



開始使用

Set up and administration

NetApp
July 15, 2022

目錄

開始使用	1
深入瞭解 Cloud Manager	1
入門檢查清單	2
註冊 NetApp Cloud Central	5
登入 Cloud Manager	6
設定NetApp帳戶	8
設定連接器	16
下一步	53

開始使用

深入瞭解 Cloud Manager

Cloud Manager 可讓 IT 專家和雲端架構設計師使用 NetApp 的雲端解決方案、集中管理混合式多雲端基礎架構。

功能

Cloud Manager 是企業級 SaaS 型管理平台、無論資料位於何處、都能讓您隨時掌控資料。

- 設定與使用 ["Cloud Volumes ONTAP"](#) 實現跨雲端的高效率多重傳輸協定資料管理。
- 設定及使用檔案儲存服務：
 - ["Azure NetApp Files"](#)
 - ["Amazon FSX for ONTAP Sf"](#)
 - ["AWS 適用的 Cloud Volumes Service"](#)
 - ["適用於 Google Cloud Cloud Volumes Service"](#)
- 建立 ONTAP 磁碟區、備份至雲端、在混合雲中複寫資料、以及將冷資料分層至雲端、藉此探索及管理內部的支援功能。
- 啟用整合式雲端服務、例如：
 - ["雲端資料感測"](#)
 - ["Cloud Insights"](#)
 - ["雲端備份"](#)

["深入瞭解 Cloud Manager"](#)。

支援的物件儲存供應商

Cloud Manager 可讓您管理雲端儲存設備、並在 Amazon Web Services、Microsoft Azure 及 Google Cloud 中使用雲端服務。

成本

Cloud Manager 軟體是由 NetApp 免費提供。

在大多數的工作中、Cloud Manager 會提示您在雲端網路中部署 Connector、這會導致雲端供應商對運算執行個體和相關儲存設備的收費。您可以選擇在內部環境中執行 Connector 軟體。

["瞭解連接器的預設組態"](#)。

Cloud Manager 的運作方式

Cloud Manager 包含與 NetApp Cloud Central 整合的 SaaS 型介面、以及可管理 Cloud Volumes ONTAP 各種效益和其他雲端服務的 Connectors。

軟體即服務

Cloud Manager 可透過存取 "[SaaS 型使用者介面](#)" 和 API 。這項SaaS體驗可讓您在最新功能發佈時自動存取、並在NetApp帳戶和連接器之間輕鬆切換。

NetApp Cloud Central

"[NetApp Cloud Central](#)" 提供集中位置以供存取和管理 "[NetApp 雲端服務](#)"。透過集中式使用者驗證、您可以使用相同的認證資料集來存取 Cloud Manager 和 Cloud Insights 其他雲端服務、例如：

NetApp帳戶

首次登入Cloud Manager時、系統會提示您建立_NetApp帳戶_。此帳戶提供多租戶共享、可讓您在隔離的 _stap 空間 _ 中組織使用者和資源。

連接器

在大多數情況下、帳戶管理員需要在雲端或內部部署網路中部署 *Connector* 。Connector 可讓 Cloud Manager 管理公有雲環境中的資源與程序。

連接器應隨時保持執行狀態。這對於您持續啟用的服務健全狀況和營運而言十分重要。

例如、連接器是Cloud Volumes ONTAP 運作過程中的關鍵要素。如果連接器關機、Cloud Volumes ONTAP 具有節點型授權的現象將會在與連接器失去通訊超過14天之後關閉。

["深入瞭解何時需要連接器及其運作方式"](#)。

SOC 2類型2認證

一家獨立認證的公共會計公司和服務稽核員、負責審查Cloud Manager Cloud Sync 、NetApp、Cloud Tiering 、Cloud Data Sense和Cloud Backup (Cloud Manager平台)、並確認他們已根據適用的信任服務條件、達成SOC 2類報告。

["檢視NetApp的SOC 2報告"](#)

入門檢查清單

請使用此檢查清單、瞭解在連接器具有傳出網際網路存取權限的典型部署中、使用Cloud Manager進行運作所需的條件。

NetApp Cloud Central登入

您必須註冊 "[NetApp Cloud Central](#)" 以便存取Cloud Manager和其他雲端服務。

從網頁瀏覽器存取多個端點的網路

Cloud Manager使用者介面可從網頁瀏覽器存取。當您使用Cloud Manager使用者介面時、IT人員會聯絡數個端點、以完成資料管理工作。執行網頁瀏覽器的機器必須連線至下列端點。

端點	目的
http://cloudmanager.netapp.com	使用SaaS UI時、您的網頁瀏覽器會連絡此URL。

端點	目的
<p>AWS 服務 (amazonaws.com):</p> <ul style="list-style-type: none"> • CloudFormation • Cognito • 彈性運算雲端 (EC2) • 金鑰管理服務 (KMS) • 安全性權杖服務 (STOS) • 簡易儲存服務 (S3) 	<p>需要從AWS的Cloud Manager部署Connector。確切的端點取決於部署Connector的區域。"如需詳細資料、請參閱 AWS 文件。"</p>
<p>https://management.azure.com https://login.microsoftonline.com</p>	<p>在大多數Azure地區部署Cloud Manager連接器時、都必須使用此功能。</p>
<p>https://management.microsoftazure.de https://login.microsoftonline.de</p>	<p>需要在Azure Germany地區部署Cloud Manager的Connector。</p>
<p>https://management.usgovcloudapi.net https://login.microsoftonline.com</p>	<p>需要在Azure US Gov地區部署Cloud Manager的Connector。</p>
<p>https://www.googleapis.com</p>	<p>需要在Google Cloud中部署Cloud Manager的Connector。</p>
<p>https://signin.b2c.netapp.com</p>	<p>需要更新NetApp支援網站 (NSS) 認證或新增新的NSS-認證至Cloud Manager。</p>
<p>https://netapp-cloud-account.auth0.com https://cdn.auth0.com https://services.cloud.netapp.com</p>	<p>您的網頁瀏覽器會連線至這些端點、以便透過NetApp Cloud Central 進行集中式使用者驗證。</p>
<p>https://widget.intercom.io</p>	<p>產品內對談可讓您與 NetApp 雲端專家交談。</p>
<p>連接器的IP位址</p>	<p>在大多數情況下、您應該使用SaaS UI中的Cloud Manager、但是 "如果您使用本機UI"然後您必須從網頁瀏覽器輸入主機的IP位址。</p> <p>視雲端供應商的連線能力而定、請使用指派給主機的私有IP或公有IP：</p> <ul style="list-style-type: none"> • 如果您有VPN並直接存取虛擬網路、則私有IP可正常運作 • 公有 IP 適用於任何網路情境 <p>無論是哪一種情況、請確保安全群組規則僅允許從授權的IP或子網路存取、以確保網路存取安全。</p>

連接器的傳出網路

登入Cloud Manager之後、帳戶管理員必須在雲端供應商或內部部署網路中部署_Connector_。Connector 可讓 Cloud Manager 管理公有雲環境中的資源與程序。連接器不需要Azure NetApp Files 用在功能不全的地方、Cloud Volumes Service 但Cloud Sync Cloud Manager中的所有其他服務和功能都需要連接器。"深入瞭解連接器及其運作方式"。

- 您部署Connector的網路位置必須具有傳出網際網路連線。

連接器需要存取傳出網際網路、才能連絡下列端點、以便管理公有雲環境中的資源和程序。

端點	目的
https://support.netapp.com	以取得授權資訊、並將AutoSupport 資訊傳送給NetApp支援部門。
https://*.cloudmanager.cloud.netapp.com	在Cloud Manager中提供SaaS功能與服務。
https://cloudmanagerinfraproduct.azurecr.io https://*.blob.core.windows.net	升級Connector及其Docker元件。

- 如果您選擇在自己的Linux主機上手動安裝Connector（而非直接從Cloud Manager介面安裝）、則Connector的安裝程式在安裝過程中需要存取下列端點：
 - <https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm>
 - <https://s3.amazonaws.com/aws-cli/awscli-bundle.zip>
 - https://*.blob.core.windows.net或<https://hub.docker.com>

主機可能會在安裝期間嘗試更新作業系統套件。主機可聯絡不同的鏡射站台、以取得這些 OS 套件。

- 除非您啟動連接器、否則不會有傳入流量進入連接器。

HTTP（80）和HTTPS（443）可存取本機UI、在極少數情況下使用。只有在需要連線至主機進行疑難排解時、才需要SSH（22）。

雲端供應商權限

您需要擁有權限的帳戶、才能直接從Cloud Manager在雲端供應商中部署Connector。



建立連接器的方法有許多種：您可以從建立連接器 ["AWS Marketplace"](#)、["Azure Marketplace"](#)或是您可以 ["手動安裝軟體"](#)。

位置	高階步驟	詳細步驟
AWS	<ol style="list-style-type: none"> 1. 使用包含在AWS中建立IAM原則所需權限的Json檔案。 2. 將原則附加至IAM角色或IAM使用者。 3. 建立Connector時、請為Cloud Manager提供IAM角色的ARN或IAM使用者的AWS存取金鑰和秘密金鑰。 	"按一下此處以檢視詳細步驟" 。
Azure	<ol style="list-style-type: none"> 1. 使用包含必要權限的Json檔案、在Azure中建立自訂角色。 2. 將角色指派給將從Cloud Manager建立Connector的使用者。 3. 當您建立Connector時、請使用具有所需權限的Microsoft帳戶（Microsoft擁有並裝載的登入提示）登入。 	"按一下此處以檢視詳細步驟" 。

位置	高階步驟	詳細步驟
Google Cloud	<ol style="list-style-type: none"> 1. 使用Yaml檔案、其中包含在Google Cloud中建立自訂角色所需的權限。 2. 將該角色附加至將從Cloud Manager建立Connector的使用者。 3. 如果您打算使用Cloud Volumes ONTAP 此功能、請設定具有所需權限的服務帳戶。 4. 啟用Google Cloud API。 5. 當您建立Connector時、請使用具有所需權限的Google帳戶登入（登入提示由Google擁有並裝載）。 	"按一下此處以檢視詳細步驟"。

個別服務的網路功能

完成設定之後、您就可以開始使用Cloud Manager提供的服務。請注意、每項服務都有自己的網路需求。如需詳細資料、請參閱下列頁面。

- ["AWS 適用的 Cloud Volumes ONTAP"](#)
- ["適用於 Azure Cloud Volumes ONTAP"](#)
- ["適用於 GCP Cloud Volumes ONTAP"](#)
- ["資料複寫 ONTAP 功能"](#)
- ["部署Cloud Data Sense"](#)
- ["內部 ONTAP 部署的叢集"](#)
- ["雲端分層"](#)
- ["雲端備份"](#)

註冊 NetApp Cloud Central

註冊 NetApp Cloud Central 、即可存取 NetApp 的雲端服務。



您可以使用單一登入、從公司目錄（聯盟身分識別）使用認證登入。若要深入瞭解、請前往 ["Cloud Central說明中心"](#) 然後按一下* Cloud Central登入選項*。

步驟

1. 開啟網頁瀏覽器並前往 ["NetApp Cloud Central"](#)。
2. 按一下 * 註冊 *。
3. 您有兩種選擇：
 - a. 填寫表單、然後按一下 * 註冊 *。



The image shows a web form titled "Log In to NetApp Cloud Central". Below the title is a link "Already signed up? [Login](#)". The form contains several input fields: an email field with "user@example.com", a password field with masked characters, a "NetApp" field, a "New user" field, and a "Phone" field with a "*optional" label. At the bottom is a large blue "SIGN UP" button and a checkbox labeled "I accept the terms and conditions.".

- b. 如果您有已註冊的NetApp支援網站帳戶、請按一下*登入NetApp*、然後輸入您的NetApp支援網站認證資料。

每次登入時、您都必須使用在此註冊程序中選擇的選項。



當您使用NetApp登入時、您的NetApp支援網站認證不會新增至Support Dashboard中的Cloud Manager。

4. 等待 NetApp Cloud Central 寄送電子郵件。
5. 按一下電子郵件中的連結、確認您的電子郵件地址。

您現在擁有作用中的 Cloud Central 使用者登入權限。

登入 Cloud Manager

Cloud Manager 介面可透過 SaaS 型使用者介面存取、方法是前往 <https://cloudmanager.netapp.com>。

如果您是從政府區域或沒有外傳網際網路存取權限的站台存取Cloud Manager、則必須登入連接器上執行的本機使用者介面。"瞭解如何存取Connector上的本機UI"。



您可以使用單一登入、從公司目錄（聯盟身分識別）使用認證登入。若要深入瞭解、請前往"[Cloud Central說明中心](#)" 然後按一下* Cloud Central登入選項*。

步驟

1. 開啟網頁瀏覽器並前往 <https://cloudmanager.netapp.com>。
2. 輸入您的NetApp Cloud Central認證資料、或按一下*登入NetApp*並輸入您的NetApp支援網站認證資料、即可登入。

您必須選擇註冊Cloud Central時使用的選項。

- 如果您註冊時輸入了電子郵件和密碼、則每次登入時都必須輸入這些認證資料。
- 如果您以NetApp支援網站認證登入、則每次都需要使用該登入選項。

Log In to NetApp Cloud Central

Don't have an account yet? [Sign Up](#)

LOG IN

[Forgot password?](#)

Or

Have a registered NetApp Support Site account?

Log In with NetApp

您現在已經登入、可以開始使用Cloud Manager來管理混合式多雲端基礎架構。

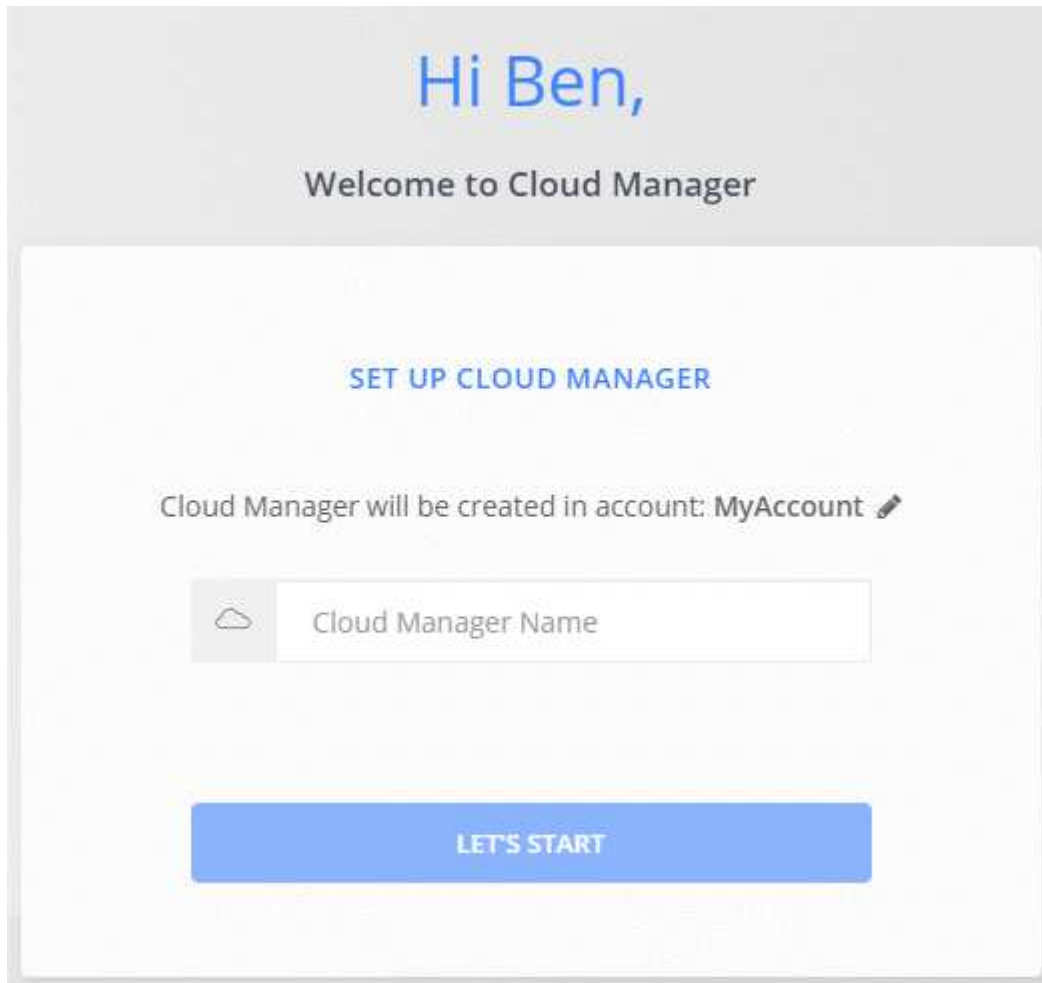
設定NetApp帳戶

瞭解NetApp客戶

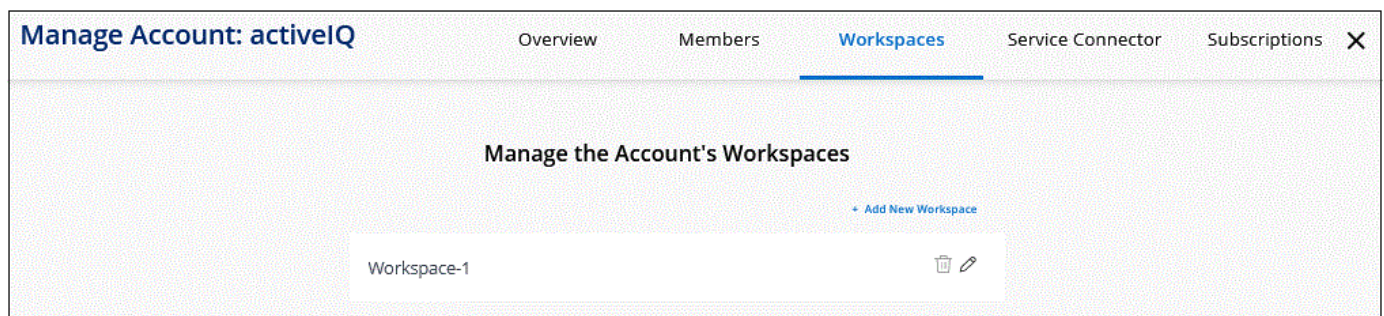
NetApp帳戶_提供多租戶共享、讓您從Cloud Manager內部、在隔離的工作區中組織使用者和資源。

例如、多位使用者可以在 Cloud Volumes ONTAP 稱為 _stap空間_ 的隔離環境中部署及管理各種不一致的系統。除非共用這些工作區、否則其他使用者無法看到這些工作區。

第一次存取Cloud Manager時、系統會提示您選擇或建立NetApp帳戶：



接著、帳戶管理員可以管理使用者（成員）、工作區、連接器及訂閱、藉此修改此帳戶的設定：



如需逐步指示、請參閱 ["設定NetApp帳戶"](#)。

帳戶設定

Cloud Manager中的「管理帳戶」小工具可讓客戶管理員管理NetApp帳戶。如果您剛建立帳戶、就會從頭開始。但如果您已經設定帳戶、您會看到 **_ 全部 _** 與帳戶相關聯的使用者、工作區、連接器和訂閱。

總覽

「總覽」頁面會顯示「帳戶名稱」和「帳戶ID」。註冊某些服務時、您可能需要提供您的帳戶ID。本頁也包含一些Cloud Manager組態選項。

成員

成員是您與NetApp帳戶建立關聯的NetApp Cloud Central使用者。將使用者與該帳戶中的帳戶和一或多個工作區建立關聯、可讓這些使用者在 Cloud Manager 中建立及管理工作環境。

當您建立使用者關聯時、您會指派一個角色給他們：

- *Account admin*：可在 Cloud Manager 中執行任何動作。
- *_Workspace 管理 _*：可在指派的工作區中建立及管理資源。
- *Compliance Viewer*：只能檢視Cloud Data Sense法規遵循資訊、並針對擁有存取權限的系統產生報告。
- *SURFAD_*：可以使用「支援服務」來建立應用程式一致的備份、並使用這些備份來還原資料。SnapCenter SnapCenter_此服務目前為試用版。_

["深入瞭解這些角色"](#)。

工作區

在 Cloud Manager 中、工作區會將任何數量的工作環境與其他工作環境隔離。除非帳戶管理員將該管理員與該工作區建立關聯、否則 Workspace 系統管理員無法存取工作區中的工作環境。

工作環境代表儲存系統：

- 單節點 Cloud Volumes ONTAP 的不完整系統或 HA 配對
- 您網路中的內部部署 ONTAP 式叢集
- NetApp 私有儲存組態中的一個叢集 ONTAP

["瞭解如何新增工作區"](#)。

連接器

Connector 可讓 Cloud Manager 管理公有雲環境中的資源與程序。Connector 可在您部署在雲端供應商的虛擬機器執行個體上執行、或是在您設定的內部部署主機上執行。

您可以使用連接器搭配多個 NetApp 雲端資料服務。例如、如果您已有 Connector for Cloud Manager、則可在設定雲端分層服務時加以選取。

["深入瞭解連接器"](#)。

訂閱

這些是與所選帳戶相關的NetApp訂閱。

當您從雲端供應商的市場訂閱 Cloud Manager 時、系統會將您重新導向至 Cloud Central 、您需要在其中儲存訂閱內容、並將其與特定帳戶建立關聯。

訂閱之後、即可從「管理帳戶」小工具取得每份訂閱。您只會看到與您目前檢視的帳戶相關聯的訂閱內容。

您可以選擇重新命名訂閱、以及取消訂閱與一或多個帳戶的關聯。

例如、假設您有兩個帳戶、每個帳戶都是透過個別的訂閱付費。您可能會取消訂閱與其中一個帳戶的關聯、因此該帳戶中的使用者在建立 Cloud Volume ONTAP 的工作環境時、不會意外選擇錯誤的訂閱。

["瞭解如何管理訂閱"](#)。

範例

下列範例說明您如何設定帳戶。



在後續的兩個範例影像中、Connector和Cloud Volumes ONTAP the SURF系 實際上並未駐留NetApp帳戶、而是在雲端供應商中執行。這是每個元件之間關係的概念呈現。

範例 1.

下列範例顯示使用兩個工作區來建立隔離環境的帳戶。第一個工作區適用於正式作業環境、第二个工作區適用於開發環境。

Account



範例 2.

以下是另一個使用兩個獨立NetApp帳戶顯示最高層級的多租戶共享的範例。例如、服務供應商可能會在一個帳戶中使用 Cloud Manager 來為客戶提供服務、而使用另一個帳戶來為其中一個業務單位提供災難恢復。

請注意、帳戶 2 包含兩個獨立的連接器。如果您的系統位於不同的地區、或是位於不同的雲端供應商、就可能發生這種情況。



在您的NetApp帳戶中設定工作區和使用者

首次登入Cloud Manager時、系統會提示您建立_NetApp帳戶_。此帳戶提供多租戶共享、可讓您在隔離的 _stap空間_ 中組織使用者和資源。

["深入瞭解NetApp客戶的運作方式"](#)。

設定您的NetApp帳戶、讓使用者能夠存取Cloud Manager、並存取工作區中的工作環境。只要新增單一使用者或新增多個使用者和工作區即可。

新增工作區

在 Cloud Manager 中、工作區可讓您將一組工作環境與其他工作環境和其他使用者隔離。例如、您可以建立兩個工作區、並將個別使用者與每個工作區建立關聯。

步驟

1. 從上而下 "Cloud Manager"，單擊* Account（帳戶）*下拉列表。



2. 按一下目前選取帳戶旁的 * 管理帳戶 *。



3. 按一下 * 工作區 * 。
4. 按一下「* 新增工作區 *」。
5. 輸入工作區名稱、然後按一下 * 「Add*（新增*）」。

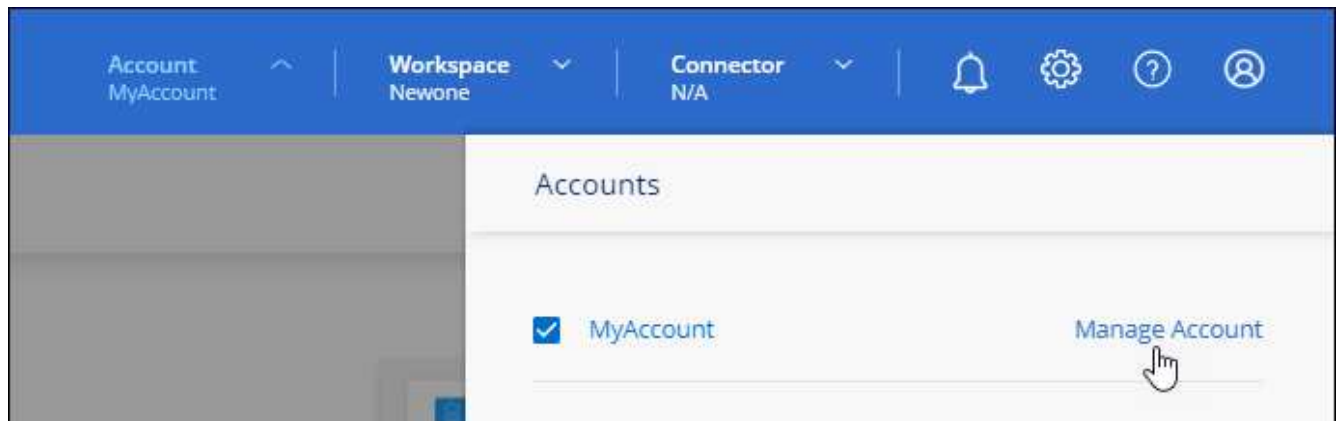
如果「工作區管理」需要存取此工作區、您就必須建立使用者的關聯。您也需要將 Connectors 與工作區建立關聯、讓 Workspace Admins 能夠使用這些 Connectors 。

新增使用者

將Cloud Central使用者與NetApp帳戶建立關聯、讓這些使用者可以在Cloud Manager中建立及管理工作環境。

步驟

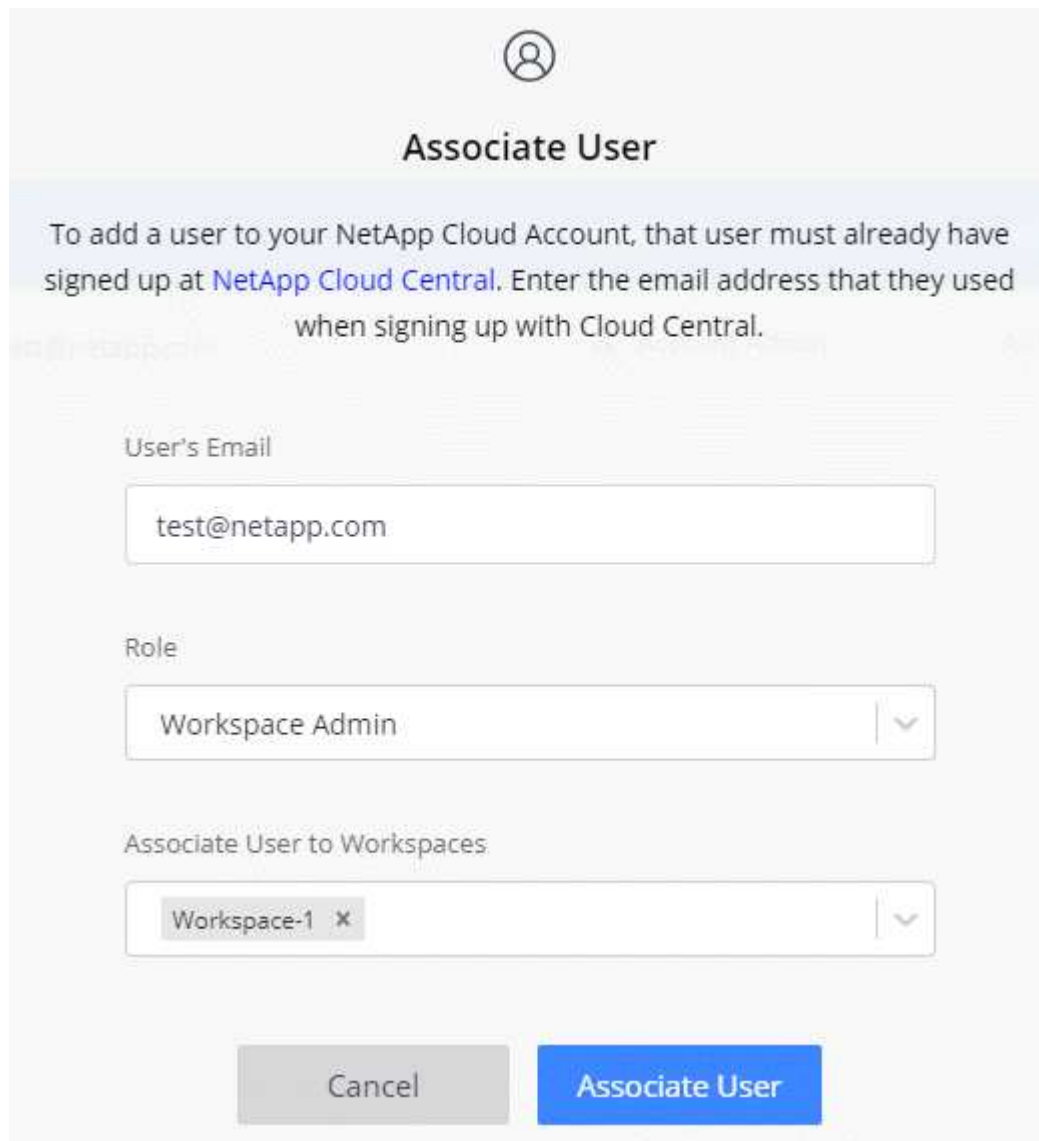
1. 如果使用者尚未這麼做、請要求使用者前往 "NetApp Cloud Central" 並註冊。
2. 從上而下 "Cloud Manager"，單擊* Account（帳戶）下拉列表並單擊 Manage Account*（管理帳戶）。



3. 在「成員」索引標籤中、按一下「關聯使用者」。
4. 輸入使用者的電子郵件地址、然後為使用者選取角色：
 - * 客戶管理 *：可在 Cloud Manager 中執行任何動作。
 - * 工作區管理 *：可在指派的工作區中建立及管理資源。
 - 法規遵循檢視器：只能檢視Cloud Data Sense控管與法規遵循資訊、並針對有權存取的工作區產生報告。
 - 《管理員》：可以使用「支援服務」來建立應用程式一致的備份、並使用這些備份來還原資

料。SnapCenter SnapCenter此服務目前為試用版。

5. 如果您選取帳戶管理員以外的帳戶、請選取一個或多個工作區以與該使用者建立關聯。



The image shows a web-based dialog box titled "Associate User". At the top, there is a user icon. Below the title, a message states: "To add a user to your NetApp Cloud Account, that user must already have signed up at [NetApp Cloud Central](#). Enter the email address that they used when signing up with Cloud Central." The form contains three fields: "User's Email" with the text "test@netapp.com", "Role" with a dropdown menu showing "Workspace Admin", and "Associate User to Workspaces" with a dropdown menu showing "Workspace-1" and a close button (X). At the bottom, there are two buttons: "Cancel" and "Associate User".

6. 按一下「* 經銷 *」。

使用者應收到 NetApp Cloud Central 寄送的電子郵件、標題為「Account Association（客戶關聯）」。電子郵件中包含存取 Cloud Manager 所需的資訊。

將 **Workspace Admins** 與工作區建立關聯

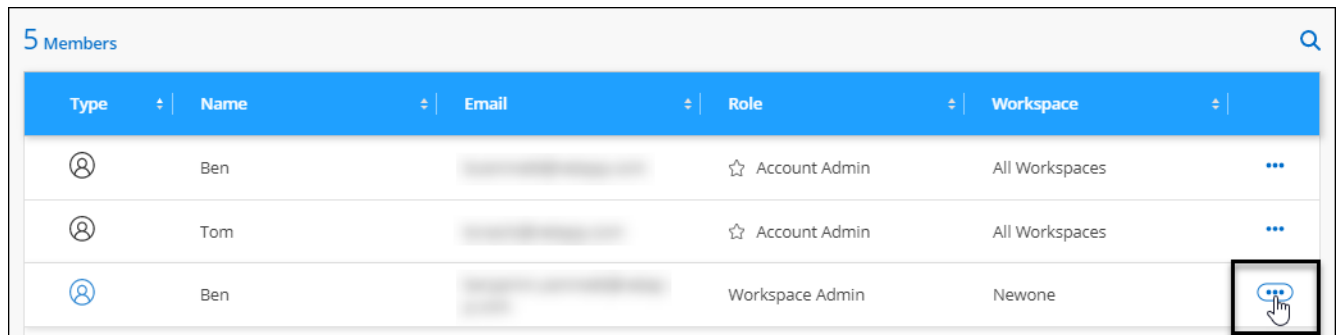
您可以隨時將 Workspace Admins 與其他工作區建立關聯。建立使用者關聯可讓他們在該工作區中建立及檢視工作環境。

步驟

1. 從 Cloud Manager 頂端、按一下 * Account* 下拉式清單、然後按一下 * Manage Account* 。



2. 在「成員」索引標籤中、按一下對應使用者列中的動作功能表。



3. 按一下 * 管理工作區 * 。

4. 選取一或多個工作區、然後按一下「* 套用 *」。

只要 Connector 也與工作區相關聯、使用者就能從 Cloud Manager 存取這些工作區。

將Connectors與工作區建立關聯

您需要將 Connector 與工作空間建立關聯、讓 Workspace Admins 可以使用這些 Connectors 來建立 Cloud Volumes ONTAP 一套系統。

如果您只有帳戶管理員、則不需要將 Connector 與工作區建立關聯。根據預設、Account Admins 可存取 Cloud Manager 中的所有工作區。

"深入瞭解使用者、工作區和連接器"。

步驟

1. 從 Cloud Manager 頂端、按一下 * Account* 下拉式清單、然後按一下 * Manage Account* 。



2. 按一下 * Connector* 。
3. 針對您要建立關聯的連接器、按一下 * 管理工作區 * 。
4. 選取一或多個工作區、然後按一下「* 套用 *」。

Workspace 管理員現在可以使用這些連接器來建立 Cloud Volumes ONTAP 功能不一的系統。

接下來呢？

現在您已經設定好帳戶、您可以隨時移除使用者、管理工作區、連接器和訂閱、來管理帳戶。 ["瞭解如何管理您的帳戶"](#)。

設定連接器

深入瞭解連接器

在大多數情況下、帳戶管理員需要在雲端或內部部署網路中部署 *Connector* 。Connector 是Cloud Manager日常使用的重要元件。Connector可讓Cloud Manager管理公有雲環境中的資源與程序。

需要連接器時

需要連接器才能使用Cloud Manager中的許多功能和服務。

服務

- Amazon FSX提供ONTAP 功能完善的管理功能
- Amazon S3探索
- Azure Blob探索
- 雲端備份
- 雲端資料感測
- 雲端分層
- Cloud Volumes ONTAP
- 全域檔案快取

- Google Cloud Storage探索
- Kubernetes叢集
- 監控
- 內部部署 ONTAP 的叢集

下列服務需要*非_*連接器：

- 《數位顧問》 Active IQ
- Amazon FSX- ONTAP 用於建立工作環境、而Connector不需要建立工作環境、則需要建立及管理磁碟區、複寫資料、並將FSX與ONTAP NetApp雲端服務整合、例如Data Sense和Cloud Sync Sfor。
- Azure NetApp Files

雖然不需要連接器來設定和管理Azure NetApp Files 功能、但如果您想要使用Cloud Data Sense來掃描Azure NetApp Files 支援資料、則需要連接器。

- 適用於 Google Cloud Cloud Volumes Service
- Cloud Sync

數位錢包

在幾乎所有情況下、您都可以在沒有連接器的情況下、將授權新增至Digital Wallet。

連接器新增授權至Digital Wallet所需的唯一時間、是Cloud Volumes ONTAP 針對以節點為基礎的_授權。在這種情況下需要連接器、因為資料是取自Cloud Volumes ONTAP 安裝在效益分析系統上的授權。

支援的位置

下列位置支援連接器：

- Amazon Web Services
- Microsoft Azure
- Google Cloud
- 在您的內部環境中
- 不需存取網際網路、就能在內部部署

Azure部署注意事項

如果您在Azure中部署Connector、則該連接器應部署在Cloud Volumes ONTAP 其所管理的、或是所管理的各個系統所在的Azure區域 "[Azure區域配對](#)" 適用於整個系統。Cloud Volumes ONTAP這項需求可確保Cloud Volumes ONTAP Azure Private Link連線可用於連接至相關的儲存帳戶。"[瞭解Cloud Volumes ONTAP 解如何使用Azure Private Link](#)"。

Google Cloud部署注意事項

如果您想要在Cloud Volumes ONTAP Google Cloud中建立一個不完整的系統、那麼您也必須在Google Cloud上執行一個Connector。您無法使用在AWS、Azure或內部執行的Connector。

連接器應保持運作

連接器應隨時保持執行狀態。這對於您持續啟用的服務健全狀況和營運而言十分重要。

例如、連接器是Cloud Volumes ONTAP 運作過程中的關鍵要素。如果連接器關機、Cloud Volumes ONTAP 具有節點型授權的現象將會在與連接器失去通訊超過14天之後關閉。

如何建立連接器

「帳戶管理員Cloud Volumes ONTAP 」必須先建立連接器、工作區管理員才能建立運作環境、並使用上述任何其他服務。管理員可以透過多種方式建立Connector：

- 直接從 Cloud Manager （建議）
 - ["在 AWS 中建立"](#)
 - ["在 Azure 中建立"](#)
 - ["在 GCP 中建立"](#)
- 在您自己的Linux主機上手動安裝軟體
 - ["在可存取網際網路的主機上"](#)
 - ["在內部主機上、但無法存取網際網路"](#)
- 從雲端供應商的市場
 - ["AWS Marketplace"](#)
 - ["Azure Marketplace"](#)

Cloud Manager會在需要建立連接器以完成動作時提示您建立連接器。

權限

建立 Connector 需要特定權限、而且 Connector 執行個體本身需要另一組權限。

建立 Connector 的權限

從 Cloud Manager 建立 Connector 的使用者需要特定權限、才能在您選擇的雲端供應商中部署執行個體。Cloud Manager 會在您建立 Connector 時提醒您權限要求。

- ["檢視所需的AWS權限"](#)
- ["檢視必要的Azure權限"](#)
- ["檢視必要的Google Cloud權限"](#)

Connector 執行個體的權限

Connector 需要特定的雲端供應商權限、才能代表您執行作業。例如、部署及管理 Cloud Volumes ONTAP 功能。

當您直接從 Cloud Manager 建立 Connector 時、Cloud Manager 會以所需的權限來建立 Connector。您無需做任何事。

如果您是從 AWS Marketplace、Azure Marketplace 或手動安裝軟體來建立 Connector、則必須確保擁有適當

的權限。

- ["瞭解Connector如何使用AWS權限"](#)
- ["瞭解Connector如何使用Azure權限"](#)
- ["瞭解Connector如何使用Google Cloud權限"](#)

連接器升級

我們通常每個月更新Connector軟體、以引進新功能並改善穩定性。雖然Cloud Manager平台的大部分服務與功能都是透過SaaS型軟體提供、但其中幾項功能和功能則取決於Connector的版本。其中包括Cloud Volumes ONTAP 支援內部的支援、ONTAP 內部的支援、叢集管理、設定及說明。

只要有、Connector 就會自動將其軟體更新至最新版本 ["傳出網際網路存取"](#) 以取得軟體更新。

每個連接器的工作環境數量

Connector可在Cloud Manager中管理多個工作環境。單一Connector應管理的工作環境數量上限各不相同。這取決於工作環境的類型、磁碟區數量、所管理的容量、以及使用者數量。

如果您有大規模部署、請與NetApp代表合作調整環境規模。如果您在過程中遇到任何問題、請使用產品內對談與我們聯絡。

何時使用多個連接器

在某些情況下、您可能只需要一個連接器、但可能需要兩個以上的連接器。

以下是幾個範例：

- 您使用的是多雲端環境（AWS 和 Azure）、因此 AWS 中有一個連接器、Azure 中有另一個連接器。每個系統都能管理 Cloud Volumes ONTAP 在這些環境中執行的不實系統。
- 服務供應商可能會使用一個NetApp帳戶來為客戶提供服務、而使用另一個帳戶來為其中一個業務單位提供災難恢復。每個帳戶都會有個別的 Connectors。

使用具有相同工作環境的多個連接器

您可以同時使用多個連接器來管理工作環境、以便進行災難恢復。如果一個連接器故障、您可以切換至另一個連接器、立即管理工作環境。

若要設定此組態：

1. ["切換至另一個連接器"](#)
2. 探索現有的工作環境。
 - ["將現有Cloud Volumes ONTAP 的不適用系統新增至Cloud Manager"](#)
 - ["探索 ONTAP 叢集"](#)
3. 設定 ["容量管理模式"](#)

只有主連接器應設定為*自動模式*。如果您切換至另一個連接器以進行DR、則可視需要變更容量管理模式。

何時在連接器之間切換

當您建立第一個 Connector 時、Cloud Manager 會針對您所建立的每個額外工作環境、自動使用該 Connector。
。建立額外的 Connector 之後、您必須在兩者之間切換、以查看每個 Connector 專屬的工作環境。

["瞭解如何在連接器之間切換"](#)。

本機使用者介面

而您應該從執行幾乎所有的工作 ["SaaS 使用者介面"](#)、連接器上仍有本機使用者介面可供使用。如果您在無法存取網際網路的環境中安裝 Connector、以及需要從 Connector 本身執行的一些工作、而非 SaaS 介面、則需要使用此介面：

- ["設定 Proxy 伺服器"](#)
- 安裝修補程式（您通常會與 NetApp 人員一起安裝修補程式）
- 下載 AutoSupport 資訊（如有問題、通常由 NetApp 人員引導）

["瞭解如何存取本機 UI"](#)。

設定連接器的網路

設定您的網路、讓 Connector 能夠管理公有雲環境中的資源和程序。最重要的步驟是確保從網際網路存取各種端點。

此頁面上的資訊適用於連接器具有傳出網際網路存取的典型部署。



如果您的網路使用 Proxy 伺服器來進行所有與網際網路的通訊、您可以從「設定」頁面指定 Proxy 伺服器。請參閱 ["將 Connector 設定為使用 Proxy 伺服器"](#)。

連線至目標網路

連接器需要網路連線至您所建立的工作環境類型以及您打算啟用的服務。

例如、如果您在公司網路中安裝 Connector、則必須設定 VPN 連線至 VPC 或 vnet、以便在其中啟動 Cloud Volumes ONTAP 更新。

可能與172範圍內的IP位址發生衝突

Cloud Manager部署連接器時、會有兩個介面、其中IP位址介於172.17.0.0/16和172.18.0.0/16範圍內。

如果您的網路已設定具有上述任一範圍的子網路、則Cloud Manager可能會發生連線失敗。例如ONTAP、在Cloud Manager中探索內部的功能不全的叢集可能會失敗。

請參閱知識庫文章 ["Cloud Manager Connector IP與現有網路發生衝突"](#) 如需如何變更連接器介面的IP位址的指示。

傳出網際網路存取

連接器需要外傳網際網路存取。

端點來管理公有雲環境中的資源

連接器需要存取傳出網際網路、才能管理公有雲環境中的資源和程序。

端點	目的
https://support.netapp.com	以取得授權資訊、並將AutoSupport 資訊傳送給NetApp支援部門。
https://*.cloudmanager.cloud.netapp.com	在Cloud Manager中提供SaaS功能與服務。
https://cloudmanagerinfraproduct.azurecr.io https://*.blob.core.windows.net	升級Connector及其Docker元件。

端點以在 **Linux** 主機上安裝 **Connector**

您可以選擇在自己的 Linux 主機上手動安裝 Connector 軟體。如果您這麼做、則 Connector 安裝程式必須在安裝過程中存取下列 URL：

- <https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm>
- <https://s3.amazonaws.com/aws-cli/awscli-bundle.zip>
- https://*.blob.core.windows.net或<https://hub.docker.com>

主機可能會在安裝期間嘗試更新作業系統套件。主機可聯絡不同的鏡射站台、以取得這些 OS 套件。

連接埠和安全性群組

除非您啟動連接器、否則不會有傳入流量進入連接器。HTTP 和 HTTPS 可存取 "本機 UI"、在極少數情況下使用。只有當您需要連線至主機進行疑難排解時、才需要 SSH。

AWS 中 Connector 的規則

Connector 的安全性群組需要傳入和傳出規則。

傳入規則

傳輸協定	連接埠	目的
SSH	22	提供對 Connector 主機的 SSH 存取權
HTTP	80	提供從用戶端 Web 瀏覽器到本機使用者介面的 HTTP 存取
HTTPS	443..	提供HTTPS存取、從用戶端網頁瀏覽器存取本機使用者介面、以及從Cloud Data Sense 執行個體連線
TCP	3128	如果您的AWS網路不使用NAT或Proxy、則可提供Cloud Data Sense執行個體以存取網際網路
TCP	9060	提供啟用和使用Cloud Data Sense的能力（僅適用於GovCloud部署）

傳出規則

Connector 的預先定義安全性群組會開啟所有傳出流量。如果可以接受、請遵循基本的傳出規則。如果您需要更嚴格的規則、請使用進階的傳出規則。

基本傳出規則

Connector 的預先定義安全性群組包括下列傳出規則。

傳輸協定	連接埠	目的
所有 TCP	全部	所有傳出流量
所有的 udp	全部	所有傳出流量

進階傳出規則

如果您需要嚴格的傳出流量規則、可以使用下列資訊、僅開啟連接器傳出通訊所需的連接埠。



來源 IP 位址為 Connector 主機。

服務	傳輸協定	連接埠	目的地	目的
API 呼叫與 AutoSupport 功能	HTTPS	443..	傳出網際網路和 ONTAP 叢集管理 LIF	API會呼叫AWS和ONTAP VMware、Cloud Data Sense、勒索軟體服務、並將AutoSupport 這些訊息傳送給NetApp
API 呼叫	TCP	3000	充當HA中介者ONTAP	與ONTAP NetApp HA中介人通訊
	TCP	8088	備份至 S3	API 呼叫備份至 S3
DNS	UDP	53.	DNS	用於 Cloud Manager 的 DNS 解析

Azure 中的 Connector 規則

Connector 的安全性群組需要傳入和傳出規則。

傳入規則

傳輸協定	連接埠	目的
SSH	22	提供對 Connector 主機的 SSH 存取權
HTTP	80	提供從用戶端 Web 瀏覽器到本機使用者介面的 HTTP 存取
HTTPS	443..	提供HTTPS存取、從用戶端網頁瀏覽器存取本機使用者介面、以及從Cloud Data Sense執行個體連線
TCP	9060	提供啟用和使用Cloud Data Sense 的能力（僅適用於政府雲端部署）

傳出規則

Connector 的預先定義安全性群組會開啟所有傳出流量。如果可以接受、請遵循基本的傳出規則。如果您需要更嚴格的規則、請使用進階的傳出規則。

基本傳出規則

Connector 的預先定義安全性群組包括下列傳出規則。

傳輸協定	連接埠	目的
所有 TCP	全部	所有傳出流量
所有的 udp	全部	所有傳出流量

進階傳出規則

如果您需要嚴格的傳出流量規則、可以使用下列資訊、僅開啟連接器傳出通訊所需的連接埠。



來源 IP 位址為 Connector 主機。

服務	傳輸協定	連接埠	目的地	目的
API 呼叫與 AutoSupport 功能	HTTPS	443..	傳出網際網路和 ONTAP 叢集管理 LIF	API會呼叫AWS和ONTAP VMware、Cloud Data Sense、勒索軟體服務、並將AutoSupport 這些訊息傳送給NetApp
DNS	UDP	53.	DNS	用於 Cloud Manager 的 DNS 解析

GCP 中的 Connector 規則

連接器的防火牆規則需要傳入和傳出規則。

傳入規則

傳輸協定	連接埠	目的
SSH	22	提供對 Connector 主機的 SSH 存取權
HTTP	80	提供從用戶端 Web 瀏覽器到本機使用者介面的 HTTP 存取
HTTPS	443..	提供 HTTPS 存取、從用戶端網頁瀏覽器存取本機使用者介面

傳出規則

連接器的預先定義防火牆規則會開啟所有傳出流量。如果可以接受、請遵循基本的傳出規則。如果您需要更嚴格的規則、請使用進階的傳出規則。

基本傳出規則

Connector 的預先定義防火牆規則包括下列傳出規則。

傳輸協定	連接埠	目的
所有 TCP	全部	所有傳出流量
所有的 udp	全部	所有傳出流量

進階傳出規則

如果您需要嚴格的傳出流量規則、可以使用下列資訊、僅開啟連接器傳出通訊所需的連接埠。



來源 IP 位址為 Connector 主機。

服務	傳輸協定	連接埠	目的地	目的
API 呼叫與 AutoSupport 功能	HTTPS	443..	傳出網際網路和 ONTAP 叢集管理 LIF	API會呼叫GCP和ONTAP VMware、Cloud Data Sense、勒索軟體服務、並將AutoSupport 此訊息傳送給NetApp
DNS	UDP	53.	DNS	用於 Cloud Manager 的 DNS 解析

內部連接器的連接埠

在內部部署的Linux主機上手動安裝Connector時、會使用下列_inbound連接埠。

這些傳入規則適用於內部部署連接器的兩種部署模式：安裝時可存取網際網路、或是無法存取網際網路。

傳輸協定	連接埠	目的
HTTP	80	提供從用戶端 Web 瀏覽器到本機使用者介面的 HTTP 存取
HTTPS	443..	提供 HTTPS 存取、從用戶端網頁瀏覽器存取本機使用者介面

從Cloud Manager在AWS中建立連接器

客戶管理員必須先部署 *Connector*、才能使用大多數 Cloud Manager 功能。Connector 可讓 Cloud Manager 管理公有雲環境中的資源與程序。["瞭解何時需要連接器"](#)。

本頁說明如何直接從 Cloud Manager 在 AWS 中建立 Connector。["瞭解部署Connector的其他方法"](#)。

這些步驟必須由具有「帳戶管理」角色的使用者完成。工作區管理員無法建立 Connector。

設定AWS驗證

Cloud Manager必須先與AWS驗證、才能在VPC中部署Connector執行個體。您可以選擇下列其中一種驗證方法

:

- 讓Cloud Manager承擔具備所需權限的IAM角色
- 為具有所需權限的IAM使用者提供AWS存取金鑰和秘密金鑰

無論使用哪一個選項、您都必須先建立包含所需權限的IAM原則。

建立IAM原則

此原則僅包含從Cloud Manager在AWS中啟動Connector執行個體所需的權限。請勿在其他情況下使用此原則。

Cloud Manager建立Connector時、會套用一組新的權限至Connector執行個體、讓Connector能夠管理公有雲環境中的資源。

步驟

1. 前往AWS IAM主控台。
2. 按一下*原則>建立原則*。
3. 按一下「* JSON*」。
4. 複製並貼上下列原則：

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "iam:CreateRole",
      "iam>DeleteRole",
      "iam:PutRolePolicy",
      "iam:CreateInstanceProfile",
      "iam>DeleteRolePolicy",
      "iam:AddRoleToInstanceProfile",
      "iam:RemoveRoleFromInstanceProfile",
      "iam>DeleteInstanceProfile",
      "iam:PassRole",
      "ec2:DescribeInstanceStatus",
      "ec2:RunInstances",
      "ec2:ModifyInstanceAttribute",
      "ec2:CreateSecurityGroup",
      "ec2>DeleteSecurityGroup",
      "ec2:DescribeSecurityGroups",
      "ec2:RevokeSecurityGroupEgress",
      "ec2:AuthorizeSecurityGroupEgress",
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:RevokeSecurityGroupIngress",
      "ec2:CreateNetworkInterface",
      "ec2:DescribeNetworkInterfaces",
```

```

        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DescribeInstances",
        "ec2:CreateTags",
        "ec2:DescribeImages",
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "iam:GetRole",
        "iam:TagRole",
        "iam:ListRoles",
        "kms:ListAliases"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:TerminateInstances"
    ],
    "Condition": {
        "StringLike": {
            "ec2:ResourceTag/OCCMInstance": "*"
        }
    },
    "Resource": [
        "arn:aws:ec2:*:*:instance/*"
    ]
}
]
}

```

5. 如有需要、請按* Next*並新增標記。
6. 單擊*下一步*並輸入名稱和說明。
7. 按一下「建立原則」。

將原則附加至Cloud Manager可以承擔的IAM角色、或附加至IAM使用者。

設定IAM角色

設定Cloud Manager可承擔的IAM角色、以便在AWS中部署Connector。

步驟

1. 前往目標帳戶中的AWS IAM主控台。
2. 在「存取管理」下、按一下*「角色」>「建立角色」*、然後依照步驟建立角色。

請務必執行下列動作：

- 在*信任的實體類型*下、選取* AWS帳戶*。
 - 選取*其他AWS帳戶*、然後輸入Cloud Manager SaaS帳戶的ID：952013314444。
 - 選取您在上一節中建立的原則。
3. 建立角色之後、請複製角色ARN、以便在建立Connector時將其貼到Cloud Manager中。

IAM角色現在擁有所需的權限。

設定IAM使用者的權限

建立Connector時、您可以為具有部署Connector執行個體所需權限的IAM使用者、提供AWS存取金鑰和秘密金鑰。

步驟

1. 從AWS IAM主控台按一下*使用者*、然後選取使用者名稱。
2. 按一下*「新增權限」>「直接附加現有原則」*。
3. 選取您建立的原則。
4. 按一下「下一步」、然後按一下「新增權限」。
5. 確保您有權存取IAM使用者的存取金鑰和秘密金鑰。

AWS 使用者現在擁有從 Cloud Manager 建立 Connector 所需的權限。當 Cloud Manager 提示您時、您需要為此使用者指定 AWS 存取金鑰。

建立連接器

Cloud Manager 可讓您直接從 AWS 使用者介面建立連接器。

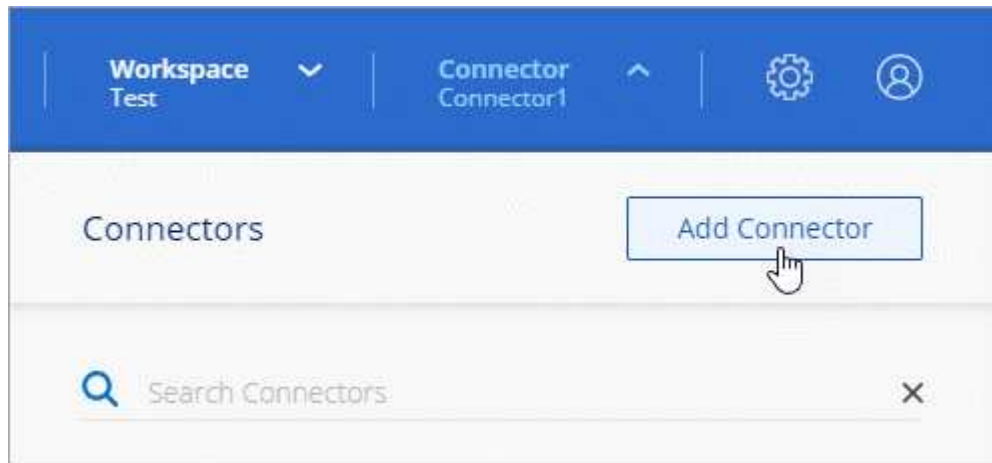
您需要的是 **#8217** ；需要的是什麼

- AWS驗證方法：Cloud Manager可以承擔的IAM角色ARN、或IAM使用者的AWS存取金鑰和秘密金鑰。
- 您選擇的 AWS 區域中的 VPC 、子網路和金鑰組。
- 如果您不想讓Cloud Manager自動為Connector建立IAM角色、則必須自行建立 ["使用此頁面上的原則"](#)。

這些是Connector管理公有雲環境中資源所需的權限。這是一組不同於您所提供的建立Connector執行個體的權限。

步驟

1. 如果您要建立第一個工作環境、請按一下 * 新增工作環境 *、然後依照提示進行。否則、請按一下「 * Connector*」下拉式清單、然後選取「 * 新增 Connector*」。



2. 選擇 * Amazon Web Services* 做為您的雲端供應商、然後按一下 * 繼續*。

請記住、連接器必須連線至您所建立的工作環境類型、以及您計畫啟用的服務。

["深入瞭解連接器的網路需求"](#)。

3. 依照精靈中的步驟建立連接器：

- 準備好：檢視您需要的內容。
- * AWS 認證資料*：指定您的AWS區域、然後選擇驗證方法、這是Cloud Manager可以承擔的IAM角色、或是AWS存取金鑰和秘密金鑰。



如果選擇 * 假定角色*、您可以從連接器部署精靈建立第一組認證。必須從「認證資料」頁面建立任何其他一組認證資料。然後、精靈會在下拉式清單中提供這些工具。 ["瞭解如何新增其他認證資料"](#)。

- 詳細資料：提供連接器的詳細資料。
 - 輸入執行個體的名稱。
 - 新增自訂標記（中繼資料）至執行個體。
 - 選擇您要Cloud Manager建立具有所需權限的新角色、或是要選取您所設定的現有角色 ["必要的權限"](#)。
 - 選擇是否要加密Connector的EBS磁碟。您可以選擇使用預設加密金鑰或使用自訂金鑰。
- 網路：指定執行個體的VPC、子網路和金鑰配對、選擇是否啟用公用IP位址、以及選擇性地指定Proxy組態。
- * 安全性群組 *：選擇是建立新的安全性群組、還是選擇允許傳入 HTTP、HTTPS 及 SSH 存取的現有安全性群組。



除非您啟動連接器、否則不會有傳入流量進入連接器。HTTP 和 HTTPS 可存取 ["本機 UI"](#)、在極少數情況下使用。只有當您需要連線至主機進行疑難排解時、才需要 SSH。

。審查：請檢閱您的選擇、確認您的設定正確無誤。

4. 按一下「* 新增 *」。

執行個體應在 7 分鐘內就緒。您應該留在頁面上、直到程序完成為止。

您需要將 Connector 與工作空間建立關聯、讓 Workspace Admins 可以使用這些 Connectors 來建立 Cloud Volumes ONTAP 一套系統。如果您只有帳戶管理員、則不需要將 Connector 與工作區建立關聯。根據預設、Account Admins 可存取 Cloud Manager 中的所有工作區。"[深入瞭解](#)"。

如果您在建立Connector的同一個AWS帳戶中有Amazon S3儲存區、則會在畫版上自動顯示Amazon S3工作環境。"[深入瞭解如何運用此工作環境](#)"。

從Cloud Manager在Azure中建立Connector

客戶管理員必須先部署 *Connector*、才能使用大多數 Cloud Manager 功能。Connector 可讓 Cloud Manager 管理公有雲環境中的資源與程序。"[瞭解何時需要連接器](#)"。

本頁說明如何直接從 Cloud Manager 在 Azure 中建立 Connector。"[瞭解部署Connector的其他方法](#)"。

這些步驟必須由具有「帳戶管理」角色的使用者完成。工作區管理員無法建立 Connector。

總覽

若要部署Connector、您必須提供Cloud Manager登入資訊、並具備在Azure中建立Connector VM所需的權限。

您有兩種選擇：

1. 出現提示時、請使用您的Microsoft帳戶登入。此帳戶必須具有特定的Azure權限。這是預設選項。

[請依照下列步驟開始使用](#)。

2. 提供Azure AD服務負責人的詳細資料。此服務主體也需要特定權限。

[請依照下列步驟開始使用](#)。

Azure地區的相關注意事項

連接器應部署在Cloud Volumes ONTAP 其所管理的或所管理的各個系統所在的Azure區域 "[Azure區域配對](#)" 適用於整個系統。Cloud Volumes ONTAP這項需求可確保Cloud Volumes ONTAP Azure Private Link連線可用於連接至相關的儲存帳戶。"[瞭Cloud Volumes ONTAP 解如何使用Azure Private Link](#)"。

使用您的Azure帳戶建立Connector

在Azure中建立Connector的預設方法是在出現提示時、使用Azure帳戶登入。登入表單由Microsoft擁有及託管。您的認證資料不會提供給 NetApp。

設定Azure帳戶的權限

在您從 Cloud Manager 部署 Connector 之前、您必須確保 Azure 帳戶擁有正確的權限。

1. 複製Azure中新自訂角色所需的權限、並將其儲存在Json檔案中。



此原則僅包含從Cloud Manager在Azure中啟動Connector VM所需的權限。請勿在其他情況下使用此原則。Cloud Manager建立Connector時、會套用新的一組權限至Connector VM、讓Connector能夠管理公有雲環境中的資源。

```
{
  "Name": "Azure SetupAsService",
  "Actions": [
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/disks/read",
    "Microsoft.Compute/disks/write",
    "Microsoft.Compute/locations/operations/read",
    "Microsoft.Compute/operations/read",
    "Microsoft.Compute/virtualMachines/instanceView/read",
    "Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/write",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Compute/virtualMachines/extensions/write",
    "Microsoft.Compute/virtualMachines/extensions/read",
    "Microsoft.Compute/availabilitySets/read",
    "Microsoft.Network/locations/operationResults/read",
    "Microsoft.Network/locations/operations/read",
    "Microsoft.Network/networkInterfaces/join/action",
    "Microsoft.Network/networkInterfaces/read",
    "Microsoft.Network/networkInterfaces/write",
    "Microsoft.Network/networkInterfaces/delete",
    "Microsoft.Network/networkSecurityGroups/join/action",
    "Microsoft.Network/networkSecurityGroups/read",
    "Microsoft.Network/networkSecurityGroups/write",

    "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Network/virtualNetworks/subnets/join/action",
    "Microsoft.Network/virtualNetworks/subnets/read",

    "Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
    "Microsoft.Network/virtualNetworks/virtualMachines/read",
    "Microsoft.Network/publicIPAddresses/write",
    "Microsoft.Network/publicIPAddresses/read",
    "Microsoft.Network/publicIPAddresses/delete",
    "Microsoft.Network/networkSecurityGroups/securityRules/read",
    "Microsoft.Network/networkSecurityGroups/securityRules/write",
    "Microsoft.Network/networkSecurityGroups/securityRules/delete",
    "Microsoft.Network/publicIPAddresses/join/action",
```



```

"Microsoft.Network/locations/virtualNetworkAvailableEndpointServices/read",
    "Microsoft.Network/networkInterfaces/ipConfigurations/read",
    "Microsoft.Resources/deployments/operations/read",
    "Microsoft.Resources/deployments/read",
    "Microsoft.Resources/deployments/delete",
    "Microsoft.Resources/deployments/cancel/action",
    "Microsoft.Resources/deployments/validate/action",
    "Microsoft.Resources/resources/read",
    "Microsoft.Resources/subscriptions/operationresults/read",
    "Microsoft.Resources/subscriptions/resourceGroups/delete",
    "Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
    "Microsoft.Resources/subscriptions/resourceGroups/write",
    "Microsoft.Authorization/roleDefinitions/write",
    "Microsoft.Authorization/roleAssignments/write",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write",
    "Microsoft.Network/networkSecurityGroups/delete",
    "Microsoft.Storage/storageAccounts/delete",
    "Microsoft.Storage/storageAccounts/write",
    "Microsoft.Resources/deployments/write",
    "Microsoft.Resources/deployments/operationStatuses/read",
    "Microsoft.Authorization/roleAssignments/read"
],
"NotActions": [],
"AssignableScopes": [],
"Description": "Azure SetupAsService",
"IsCustom": "true"
}

```

2. 將您的Azure訂閱ID新增至可指派的範圍、以修改Json。

◦ 範例 *

```

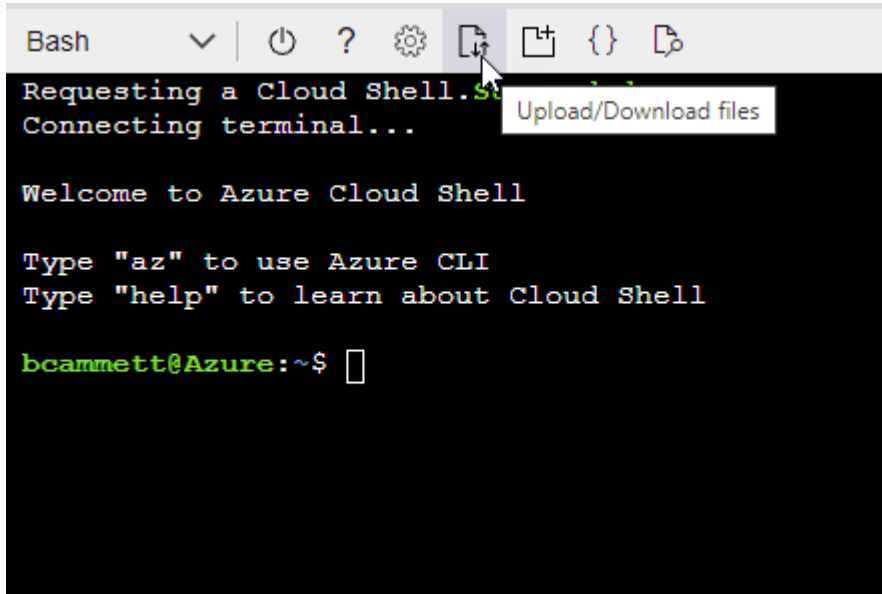
"AssignableScopes": [
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz"
],

```

3. 使用 Json 檔案在 Azure 中建立自訂角色。

下列步驟說明如何在 Azure Cloud Shell 中使用 Bash 建立角色。

- a. 開始 "Azure Cloud Shell" 並選擇 Bash 環境。
- b. 上傳 Json 檔案。



- c. 輸入下列 Azure CLI 命令：

```
az role definition create --role-definition  
Policy_for_Setup_As_Service_Azure.json
```

您現在應該擁有名為 *Azure Setup AsService* 的自訂角色。

4. 將角色指派給將從 Cloud Manager 部署 Connector 的使用者：

- a. 開啟 * 訂閱 * 服務、然後選取使用者的訂閱。
- b. 按一下 * 存取控制 (IAM) *。
- c. 按一下「* 新增 * > * 新增角色指派 *」、然後新增權限：
 - 選取「* Azure Setup AsService*」角色、然後按一下「* Next*」。



Azure Setup AsService 是 Azure 的 Connector 部署原則中提供的預設名稱。如果您為角色選擇不同的名稱、請改為選取該名稱。

- 保留 * 選取「使用者」、「群組」或「服務主體」*。
- 按一下 * 選取成員 *、選擇您的使用者帳戶、然後按一下 * 選取 *。
- 單擊 * 下一步 *。
- 按一下「檢閱+指派」。

Azure 使用者現在擁有從 Cloud Manager 部署 Connector 所需的權限。

使用您的**Azure**帳戶登入以建立**Connector**

Cloud Manager 可讓您直接從 Azure 的使用者介面建立連接器。

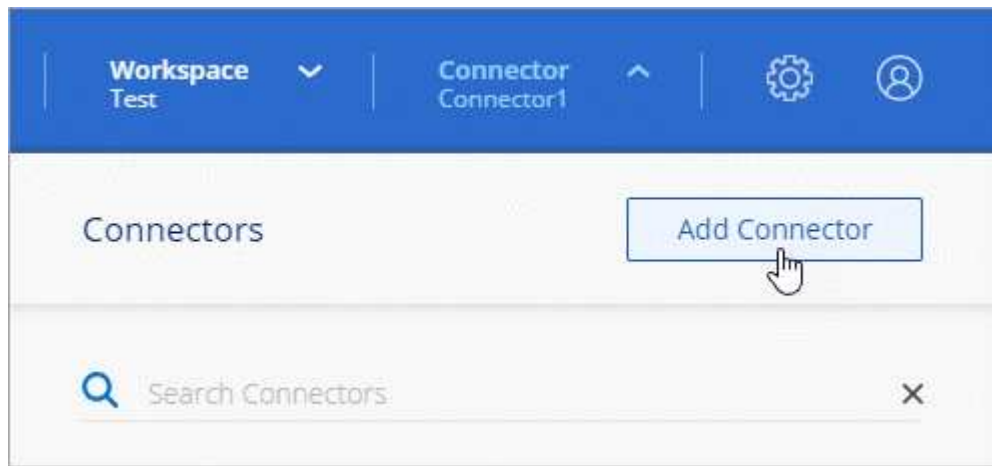
您需要的是 **#8217** ；需要的是什麼

- Azure 訂閱。
- 您所選擇的 Azure 區域中的 Vnet 和子網路。
- 如果您不想讓Cloud Manager自動為Connector建立Azure角色、則必須自行建立 "[使用此頁面上的原則](#)"。

這些權限適用於Connector執行個體本身。這是一組不同於您先前設定的權限、只要部署Connector即可。

步驟

1. 如果您要建立第一個工作環境、請按一下 * 新增工作環境 *、然後依照提示進行。否則、請按一下「 * Connector*」下拉式清單、然後選取「 * 新增 Connector*」。



2. 選擇 * Microsoft Azure * 作為雲端供應商。

請記住、連接器必須連線至您所建立的工作環境類型、以及您計畫啟用的服務。

["深入瞭解連接器的網路需求"](#)。

3. 依照精靈中的步驟建立連接器：

- 準備好：檢視您需要的內容、然後按一下*下一步*。
- 如果出現提示、請登入您的 Microsoft 帳戶、該帳戶應有建立虛擬機器所需的權限。

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



如果您已經登入 Azure 帳戶、Cloud Manager 將自動使用該帳戶。如果您有多個帳戶、則可能需要先登出、以確保您使用的是正確的帳戶。

- * VM驗證*：選擇Azure訂閱、位置、新資源群組或現有資源群組、然後選擇驗證方法。
- 詳細資料：輸入執行個體的名稱、指定標記、然後選擇是否要Cloud Manager建立具有必要權限的新角

色、或是要選取您設定的現有角色 ["必要的權限"](#)。

請注意、您可以選擇與此角色相關的訂閱。您選擇的每個訂閱都會提供Connector權限、讓他們在Cloud Volumes ONTAP 這些訂閱中部署功能。

- * 網路 * : 選擇 Vnet 和子網路、是否啟用公用 IP 位址、以及是否指定 Proxy 組態 (選用)。
- * 安全性群組 * : 選擇是建立新的安全性群組、還是選擇允許傳入 HTTP、HTTPS 及 SSH 存取的現有安全性群組。



除非您啟動連接器、否則不會有傳入流量進入連接器。HTTP 和 HTTPS 可存取 ["本機 UI"](#)、在極少數情況下使用。只有當您需要連線至主機進行疑難排解時、才需要 SSH。

- 審查: 請檢閱您的選擇、確認您的設定正確無誤。

4. 按一下「* 新增 *」。

虛擬機器應在約 7 分鐘內就緒。您應該留在頁面上、直到程序完成為止。

您需要將 Connector 與工作空間建立關聯、讓 Workspace Admins 可以使用這些 Connectors 來建立 Cloud Volumes ONTAP 一套系統。如果您只有帳戶管理員、則不需要將 Connector 與工作區建立關聯。根據預設、Account Admins 可存取 Cloud Manager 中的所有工作區。 ["深入瞭解"](#)。

如果您在建立Connector的同一個Azure帳戶中擁有Azure Blob儲存設備、您會看到Azure Blob工作環境會自動出現在Canvas。 ["深入瞭解如何運用此工作環境"](#)。

使用服務主體建立連接器

您不需要使用Azure帳戶登入、也可以選擇向Cloud Manager提供具備必要權限之Azure服務主體的認證資料。

使用服務主體授予 **Azure** 權限

在Azure Active Directory中建立及設定服務主體、並取得Cloud Manager所需的Azure認證資料、以授予在Azure中部署Connector所需的權限。

步驟

1. [\[Create an Azure Active Directory application\]](#)。
2. [\[Assign the application to a role\]](#)。
3. [\[Add Windows Azure Service Management API permissions\]](#)。
4. [\[Get the application ID and directory ID\]](#)。
5. [\[Create a client secret\]](#)。

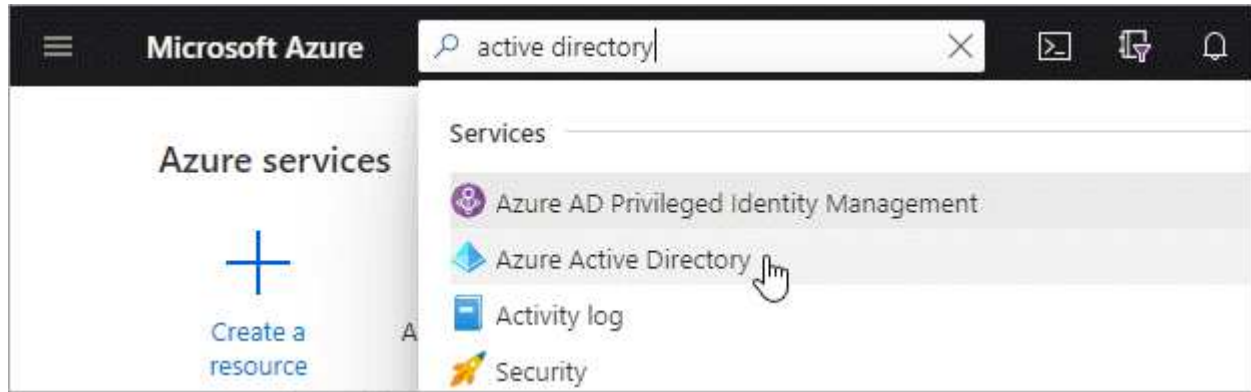
建立 **Azure Active Directory** 應用程式

建立Azure Active Directory (AD) 應用程式與服務主體、讓Cloud Manager可用來部署Connector。

您必須在 Azure 中擁有適當權限、才能建立 Active Directory 應用程式、並將應用程式指派給角色。如需詳細資訊、請參閱 ["Microsoft Azure 說明文件：必要權限"](#)。

步驟

1. 從 Azure 入口網站開啟 * Azure Active Directory * 服務。



2. 在功能表中、按一下 * 應用程式註冊 * 。
3. 按一下「* 新登錄 *」。
4. 指定應用程式的詳細資料：
 - * 名稱 *：輸入應用程式的名稱。
 - * 帳戶類型 *：選取帳戶類型（任何帳戶類型都可與 Cloud Manager 搭配使用）。
 - 重新導向URI：您可以將此欄位保留空白。
5. 按一下 * 註冊 * 。

您已建立 AD 應用程式和服務主體。

將應用程式指派給角色

您必須將服務主體繫結至您打算部署Connector的Azure訂閱、並將其指派為自訂的「Azure Setup AsService」角色。

步驟

1. 複製Azure中新自訂角色所需的權限、並將其儲存在Json檔案中。



此原則僅包含從Cloud Manager在Azure中啟動Connector VM所需的權限。請勿在其他情況下使用此原則。Cloud Manager建立Connector時、會套用新的一組權限至Connector VM、讓Connector能夠管理公有雲環境中的資源。

```
{
  "Name": "Azure SetupAsService",
  "Actions": [
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/disks/read",
    "Microsoft.Compute/disks/write",
    "Microsoft.Compute/locations/operations/read",
    "Microsoft.Compute/operations/read",
    "Microsoft.Compute/virtualMachines/instanceView/read",
    "Microsoft.Compute/virtualMachines/read",
```

```

"Microsoft.Compute/virtualMachines/write",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Compute/virtualMachines/extensions/read",
"Microsoft.Compute/availabilitySets/read",
"Microsoft.Network/locations/operationResults/read",
"Microsoft.Network/locations/operations/read",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
"Microsoft.Network/virtualNetworks/virtualMachines/read",
"Microsoft.Network/publicIPAddresses/write",
"Microsoft.Network/publicIPAddresses/read",
"Microsoft.Network/publicIPAddresses/delete",
"Microsoft.Network/networkSecurityGroups/securityRules/read",
"Microsoft.Network/networkSecurityGroups/securityRules/write",
"Microsoft.Network/networkSecurityGroups/securityRules/delete",
"Microsoft.Network/publicIPAddresses/join/action",

"Microsoft.Network/locations/virtualNetworkAvailableEndpointServices/read",
"Microsoft.Network/networkInterfaces/ipConfigurations/read",
"Microsoft.Resources/deployments/operations/read",
"Microsoft.Resources/deployments/read",
"Microsoft.Resources/deployments/delete",
"Microsoft.Resources/deployments/cancel/action",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Resources/resources/read",
"Microsoft.Resources/subscriptions/operationresults/read",
"Microsoft.Resources/subscriptions/resourceGroups/delete",
"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Authorization/roleDefinitions/write",

```

```

        "Microsoft.Authorization/roleAssignments/write",

        "Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read",

        "Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write",
        "Microsoft.Network/networkSecurityGroups/delete",
        "Microsoft.Storage/storageAccounts/delete",
        "Microsoft.Storage/storageAccounts/write",
        "Microsoft.Resources/deployments/write",
        "Microsoft.Resources/deployments/operationStatuses/read",
        "Microsoft.Authorization/roleAssignments/read"
    ],
    "NotActions": [],
    "AssignableScopes": [],
    "Description": "Azure SetupAsService",
    "IsCustom": "true"
}

```

2. 將 Azure 訂閱 ID 新增至可指派的範圍、以修改 Json 檔案。

◦ 範例 *

```

"AssignableScopes": [
    "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
]

```

3. 使用 Json 檔案在 Azure 中建立自訂角色。

下列步驟說明如何在 Azure Cloud Shell 中使用 Bash 建立角色。

- a. 開始 "Azure Cloud Shell" 並選擇 Bash 環境。
- b. 上傳 Json 檔案。



c. 輸入下列Azure CLI命令：

```
az role definition create --role-definition  
Policy_for_Setup_As_Service_Azure.json
```

您現在應該擁有名為 *Azure Setup AsService* 的自訂角色。

4. 將應用程式指派給角色：

- a. 從 Azure 入口網站開啟 * 訂閱 * 服務。
- b. 選取訂閱。
- c. 按一下 * 存取控制（IAM） > 新增 > 新增角色指派 *。
- d. 在「角色」索引標籤中、選取「* Azure Setup AsService*」角色、然後按一下「下一步」。
- e. 在「成員」索引標籤中、完成下列步驟：
 - 保留*選取「使用者」、「群組」或「服務主體」*。
 - 按一下*選取成員*。

Add role assignment ...

Got feedback?

Role **Members** Review + assign

Selected role Cloud Manager Operator 3.9.12_B

Assign access to ☒ User, group, or service principal ☐ Managed identity

Members + [Select members](#)

- 搜尋應用程式名稱。

範例如下：

Select members X

Select ⓘ

test-service-principal

test-service-principal

- 選取應用程式、然後按一下*選取*。
- 單擊 * 下一步 *。
- a. 按一下「檢閱+指派」。

服務主體現在擁有部署Connector所需的Azure權限。

新增 **Windows Azure Service Management API** 權限

服務主體必須具有「Windows Azure Service Management API」權限。

步驟

1. 在 * Azure Active Directory * 服務中、按一下 * 應用程式註冊 *、然後選取應用程式。
2. 按一下「* API 權限 > 新增權限 *」。


3. 在「* Microsoft API*」下、選取「* Azure 服務管理 *」。













Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

 Azure Batch Schedule large-scale parallel and HPC applications in the cloud	 Azure Data Catalog Programmatic access to Data Catalog resources to register, annotate and search data assets	 Azure Data Explorer Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions
 Azure Data Lake Access to storage and compute for big data analytic scenarios	 Azure DevOps Integrate with Azure DevOps and Azure DevOps server	 Azure Import/Export Programmatic control of import/export jobs
 Azure Key Vault Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults	 Azure Rights Management Services Allow validated users to read and write protected content	 Azure Service Management Programmatic access to much of the functionality available through the Azure portal
 Azure Storage Secure, massively scalable object and data lake storage for unstructured and semi-structured data	 Customer Insights Create profile and interaction models for your products	 Data Export Service for Microsoft Dynamics 365 Export data from Microsoft Dynamics CRM organization to an external destination

4. 按一下「* 以組織使用者身分存取 Azure 服務管理 *」、然後按一下「* 新增權限 *」。

Request API permissions

[← All APIs](#)



Azure Service Management

<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED



user_impersonation

Access Azure Service Management as organization users (preview) ⓘ

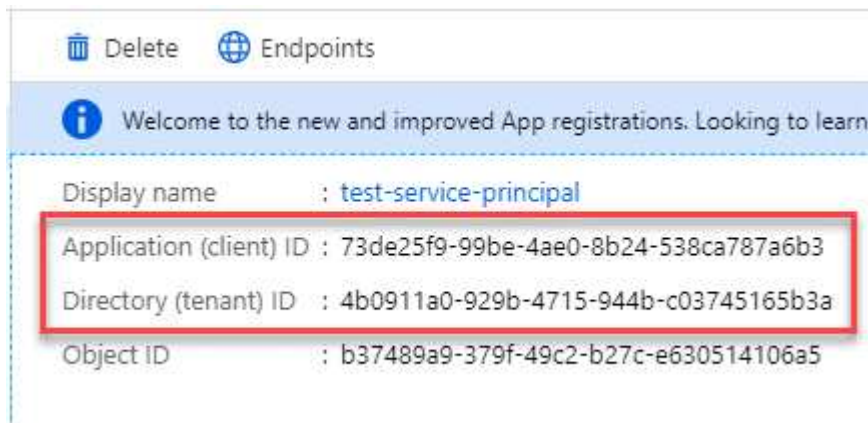
-

取得應用程式 ID 和目錄 ID

從Cloud Manager建立Connector時、您需要提供應用程式的應用程式（用戶端）ID和目錄（租戶）ID。Cloud Manager 會使用 ID 以程式設計方式登入。

步驟

1. 在 * Azure Active Directory * 服務中、按一下 * 應用程式註冊 * 、然後選取應用程式。
2. 複製 * 應用程式（用戶端）ID* 和 * 目錄（租戶）ID* 。



建立用戶端機密

您需要建立用戶端機密、然後為 Cloud Manager 提供機密的價值、以便 Cloud Manager 使用它來驗證 Azure AD 。

步驟

1. 開啟 * Azure Active Directory * 服務。
2. 按一下 * 應用程式註冊 * 、然後選取您的應用程式。

3. 按一下 * 「憑證與機密」 > 「新用戶端機密」 * 。
4. 提供機密與持續時間的說明。
5. 按一下「 * 新增 * 」。
6. 複製用戶端機密的值。

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret		
DESCRIPTION	EXPIRES	VALUE
test secret	8/16/2020	*sZ1jSe2By:D*-ZR0V4NLfdAcY7:+0vA

Copy to clipboard

您的服務主體現在已設定完成、您應該已經複製應用程式（用戶端） ID 、目錄（租戶） ID 、以及用戶端機密的值。建立Connector時、您必須在Cloud Manager中輸入此資訊。

使用服務主體登入以建立Connector

Cloud Manager 可讓您直接從 Azure 的使用者介面建立連接器。

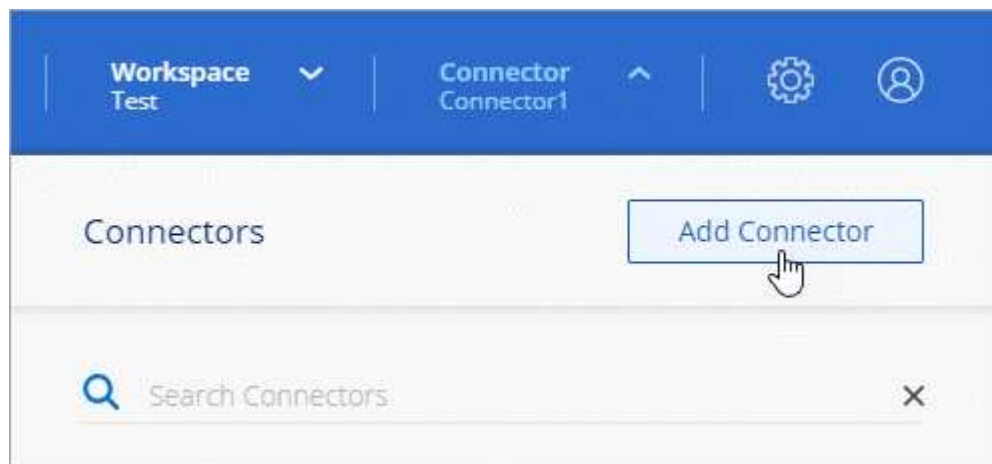
您需要的是 #8217 ；需要的是什麼

- Azure 訂閱。
- 您所選擇的 Azure 區域中的 Vnet 和子網路。
- 如果您不想讓Cloud Manager自動為Connector建立Azure角色、則必須自行建立 "[使用此頁面上的原則](#)"。

這些權限適用於Connector執行個體本身。這是一組不同於您先前設定的權限、只要部署Connector即可。

步驟

1. 如果您要建立第一個工作環境、請按一下 * 新增工作環境 * 、然後依照提示進行。否則、請按一下「 * Connector* 」下拉式清單、然後選取「 * 新增 Connector* 」。



2. 選擇 * Microsoft Azure * 作為雲端供應商。

請記住、連接器必須連線至您所建立的工作環境類型、以及您計畫啟用的服務。

"[深入瞭解連接器的網路需求](#)"。

3. 依照精靈中的步驟建立連接器：

- 準備就緒：按一下* Azure AD服務委託人*、然後輸入Azure Active Directory服務委託人的相關資訊、以授予必要的權限：
 - 應用程式（用戶端）ID：請參閱 [\[Get the application ID and directory ID\]](#)。
 - 目錄（租戶）ID：請參閱 [\[Get the application ID and directory ID\]](#)。
 - 用戶端機密：請參閱 [\[Create a client secret\]](#)。
- * VM驗證*：選擇Azure訂閱、位置、新資源群組或現有資源群組、然後選擇驗證方法。
- 詳細資料：輸入執行個體的名稱、指定標記、然後選擇是否要Cloud Manager建立具有必要權限的新角色、或是要選取您設定的現有角色 "[必要的權限](#)"。

請注意、您可以選擇與此角色相關的訂閱。您選擇的每個訂閱都會提供Connector權限、讓他們在Cloud Volumes ONTAP 這些訂閱中部署功能。

- * 網路 *：選擇 Vnet 和子網路、是否啟用公用 IP 位址、以及是否指定 Proxy 組態（選用）。
- * 安全性群組 *：選擇是建立新的安全性群組、還是選擇允許傳入 HTTP、HTTPS 及 SSH 存取的現有安全性群組。



除非您啟動連接器、否則不會有傳入流量進入連接器。HTTP 和 HTTPS 可存取 "[本機 UI](#)"、在極少數情況下使用。只有當您需要連線至主機進行疑難排解時、才需要 SSH。

- 審查：請檢閱您的選擇、確認您的設定正確無誤。

4. 按一下「* 新增 *」。

虛擬機器應在約 7 分鐘內就緒。您應該留在頁面上、直到程序完成為止。

您需要將 Connector 與工作空間建立關聯、讓 Workspace Admins 可以使用這些 Connectors 來建立 Cloud Volumes ONTAP 一套系統。如果您只有帳戶管理員、則不需要將 Connector 與工作區建立關聯。根據預設、Account Admins 可存取 Cloud Manager 中的所有工作區。"[深入瞭解](#)"。

如果您在建立Connector的同一個Azure帳戶中擁有Azure Blob儲存設備、您會看到Azure Blob工作環境會自動出現在Canvas。"[深入瞭解如何運用此工作環境](#)"。

從Cloud Manager在Google Cloud中建立Connector

客戶管理員必須先部署 *Connector*、才能使用大多數 Cloud Manager 功能。"[瞭解何時需要連接器](#)"。Connector 可讓 Cloud Manager 管理公有雲環境中的資源與程序。

本頁說明如何直接從Cloud Manager在Google Cloud中建立Connector。"[瞭解部署Connector的其他方法](#)"。

這些步驟必須由具有「帳戶管理」角色的使用者完成。工作區管理員無法建立 Connector。



當您建立第一個 Cloud Volumes ONTAP 運作環境時、如果您還沒有 Cloud Manager 、 Cloud Manager 會提示您建立 Connector 。

設定部署Connector的權限

在部署Connector之前、您必須確保Google Cloud帳戶擁有正確的權限。

步驟

1. "建立自訂角色" 包括下列權限：

```
title: Connector deployment policy
description: Permissions for the user who deploys the Connector from
Cloud Manager
stage: GA
includedPermissions:
- compute.disks.create
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.projects.get
- compute.regions.get
```

```
- compute.regions.list
- compute.subnetworks.get
- compute.subnetworks.list
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- resourcemanager.projects.get
- compute.instances.setServiceAccount
- iam.serviceAccounts.list
```

2. 將自訂角色附加至將從Cloud Manager部署Connector的使用者。

Google Cloud使用者現在擁有建立Connector所需的權限。

設定Connector的服務帳戶

需要有服務帳戶、才能讓Connector獲得管理Google Cloud資源所需的權限。建立此服務帳戶時、您會將其與Connector VM建立關聯。

服務帳戶的權限與您在上一節中設定的權限不同。

步驟

1. "建立自訂角色" 包括下列權限：

```
title: NetApp Cloud Manager
description: Permissions for the service account associated with the
Connector instance.
stage: GA
includedPermissions:
- iam.serviceAccounts.actAs
```


- `compute.regionBackendServices.create`
- `compute.regionBackendServices.get`
- `compute.regionBackendServices.list`
- `compute.networks.updatePolicy`
- `compute.backendServices.create`
- `compute.addresses.list`
- `compute.disks.create`
- `compute.disks.createSnapshot`
- `compute.disks.delete`
- `compute.disks.get`
- `compute.disks.list`
- `compute.disks.setLabels`
- `compute.disks.use`
- `compute.firewalls.create`
- `compute.firewalls.delete`
- `compute.firewalls.get`
- `compute.firewalls.list`
- `compute.globalOperations.get`
- `compute.images.get`
- `compute.images.getFromFamily`
- `compute.images.list`
- `compute.images.useReadOnly`
- `compute.instances.addAccessConfig`
- `compute.instances.attachDisk`
- `compute.instances.create`
- `compute.instances.delete`
- `compute.instances.detachDisk`
- `compute.instances.get`
- `compute.instances.getSerialPortOutput`
- `compute.instances.list`
- `compute.instances.setDeletionProtection`
- `compute.instances.setLabels`
- `compute.instances.setMachineType`
- `compute.instances.setMetadata`
- `compute.instances.setTags`
- `compute.instances.start`
- `compute.instances.stop`
- `compute.instances.updateDisplayDevice`
- `compute.machineTypes.get`
- `compute.networks.get`
- `compute.networks.list`
- `compute.projects.get`
- `compute.regions.get`
- `compute.regions.list`
- `compute.snapshots.create`
- `compute.snapshots.delete`

- compute.snapshots.get
- compute.snapshots.list
- compute.snapshots.setLabels
- compute.subnetworks.get
- compute.subnetworks.list
- compute.subnetworks.use
- compute.subnetworks.useExternalIp
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- compute.instances.setServiceAccount
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- logging.logEntries.list
- logging.privateLogEntries.list
- resourcemanager.projects.get
- storage.buckets.create
- storage.buckets.delete
- storage.buckets.get
- storage.buckets.list
- cloudkms.cryptoKeyVersions.useToEncrypt
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
- storage.buckets.update
- iam.serviceAccounts.getIamPolicy
- iam.serviceAccounts.list
- storage.objects.get
- storage.objects.list

2. "建立Google Cloud服務帳戶、並套用您剛建立的自訂角色"。

3. 如果您想要在 Cloud Volumes ONTAP 其他專案中部署 "將具有 Cloud Manager 角色的服務帳戶新增至該專案、以授予存取權"。您必須針對每個專案重複此步驟。

已設定Connector VM的服務帳戶。

共享VPC權限

如果您使用共享VPC將資源部署到服務專案、則需要下列權限。此表供參考、當IAM組態完成時、您的環境應反映權限表。

身分識別	建立者	裝載於	服務專案權限	主機專案權限	目的
用於部署Connector的Google帳戶	自訂	服務專案	<ul style="list-style-type: none"> "本節所提供的權限" 	<ul style="list-style-type: none"> compute.networkUser 	在服務專案中部署Connector
連接器服務帳戶	自訂	服務專案	<ul style="list-style-type: none"> "本節所提供的權限" 	<ul style="list-style-type: none"> compute.networkUser 部署manager.manager 	在Cloud Volumes ONTAP 服務專案中部署及維護功能與服務
服務帳戶Cloud Volumes ONTAP	自訂	服務專案	<ul style="list-style-type: none"> 儲存設備管理 成員：Cloud Manager服務帳戶：serviceAccount.user 	不適用	(選用) 用於資料分層和雲端備份
Google API服務代理程式	Google Cloud	服務專案	<ul style="list-style-type: none"> (預設) 編輯器 	<ul style="list-style-type: none"> compute.networkUser 	代表部署與Google Cloud API互動。允許Cloud Manager使用共享網路。
Google Compute Engine預設服務帳戶	Google Cloud	服務專案	<ul style="list-style-type: none"> (預設) 編輯器 	<ul style="list-style-type: none"> compute.networkUser 	代表部署部署部署部署Google Cloud執行個體和運算基礎架構。允許Cloud Manager使用共享網路。

附註：

1. 只有當您未將防火牆規則傳遞給部署、而且選擇讓Cloud Manager為您建立時、才需要在主機專案中部署manager.manager。如果未指定任何規則、Cloud Manager將在主機專案中建立包含VPC0防火牆規則的部署。
2. 只有當您未將防火牆規則傳遞至部署、並選擇讓Cloud Manager為您建立防火牆規則時、才需要使用Firewall.create和firewall.delete。這些權限位於Cloud Manager服務帳戶.yaml檔案中。如果您使用共用VPC部署HA配對、這些權限將用於建立VPC1、2和3的防火牆規則。對於所有其他部署、這些權限也會用於建立VPC0的規則。

3. 對於資料分層、分層服務帳戶必須在服務帳戶上具有serviceAccount.user角色、而不只是在專案層級。目前、如果您在專案層級指派serviceAccount.user、則當您使用getIAMPolicy查詢服務帳戶時、不會顯示權限。

啟用 **Google Cloud API**

部署 Connector 和 Cloud Volumes ONTAP 功能完善的應用程式需要多個 API 。

步驟

1. "在專案中啟用下列 [Google Cloud API](#)"。
 - Cloud Deployment Manager V2 API
 - 雲端記錄 API
 - Cloud Resource Manager API
 - 運算引擎 API
 - 身分識別與存取管理（ IAM ） API

在**Google Cloud**中建立**Connector**

直接從Cloud Manager使用者介面或使用gCloud在Google Cloud中建立Connector。

您需要的是 **#8217** ；需要的是什麼

- 您的Google Cloud帳戶所需的權限、如本頁第一節所述。
- Google Cloud 專案。
- 擁有建立及管理Cloud Volumes ONTAP 功能所需權限的服務帳戶、如本頁第一節所述。
- 您所選的 Google Cloud 區域中的 VPC 和子網路。

Cloud Manager

1. 如果您要建立第一個工作環境、請按一下 * 新增工作環境 *、然後依照提示進行。否則、請按一下「* Connector*」下拉式清單、然後選取「* 新增 Connector*」。



2. 選擇 * Google Cloud Platform * 做為雲端供應商。

請記住、連接器必須連線至您所建立的工作環境類型、以及您計畫啟用的服務。

["深入瞭解連接器的網路需求"](#)。

3. 依照精靈中的步驟建立連接器：

- 準備好：檢視您需要的內容。
- 如果出現提示、請登入您的 Google 帳戶、該帳戶應有建立虛擬機器執行個體所需的權限。

這份表單由 Google 擁有及託管。您的認證資料不會提供給 NetApp。

- 基本設定：輸入虛擬機器執行個體的名稱、指定標記、選取專案、然後選取具有必要權限的服務帳戶（如需詳細資料、請參閱上節）。
- * 位置 *：指定執行個體的區域、區域、VPC 和子網路。
- * 網路 *：選擇是否啟用公用 IP 位址、並選擇性地指定 Proxy 組態。
- * 防火牆原則 *：選擇是建立新的防火牆原則、還是選擇允許傳入 HTTP、HTTPS 及 SSH 存取的現有防火牆原則。



除非您啟動連接器、否則不會有傳入流量進入連接器。HTTP 和 HTTPS 可存取 ["本機 UI"](#)、在極少數情況下使用。只有當您需要連線至主機進行疑難排解時、才需要 SSH。

- 審查：請檢閱您的選擇、確認您的設定正確無誤。

4. 按一下「* 新增 *」。

執行個體應在 7 分鐘內就緒。您應該留在頁面上、直到程序完成為止。

gCloud

1. 使用您偏好的方法登入gCloud SDK。

在我們的範例中、我們會使用已安裝gCloud SDK的本機Shell、但您可以在Google Cloud主控台使用原生Google Cloud Shell。

如需Google Cloud SDK的詳細資訊、請參閱 ["Google Cloud SDK文件頁面"](#)。

2. 請確認您以具有上述區段所定義之必要權限的使用者身分登入：

```
gcloud auth list
```

輸出應顯示下列項目、其中*使用者帳戶是所需的使用者帳戶、以下列身分登入：

```
Credentialed Accounts
ACTIVE  ACCOUNT
      some_user_account@domain.com
*      desired_user_account@domain.com
To set the active account, run:
$ gcloud config set account `ACCOUNT`
Updates are available for some Cloud SDK components. To install
them,
please run:
$ gcloud components update
```

3. 執行「gCloud運算執行個體create (gCloud compute instances create) 」命令：

```
gcloud compute instances create <instance-name>
  --machine-type=n1-standard-4
  --image-project=netapp-cloudmanager
  --image-family=cloudmanager
  --scopes=cloud-platform
  --project=<project>
  --service-account=<<service-account>>
  --zone=<zone>
  --no-address
  --tags <network-tag>
  --network <network-path>
  --subnet <subnet-path>
  --boot-disk-kms-key <kms-key-path>
```

執行個體名稱

VM執行個體所需的執行個體名稱。

專案

(選用) 您要部署VM的專案。

服務帳戶

步驟2輸出中指定的服務帳戶。

區域

您要部署VM的區域

無位址

(選用) 不使用外部IP位址 (您需要雲端NAT或Proxy才能將流量路由至公有網際網路)

網路標籤

(選用) 新增網路標記、使用標記將防火牆規則連結至連接器執行個體

網路路徑

(選用) 新增要部署連接器的網路名稱 (若為共享VPC、您需要完整路徑)

子網路路徑

(選用) 新增要部署連接器的子網路名稱 (對於共享VPC、您需要完整路徑)

kms-key-path

(選用) 新增KMS金鑰以加密連接器的磁碟 (也需要套用IAM權限)

如需這些旗標的詳細資訊、請參閱 ["Google Cloud Compute SDK文件"](#)。

+

執行命令會使用NetApp黃金映像部署Connector。Connector 執行個體和軟體應在大約五分鐘內執行。

1. 從連線至 Connector 執行個體的主機開啟網頁瀏覽器、然後輸入下列 URL：

`http://ipaddress:80[]`

2. 登入後、設定 Connector：

- a. 指定要與Connector建立關聯的NetApp帳戶。

["瞭解NetApp客戶"](#)。

- b. 輸入系統名稱。



現在已安裝Connector、並使用您的NetApp帳戶進行設定。當您建立新的工作環境時、Cloud Manager 會自動使用此 Connector。但如果您有多個連接器、就需要 ["在兩者之間切換"](#)。

如果您在建立Connector的同一個Google Cloud帳戶中有Google Cloud Storage儲存桶、您會在畫版上看到Google Cloud Storage工作環境自動出現。 ["深入瞭解如何運用此工作環境"](#)。

下一步

現在您已經登入並設定 Cloud Manager、使用者就能開始建立及探索工作環境。

- ["開始使用 Cloud Volumes ONTAP 適用於 AWS 的解決方法"](#)
- ["立即開始使用 Cloud Volumes ONTAP 適用於 Azure 的解決方法"](#)
- ["立即開始使用 Cloud Volumes ONTAP 適用於 Google Cloud 的解決方案"](#)
- ["設定 Azure NetApp Files 功能"](#)
- ["設定Amazon FSxfor ONTAP Sfor Sfor"](#)
- ["設定 Cloud Volumes Service AWS 的功能"](#)
- ["探索內部部署 ONTAP 的叢集"](#)
- ["探索您的 Amazon S3 儲存庫"](#)

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。