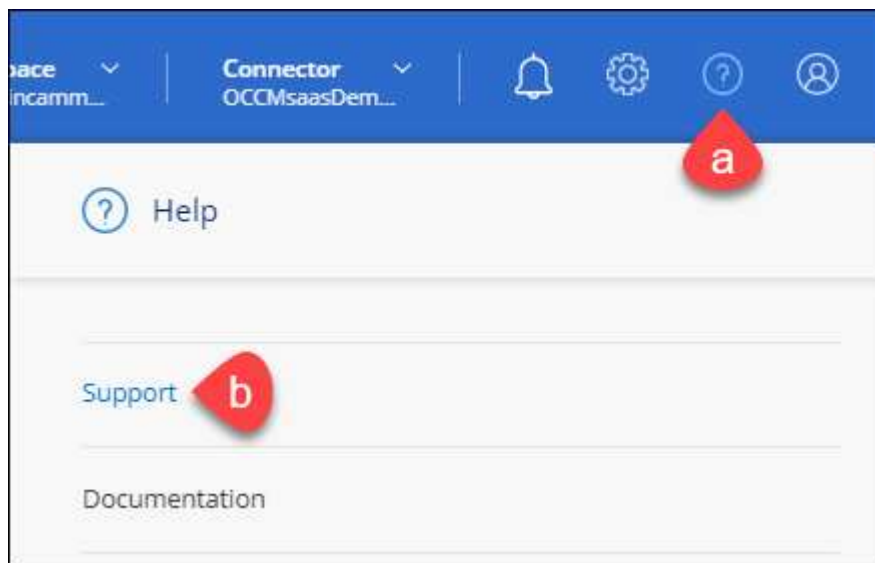
將 NSS 憑證與您的NetApp Console帳戶關聯與將 NSS 帳戶與控制台使用者登入相關聯。

這些 NSS 憑證與您的特定控制台帳戶 ID 相關聯。屬於控制台組織的使用者可以從*支援 > NSS 管理*存取這些憑證。

- 如果您有客戶級帳戶，則可以新增一個或多個 NSS 帳戶。
- 如果您有合作夥伴或經銷商帳戶，則可以新增一個或多個 NSS 帳戶，但不能與客戶級帳戶一起新增。

步驟

1. 在控制台的右上角，選擇「幫助」圖標，然後選擇「支援」。



2. 選擇*NSS 管理 > 新增 NSS 帳號*。
3. 當出現提示時，選擇「繼續」以重新導向至 Microsoft 登入頁面。

NetApp使用 Microsoft Entra ID 作為特定於支援和授權的身份驗證服務的身份提供者。

4. 在登入頁面，提供您的NetApp支援網站註冊的電子郵件地址和密碼以執行驗證程序。

這些操作使控制台能夠使用您的 NSS 帳戶進行許可證下載、軟體升級驗證和未來支援註冊等操作。

請注意以下事項：

- NSS 帳戶必須是客戶級帳戶（不是訪客或臨時帳戶）。您可以擁有多個客戶級 NSS 帳戶。
- 如果該帳戶是合作夥伴等級帳戶，則只能有一個 NSS 帳戶。如果您嘗試新增客戶級 NSS 帳戶且合作夥伴級帳戶已存在，您將收到以下錯誤訊息：

“此帳戶不允許使用 NSS 客戶類型，因為已經存在不同類型的 NSS 用戶。”

如果您已有客戶級 NSS 帳戶並嘗試新增合作夥伴級帳戶，情況也是如此。

- 成功登入後，NetApp將儲存 NSS 使用者名稱。

這是系統產生的映射到您的電子郵件的 ID。在*NSS 管理*頁面上，您可以顯示來自  菜單。

- 如果您需要刷新登入憑證令牌，還有一個*更新憑證*選項  菜單。

使用此選項會提示您再次登入。請注意，這些帳戶的令牌將在 90 天後過期。我們將發布通知來提醒您此事。

獲取協助

NetApp以多種方式為BlueXP及其雲端服務提供支援。我們提供全天候 (24/7) 的大量免費自助支援選項，例如知識庫 (KB) 文章和社群論壇。您的支援註冊包含透過網路工單取得的遠端技術支援。

獲取雲端提供者文件服務的支持

有關雲端提供者文件服務、其基礎設施或使用該服務的任何解決方案的技術支持，請參閱該產品的BlueXP文件中的「取得協助」。

- ["適用於ONTAP 的Amazon FSx"](#)
- ["Azure NetApp Files"](#)
- ["Google Cloud NetApp Volumes"](#)

要獲得針對BlueXP及其儲存解決方案和服務的技術支持，請使用下面所述的支援選項。

使用自助選項

這些選項每週 7 天、每天 24 小時免費提供：

- 文件

您目前正在檢視的BlueXP文件。

- ["知識庫"](#)

搜尋BlueXP知識庫以尋找有助於解決問題的文章。

- ["社群"](#)

加入BlueXP社群以關注正在進行的討論或創建新的討論。

向NetApp支援建立案例

除了上述自助支援選項之外，您還可以在啟動支援後與NetApp支援專家合作解決任何問題。

開始之前

- 若要使用「建立案例」功能，您必須先將您的NetApp支援網站憑證與您的BlueXP登入名稱關聯。 ["了解如何管理與BlueXP登入相關的憑證"](#)。
- 如果您要為具有序號的ONTAP系統開啟案例，那麼您的 NSS 帳戶必須與該系統的序號相關聯。

步驟

1. 在BlueXP中，選擇 幫助 > 支持。
2. 在「資源」頁面上，選擇「技術支援」下的可用選項之一：
 - a. 如果您想透過電話與某人交談，請選擇「致電我們」。您將被引導至 netapp.com 上的一個頁面，其中列出了您可以撥打的電話號碼。
 - b. 選擇「建立案例」向NetApp支援專家開立票據：
 - 服務：選擇與問題相關的服務。例如， BlueXP專門針對服務中的工作流程或功能的技術支援問題。
 - 工作環境：如果適用於存儲，請選擇* Cloud Volumes ONTAP* 或 **On-Prem**，然後選擇相關的工作環境。

工作環境清單屬於您在服務頂部橫幅中所選的BlueXP組織（或帳戶）、專案（或工作區）和連接器的範圍內。
 - 個案優先級：選擇個案的優先級，可以是低、中、高或嚴重。

要了解有關這些優先事項的更多詳細信息，請將滑鼠懸停在欄位名稱旁邊的資訊圖示上。
 - 問題描述：提供問題的詳細描述，包括任何適用的錯誤訊息或您執行的故障排除步驟。
 - 其他電子郵件地址：如果您想讓其他人知道此問題，請輸入其他電子郵件地址。
 - 附件（選購）：一次最多上傳五個附件。

每個附件檔案大小限制為 25 MB。支援以下檔案副檔名：txt、log、pdf、jpg/jpeg、rtf、doc/docx、xls/xlsx 和 csv。

ntapitdemo 

NetApp Support Site Account

Service

Select ▼

Working Enviroment

Select ▼

Case Priority 

Low - General guidance ▼

Issue Description

Provide detailed description of problem, applicable error messages and troubleshooting steps taken.

Additional Email Addresses (Optional) 

Type here

Attachment (Optional)

No files selected

 Upload 

完成後

將會出現一個彈出窗口，其中顯示您的支援案例編號。NetApp支援專家將審查您的案例並儘快回覆您。

若要查看支援案例的歷史記錄，您可以選擇*設定>時間軸*並尋找名為「建立支援案例」的操作。最右邊的按鈕可讓您展開操作以查看詳細資訊。

嘗試建立案例時，您可能會遇到以下錯誤訊息：

“您無權針對所選服務建立案例”

此錯誤可能表示 NSS 帳戶及其關聯的記錄公司與BlueXP帳戶序號的記錄公司不是同一家（即。960xxxx）或工作環境序號。您可以使用以下選項之一尋求協助：

- 使用產品內聊天
- 提交非技術案例 <https://mysupport.netapp.com/site/help>

管理您的支援案例（預覽）

您可以直接從BlueXP查看和管理活動和已解決的支援案例。您可以管理與您的 NSS 帳戶和公司相關的案例。

案例管理目前可作為預覽版。我們計劃在即將發布的版本中完善這種體驗並增加增強功能。請使用產品內聊天向我們發送回饋。

請注意以下事項：

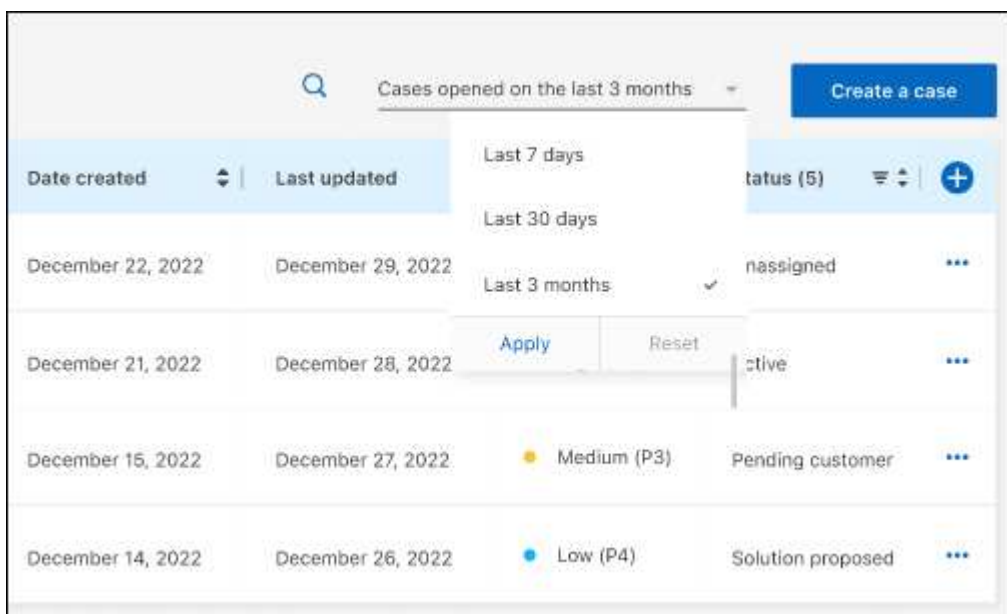
- 頁面頂部的案例管理儀表板提供兩種視圖：
 - 左側視圖顯示了您提供的使用者 NSS 帳戶在過去 3 個月內開啟的案件總數。
 - 右側的視圖根據您的使用者 NSS 帳戶顯示了過去 3 個月內貴公司層級開設的案件總數。表中的結果反映了與您選擇的視圖相關的案例。
 - 您可以新增或刪除感興趣的列，並且可以過濾優先順序和狀態等列的內容。其他欄位僅提供排序功能。
- 請查看以下步驟以了解更多詳細資訊。
- 在每個案件級別，我們提供更新案件記錄或關閉尚未關閉或待關閉狀態的案件的機能。

步驟

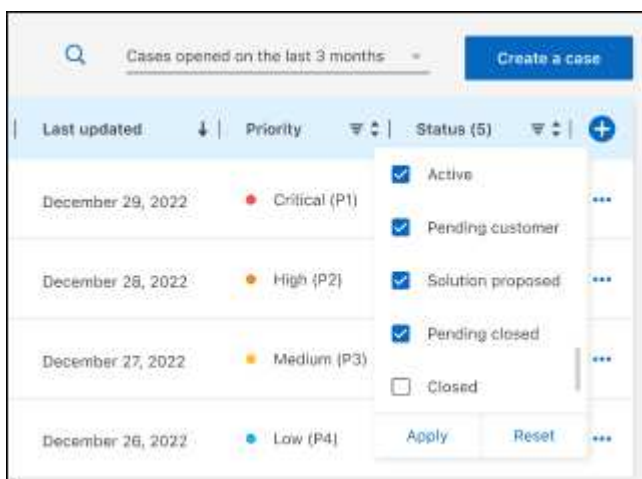
1. 在BlueXP中，選擇 幫助 > 支持。
2. 選擇*案例管理*，如果出現提示，請將您的 NSS 帳戶新增至BlueXP。

案例管理*頁面顯示與您的BlueXP使用者帳戶相關的 NSS 帳戶相關的未結案例。這與出現在 *NSS 管理 頁面頂部的 NSS 帳戶相同。

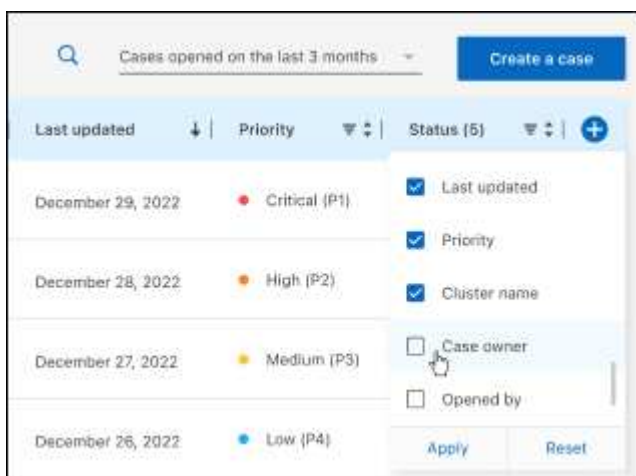
3. （可選）修改表中顯示的資訊：
 - 在「組織的案例」下，選擇「查看」以查看與您的公司相關的所有案例。
 - 透過選擇精確的日期範圍或選擇不同的時間範圍來修改日期範圍。



- 過濾列的內容。



- 透過選擇  然後選擇您想要顯示的列。



4. 透過選擇管理現有案例並選擇其中一個可用選項：

- 查看案例：查看有關特定案例的完整詳細資訊。
- 更新案例說明：提供有關您的問題的更多詳細信息，或選擇*上傳文件*以附加最多五個文件。

每個附件檔案大小限制為 25 MB。支援以下檔案副檔名：txt、log、pdf、jpg/jpeg、rtf、doc/docx、xls/xlsx 和 csv。

- 結案：提供有關結案原因的詳細信息，然後選擇*結案*。

ed on the last 30 days

Create a case

Priority	Status	
Critical (P1)	Active	...
High (P2)	Active	...
Medium (P3)	Pe	View case Update case notes Close case
Low (P4)	So	
Low (P4)	Closed	...

法律聲明

法律聲明提供對版權聲明、商標、專利等的存取。

版權

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

商標

NETAPP、NETAPP 標誌和NetApp商標頁面上列出的標誌是NetApp, Inc. 的商標。其他公司和產品名稱可能是其各自所有者的商標。

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

專利

NetApp擁有的專利的最新清單可在以下位置找到：

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

隱私權政策

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

開源

通知文件提供有關NetApp軟體中使用的第三方版權和許可的資訊。

["NetApp Copy and Sync通知"](#)

版權資訊

Copyright © 2025 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。