在來源和目標之間同步數據

NetApp Copy and Sync

NetApp
December 16, 2025

目錄

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

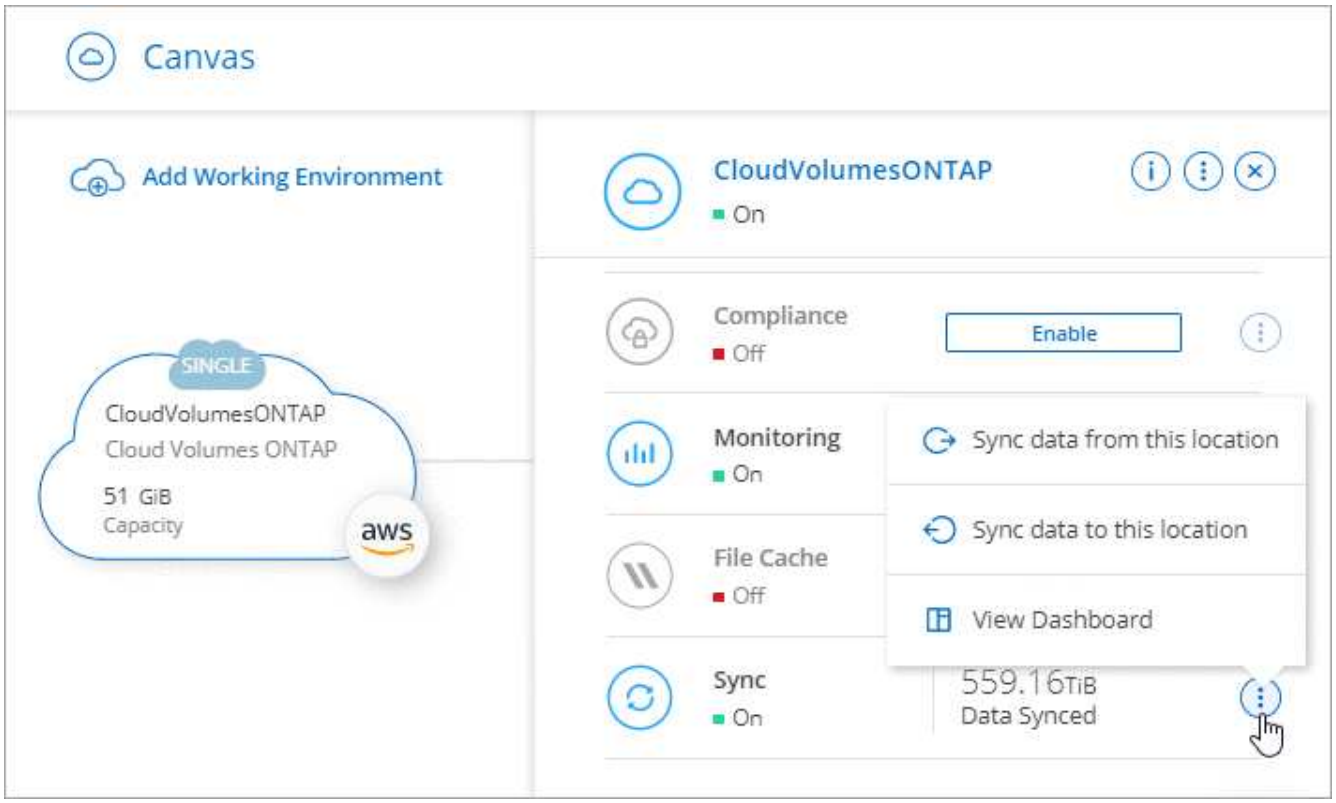
如果您想要為以下任何一項建立同步關係，那麼您首先需要建立或發現系統：

- 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。

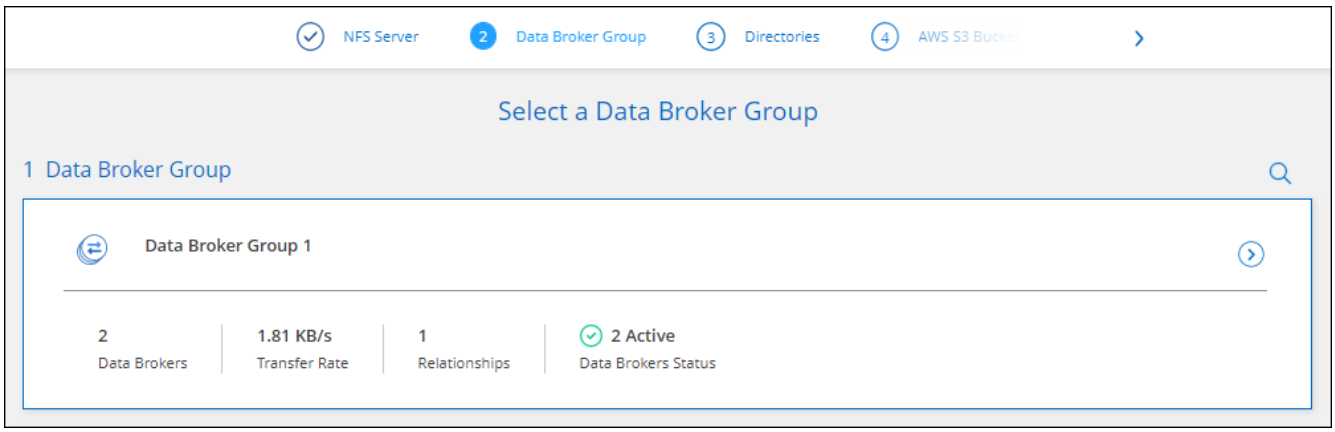
3. 在 **NFS** 伺服器 頁面上，輸入要同步到 AWS 的 NFS 伺服器的 IP 位址或完全限定網域名稱。
4. 在*資料代理群組*頁面上，依照指示在 AWS、Azure 或 Google Cloud Platform 中建立資料代理虛擬機，或在現有的 Linux 主機上安裝資料代理軟體。

   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*。

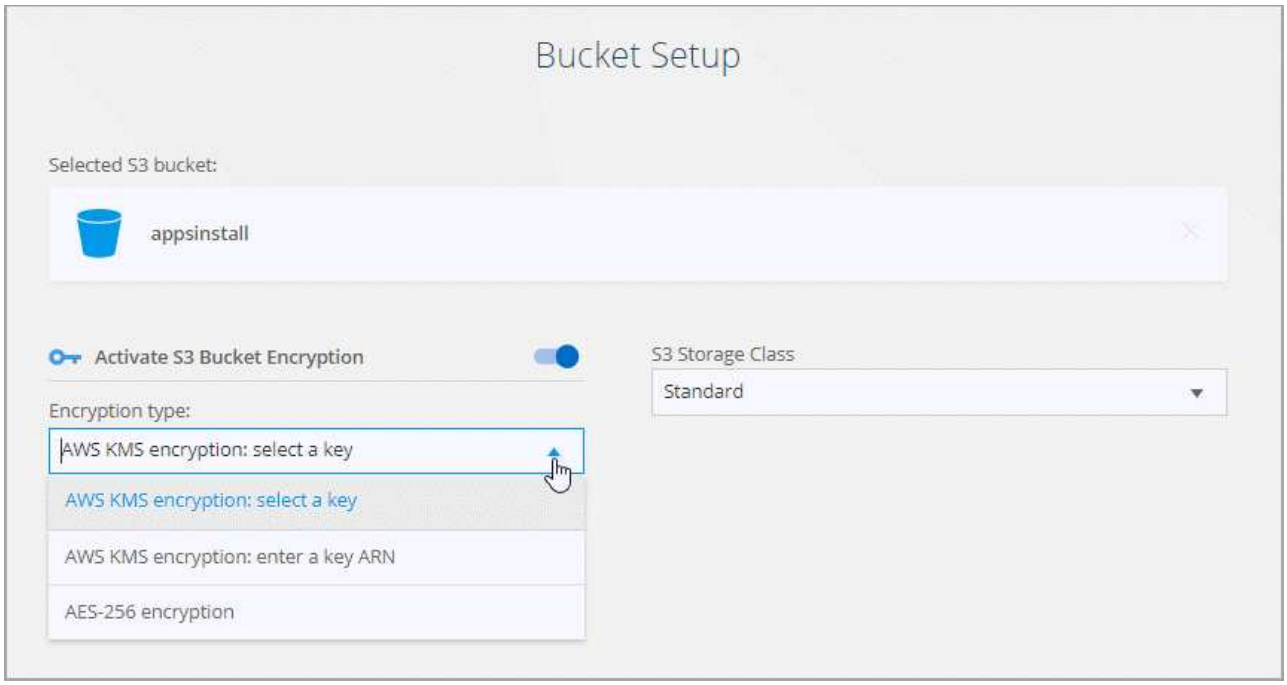


6. 在*目錄*頁面上，選擇頂級目錄或子目錄。

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。

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：

i. 前往外部儲存桶專案的 Google Cloud 控制台。

ii. 前往*雲端儲存>設定>雲端儲存服務帳戶*。

iii. 更新 local.json 檔案：

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

iv. 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。

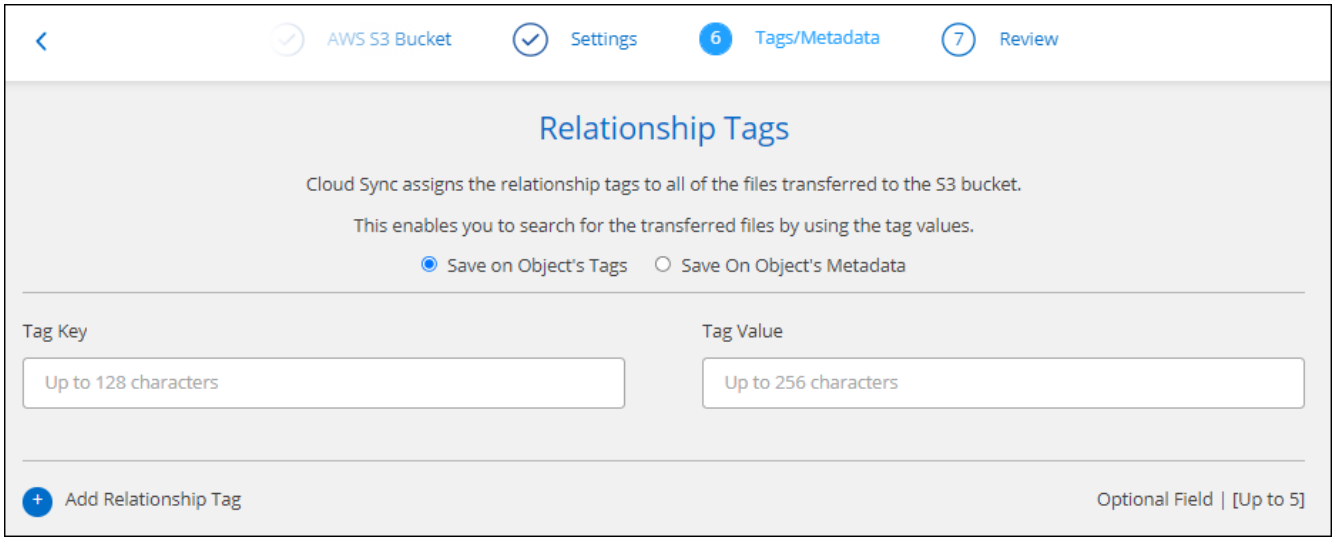
建立日期

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。



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*。

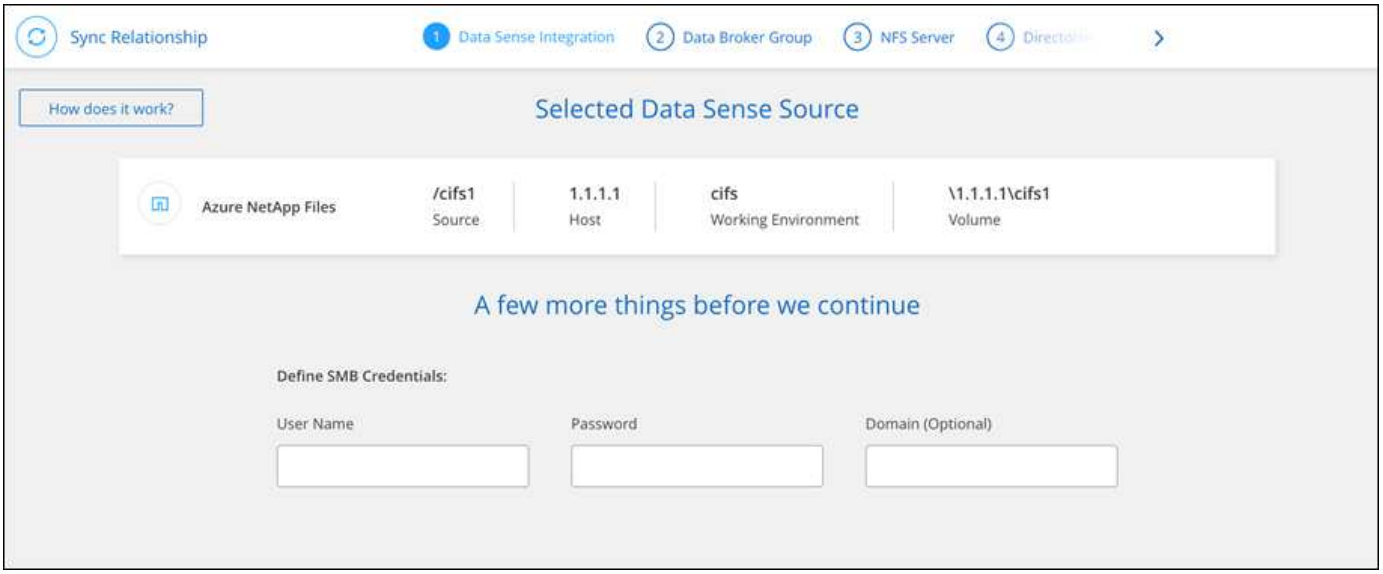
結果

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

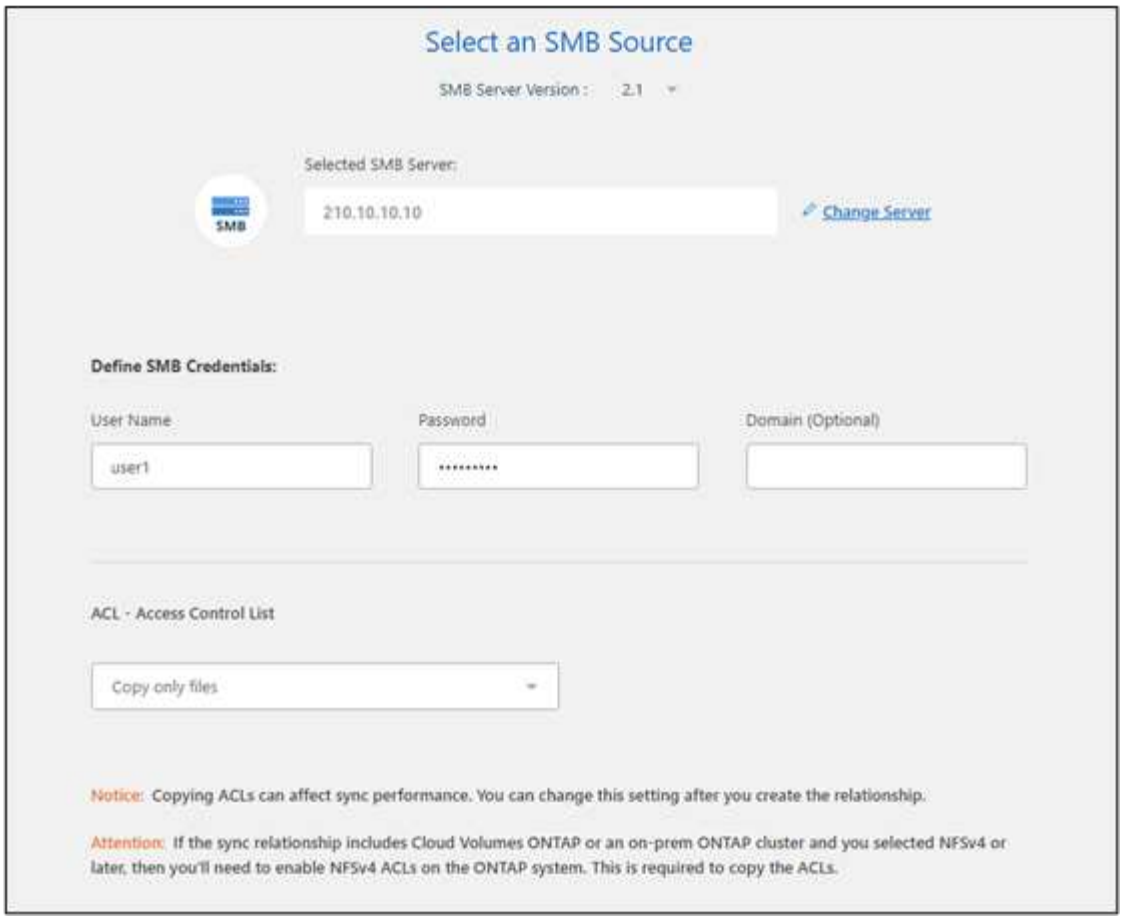
透過在建立關係時或建立關係後啟用設置，在 SMB 共用之間以及 SMB 共用和物件儲存之間複製 ACL。

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*。



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。

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>

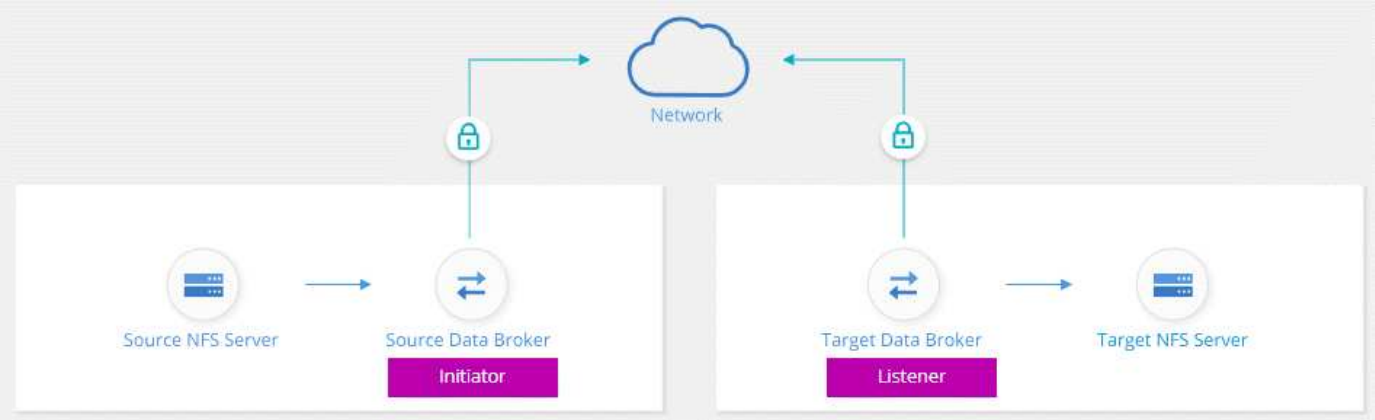
使用**NetApp Copy and Sync**中的資料傳輸加密同步 **NFS** 數據

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。

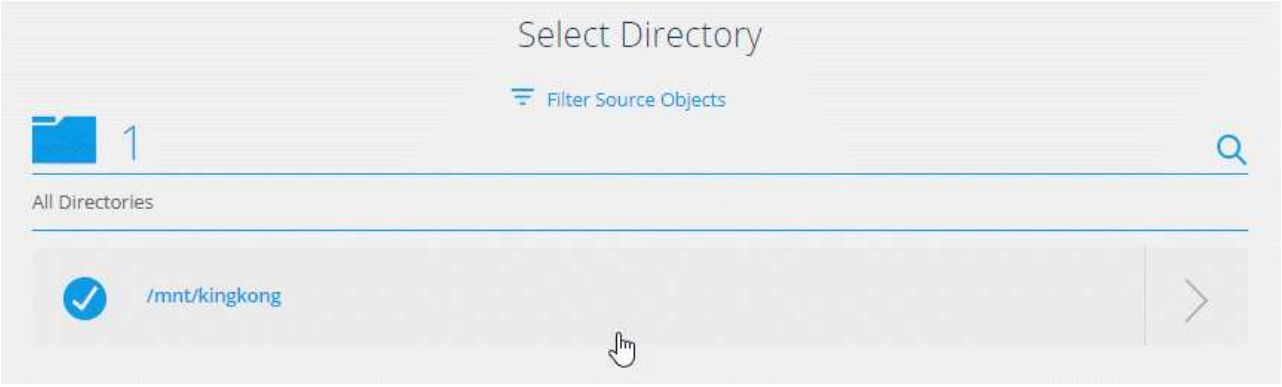
    c. 資料代理：依照提示新增新的來源資料代理程式或選擇現有的資料代理程式。

    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。

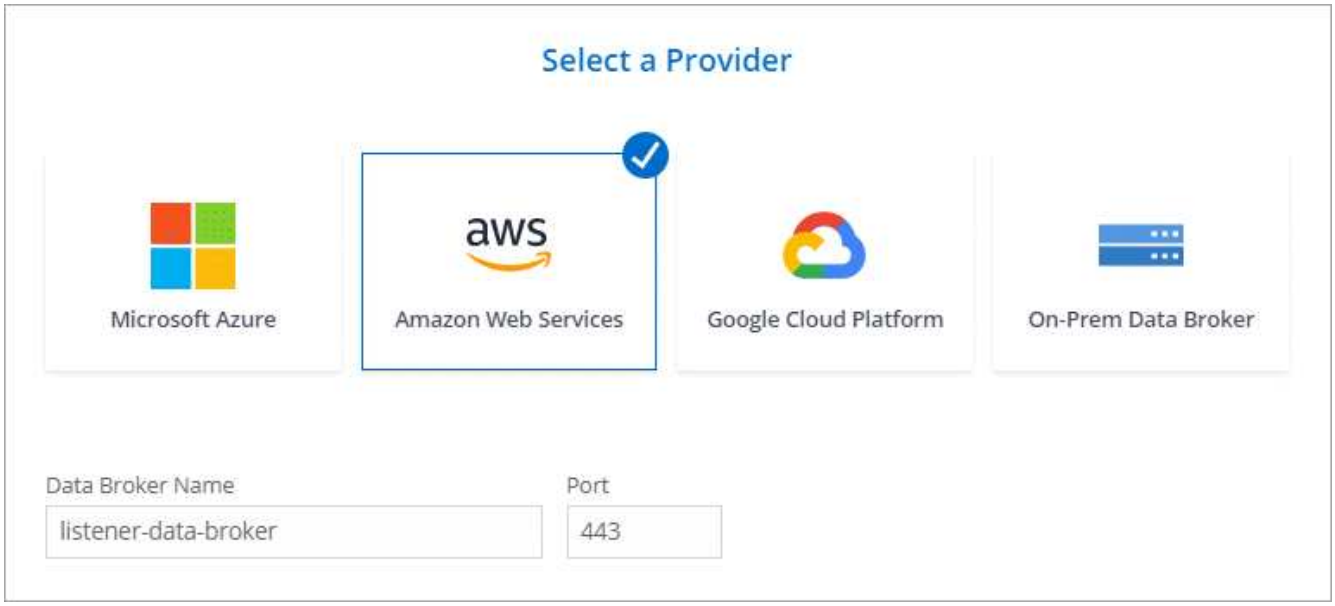


e. 目標 **NFS** 伺服器/目標**Azure NetApp Files**：選擇 NFS 版本，然後輸入新的 NFS 目標或選擇現有伺服器。

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。

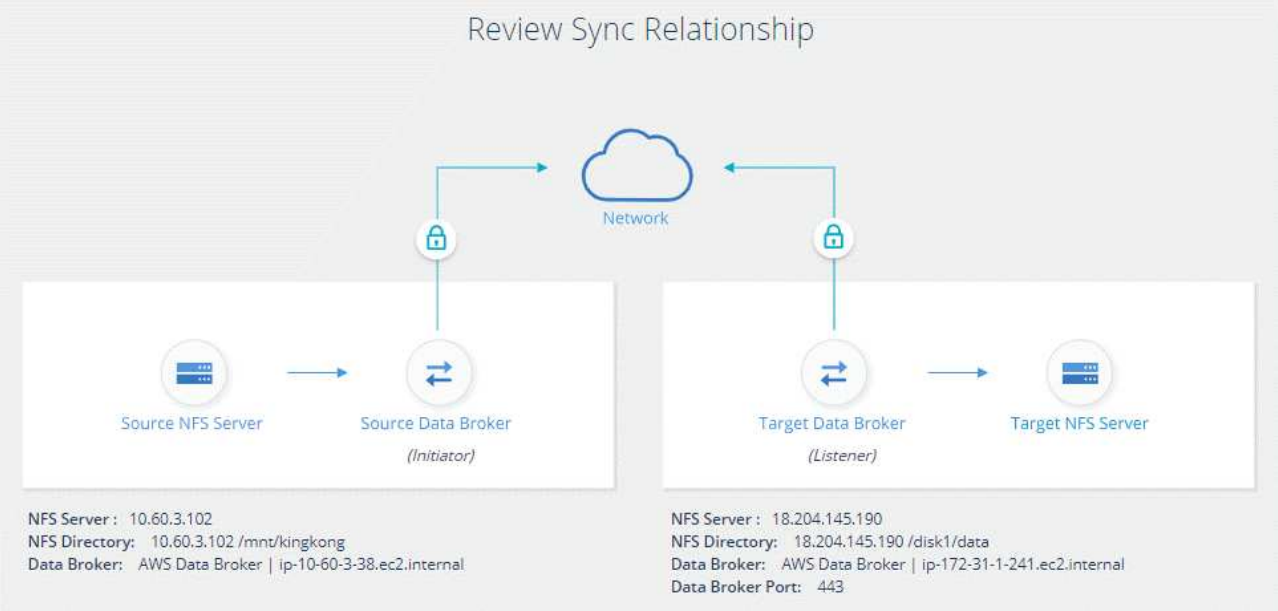
以下是目標資料代理程式作為監聽器時的提示範例。注意指定連接埠的選項。



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*在儀表板中查看*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"
        }
    }
}
```

版權資訊

商標資訊