



# 本文檔 **Cloud Sync**

## Cloud Sync

NetApp  
May 25, 2022

# 目錄

本文檔 Cloud Sync	1
版本資訊	2
更新功能Cloud Sync	2
限制	12
開始使用	13
概述 Cloud Sync	13
快速入門 Cloud Sync	15
支援的同步關係	16
準備來源和目標	23
網路概述 Cloud Sync	29
安裝資料代理程式	32
使用Cloud Sync	46
在來源與目標之間同步資料	46
免費試用結束後、請支付同步關係的費用	63
管理同步關係	65
管理資料代理群組	70
建立及檢視報告以調整組態	77
解除安裝資料代理程式	80
資訊 API Cloud Sync	82
快速入門	82
API 參考	83
使用清單 API	83
概念	86
授權總覽	86
資料隱私	87
技術常見問題集 Cloud Sync	87
知識與支援	94
註冊以取得支援	94
取得協助	95
法律聲明	97
版權	97
商標	97
專利	97
隱私權政策	97
開放原始碼	97

# 本文檔 Cloud Sync

# 版本資訊

## 更新功能Cloud Sync

瞭解Cloud Sync 解更新功能。

**2022年5月1日**

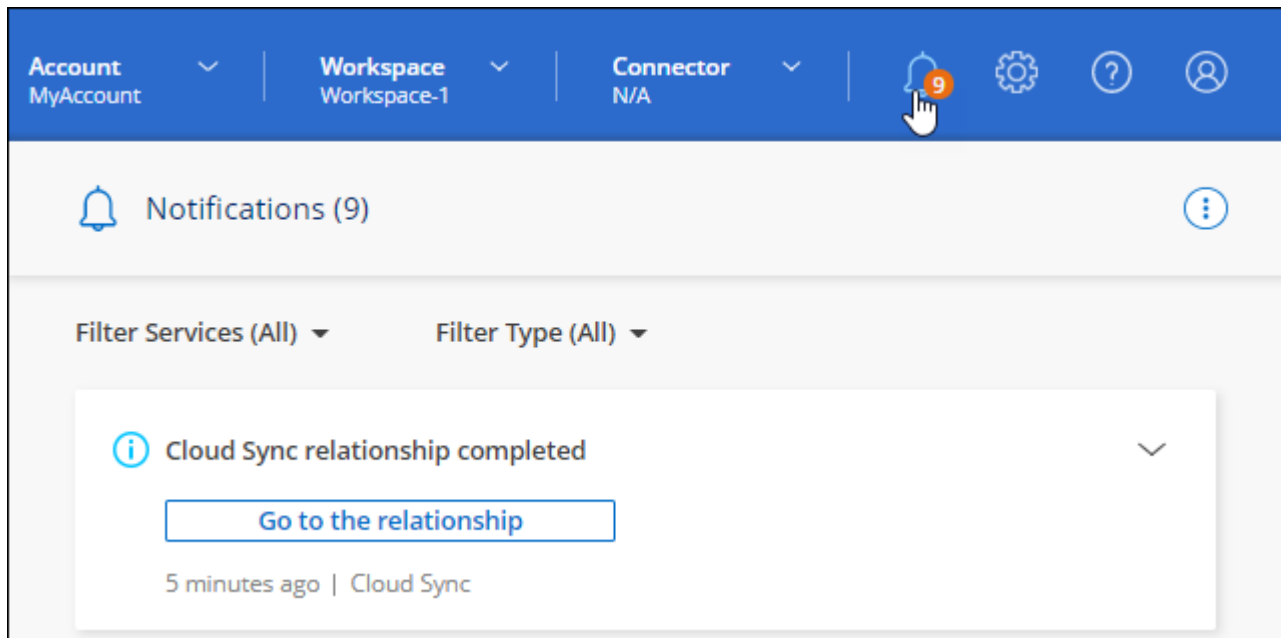
### 同步逾時

現在有一項新的\*同步逾時\*設定可供同步關係使用。此設定可讓您定義Cloud Sync 當同步尚未在指定的時數或天數內完成時、是否應取消資料同步。

["深入瞭解如何變更同步關係的設定"](#)。

### 通知

現在有一項新的\*通知\*設定可供同步關係使用。此設定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。



["深入瞭解如何變更同步關係的設定"](#)。

**2022年4月3日**

### 資料代理群組增強功能

我們對資料代理商群組進行了多項增強：

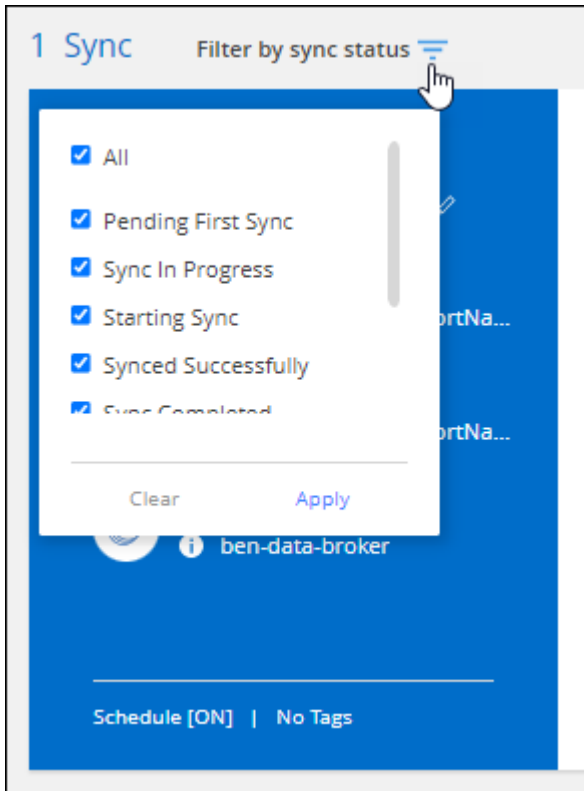
- 您現在可以將資料代理程式移至新的或現有的群組。
- 您現在可以更新資料代理程式的Proxy組態。

- 最後、您也可以刪除資料代理人群組。

"瞭解如何管理資料代理人群組"。

### 儀表板篩選器

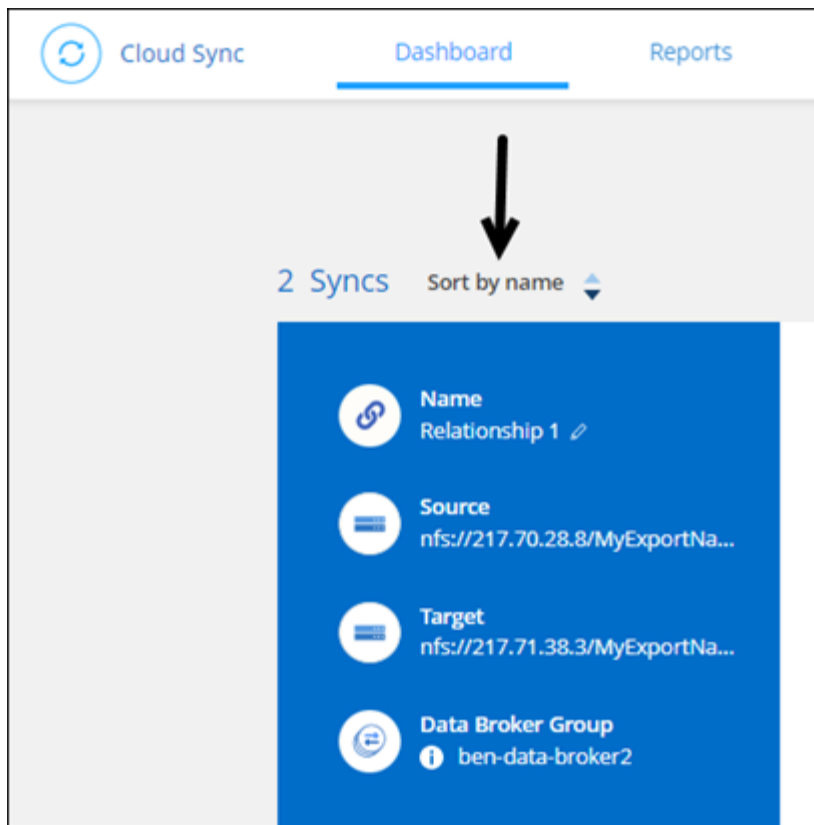
您現在可以篩選「同步儀表板」的內容、更輕鬆地找到符合特定狀態的同步關係。例如、您可以篩選狀態為「失敗」的同步關係



**2022年3月3日**

### 在儀表板中排序

您現在可以依照同步關係名稱來排序儀表板。



## 資料感測整合的增強功能

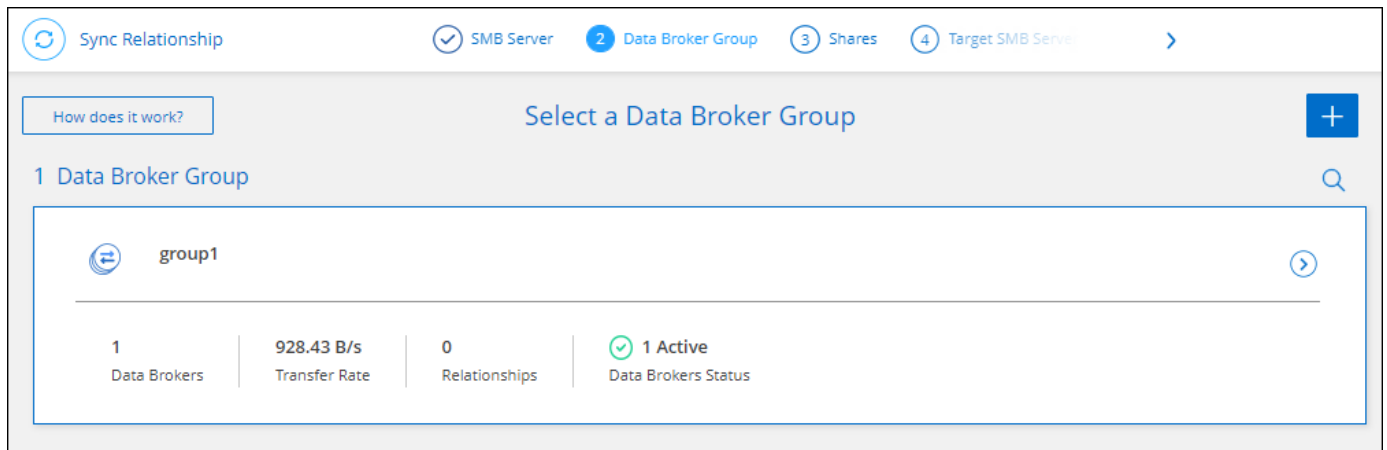
在先前的版本中、我們推出Cloud Sync 了與Cloud Data Sense整合的功能。在此更新中、我們透過更輕鬆地建立同步關係來強化整合。從Cloud Data Sense啟動資料同步之後、所有來源資訊都會包含在單一步驟中、而且只需要輸入一些重要詳細資料即可。

## 2022年2月6日

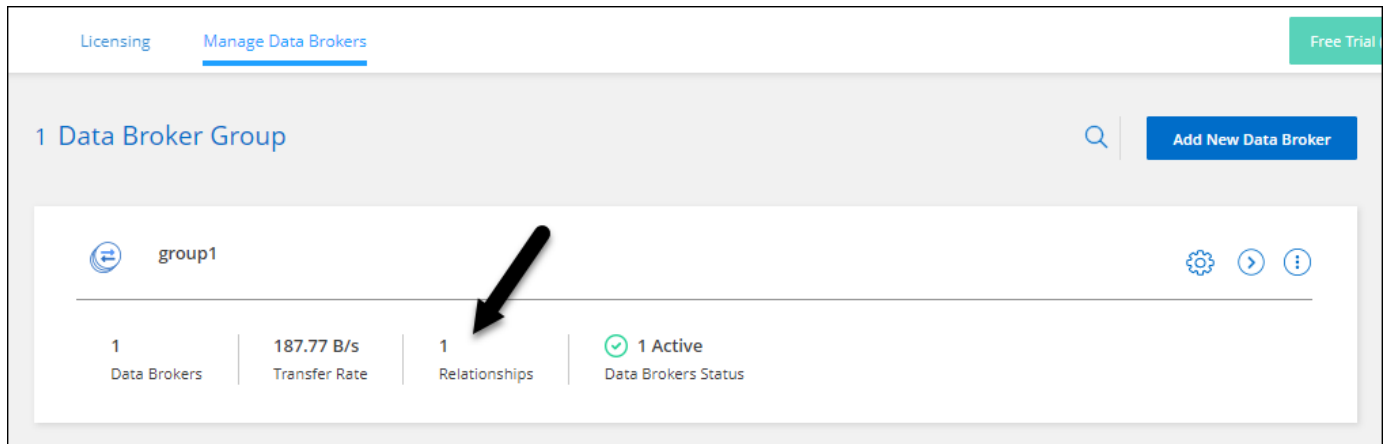
## 資料代理群組的增強功能

我們強調資料代理商\_群組\_、改變了您與資料代理人的互動方式。

例如、當您建立新的同步關係時、請選取要與關係搭配使用的資料代理\_群組\_、而非特定的資料代理程式。



在\*管理資料代理人\*索引標籤中、我們也會顯示資料代理人群組正在管理的同步關係數目。



## 下載PDF報告

您現在可以下載報告的PDF。

["深入瞭解報告"](#)。

## 2022年1月2日

### 新的Box同步關係

支援兩種新的同步關係：

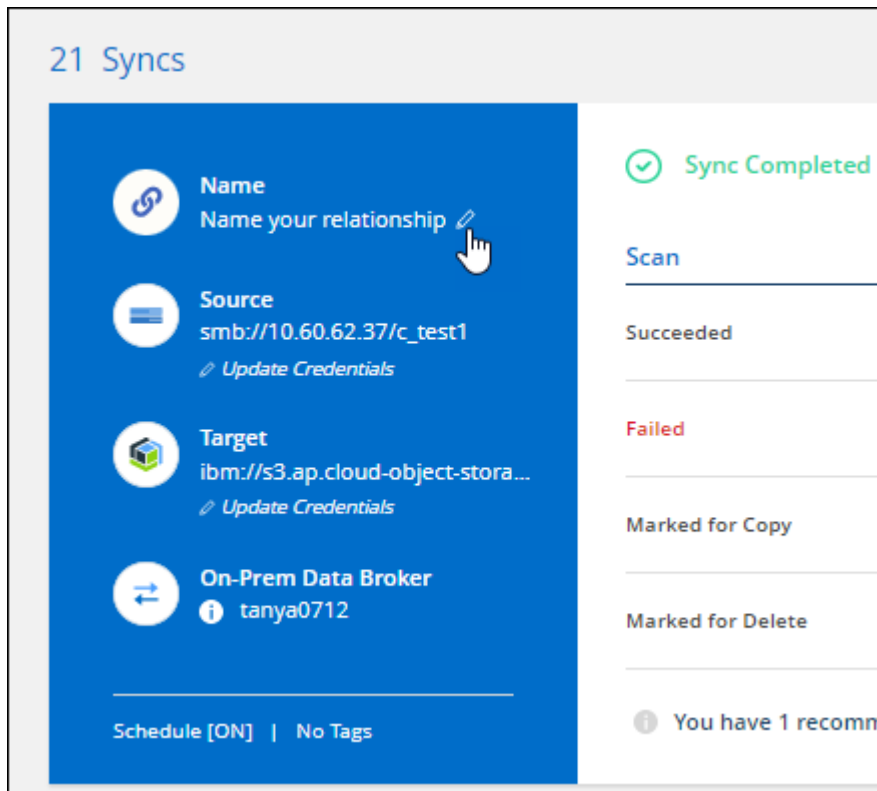
- Box to Azure NetApp Files
- Box to Amazon FSx for ONTAP Sfx

["檢視支援的同步關係清單"](#)。

### 關係名稱

您現在可以為每個同步關係提供有意義的名稱、以便更輕鬆地識別每個關係的目的。您可以在建立關聯時新增名

稱、也可以在之後的任何時間新增。



### S3私有連結

當您在Amazon S3之間或從Amazon S3同步資料時、可以選擇是否使用S3私有連結。當資料代理人將資料從來源複製到目標時、便會透過私有連結。

請注意、與您的資料代理人相關聯的IAM角色需要下列權限才能使用此功能：

```
"ec2:DescribeVpcEndpoints"
```

此權限會自動新增至您所建立的任何新資料代理人。

### Glacier即時擷取

現在、當Amazon S3成為同步關係的目標時、您可以選擇\_Glacier即時擷取\_儲存類別。

### 從物件儲存到SMB共用的ACL

目前支援將ACL從物件儲存設備複製到SMB共用區。Cloud Sync之前、我們只支援將ACL從SMB共用區複製到物件儲存區。

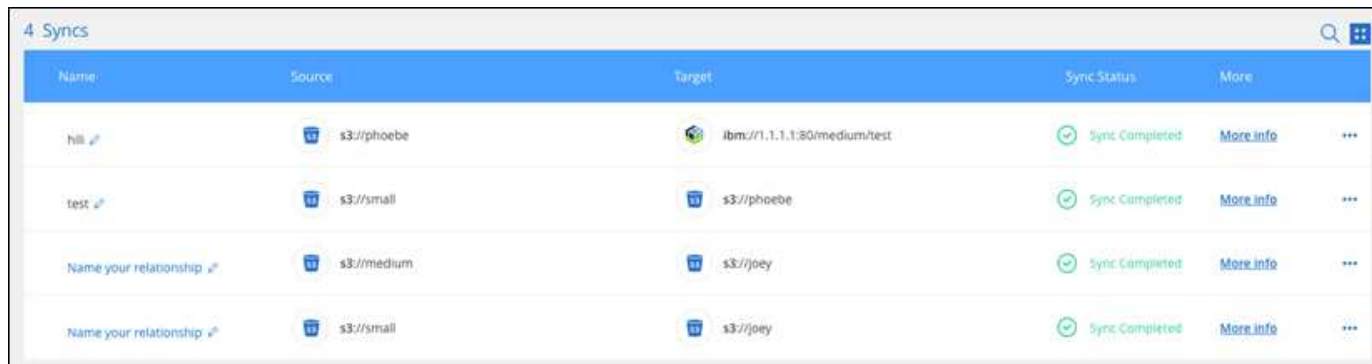
### SFTP至S3

使用者介面現在支援從SFTP建立與Amazon S3的同步關係。此同步關係先前僅受到API支援。



## 表格檢視增強功能

我們重新設計儀表板上的表格檢視、以方便使用。如果您按一下\*更多資訊\*、Cloud Sync 則此功能會篩選儀表板、以顯示有關該特定關係的更多資訊。



Name	Source	Target	Sync Status	More
hili	s3://phoebe	ibmc/71.1.1.1:80/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

## 支援Jarkarta地區

目前支援在AWS亞太地區（雅加達）部署資料代理商。Cloud Sync

## 2021年11月28日

### 從SMB到物件儲存的ACL

現在、當從來源SMB共用區設定同步關係到物件儲存（除了不包括S3）時、即可複製存取控制清單（ACL）Cloud Sync ONTAP。

不支援將ACL從物件儲存區複製到SMB共用區。Cloud Sync

"瞭解如何從SMB共用區複製ACL"。

### 更新授權

您現在可以更新Cloud Sync 擴充的更新版的支援。

如果您延長Cloud Sync 從NetApp購買的支援對象、您可以再次新增授權、以重新更新到期日。

"瞭解如何更新授權"。

### 更新Box認證資料

您現在可以更新現有同步關係的Box認證資料。

"瞭解如何更新認證資料"。

## 2021年10月31日

### Box支援

Box支援現可在Cloud Sync 支援畫面的使用者介面中預覽。

Box可以是多種同步關係類型的來源或目標。 ["檢視支援的同步關係清單"](#)。

## 建立日期設定

當SMB伺服器為來源時、稱為「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。

["深入瞭解Cloud Sync 解有關功能的設定"](#)。

## 2021年10月4日

### 額外的Box支援

目前支援的其他同步關係Cloud Sync ["方塊"](#) 使用Cloud Sync API時：

- Amazon S3 to Box
- IBM Cloud Object Storage to Box
- 包裝盒StorageGRID
- Box移轉至NFS伺服器
- 適用於SMB伺服器

["瞭解如何使用API設定同步關係"](#)。

### SFTP路徑報告

您現在可以了 ["建立報告"](#) 適用於SFTP路徑。

## 2021年9月2日

### 支援FSX for ONTAP Sf

您現在可以將資料同步至Amazon FSX for ONTAP Sf for系統、或從Amazon FSX同步資料。

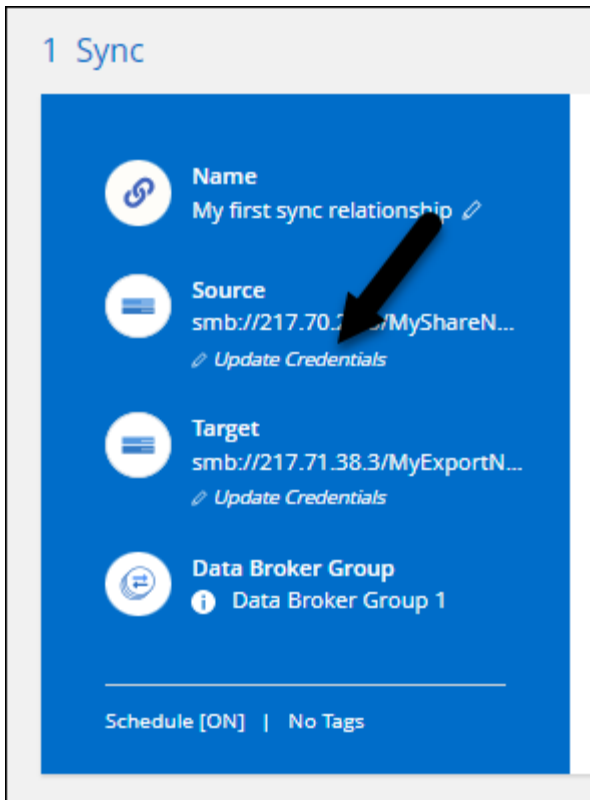
- ["深入瞭解Amazon FSX for ONTAP Sf"](#)
- ["檢視支援的同步關係"](#)
- ["瞭解如何為Amazon FSX for ONTAP Synf2建立同步關係"](#)

## 2021年8月1日

### 更新認證資料

利用目前的支援功能、您可以在現有的同步關係中、以來源或目標的最新認證來更新資料代理程式。Cloud Sync

如果您的安全性原則要求您定期更新認證資料、這項增強功能將有助於您。 ["瞭解如何更新認證資料"](#)。



物件儲存目標的標記

建立同步關係時、您現在可以在同步關係中將標記新增至物件儲存目標。

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

支援Box

支援的支援Cloud Sync "方塊" 當使用此解決方案時、可作為與Amazon S3、StorageGRID Syn性質 及IBM Cloud Object Storage的同步關係來源Cloud Sync。

"瞭解如何使用API設定同步關係"。

## Google Cloud資料代理商的公有IP

在Google Cloud中部署資料代理程式時、您現在可以選擇啟用或停用虛擬機器執行個體的公有IP位址。

["瞭解如何在Google Cloud中部署資料代理商"](#)。

## 雙傳輸協定Volume Azure NetApp Files 、提供更多功能

當您選擇Azure NetApp Files 來源或目標Volume進行更新時、Cloud Sync 無論您選擇哪種傳輸協定來進行同步關係、現在只要顯示雙傳輸協定Volume即可。

## 2021年7月7日

### S3儲存設備與Google Cloud Storage ONTAP

現在、支援從使用者介面同步處理S3儲存設備與Google Cloud Storage儲存桶之間的關係。Cloud Sync ONTAP

["檢視支援的同步關係清單"](#)。

### 物件中繼資料標記

建立同步關係並啟用設定時、即可在物件型儲存設備之間複製物件中繼資料和標記。Cloud Sync

["深入瞭解「複製物件」設定"](#)。

### 支援HashiCorp資料錯誤

您現在可以設定資料代理程式、透過Google Cloud服務帳戶驗證、從外部HashiCorp Vault存取認證資料。

["深入瞭解搭配資料代理程式使用HashiCorp Vault的相關資訊"](#)。

### 定義S3儲存區的標記或中繼資料

設定Amazon S3儲存區的同步關係時、同步關係精靈現在可讓您定義要儲存在目標S3儲存區物件上的標記或中繼資料。

標記選項先前是同步關係設定的一部分。

## 2021年6月7日

### Google Cloud的儲存課程

當Google Cloud Storage資源桶成為同步關係的目標時、您現在可以選擇想要使用的儲存類別。支援下列儲存類別：Cloud Sync

- 標準
- 近線
- 冷線
- 歸檔

## 2021年5月2日

### 報告中的錯誤

您現在可以檢視報告中的錯誤、並刪除最後一份報告或所有報告。

["深入瞭解如何建立及檢視報告以調整組態"](#)。

### 比較屬性

現在每個同步關係都有一個新的\*比較依據\*設定可供使用。

這項進階設定可讓您選擇Cloud Sync 在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。

["深入瞭解如何變更同步關係的設定"](#)。

## 2021年4月11日

### 獨立Cloud Sync 式的版不使用此服務

獨立Cloud Sync 式的不再使用此功能。您現在應該Cloud Sync 直接從Cloud Manager存取、因為Cloud Manager具備所有相同的功能。

登入Cloud Manager之後、您可以切換至頂端的「Sync」（同步）索引標籤、檢視您的關係、就像以往一樣。

### Google Cloud會在不同專案中儲存貯體

設定同步關係時、如果您提供資料代理商服務帳戶所需的權限、您可以從不同專案的Google Cloud儲存庫中進行選擇。

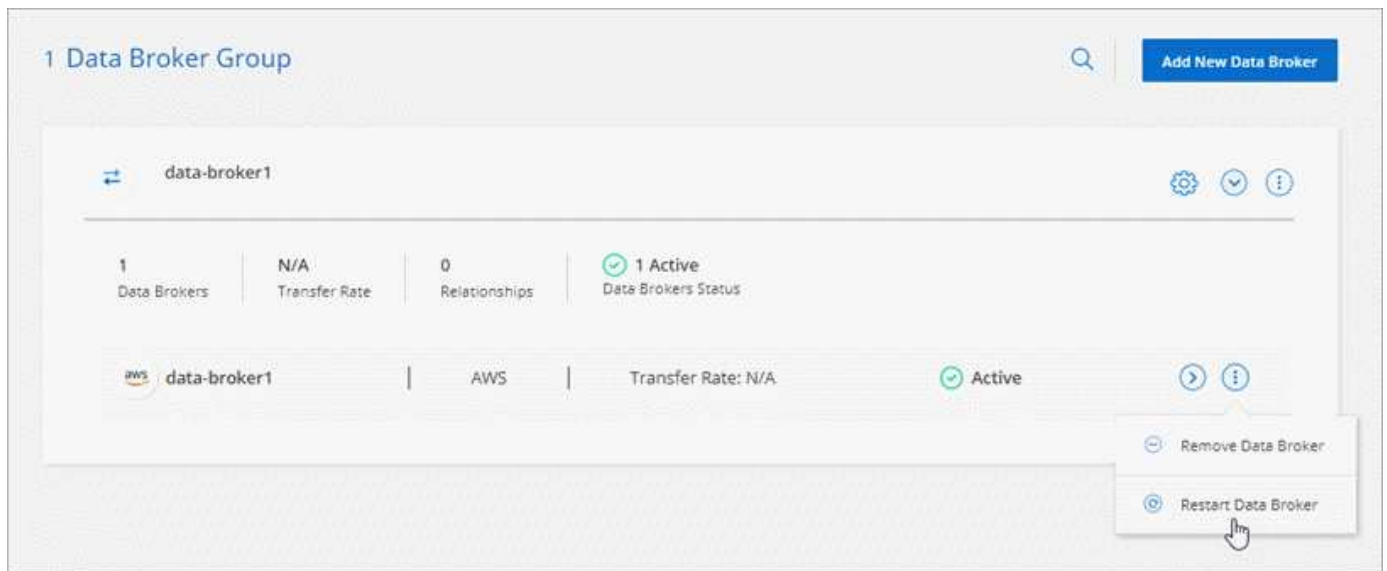
["瞭解如何設定服務帳戶"](#)。

### Google Cloud Storage與S3之間的中繼資料

目前、支援在Google Cloud Storage和S3供應商（AWS S3、支援、IBM Cloud Object Storage）之間複製中繼資料。Cloud Sync StorageGRID

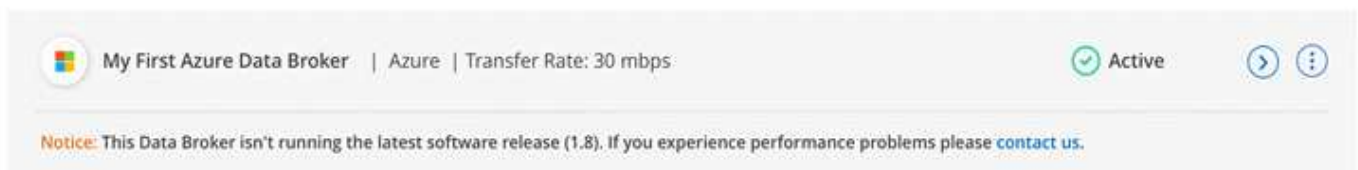
### 重新啟動資料代理人

您現在可以從Cloud Sync 功能不再需要的地方重新啟動資料代理程式。



未執行最新版本時的訊息

目前可識別資料代理程式何時未執行最新的軟體版本。Cloud Sync此訊息有助於確保您獲得最新的功能。



## 限制

已知限制指出本產品版本不支援的平台、裝置或功能、或是無法與產品正確互通的平台、裝置或功能。請仔細檢閱這些限制。

- 中國不支援此功能。Cloud Sync
- 除了中國以外、Cloud Sync 下列地區不支援 The Sun 的資料代理程式：
  - Azure US Gov
  - Azure US DoD

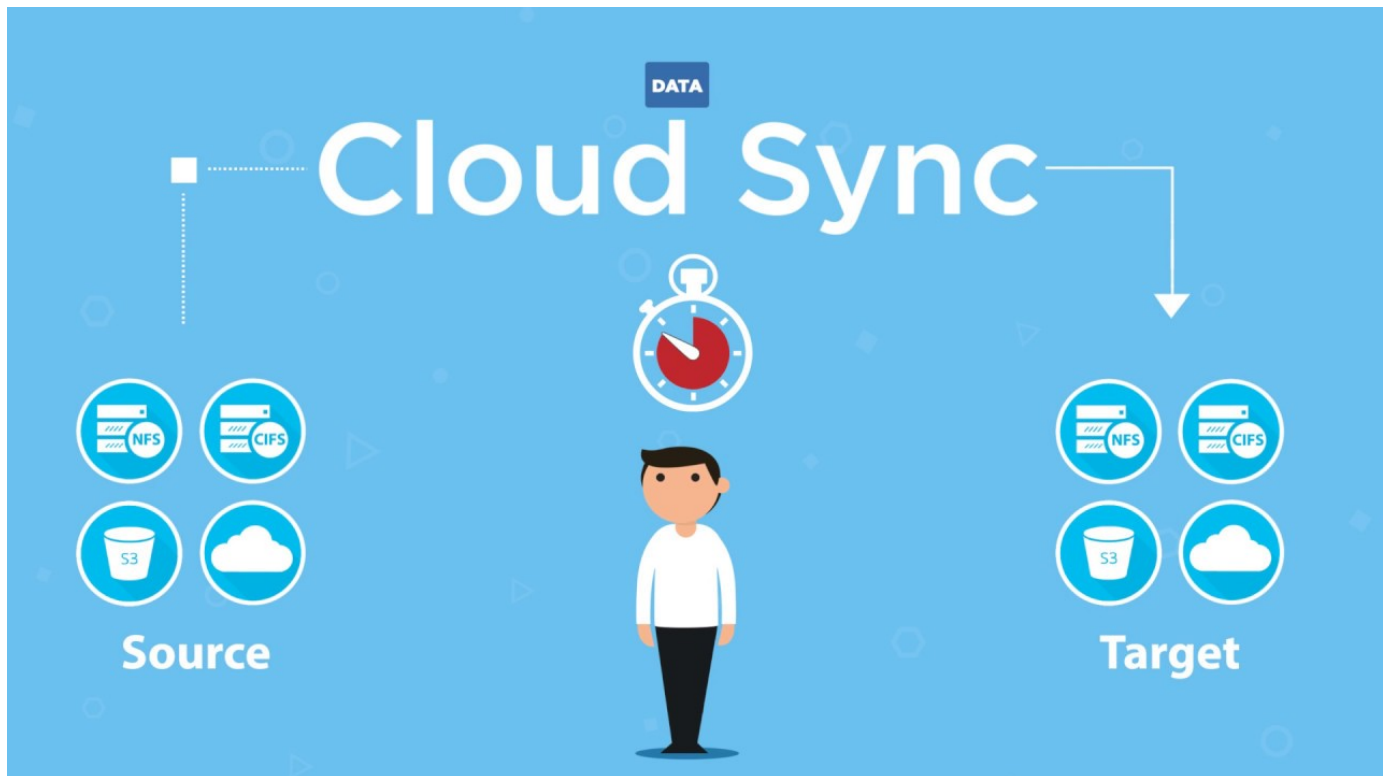
# 開始使用

## 概述 Cloud Sync

NetApp Cloud Sync 支援服務提供簡單、安全且自動化的方式、可將您的資料移轉至雲端或內部部署的任何目標。無論是檔案型 NAS 資料集（NFS 或 SMB）、Amazon Simple Storage Service（S3）物件格式、NetApp StorageGRID S還原® 應用裝置、或是任何其他雲端供應商物件存放區、Cloud Sync 均可將其轉換並移動。

### 功能

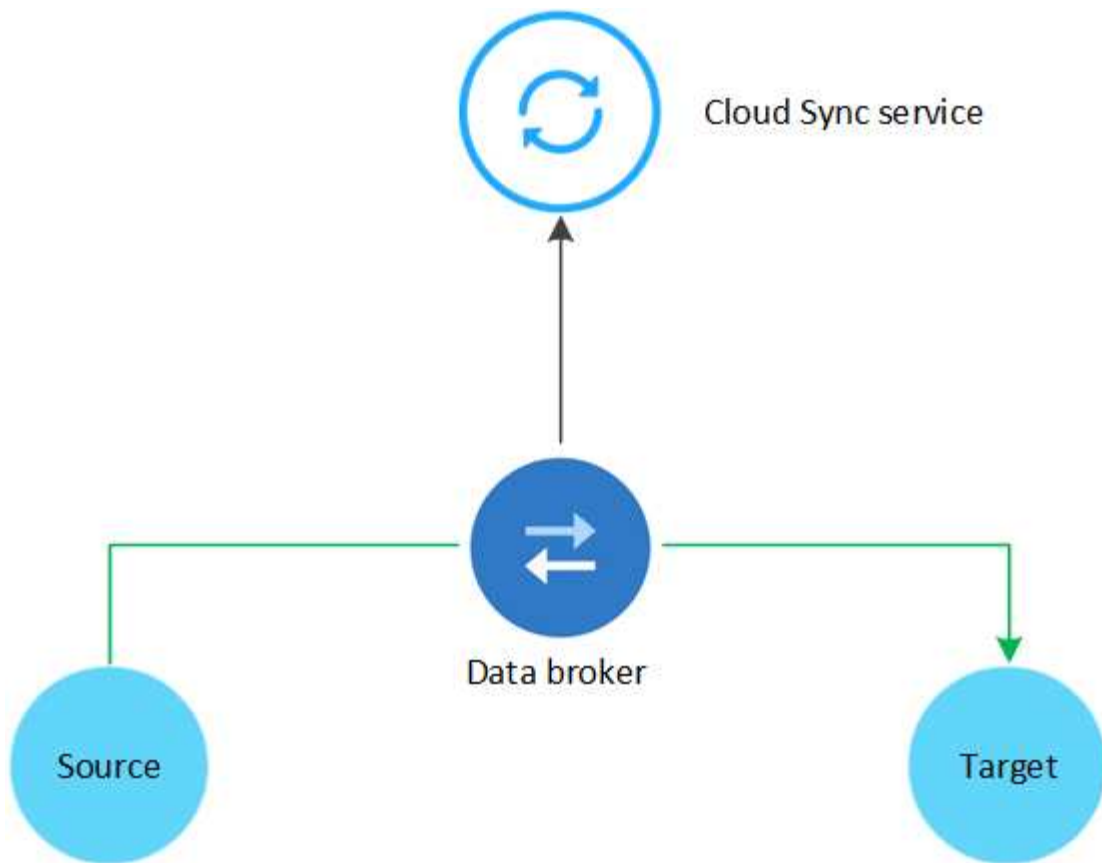
觀看下列影片、瞭解 Cloud Sync 有關下列功能的概述：



## 運作原理 Cloud Sync

VMware是軟體即服務（SaaS）平台、由資料代理商群組、雲端型介面（可透過Cloud Manager取得）、以及來源與目標組成。Cloud Sync

下圖顯示 Cloud Sync 了各個元件之間的關係：



NetApp 資料代理軟體會將資料從來源同步至目標（這稱為 `_sync 關係_`）。您可以在 AWS、Azure、Google Cloud Platform 或內部部署環境中執行資料代理程式。由一或多個資料代理人所組成的資料代理人群組、需要透過連接埠 443 建立傳出網際網路連線、以便與 Cloud Sync 該服務進行通訊、並聯絡其他服務與儲存庫。 [檢視端點清單](#)。

初始複本之後、服務會根據您設定的排程同步任何變更的資料。

## 支援的儲存類型

支援下列儲存類型： Cloud Sync

- 任何 NFS 伺服器
- 任何 SMB 伺服器
- Amazon EFS
- Amazon FSx for ONTAP Sf
- Amazon S3
- Azure Blob
- Azure NetApp Files
- Box（可預覽）
- Cloud Volumes Service
- Cloud Volumes ONTAP
- Google Cloud Storage



- IBM Cloud 物件儲存設備
- 內部部署 ONTAP 的叢集
- SS3 儲存設備 ONTAP
- SFTP（僅使用API）
- StorageGRID

["檢視支援的同步關係"](#)。

## 成本

有兩種成本與 Cloud Sync 使用效益有關：資源費用和服務費用。

### 資源費用

資源費用與在雲端執行一或多個資料代理人的運算和儲存成本有關。

### 服務費用

在您的 14 天免費試用結束後、有兩種方式可以支付同步關係的費用。第一個選項是向 AWS 或 Azure 訂閱、這可讓您每小時或每年付費。第二種選擇是直接向 NetApp 購買授權。

["瞭解授權的運作方式"](#)。

## 快速入門 Cloud Sync

使用此功能包括幾個步驟。Cloud Sync

確認您的來源和目標是否受到支援和設定。最重要的要求是驗證資料代理群組與來源和目標位置之間的連線能力。

- ["檢視支援的關係"](#)
- ["準備來源和目標"](#)

NetApp 資料代理軟體會將資料從來源同步至目標（這稱為 `_sync 關係_`）。您可以在 AWS、Azure、Google Cloud Platform 或內部部署環境中執行資料代理程式。由一或多個資料代理人所組成的資料代理人群組、需要透過連接埠443建立傳出網際網路連線、以便與Cloud Sync 該服務進行通訊、並聯絡其他服務與儲存庫。 ["檢視端點清單"](#)。

建立同步關係時、會引導您完成安裝程序、此時您可以在雲端部署資料代理程式、或為自己的Linux主機下載安裝指令碼。Cloud Sync

- ["檢閱 AWS 安裝"](#)
- ["檢閱 Azure 安裝"](#)
- ["檢閱Google Cloud安裝"](#)
- ["檢閱 Linux 主機安裝"](#)

登入 ["Cloud Manager"](#)，單擊 \* Sync\*（同步），然後拖放源和目標的選擇。依照提示完成設定。 ["深入瞭解"](#)。

從 AWS 或 Azure 訂閱、即可隨用隨付或每年付費。或直接向 NetApp 購買授權。只要前往 Cloud Sync「授權

設定」頁面即可設定。["深入瞭解"](#)。

## 支援的同步關係

利用此功能、您可以將資料從來源同步到目標。Cloud Sync這稱為同步關係。開始之前、您應該先瞭解支援的關係。

來源位置	支援的目標位置
Amazon EFS	<ul style="list-style-type: none"><li>• Amazon EFS</li><li>• Amazon FSX for ONTAP Sf</li><li>• Amazon S3</li><li>• Azure Blob</li><li>• Azure NetApp Files</li><li>• Cloud Volumes ONTAP</li><li>• Cloud Volumes Service</li><li>• Google Cloud Storage</li><li>• IBM Cloud 物件儲存設備</li><li>• NFS 伺服器</li><li>• 內部部署 ONTAP 的叢集</li><li>• SMB 伺服器</li><li>• StorageGRID</li></ul>
Amazon FSX for ONTAP Sf	<ul style="list-style-type: none"><li>• Amazon EFS</li><li>• Amazon FSX for ONTAP Sf</li><li>• Amazon S3</li><li>• Azure Blob</li><li>• Azure NetApp Files</li><li>• Cloud Volumes ONTAP</li><li>• Cloud Volumes Service</li><li>• Google Cloud Storage</li><li>• IBM Cloud 物件儲存設備</li><li>• NFS 伺服器</li><li>• 內部部署 ONTAP 的叢集</li><li>• SMB 伺服器</li><li>• StorageGRID</li></ul>

來源位置	支援的目標位置
Amazon S3	<ul style="list-style-type: none"> <li>• Amazon EFS</li> <li>• Amazon FSX for ONTAP Sf</li> <li>• Amazon S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files</li> <li>• 方塊<sup>1</sup></li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Google Cloud Storage</li> <li>• IBM Cloud 物件儲存設備</li> <li>• NFS 伺服器</li> <li>• 內部部署 ONTAP 的叢集</li> <li>• SMB 伺服器</li> <li>• StorageGRID</li> </ul>
Azure Blob	<ul style="list-style-type: none"> <li>• Amazon EFS</li> <li>• Amazon FSX for ONTAP Sf</li> <li>• Amazon S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files</li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Google Cloud Storage</li> <li>• IBM Cloud 物件儲存設備</li> <li>• NFS 伺服器</li> <li>• 內部部署 ONTAP 的叢集</li> <li>• SMB 伺服器</li> <li>• StorageGRID</li> </ul>

來源位置	支援的目標位置
Azure NetApp Files	<ul style="list-style-type: none"> <li>• Amazon EFS</li> <li>• Amazon FSX for ONTAP Sf</li> <li>• Amazon S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files</li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Google Cloud Storage</li> <li>• IBM Cloud 物件儲存設備</li> <li>• NFS 伺服器</li> <li>• 內部部署 ONTAP 的叢集</li> <li>• SMB 伺服器</li> <li>• StorageGRID</li> </ul>
方塊 <sup>1</sup>	<ul style="list-style-type: none"> <li>• Amazon FSX for ONTAP Sf</li> <li>• Amazon S3</li> <li>• Azure NetApp Files</li> <li>• Cloud Volumes ONTAP</li> <li>• IBM Cloud 物件儲存設備</li> <li>• NFS 伺服器</li> <li>• SMB 伺服器</li> <li>• StorageGRID</li> </ul>

來源位置	支援的目標位置
Cloud Volumes ONTAP	<ul style="list-style-type: none"> <li>• Amazon EFS</li> <li>• Amazon FSX for ONTAP Sf</li> <li>• Amazon S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files</li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Google Cloud Storage</li> <li>• IBM Cloud 物件儲存設備</li> <li>• NFS 伺服器</li> <li>• 內部部署 ONTAP 的叢集</li> <li>• SMB 伺服器</li> <li>• StorageGRID</li> </ul>
Cloud Volumes Service	<ul style="list-style-type: none"> <li>• Amazon EFS</li> <li>• Amazon FSX for ONTAP Sf</li> <li>• Amazon S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files</li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Google Cloud Storage</li> <li>• IBM Cloud 物件儲存設備</li> <li>• NFS 伺服器</li> <li>• 內部部署 ONTAP 的叢集</li> <li>• SMB 伺服器</li> <li>• StorageGRID</li> </ul>

來源位置	支援的目標位置
Google Cloud Storage	<ul style="list-style-type: none"> <li>• Amazon EFS</li> <li>• Amazon FSX for ONTAP Sf</li> <li>• Amazon S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files</li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Google Cloud Storage</li> <li>• IBM Cloud 物件儲存設備</li> <li>• NFS 伺服器</li> <li>• 內部部署 ONTAP 的叢集</li> <li>• SS3 儲存設備 ONTAP</li> <li>• SMB 伺服器</li> <li>• StorageGRID</li> </ul>
IBM Cloud 物件儲存設備	<ul style="list-style-type: none"> <li>• Amazon EFS</li> <li>• Amazon FSX for ONTAP Sf</li> <li>• Amazon S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files</li> <li>• 方塊<sup>1</sup></li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Google Cloud Storage</li> <li>• IBM Cloud 物件儲存設備</li> <li>• NFS 伺服器</li> <li>• 內部部署 ONTAP 的叢集</li> <li>• SMB 伺服器</li> <li>• StorageGRID</li> </ul>

來源位置	支援的目標位置
NFS 伺服器	<ul style="list-style-type: none"> <li>• Amazon EFS</li> <li>• Amazon FSX for ONTAP Sf</li> <li>• Amazon S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files</li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Google Cloud Storage</li> <li>• IBM Cloud 物件儲存設備</li> <li>• NFS 伺服器</li> <li>• 內部部署 ONTAP 的叢集</li> <li>• SMB 伺服器</li> <li>• StorageGRID</li> </ul>
內部ONTAP 使用的叢集	<ul style="list-style-type: none"> <li>• Amazon EFS</li> <li>• Amazon FSX for ONTAP Sf</li> <li>• Amazon S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files</li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Google Cloud Storage</li> <li>• IBM Cloud 物件儲存設備</li> <li>• NFS 伺服器</li> <li>• 內部部署 ONTAP 的叢集</li> <li>• SMB 伺服器</li> <li>• StorageGRID</li> </ul>
SS3 儲存設備 ONTAP	<ul style="list-style-type: none"> <li>• Google Cloud Storage</li> <li>• SMB 伺服器</li> <li>• StorageGRID</li> <li>• SS3 儲存設備 ONTAP</li> </ul>
SFTP <sup>2</sup>	S3

來源位置	支援的目標位置
SMB 伺服器	<ul style="list-style-type: none"> <li>• Amazon EFS</li> <li>• Amazon FSX for ONTAP Sf</li> <li>• Amazon S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files</li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Google Cloud Storage</li> <li>• IBM Cloud 物件儲存設備</li> <li>• NFS 伺服器</li> <li>• 內部部署 ONTAP 的叢集</li> <li>• SS3 儲存設備 ONTAP</li> <li>• SMB 伺服器</li> <li>• StorageGRID</li> </ul>
StorageGRID	<ul style="list-style-type: none"> <li>• Amazon EFS</li> <li>• Amazon FSX for ONTAP Sf</li> <li>• Amazon S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files</li> <li>• 方塊<sup>1</sup></li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Google Cloud Storage</li> <li>• IBM Cloud 物件儲存設備</li> <li>• NFS 伺服器</li> <li>• 內部部署 ONTAP 的叢集</li> <li>• SS3 儲存設備 ONTAP</li> <li>• SMB 伺服器</li> <li>• StorageGRID</li> </ul>

附註：

1. Box支援可預覽。
2. 只有使用Cloud Sync 支援與此來源/目標的同步關係、才能支援此功能。
3. 當 Blob 容器為目標時、您可以選擇特定的 Azure Blob 儲存層：



- 熱儲存
- 超酷儲存設備

4. [[storage類別]當Amazon S3為目標時、您可以選擇特定的S3儲存類別：

- 標準（這是預設類別）
- 智慧分層
- 標準非常用存取
- 單一區域不常用存取
- 冰川
- Glacier Deep 歸檔

5. 當Google Cloud Storage儲存桶成為目標時、您可以選擇特定的儲存類別：

- 標準
- 近線
- 冷線
- 歸檔

## 準備來源和目標

確認您的來源和目標符合下列要求。

### 網路

- 來源和目標必須與資料代理群組建立網路連線。

例如、如果您的資料中心有NFS伺服器、而且資料代理程式位於AWS中、則您需要從網路連線（VPN或Direct Connect）到VPC。

- NetApp建議將來源、目標和資料代理人設定為使用網路時間傳輸協定（NTP）服務。三個元件之間的時間差異不應超過 5 分鐘。

### 目標目錄

建立同步關係時Cloud Sync、利用支援功能、您可以選取現有的目標目錄、然後在該目錄中建立新的資料夾（可選）。因此請確定您偏好的目標目錄已經存在。

### 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、Cloud Sync 需要目錄或資料夾的讀取權限。

#### NFS

必須在來源/目標上定義權限、並在檔案和目錄上使用uid / gid。

#### 物件儲存

- 對於AWS和Google Cloud、資料代理程式必須擁有清單物件權限（如果您依照資料代理程式的安裝步驟

執行、預設會提供這些權限)。

- 對於 Azure、StorageGRID 物件和 IBM、您在設定同步關係時輸入的認證資料必須具有清單物件權限。

## 中小企業

設定同步關係時輸入的 SMB 認證必須具有清單資料夾權限。



資料代理程式預設會忽略下列目錄：.snapshot、~snapshot、.Copy-卸 載

## Amazon S3 儲存桶需求

請確定您的 Amazon S3 儲存庫符合下列要求。

### Amazon S3 支援的資料代理位置

包含 S3 儲存設備的同步關係需要部署在 AWS 或內部部署的資料代理程式。無論是哪一種情況 Cloud Sync、安裝期間、資訊中心都會提示您將資料代理程式與 AWS 帳戶建立關聯。

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

### 支援的 AWS 區域

除了中國地區以外、所有地區都受到支援。

### 其他 AWS 帳戶中 S3 儲存區所需的權限

設定同步關係時、您可以指定 S3 儲存區、該儲存區位於與資料代理程式無關的 AWS 帳戶中。

["此 Json 檔案所含的權限"](#) 必須套用至該 S3 儲存區、資料代理人才能存取該儲存區。這些權限可讓資料代理人將資料複製到儲存庫、或從儲存庫複製資料、並列出儲存庫中的物件。

請注意以下關於 Json 檔案所含權限的資訊：

1. `<BucketName>` 是儲存在 AWS 帳戶中、與資料代理程式無關的儲存區名稱。
2. `<RoleARN>` 應更換為下列其中一項：
  - 如果資料代理程式是手動安裝在 Linux 主機上、則 `_ROLEARN_` 應該是 AWS 使用者的 ARN、您在部署資料代理程式時會提供 AWS 認證。
  - 如果使用 CloudFormation 範本在 AWS 中部署資料代理程式、則 `_RoleARN_` 應該是範本所建立之 IAM 角色的 ARN。

您可以前往 EC2 主控台、選取資料代理執行個體、然後按一下「Description (說明)」索引標籤中的 IAM 角色、以找到角色 ARN。接著、您應該會在 IAM 主控台中看到「摘要」頁面、其中包含角色 ARN。

## Summary

[Delete role](#)

**Role ARN** `arn:aws:iam::642991779896:role/tanyaBroker0304-DataBrokerIamRole-1VMHWXMW3AQ05` [Copy](#)

**Role description** [Edit](#)

### Azure Blob 儲存需求

請確定您的 Azure Blob 儲存設備符合下列需求。

#### Azure Blob 支援的資料代理程式位置

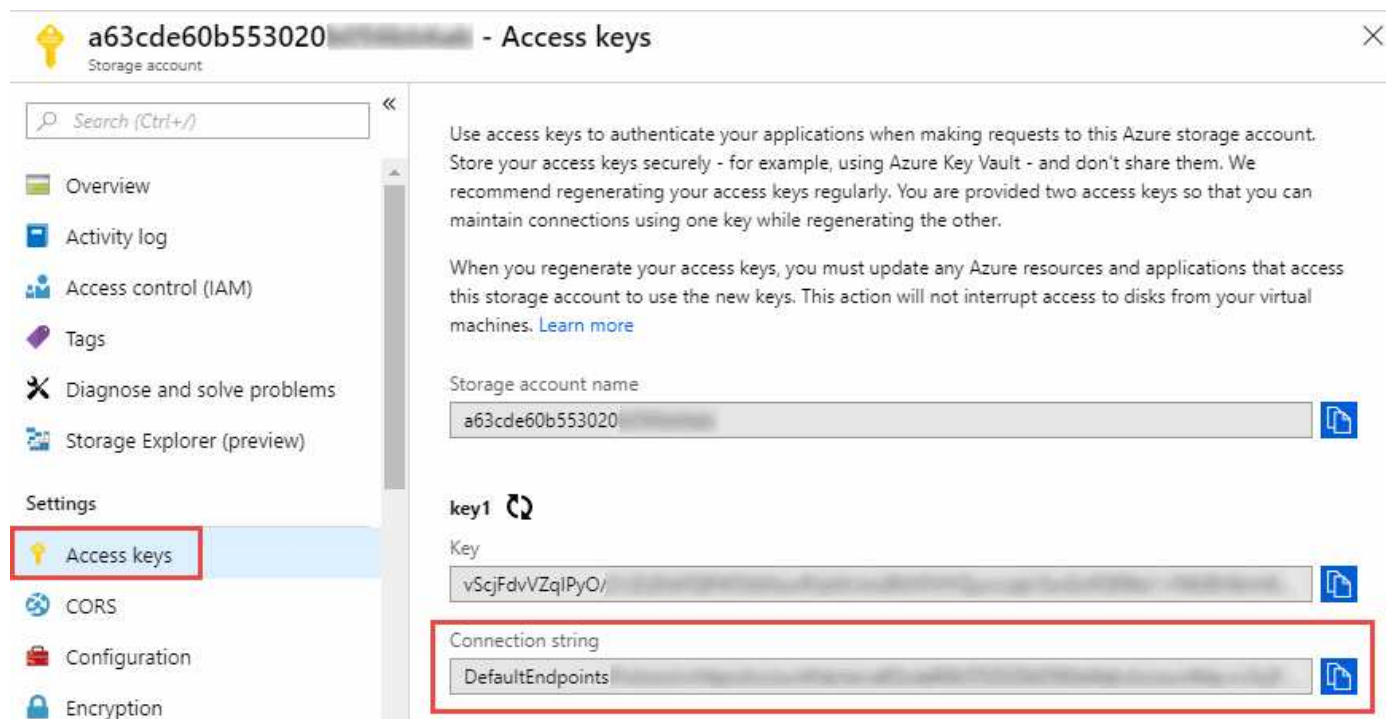
當同步關係包含 Azure Blob 儲存設備時、資料代理程式可位於任何位置。

#### 支援的 Azure 地區

除了中國、美國 Gov 和美國 DoD 地區之外、所有地區都受到支援。

#### 包括 Azure Blob 和 NFS/SMB 之關係的連線字串

在 Azure Blob 容器和 NFS 或 SMB 伺服器之間建立同步關係時、您需要提供含有儲存帳戶連線字串的功能：



**a63cde60b553020** - Access keys

Storage account

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

如果您想要在兩個 Azure Blob 容器之間同步資料、則連線字串必須包含 a "共享存取簽名" (SAS)。您也可以選擇在 Blob 容器與 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 也必須包含下列權限：

- 對於來源 Blob 容器：讀取並列出
- 對於目標 Blob 容器：讀取、寫入、清單、新增及建立

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

## 需求 Azure NetApp Files

在 Azure NetApp Files 將資料同步至或從支援中心同步時、請使用 Premium 或 Ultra 服務層級。如果磁碟服務層級為「Standard（標準）」、您可能會遇到故障和效能問題。

如果您需要協助判斷適當的服務層級、請洽詢解決方案架構設計師。磁碟區大小和磁碟區層會決定您可以獲得的處理量。

"深入瞭解 Azure NetApp Files 解有關服務層級和處理量的資訊"。

## Box需求

- 若要建立包含Box的同步關係、您必須提供下列認證資料：
  - 用戶端ID
  - 用戶端機密
  - 私密金鑰
  - 公開金鑰ID
  - 通關密碼

26

- 企業ID
  - 如果您從Amazon S3建立同步關係至Box、則必須使用統一組態的資料代理人群組、其中下列設定設為1：
    - 掃描器並行性
    - 掃描器處理程序限制
    - Transferrer並行性
    - Transferrer處理程序限制
- ["瞭解如何定義資料代理群組的統一化組態"](#)。

## Google Cloud Storage 儲存桶需求

請確定您的 Google Cloud Storage 儲存庫符合下列需求。

### Google Cloud Storage 支援的資料代理商位置

包括Google Cloud Storage在內的同步關係需要部署在Google Cloud或內部部署的資料代理商。建立同步關係時、可利用此功能引導您完成資料代理程式的安裝程序。 Cloud Sync

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

### 支援的 Google Cloud 地區

支援所有地區。

### 其他Google Cloud專案中的儲存區權限

設定同步關係時、如果您提供資料代理商服務帳戶所需的權限、您可以從不同專案的Google Cloud儲存庫中進行選擇。 ["瞭解如何設定服務帳戶"](#)。

### SnapMirror 目的地的權限

如果同步關係的來源是 SnapMirror 目的地（唯讀）、「讀取 / 清單」權限就足以將資料從來源同步至目標。

## NFS 伺服器需求

- NFS 伺服器可以是 NetApp 系統或非 NetApp 系統。
- 檔案伺服器必須允許資料代理主機透過所需的連接埠存取匯出。
  - 111 TCP / udp
  - 2049 TCP/IP
  - 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。

- 如果您想要從 ONTAP 某個支援系統同步 NFS 資料、請確定已啟用 SVM 的 NFS 匯出清單（已啟用 `vserver NFS modify -vserver svm_name -showmount`）。



showmount 的預設設定為「啟用 \_」、從 ONTAP SURF9.2 開始。

## 需求 ONTAP

如果同步關係包含 Cloud Volumes ONTAP 了不同步或內部 ONTAP 使用的叢集、而您選擇 NFSv4 或更新版本、則需要在 ONTAP 不同步系統上啟用 NFSv4 ACL。這是複製 ACL 所必需的。

## SS3 儲存需求 ONTAP

當您設定包含的同步關係時 "[SS3 儲存設備 ONTAP](#)"、您需要提供下列項目：

- 連接 ONTAP 到 SS3 的 LIF IP 位址
- 設定使用的存取金鑰和秘密金鑰 ONTAP

## SMB 伺服器需求

- SMB 伺服器可以是 NetApp 系統或非 NetApp 系統。
- 您需要提供 Cloud Sync 對 SMB 伺服器具有權限的認證資料。
  - 對於來源 SMB 伺服器、需要下列權限：清單和讀取。

來源 SMB 伺服器支援 Backup Operators 群組成員。
  - 對於目標 SMB 伺服器、需要下列權限：清單、讀取和寫入。
- 檔案伺服器必須允許資料代理主機透過所需的連接埠存取匯出。
  - 139 TCP
  - 445 TCP
  - 137-138 udp
- 支援 SMB 1.0、2.0、2.1、3.0 和 3.11. 版。
- 授予「系統管理員」群組對來源和目標資料夾具有「完全控制」權限。

如果您未授予此權限、資料代理程式可能沒有足夠的權限、無法取得檔案或目錄上的 ACL。如果發生這種情況、您將會收到下列錯誤：「getxattr 錯誤 95」

## 隱藏目錄和檔案的 SMB 限制

SMB 限制會在 SMB 伺服器之間同步資料時、影響隱藏的目錄和檔案。如果來源 SMB 伺服器上的任何目錄或檔案透過 Windows 隱藏、則不會將隱藏屬性複製到目標 SMB 伺服器。

## SMB 同步行為是因為不區分大小寫的限制

SMB 傳輸協定不區分大小寫、這表示大小寫字母會被視為相同。如果同步關係包含 SMB 伺服器、且目標上已存在資料、則此行為可能會導致覆寫檔案和目錄複製錯誤。

例如、假設來源上有一個名為「A」的檔案、而目標上有一個名為「A」的檔案。當將名為「A」的檔案複製到目標時、檔案「A」會被來源的檔案「A」覆寫。Cloud Sync

就目錄而言、假設來源上有一個名為「b」的目錄、而目標上有一個名為「B」的目錄。當試圖將名為「b」的目錄複製到目標時、會收到錯誤訊息指出該目錄已經存在。Cloud Sync因此 Cloud Sync、無法複製名為「b」的目錄。

避免此限制的最佳方法是確保您將資料同步至空白目錄。

## 網路概述 Cloud Sync

適用於此技術的網路Cloud Sync 功能包括資料代理群組與來源和目標位置之間的連線、以及透過連接埠443從資料代理程式傳出的網際網路連線。

### 資料代理程式位置

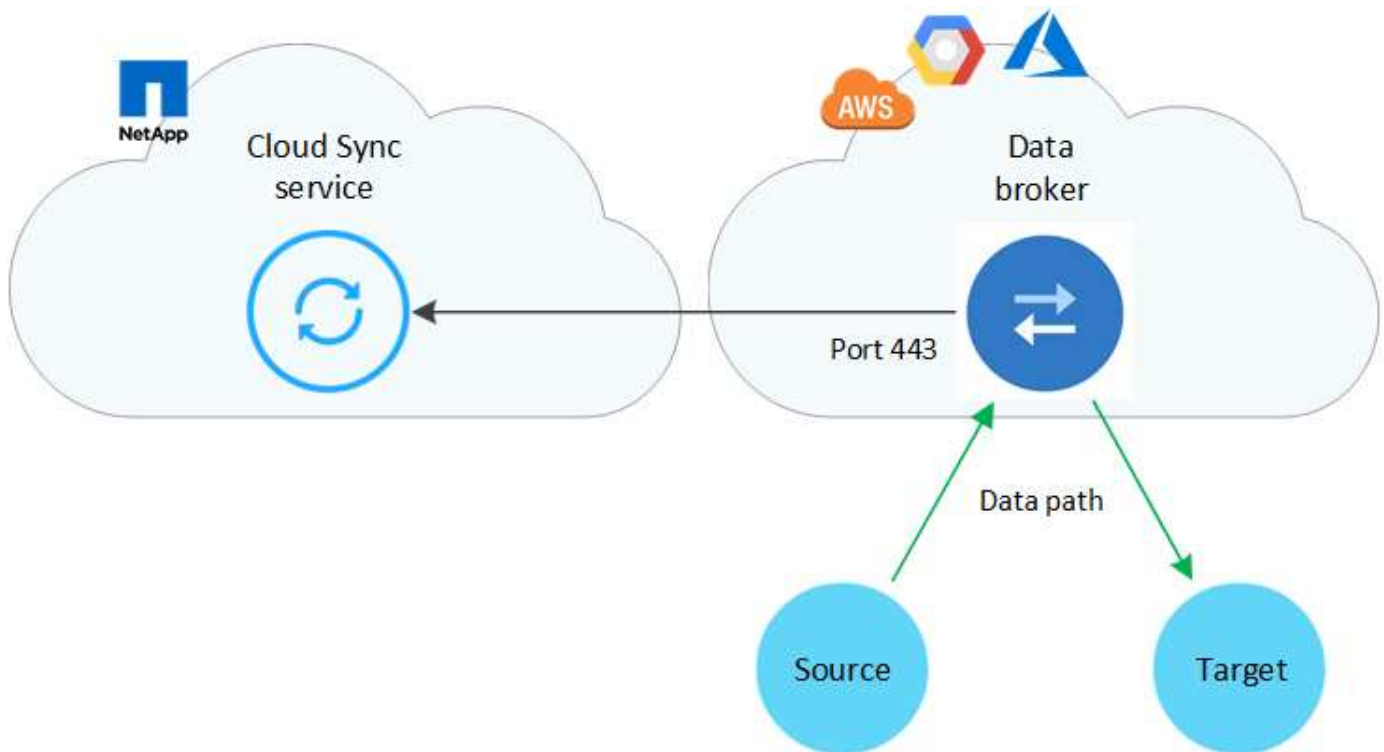
資料代理人群組由安裝在雲端或內部部署中的一或多個資料代理人所組成。

#### 雲端資料代理商

下圖顯示在AWS、Google Cloud或Azure雲端上執行的資料代理程式。只要有資料代理的連線、來源和目標就可以位於任何位置。例如、您的資料中心與雲端供應商之間可能有VPN連線。



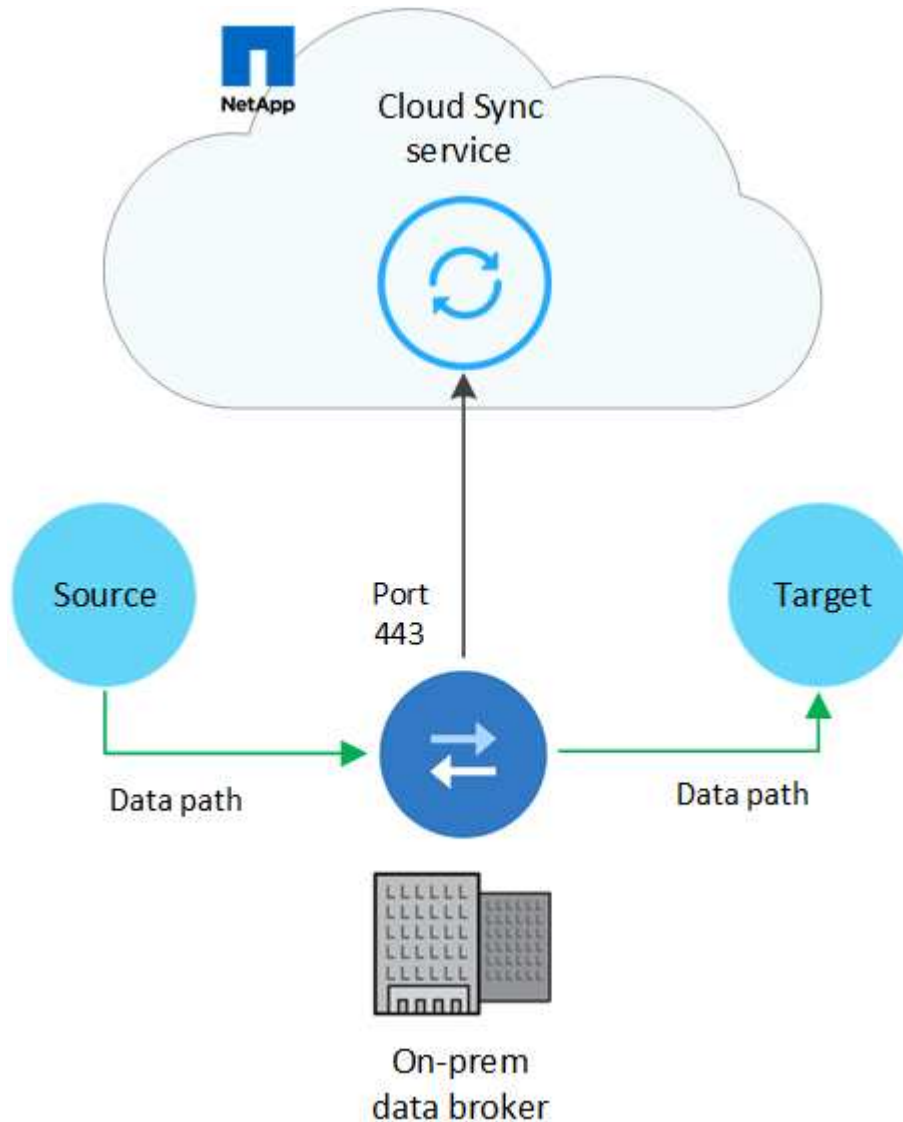
當在AWS、Azure或Google Cloud中部署資料代理程式時、它會建立一個安全群組、以啟用必要的傳出通訊。Cloud Sync





## 內部部署的資料代理程式

下圖顯示資料中心內部執行的資料代理程式。同樣地、只要有資料代理的連線、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群組建立網路連線。

例如、如果您的資料中心有NFS伺服器、而且資料代理程式位於AWS中、則您需要從網路連線（VPN或Direct Connect）到VPC。

- 資料代理人需要傳出的網際網路連線、以便透過Cloud Sync 連接埠443輪詢該服務的工作。
- NetApp建議將來源、目標和資料代理人設定為使用網路時間傳輸協定（NTP）服務。三個元件之間的時間差異不應超過 5 分鐘。



## 網路端點

NetApp 資料代理商需要透過連接埠 443 進行傳出網際網路存取、才能與 Cloud Sync 該服務進行通訊、並聯絡其他服務與儲存庫。您的本機網頁瀏覽器也需要存取端點才能執行特定動作。如果您需要限制傳出連線、請參閱下列端點清單、以設定傳出流量的防火牆。

### 資料代理端點

資料代理程式會連絡下列端點：

端點	目的
<a href="https://olcentgbl.trafficmanager.net">https://olcentgbl.trafficmanager.net</a>	聯絡儲存庫以更新資料代理主機的 CentOS 套件。只有在 CentOS 主機上手動安裝資料代理程式時、才會聯絡此端點。
<a href="https://rpm.nodesource.com">https://rpm.nodesource.com</a> <a href="https://registry.npmjs.org">https://registry.npmjs.org</a> <a href="https://nodejs.org">https://nodejs.org</a> :	聯絡儲存庫以更新開發中使用的 Node.js、nPM 及其他協力廠商套件。
<a href="https://tgz.pm2.io">https://tgz.pm2.io</a>	存取儲存庫以更新 PM2、這是用於監控 Cloud Sync 顯示器的第三方套件。
<a href="https://sqs.us-east-1.amazonaws.com">https://sqs.us-east-1.amazonaws.com</a> <a href="https://kinesis.us-east-1.amazonaws.com">https://kinesis.us-east-1.amazonaws.com</a>	聯絡 Cloud Sync 支援營運的 AWS 服務（佇列檔案、登錄行動、以及提供資料代理程式的更新）。
<a href="https://s3.region.amazonaws.com">https://s3.region.amazonaws.com</a> 例如： <a href="https://s3.us-east-2.amazonaws.com:443https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region">s3.us-east-2.amazonaws.com:443https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region</a> ["如需 S3 端點清單、請參閱 AWS 文件"]	在同步關係包含 S3 儲存區時聯絡 Amazon S3。
<a href="https://s3.us-east-1.amazonaws.com">https://s3.us-east-1.amazonaws.com</a>	當您從 Cloud Sync S 動物性 下載資料代理記錄時、資料代理程式會將其記錄目錄壓縮、並將記錄上傳至美東1區的預先定義S3儲存區。
<a href="https://cf.cloudsync.netapp.com">https://cf.cloudsync.netapp.com</a> <a href="https://repo.cloudsync.netapp.com">https://repo.cloudsync.netapp.com</a>	聯絡 Cloud Sync 服務部門。
<a href="https://support.netapp.com">https://support.netapp.com</a>	在使用 BYOL 授權進行同步關係時聯絡 NetApp 支援部門。
<a href="https://fedoraproject.org">https://fedoraproject.org</a>	在安裝與更新期間、在資料代理虛擬機器上安裝 7z。需要 7z 將 AutoSupport 資訊傳送給 NetApp 技術支援部門。
<a href="https://sts.amazonaws.com">https://sts.amazonaws.com</a>	可在資料代理程式部署於AWS或部署於內部部署且提供AWS認證資料時、驗證AWS認證資料。資料代理程式會在部署期間、更新時及重新啟動時聯絡此端點。
<a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a> <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a>	若要在使用Data Sense選取新同步關係的來源檔案時聯絡Cloud Data Sense。

### Web 瀏覽器端點

您的網路瀏覽器需要存取下列端點、才能下載記錄以進行疑難排解：

[logs.cloudsync.netapp.com:443](https://logs.cloudsync.netapp.com:443)

# 安裝資料代理程式

## 在AWS中建立新的資料代理程式

當您建立新的資料代理人群組時、請選擇Amazon Web Services、在VPC的新EC2執行個體上部署資料代理人軟體。本頁將會重複提供安裝程序的支援、協助您做好安裝準備。  
Cloud Sync

您也可以選擇在雲端或內部部署的現有 Linux 主機上安裝資料代理程式。["深入瞭解"](#)。

### 支援的 AWS 區域

除了中國地區以外、所有地區都受到支援。

### 網路需求

- 資料代理人需要傳出的網際網路連線、以便透過 Cloud Sync 連接埠 443 輪詢該服務的工作。

當在 AWS 中部署資料代理程式時 Cloud Sync、它會建立一個安全群組、以啟用必要的傳出通訊。請注意、您可以設定資料代理程式在安裝過程中使用 Proxy 伺服器。

如果您需要限制傳出連線、請參閱 ["資料代理所連絡的端點清單"](#)。

- NetApp 建議將來源、目標及資料代理程式設定為使用網路時間傳輸協定（NTP）服務。三個元件之間的時間差異不應超過 5 分鐘。

## 在 AWS 中部署資料代理程式所需的權限

您用來部署資料代理程式的 AWS 使用者帳戶必須具有中所含的權限 ["此 NetApp 提供的原則"](#)。

### 將您自己的 IAM 角色用於 AWS 資料代理程式的要求

當執行數據代理部署時、它會為資料代理執行個體建立 IAM 角色。Cloud Sync您可以視需要使用自己的 IAM 角色來部署資料代理程式。如果您的組織具有嚴格的安全性原則、您可以使用此選項。

IAM 角色必須符合下列要求：

- 必須允許 EC2 服務以信任實體的身分承擔 IAM 角色。
- ["在此 Json 檔案中定義的權限"](#) 必須附加至 IAM 角色、資料代理才能正常運作。

部署資料代理程式時、請依照下列步驟指定 IAM 角色。

### 建立資料代理程式

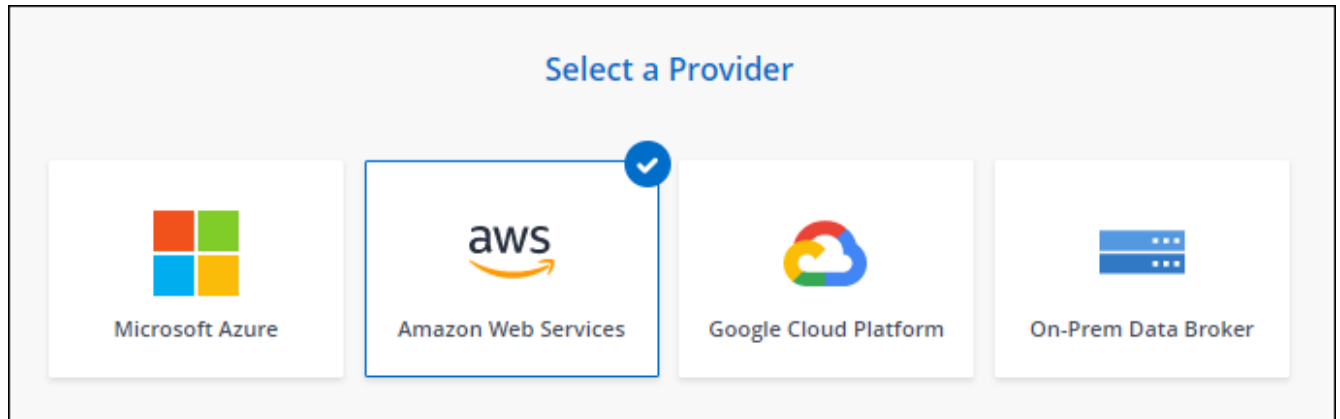
有幾種方法可以建立新的資料代理程式。這些步驟說明如何在建立同步關係時、在AWS中安裝資料代理程式。

#### 步驟

- 按一下「\* 建立新同步 \*」。
- 在「\* 定義同步關係 \*」頁面上、選擇來源和目標、然後按一下「\* 繼續 \*」。

完成這些步驟、直到您到達「資料代理人群組」頁面為止。

3. 在「資料代理人群組」頁面上、按一下「建立資料代理人」、然後選取「\* Amazon Web Services\*」。



4. 輸入資料代理的名稱、然後按一下 \* 繼續 \*。
5. 輸入 AWS 存取金鑰、Cloud Sync 以便讓支援代表您在 AWS 中建立資料代理程式。

金鑰不會儲存或用於任何其他用途。

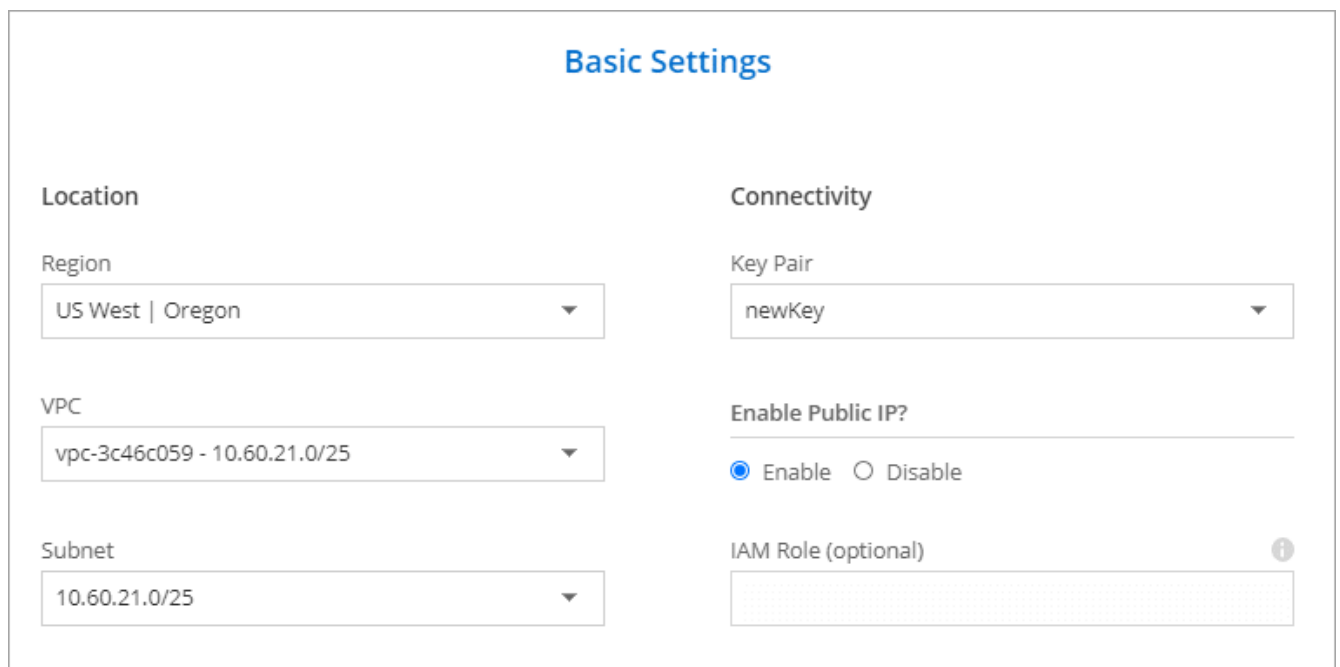
如果您不想提供存取金鑰、請按一下頁面底部的連結、改用 CloudFormation 範本。使用此選項時、您不需要提供認證、因為您是直接登入 AWS。

[CFT] 下列影片說明如何使用 CloudFormation 範本啟動資料代理執行個體：

► [https://docs.netapp.com/zh-tw/cloud-manager-sync//media/video\\_cloud\\_sync.mp4](https://docs.netapp.com/zh-tw/cloud-manager-sync//media/video_cloud_sync.mp4) (video)

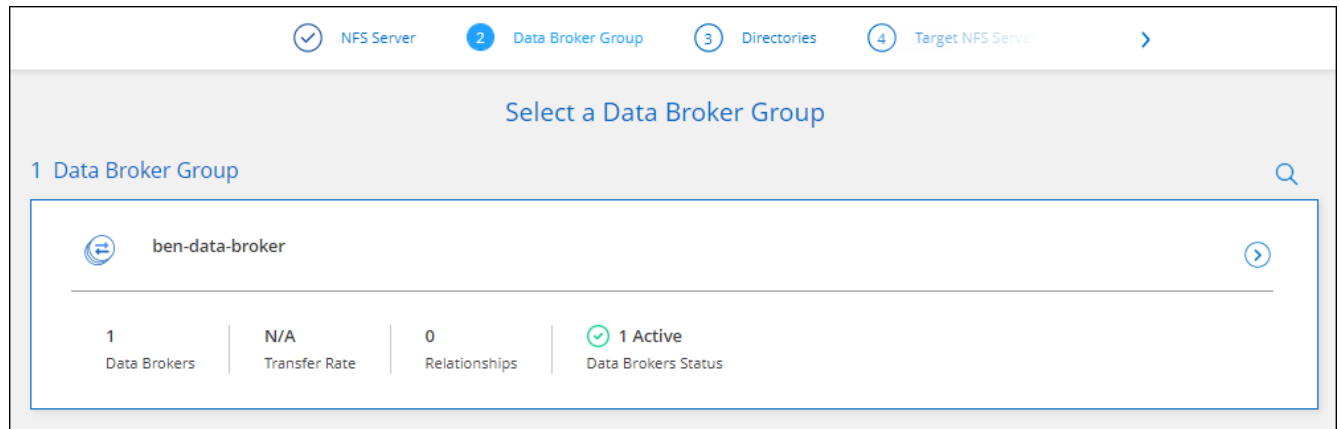
6. 如果您輸入 AWS 存取金鑰、請選取執行個體的位置、選取金鑰組、選擇是否啟用公用 IP 位址、然後選取現有的 IAM 角色、或將欄位保留空白、Cloud Sync 以便讓 NetApp 為您建立角色。

如果您選擇自己的 IAM 角色、[您需要提供必要的權限](#)。



7. 如果 VPC 中的網際網路存取需要 Proxy 、請指定 Proxy 組態。
8. 在資料代理程式可用之後、按 Cloud Sync 一下「」中的「\* 繼續 \*」。

下列影像顯示 AWS 中已成功部署的執行個體：



9. 完成精靈中的頁面、以建立新的同步關係。

您已在 AWS 中部署資料代理程式、並建立新的同步關係。您可以使用此資料代理人群組與其他同步關係。

資料代理執行個體的詳細資料

使用下列組態、在AWS中建立資料代理程式。Cloud Sync

執行個體類型

m5n.xlarge（如果該地區有）、否則m5.xlarge

**vCPU**

4.

**RAM**

16 GB

作業系統

Amazon Linux 2.

磁碟大小與類型

10 GB GP2 SSD

在**Azure**中建立新的資料代理程式

當您建立新的資料代理人群組時、請選擇Microsoft Azure、將資料代理人軟體部署在vnet中的新虛擬機器上。本頁將會重複提供安裝程序的支援、協助您做好安裝準備。 Cloud Sync

您也可以選擇在雲端或內部部署的現有 Linux 主機上安裝資料代理程式。 ["深入瞭解"](#)。

## 支援的 Azure 地區

除了中國、美國 Gov 和美國 DoD 地區之外、所有地區都受到支援。

## 網路需求

- 資料代理人需要傳出的網際網路連線、以便透過 Cloud Sync 連接埠 443 輪詢該服務的工作。

當在 Azure 中部署資料代理程式時 Cloud Sync、它會建立一個安全群組、以啟用必要的傳出通訊。

如果您需要限制傳出連線、請參閱 ["資料代理所連絡的端點清單"](#)。

- NetApp 建議將來源、目標及資料代理程式設定為使用網路時間傳輸協定（NTP）服務。三個元件之間的時間差異不應超過 5 分鐘。

## 在 Azure 中部署資料代理程式所需的權限

請確定您用來部署資料代理程式的 Azure 使用者帳戶具有下列權限。

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

```

## 驗證方法

部署資料代理程式時、您需要為虛擬機器選擇驗證方法：密碼或SSH公用-私密金鑰配對。

如需建立金鑰配對的協助、請參閱 ["Azure 說明文件：為 Azure 中的 Linux VM 建立及使用 SSH 公開私密金鑰配對"](#)。

## 建立資料代理程式

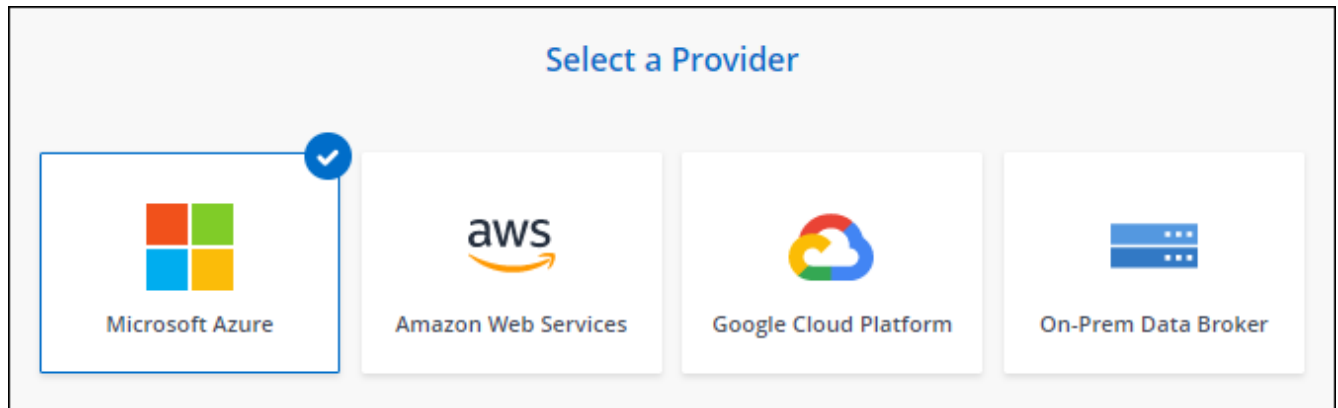
有幾種方法可以建立新的資料代理程式。這些步驟說明如何在建立同步關係時、在Azure中安裝資料代理程式。

### 步驟

1. 按一下「\* 建立新同步 \*」。
2. 在「\* 定義同步關係 \*」頁面上、選擇來源和目標、然後按一下「\* 繼續 \*」。

完成這些步驟、直到您到達「資料代理人群組」頁面為止。

3. 在「資料代理人群組」頁面上、按一下「建立資料代理人」、然後選取「\* Microsoft Azure \*」。



4. 輸入資料代理的名稱、然後按一下 \* 繼續 \* 。
5. 如果出現提示、請登入您的 Microsoft 帳戶。如果系統沒有提示、請按一下 \* 登入 Azure \* 。

此表單由 Microsoft 擁有及託管。您的認證資料不會提供給 NetApp 。

6. 選擇資料代理的位置、然後輸入虛擬機器的基本詳細資料。

7. 如果 Vnet 中的網際網路存取需要 Proxy 、請指定 Proxy 組態。
8. 按一下「\* 繼續 \*」並保持頁面開啟、直到部署完成為止。

此程序可能需要 7 分鐘的時間。

9. 在本功能中、當資料代理程式可供使用時、請按一下 \* 繼續 \* 。 Cloud Sync
10. 完成精靈中的頁面、以建立新的同步關係。



您已在 Azure 中部署資料代理程式、並建立新的同步關係。您可以將此資料代理程式與其他同步關係搭配使用。

### 是否收到需要管理員同意的訊息？

如果 Microsoft 通知您需要系統管理員核准、因為 Cloud Sync 支援功能需要權限才能代表您存取組織中的資源、那麼您有兩種選擇：

1. 請您的 AD 管理員提供下列權限給您：

在 Azure 中、請前往 \* 管理中心 > Azure AD > 使用者與群組 > 使用者設定 \*、並啟用 \* 使用者可以同意代表他們存取公司資料的應用程式 \*。

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

[https://login.microsoftonline.com/{FILL 這裡是您的租戶 ID } /v2.0/adminfit? client\\_id=8ee4ca3a-bAa-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/{FILL 這裡是您的租戶 ID } /v2.0/adminfit? client_id=8ee4ca3a-bAa-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 為 <https://cloudsync.netapp.com>、應用程式用戶端 ID 為 8ee4ca3a-bfa-4831-97cc-5a38923cab85。

### 資料代理VM的詳細資料

使用下列組態、在 Azure 中建立資料代理程式。Cloud Sync

#### VM 類型

標準 DS4 v2

#### vCPU

8.

#### RAM

28 GB

#### 作業系統

CentOS 7.7

#### 磁碟大小與類型

64 GB Premium SSD

### 在 Google Cloud 中建立新的資料代理商

當您建立新的資料代理人群組時、請選擇 Google Cloud Platform、在 Google Cloud VPC 的新虛擬機器執行個體上部署資料代理人軟體。本頁將會重複提供安裝程序的支援、協助您做好安裝準備。Cloud Sync



您也可以選擇在雲端或內部部署的現有 Linux 主機上安裝資料代理程式。"深入瞭解"。

支援的 **Google Cloud** 地區

支援所有地區。

網路需求

- 資料代理人需要傳出的網際網路連線、以便透過 Cloud Sync 連接埠 443 輪詢該服務的工作。

當在Google Cloud中部署資料代理程式時Cloud Sync、它會建立一個安全群組、以啟用必要的傳出通訊。

如果您需要限制傳出連線、請參閱 "資料代理所連絡的端點清單"。

- NetApp 建議將來源、目標及資料代理程式設定為使用網路時間傳輸協定（NTP）服務。三個元件之間的時間差異不應超過 5 分鐘。

在**Google Cloud**中部署資料代理商所需的權限

確保部署資料代理程式的Google Cloud使用者具有下列權限：

```
- 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、您需要選取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.*
- iam.serviceAccounts.signJwt
```



只有當您打算設定資料代理程式使用外部HashiCorp保存庫時、才需要iam.serviceAccounts.signJwt"權限。

建立資料代理程式

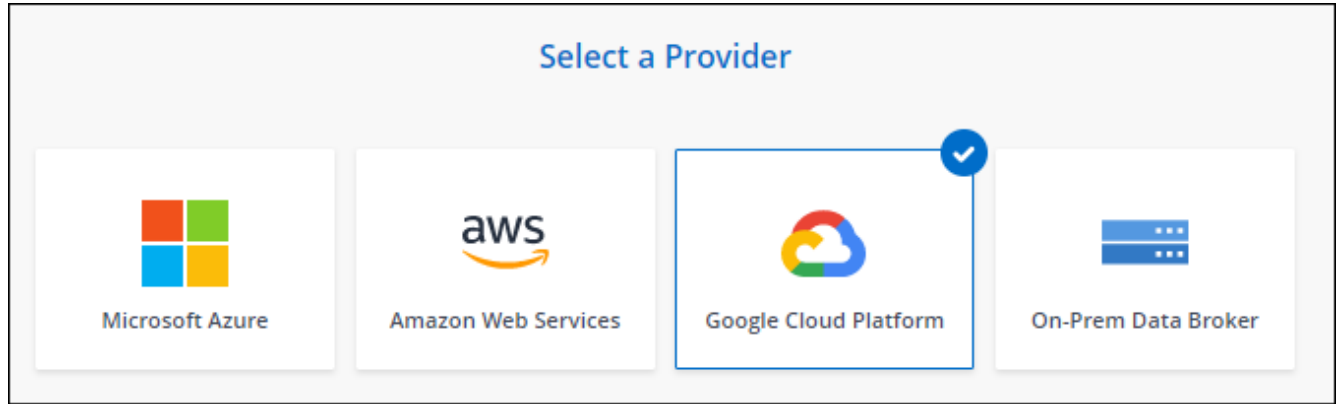
有幾種方法可以建立新的資料代理程式。這些步驟說明如何在建立同步關係時、在Google Cloud中安裝資料代理程式。

## 步驟

1. 按一下「\* 建立新同步 \*」。
2. 在「\* 定義同步關係 \*」頁面上、選擇來源和目標、然後按一下「\* 繼續 \*」。

完成這些步驟、直到您到達「資料代理人群組」頁面為止。

3. 在「資料代理人群組」頁面上、按一下「建立資料代理人」、然後選取「\* Microsoft Azure \*」。



4. 輸入資料代理的名稱、然後按一下 \* 繼續 \* 。
  5. 如果出現提示、請使用 Google 帳戶登入。
- 這份表單由 Google 擁有及託管。您的認證資料不會提供給 NetApp 。
6. 選取專案和服務帳戶、然後選擇資料代理的位置、包括要啟用或停用公用IP位址。

如果您未啟用公用IP位址、則需要在下一步定義Proxy伺服器。

### Basic Settings

**Project**

Project

OCCM-Dev

**Location**

Region

us-west1

**Service Account**

test

**Zone**

us-west1-a

Select a Service Account that includes [these permissions](#)

**VPC**

default

**Subnet**

default

**Public IP**

Enable

7. 如果 VPC 中的網際網路存取需要 Proxy 、請指定 Proxy 組態。

如果網際網路存取需要 Proxy 、則 Proxy 必須位於 Google Cloud 中、並使用與資料代理相同的服務帳戶。

8. 一旦資料代理程式可供使用、請按 Cloud Sync 一下《》中的 \* 「Continue」 （繼續） \* 。

執行個體部署約需 5 至 10 分鐘。您可以監控 Cloud Sync 來自於此服務的進度、當執行個體可用時、此服務會自動重新整理。

9. 完成精靈中的頁面、以建立新的同步關係。

您已在Google Cloud中部署資料代理商、並建立新的同步關係。您可以將此資料代理程式與其他同步關係搭配使用。

提供在其他**Google Cloud**專案中使用儲存區的權限

當您建立同步關係並選擇Google Cloud Storage作為來源或目標時、Cloud Sync 即可從資料代理商的服務帳戶擁有權限的庫位中進行選擇。依預設、這包括\_相同\_專案中的儲存區與資料代理服務帳戶。但如果您提供必要的權限、您可以從\_其他\_專案中選擇儲存區。

步驟

1. 開啟Google Cloud Platform主控台並載入Cloud Storage服務。
2. 按一下您要在同步關係中作為來源或目標的儲存區名稱。

3. 按一下\*權限\*。
4. 按一下「\* 新增 \*」。
5. 輸入資料代理的服務帳戶名稱。
6. 選取提供的角色 [與上述相同的權限](#)。
7. 按一下「\* 儲存 \*」。

設定同步關係時、您現在可以選擇該儲存區做為同步關係中的來源或目標。

資料代理**VM**執行個體的詳細資料

使用下列組態、在Google Cloud中建立資料代理程式。Cloud Sync

機器類型

N1-標準-4

**vCPU**

4.

**RAM**

15 GB

作業系統

Red Hat Enterprise Linux 7.7

磁碟大小與類型

20 GB HDD PD-Standard

## 在 **Linux** 主機上安裝資料代理程式

當您建立新的資料代理人群組時、請選擇「內部部署的Data Broker」選項、將資料代理人軟體安裝在內部部署的Linux主機上、或安裝在雲端的現有Linux主機上。本頁將會重複提供安裝程序的支援、協助您做好安裝準備。Cloud Sync

**Linux** 主機需求

- \* 作業系統 \* :
  - CentOS 7.0 、 7.7 及 8.0
  - 不支援CentOS串流。
  - Red Hat Enterprise Linux 7.7 與 8.0
  - Ubuntu Server 20.04 LTS
  - SUSE Linux Enterprise Server 15 SP1

在安裝資料代理程式之前、必須先在主機上執行「yum update all」命令。

Red Hat Enterprise Linux 系統必須在 Red Hat 訂購管理中註冊。如果未註冊、系統將無法在安裝期間存取

儲存庫來更新所需的協力廠商軟體。

- \* RAM\* : 16 GB
- \* CPU\* : 4 核心
- \* 可用磁碟空間 \* : 10 GB
- \* SELinux \* : 建議您停用 "SELinux" 在主機上。

SELinux 會強制執行封鎖資料代理程式軟體更新的原則、並封鎖資料代理程式、使其無法連絡正常作業所需的端點。

## 網路需求

- Linux 主機必須連線至來源和目標。
- 檔案伺服器必須允許 Linux 主機存取匯出。
- 連接埠 443 必須在 Linux 主機上開啟、才能傳出流量至 AWS（資料代理程式會持續與 Amazon SQS 服務通訊）。
- NetApp 建議將來源、目標及資料代理程式設定為使用網路時間傳輸協定（NTP）服務。三個元件之間的時間差異不應超過 5 分鐘。

## 可存取 AWS

如果您計畫使用內含 S3 儲存區之同步關係的資料代理程式、則應準備 Linux 主機以進行 AWS 存取。安裝資料代理程式時、您必須為具有程式化存取權和特定權限的 AWS 使用者提供 AWS 金鑰。

### 步驟

1. 使用建立 IAM 原則 ["此 NetApp 提供的原則"](#)

["檢視 AWS 指示"](#)

2. 建立具有程式化存取權限的 IAM 使用者。

["檢視 AWS 指示"](#)

請務必複製 AWS 金鑰、因為您在安裝資料代理軟體時必須指定這些金鑰。

## 可存取 Google Cloud

如果您計畫使用資料代理商的同步關係、包括 Google Cloud Storage 儲存庫、則應準備 Linux 主機以進行 Google Cloud 存取。安裝資料代理程式時、您必須提供具有特定權限的服務帳戶金鑰。

### 步驟

1. 如果您還沒有 Google Cloud 服務帳戶、請建立具有 Storage Admin 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。

["檢視 Google Cloud 指示"](#)

檔案應至少包含下列內容：「project\_id」、「Private\_key」和「client\_email」



當您建立金鑰時、檔案會產生並下載到您的機器上。

3. 將 Json 檔案儲存至 Linux 主機。

## 可存取 Microsoft Azure

透過在「同步關係」精靈中提供儲存帳戶和連線字串、即可根據關係定義 Azure 存取權。

## 安裝資料代理程式

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. 按一下「\* 建立新同步 \*」。
2. 在「\* 定義同步關係 \*」頁面上、選擇來源和目標、然後按一下「\* 繼續 \*」。

完成這些步驟、直到您到達「資料代理人群組」頁面為止。

3. 在「資料代理人群組」頁面上、按一下「建立資料代理人」、然後選取「內部資料代理人」。



即使選項標示為「\*\_ON-Prem\_Data Broners\*」、也適用於內部部署或雲端上的 Linux 主機。

4. 輸入資料代理的名稱、然後按一下 \* 繼續 \*。

指示頁面即將載入。您必須遵循這些指示、其中包含下載安裝程式的獨特連結。

5. 在說明頁面上：
  - a. 選擇是否啟用 \* AWS\* 、 \* Google Cloud \* 或兩者的存取。
  - b. 選擇一個安裝選項： \* 無代理 \* 、 \* 使用 Proxy 伺服器 \* 或 \* 使用 Proxy 伺服器搭配驗證 \* 。
  - c. 使用命令下載及安裝資料代理程式。

下列步驟提供每個可能安裝選項的詳細資訊。請依照指示頁面、根據您的安裝選項取得確切的命令。

- d. 下載安裝程式：

- 無代理：

```
「 curl <URI> -o data_Broker_installer.sh 」
```

- 使用 Proxy 伺服器：

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

- 使用 Proxy 伺服器進行驗證：

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

#### 開放的我們

在指示頁面上顯示安裝檔案的 URI、當您依照提示部署內部部署的 Prem Data Broker 時、就會載入此頁面。Cloud Sync 此 URI 不會重複出現、因為連結是動態產生的、只能使用一次。請遵循下列步驟、從 Cloud Sync 無法取得 URI。

- e. 切換至超級使用者、執行安裝程式並安裝軟體：



下列每個命令都包含 AWS 存取和 Google Cloud 存取的參數。請依照指示頁面、根據您的安裝選項取得確切的命令。

- 無 Proxy 組態：

```
「 Udo -s chmod+x data_broker_installer.sh ./data_broker_installer.sh -a <AWs_access_key> -s  
<AWs_secret 鍵> -g <jure_path_to_the_json_file> 」
```

- Proxy 組態：

```
"Udo -s chmod+x data_broker_installer.sh ./data_broker_installer.sh -a <AWs_access_key> -s  
<AWs_secret 鍵> -g <jure_path_to_the_json_file> -h <prox_host> -p <prox_port>'
```

- Proxy 組態搭配驗證：

```
s chmod+x data_broker_installer.sh ./data_broker_installer.sh -a <AWs_access_key> -s  
<AWs_secret 鍵> -g <jure_path_to_the_json_file> -h <proxy_host> -p <proxy_port> -u  
<proxy_username>-w <proxy_password>`
```

#### AWS 金鑰

這些是您應該準備的使用者金鑰 請依照下列步驟操作。AWS 金鑰會儲存在資料代理程式上、該代理程式會在內部部署或雲端網路中執行。NetApp 不會使用資料代理程式以外的金鑰。

#### Json 檔案

這是 Json 檔案、其中包含您應該準備的服務帳戶金鑰 請依照下列步驟操作。

6. 一旦資料代理程式可供使用、請按 Cloud Sync 一下 《》 中的 \* 「 Continue 」 （繼續） \* 。
7. 完成精靈中的頁面、以建立新的同步關係。

# 使用Cloud Sync

## 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

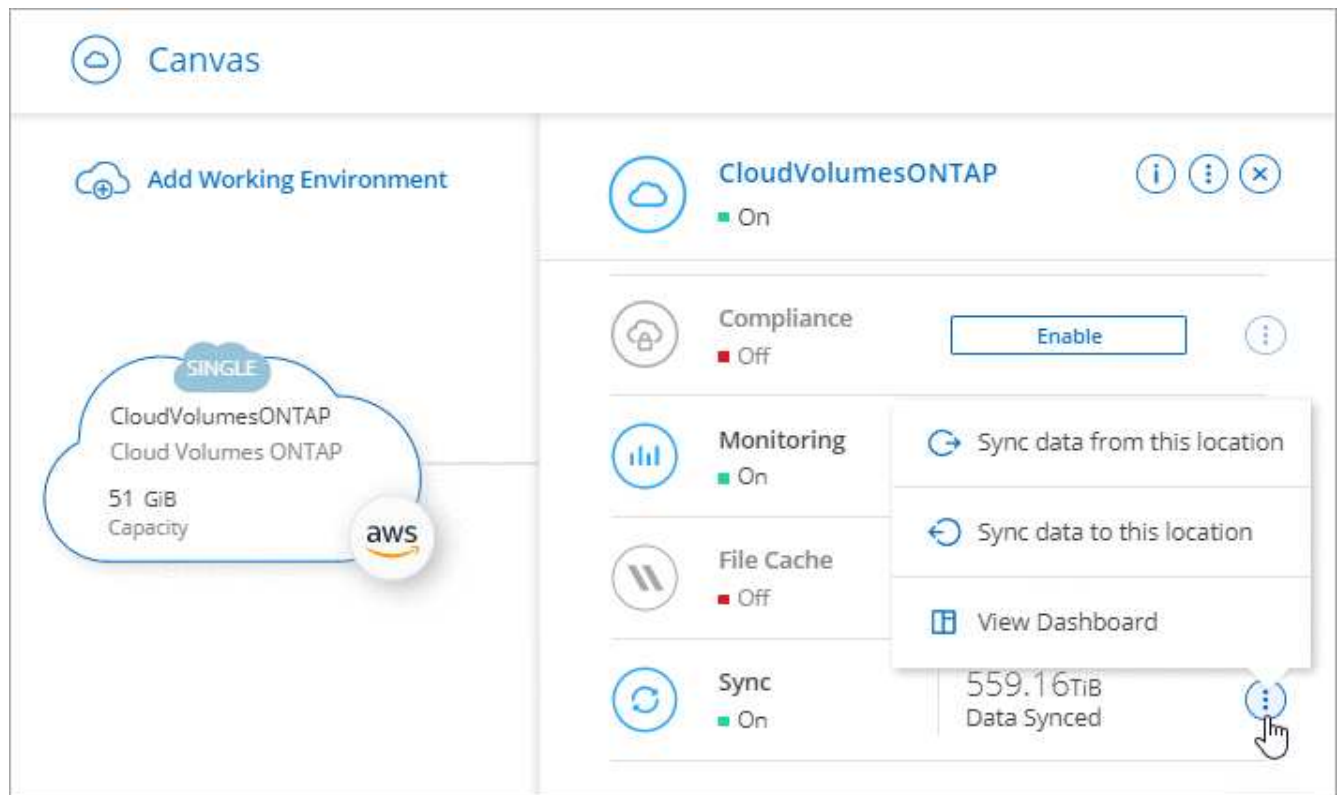
如果您想為下列任一項目建立同步關係、則首先需要建立或探索工作環境：

- 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。





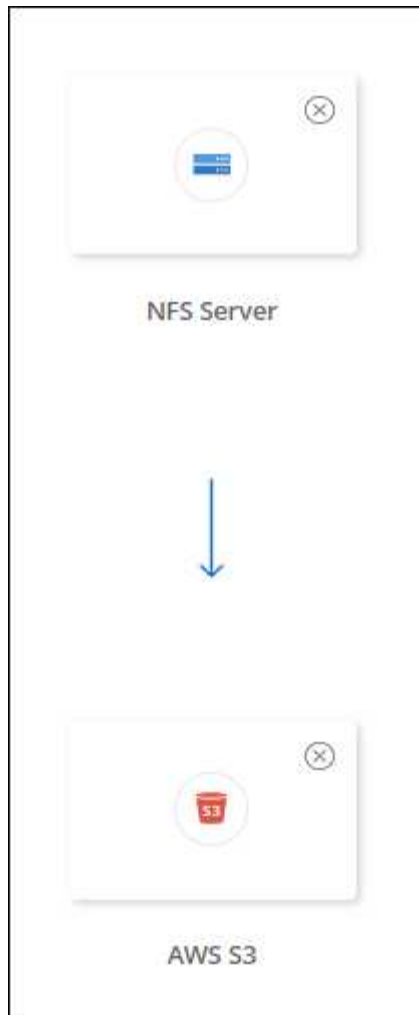
5. 選擇\*從此位置同步資料\*或\*同步資料至此位置\*、然後依照提示設定同步關係。

#### 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。

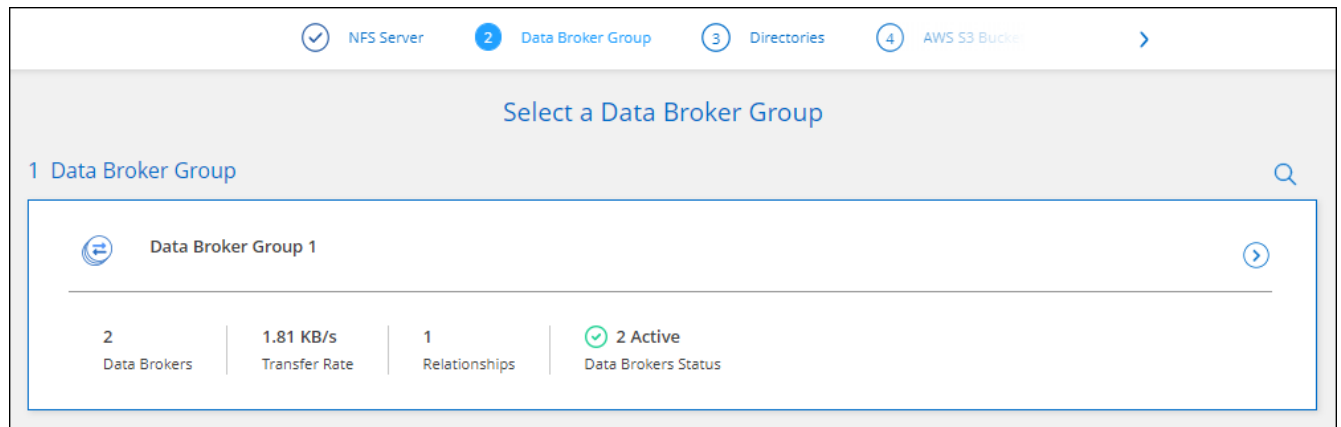


3. 在「\* NFS 伺服器 \*」頁面上、輸入您要同步到 AWS 的 NFS 伺服器 IP 位址或完整網域名稱。
4. 在\*資料代理人群組\*頁面上、依照提示在AWS、Azure或Google Cloud Platform中建立資料代理人虛擬機器、或是在現有的Linux主機上安裝資料代理人軟體。

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。



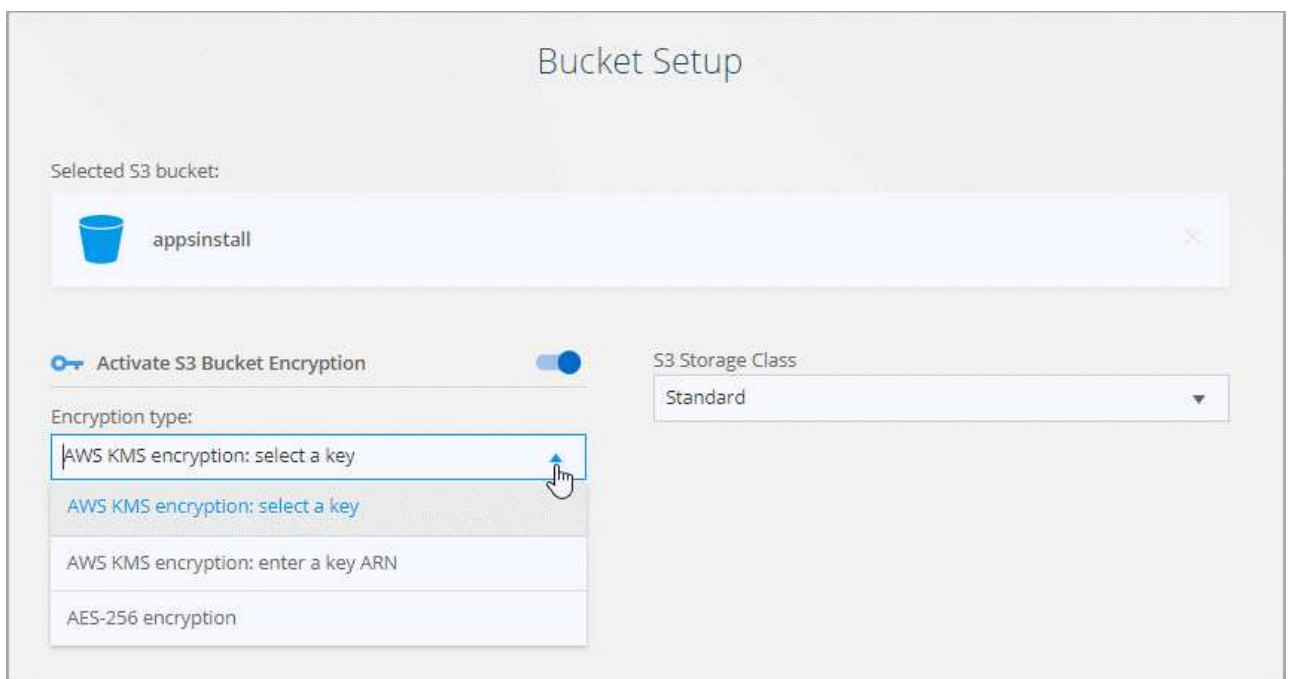
如果您想要同步 NFS 伺服器上的多個目錄、則必須在完成之後建立其他同步關係。

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。

## 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S3相容的端點（S3、StorageGRID S基 板或IBM Cloud Object Storage）。

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](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共用區之間的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。


此功能適用於任何類型的資料代理商：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 \***。

### Select an SMB Source

SMB Version: 2.1 ▼



Selected SMB Server:

10.20.30.152

Define SMB Credentials:

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

ACL - Access Control List

☒ Copy Access Control Lists to the target

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

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。

<
>
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	Metadata Value
Up to 128 characters	Up to 256 characters

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

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 共用區之間的 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>\

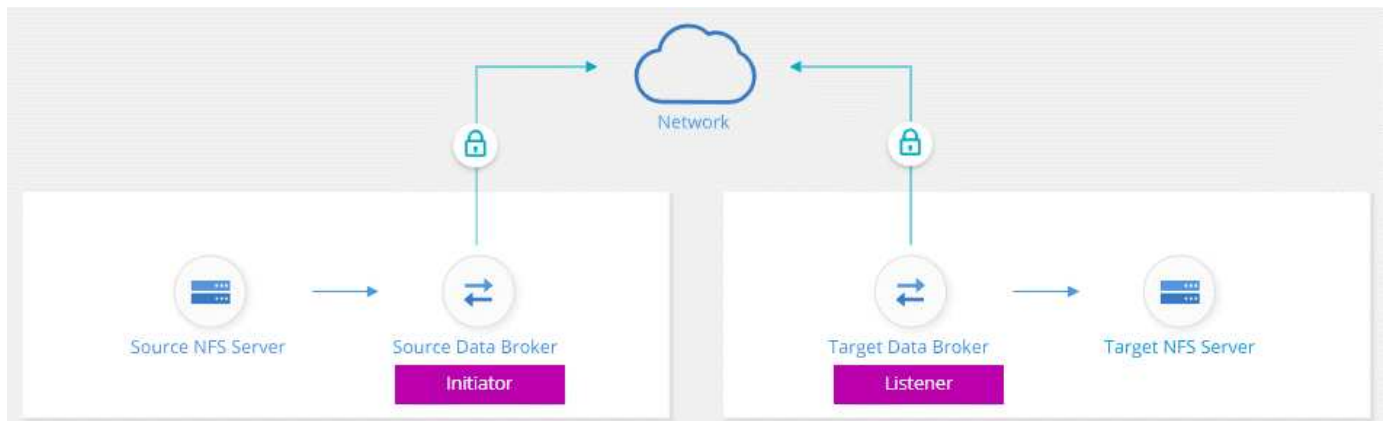
### 使用資料傳輸加密來同步 NFS 資料

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組、則該組必須只有一個資料代理人。加密的同步關係不支援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。

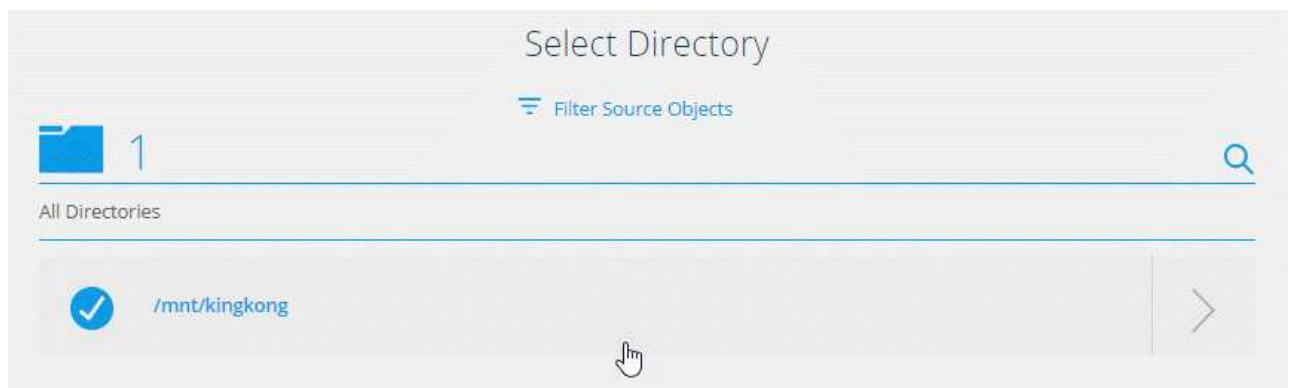
### 步驟

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。


**Select a Provider**




Microsoft Azure



Amazon Web Services



Google Cloud Platform

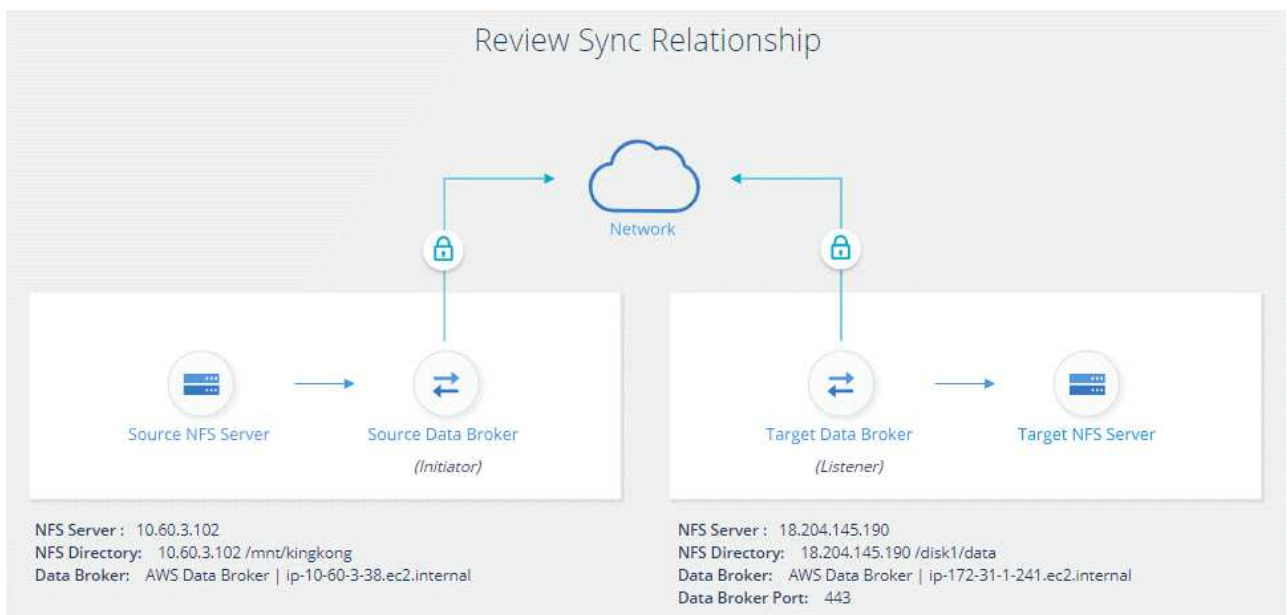


On-Prem Data Broker

Data Broker Name

Port

- 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 `_n32hcbnj2`、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"
    }
  }
}
```

## 免費試用結束後、請支付同步關係的費用

在您的 14 天免費試用結束後、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、以隨用隨付或每年付費。第二種選擇是直接向 NetApp 購買授權。

您可以從AWS Marketplace或Azure Marketplace訂閱。您無法同時訂閱兩者。

您可以選擇以Marketplace訂閱方式使用NetApp的授權。例如、如果您有 25 個同步關係、您可以使用授權支付前 20 個同步關係的費用、然後從 AWS 或 Azure 購買剩餘的 5 個同步關係。

["深入瞭解授權的運作方式"](#)。

### 如果我在免費試用結束後、不立即付款、該怎麼辦？

您將無法建立任何其他關係。現有的關係不會刪除、但您必須先訂閱或輸入授權、才能對其進行任何變更。

## 訂閱 AWS

AWS 可讓您隨用隨付或每年付費。

#### 隨用隨付的步驟

1. 按一下 \* 同步 > 授權 \* 。
2. 選擇 \* AWS\*。
3. 按一下「\* 訂閱 \*」、然後按一下「\* 繼續 \*」。
4. 從 AWS Marketplace 訂閱、然後重新登入 Cloud Sync 到該服務以完成註冊。

下列影片顯示此程序：

► [https://docs.netapp.com/zh-tw/cloud-manager-sync//media/video\\_cloud\\_sync\\_registering.mp4](https://docs.netapp.com/zh-tw/cloud-manager-sync//media/video_cloud_sync_registering.mp4) (video)

#### 每年支付的步驟

1. "前往 [AWS Marketplace 頁面](#)"。
2. 按一下 \* 繼續訂閱 \* 。
3. 選取您的合約選項、然後按一下 \* 建立合約 \* 。

### 訂閱 Azure

Azure 可讓您隨用隨付或每年付費。

具備相關訂閱之「參與者」或「擁有者」權限的 Azure 使用者帳戶。

#### 步驟

1. 按一下 \* 同步 > 授權 \* 。
2. 選擇 \* Azure \* 。
3. 按一下「\* 訂閱 \*」、然後按一下「\* 繼續 \*」。
4. 在 Azure 入口網站中、按一下 \* 「Create」（建立） \* 、選取您的選項、然後按一下 \* 「訂購」 \* 。

選擇 \* 每月 \* 按小時付費、或 \* 每年 \* 預付一年。

5. 部署完成後、按一下通知快顯視窗中的 SaaS 資源名稱。
6. 按一下「\* 設定帳戶 \*」以返回 Cloud Sync 到「支援」。

下列影片顯示此程序：

► [https://docs.netapp.com/zh-tw/cloud-manager-sync//media/video\\_cloud\\_sync\\_registering\\_azure.mp4](https://docs.netapp.com/zh-tw/cloud-manager-sync//media/video_cloud_sync_registering_azure.mp4)

(video)

## 向 NetApp 購買授權、並將其新增 Cloud Sync 至

若要預付同步關係的費用、您必須購買一或多份授權、並將其新增至 Cloud Sync 該服務。

您將需要授權的序號、以及授權所關聯之NetApp Support Site帳戶的使用者名稱和密碼。

### 步驟

1. 請透過 mailto : [ng-cloudsync-contact@netapp.com](mailto:ng-cloudsync-contact@netapp.com) ® Subject=Cloud %20Sync%20Service%20-%20BYOL%20License%20Purche%20Request 購買授權（聯絡 NetApp ）。
2. 在 Cloud Manager 中、按一下 \* 同步 > 授權 \* 。
3. 按一下\*新增授權\*並新增必要資訊：
  - a. 輸入序號。
  - b. 選取與您要新增之授權相關的NetApp支援網站帳戶：
    - 如果您的帳戶已新增至Cloud Manager、請從下拉式清單中選取。
    - 如果您的帳戶尚未新增、請按一下「新增**NSSCredential**」、輸入使用者名稱和密碼、按一下「註冊」、然後從下拉式清單中選取。
  - c. 按一下「\* 新增 \*」。

## 更新授權

如果您延長Cloud Sync 從NetApp購買的更新版的支援、新的到期日將不會自動更新Cloud Sync 到更新版。您需要再次新增授權、以重新整理到期日。

### 步驟

1. 在 Cloud Manager 中、按一下 \* 同步 > 授權 \* 。
2. 按一下\*新增授權\*並新增必要資訊：
  - a. 輸入序號。
  - b. 選取與您要新增之授權相關的NetApp支援網站帳戶。
  - c. 按一下「\* 新增 \*」。

以新的到期日更新現有授權。Cloud Sync


## 管理同步關係

您可以立即同步資料、變更排程等、隨時管理同步關係。

### 立即執行資料同步

您可以按下按鈕、在來源和目標之間立即同步資料、而不必等到下次排程同步。

### 步驟

1. 從\*儀表板\*瀏覽至同步關係、然後按一下 
2. 按一下「\* 立即同步 \*」、然後按一下「\* 同步 \*」進行確認。

執行資料同步處理程序。Cloud Sync

## 加速同步效能

將額外的資料代理程式新增至管理關聯的群組、以加速同步關係的效能。額外的資料代理程式必須是 `_new` 資料代理程式。


如果資料代理人群組管理其他同步關係、則您新增至群組的新資料代理人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由資料代理群組A管理
- 關係2由資料代理群組B管理
- 關係3由資料代理群組A管理

您想要加速關係1的效能、以便將新的資料代理程式新增至資料代理群組A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家資料代理人處於線上狀態。
2. 從\*儀表板\*瀏覽至同步關係、然後按一下 
3. 按一下 \* 加速 \*。
4. 依照提示建立新的資料代理程式。

將新的資料代理程式新增至群組。Cloud Sync下一次資料同步的效能應該加快。

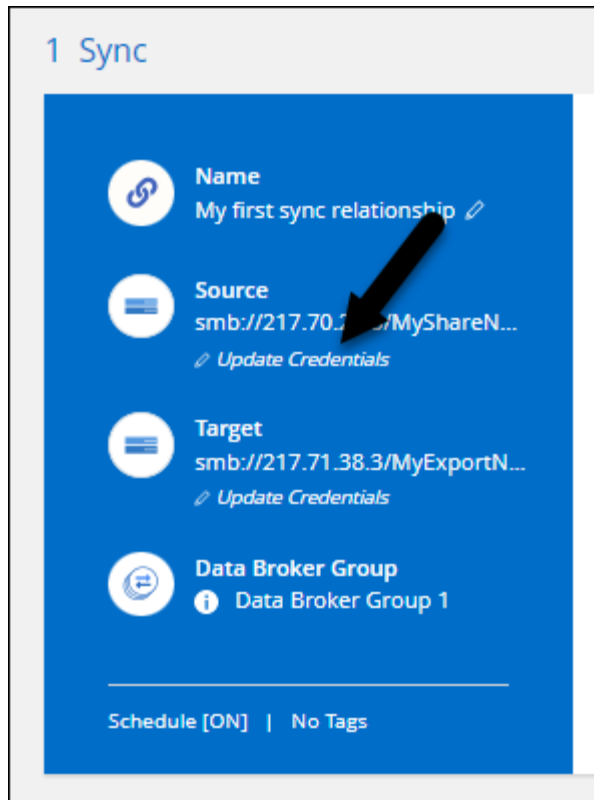
## 正在更新認證資料

您可以使用現有同步關係中來源或目標的最新認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認證資料、更新認證資料將有助益。

任何來源或目標Cloud Sync 如Azure Blob、Box、IBM Cloud Object Storage、StorageGRID 更新認證、支援更新認證、如不需要認證、則可用於下列用途ONTAP：Azure Blob、Box、IBM Cloud Object Storage、更新支援、不支援更新支援、SS3 Storage、SFTP及SMB伺服器。

### 步驟

1. 從\*同步儀表板\*移至需要認證的同步關係、然後按一下\*更新認證\*。



2. 輸入認證資料、然後按一下\*更新\*。


SMB伺服器的相關注意事項：如果網域是新的、則您需要在更新認證時加以指定。如果網域尚未變更、您就不需要重新輸入。

如果您在建立同步關係時輸入網域、但在更新認證資料時卻未輸入新網域、Cloud Sync 則會繼續使用您提供的原始網域。

更新資料代理程式上的認證資料。Cloud Sync資料代理程式開始使用更新的認證資料進行同步之前、可能需要10分鐘的時間。

## 變更同步關係的設定

修改設定、定義如何在目標位置同步及維護來源檔案和資料夾。

1. 從\*儀表板\*瀏覽至同步關係、然後按一下 
2. 按一下 \* 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

[[deleteonSOURS] 以下是每項設定的簡短說明：

#### 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。

## 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

建立關聯之後、您無法編輯此選項。

## 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。預設值是從不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](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。


#### 4. 按一下 \* 儲存設定 \* 。

利用新的設定修改同步關係。 Cloud Sync

## 刪除關係

如果不再需要在來源與目標之間同步資料、您可以刪除同步關係。此動作不會刪除資料代理群組（或個別資料代理執行個體）、也不會從目標刪除資料。

### 步驟

1. 從\*儀表板\*瀏覽至同步關係、然後按一下 。
2. 單擊 \* 刪除 \*，然後再次單擊 \* 刪除 \* 進行確認。

執行此動作會刪除同步關係。 Cloud Sync

## 管理資料代理群組

資料代理人群組會將來源位置的資料同步到目標位置。您所建立的每個同步關係、群組中至少需要一個資料代理程式。透過新增資料代理程式至群組、檢視群組相關資訊等方式來管理資料代理群組。

### 資料代理程式群組的運作方式

資料代理人群組可以包含一或多個資料代理人。將資料代理人集中在一起、有助於提升同步關係的效能。

### 群組可以管理多個關係

資料代理人群組一次可以管理一或多個同步關係。

例如、假設您有三種關係：

- 關係1由資料代理群組A管理
- 關係2由資料代理群組B管理



- 關係3由資料代理群組A管理

您想要加速關係1的效能、以便將新的資料代理程式新增至資料代理群組A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。

#### 群組中的資料代理人數目

在許多情況下、單一資料代理程式可滿足同步關係的效能要求。如果沒有、您可以在群組中新增額外的資料代理人、以加速同步效能。但您應該先檢查其他可能影響同步效能的因素。"[深入瞭解如何判斷何時需要多個資料代理人](#)"。

## 安全性建議

為確保資料代理機器的安全性、NetApp建議：

- SSH不應允許進行X11轉送
- SSH不應允許TCP連線轉送
- SSH不應允許使用通道
- SSH不應接受用戶端環境變數

這些安全建議有助於防止未獲授權的資料代理機器連線。

## 將新的資料代理程式新增至群組

建立新的資料代理程式有幾種方法：

- 建立新的同步關係時

"[瞭解如何在建立同步關係時建立新的資料代理程式](#)"。

- 在「\* 管理資料代理人 \*」頁面中、按一下「\* 新增資料代理人 \*」、即可在新群組中建立資料代理人
- 在 \* 管理資料代理 \* 頁面中、建立現有群組中的新資料代理程式

#### 開始之前

- 您無法將資料代理人新增至管理加密同步關係的群組。
- 如果您要在現有群組中建立資料代理程式、資料代理程式必須是內部資料代理程式或相同類型的資料代理程式。

例如、如果某個群組包含 AWS 資料代理程式、則您可以在該群組中建立 AWS 資料代理程式或內部部署資料代理程式。您無法建立Azure資料代理人或Google Cloud資料代理人、因為他們的資料代理人類型不同。

#### 在新群組中建立資料代理程式的步驟

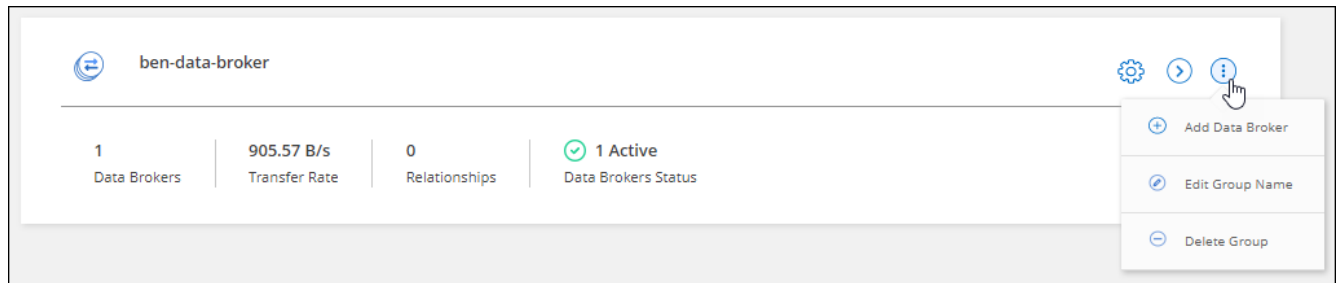
1. 按一下 \* 同步 > 管理資料代理人 \* 。
2. 按一下「\* 新增資料代理人 \*」。
3. 依照提示建立資料代理程式。

如需協助、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"](#)

在現有群組中建立資料代理程式的步驟

1. 按一下 \* 同步 > 管理資料代理人 \* 。
2. 按一下動作功能表、然後選取 \* 新增資料代理人 \* 。



3. 依照提示在群組中建立資料代理程式。

如需協助、請參閱下列頁面：

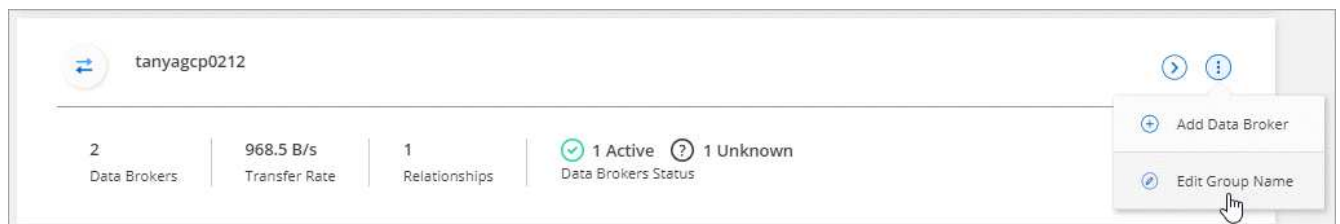
- ["在AWS中建立資料代理程式"](#)
- ["在Azure中建立資料代理程式"](#)
- ["在Google Cloud中建立資料代理商"](#)
- ["在 Linux 主機上安裝資料代理程式"](#)

## 編輯群組名稱

隨時變更資料代理群組的名稱。

步驟

1. 按一下 \* 同步 > 管理資料代理人 \* 。
2. 按一下動作功能表、然後選取 \* 編輯群組名稱 \* 。



3. 輸入新名稱、然後按一下「 \* 儲存 \* 」。

更新資料代理群組的名稱。 Cloud Sync

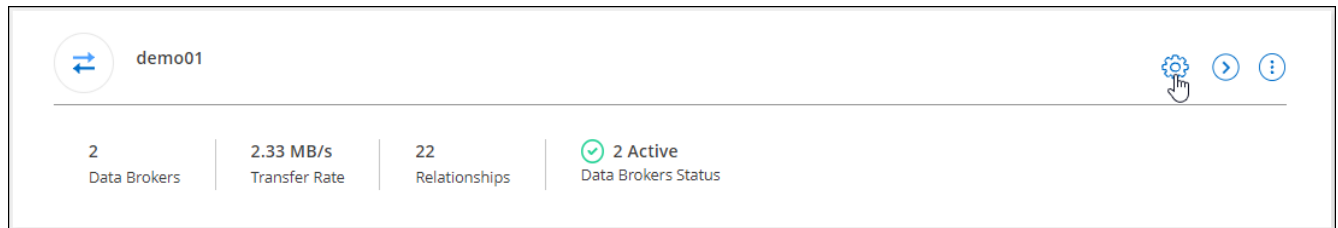
## 設定統一化組態

如果同步關係在同步處理期間發生錯誤、統一資料代理群組的並行處理有助於減少同步錯誤的數量。請注意、群組組態的變更可能會減緩傳輸速度、進而影響效能。

我們不建議您自行變更組態。您應諮詢NetApp、瞭解何時變更組態及如何變更組態。

### 步驟

1. 按一下\*管理資料代理人\*。
2. 按一下資料代理群組的「設定」圖示。



3. 視需要變更設定、然後按一下「統一化組態」。

請注意下列事項：

- 您可以選擇要變更的設定、而不需要一次變更全部四個設定。
- 將新組態傳送至資料代理程式之後、資料代理程式會自動重新啟動並使用新組態。
- 這項變更可能需要一分鐘的時間才能完成、而且可在Cloud Sync 整個視覺介面中看到。
- 如果資料代理程式未執行、因為Cloud Sync 無法與它通訊、所以它的組態不會改變。資料代理程式重新啟動後、組態將會變更。
- 設定統一化組態之後、任何新的資料代理人都會自動使用新組態。

## 在群組之間移動資料代理人


如果您需要加速目標資料代理群組的效能、請將資料代理程式從一個群組移至另一個群組。

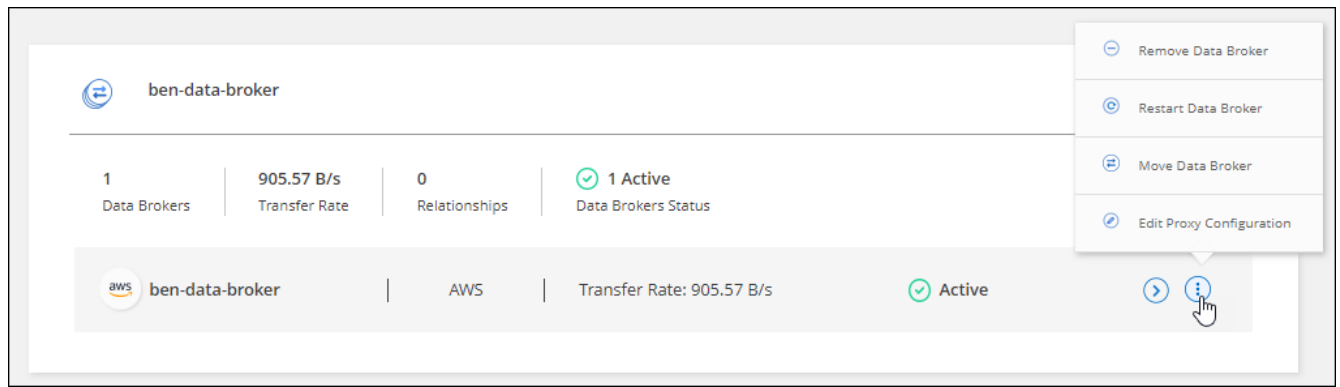
例如、如果資料代理人不再管理同步關係、您可以輕鬆地將其移至另一個管理同步關係的群組。

### 限制

- 如果資料代理人群組正在管理同步關係、而且群組中只有一個資料代理人、則您無法將該資料代理人移至其他群組。
- 您無法將資料代理移至或移出管理加密同步關係的群組。
- 您無法移動目前正在部署的資料代理程式。

### 步驟

1. 按一下 \* 同步 > 管理資料代理人 \*。
2. 按一下  展開群組中的資料代理程式清單。
3. 按一下資料代理的動作功能表、然後選取\*移動資料代理\*。




4. 建立新的資料代理人群組、或選取現有的資料代理人群組。
5. 按一下\*移動\*。

將資料代理程式移至新的或現有的資料代理程式群組。Cloud Sync如果前一個群組中沒有其他資料代理人、Cloud Sync 則由NetApp刪除。

## 更新Proxy組態

若要更新資料代理程式的Proxy組態、請新增新Proxy組態的詳細資料、或編輯現有的Proxy組態。

### 步驟

1. 按一下 \* 同步 > 管理資料代理人 \*。
2. 按一下  展開群組中的資料代理程式清單。
3. 按一下資料代理的動作功能表、然後選取\*編輯Proxy組態\*。
4. 指定Proxy的詳細資料：主機名稱、連接埠號碼、使用者名稱和密碼。
5. 按一下 \* 更新 \*。

更新資料代理程式以使用Proxy組態存取網際網路。Cloud Sync

## 檢視資料代理程式的組態

您可能想要檢視資料代理程式的詳細資料、以識別其主機名稱、IP 位址、可用的 CPU 和 RAM 等項目。



提供下列資料代理程式的詳細資料：Cloud Sync

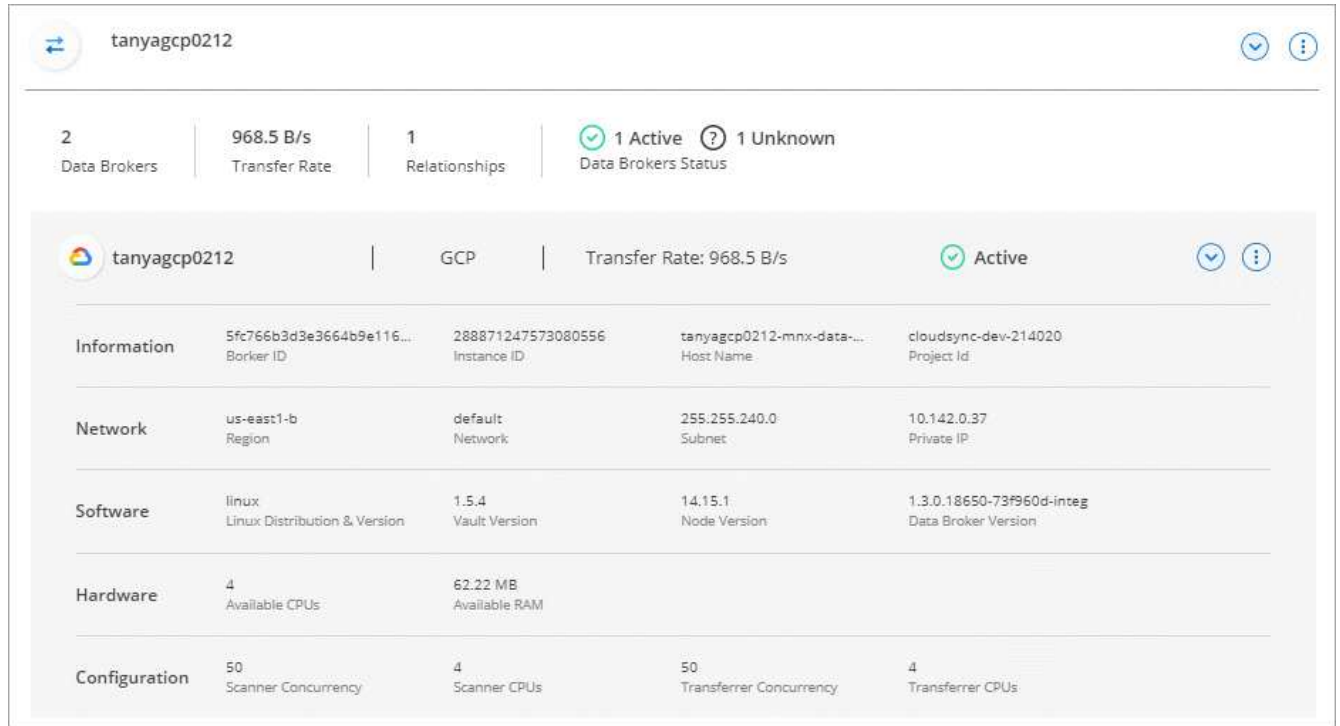
- 基本資訊：執行個體 ID、主機名稱等
- 網路：地區、網路、子網路、私有 IP 等
- 軟體：Linux 發佈、資料代理程式版本等
- 硬體：CPU 和 RAM
- 組態：資料代理程式兩種主要程序的詳細資料、包括掃描器和傳輸器



掃描器會掃描來源和目標、並決定要複製的項目。傳輸器執行實際複製。NetApp 人員可能會使用這些組態詳細資料來建議可最佳化效能的行動。

## 步驟

1. 按一下 \* 同步 > 管理資料代理人 \* 。
2. 按一下  展開群組中的資料代理程式清單。
3. 按一下  可查看有關數據代理的詳細信息。



介面顯示了 tanyagcp0212 的概況和詳細配置。概況欄顯示有 2 個 Data Brokers，傳輸速率為 968.5 B/s，1 個 Relationships，以及 1 個 Active 和 1 個 Unknown 的 Data Brokers Status。詳細資訊表如下：

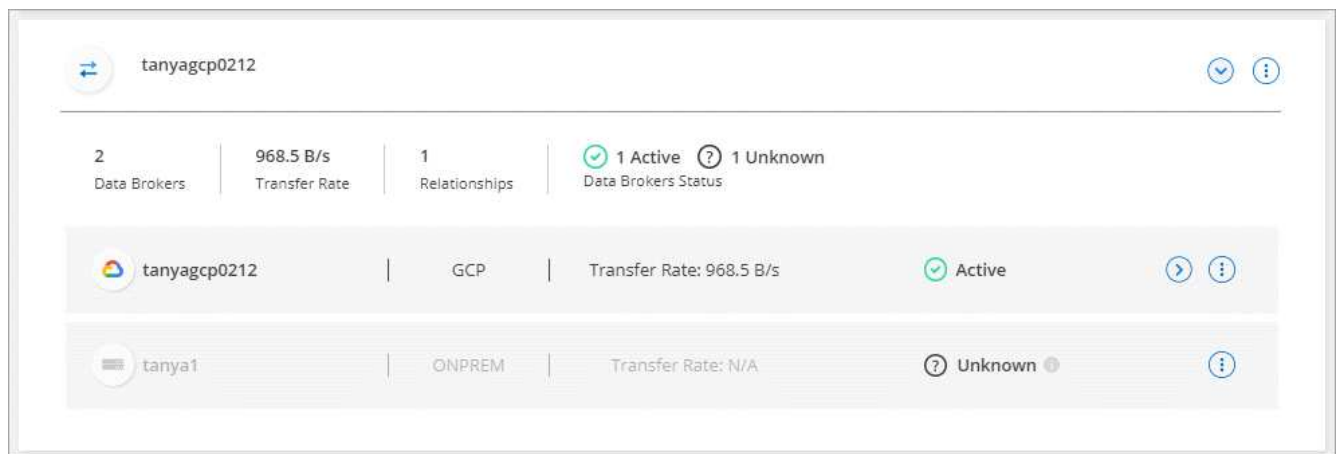
Category	Item 1	Item 2	Item 3	Item 4
Information	5fc766b3d3e3664b9e116... Broker ID	288871247573080556 Instance ID	tanyagcp0212-mnx-data-... Host Name	cloudsync-dev-214020 Project Id
Network	us-east1-b Region	default Network	255.255.240.0 Subnet	10.142.0.37 Private IP
Software	linux Linux Distribution & 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 Transferer Concurrency	4 Transferer CPUs

## 解決資料代理程式的問題

顯示每個資料代理程式的狀態、協助您疑難排解問題。Cloud Sync

## 步驟

1. 識別任何狀態為「未知」或「失敗」的資料代理人。



介面顯示了多個資料代理程式的狀態。概況欄顯示有 2 個 Data Brokers，傳輸速率為 968.5 B/s，1 個 Relationships，以及 1 個 Active 和 1 個 Unknown 的 Data Brokers Status。詳細資訊表如下：

Item	Region	Transfer Rate	Status
tanyagcp0212	GCP	968.5 B/s	Active
tanya1	ONPREM	N/A	Unknown

2. 將游標暫留在上方  圖示以查看故障原因。

### 3. 修正問題。

例如、您可能只需要在資料代理程式離線時重新啟動、或是在初始部署失敗時移除資料代理程式。


## 從群組中移除資料代理程式

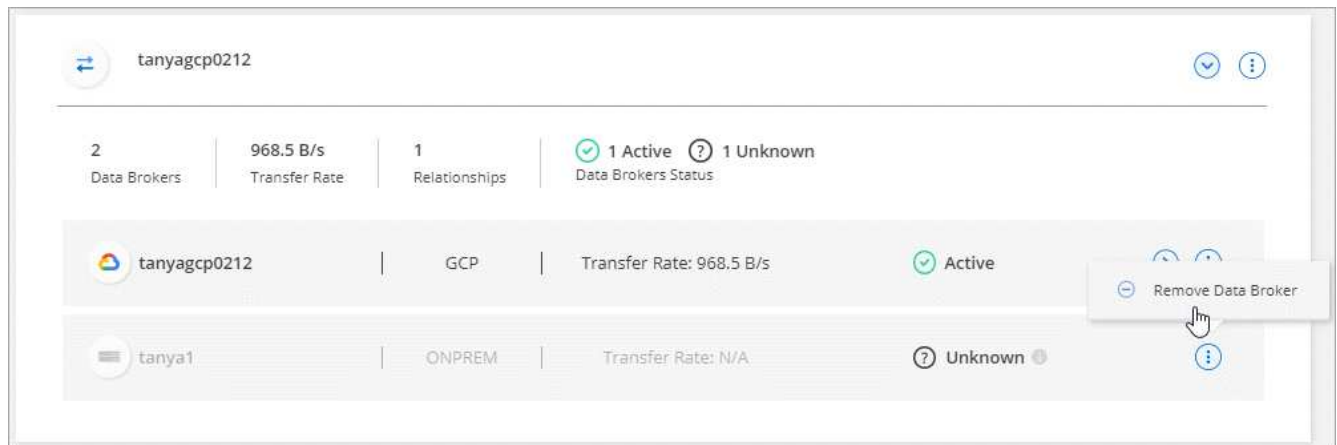
如果不再需要資料代理人、或是初始部署失敗、您可以將其從群組中移除。此動作僅會從 Cloud Sync 的記錄中刪除資料代理程式。您必須自行手動刪除資料代理人及任何其他雲端資源。

您應該知道的事

- 當您從群組中移除最後一個資料代理程式時、會刪除群組。 Cloud Sync
- 如果有使用該群組的關聯、您就無法從群組中移除最後一個資料代理。

步驟

1. 按一下 \* 同步 > 管理資料代理人 \* 。
2. 按一下  展開群組中的資料代理程式清單。
3. 按一下資料代理的動作功能表、然後選取 \* 移除資料代理 \* 。



4. 按一下「\* 移除資料代理人 \*」。

從群組中移除資料代理程式。 Cloud Sync

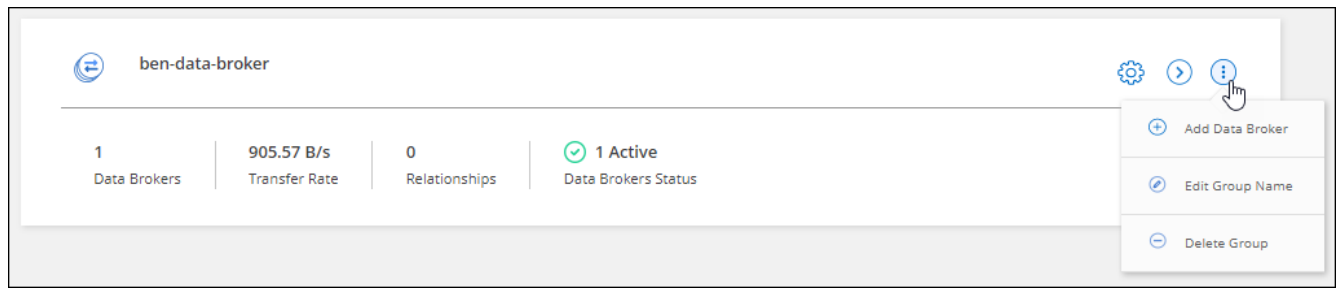
## 刪除資料代理群組

如果資料代理人群組不再管理任何同步關係、您可以刪除該群組、這樣會從Cloud Sync 停止執行所有資料代理人。

只會從Cloud Sync的記錄中刪除不含資料的資料代理人Cloud Sync。您需要從雲端供應商手動刪除資料代理執行個體、以及任何其他雲端資源。

步驟

1. 按一下 \* 同步 > 管理資料代理人 \* 。
2. 按一下動作功能表、然後選取\*刪除群組\*。



3. 若要確認、請輸入群組名稱、然後按一下\*刪除群組\*。

此功能會移除資料代理人並刪除群組。Cloud Sync

## 建立及檢視報告以調整組態

建立並檢視報告、以取得可在NetApp人員協助下使用的資訊、以調整資料代理的組態並改善效能。

每份報告都會提供有關同步關係中路徑的深入詳細資料。例如、檔案系統的報告會顯示目錄和檔案的數量、檔案大小的發佈、目錄的深度和範圍等。

### 建立報告

每次建立報告時Cloud Sync、將會掃描路徑、然後將詳細資料編譯成報告。

#### 步驟

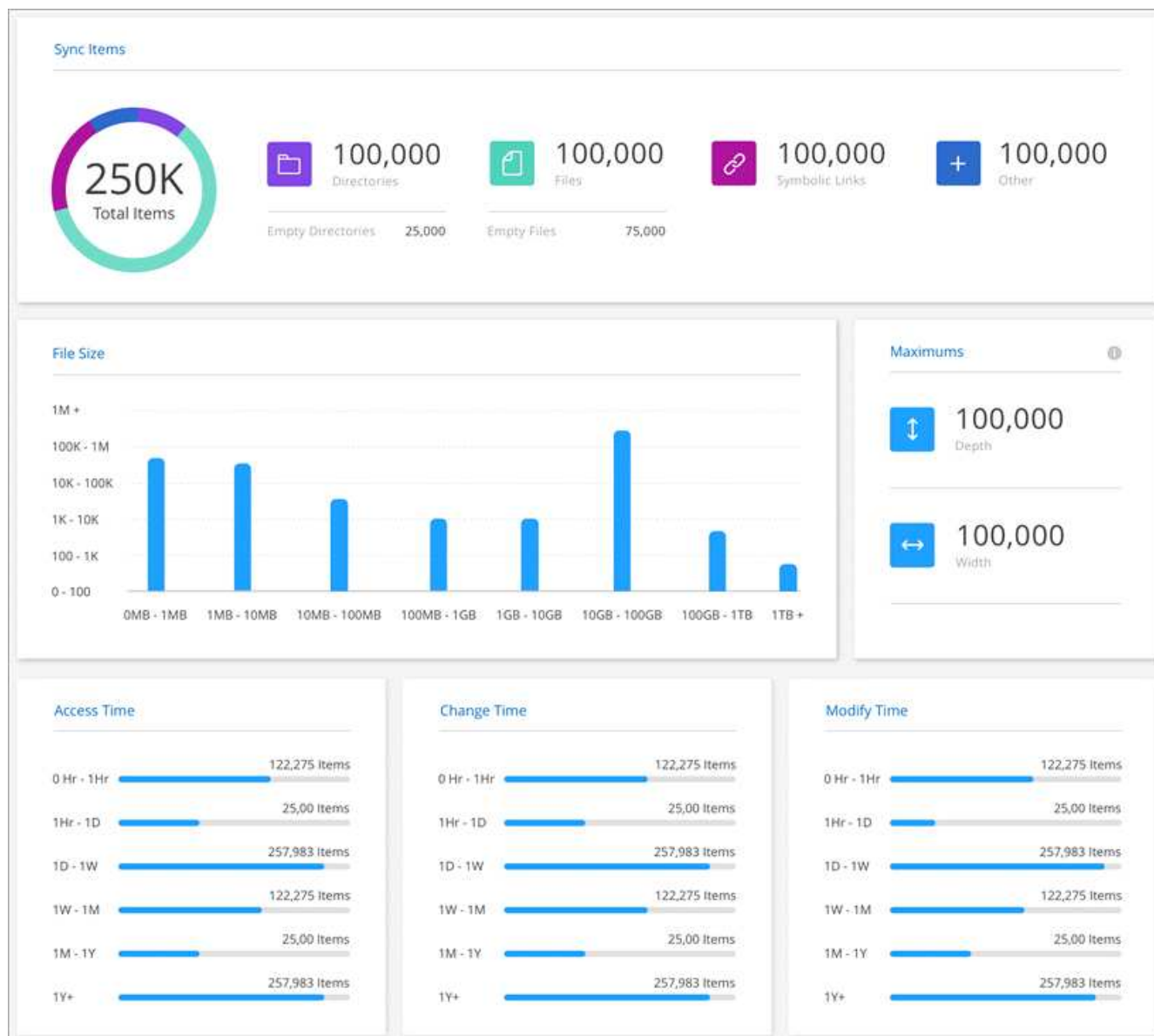
1. 按一下\*同步>報告\*。

每個同步關係中的路徑（來源或目標）都會顯示在表格中。

2. 在「報告動作」欄中、移至特定路徑並按一下「建立」、或按一下動作功能表並選取「建立新的」。

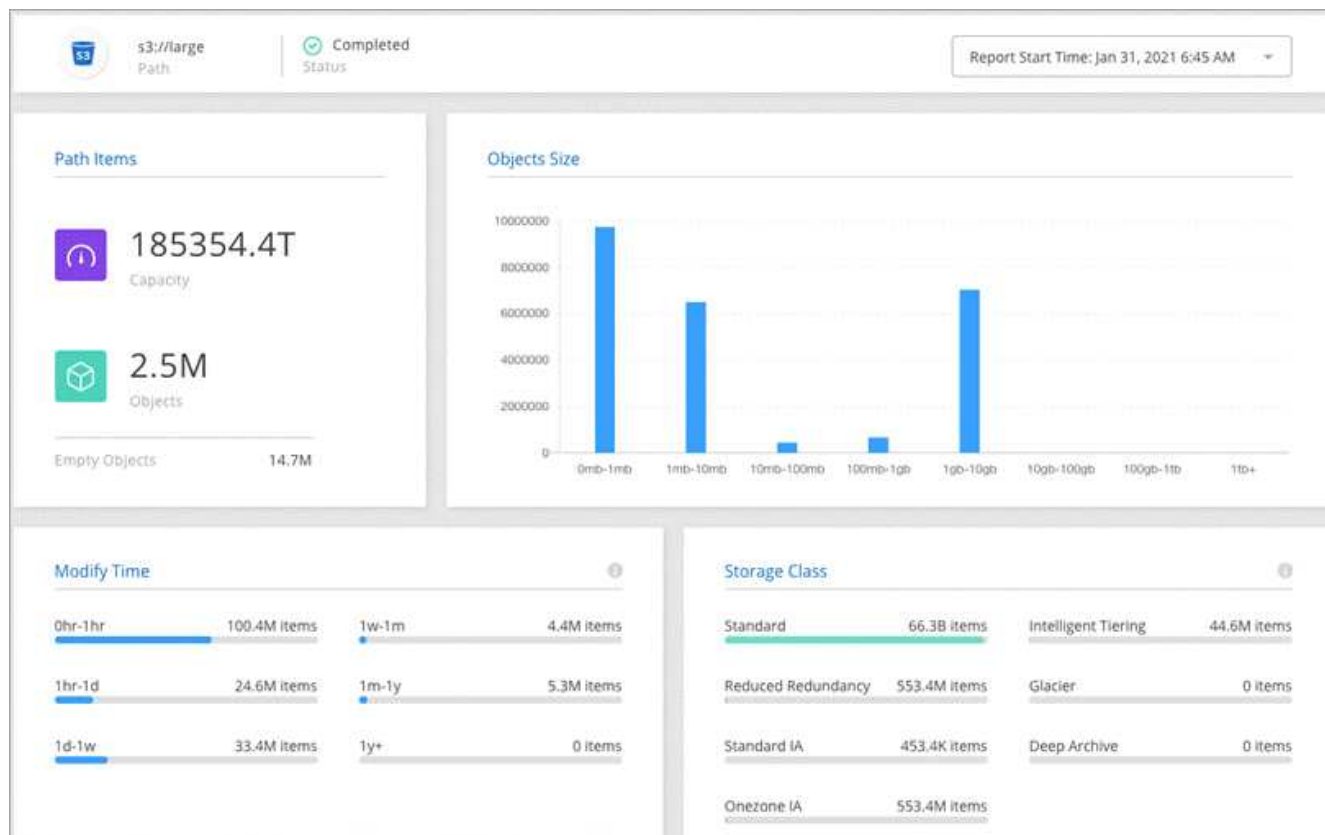
3. 報告準備就緒後、按一下動作功能表、然後選取\*檢視\*。

以下是檔案系統路徑的範例報告。



以下是物件儲存的範例報告。



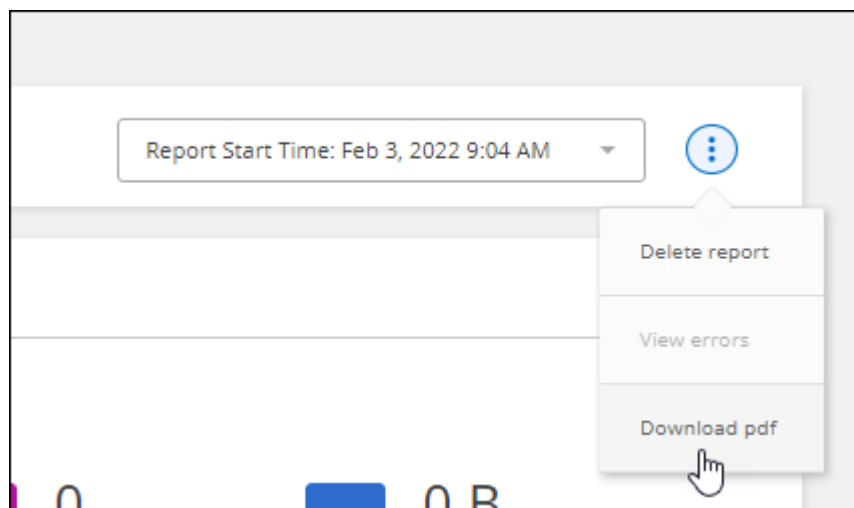


## 正在下載報告

您可以下載PDF格式的報告、以便離線檢視或分享。

### 步驟

1. 按一下\*同步>報告\*。
2. 在\*報告動作\*欄中、按一下動作功能表、然後選取\*檢視\*。
3. 在報告右上角、按一下動作功能表、然後選取\*下載pdf\*。



## 檢視報告錯誤

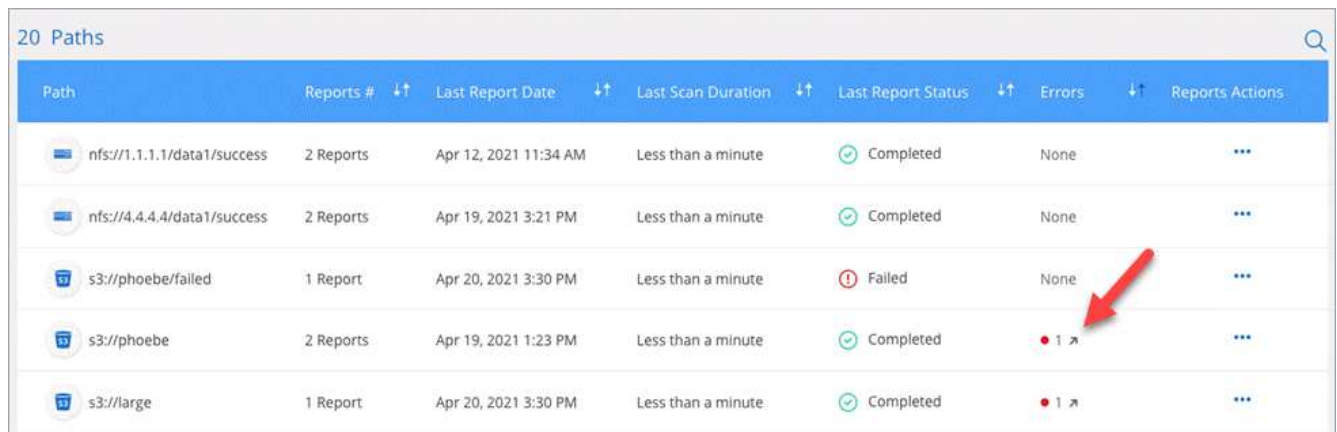
Paths表格可識別最近一次報告中是否有任何錯誤。錯誤會指出Cloud Sync 掃描路徑時出現的問題。

例如、報告可能包含「權限遭拒」錯誤。這類錯誤可能會影響Cloud Sync掃描整組檔案和目錄的能力。

檢視錯誤清單之後、您就可以解決這些問題、然後再次執行報告。

### 步驟

1. 按一下\*同步>報告\*。
2. 在「錯誤」欄中、識別報告中是否有任何錯誤。
3. 如果出現錯誤、請按一下錯誤數旁的箭頭。



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	...

4. 使用錯誤中的資訊來修正問題。

解決問題之後、下次執行報告時、就不會出現錯誤。

## 刪除報告

您可以刪除報告中包含您修正的錯誤、或是報告與您移除的同步關係有關。

### 步驟

1. 按一下\*同步>報告\*。
2. 在「報告動作」欄中、按一下路徑的動作功能表、然後選取\*刪除上次報告\*或\*刪除所有報告\*。
3. 確認您要刪除報告。

## 解除安裝資料代理程式

如有需要、請執行解除安裝指令碼、以移除安裝資料代理程式時所建立的資料代理程式、以及套件和目錄。

### 步驟

1. 登入資料代理主機。
2. 變更至資料代理人目錄：「/opt /NetApp/databasroker」

3. 執行下列命令：

```
"chmod+x uninstaller-DataBromer.sh" 、 "./uninstaller-DataBromer.sh"
```

4. 按「y」確認解除安裝。

# 資訊 API Cloud Sync

REST 風格的 API 也提供網路 UI 所提供的功能。 Cloud Sync

## 快速入門

若要開始使用 Cloud Sync 此解決方案、您需要取得使用者權杖和 Cloud Central 帳戶 ID 。進行 API 呼叫時、您必須將權杖和帳戶 ID 新增至「授權」標頭。

### 步驟

1. 從 NetApp Cloud Central 取得使用者權杖。

```
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>"
}
```

2. 取得您的 Cloud Central 帳戶 ID 。

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

此 API 會傳回如下回應：

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

3. 在每個 API 呼叫的「授權」標頭中新增使用者權杖和帳戶 ID 。

◦ 範例 \*

下列範例顯示在 Microsoft Azure 中建立資料代理程式的 API 呼叫。您只需將 <user\_token>（使用者權杖）> 和 <AccountID> 替換成您在先前步驟中取得的權杖和 ID 即可。

```
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" }
```

### 權杖過期時該怎麼辦？

NetApp Cloud Central 的使用者權杖有到期日。若要重新整理權杖、您需要再次從步驟 1 呼叫 API。

API 回應包含「Expire\_in」欄位、指出權杖過期的時間。

## API 參考

如需每 Cloud Sync 個版本的資料、請參閱 <https://api.cloudsync.netapp.com/docs>。

## 使用清單 API

清單 API 為非同步 API、因此不會立即傳回結果（例如：「Get /data-kers/{id}/list-nfs\_export-folders」和「Get /data-ker/{id}/list-s3-buckets」）。伺服器唯一的回應是 HTTP 狀態 202。若要取得實際結果、您必須使用「Get /Messages / Client（取得 / 訊息 / 用戶端）」API。

### 步驟

1. 呼叫您要使用的清單 API。
2. 使用「Get /Messages / Client（取得 / 訊息 / 用戶端）」API 來檢視作業結果。
3. 使用相同的 API、將它附加到您剛收到的 ID：「Get   
http://api.cloudsync.netapp.com/api/messages/client?last=<id\_from\_step\_2>」

請注意、每次您呼叫「Get /Messages / Client（取得 / 訊息 / 用戶端）」API 時、ID 都會變更。

◦ 範例 \*

當您呼叫「list-s3-buckets」API 時、不會立即傳回結果：

```
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 、表示訊息已被接受、但尚未處理。

若要取得作業結果、您需要使用下列 API：

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

結果是一個陣列、其中一個物件包含 ID 欄位。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"
  }
]
```

您現在可以使用剛收到的 ID 進行下列 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物件、其中包含作業名稱（做為金鑰）及其結果（做為值）。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"
  }
]
```

# 概念

## 授權總覽

在您的 14 天免費試用結束後、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、以隨用隨付或每年付費。第二種選擇是直接向 NetApp 購買授權。

### 市場訂閱

訂閱 Cloud Sync AWS 或 Azure 提供的支援服務、可讓您以每小時的費率付款、或是每年付費。"[您可以透過 AWS 或 Azure 訂閱](#)"（視您要帳單的地點而定）。

#### 每小時訂閱

透過每小時隨用隨付訂閱、您將根據所建立的同步關係數、每小時收取一次費用。

- "[在 Azure 中檢視定價](#)"
- "[在 AWS 中檢視隨用隨付定價](#)"

#### 一年訂閱

一年訂閱可提供 20 種同步關係的授權、您可以預付費用。如果您的同步關係超過20個、而且您已透過AWS訂閱、則需在一小時內支付額外的關係費用。

"[在 AWS 中檢視年度定價](#)"

## NetApp 授權

另一種預付同步關係費用的方法是直接向 NetApp 購買授權。每個授權可讓您建立最多 20 個同步關係。

您可以搭配 AWS 或 Azure 訂閱使用這些授權。例如、如果您有 25 個同步關係、您可以使用授權支付前 20 個同步關係的費用、然後從 AWS 或 Azure 購買剩餘的 5 個同步關係。

"[瞭解如何購買授權、並將其新增 Cloud Sync 至](#)"。

### 授權條款

購買「自帶授權（BYOL）到 Cloud Sync 該服務」的客戶、應注意授權權利的相關限制。

- 自交付日起一年內、客戶有權使用 BYOL 授權。
- 客戶有權利用 BYOL 授權、在來源與目標之間建立且不超過 20 個個別連線（每個連線都是「同步關係」）。
- 客戶的權利將在一年授權期限結束時到期、無論客戶是否達到 20 個同步關係限制。
- 如果客戶選擇續約其授權、則與先前授權授予相關的未使用同步關係不會滾存至授權續約。



# 資料隱私

NetApp 無法存取您在使用 Cloud Sync 此服務時提供的任何認證資料。這些認證資料會直接儲存在網路中的資料代理機器上。

根據您選擇的組態、Cloud Sync 當您建立新關係時、可能會提示您輸入認證資料。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。

這些認證資料一律會直接儲存至資料代理程式本身。資料代理商位於網路中的機器上、無論是內部部署或雲端帳戶。這些認證資料絕不會提供給 NetApp。

這些認證資料會使用 HashiCorp Vault 在資料代理機器上進行本機加密。

## 技術常見問題集 Cloud Sync

如果您只是想要快速回答問題、這個常見問題集就能幫上忙。

### 快速入門

下列問題與 Cloud Sync 使用指南有關。

#### 如何運作呢？ Cloud Sync

使用 NetApp 資料代理軟體、將資料從來源同步至目標（這稱為 `_sync 關係 _`） Cloud Sync。

資料代理人群組可控制來源與目標之間的同步關係。設定同步關係之後 Cloud Sync、即可分析來源系統、並將其分成多個複寫串流、以推送至您所選的目標資料。

初始複本之後、服務會根據您設定的排程同步任何變更的資料。

#### 14 天免費試用如何運作？

14 天免費試用版會在您註冊 Cloud Sync 使用 VMware 服務時開始。您不需支付 NetApp 的 Cloud Sync 費用、即可建立 14 天的穩固關係。不過、您部署的任何資料代理人的所有資源費用仍適用。

#### 此功能需要多少成本？ Cloud Sync

有兩種成本與 Cloud Sync 使用效益有關：服務費用和資源費用。

- 服務費用 \*

針對隨用隨付定價、Cloud Sync 根據您所建立的同步關係數量、不收取每小時的服務費用。

- ["在 AWS 中檢視隨用隨付定價"](#)
- ["在 AWS 中檢視年度定價"](#)
- ["在 Azure 中檢視定價"](#)

您也可以透過 NetApp 代表取得此套軟體授權。Cloud Sync 每個授權可在 12 個月內建立 20 個同步關係。

["深入瞭解授權"](#)。



不需再為其提供任何功能、Cloud Sync Cloud Volumes Service Azure NetApp Files

- 資源費用 \*

資源費用與在雲端執行資料代理商所需的運算和儲存成本有關。

### 如何收費？ **Cloud Sync**

在您的 14 天免費試用結束後、有兩種方式可以支付同步關係的費用。第一個選項是向 AWS 或 Azure 訂閱、讓您可以隨用隨付或每年付費。第二種選擇是直接向 NetApp 購買授權。

我可以在 **Cloud Sync** 雲端以外使用這個功能嗎？

是的、Cloud Sync 您可以在非雲端架構中使用來源和目標可以駐留在內部部署、資料代理軟體也可以駐留在內部。

請注意以下關於 Cloud Sync 在雲端外部使用功能的重點：

- 若要進行內部部署同步、可透過 NetApp StorageGRID 推出私有 Amazon S3 儲存庫。
- 資料代理人群組需要網際網路連線才能與 Cloud Sync 該服務進行通訊。
- 如果您不直接向 NetApp 購買授權、您將需要 AWS 或 Azure 帳戶來 Cloud Sync 支付 PAYGO 服務費用。

我該如何存取 **Cloud Sync** 才能存取的問題？

Cloud Manager 可在 \* Sync\* 索引標籤中找到這個解決方案。Cloud Sync

什麼是資料代理群組？

每個資料代理程式都屬於資料代理程式群組。將資料代理人集中在一起、有助於提升同步關係的效能。

### 支援的來源和目標

下列問題與同步關係中支援的來源和目標有關。

哪些來源和目標 **Cloud Sync** 不支援呢？

支援多種不同類型的同步關係。Cloud Sync ["檢視完整清單"](#)。

哪些 **NFS** 和 **SMB** 版本 **Cloud Sync** 支援呢？

支援 NFS 版本 3 及更新版本、以及 SMB 版本 1 及更新版本。Cloud Sync

["深入瞭解同步需求"](#)。

當 **Amazon S3** 成為目標時、資料是否可以分層至特定的 **S3** 儲存類別？

是的、當 AWS S3 為目標時、您可以選擇特定的 S3 儲存類別：

- 標準（這是預設類別）
- 智慧分層
- 標準非常用存取
- 單一區域不常用存取
- 冰川
- Glacier Deep 歸檔

**Azure Blob** 儲存設備的儲存層又如何？

當 Blob 容器為目標時、您可以選擇特定的 Azure Blob 儲存層：

- 熱儲存
- 超酷儲存設備

您是否支援**Google Cloud**儲存層？

是的、當Google Cloud Storage資源桶成為目標時、您可以選擇特定的儲存類別：

- 標準
- 近線
- 冷線
- 歸檔

## 網路

下列問題與 Cloud Sync 關於功能的網路需求有關。

哪些網路需求 **Cloud Sync** 是關於功能的？

由於此環境要求資料代理群組透過所選的傳輸協定或物件儲存API（Amazon S3、Azure Blob、IBM Cloud Object Storage）、與來源和目標連線。Cloud Sync

此外、資料代理人群組需要透過連接埠443的傳出網際網路連線、以便與Cloud Sync 該服務進行通訊、並聯絡其他服務與儲存庫。

如需詳細資料、["檢閱網路需求"](#)。

我可以將 **Proxy** 伺服器與資料代理程式搭配使用嗎？

是的。

支援 Proxy 伺服器、無論是否具備基本驗證。Cloud Sync如果您在部署資料代理程式時指定 Proxy 伺服器、則來自資料代理程式的所有 HTTP 和 HTTPS 流量都會透過 Proxy 路由傳送。請注意、NFS 或 SMB 等非 HTTP 流量無法透過 Proxy 伺服器路由傳送。

唯一的 Proxy 伺服器限制是使用即時資料加密搭配 NFS 或 Azure NetApp Files 不同步關係。加密資料會透過 HTTPS 傳送、無法透過 Proxy 伺服器路由傳送。

## 資料同步

下列問題與資料同步的運作方式有關。

同步處理的頻率為何？

預設排程設定為每日同步。初始同步之後、您可以：

- 將同步排程修改為所需的天數、小時數或分鐘數
- 停用同步排程
- 刪除同步排程（不會遺失任何資料；只會移除同步關係）

最低同步排程是多少？

您可以排程關係、每 1 分鐘同步一次資料。

當檔案無法同步時、資料代理群組是否會重試？還是超時？

當單一檔案無法傳輸時、資料代理群組不會逾時。相反地、資料代理群組會在跳過檔案之前重試3次。重試值可在同步關係的設定中設定。

["瞭解如何變更同步關係的設定"](#)。

如果我有很大的資料集該怎麼辦？

如果單一目錄包含60、000個以上的檔案、[請寄送電子郵件至ng-cloudsync-support@netapp.com](mailto:ng-cloudsync-support@netapp.com)（請與我們聯絡）、以便我們協助您設定資料代理群組來處理有效負載。我們可能需要新增額外的記憶體至資料代理群組。

請注意、掛載點中的檔案總數沒有限制。擁有60萬個以上檔案的大型目錄需要額外的記憶體、無論其在階層架構中的層級為何（上層目錄或子目錄）。

## 安全性

下列與安全性有關的問題。

是否安全無虞？ **Cloud Sync**

是的。所有 Cloud Sync 的服務網路連線都是使用來完成 "[Amazon Simple Queue Service （SQS）](#)"。

資料代理人群組與Amazon S3、Azure Blob、Google Cloud Storage和IBM Cloud Object Storage之間的所有通訊都是透過HTTPS傳輸協定進行。

如果 Cloud Sync 您使用的是內部部署（來源或目的地）系統的功能、以下是幾個建議的連線選項：

- AWS Direct Connect、Azure ExpressRoute 或 Google Cloud InterConnect 連線、非網際網路路由（而且只能與您指定的雲端網路通訊）
- 內部部署閘道裝置與雲端網路之間的 VPN 連線
- 若要使用 S3 儲存區、Azure Blob 儲存設備或 Google Cloud Storage、Amazon Private S3 端點、Azure Virtual Network 服務端點或私有 Google Access 進行額外安全的資料傳輸。

以上任何一種方法都會在內部部署的NAS伺服器和Cloud Sync 一個可靠的資料代理群組之間建立安全的連線。

資料是否以 **Cloud Sync** 不加密的方式加密？

- 支援來源與目標 NFS 伺服器之間的資料傳輸加密。Cloud Sync ["深入瞭解"](#)。
- 對於SMB、Cloud Sync 支援伺服器端加密的SMB 3.0和3.11資料。將加密資料從來源複製到資料保持加密的目標。Cloud Sync

無法加密SMB資料本身。Cloud Sync

- 當 Amazon S3 儲存區是同步關係的目標時、您可以選擇是否使用 AWS 加密或 AES-256 加密來啟用資料加密。

## 權限

下列問題與資料權限有關。

**SMB** 資料權限是否同步至目標位置？

您可以設定Cloud Sync 支援功能、在來源SMB共用區和目標SMB共用區之間、以及從來源SMB共用區到物件儲存區之間保留存取控制清單（ACL除外ONTAP）。



不支援將ACL從物件儲存區複製到SMB共用區。Cloud Sync

["瞭解如何在 SMB 共用區之間複製 ACL"](#)。

**NFS** 資料權限是否同步至目標位置？

下列項目可自動複製 NFS 伺服器之間的 NFS 權限：Cloud Sync

- NFS 版本 3：Cloud Sync 此功能可複製權限和使用者群組擁有者。
- NFS 第 4 版：Cloud Sync 以程式複製 ACL。

## 物件儲存中繼資料

針對下列類型的同步關係、將物件儲存中繼資料從來源複製到目標：Cloud Sync

- Amazon S3 → Amazon S3 <sup>1</sup>
- Amazon S3 → StorageGRID
- 支援：→ Amazon S3 StorageGRID
- 《》 → 《StorageGRID StorageGRID
- 資料中心→ Google Cloud Storage StorageGRID
- Google Cloud Storage → StorageGRID 功能
- Google Cloud Storage → IBM Cloud Object Storage（IBM雲端物件儲存設備）<sup>1</sup>
- Google Cloud Storage → Amazon S3 <sup>1</sup>
- Amazon S3 → Google Cloud Storage

- IBM Cloud Object Storage → Google Cloud Storage
- 《》 → 《IBM Cloud Object Storage》 StorageGRID
- IBM Cloud Object Storage → StorageGRID
- IBM Cloud Object Storage → IBM Cloud Object Storage

您必須在這些同步關係中 "[建立同步關係時啟用設定](#)"。

## 效能

下列問題與 Cloud Sync 效能不一致有關。

同步關係的進度指標代表什麼？

同步關係顯示資料代理群組網路卡的處理量。如果您使用多個資料代理人來加速同步效能、則處理量是所有流量的總和。此處理量每 20 秒重新整理一次。

我遇到效能問題。我們可以限制並行傳輸的數量嗎？

如果您有非常大的檔案（每個都有多個Tib）、可能需要很長時間才能完成傳輸程序、而且效能可能會受到影響。

限制並行傳輸的數量有助於提高效率。mailto : [ng-cloudsync-support@netapp.com](mailto:ng-cloudsync-support@netapp.com) [ 請聯絡我們尋求協助 ]。

為什麼 **Azure NetApp Files** 我使用 **VMware** 時效能不佳？

當您將資料同步至 Azure NetApp Files 或從 VMware 同步時、如果磁碟服務層級為「Standard（標準）」、您可能會遇到故障和效能問題。

將服務層級變更為 Premium 或 Ultra、以提升同步效能。

["深入瞭解 Azure NetApp Files 解有關服務層級和處理量的資訊"](#)。

為什麼 **Cloud Volumes Service** 我使用適用於 **AWS** 的解決方法時效能不佳？

當您在雲端磁碟區之間或從雲端磁碟區同步資料時、如果雲端磁碟區的效能等級為「Standard（標準）」、可能會發生故障和效能問題。

將「服務層級」變更為「進階」或「極致」、以增強同步效能。

群組中需要多少個資料代理人？

當您建立新關係時、首先要從群組中的單一資料代理程式開始（除非您選取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滿足同步關係的效能要求。如果沒有、您可以在群組中新增額外的資料代理人、以加速同步效能。但您應該先檢查其他可能影響同步效能的因素。

多種因素可能會影響資料傳輸效能。整體同步效能可能會因為網路頻寬、延遲和網路拓撲、以及資料代理 VM 規格和儲存系統效能而受到影響。例如、群組中的單一資料代理程式可以達到100 MB/s、而目標上的磁碟處理量可能只允許64 MB/s因此、資料代理人群組會持續嘗試複製資料、但目標無法達到資料代理人群組的效能。

因此、請務必檢查網路效能和目標磁碟處理量。

然後、您可以考慮在群組中新增額外的資料代理人、以共享該關係的負載、藉此加速同步效能。"[瞭解如何加速同步效能](#)"。

## 刪除物件

下列問題與刪除來源和目標的同步關係和資料有關。

如果我刪除 **Cloud Sync** 我的不確定關係、會發生什麼事？

刪除關係會停止所有未來的資料同步、並終止付款。同步至目標的任何資料都會維持原樣。

如果我從來源伺服器刪除某些內容、會發生什麼事？是否也從目標中移除？

根據預設、如果您有作用中的同步關係、則在下次同步處理期間、從來源伺服器刪除的項目不會從目標中刪除。但每個關係的同步設定中都有一個選項、您可以定義 Cloud Sync 如果檔案從來源中刪除、將會刪除目標位置的檔案。

"[瞭解如何變更同步關係的設定](#)"。

如果我從目標中刪除某項內容、會發生什麼事？是否也從來源移除？

如果項目從目標中刪除、則不會從來源中移除。這種關係是單向的、從來源到目標。在下一個同步週期中 Cloud Sync、Sync-比較 來源與目標、找出項目遺失、Cloud Sync 並再次將其從來源複製到目標。

## 疑難排解

"[NetApp 知識庫 Cloud Sync：解決常見問題集：支援與疑難排解](#)"

## 資料代理商深入探討

下列問題與資料代理程式有關。

您可以說明資料代理商的架構嗎？

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。
- 下列項目可部署資料代理程式：Cloud Sync
  - AWS：使用 AWS CloudFormation 範本
  - Azure：來自 Azure 資源管理程式
  - Google：來自 Google Cloud Deployment Manager
  - 如果您使用自己的 Linux 主機、則需要手動安裝軟體
- 資料代理軟體會自動升級至最新版本。
- 資料代理商使用 AWS SQS 作為可靠且安全的通訊通道、並用於控制和監控。SQS 也提供持續性層。
- 您可以新增其他資料代理人至群組、以提高傳輸速度並增加高可用度。如果某個資料代理程式故障、就會有服務恢復功能。



# 知識與支援

## 註冊以取得支援

在您透過NetApp技術支援開啟支援案例之前、您必須先將NetApp支援網站帳戶新增至Cloud Manager、然後註冊以取得支援。

### 新增一個NSS帳戶

「支援儀表板」可讓您從單一位置新增及管理所有NetApp支援網站帳戶。

#### 步驟

1. 如果您還沒有 NetApp 支援網站帳戶、"[註冊一項](#)"。
2. 在Cloud Manager主控台右上角、按一下「說明」圖示、然後選取\*「支援」\*。



3. 按一下「[nss管理](#)」>「新增nssAccount」。
4. 出現提示時、按一下\*繼續\*以重新導向至Microsoft登入頁面。

NetApp使用Microsoft Azure Active Directory做為身分識別供應商、提供專為支援與授權所設計的驗證服務。

5. 在登入頁面上、提供您的NetApp支援網站註冊電子郵件地址和密碼、以執行驗證程序。

此動作可讓Cloud Manager使用您的NSS帳戶。

附註：帳戶必須是客戶層級的帳戶（非來賓帳戶或臨時帳戶）。

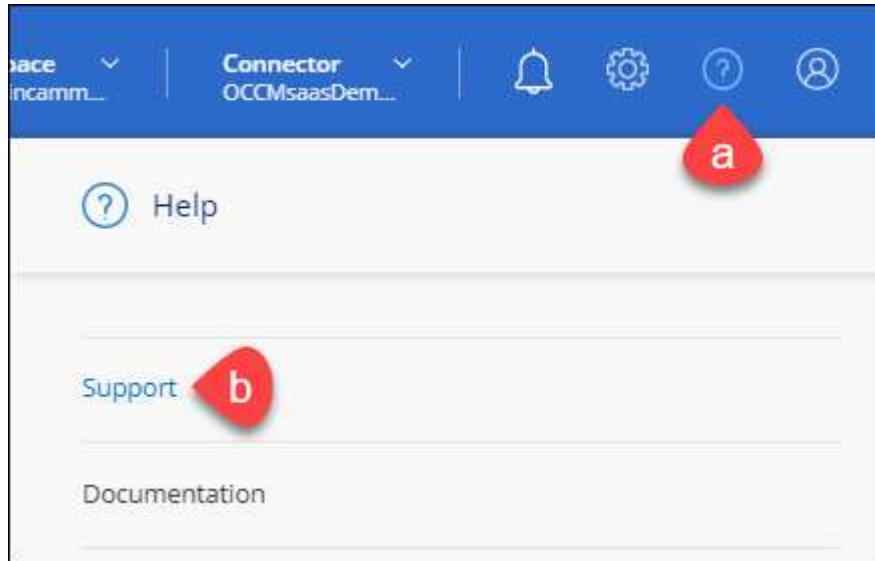
### 註冊您的帳戶以取得支援

支援註冊可從支援儀表板的Cloud Manager取得。

#### 步驟



1. 在Cloud Manager主控台右上角、按一下「說明」圖示、然後選取\*「支援」\*。



2. 在\* Resources（資源）選項卡中，單擊 Register for Support\*（註冊以獲得支持\*）。
3. 選取您要登錄的NSS認證、然後按一下「登錄」。

## 取得協助

NetApp以多種方式支援Cloud Manager及其雲端服務。我們全年無休提供豐富的免費自助支援選項、例如知識庫（KB）文章和社群論壇。您的支援註冊包括透過網路票證提供遠端技術支援。

### 自我支援

這些選項可供免費使用、一天24小時、一週7天：

- "知識庫"

請搜尋Cloud Manager知識庫、找出有助於疑難排解問題的文章。

- "社群"

加入Cloud Manager社群、追蹤後續討論或建立新討論。

- 文件

您目前正在檢視的Cloud Manager文件。

- mailto：[ng-cloudmanager-feedback@netapp.com](mailto:ng-cloudmanager-feedback@netapp.com) [意見反應電子郵件]

我們非常重視您的意見。提交意見反應、協助我們改善Cloud Manager。

### NetApp支援

除了上述的自我支援選項、您也可以與NetApp支援工程師合作、在您啟動支援之後解決任何問題。

## 步驟

1. 在Cloud Manager中、按一下\*「說明」>「支援」\*。
2. 在「Technical Support（技術支援）」下選擇可用的選項之一：
  - a. 按一下\*致電我們\*以尋找NetApp技術支援的電話號碼。
  - b. 按一下「開啟問題」、選取其中一個選項、然後按一下「傳送」。

NetApp代表將審查您的案例、並盡快回覆您。

# 法律聲明

法律聲明提供版權聲明、商標、專利等存取權限。

## 版權

<http://www.netapp.com/us/legal/copyright.aspx>

## 商標

NetApp、NetApp 標誌及 NetApp 商標頁面上列出的標章均為 NetApp、Inc. 的商標。其他公司與產品名稱可能為其各自所有者的商標。

<http://www.netapp.com/us/legal/netapptmlist.aspx>

## 專利

如需最新的 NetApp 擁有專利清單、請參閱：

<https://www.netapp.com/us/media/patents-page.pdf>

## 隱私權政策

<https://www.netapp.com/us/legal/privacypolicy/index.aspx>

## 開放原始碼

通知檔案提供有關 NetApp 軟體所使用之協力廠商版權與授權的資訊。

"關於本產品的注意事項 Cloud Sync"

## 版權資訊

Copyright©2022 NetApp、Inc.版權所有。美國印製本文件中版權所涵蓋的任何部分、不得以任何形式或任何方式（包括影印、錄製、在未事先取得版權擁有者書面許可的情況下、在電子擷取系統中進行錄音或儲存。

衍生自受版權保護之NetApp資料的軟體必須遵守下列授權與免責聲明：

本軟體係由NetApp「依現狀」提供、不含任何明示或暗示的保證、包括但不限於適售性及特定用途適用性的暗示保證、特此聲明。在任何情況下、NetApp均不對任何直接、間接、偶發、特殊、示範、或衍生性損害（包括但不限於採購替代商品或服務；使用損失、資料或利潤損失；或業務中斷）、無論是在合約、嚴格責任或侵權行為（包括疏忽或其他）中、無論是因使用本軟體而產生的任何責任理論（包括疏忽或其他）、即使已被告知可能造成此類損害。

NetApp保留隨時變更本文所述之任何產品的權利、恕不另行通知。除非NetApp以書面明確同意、否則NetApp不承擔因使用本文所述產品而產生的任何責任或責任。使用或購買本產品並不代表NetApp擁有任何專利權利、商標權利或任何其他智慧財產權。

本手冊所述產品可能受到一或多個美國國家/地區的保護專利、國外專利或申請中。

限制權利圖例：政府使用、複製或揭露受DFARS 252.277-7103（1988年10月）和FAR 52-227-19（1987年6月）技術資料與電腦軟體權利條款（c）（1）（ii）分段所述限制。

## 商標資訊

NetApp、NetApp標誌及所列的標章 <http://www.netapp.com/TM> 為NetApp、Inc.的商標。其他公司和產品名稱可能為其各自所有者的商標。