在來源與目標之間同步資料

Cloud Sync

NetApp
June 13, 2022

目錄

在來源與目標之間同步資料

建立同步關係

當您建立同步關係時、 Cloud Sync SyndService 會將檔案從來源複製到目標。初始複本之後、服務會每 24 小時同步所有變更的資料。

在建立某些類型的同步關係之前、您首先需要在Cloud Manager中建立工作環境。

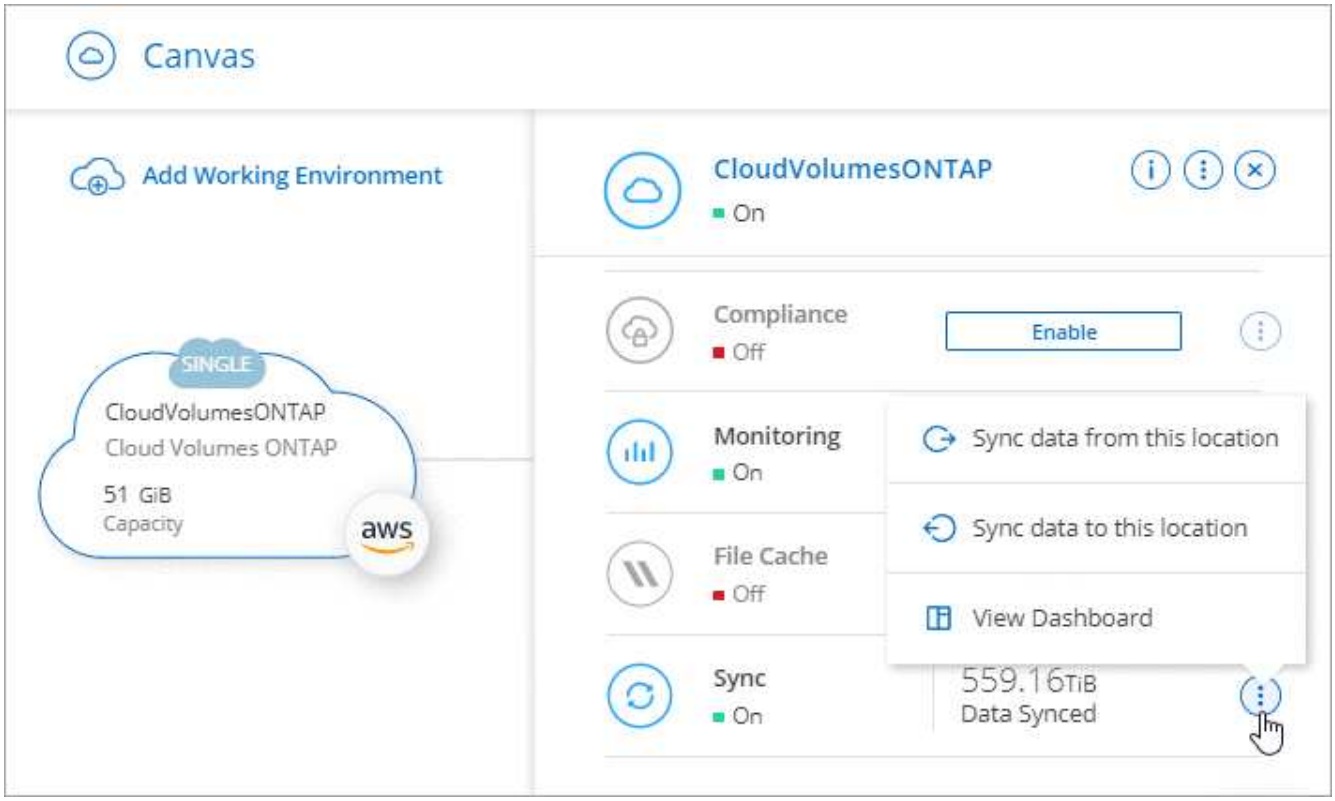
針對特定類型的工作環境建立同步關係

如果您想為下列任一項目建立同步關係、則首先需要建立或探索工作環境：

- Amazon FSX for ONTAP Sf
- Azure NetApp Files
- Cloud Volumes ONTAP
- 內部 ONTAP 部署的叢集

步驟

1. 建立或探索工作環境。
    - "建立Amazon FSX以利ONTAP 不工作環境"
    - "設定及探索Azure NetApp Files 功能"
    - "在 Cloud Volumes ONTAP AWS 中啟動"
    - "在 Cloud Volumes ONTAP Azure 中啟動"
    - "在Cloud Volumes ONTAP Google Cloud上啟動"
    - "新增現有Cloud Volumes ONTAP 的系統"
    - "探索 ONTAP 叢集"
2. 按一下 * Canvas* 。
3. 選取符合上述任一類型的工作環境。
4. 選取同步旁邊的動作功能表。



5. 選擇*從此位置同步資料*或*同步資料至此位置*、然後依照提示設定同步關係。

建立其他類型的同步關係

請使用這些步驟、將資料同步至或從Amazon FSX以外的支援儲存類型、以利ONTAP 進行支援的資料、以利進行邊、Azure NetApp Files 邊、Cloud Volumes ONTAP 邊、邊ONTAP 等的資料叢集。下列步驟提供範例、說明如何設定從 NFS 伺服器到 S3 儲存區的同步關係。

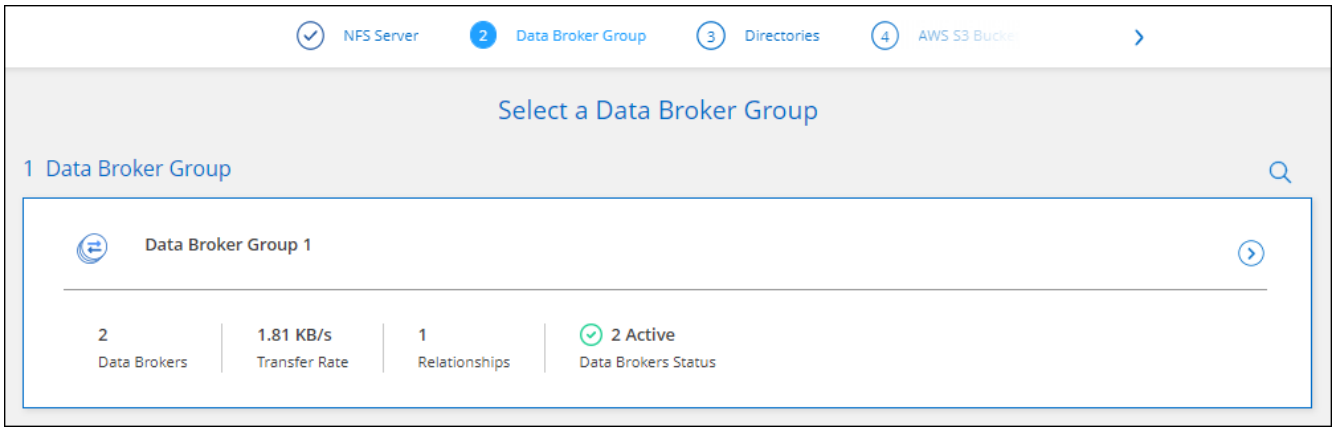
1. 在 Cloud Manager 中、按一下 * Sync* 。
2. 在「 * 定義同步關係 * 」頁面上、選擇來源和目標。

   下列步驟提供範例、說明如何從 NFS 伺服器建立至 S3 儲存區的同步關係。

3. 在「 * NFS 伺服器 * 」頁面上、輸入您要同步到 AWS 的 NFS 伺服器 IP 位址或完整網域名稱。
4. 在*資料代理人群組*頁面上、依照提示在AWS、Azure或Google Cloud Platform中建立資料代理人虛擬機器、或是在現有的Linux主機上安裝資料代理人軟體。

   如需詳細資料、請參閱下列頁面：

   - "在AWS中建立資料代理程式"
   - "在Azure中建立資料代理程式"
   - "在Google Cloud中建立資料代理商"
   - "在 Linux 主機上安裝資料代理程式"
5. 安裝資料代理程式之後、按一下 * 繼續 * 。

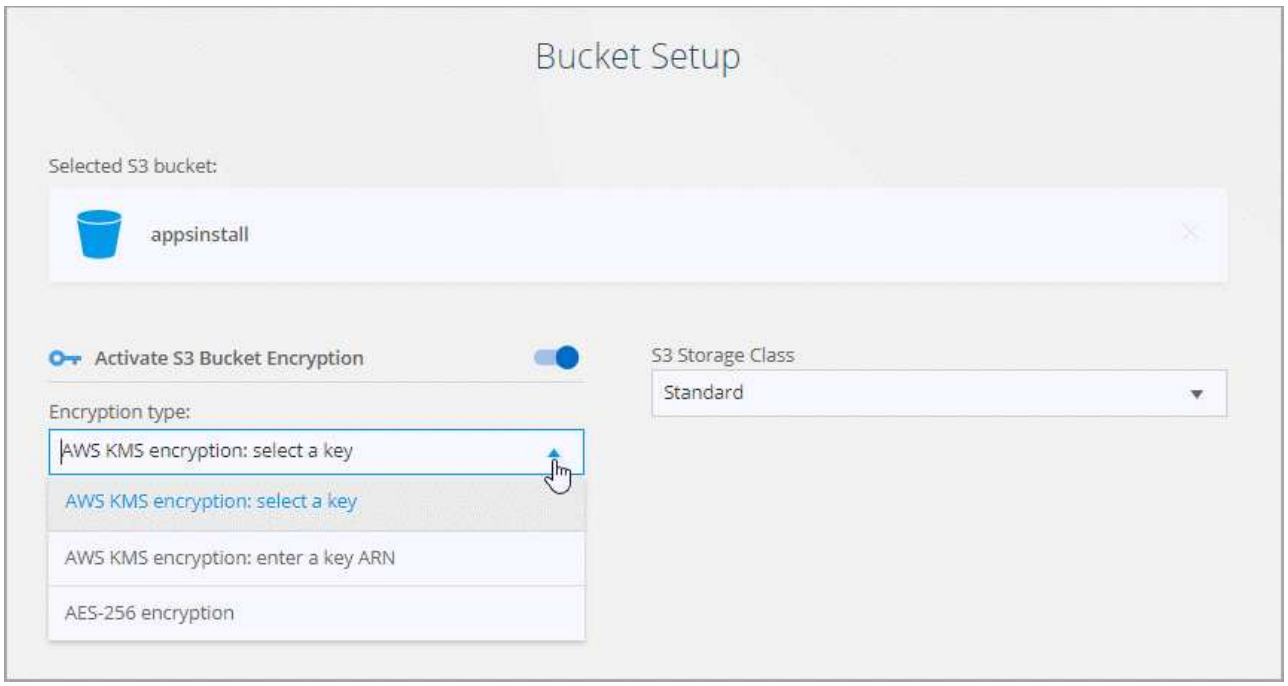


6. [[FIL篩選 器] 在 * 目錄 * 頁面上、選取最上層目錄或子目錄。

   如果 Cloud Sync 無法擷取匯出、請按一下 * 手動新增匯出 * 、然後輸入 NFS 匯出的名稱。

   如果您想要同步 NFS 伺服器上的多個目錄、則必須在完成之後建立其他同步關係。

7. 在「 * AWS S3 Bucket * 」頁面上、選取一個儲存區：
   - 向下切入以選取儲存區內現有的資料夾、或選取您在儲存區內建立的新資料夾。
   - 按一下 * 「Add to the list* （新增至清單 * ）」以選取與 AWS 帳戶無關的 S3 儲存區。 "必須將特定權限套用至 S3 儲存區"。
8. 在 * 庫位設定 * 頁面上、設定庫位：
   - 選擇是否啟用 S3 儲存區加密、然後選取 AWS KMS 金鑰、輸入 KMS 金鑰的 ARN 、或選取 AES-256 加密。
   - 選取 S3 儲存類別。 "檢視支援的儲存類別"。



9. [[Settings]在*設定*頁面上、定義如何在目標位置同步及維護來源檔案與資料夾：

排程

選擇週期性排程以供未來同步或關閉同步排程。您可以排程關係、每 1 分鐘同步一次資料。

同步逾時

定義Cloud Sync 如果同步尚未在指定的時數或天數內完成、則是否應取消資料同步。

通知

可讓您選擇是否要在Cloud Sync Cloud Manager的通知中心接收功能不全的通知。您可以啟用通知、以便成功同步資料、同步失敗資料及取消資料同步。

重試次數

定義 Cloud Sync 在跳過檔案之前、應重試同步檔案的次數。

持續同步

初始資料同步之後Cloud Sync 、Syncset會偵聽來源S3儲存區的變更、並在目標發生時持續同步任何變更。不需要以排定的時間間隔重新掃描來源。

此設定僅適用於建立同步關係、以及當您從S3儲存區同步至S3、Google Cloud Storage、Azure Blob儲存設備、StorageGRID 更新版本或IBM Storage時。

如果啟用此設定、則會影響其他功能、如下所示：

- 同步排程已停用。
- 下列設定會還原為預設值：同步逾時、最近修改的檔案及修改日期。
- 依大小篩選只會在複本事件上作用（而非刪除事件）。
- 建立關係之後、您只能加速或刪除關係。您無法中止同步、修改設定或檢視報告。

比較依據

選擇Cloud Sync 當判斷檔案或目錄是否已變更且應重新同步時、是否應比較某些屬性。

即使您取消核取這些屬性、Cloud Sync 透過檢查路徑、檔案大小和檔案名稱、即可將來源與目標進行比較。如果有任何變更、就會同步這些檔案和目錄。

您可以選擇啟用或停用Cloud Sync 下列屬性之比較功能：

- * mtime*：檔案的上次修改時間。此屬性對目錄無效。
- * uid*、* gid*和* mode*：Linux的權限旗標。

物件複本

啟用此選項可複製物件儲存中繼資料和標記。如果使用者變更來源上的中繼資料、Cloud Sync 則下次同步時、會將此物件複製下來、但如果使用者變更來源上的標記（而非資料本身）、Cloud Sync 則下次同步時、不會複製物件。

建立關聯之後、您無法編輯此選項。

支援複製標記的同步關係包括Azure Blob或S3相容端點（S3、StorageGRID 支援、或IBM Cloud Object Storage）作為目標。

下列任一端點之間的「雲端對雲端」關係均支援複製中繼資料：

- AWS S3
- Azure Blob
- Google Cloud Storage
- IBM Cloud 物件儲存設備
- StorageGRID

最近修改的檔案

選擇排除最近在排程同步之前修改的檔案。

刪除來源上的檔案

選擇在將檔案複製到目標位置後、從來源位置刪除檔案 Cloud Sync 。此選項包括資料遺失的風險、因為來源檔案在複製後會被刪除。

如果啟用此選項、您也需要變更資料代理程式上 local.json 檔案中的參數。開啟檔案並更新如下：

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

刪除目標上的檔案

如果檔案已從來源中刪除、請選擇從目標位置刪除。預設值是永遠不要從目標位置刪除檔案。

檔案類型

定義要包含在每個同步中的檔案類型：檔案、目錄和符號連結。

排除檔案副檔名

輸入副檔名並按 * Enter * 鍵、指定要從同步中排除的副檔名。例如、輸入 *log* 或 *.log* 以排除 * 。 log 檔案。多個副檔名不需要分隔符號。以下影片提供簡短示範：

► https://docs.netapp.com/zh-tw/cloud-manager-sync//media/video_file_extensions.mp4 *(video)*

檔案大小

無論檔案大小為何、或只是特定大小範圍內的檔案、都可以選擇同步所有檔案。

修改日期

無論檔案上次修改日期、在特定日期之後修改的檔案、在特定日期之前修改的檔案、或是在某個時間範圍之間、都要選擇所有檔案。

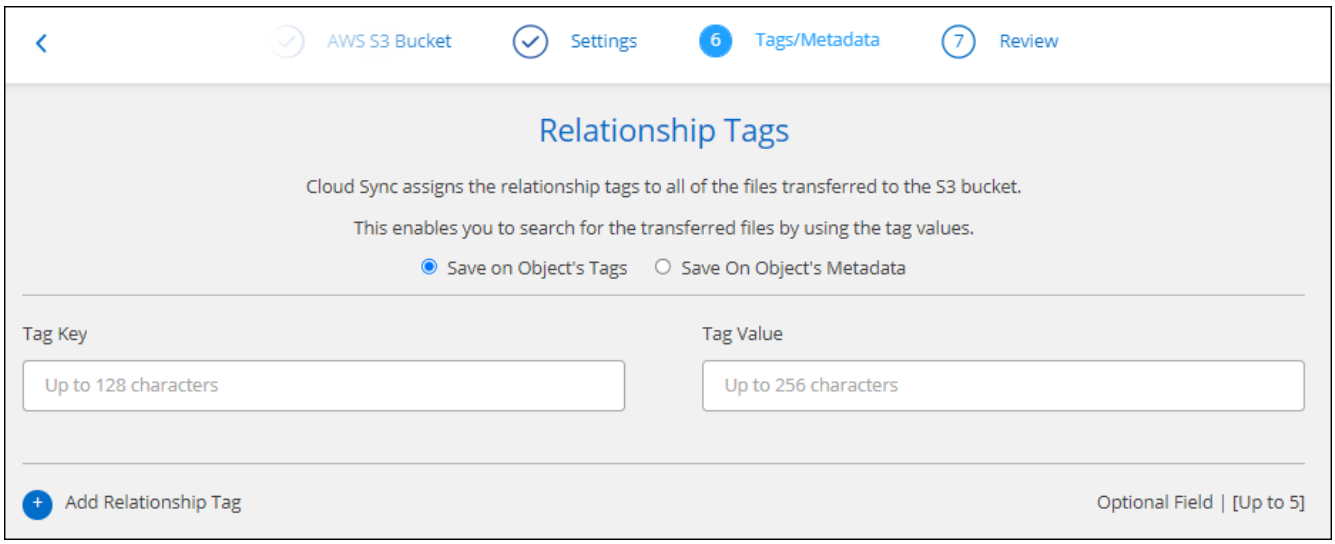
建立日期

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

ACL -存取控制清單

在建立關聯或建立關聯之後、啟用設定、即可從SMB伺服器複製ACL。

10. 在「標記/中繼資料」頁面上、選擇是否要將金鑰值配對另存為標記、以便傳輸至S3儲存區的所有檔案、或是在所有檔案上指派中繼資料金鑰值配對。



將資料同步至StorageGRID 物件儲存設備時、也可使用此功能。對於Azure和Google Cloud Storage、只有中繼資料選項可用。

11. 檢閱同步關係的詳細資料、然後按一下 * 建立關係 * 。

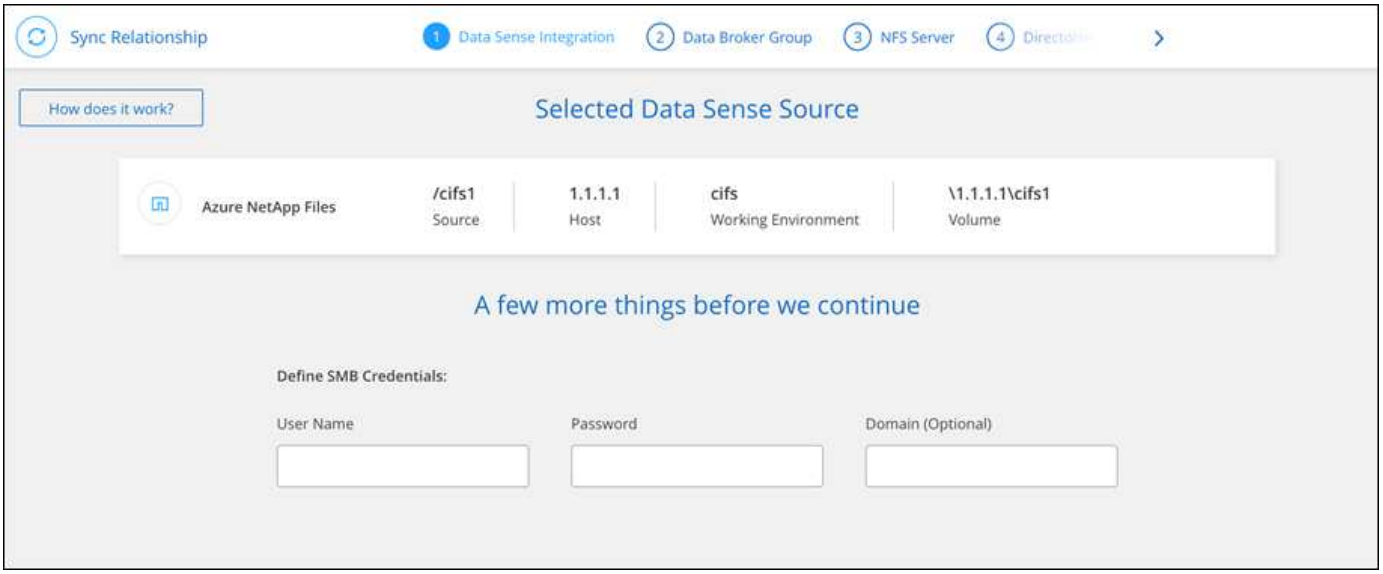
◦ 結果 *

從來源與目標之間開始同步資料。 Cloud Sync

從Cloud Data Sense建立同步關係

支援與Cloud Data Sense整合。Cloud Sync從Data感應範圍內、您可以使用Cloud Sync 下列功能、選取您要同步到目標位置的來源檔案：

從Cloud Data Sense啟動資料同步之後、所有來源資訊都會包含在單一步驟中、而且只需要輸入一些重要詳細資料即可。然後選擇新同步關係的目標位置。



"瞭解如何從Cloud Data Sense開始同步關係"。

從SMB共用區複製ACL

支援將來源SMB共用區與目標SMB共用區之間的存取控制清單（ACL）複製、或從來源SMB共用區複製到物件儲存區（不包括不適用於S3）Cloud Sync ONTAP 。如有需要、您也可以選擇使用Robocopy手動保留SMB共用之間的ACL。

不支援將ACL從物件儲存區複製回SMB共用區。Cloud Sync

選擇

- 設定 Cloud Sync 功能以自動複製 ACL
- 在SMB共用區之間手動複製ACL

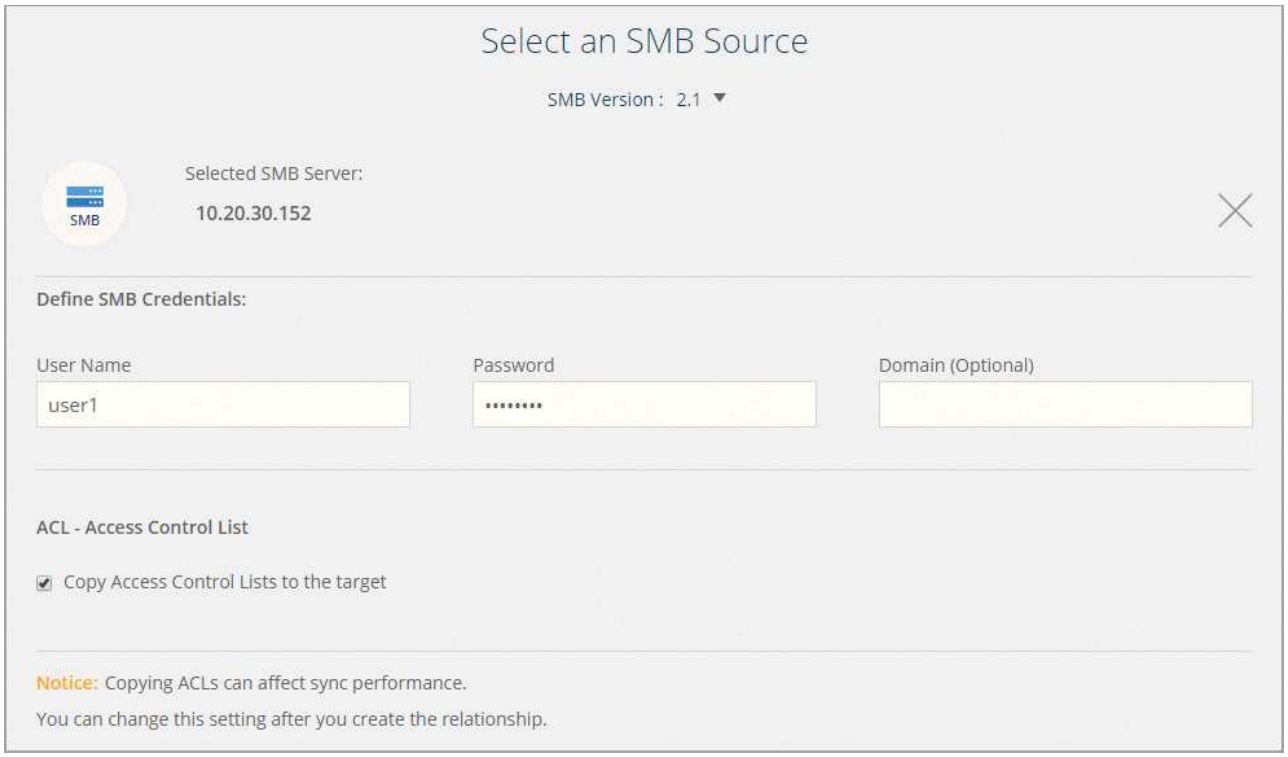
設定Cloud Sync 支援從SMB伺服器複製ACL

在建立關聯或建立關聯之後、啟用設定、即可從SMB伺服器複製ACL。

此功能適用於 _any 類型的資料代理商： AWS 、 Azure 、 Google Cloud Platform 或內部資料代理商。內部資料代理程式可以執行 "任何支援的作業系統"。

建立新關係的步驟

1. 從本頁中、按一下 * 建立新同步 * 。 Cloud Sync
2. 將* SMB Server*拖放到來源、選擇SMB伺服器或物件儲存做為目標、然後按一下*繼續*。
3. 在「 * SMB 伺服器 * 」頁面上：
   a. 輸入新的 SMB 伺服器或選取現有的伺服器、然後按一下 * 繼續 * 。
   b. 輸入 SMB 伺服器的認證資料。
   c. 選擇 * 將存取控制清單複製到目標 * 、然後按一下 * 繼續 * 。



4. 依照其餘的提示建立同步關係。

   當您將ACL從SMB複製到物件儲存設備時、可以根據目標、選擇將ACL複製到物件的標記或物件的中繼資料。對於Azure和Google Cloud Storage、只有中繼資料選項可用。

   下列螢幕擷取畫面顯示您可以選擇此步驟的範例。

現有關係的步驟

1. 將游標暫留在同步關係上、然後按一下動作功能表。
2. 按一下 * 設定 * 。
3. 選取 * 將存取控制清單複製到目標 * 。
4. 按一下 * 儲存設定 * 。

同步資料時Cloud Sync 、此功能會保留來源與目標SMB共用之間的ACL、或是從來源SMB共用區到物件儲存區的ACL。

在SMB共用區之間手動複製ACL

您可以使用 Windows Robocopy 命令、手動保留 SMB 共用區之間的 ACL 。

步驟

1. 識別擁有兩個 SMB 共用區完整存取權的 Windows 主機。
2. 如果任一端點需要驗證、請使用 * net use * 命令、從 Windows 主機連線至端點。

   您必須先執行此步驟、才能使用 Robocopy 。

3. 從這個範圍來 Cloud Sync 說、在來源與目標 SMB 共用之間建立新的關係、或是同步現有的關係。
4. 資料同步完成後、請從 Windows 主機執行下列命令、以同步處理 ACL 和擁有權：

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

   _ 來源 _ 和 _ 目標 _ 都應使用 UNC 格式來指定。例如： \<server>\<share>\

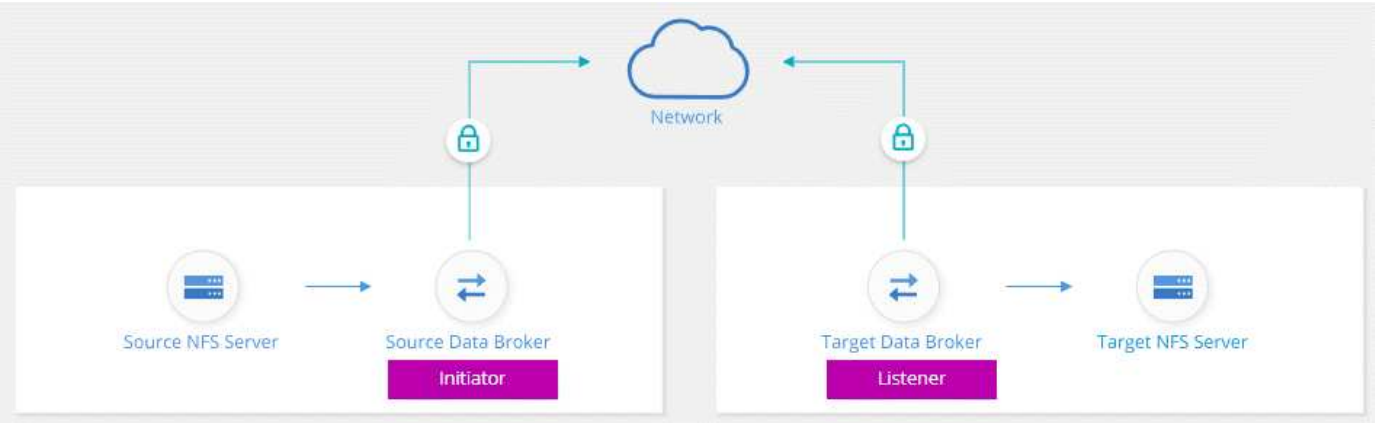
使用資料傳輸加密來同步 NFS 資料

如果您的企業有嚴格的安全性原則、您可以使用即時資料加密來同步 NFS 資料。從 NFS 伺服器到另一個 NFS 伺服器、以及 Azure NetApp Files 從功能到 Azure NetApp Files 功能的支援。

例如、您可能想要在不同網路中的兩個 NFS 伺服器之間同步資料。或者、您可能需要在 Azure NetApp Files 子網路或區域之間安全地傳輸有關的資料。

資料傳輸加密的運作方式

資料傳輸加密功能可在兩個資料代理人之間透過網路傳送 NFS 資料時、加密 NFS 資料。下圖顯示兩部 NFS 伺服器與兩個資料代理人之間的關係：



一個資料代理會做為 _initiator 。當需要同步資料時、它會傳送連線要求給另一個資料代理程式（即 _listener

）。該資料代理程式會偵聽連接埠 443 上的要求。如果需要、您可以使用不同的連接埠、但請務必檢查連接埠是否未被其他服務使用。

例如、如果您將內部部署 NFS 伺服器的資料同步到雲端型 NFS 伺服器、您可以選擇哪些資料代理程式會接聽連線要求、以及哪些資料代理程式會傳送這些要求。

以下是機上加密的運作方式：

1. 建立同步關係之後、啟動器會啟動與其他資料代理的加密連線。
2. 來源資料代理人會使用 TLS 1.3 加密來源的資料。
3. 然後、它會透過網路將資料傳送至目標資料代理程式。
4. 目標資料代理人會先解密資料、再將其傳送至目標。
5. 初始複本之後、服務會每 24 小時同步所有變更的資料。如果有要同步的資料、程序會從啟動器開啟與其他資料代理的加密連線開始。

   如果您偏好更頻繁地同步資料、 "您可以在建立關係之後變更排程"。

支援的 NFS 版本

- 對於 NFS 伺服器、 NFS 版本 3 、 4.0 、 4.1 和 4.2 支援傳輸中資料加密。
- 對於更新、 NFS 版本 3 和 4.1 支援資料傳輸加密。 Azure NetApp Files

Proxy 伺服器限制

如果您建立加密的同步關係、加密資料會透過 HTTPS 傳送、而且無法透過 Proxy 伺服器路由傳送。

您需要什麼才能開始使用

請務必具備下列項目：

- 兩部 NFS 伺服器 "來源與目標需求" 或 Azure NetApp Files 是兩個子網路或區域的不二選擇。
- 伺服器的 IP 位址或完整網域名稱。
- 兩個資料代理人的網路位置。

  您可以選取現有的資料代理程式、但它必須做為啟動器。接聽程式資料代理程式必須是 _new 資料代理程式。

  如果您想要使用現有的資料代理人群組、則該群組必須只有一個資料代理人。加密的同步關係不支援群組中的多個資料代理人。

  如果您尚未部署資料代理程式、請檢閱資料代理程式的需求。由於您有嚴格的安全原則、因此請務必檢閱網路需求、包括連接埠 443 和的傳出流量 "網際網路端點" 讓資料代理能夠聯絡。

  - "檢閱 AWS 安裝"
  - "檢閱 Azure 安裝"
  - "檢閱Google Cloud安裝"

。"檢閱 Linux 主機安裝"

使用資料傳輸加密來同步 **NFS** 資料

在兩部 NFS 伺服器之間或 Azure NetApp Files 在彼此之間建立新的同步關係、啟用即時加密選項、然後依照提示進行。

步驟

1. 按一下「 * 建立新同步 * 」。
2. 將 * NFS 伺服器 * 拖放到來源和目標位置、或 * Azure NetApp Files 《 * 》 * 拖放到來源和目標位置、然後選取 * 「是 * 」以啟用資料傳輸加密。
3. 依照提示建立關係：

   a. * NFS Server* / * Azure NetApp Files * ：選擇 NFS 版本、然後指定新的 NFS 來源或選取現有的伺服器。

   b. * 定義 Data Broker Function* ：定義哪個資料代理程式偵聽連接埠上的連線要求、以及哪個 _ 啟動 _ 連線。根據您的網路需求做出選擇。

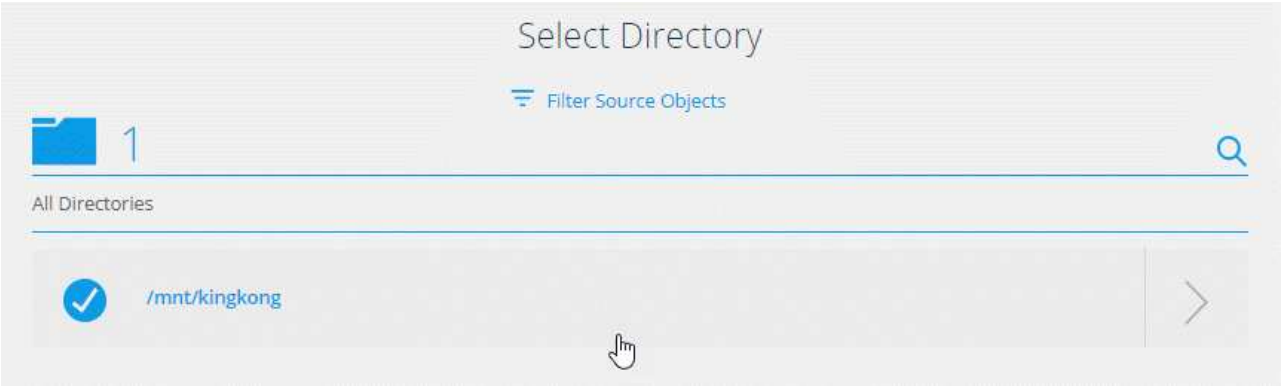
   c. * 資料代理人 * ：依照提示新增來源資料代理人或選取現有的資料代理人。

      請注意下列事項：

      - 如果您想要使用現有的資料代理人群組、則該群組必須只有一個資料代理人。加密的同步關係不支援群組中的多個資料代理人。
      - 如果來源資料代理做為接聽程式、則必須是新的資料代理程式。
      - 如果您需要新的資料代理程式、 Cloud Sync 則會以安裝說明提示您。您可以在雲端部署資料代理程式、或下載適用於您自己 Linux 主機的安裝指令碼。

   d. * 目錄 * ：選取所有目錄或向下切入並選取子目錄、以選擇要同步的目錄。

      按一下「 * 篩選來源物件 * 」以修改設定、定義如何在目標位置同步及維護來源檔案與資料夾。

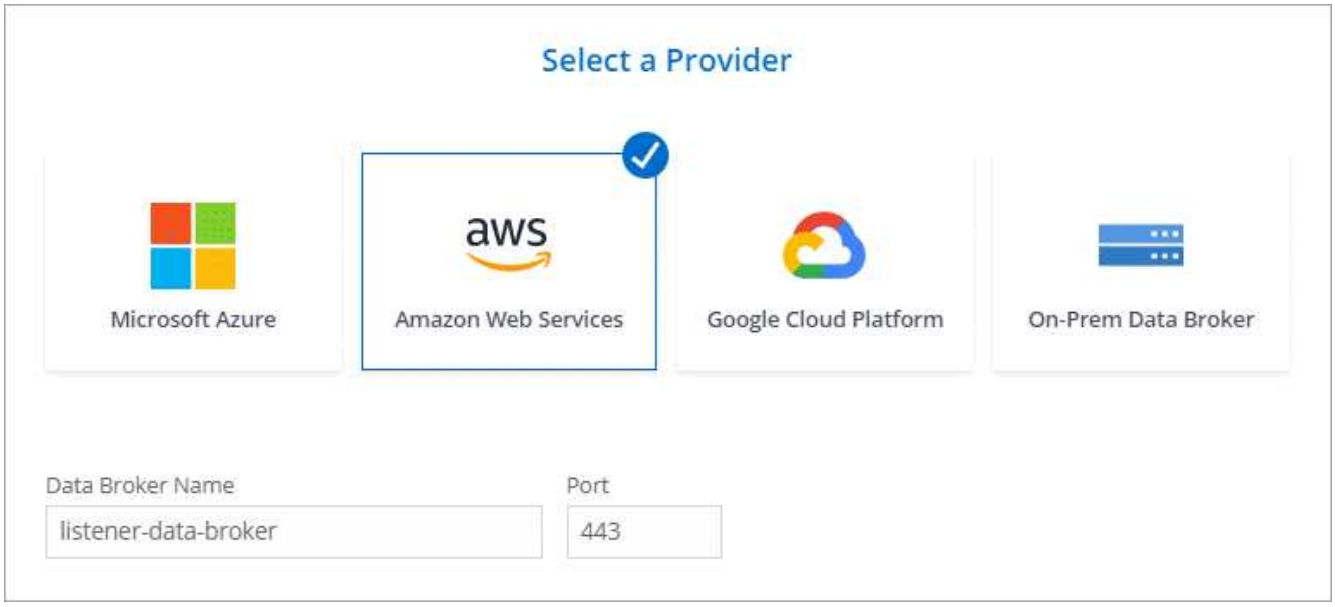
      

   e. * 目標 NFS 伺服器 * / * 目標 Azure NetApp Files * ：選擇 NFS 版本、然後輸入新的 NFS 目標或選取現有的伺服器。

   f. * 目標資料代理 * ：依照提示新增來源資料代理程式或選取現有的資料代理程式。

      如果目標資料代理做為接聽程式、則必須是新的資料代理程式。

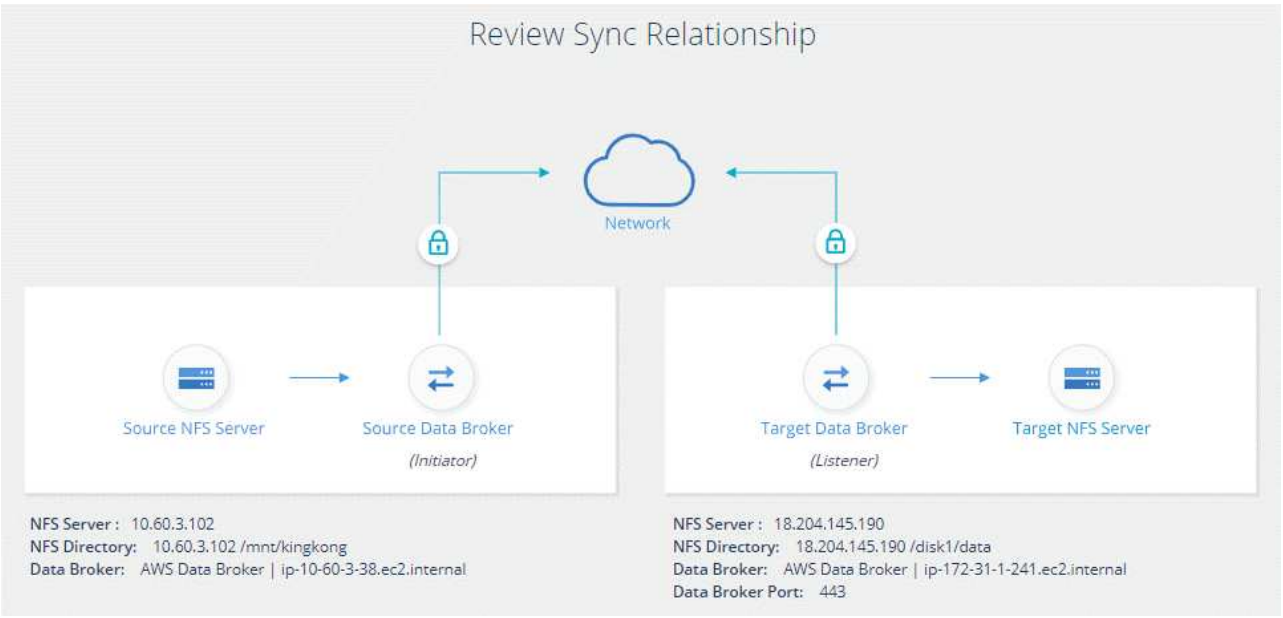
以下是當目標資料代理程式做為接聽程式時提示的範例。請注意指定連接埠的選項。



a. * 目標目錄 * ：選取最上層目錄、或向下切入以選取現有的子目錄、或在匯出中建立新的資料夾。

b. * 設定 * ：定義如何在目標位置同步及維護來源檔案與資料夾。

c. * 審查 * ：檢閱同步關係的詳細資料、然後按一下 * 建立關係 * 。



從建立新的同步關係開始。 Cloud Sync完成後、按一下「儀表板」中的 * 「檢視」 * 即可檢視新關係的詳細資料。

設定資料代理群組以使用外部HashiCorp Vault

當您建立需要 Amazon S3 、 Azure 或 Google Cloud 認證的同步關係時、必須透過 Cloud Sync 「支援」使用者介面或 API 來指定這些認證資料。另一種方法是設定資料代理人群組、以便直接從外部HashiCorp Vault存取認證（或_h秘密_）。

此功能可透過 Cloud Sync 使用需取得 Amazon S3 、 Azure 或 Google Cloud 認證的同步關係之支援。

設定URL、準備資料庫以提供認證給資料代理人群組。保存庫中機密的 URL 必須以 *Creds* 結尾。

修改群組中每個資料代理程式的本機組態檔、準備從外部資料保存庫擷取認證資料的資料代理群組。

現在一切都已設定完成、您可以傳送 API 呼叫來建立同步關係、使用您的保存庫來獲取機密資料。

準備保存庫

您需要提供 Cloud Sync URL 給資料庫中的機密資料。設定這些 URL 來準備保存庫。您需要在您打算建立的同步關係中、設定每個來源和目標的認證 URL 。

URL 必須設定如下：

路徑
: 密碼的前置路徑。這可以是您唯一的任何值。

申請 **ID**
: 您需要產生的要求 ID 。建立同步關係時、您必須在 API POST 要求的其中一個標頭中提供 ID 。

端點傳輸協定
: 下列其中一項協定、如定義 "在 POST 關係 v2 文件中"： S3 、 Azure 或 GCP （每個都必須大寫）。

建立
: URL 必須以 *Creds* 結尾。

範例

下列範例顯示了機密的 URL 。

來源認證的完整 **URL** 和路徑範例
: http://example.vault.com:8200/my-path/all-secrets/hb312vdasr2/S3Creds

  如範例所示、首碼路徑為 //my-path/all-h秘密 / _ 、要求 ID 為 _hb312vdasr2 、來源端點為 S3 。

目標認證的完整 **URL** 和路徑範例
: http://example.vault.com:8200/my-path/all-secrets/n32hcbnejk2/AZURECreds

  首碼路徑為： //my-path/all-hcides/ _ 、要求 ID 為 _n32hcbnjk2 、目標端點為 Azure 。

準備資料代理程式群組

修改群組中每個資料代理程式的本機組態檔、準備從外部資料保存庫擷取認證資料的資料代理群組。

步驟

1. SSH至群組中的資料代理程式。
2. 編輯位於 /opt/NetApp/databasroker/config 中的 local.json 檔案。
3. 將 enable 設為 * true* 、然後在 *exter-in*集成 *.hashicorp* 下設定組態參數欄位、如下所示：

已啟用

- 有效值： true/false
- 類型：布林值
- 預設值：假
- 對：資料代理人會從您自己的外部 HashiCorp Vault 取得機密
- 假：資料代理程式會將認證資料儲存在其本機保存庫中

URL

- 類型：字串
- 值：外部保存庫的 URL

路徑

- 類型：字串
- 值：以認證資料做為密碼的前置路徑

拒絕未獲授權的

- 決定您是否要資料代理程式拒絕未獲授權的外部資料庫
- 類型：布林值
- 預設值：假

驗證方法

- 資料代理程式應使用的驗證方法、從外部資料庫存取認證資料
- 類型：字串
- 有效值：「AWS/IAM」/「role應用程式」/「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）

Sec淘汰 與 **roid**

- 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（ X-Vault-Namespace 標頭（如有需要）

4. 針對群組中的任何其他資料代理人重複這些步驟。

AWS角色驗證範例

```
{
          “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**驗證時設定權限

如果您使用_GCP-iam_驗證方法、則資料代理程式必須具有下列GCP權限：

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

"深入瞭解資料代理商的GCP權限要求"。

使用資料庫中的機密建立新的同步關係

現在一切都已設定完成、您可以傳送 API 呼叫來建立同步關係、使用您的保存庫來獲取機密資料。

使用 Cloud Sync REST API 張貼關係。

```
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
```

- 若要取得使用者權杖和 Cloud Central 帳戶 ID 、 "請參閱文件中的本頁"。
- 為您的貼文關係建立一個實體、 "請參閱第 2 版關係 API 呼叫"。

範例

POST 要求的範例：

```
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"
        }
    }
}
```