



設定及管理**Cloud Manager**

Set up and administration

NetApp
July 13, 2022

目錄

設定及管理Cloud Manager	1
版本資訊	2
新功能	2
已知限制	10
開始使用	13
深入瞭解 Cloud Manager	13
入門檢查清單	14
註冊 NetApp Cloud Central	17
登入 Cloud Manager	18
設定NetApp帳戶	20
設定連接器	28
下一步	65
管理 Cloud Manager	66
NetApp客戶	66
連接器	81
AWS認證資料	107
Azure認證	115
Google Cloud認證資料	128
在Cloud Manager中新增及管理NetApp支援網站帳戶	135
參考資料	142
Cloud Manager的權限摘要	142
Connector的AWS權限	143
連接器的Azure權限	166
Connector的Google Cloud權限	174
知識與支援	179
註冊以取得支援	179
取得協助	180
法律聲明	182
版權	182
商標	182
專利	182
隱私權政策	182
開放原始碼	182

設定及管理Cloud Manager

版本資訊

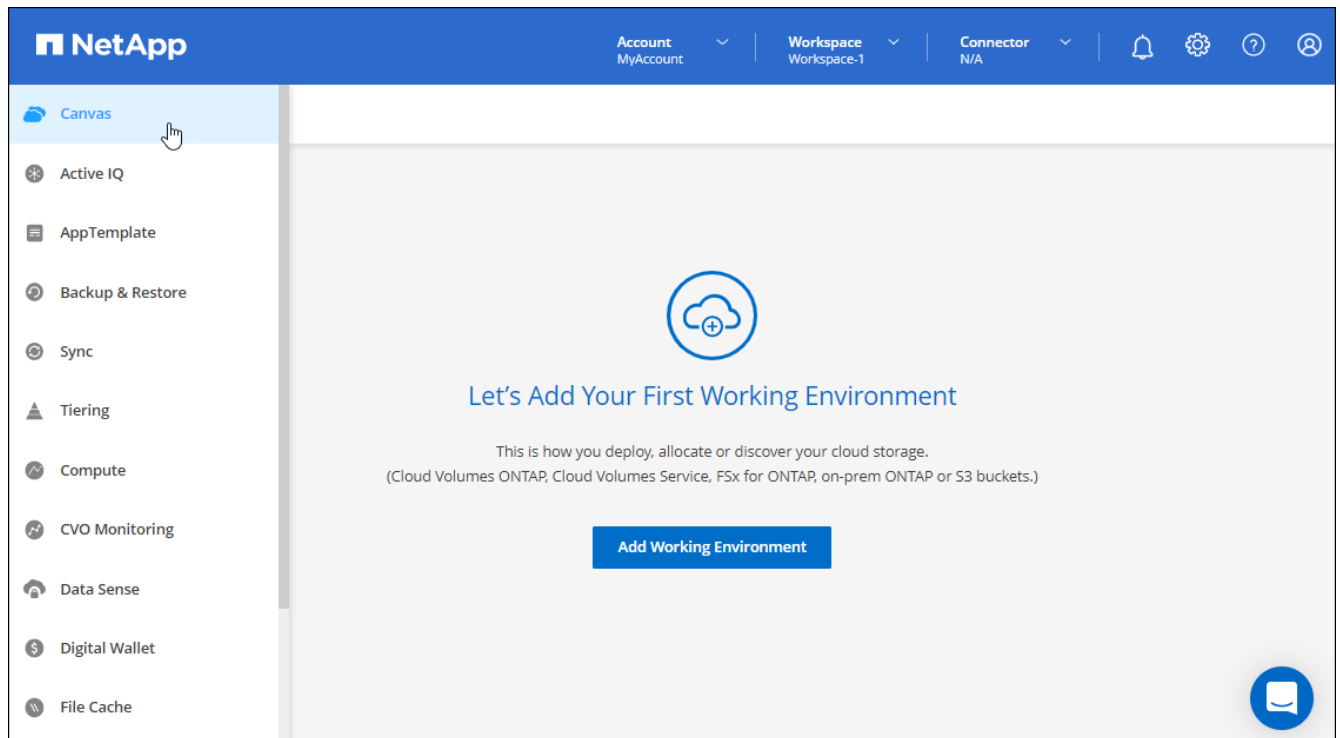
新功能

瞭解Cloud Manager管理功能的新功能：NetApp客戶、連接器、雲端供應商認證等。

2022年7月3日

連接器3.9.20

- 我們推出新的方法、可導覽至Cloud Manager介面不斷增加的功能清單。現在只要將游標放在左側面板上、即可輕鬆找到所有熟悉的Cloud Manager功能。



- 您現在可以設定Cloud Manager以電子郵件傳送通知、即使您尚未登入系統、也能得知重要的系統活動。


["深入瞭解監控帳戶運作的相關資訊"](#)。

- Cloud Manager現在支援Azure Blob儲存設備和Google Cloud Storage做為工作環境、類似於Amazon S3支援。


在Azure或Google Cloud中安裝Connector之後、Cloud Manager現在會自動探索Azure訂閱中Azure Blob儲存設備的相關資訊、或是在安裝Connector的專案中探索Google Cloud Storage的相關資訊。Cloud Manager會將物件儲存設備顯示為工作環境、您可以開啟以檢視更多詳細資訊。

以下是Azure Blob工作環境的範例：


Overview



283
Total Storage Accounts



2.26 TiB
Total Capacity



7
Total Locations

283 Storage Accounts

Storage Account Name	Subscription	Location	Creation Date	Resource Group	Blob Capacity
fqlcxn3ciw6dtim	OCCM Dev	West Europe	June 28, 2022	KobiAzureCvoSpillover2-rg	618.75 KiB
qniz6nq8x0yakb6	OCCM Dev	West Europe	June 28, 2022	KobiAzureCvoSpillover2-rg	170 B
8mqefjrtjco24lp	OCCM Dev	West Europe	June 28, 2022	KobiAzureCvoSpillover-rg	170 B
8tqosluboxoedvk	OCCM Dev	West Europe	June 28, 2022	KobiAzureCvoSpillover-rg	618.75 KiB

- 我們重新設計Amazon S3工作環境的資源頁面、提供更詳細的S3儲存區資訊、例如容量、加密詳細資料等。
- 下列Google Cloud區域現在支援Connector：
 - 馬德里（歐洲-西南1）
 - 巴黎（歐洲-西9）
 - 華沙（歐洲中心2）
- 現在Azure West US 3區域支援Connector。

["檢視支援區域的完整清單"](#)

- 此版本的Connector也包含Cloud Volumes ONTAP 了一些功能強化功能。

["深入瞭解Cloud Volumes ONTAP 解功能強化功能"](#)

2022年6月28日

使用NetApp認證登入

當新使用者註冊Cloud Central時、他們現在可以選擇*登入NetApp*選項、以NetApp支援網站認證登入。這是輸入電子郵件地址和密碼的替代方法。



使用電子郵件地址和密碼的現有登入必須持續使用該登入方法。「以NetApp登入」選項適用於註冊的新使用者。

2022年6月7日

連接器3.9.19

- 現在AWS雅加達地區（ap東南3區）支援Connector。
- 現在Azure Brazil東南地區支援Connector。

["檢視支援區域的完整清單"](#)

- 此版本的Connector也包含Cloud Volumes ONTAP 了加強功能的功能、以及內部ONTAP 的叢集增強功能。
 - ["深入瞭解Cloud Volumes ONTAP 解功能強化功能"](#)
 - ["深入瞭解ONTAP 解內部叢集增強功能"](#)

2022年5月12日

連接器3.9.18修補程式

我們更新了Connector、推出錯誤修正。最值得注意的是Cloud Volumes ONTAP 、當Connector位於共享VPC 時、會影響到Google Cloud中的功能不均部署。

2022年5月2日

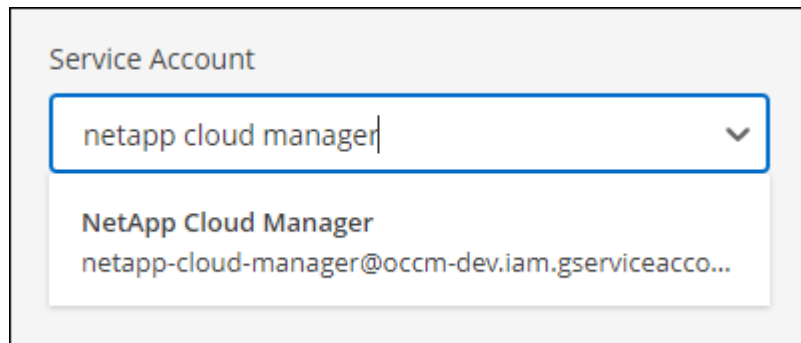
連接器3.9.18

- 下列Google Cloud區域現在支援Connector：

- 德里（亞洲-南2）
- 墨爾本（澳洲-蘇特斯塔2）
- 米蘭（歐洲-西8）
- 聖地牙哥（西南1）

["檢視支援區域的完整清單"](#)

- 當您選取要搭配Connector使用的Google Cloud服務帳戶時、Cloud Manager現在會顯示與每個服務帳戶相關聯的電子郵件地址。檢視電子郵件地址可讓您更容易區分共用相同名稱的服務帳戶。



- 我們已在支援的OS上、在VM執行個體上、在Google Cloud上認證Connector ["防護VM功能"](#)
- 此版本的Connector也包含Cloud Volumes ONTAP 了一些功能強化功能。 ["瞭解這些增強功能"](#)
- Connector需要新的AWS權限才能部署Cloud Volumes ONTAP 功能。

在單一可用度區域（AZ）中部署HA配對時、現在需要下列權限才能建立AWS分散配置群組：

```
"ec2:DescribePlacementGroups",
"iam:GetRolePolicy",
```

現在需要這些權限、才能最佳化Cloud Manager建立放置群組的方式。

請務必為您新增至Cloud Manager的每組AWS認證資料提供這些權限。 ["檢視Connector的最新IAM原則"](#)。

2022年4月3日

連接器3.9.17

- 您現在可以透過讓Cloud Manager承擔您在環境中設定的IAM角色來建立Connector。這種驗證方法比共用AWS存取金鑰和秘密金鑰更安全。

["瞭解如何使用IAM角色建立連接器"](#)。

- 此版本的Connector也包含Cloud Volumes ONTAP 了一些功能強化功能。 ["瞭解這些增強功能"](#)

2022年2月27日

連接器3.9.16

- 當您在Google Cloud中建立新的Connector時、Cloud Manager現在會顯示所有現有的防火牆原則。之前Cloud Manager不會顯示任何沒有目標標記的原則。
- 此版本的Connector也包含Cloud Volumes ONTAP 了一些功能強化功能。 ["瞭解這些增強功能"](#)

2022年1月30日

連接器3.9.15

此版本的Connector包含Cloud Volumes ONTAP 一些功能強化功能。 ["瞭解這些增強功能"](#)

2022年1月2日

減少連接器的端點數量

為了管理公有雲環境中的資源和程序、我們減少了Connector需要聯絡的端點數量。

["檢視所需端點的清單"](#)。

連接器的EBS磁碟加密

當您從Cloud Manager在AWS中部署新的Connector時、您現在可以選擇使用預設的主要金鑰或管理金鑰來加密Connector的EBS磁碟。

Get Ready

AWS Credentials

Details

Network

Security Group

Review

Details

Connector Instance Name

Connector1

Connector Role

Create Role

Select an existing Role

Role Name

Cloud-Manager-Operator-9yils3K

Add Tags to Connector Instance

AWS Managed Encryption

Master Key: aws/ebs (default)

Change Key

適用於**NSS**帳戶的電子郵件地址

Cloud Manager現在可以顯示與NetApp支援網站帳戶相關的電子郵件地址。



2021年11月28日

NetApp支援網站帳戶所需的更新

自2021年12月起、NetApp現在使用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。此更新之後、Cloud Manager會提示您更新先前新增之任何現有NetApp Support網站帳戶的認證資料。

如果您尚未將您的NSS帳戶移轉至IDaaS、首先需要移轉帳戶、然後在Cloud Manager中更新您的認證資料。

- ["瞭解如何將新的驗證方法更新至新的NSS帳戶"](#)。
- ["深入瞭解NetApp使用Microsoft Azure AD進行身分識別管理的相關資訊"](#)

變更NSS帳戶Cloud Volumes ONTAP 以供使用

如果您的組織有多個NetApp Support Site帳戶、您現在可以變更Cloud Volumes ONTAP 哪個帳戶與某個系統相關聯。

["瞭解如何將工作環境附加至不同的NSS帳戶"](#)。

2021年11月4日

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"](#)。

連接器不再支援做為Proxy

您無法再使用Cloud Manager Connector做為Proxy伺服器、從AutoSupport 停止傳送消息Cloud Volumes ONTAP。此功能已移除、不再受支援。您必須AutoSupport 透過NAT執行個體或環境的Proxy服務提供不必要的連線功能。

["深入瞭解驗證AutoSupport 使用Cloud Volumes ONTAP 效益的方法"](#)

2021年10月31日

使用服務主體進行驗證

當您在Microsoft Azure中建立新的Connector時、現在可以使用Azure服務主體進行驗證、而非使用Azure帳戶認證。

["瞭解如何與Azure服務主體進行驗證"](#)。

認證增強

我們重新設計了「認證」頁面、以方便使用、並符合Cloud Manager介面的目前外觀與風格。

2021年9月2日

已新增通知服務

通知服務已推出、因此您可以檢視在目前登入工作階段期間所啟動的Cloud Manager作業狀態。您可以驗證作業是否成功、或是否失敗。 ["瞭解如何監控您帳戶中的營運"](#)。

2021年8月1日

連接器支援RHEL 7.9

連接器現在支援執行Red Hat Enterprise Linux 7.9的主機。

["檢視Connector的系統需求"](#)。

2021年7月7日

新增連接器精靈的增強功能

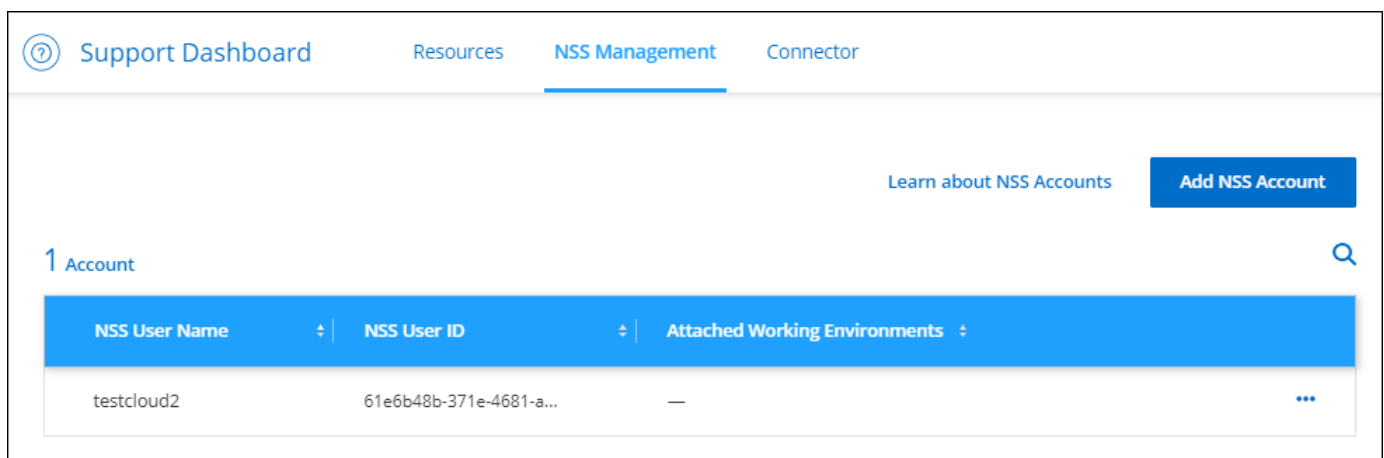
我們重新設計了「新增連接器」精靈、以新增選項並使其更易於使用。您現在可以新增標記、指定角色（適用於AWS或Azure）、上傳Proxy伺服器的根憑證、檢視Terraform自動化程式碼、檢視進度詳細資料等。

- ["在 AWS 中建立連接器"](#)
- ["在 Azure 中建立 Connector"](#)
- ["在 GCP 中建立連接器"](#)

支援儀表板的NSS帳戶管理

NetApp支援網站（NSS）帳戶現在可從支援儀表板進行管理、而非從「設定」功能表進行管理。這項變更可讓您更輕鬆地從單一位置尋找及管理所有支援相關資訊。

["瞭解如何管理NSS帳戶"](#)。



2021年5月5日

時間軸中的帳戶

Cloud Manager中的時間表現在顯示與帳戶管理相關的行動和事件。這些動作包括建立使用者關聯、建立工作區及建立連接器等項目。如果您需要識別執行特定行動的人員、或是需要識別行動的狀態、檢查時間表會很有幫助。

["瞭解如何將時間表篩選為「租賃」服務"](#)。

2021年4月11日

API直接呼叫Cloud Manager

如果您已設定Proxy伺服器、現在可以啟用選項、將API呼叫直接傳送至Cloud Manager、而無需透過Proxy。此選項受AWS或Google Cloud中執行的Connectors支援。

["深入瞭解此設定"](#)。

服務帳戶使用者

您現在可以建立服務帳戶使用者。

服務帳戶扮演「使用者」的角色、可撥打授權API呼叫至Cloud Manager進行自動化。如此一來、您就不需要根據實際使用者帳戶建置自動化指令碼、也能隨時離開公司、因此更容易管理自動化作業。如果您使用同盟、則可以建立權杖、而不需從雲端產生更新權杖。

["深入瞭解如何使用服務帳戶"](#)。

私有預覽

您現在可以允許帳戶中的私有預覽、以在Cloud Manager中預覽新的NetApp雲端服務。

["深入瞭解此選項"](#)。

第三方服務

您也可以允許帳戶中的第三方服務存取Cloud Manager中提供的第三方服務。

["深入瞭解此選項"](#)。

2021年2月9日

支援儀表板改良功能

我們已更新「支援儀表板」、讓您新增NetApp支援網站認證資料、以註冊您的支援。您也可以直接從儀表板啟動NetApp支援案例。只要按一下「說明」圖示、然後按*「支援」*即可。

已知限制

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。

這些限制僅適用於Cloud Manager的設定與管理：Connector、SaaS平台等。

連接器限制

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。

僅支援HTTP Proxy伺服器

如果您的企業原則要求您使用Proxy伺服器來進行所有的HTTP通訊至網際網路、則必須設定連接器以使用該HTTP Proxy伺服器。Proxy 伺服器可以位於雲端或網路中。

Cloud Manager不支援使用連接器的HTTPS Proxy。

不支援SSL解密

Cloud Manager不支援啟用SSL解密的防火牆組態。如果啟用SSL解密、Cloud Manager會顯示錯誤訊息、而Connector執行個體則會顯示為非作用中。

為了增強安全性、您可以選擇 ["安裝由憑證授權單位（CA）簽署的HTTPS憑證"](#)。

載入本機UI時顯示空白頁面

如果您載入連接器的本機使用者介面、UI有時可能無法顯示、您只會看到空白頁面。

此問題與快取問題有關。因應措施是使用無痕式或私有網路瀏覽器工作階段。

不支援共享 Linux 主機

與其他應用程式共用的VM不支援Connector。VM必須專用於Connector軟體。

第三方代理程式與擴充功能

Connector VM不支援協力廠商代理程式或VM擴充。

SaaS限制

SaaS 平台在政府區域中已停用

如果您在 AWS GovCloud 區域、Azure Gov 區域或 Azure DoD 區域部署 Connector 、則只能透過 Connector 的主機 IP 位址存取 Cloud Manager 。系統會停用整個帳戶的 SaaS 平台存取權。

這表示只有能夠存取終端使用者內部 VPC/vnet 的授權使用者、才能使用 Cloud Manager 的 UI 或 API 。

請注意、這些地區僅支援Cloud Volumes ONTAP 的服務包括：功能完善、雲端備份、雲端資料認證及複寫。政府區域不支援其他NetApp服務。

["瞭解如何存取Connector上的本機UI"](#)。

市場限制

Azure和Google Cloud合作夥伴不提供隨用隨付功能

如果您是Microsoft Cloud Solution Provider（CSP）合作夥伴或Google Cloud合作夥伴、則無法使用NetApp隨用隨付訂閱。您必須購買授權、並以BYOL授權部署NetApp雲端解決方案。

下列NetApp雲端服務不提供隨用隨付訂閱：

- Cloud Volumes ONTAP
- 雲端分層
- 雲端備份
- 雲端資料感測

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://cloudmanagerinfraprod.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

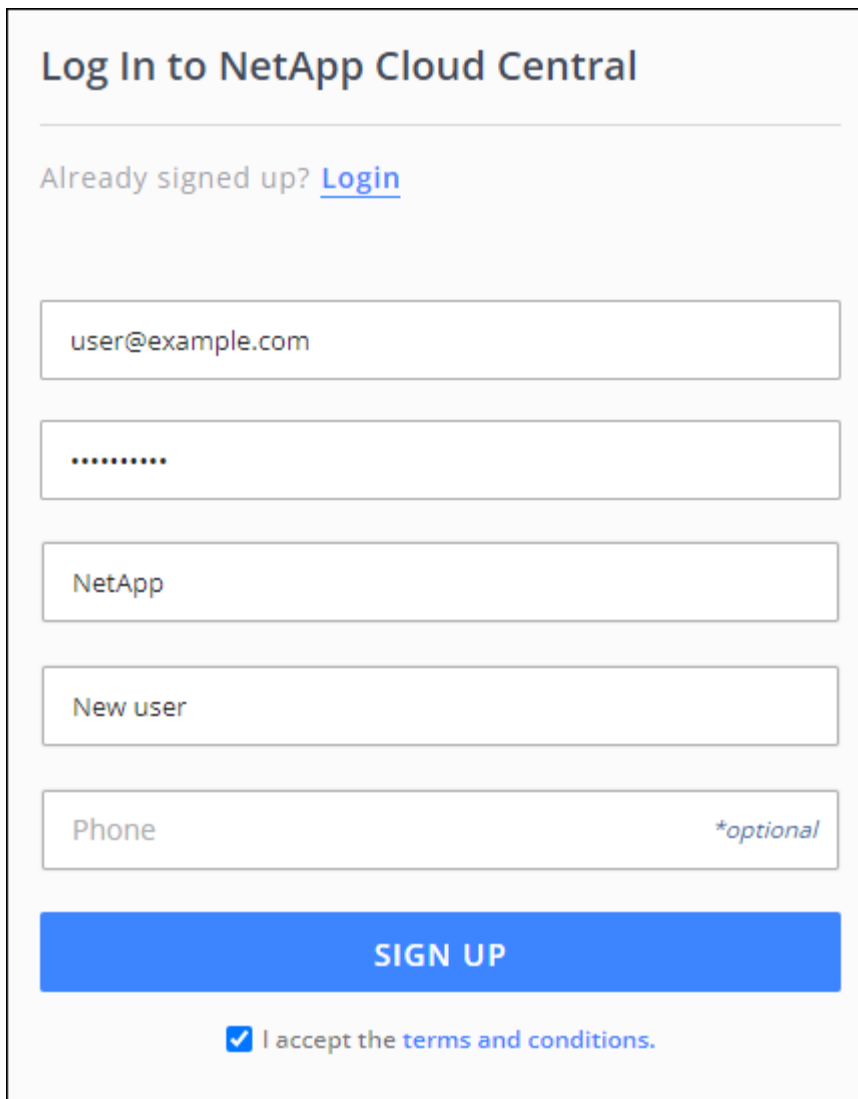
註冊 NetApp Cloud Central 、即可存取 NetApp 的雲端服務。



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: a text field with "user@example.com", a password field with masked dots, a dropdown menu with "NetApp" selected, a text field with "New user", and a text field with "Phone" and a note "*optional". At the bottom is a large blue button labeled "SIGN UP" and a checkbox labeled "I accept the terms and conditions." which is checked.

- 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](#)

Email

Password

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。

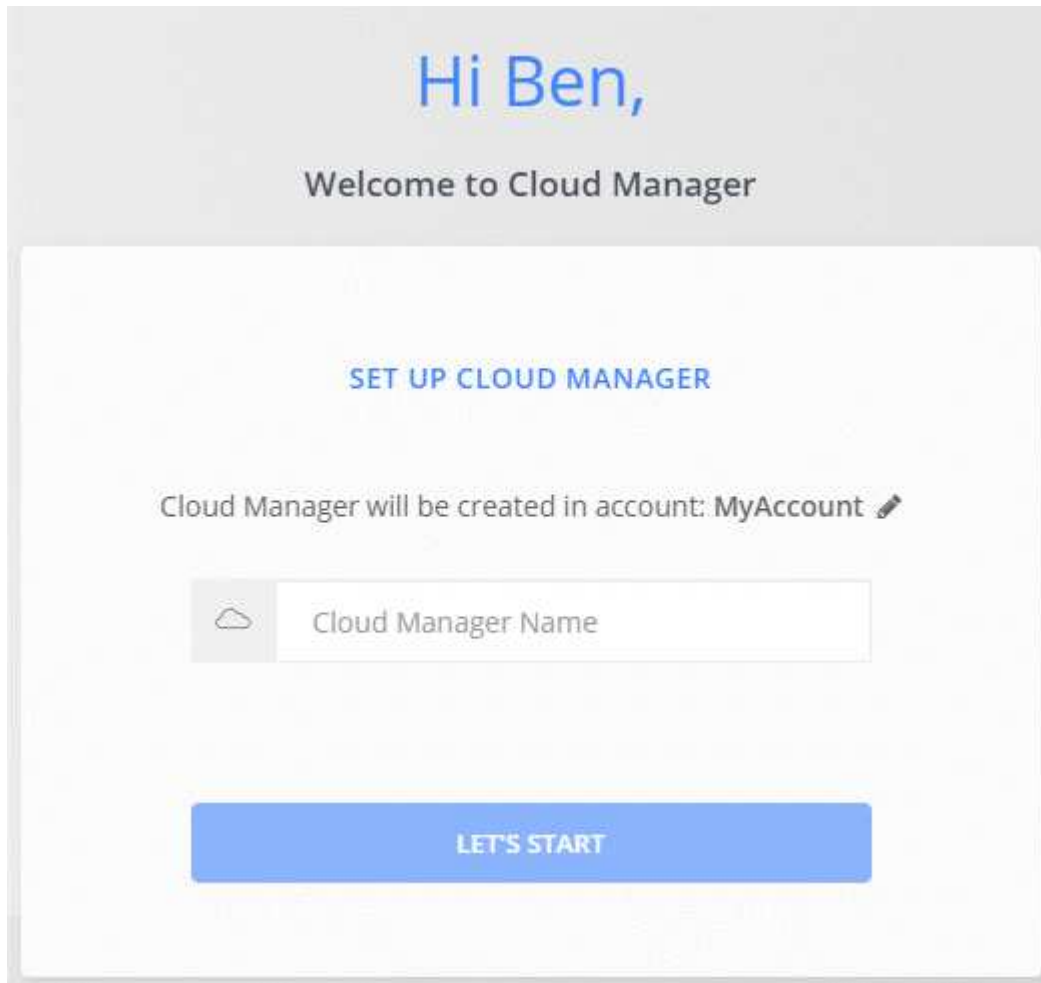
設定NetApp帳戶

瞭解NetApp客戶

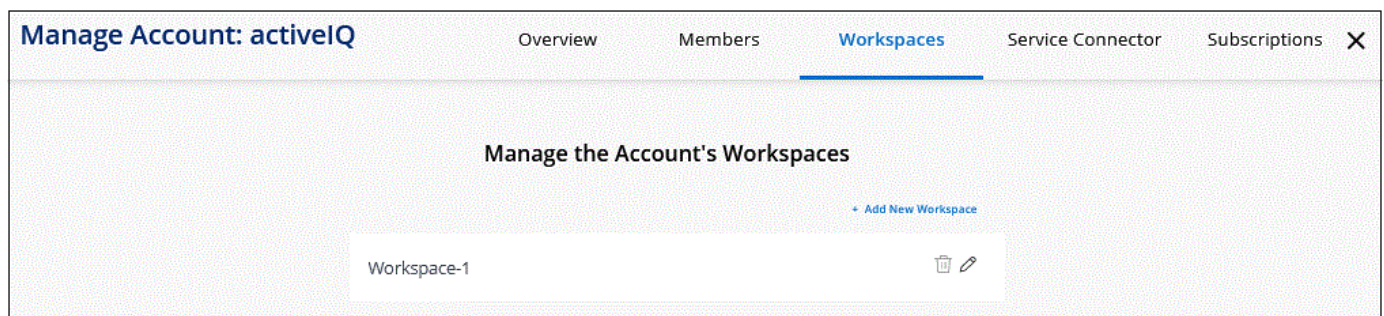
NetApp帳戶_提供多租戶共享、讓您從Cloud Manager內部、在隔離的工作區中組織使用者和資源。

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。

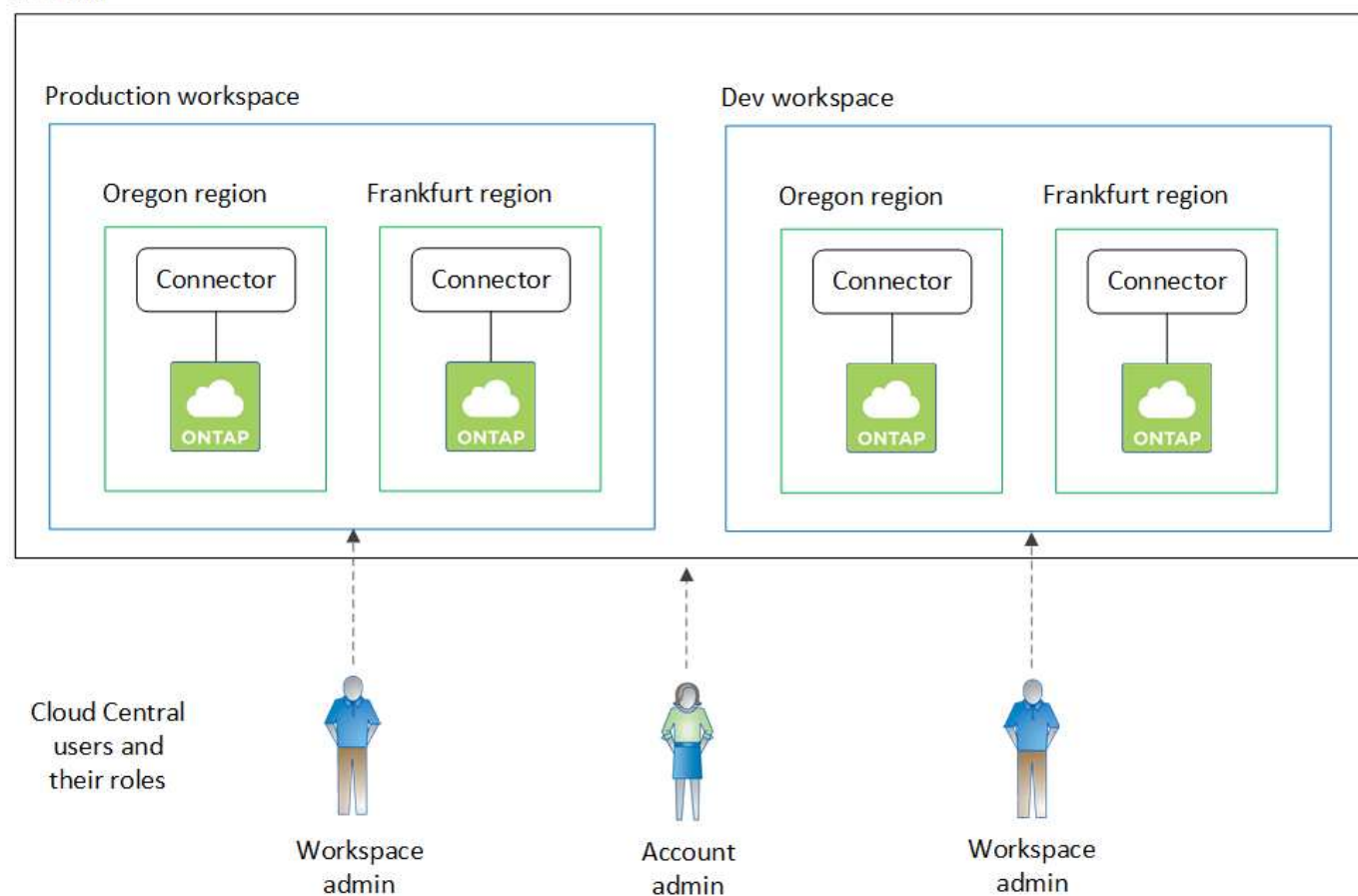


在後續的兩個範例影像中、Connector和Cloud Volumes ONTAP the SURF系 實際上並未駐留NetApp帳戶、而是在雲端供應商中執行。這是每個元件之間關係的概念呈現。

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。

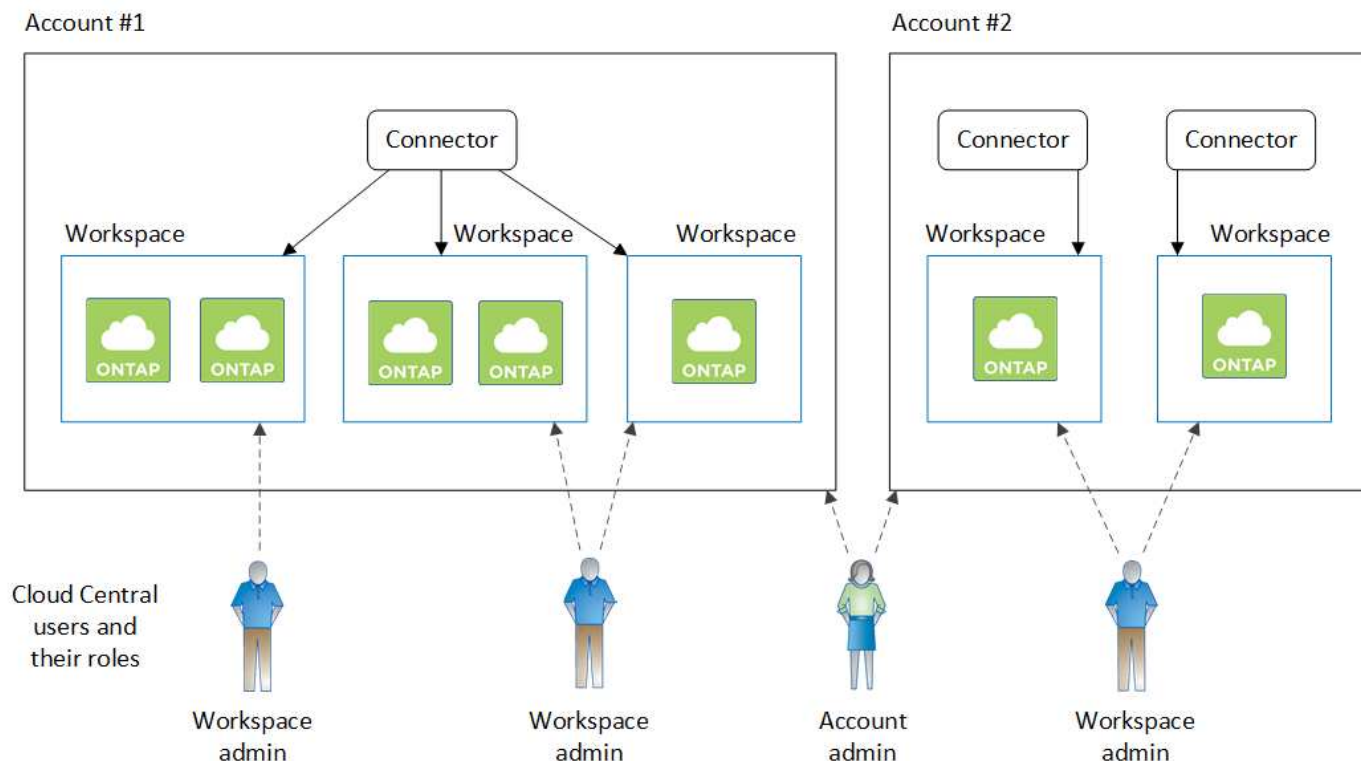
Account



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*）」。

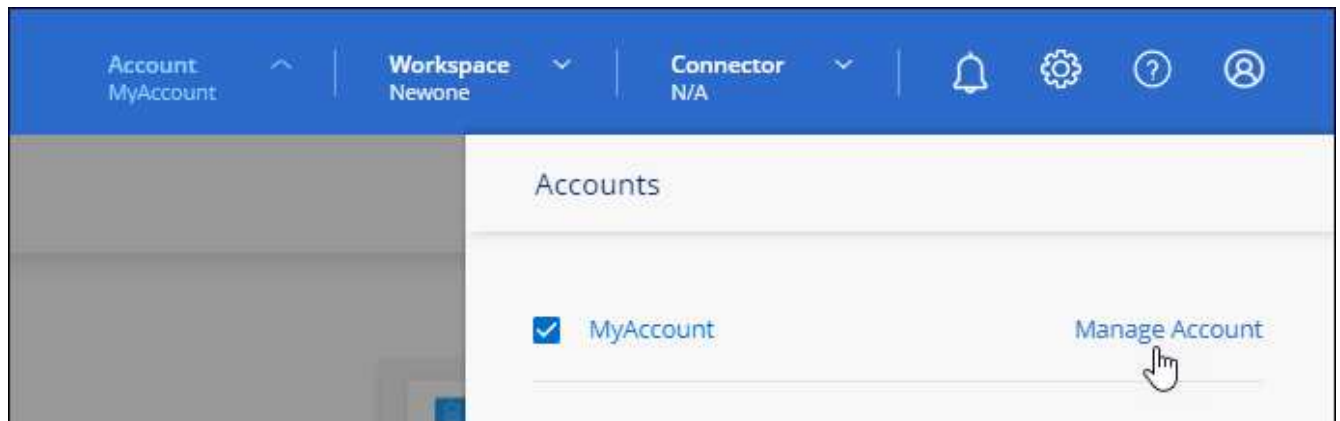
如果「工作區管理」需要存取此工作區、您就必須建立使用者的關聯。您也需要將 Connectors 與工作區建立關聯、讓 Workspace Admins 能夠使用這些 Connectors 。

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

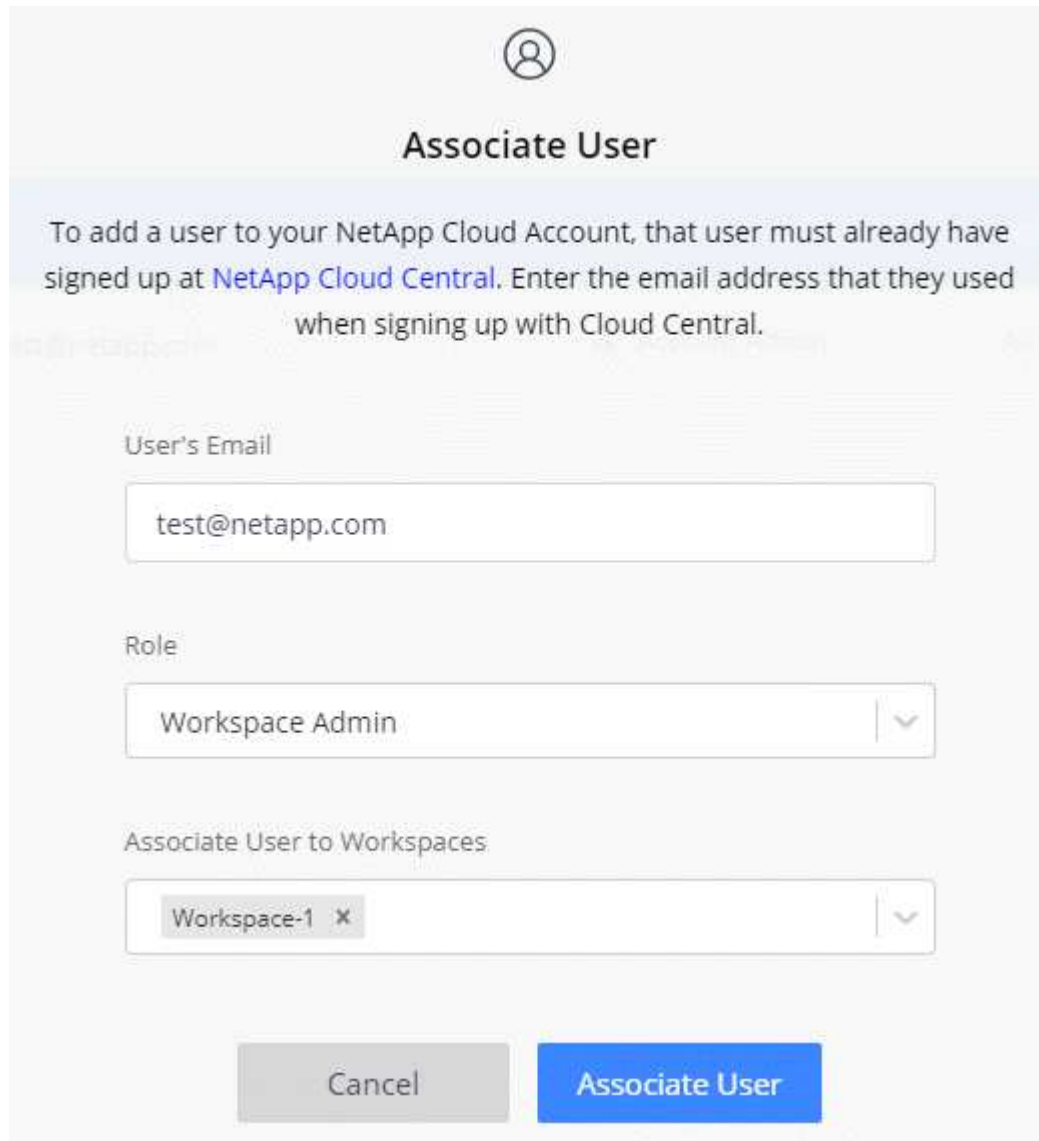
1. 如果使用者尚未這麼做、請要求使用者前往 "NetApp Cloud Central" 並註冊。
2. 從上而下 "Cloud Manager"，單擊* Account（帳戶）下拉列表並單擊 Manage Account*（管理帳戶）。



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 dialog box titled "Associate User" with a user icon at the top. Below the title, there is a light blue box containing the text: "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." Below this, there are three input 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

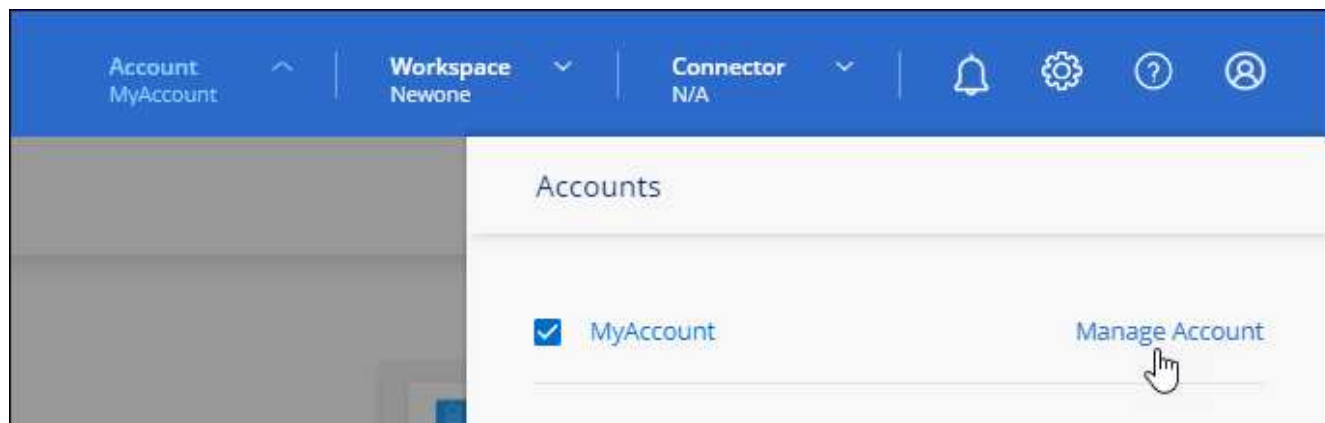
您需要將 Connector 與工作空間建立關聯、讓 Workspace Admins 可以使用這些 Connectors 來建立 Cloud Volumes ONTAP 一套系統。

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。

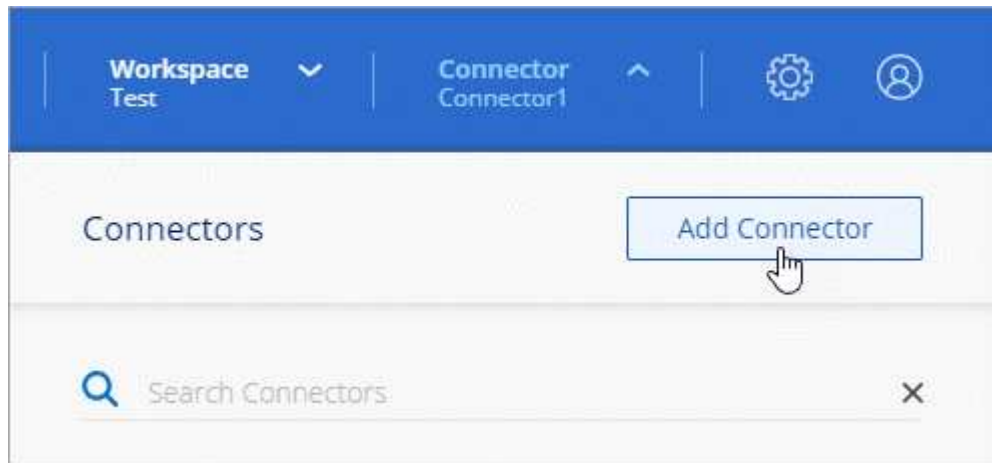
您需要的是 **#8217** ；需要的是什麼

- 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](#)"。

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。"[瞭解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。

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/rea
```

```

d",
    "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 *

```

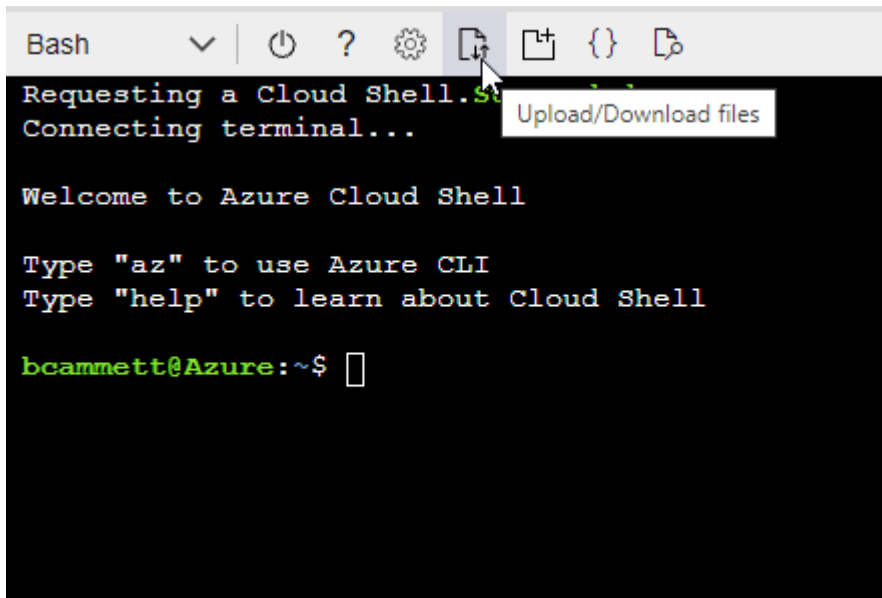
"AssignableScopes": [
    "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz"
],

```

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。

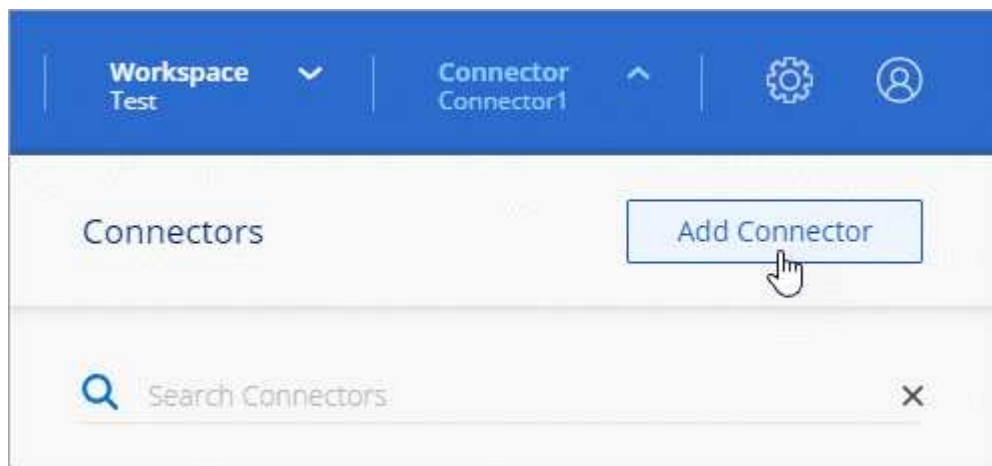
您需要的是 **#8217** ；需要的是什麼

- 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](#)"。

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](#)

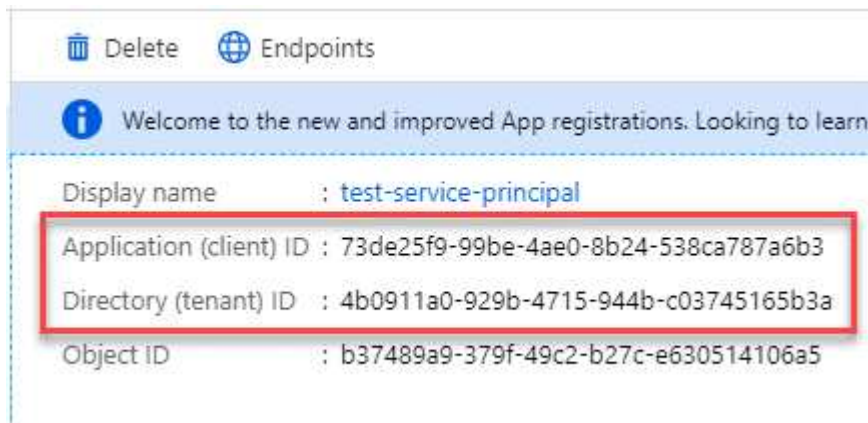
Type to search	
PERMISSION	ADMIN CONSENT REQUIRED
<input checked="" type="checkbox"/> user_impersonation Access Azure Service Management as organization users (preview) ⓘ	-

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。

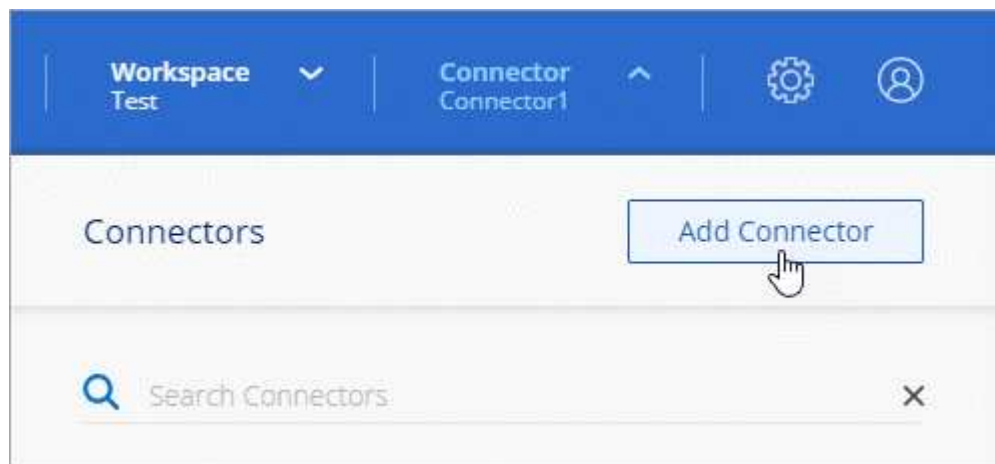
您需要的是 #8217 ；需要的是什麼

- 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"。

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	• "本節所提供的權限"	• compute.networkUser	在服務專案中部署Connector
連接器服務帳戶	自訂	服務專案	• "本節所提供的權限"	• 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	• 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	• (預設) 編輯器	• 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	• (預設) 編輯器	• compute.networkUser	代表部署部署部署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：

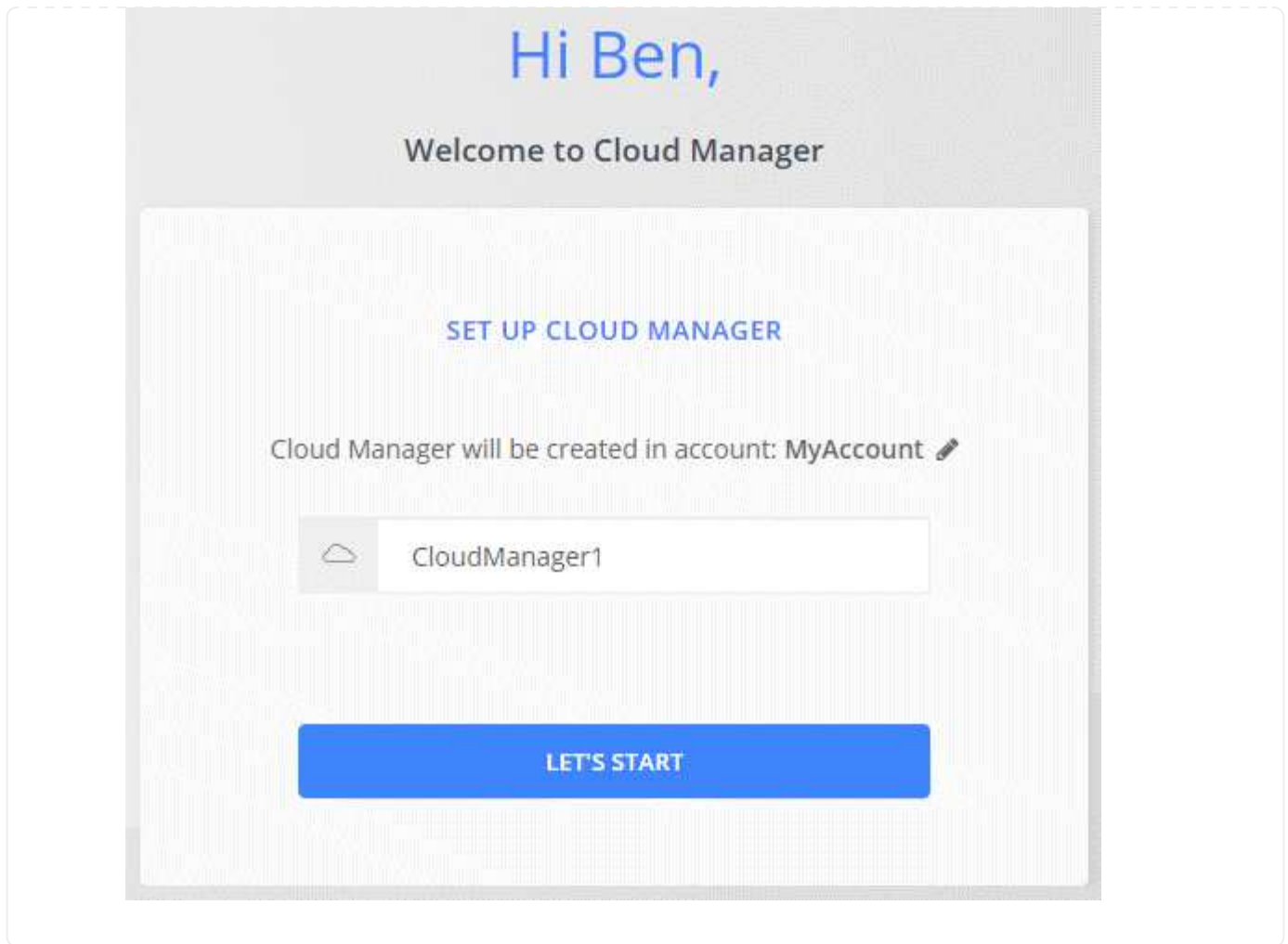
`http://ipaddress:80[]`

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"](#)。

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"](#)

管理 Cloud Manager

NetApp客戶

管理您的**NetApp**帳戶

"[執行初始設定之後](#)"，您可以稍後管理使用者、服務帳戶、工作區、連接器及訂閱，以管理帳戶設定。

"[深入瞭解NetApp客戶的運作方式](#)"。

使用**Tenancy API**管理您的帳戶

如果您想要透過傳送API要求來管理帳戶設定、則必須使用_Tenancy API。此API與Cloud Manager API不同、您可用來建立及管理Cloud Volumes ONTAP 各種運作環境。

"[檢視Tenancy API的端點](#)"

建立及管理使用者

您帳戶中的使用者可以存取帳戶工作區中的管理資源。

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

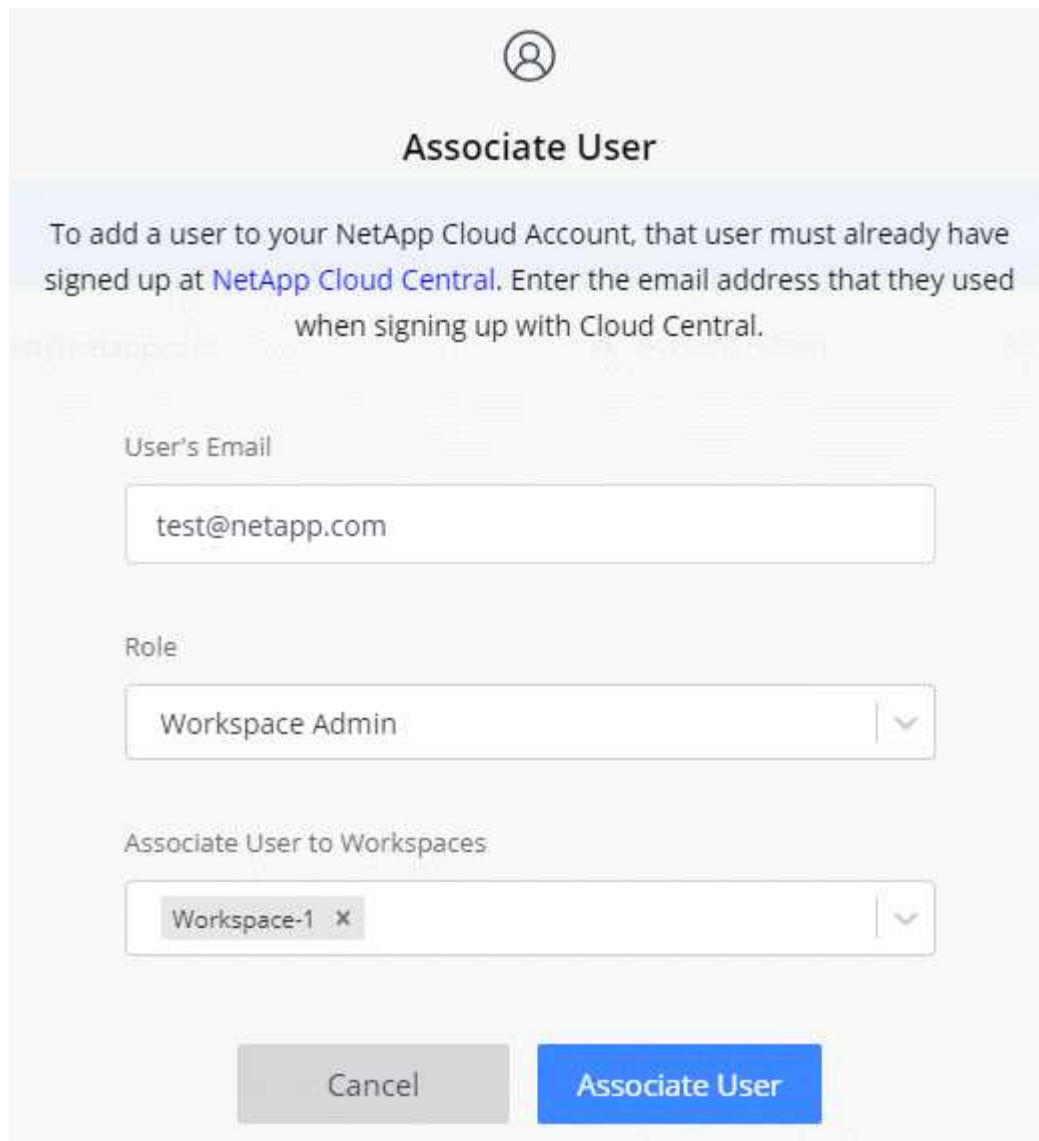
1. 如果使用者尚未這麼做、請要求使用者前往 "[NetApp Cloud Central](#)" 並註冊。
2. 從 Cloud Manager 頂端、按一下「* Account *（帳戶 *）」下拉式清單。




3. 按一下目前選取帳戶旁的 * 管理帳戶 *。



4. 在「成員」索引標籤中、按一下「關聯使用者」。
5. 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。_
6. 如果您選取「工作區管理」或「法規遵循檢視器」、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 light blue banner contains the text: "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 main form area has three sections: "User's Email" with a text input field containing "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: a grey "Cancel" button and a blue "Associate User" button.



Associate User

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.

User's Email

test@netapp.com

Role

Workspace Admin

Associate User to Workspaces

Workspace-1 X

Cancel Associate User

7. 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。

移除使用者

取消使用者關聯後、使用者便無法再存取NetApp帳戶中的資源。

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。

5 Members

Type	Name	Email	Role	Workspace	
	Ben		☆ Account Admin	All Workspaces	...
	Tom		☆ Account Admin	All Workspaces	...
	Ben		Workspace Admin	Newone	

3. 按一下 * 解除使用者關聯 *、然後按一下 * 解除關聯 * 以確認。

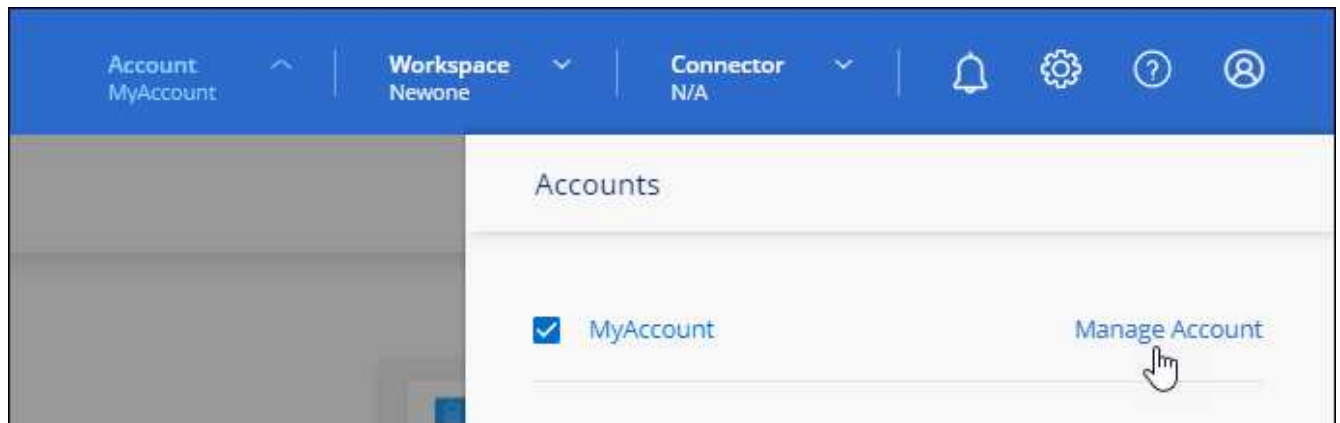
使用者無法再存取此NetApp帳戶中的資源。

管理 **Workspace** 管理的工作區

您可以隨時建立工作區管理員與工作區的關聯和取消關聯。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。

5 Members

Type	Name	Email	Role	Workspace	
	Ben		☆ Account Admin	All Workspaces	...
	Tom		☆ Account Admin	All Workspaces	...
	Ben		Workspace Admin	Newone	

3. 按一下 * 管理工作區 * 。

4. 選取要與使用者建立關聯的工作區、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。

建立及管理服務帳戶

服務帳戶扮演「使用者」的角色、可撥打授權API呼叫至Cloud Manager進行自動化。如此一來、您就不需要根據實際使用者帳戶建置自動化指令碼、也能隨時離開公司、因此更容易管理自動化作業。如果您使用同盟、則可以建立權杖、而不需從雲端產生更新權杖。

您可以將服務帳戶指派為角色、就像其他Cloud Manager使用者一樣、為其授予權限。您也可以將服務帳戶與特定工作區建立關聯、以控制服務可以存取的工作環境（資源）。

建立服務帳戶時、Cloud Manager可讓您複製或下載服務帳戶的用戶端ID和用戶端機密。此金鑰配對用於Cloud Manager驗證。

建立服務帳戶

建立所需數量的服務帳戶、以管理工作環境中的資源。

步驟

1. 從 Cloud Manager 頂端、按一下「* Account *（帳戶*）」下拉式清單。



2. 按一下目前選取帳戶旁的 * 管理帳戶 * 。



3. 在「成員」索引標籤中、按一下「建立服務帳戶」。
4. 輸入名稱並選取角色。如果您選擇帳戶管理員以外的角色、請選擇要與此服務帳戶建立關聯的工作區。
5. 按一下「* 建立 *」。
6. 複製或下載用戶端ID和用戶端密碼。

用戶端機密只會顯示一次、Cloud Manager不會儲存在任何位置。複製或下載機密、並安全地儲存。

7. 按一下 * 關閉 *。

取得服務帳戶的承載權杖

以便對進行API呼叫 "租戶API"、您需要取得服務帳戶的承載權杖。

```
curl --location --request POST 'https://netapp-cloud-account.auth0.com/oauth/token' \
--header 'Content-Type: application/json' \
--data-raw '{
  "grant_type": "client_credentials",
  "client_secret": "<client secret>",
  "audience": "https://api.cloud.netapp.com",
  "client_id": "<client id>"
}'
```

複製用戶端ID

您可以隨時複製服務帳戶的用戶端ID。

步驟

1. 在「成員」索引標籤中、按一下對應於服務帳戶的列中的動作功能表。



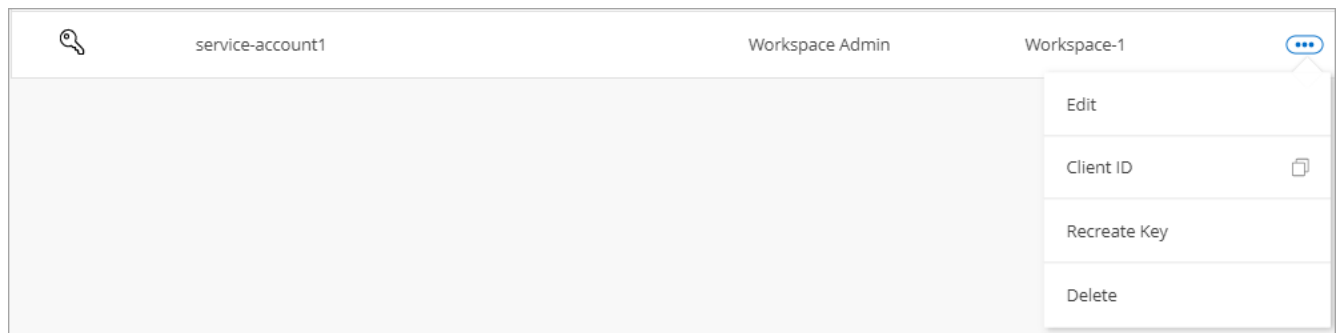
2. 按一下*用戶端ID*。
3. ID會複製到剪貼簿。

重新建立金鑰

重新建立金鑰會刪除此服務帳戶的現有金鑰、然後建立新金鑰。您將無法使用上一個金鑰。

步驟

1. 在「成員」索引標籤中、按一下對應於服務帳戶的列中的動作功能表。



2. 按一下「重新建立金鑰」。
3. 按一下「重新建立」以確認。
4. 複製或下載用戶端ID和用戶端密碼。

用戶端機密只會顯示一次、Cloud Manager不會儲存在任何位置。複製或下載機密、並安全地儲存。

5. 按一下 * 關閉 * 。

刪除服務帳戶

如果您不再需要使用服務帳戶、請將其刪除。

步驟

1. 在「成員」索引標籤中、按一下對應於服務帳戶的列中的動作功能表。



2. 按一下*刪除*。
3. 再按一下 * 刪除 * 以確認。

管理工作區

透過建立、重新命名及刪除工作區來管理工作區。請注意、如果工作區包含任何資源、您就無法刪除該工作區。它必須是空的。

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 * 工作區 * 。
3. 請選擇下列其中一個選項：
 - 按一下 * 新增工作區 * 以建立新的工作區。
 - 按一下 * 重新命名 * 以重新命名工作區。
 - 按一下 * 刪除 * 以刪除工作區。

管理 **Connector** 的工作空間

您需要將 Connector 與工作區建立關聯、讓 Workspace Admins 能夠從 Cloud Manager 存取這些工作區。

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. 選取要與 Connector 建立關聯的工作區、然後按一下「* 套用 *」。

管理訂閱

從雲端供應商的市場訂閱之後、您可以從「帳戶設定」小工具取得每份訂閱內容。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。

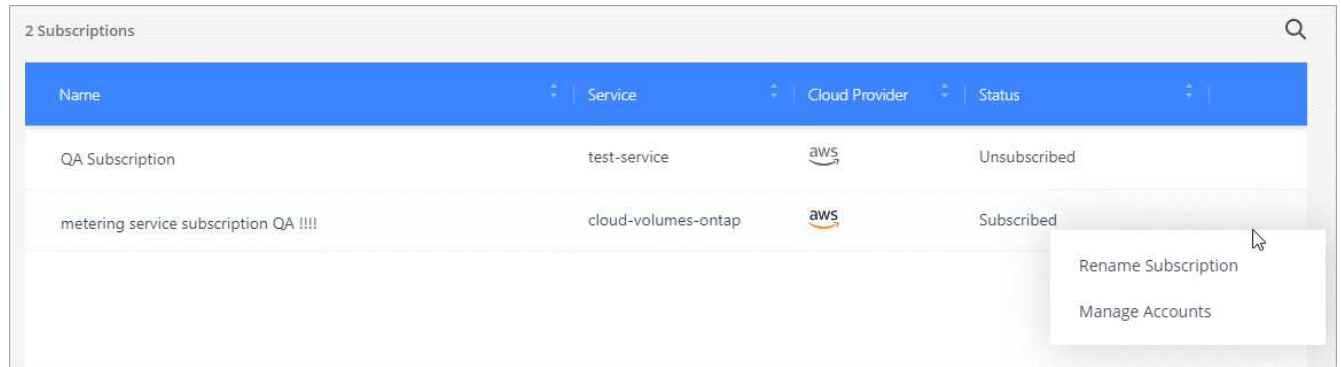
["深入瞭解訂閱內容"](#)。

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 * 訂閱 * 。

您只會看到與您目前檢視的帳戶相關聯的訂閱內容。

3. 按一下您要管理之訂閱對應列中的動作功能表。



4. 選擇重新命名訂閱、或管理與訂閱相關的帳戶。

變更您的帳戶名稱

隨時變更您的帳戶名稱、將其變更為對您有意義的名稱。

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「* 總覽 *」標籤中、按一下帳戶名稱旁的編輯圖示。
3. 輸入新的帳戶名稱、然後按一下 * 「 Saving* （儲存 *）」 。

允許私有預覽

允許您帳戶中的私有預覽、以取得新的NetApp雲端服務、這些服務可在Cloud Manager中預覽。

私有預覽中的服務無法保證其行為符合預期、而且可能會持續中斷運作並喪失功能。

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「總覽」標籤中、啟用「允許私有預覽」設定。

允許第三方服務

允許您帳戶中的第三方服務存取Cloud Manager中提供的第三方服務。第三方服務是類似NetApp所提供服務的雲端服務、但由第三方公司管理及支援。

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「總覽」標籤中、啟用「允許協力廠商服務」設定。

停用SaaS平台

除非您必須遵守公司的安全原則、否則我們不建議停用 SaaS 平台。停用 SaaS 平台會限制您使用 NetApp 整合式雲端服務的能力。

如果停用 SaaS 平台、Cloud Manager 將無法提供下列服務：

- 雲端資料感測
- Kubernetes
- 雲端分層
- 全域檔案快取

如果您停用SaaS平台、則必須執行的所有工作 "[連接器上可用的本機使用者介面](#)"。



這是一項無法還原的行動、會使您無法使用Cloud Manager SaaS平台。您需要從本機連接器執行動作。您將無法使用NetApp的許多整合式雲端服務、而重新啟用SaaS平台將需要NetApp支援的協助。

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「總覽」索引標籤中、切換停用SaaS平台的選項。

監控您帳戶中的作業

您可以監控Cloud Manager執行的作業狀態、查看是否有任何需要解決的問題。您可以在「通知中心」、「時間表」中檢視狀態、或將通知傳送至您的電子郵件。

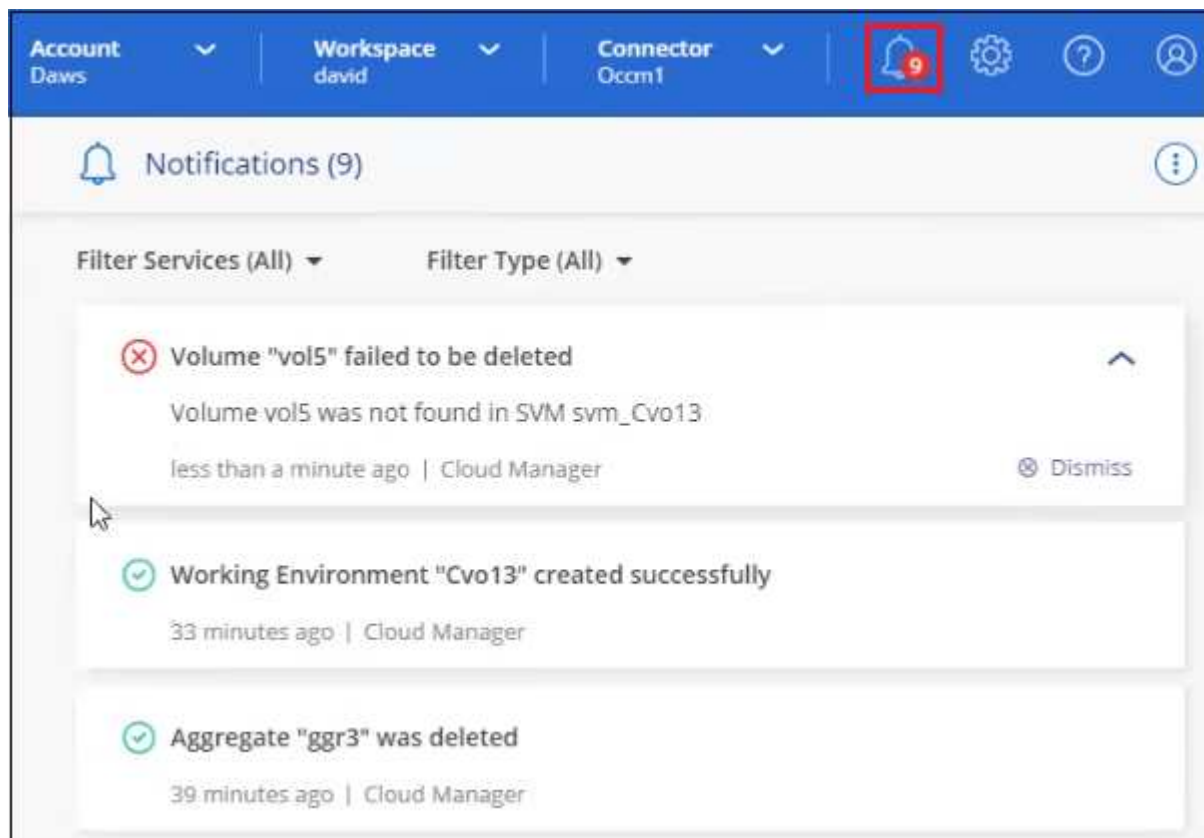
此表格提供通知中心與時間表的比較、讓您瞭解每項服務的內容。

通知中心	時間表
顯示事件和行動的高層級狀態	提供每個事件或行動的詳細資料、以供進一步調查
顯示目前登入工作階段的狀態：登出後、資訊不會出現在通知中心	保留上個月的狀態
僅顯示在使用者介面中啟動的動作	顯示UI或API的所有動作
顯示使用者啟動的動作	顯示所有動作、無論是使用者啟動或系統啟動
依重要性篩選結果	依服務、行動、使用者、狀態及其他項目篩選
可將通知以電子郵件傳送給帳戶使用者和其他人	無電子郵件功能

使用通知中心監控活動

通知會追蹤您在Cloud Manager中啟動的作業進度、以便您確認作業是否成功。您可透過這些工具來檢視目前登入工作階段期間所啟動的許多Cloud Manager作業狀態。目前並非所有服務都會將資訊報告至通知中心。

您可以按一下通知鈴聲 (🔔⁹)。警示中的小球型罩顏色代表作用中的最高層級嚴重性通知。因此、如果您看到紅色的球型罩、就表示您應該查看重要通知。



您也可以設定Cloud Manager以電子郵件傳送通知、即使您尚未登入系統、也能得知重要的系統活動。電子郵件可傳送給屬於您NetApp雲端帳戶一部分的任何Cloud Central使用者、或傳送給任何其他需要注意特定系統活動類型的收件者。請參閱 [設定電子郵件通知設定](#) 以下。

通知類型

通知分為下列類別：

通知類型	說明
關鍵	如果未立即採取修正行動、可能導致服務中斷。
錯誤	某項行動或程序因故障而結束、或是在未採取修正行動時可能導致故障。
警告	您應注意的問題、以確保其未達到嚴重嚴重性。此嚴重性的通知不會造成服務中斷、因此可能不需要立即採取修正行動。
建議	系統建議您採取行動來改善系統或特定服務、例如：節省成本、建議新服務、建議的安全組態等
資訊	提供有關行動或程序的其他資訊的訊息。

通知類型	說明
成功	已成功完成行動或程序。

篩選通知

依預設、您會看到所有通知。您可以篩選在「通知中心」中看到的通知、只顯示對您重要的通知。您可以依Cloud Manager的「服務」和通知「類型」進行篩選。

The screenshot shows two side-by-side filter panels. The left panel, titled 'Filter Services (All)', contains three items: 'Digital Wallet (3)' with a checked checkbox, 'Active IQ (2)' with a checked checkbox, and 'AppTemplate (1)' with an unchecked checkbox. Below these items are 'Clear' and 'Apply' buttons. The right panel, titled 'Filter Type (All)', contains six items: 'Information (0)' (unchecked), 'Success (1)' (unchecked), 'Warning (2)' (checked), 'Error (1)' (checked), 'Critical (0)' (checked with a greyed-out checkbox), and 'Recommendation (0)' (unchecked). Below these items are 'Clear' and 'Apply' buttons.

例如、如果您只想查看Cloud Manager作業的「錯誤」和「警告」通知、請選取這些項目、您只會看到這些通知類型。

設定電子郵件通知設定

您可以透過電子郵件傳送特定類型的通知、即使您尚未登入Cloud Manager、也能得知重要的系統活動。電子郵件可傳送給您的NetApp帳戶中的任何使用者、或是任何其他需要注意特定系統活動類型的收件者。

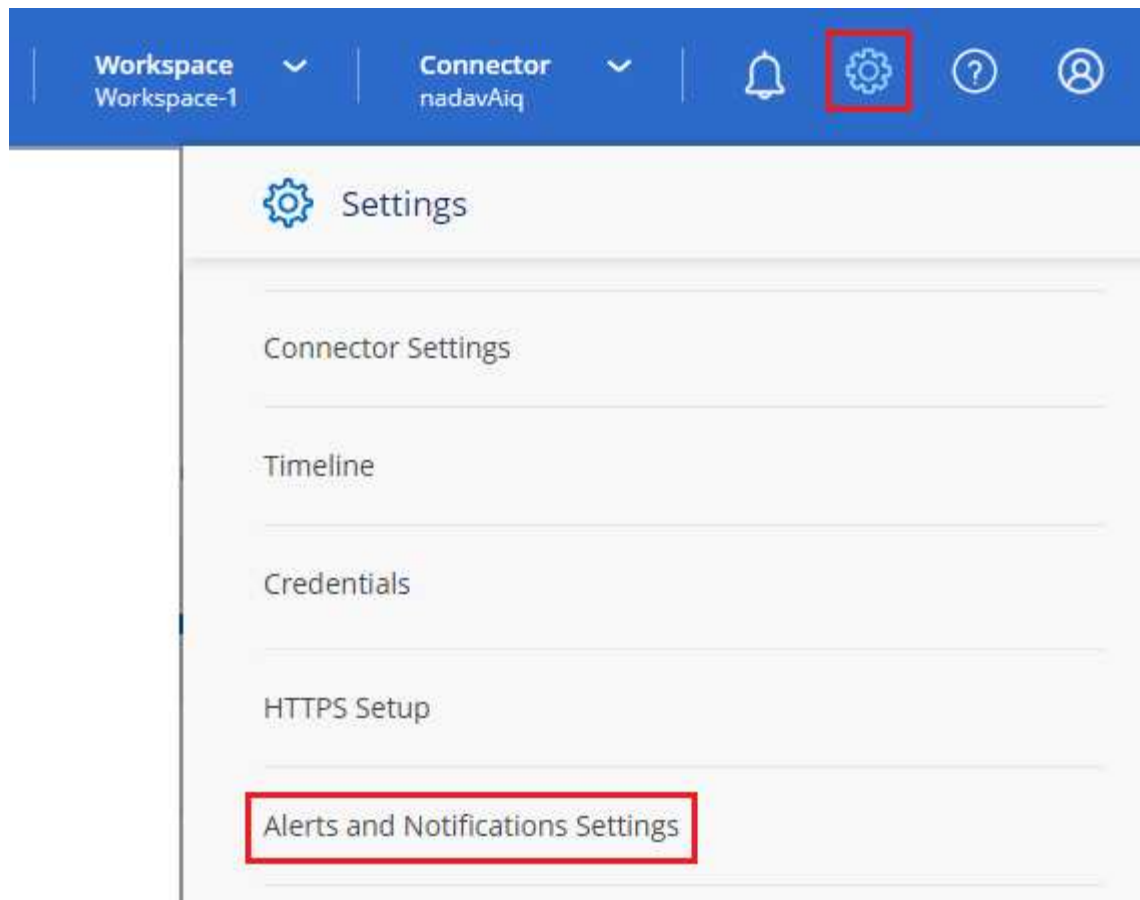
*附註：*若連接器安裝在沒有網際網路存取的網站上、則不支援傳送電子郵件通知。

依預設、帳戶管理員會收到所有「重大」和「建議」通知的電子郵件。根據預設、所有其他使用者和收件者都會設定為不接收任何通知電子郵件。

您必須是帳戶管理員、才能自訂通知設定。

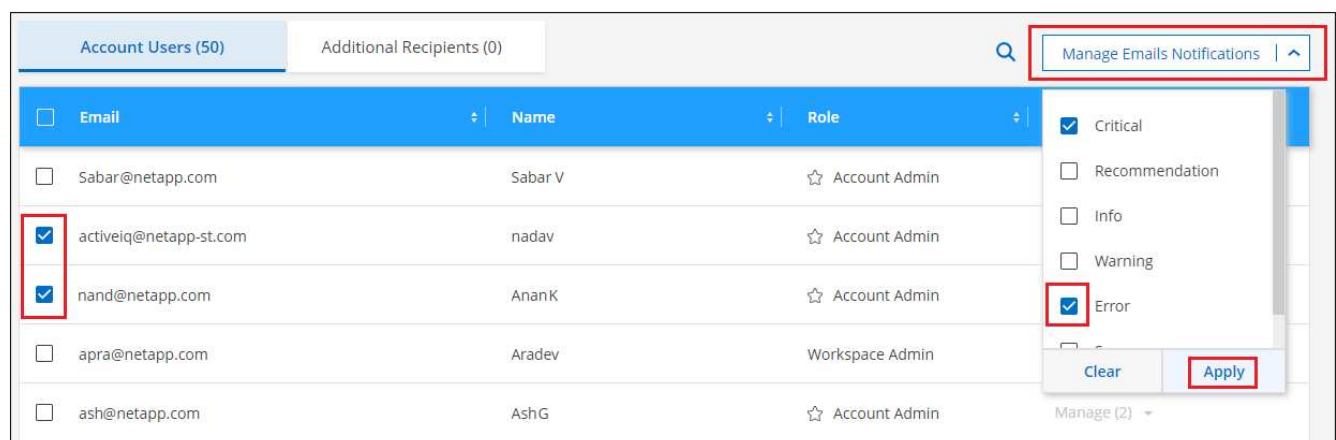
步驟

1. 在Cloud Manager功能表列中、按一下*設定>警示與通知設定*。



2. 從「帳戶使用者」索引標籤或「其他收件者」索引標籤中選取一位或多位使用者、然後選擇要傳送的通知類型：

- 若要變更單一使用者、請按一下該使用者「通知」欄中的功能表、檢查要傳送的通知類型、然後按一下「套用」。
- 若要變更多位使用者、請勾選每位使用者的方塊、按一下*管理電子郵件通知*、勾選要傳送的通知類型、然後按一下*套用*。

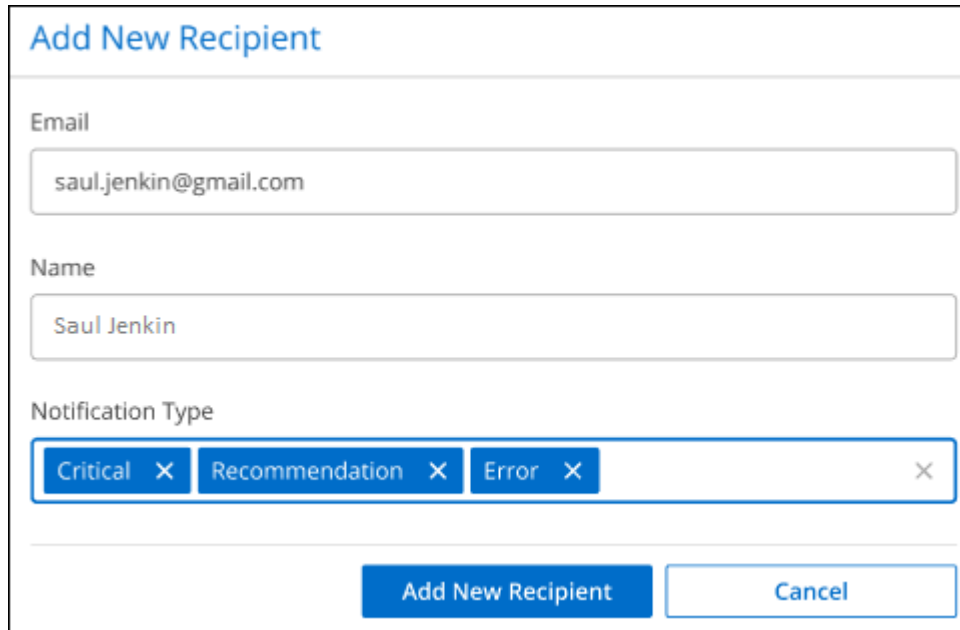


新增其他電子郵件收件者

出現在「Account Users」（帳戶使用者）標籤的使用者、會自動從您NetApp帳戶中的使用者（從 ["管理帳戶頁面"](#)）。您可以在「其他收件者」索引標籤中新增電子郵件地址、以供無權存取Cloud Manager但需要收到特定警示和通知類型通知的其他人員或群組使用。

步驟


1. 在「警示與通知設定」頁面中、按一下*「新增收件者」*。

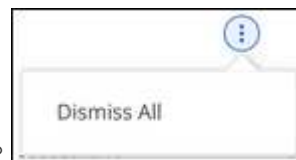
A form titled "Add New Recipient" with three input fields: "Email" containing "saul.jenkin@gmail.com", "Name" containing "Saul Jenkin", and "Notification Type" which is a multi-select dropdown showing "Critical", "Recommendation", and "Error". At the bottom are two buttons: "Add New Recipient" and "Cancel".

2. 輸入姓名、電子郵件地址、然後選取收件者要接收的通知類型、然後按一下*「Add New Recipient*（新增收件者*）」。

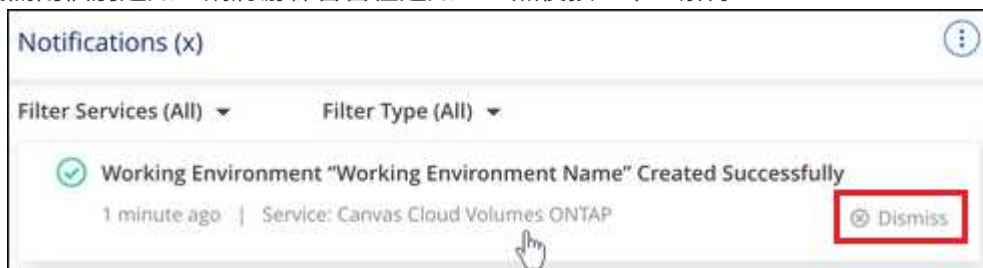
取消通知

如果您不再需要查看通知、可以從頁面移除通知。您可以一次關閉所有通知、也可以關閉個別通知。

若要關閉所有通知、請在通知中心按一下  並選擇*全部關閉*。



若要關閉個別通知、請將游標暫留在通知上、然後按一下「解除



稽核您帳戶中的使用者活動

Cloud Manager中的時間表顯示使用者完成的帳戶管理動作。這包括關聯使用者、建立工作區、建立連接器等管理動作。

如果您需要識別執行特定行動的人員、或是需要識別行動的狀態、檢查時間表會很有幫助。

步驟

1. 在Cloud Manager功能表列中、按一下*設定>時間軸*。
2. 在「篩選器」下、按一下「服務」、「啟用*佔用*」、然後按一下「套用」。

時間軸會更新以顯示帳戶管理動作。

角色

「帳戶管理員」、「工作區管理員」、「法規遵循檢視器」及SnapCenter「支援對象管理員」角色、可為使用者提供特定權限。

Compliance Viewer角色適用於唯讀的Cloud Data Sense存取。

工作	帳戶管理員	工作區管理	法規遵循檢視器	系統管理員SnapCenter
管理工作環境	是的	是的	否	否
在工作環境中啟用服務	是的	是的	否	否
檢視資料複寫狀態	是的	是的	否	否
檢視時間表	是的	是的	否	否
在工作區之間切換	是的	是的	是的	否
檢視資料感應掃描結果	是的	是的	是的	否
刪除工作環境	是的	否	否	否
將 Kubernetes 叢集連接至工作環境	是的	否	否	否
接收 Cloud Volumes ONTAP 此報告	是的	否	否	否
建立連接器	是的	否	否	否
管理NetApp帳戶	是的	否	否	否
管理認證資料	是的	否	否	否
修改 Cloud Manager 設定	是的	否	否	否
檢視及管理支援儀表板	是的	否	否	否
從 Cloud Manager 移除工作環境	是的	否	否	否
安裝 HTTPS 憑證	是的	否	否	否
使用SnapCenter《支援服務	是的	是的	否	是的

相關連結

- ["在NetApp帳戶中設定工作區和使用者"](#)
- ["管理NetApp帳戶中的工作區和使用者"](#)

連接器

進階部署

從AWS Marketplace建立連接器

最好直接從 Cloud Manager 建立 Connector 、但如果您不想指定 AWS 存取金鑰、可以從 AWS Marketplace 啟動 Connector 。建立並設定 Connector 之後、Cloud Manager 會在您建立新的工作環境時自動使用。

步驟

1. 在AWS中設定權限：
 - a. 從IAM主控台複製並貼上的內容、以建立您自己的原則 "[連接器的IAM原則](#)" 。
 - b. 建立角色類型為 Amazon EC2 的 IAM 角色、並將您在上一步建立的原則附加至角色。
2. 現在請前往 "[AWS Marketplace 上的 Cloud Manager 頁面](#)" 從 AMI 部署 Cloud Manager 。

IAM 使用者必須擁有 AWS Marketplace 權限才能訂閱及取消訂閱。

3. 在 Marketplace 頁面上、按一下 * 繼續訂閱 * 、然後按一下 * 繼續進行組態 * 。

a

es ▾ Delivery Methods ▾ Solutions ▾ Migration Mapping Assistant Your Saved List 2 Partners Sell in AWS Marketplace Amazon Web Services Home

NetApp

Cloud Manager - Manual Installation without access keys

By: [NetApp, Inc.](#) Latest Version: 3.8.4

Read below for instructions on how to deploy Cloud Volumes ONTAP.

Linux/Unix ★★★★★ 6 AWS reviews

[Continue to Subscribe](#)

[Save to List](#)

Typical Total Price
\$0.226/hr
Total pricing per instance for services hosted on t3.xlarge in US East (N. Virginia). [View Details](#)

Overview Pricing Usage Support Reviews

Product Overview

Do NOT subscribe on this page unless instructed by NetApp or redirected here from the NetApp website.

This listing lets you manually launch a Cloud Manager instance without providing your AWS credentials. After launching the Cloud Manager software in AWS, you can access it by entering the instance's IP address in a web browser. If you subscribe here, you still need to subscribe on the listing below for PAYGO charges.

Highlights

- See Product Overview for instructions on how to deploy NetApp Cloud Manager.

b

es ▾ Delivery Methods ▾ Solutions ▾ Migration Mapping Assistant Your Saved List 2 Partners Sell in AWS Marketplace Amazon Web Services Home

NetApp

Cloud Manager - Manual Installation without access keys

[Continue to Configuration](#)

[< Product Detail](#) [Subscribe](#)

Subscribe to this software

You're subscribed to this software. Please see the terms and pricing details below or click the button above to configure your software.

Terms and Conditions

NetApp, Inc. Offer

You have subscribed to this software and agreed that your use of this software is subject to the pricing terms and the seller's [End User License Agreement \(EULA\)](#). You agreed that AWS may share information about this transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the [AWS Privacy Notice](#). Your use of AWS services remains subject to the [AWS Customer Agreement](#) or other agreement with AWS governing your use of such services.

- 變更任何預設選項、然後按一下 * 繼續啟動 * 。
- 在「* 選擇行動 *」下、選取「* 透過 EC2* 啟動」、然後按一下「* 啟動 *」。

這些步驟說明如何從 EC2 主控台啟動執行個體、因為主控台可讓您將 IAM 角色附加至 Cloud Manager 執行個體。這無法使用 * 從網站啟動 * 動作。

- 依照提示設定及部署執行個體：
 - * 選擇執行個體類型 *：視區域可用度而定、請選擇其中一種支援的執行個體類型（建議使用 T3.xlarge）。

"檢閱執行個體需求"。

- * 設定執行個體 *：選取 VPC 和子網路、選擇您在步驟 1 中建立的 IAM 角色、啟用終止保護（建議）、並選擇符合您需求的任何其他組態選項。

Number of instances	1	Launch into Auto Scaling Group
Purchasing option	<input type="checkbox"/> Request Spot instances	
Network	vpc-a76d91c2 VPC4QA (default)	Create new VPC
Subnet	subnet-39536c13 QASubnet1 us-east-1b 155 IP Addresses available	Create new subnet
Auto-assign Public IP	Enable	
Placement group	<input type="checkbox"/> Add instance to placement group	
Capacity Reservation	Open	Create new Capacity Reservation
IAM role	Cloud_Manager	Create new IAM role
CPU options	<input type="checkbox"/> Specify CPU options	
Shutdown behavior	Stop	
Enable termination protection	<input checked="" type="checkbox"/> Protect against accidental termination	
Monitoring	<input type="checkbox"/> Enable CloudWatch detailed monitoring Additional charges apply.	

- * 新增儲存設備 *：保留預設的儲存選項。
- * 新增標記 *：視需要輸入執行個體的標記。
- * 設定安全性群組 *：指定連接器執行個體所需的連線方法：SSH、HTTP 和 HTTPS。
- * 審查 *：檢閱您的選擇、然後按一下 * 啟動 *。

AWS 會以指定的設定啟動軟體。Connector 執行個體和軟體應在大約五分鐘內執行。

- 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[]`

- 登入後、設定 Connector：

- 指定要與 Connector 建立關聯的 NetApp 帳戶。

"[瞭解 NetApp 客戶](#)"。

- 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"](#)。

從Azure Marketplace建立連接器

最好直接從 Cloud Manager 建立 Connector、但您也可以從 Azure Marketplace（如有需要）啟動 Connector。建立並設定 Connector 之後、Cloud Manager 會在您建立新的工作環境時自動使用。

在 Azure 中建立 Connector

使用Azure Marketplace中的映像部署Connector、然後登入Connector以指定您的NetApp帳戶。

步驟

1. 前往Azure Marketplace的NetApp Connector VM頁面。
 - ["適用於商業區域的Azure Marketplace頁面"](#)
 - ["Azure政府區域的Azure Marketplace頁面"](#)
2. 按一下「* 立即取得 *」、然後按一下「* 繼續 *」。
3. 從 Azure 入口網站按一下「* Create」（建立）*、然後依照步驟設定虛擬機器。

設定 VM 時請注意下列事項：

- Cloud Manager 可搭配 HDD 或 SSD 磁碟以最佳方式執行。
- 選擇符合 CPU 和 RAM 需求的 VM 大小。我們建議使用 DS3 v2。

["檢閱 VM 需求"](#)。

- 對於網路安全性群組、Connector 需要使用 SSH、HTTP 和 HTTPS 的傳入連線。

["深入瞭解 Connector 的安全性群組規則"](#)。

- 在「* 管理 *」下、選取「* 開啟 *」、為連接器啟用 * 系統指派的託管身分識別 *。

此設定非常重要、因為託管身分識別可讓 Connector 虛擬機器在 Azure Active Directory 中識別自己、而無需提供任何認證。["深入瞭解 Azure 資源的託管身分識別"](#)。

4. 在「* 檢閱 + 建立 *」頁面上、檢閱您的選擇、然後按一下「* 建立 *」開始部署。

Azure 以指定的設定部署虛擬機器。虛擬機器和 Connector 軟體應在大約五分鐘內執行。

5. 從連線至 Connector 虛擬機器的主機開啟網頁瀏覽器、然後輸入下列 URL：

`http://ipaddress:80[]`

6. 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。



現在已安裝並設定 Connector。您必須先授予 Azure 權限、使用者才能在 Cloud Volumes ONTAP Azure 中部署不必要的功能。

授予 Azure 權限

當您在 Azure 中部署 Connector 時、您應該已啟用 "[系統指派的託管身分識別](#)"。您現在必須建立自訂角色、然後將角色指派給 Connector 虛擬機器以進行一或多項訂閱、以授予必要的 Azure 權限。

步驟

1. 建立自訂角色：
 - a. 複製的內容 "[Connector 的自訂角色權限](#)" 並將它們儲存在 Json 檔案中。
 - b. 將 Azure 訂閱 ID 新增至可指派的範圍、以修改 Json 檔案。

您應該為使用者建立 Cloud Volumes ONTAP 的各個 Azure 訂閱新增 ID。

▪ 範例 *

```
"AssignableScopes": [  
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",  
  "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",  
  "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
```


- c. 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。

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



- 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 Cloud Manager 的自訂角色、可以指派給 Connector 虛擬機器。

2. 將角色指派給連接器虛擬機器以進行一或多項訂閱：

- a. 開啟 *「訂閱」* 服務、然後選取您要在其中部署 Cloud Volumes ONTAP 的訂閱。
- b. 按一下*存取控制 (IAM) >*新增>*新增角色指派*。
- c. 在「角色」索引標籤中、選取「* Cloud Manager operator*」角色、然後按一下「下一步」。



Cloud Manager 操作員是 Cloud Manager 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。

- d. 在「成員」索引標籤中、完成下列步驟：

- 指派*託管身分識別*的存取權。
- 按一下*選取成員*、選取建立連接器虛擬機器的訂閱、選擇*虛擬機器*、然後選取連接器虛擬機器。
- 按一下*選取*。
- 單擊 * 下一步 *。

e. 按一下「檢閱+指派」。

f. 如果您想要從 Cloud Volumes ONTAP 其他訂閱中部署、請切換至該訂閱、然後重複這些步驟。

Connector 現在擁有管理公有雲環境中資源和程序所需的權限。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"](#)。

在現有的Linux主機上安裝連接器、該主機可存取網際網路

建立 Connector 最常見的方法是直接從 Cloud Manager 或雲端供應商的市場建立 Connector。但您可以選擇在網路或雲端的現有 Linux 主機上下載並安裝 Connector 軟體。這些步驟僅適用於可存取網際網路的主機。

["瞭解部署Connector的其他方法"](#)。



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。

驗證主機需求

Connector 軟體必須在符合特定作業系統需求、RAM 需求、連接埠需求等的主機上執行。

需要專用主機

與其他應用程式共用的主機不支援 Connector。主機必須是專屬主機。

CPU

4 個核心或 4 個 vCPU

RAM

16 GB

AWS EC2 執行個體類型

符合上述 CPU 和 RAM 需求的執行個體類型。建議使用T3.xLarge。

Azure VM 大小

符合上述 CPU 和 RAM 需求的執行個體類型。我們建議使用 DS3 v2。

GCP 機器類型

符合上述 CPU 和 RAM 需求的執行個體類型。建議使用n1-Standard-4。

Google Cloud支援Connector的VM執行個體、其作業系統可支援此連接器 ["防護VM功能"](#)

支援的作業系統

- CentOS 7.6.
- CentOS 7.7
- CentOS 7.8
- CentOS 7.9
- Red Hat Enterprise Linux 7.6

- Red Hat Enterprise Linux 7.7
- Red Hat Enterprise Linux 7.8
- Red Hat Enterprise Linux 7.9

Red Hat Enterprise Linux 系統必須在 Red Hat 訂購管理中註冊。如果未登錄、系統將無法在 Connector 安裝期間存取儲存庫來更新所需的協力廠商軟體。

這些作業系統的英文版本支援 Connector。

Hypervisor

通過認證可執行 CentOS 或 Red Hat Enterprise Linux 的裸機或託管

Hypervisor<https://access.redhat.com/certified-hypervisors>["Red Hat 解決方案：哪些 Hypervisor 已通過認證、可執行 Red Hat Enterprise Linux ?"]

/opt 中的磁碟空間

必須有 100 GiB 的可用空間

/var 中的磁碟空間

必須提供 20 GiB 的空間

傳出網際網路存取

安裝 Connector 和 Connector 時、需要外傳網際網路存取、才能管理公有雲環境中的資源和程序。如需端點清單、請參閱 ["連接器的網路需求"](#)。

安裝 Connector

驗證是否有支援的 Linux 主機之後、您就可以取得 Connector 軟體、然後再進行安裝。

需要 root 權限才能安裝 Connector。

關於這項工作

- 安裝會安裝 AWS 命令列工具（awscli）、以啟用 NetApp 支援的還原程序。

如果您收到安裝 awscli 失敗的訊息、您可以放心忽略該訊息。無需使用工具、連接器即可順利運作。

- NetApp 支援網站上提供的安裝程式可能是較早的版本。安裝後、如果有新版本可用、Connector 會自動自行更新。

步驟

1. 從下載 Cloud Manager 軟體 ["NetApp 支援網站"](#)，然後將其複製到 Linux 主機。

如需將檔案連線及複製到 AWS 中 EC2 執行個體的說明、請參閱 ["AWS 文件：使用 SSH 連線至 Linux 執行個體"](#)。

2. 指派執行指令碼的權限。

```
chmod +x OnCommandCloudManager-V3.9.19.sh
```

3. 執行安裝指令碼。

如果您有Proxy伺服器、則必須輸入命令參數、如下所示。安裝程式不會提示您提供Proxy的相關資訊。

```
./OnCommandCloudManager-V3.9.19.sh [silent] [proxy=ipaddress]  
[proxyport=port] [proxyuser=user_name] [proxypwd=password]
```

silent 在不提示您提供資訊的情況下執行安裝。

如果主機位於 Proxy 伺服器之後、則需要 *proxy*。

proxyport 是 Proxy 伺服器的連接埠。

proxyuser 是 Proxy 伺服器的使用者名稱（如果需要基本驗證）。

proxypwd 是您指定之使用者名稱的密碼。

4. 除非您指定無聲參數、否則請輸入 *Y* 繼續安裝。

Cloud Manager 現已安裝。安裝結束時、如果您指定 Proxy 伺服器、Cloud Manager 服務（occm）會重新啟動兩次。

5. 開啟網頁瀏覽器並輸入下列 URL：

<https://ipaddress/>

ipaddress 可以是 localhost、私有 IP 位址或公有 IP 位址、視主機的組態而定。例如、如果連接器位於沒有公有 IP 位址的公有雲中、您必須輸入連接至連接器主機之主機的私有 IP 位址。

6. 請在 NetApp Cloud Central 註冊或登入。

7. 如果您在 Google Cloud 中安裝 Connector、請設定具有 Cloud Manager 所需權限的服務帳戶、以便在 Cloud Volumes ONTAP 專案中建立及管理各種系統。

- "[在 GCP 中建立角色](#)" 這包括在中定義的權限 "[GCP的連接器原則](#)"。
- "[建立 GCP 服務帳戶、並套用您剛建立的自訂角色](#)"。
- "[將此服務帳戶與 Connector VM 建立關聯](#)"。
- 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。

8. 登入之後、請設定 Cloud Manager：

- 指定要與 Connector 建立關聯的 NetApp 帳戶。

"[瞭解 NetApp 客戶](#)"。

- 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。

設定權限、讓 Cloud Manager 能夠管理公有雲環境中的資源和程序：

- AWS：["設定 AWS 帳戶、然後將其新增至 Cloud Manager"](#)
- Azure：["設定 Azure 帳戶、然後將其新增至 Cloud Manager"](#)
- Google Cloud：請參閱上述步驟7

在內部安裝**Connector**、無需網際網路存取

您可以將Connector安裝在無法存取網際網路的內部部署Linux主機上。接著您可以探索內部ONTAP 的支援叢集、在叢集之間複寫資料、使用Cloud Backup備份磁碟區、然後使用Cloud Data Sense進行掃描。

這些安裝說明特別適用於上述使用案例。["瞭解部署Connector的其他方法"](#)。

驗證主機需求

Connector 軟體必須在符合特定作業系統需求、RAM 需求、連接埠需求等的主機上執行。

需要專用主機

與其他應用程式共用的主機不支援 Connector。主機必須是專屬主機。

CPU

4 個核心或 4 個 vCPU

RAM

16 GB

支援的作業系統

- CentOS 7.6.
- CentOS 7.7
- CentOS 7.8
- CentOS 7.9
- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7
- Red Hat Enterprise Linux 7.8
- Red Hat Enterprise Linux 7.9

Red Hat Enterprise Linux 系統必須在 Red Hat 訂購管理中註冊。如果未登錄、系統將無法在 Connector 安裝期間存取儲存庫來更新所需的協力廠商軟體。

這些作業系統的英文版本支援 Connector。

Hypervisor

通過認證可執行 CentOS 或 Red Hat Enterprise Linux 的裸機或託管

Hypervisor<https://access.redhat.com/certified-hypervisors>["Red Hat 解決方案：哪些 Hypervisor 已通過認證、可執行 Red Hat Enterprise Linux ？"]

磁碟類型

需要SSD

/opt 中的磁碟空間

必須有100 GiB的可用空間

/var.中的磁碟空間

必須提供20 GiB的空間

Docker引擎

安裝Connector之前、主機上需要Docker Engine 19版或更新版本。"檢視安裝指示"。

安裝Connector

驗證是否有支援的Linux主機之後、您就可以取得Connector軟體、然後再進行安裝。

需要root權限才能安裝Connector。

步驟

1. 確認已啟用並執行Docker。

```
sudo systemctl enable docker && sudo systemctl start docker
```

2. 從下載 Cloud Manager 軟體 "[NetApp 支援網站](#)"。
3. 將安裝程式複製到Linux主機。
4. 指派執行指令碼的權限。

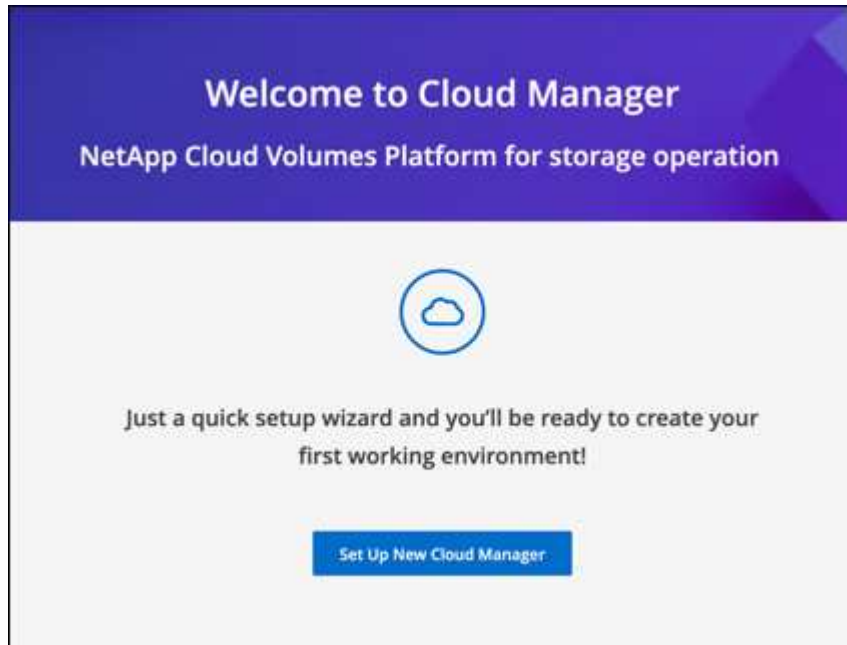
```
chmod +x /path/cloud-manager-connector-offline-v3.9.19
```

5. 執行安裝指令碼：

```
sudo /path/cloud-manager-connector-offline-v3.9.19
```

6. 開啟網頁瀏覽器並輸入 `https://ipaddress[]` 其中 `_ipaddress_` 是Linux主機的IP位址。

您應該會看到下列畫面。



7. 按一下*設定新的Cloud Manager*、然後依照提示設定系統。
 - 系統詳細資料：輸入Cloud Manager系統的名稱和公司名稱。

- 建立管理使用者：建立系統的管理使用者。

此使用者帳戶在本機系統上執行。無法連線至NetApp Cloud Central。

- 審查：檢閱詳細資料、接受授權合約、然後按一下*設定*。

8. 使用您剛建立的管理員使用者登入Cloud Manager。

現在已安裝Connector、您可以開始使用適用於黑暗站台部署的Cloud Manager功能。

接下來是什麼？#8217？

- "探索內部ONTAP 的叢集"
- "在內部ONTAP 的等量叢集之間複寫資料"
- "使用Cloud Backup將ONTAP 內部的等量資料備份StorageGRID 至不實"
- "使用ONTAP Cloud Data SENSE掃描內部的不全區資料"

當新版Connector軟體推出時、這些軟體將發佈至NetApp支援網站。"瞭解如何升級Connector"。

尋找連接器的系統ID

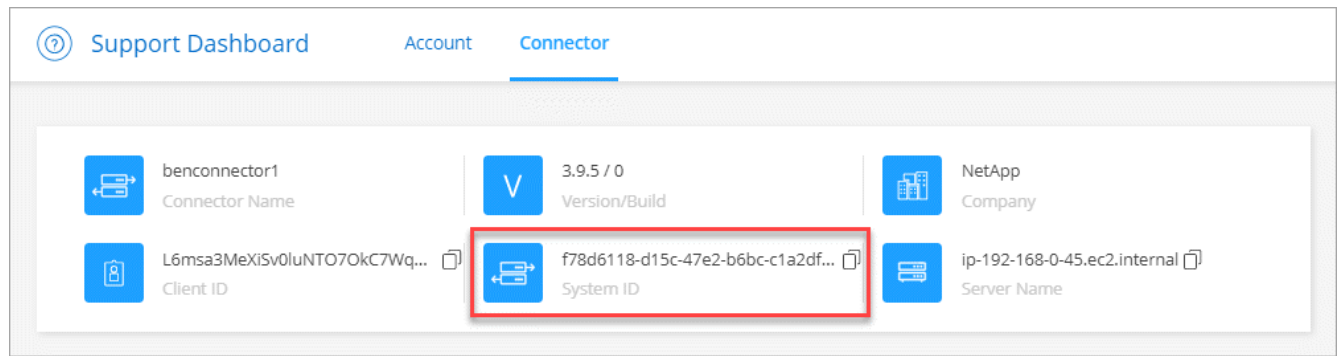
為協助您開始使用、NetApp代表可能會要求您提供Connector的系統ID。此 ID 通常用於授權和疑難排解。

步驟

1. 在 Cloud Manager 主控台右上角、按一下「說明」圖示。
2. 按一下*支援> Connector*。

系統ID會顯示在頂端。

- 範例 *



管理現有的連接器

建立一或多個連接器之後、您可以在連接器之間切換、連線至連接器上執行的本機使用者介面等、來管理連接器。

在連接器之間切換

如果您有多個連接器、可以在它們之間切換、以查看與特定連接器相關聯的工作環境。

例如、假設您是在多個雲端環境中工作。您可能在 AWS 中有一個 Connector、在 Google Cloud 中有一個 Connector。您必須在這些連接器之間切換、才能管理 Cloud Volumes ONTAP 在雲端上執行的各種功能。

步驟

1. 按一下「* Connector*（* 連接器 *）」下拉式清單、選取「Another Connector（另一個連接器）」、然後按一下「* Switch*」



Cloud Manager 會重新整理並顯示與所選 Connector 相關的工作環境。

存取本機UI

雖然您應該從 SaaS 使用者介面執行幾乎所有的工作、但連接器上仍有本機使用者介面可供使用。如果您是從政府區域或沒有外傳網際網路存取的網站存取Cloud Manager、則必須使用連接器上執行的本機使用者介面。

步驟

1. 開啟網頁瀏覽器並輸入下列 URL：

`https://ipaddress[]`

ipaddress 可以是 localhost、私有 IP 位址或公有 IP 位址、視主機的組態而定。例如、如果連接器位於沒有公有 IP 位址的公有雲中、您必須輸入連接至連接器主機之主機的私有 IP 位址。

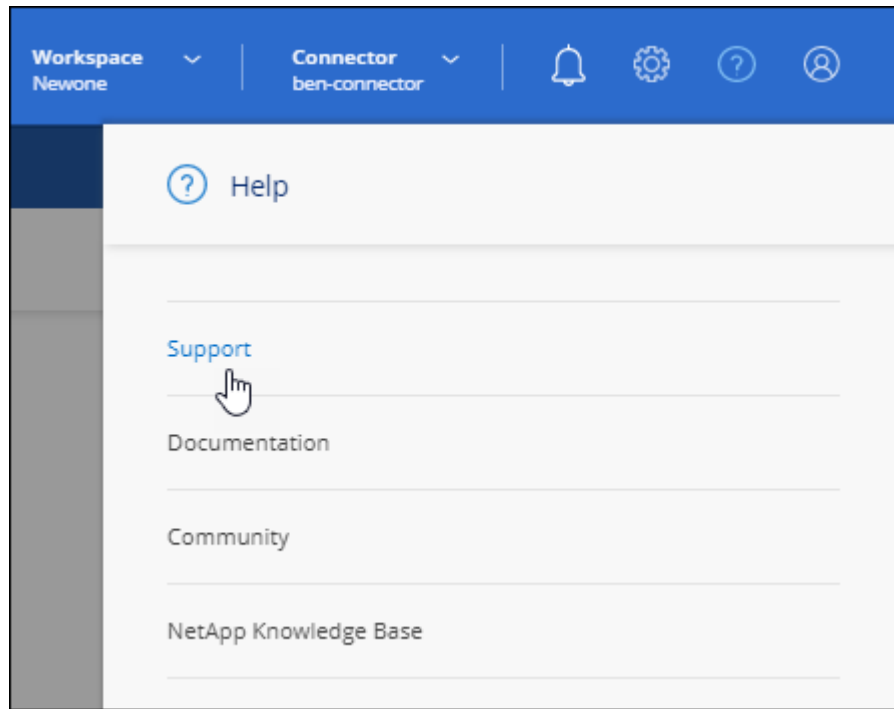
2. 輸入您的使用者名稱和密碼以登入。

下載AutoSupport 或傳送更新訊息

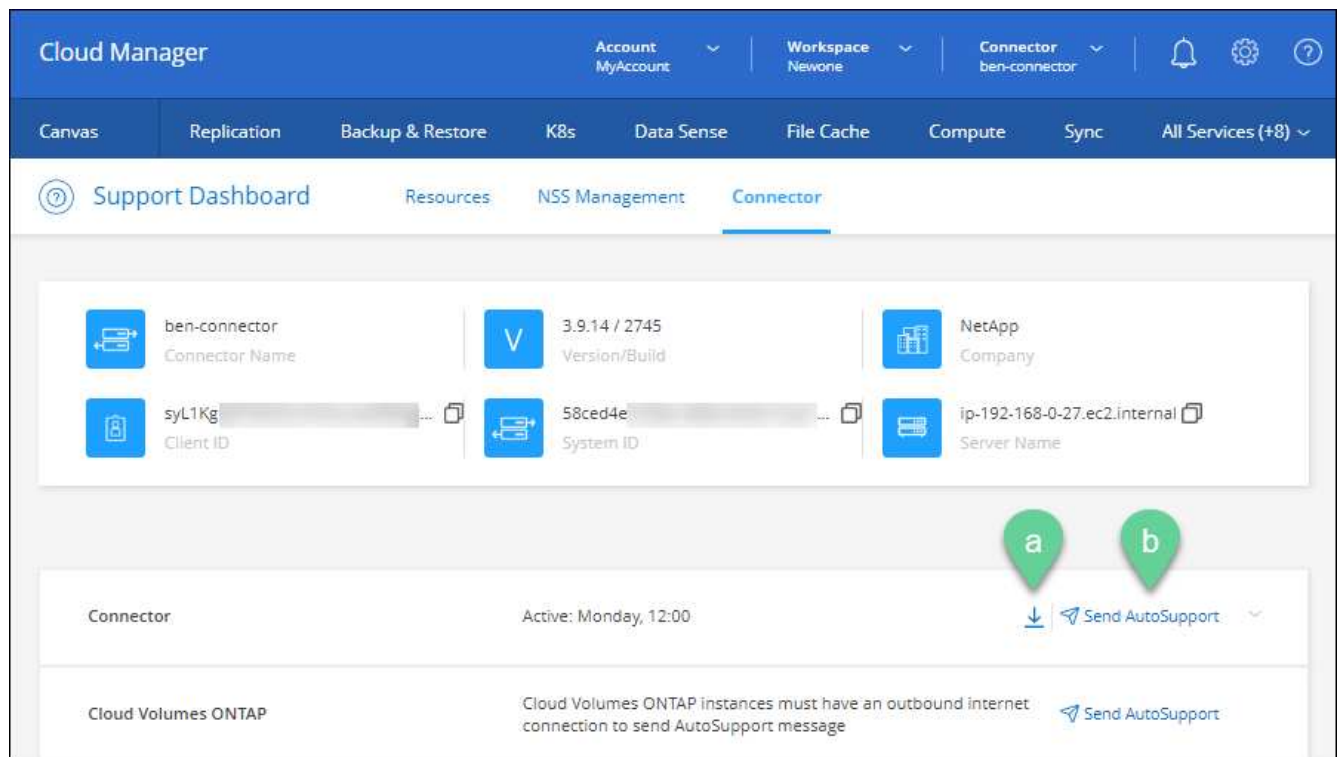
如果您有任何問題、NetApp人員可能會要求您傳送AutoSupport 一份關於解決疑難的消息給NetApp支援部門。

步驟

1. 連接到連接器本機UI、如前節所述。
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 * Connector* 。
4. 根據您傳送資訊給NetApp支援部門的方式、請選擇下列其中一個選項：
 - a. 選取選項、將AutoSupport 此資訊下載到您的本機機器。然後、您可以使用偏好的方法將其傳送給NetApp支援部門。
 - b. 按一下「傳送**AutoSupport S編**」、直接將訊息傳送給NetApp支援部門。



連線至Linux VM

如果您需要連線至執行Connector的Linux VM、可以使用雲端供應商提供的連線選項來執行。

AWS

在AWS中建立Connector執行個體時、您提供了AWS存取金鑰和秘密金鑰。您可以將此金鑰配對用於執行個體的SSH。

["AWS文件：連線至您的Linux執行個體"](#)

Azure

在Azure中建立Connector VM時、您選擇使用密碼或SSH公開金鑰進行驗證。使用您選擇的驗證方法來連線至VM。

["Azure文件：SSH進入VM"](#)

Google Cloud

在Google Cloud中建立Connector時、您無法指定驗證方法。不過、您可以使用Google Cloud Console或Google Cloud CLI (gcloud) 連線至Linux VM執行個體。

["Google Cloud Docs：連線至Linux VM"](#)

套用安全性更新

更新Connector上的作業系統、確保其已安裝最新的安全性更新。

步驟

1. 存取Connector主機上的CLI Shell。
2. 以提高的權限執行下列命令：

```
sudo -s
service service-manager stop
yum -y update --security
service service-manager start
```

變更連接器的IP位址

如果貴企業需要、您可以變更由雲端供應商自動指派之Connector執行個體的內部IP位址和公有IP位址。

步驟

1. 依照雲端供應商的指示、變更連接器執行個體的本機IP位址或公有IP位址（或兩者）。
2. 如果您變更了公有IP位址、而且需要連線至連接器上執行的本機使用者介面、請重新啟動連接器執行個體、以Cloud Manager登錄新的IP位址。
3. 如果您變更了私有IP位址、請更新Cloud Volumes ONTAP 支援的還原組態檔案備份位置、以便將備份傳送到Connector上的新私有IP位址。

- a. 從Cloud Volumes ONTAP 支援的CLI執行下列命令、以移除目前的備份目標：

```
system configuration backup settings modify -destination ""
```

- b. 前往Cloud Manager、開啟工作環境。
- c. 按一下功能表、然後選取*進階>組態備份*。
- d. 按一下*設定備份目標*。

編輯連接器的URI

新增及移除連接器的URI。

步驟

1. 按一下Cloud Manager標頭中的* Connector*下拉式清單。
2. 按一下「管理連接器」。
3. 按一下連接器的動作功能表、然後按一下*編輯URI*。
4. 新增及移除URI、然後按一下「套用」。

修正使用Google Cloud NAT閘道時的下載失敗

Connector會自動下載Cloud Volumes ONTAP 適用於更新的軟體。如果您的組態使用Google Cloud NAT閘道、下載可能會失敗。您可以限制軟體映像分成的零件數量來修正此問題。此步驟必須使用Cloud Manager API完成。

步驟

1. 將PUT要求提交至/occm/config、並以下列Json做為本文：

```
{
  "maxDownloadSessions": 32
}
```

_MaxDownloadSessions_的值可以是1或任何大於1的整數。如果值為1、則下載的映像不會分割。

請注意、32為範例值。您應該使用的值取決於NAT組態和可同時使用的工作階段數目。

["深入瞭解/occm/config API呼叫"](#)。

升級內部部署的Connector、不需存取網際網路

如果您 ["將Connector安裝在無法存取網際網路的內部部署主機上"](#)、您可以在NetApp支援網站提供較新版本時升級Connector。

在升級過程中、連接器需要重新啟動、以便在升級期間無法使用使用者介面。

步驟

1. 從下載 Cloud Manager 軟體 "[NetApp 支援網站](#)"。
2. 將安裝程式複製到Linux主機。
3. 指派執行指令碼的權限。

```
chmod +x /path/cloud-manager-connector-offline-v3.9.14
```

4. 執行安裝指令碼：

```
sudo /path/cloud-manager-connector-offline-v3.9.14
```

5. 升級完成後、您可以前往*「Help」（說明）>「Support」（支援）>「Connector*」（連接器*）來驗證連接器的版本。

在可存取網際網路的主機上進行軟體升級呢？

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。

從Cloud Manager移除Connectors

如果連接器處於非作用中狀態、您可以將其從 Cloud Manager 的連接器清單中移除。如果您刪除了 Connector 虛擬機器、或是卸載了 Connector 軟體、則可以這麼做。

請注意下列關於移除連接器的事項：

- 此動作不會刪除虛擬機器。
- 此動作無法還原、只要從 Cloud Manager 移除 Connector、就無法將其新增回 Cloud Manager。

步驟

1. 按一下Cloud Manager標頭中的* Connector*下拉式清單。
2. 按一下「管理連接器」。
3. 按一下非作用中連接器的動作功能表、然後按一下 * 移除連接器 *。



4. 輸入要確認的連接器名稱、然後按一下「移除」。

Cloud Manager 會將 Connector 從記錄中移除。

解除安裝Connector軟體

解除安裝Connector軟體以疑難排解問題、或從主機上永久移除軟體。您需要使用的步驟取決於連接器是安裝在可存取網際網路的主機上、還是安裝在無法存取網際網路的受限網路中。

從可存取網際網路的主機解除安裝

線上連接器包含一個解除安裝指令碼、可用來解除安裝軟體。

步驟

1. 從 Linux 主機執行解除安裝指令碼：
 - `/opt/application/NetApp/cloudmanager/in/uninstall.sh [silined]*`

silon 執行指令碼時不會提示您確認。

從無法存取網際網路的主機解除安裝

如果您從NetApp支援網站下載Connector軟體、並將其安裝在無法存取網際網路的受限網路中、請使用這些命令。

步驟

1. 從Linux主機執行下列命令：

```
docker-compose -f /opt/application/netapp/ds/docker-compose.yml down -v  
rm -rf /opt/application/netapp/ds
```

管理 HTTPS 憑證以確保安全存取

根據預設、Cloud Manager 會使用自我簽署的憑證來存取 Web 主控台的 HTTPS。您可以安裝由憑證授權單位（CA）簽署的憑證、以提供比自我簽署憑證更好的安全保護。

開始之前

您必須先建立連接器、才能變更 Cloud Manager 設定。"瞭解方法"。

安裝 HTTPS 憑證

安裝由 CA 簽署的憑證、以確保安全存取。

步驟

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



2. 在「HTTPS 設定」頁面中、產生憑證簽署要求（CSR）或安裝您自己的 CA 簽署憑證來安裝憑證：

選項	說明
產生 CSR	<ol style="list-style-type: none">a. 輸入連接器主機的主機名稱或 DNS（其一般名稱）、然後按一下 * 產生 csr*。Cloud Manager 會顯示憑證簽署要求。b. 使用 CSR 將 SSL 憑證要求提交給 CA。憑證必須使用隱私增強型郵件（PEF）Base - 64 編碼的 X · 509 格式。c. 上傳憑證檔案、然後按一下「安裝」。
安裝您自己的 CA 簽署憑證	<ol style="list-style-type: none">a. 選擇 * 安裝 CA 簽署的憑證*。b. 同時載入憑證檔案和私密金鑰、然後按一下「* 安裝*」。憑證必須使用隱私增強型郵件（PEF）Base - 64 編碼的 X · 509 格式。

Cloud Manager 現在使用 CA 簽署的憑證來提供安全的 HTTPS 存取。下圖顯示 Cloud Manager 系統的安全存取設定：



續約 Cloud Manager HTTPS 憑證

您應該在 Cloud Manager HTTPS 憑證過期之前更新、以確保安全存取 Cloud Manager 網路主控台。如果您在憑證到期之前未續約、當使用者使用 HTTPS 存取 Web 主控台時、會出現警告。

步驟

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

顯示 Cloud Manager 憑證的詳細資料、包括到期日。

2. 按一下*變更憑證*、然後依照步驟產生CSR或安裝您自己的CA簽署憑證。

Cloud Manager 使用新的 CA 簽署憑證來提供安全的 HTTPS 存取。

設定連接器以使用HTTP Proxy伺服器

如果您的企業原則要求您使用Proxy伺服器來進行所有的HTTP通訊至網際網路、則必須設定連接器以使用該HTTP Proxy伺服器。Proxy 伺服器可以位於雲端或網路中。

Cloud Manager不支援使用連接器的HTTPS Proxy。

在連接器上啟用Proxy

當您將連接器設定為使用 Proxy 伺服器、連接器及 Cloud Volumes ONTAP 其所管理的各種系統（包括任何 HA 協調器）時、都會使用 Proxy 伺服器。

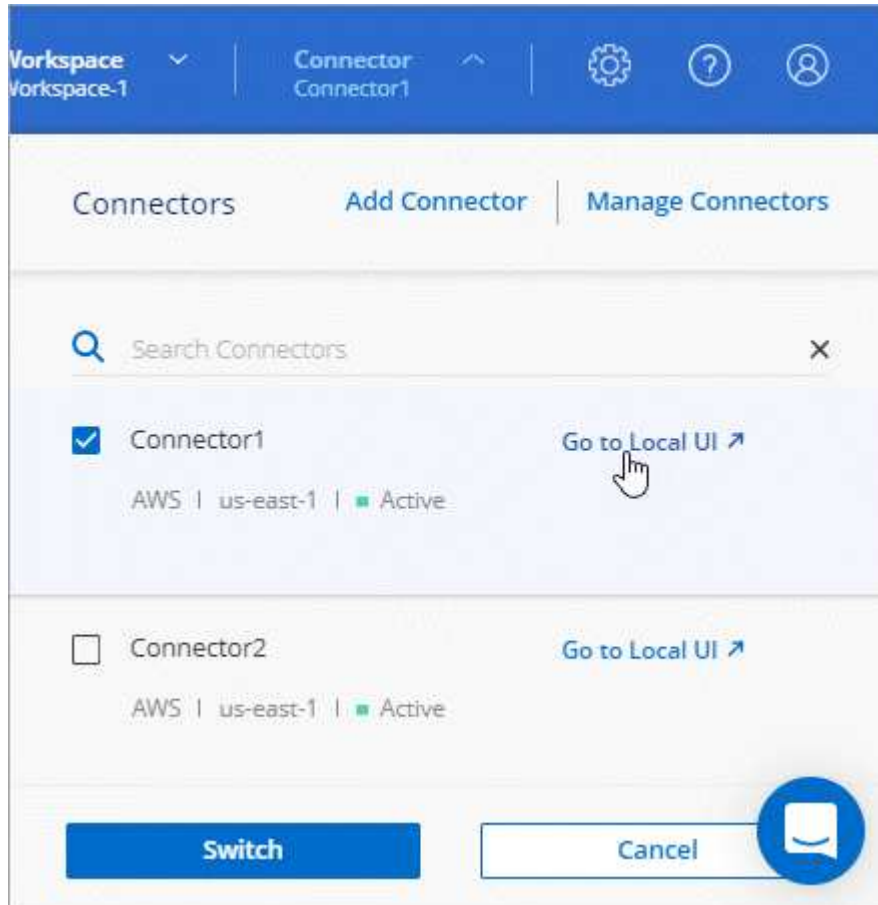
請注意、此作業會重新啟動Connector。在繼續之前、請確定Connector未執行任何作業。

步驟

1. "登入 Cloud Manager SaaS 介面" 從連線至連接器執行個體的機器。

如果連接器沒有公有 IP 位址、您將需要 VPN 連線、或是需要從連接器所在的同一個網路中的跨接主機連線。

2. 按一下「* Connector* (* 連接器 *)」下拉式清單、然後按一下「* 移至本機 Ui* (針對特定連接器)」。



在 Connector 上執行的 Cloud Manager 介面會載入新的瀏覽器索引標籤。

3. 在Cloud Manager主控台右上角、按一下「設定」圖示、然後選取「連接器設定」。



4. 按一下「一般」下的「* HTTP Proxy組態*」。
5. 設定Proxy：
 - a. 按一下*啟用Proxy*。
 - b. 使用語法指定伺服器 `http://address:port[]`
 - c. 如果伺服器需要基本驗證、請指定使用者名稱和密碼
 - d. 按一下「* 儲存 *」。



Cloud Manager 不支援包含 @ 字元的密碼。

指定 Proxy 伺服器之後、系統 Cloud Volumes ONTAP 會自動設定新的更新功能、讓您在傳送 AutoSupport 更新訊息時使用 Proxy 伺服器。如果您在使用者建立 Cloud Volumes ONTAP 完整系統之前未指定 Proxy 伺服器、則他們必須使用 System Manager 在 AutoSupport 各個系統的「更新」選項中手動設定 Proxy 伺服器。

啟用直接API流量

如果您已設定Proxy伺服器、則可直接將API呼叫傳送至Cloud Manager、而無需透過Proxy。此選項受AWS、Azure或Google Cloud中執行的Connectors支援。

步驟

1. 在Cloud Manager主控台右上角、按一下「設定」圖示、然後選取「連接器設定」。



2. 在* General 下、按一下 Support Direct API Traffic *。
3. 按一下核取方塊以啟用選項、然後按一下*「Saved*」。

Connector 的預設組態

您可能想要在部署連接器之前、或是需要疑難排解任何問題時、先深入瞭解連接器。

具備網際網路存取的預設組態

如果您是從Cloud Manager、雲端供應商的市場部署Connector、或是在可存取網際網路的內部部署Linux主機上手動安裝Connector、則適用下列組態詳細資料。

AWS詳細資料

如果您是從Cloud Manager或雲端供應商的市場部署Connector、請注意下列事項：

- EC2執行個體類型為T3.xLarge。
- 映像的作業系統為Red Hat Enterprise Linux 7.6 (HVM)。

作業系統不含 GUI。您必須使用終端機來存取系統。

- EC2 Linux執行個體的使用者名稱為EC2使用者。
- 預設的系統磁碟為50 GiB gp2磁碟。

Azure詳細資料

如果您是從Cloud Manager或雲端供應商的市場部署Connector、請注意下列事項：

- VM類型為DS3 v2。

- 映像的作業系統為CentOS 7.6。

作業系統不含 GUI。您必須使用終端機來存取系統。

- 預設系統磁碟為100 GiB優質SSD磁碟。

Google Cloud詳細資料

如果您是從Cloud Manager或雲端供應商的市場部署Connector、請注意下列事項：

- VM執行個體為n1-Standard-4。
- 映像的作業系統為CentOS 7.9。

作業系統不含 GUI。您必須使用終端機來存取系統。

- 預設系統磁碟為100 GiB SSD持續磁碟。

安裝資料夾

Connector 安裝資料夾位於下列位置：

/opt/application/NetApp/cloudmanager

記錄檔

記錄檔包含在下列資料夾中：

- /opt/application/NetApp/cloudmanager/log

此資料夾中的記錄提供有關Connector和Docker影像的詳細資料。

- /opt/application/netapp/cloudmanager/dock_occm/data/log

此資料夾中的記錄提供有關在Connector上執行雲端服務和Cloud Manager服務的詳細資料。

連接器服務

- Cloud Manager 服務的名稱為 occm。
- occm 服務取決於 MySQL 服務。

如果 MySQL 服務當機、則 occm 服務也會停機。

套件

Cloud Manager 會在 Linux 主機上安裝下列套件（如果尚未安裝）：

- 7Zip
- AWSCLI
- Docker
- Java

- Kubecl
- MySQL
- Tridentctl
- 拉出
- WGet

連接埠

連接器在 Linux 主機上使用下列連接埠：

- 80 （用於 HTTP 存取）
- 用於 HTTPS 存取的 443
- 適用於 Cloud Manager 資料庫的 3306
- 8080 for the Cloud Manager API Proxy
- 8666 、適用於 Service Manager API
- 8777 、適用於 Health 檢查器 Container Service API

預設組態、不含網際網路存取

如果您手動將Connector安裝在無法存取網際網路的內部部署Linux主機上、則適用下列組態。 ["深入瞭解此安裝選項"](#)。

- Connector 安裝資料夾位於下列位置：

`/opt/application/NetApp/DS`

- 記錄檔包含在下列資料夾中：

`/var/lib/docker/volumes/ds_occmdata/log`

此資料夾中的記錄提供有關Connector和Docker影像的詳細資料。

- 所有服務都在Docker容器內執行

這些服務取決於執行的Docker執行時間服務

- 連接器在 Linux 主機上使用下列連接埠：

- 80 （用於 HTTP 存取）
- 用於 HTTPS 存取的 443

AWS認證資料

AWS 認證與權限

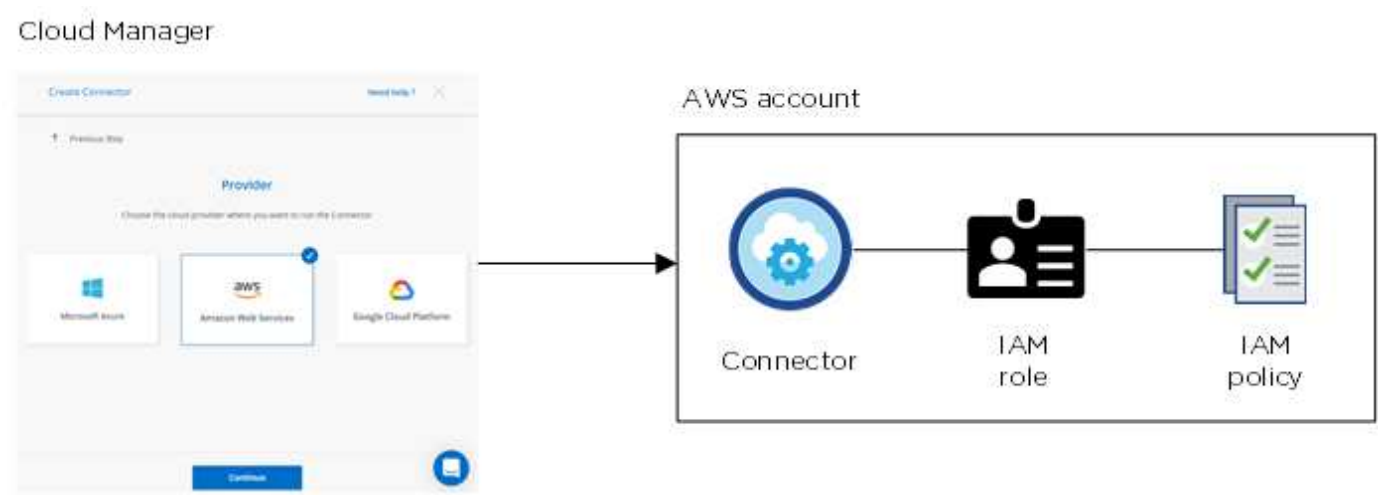
Cloud Manager 可讓您選擇部署 Cloud Volumes ONTAP 時要使用的 AWS 認證資料。您可以 Cloud Volumes ONTAP 使用初始 AWS 認證來部署所有的資訊系統、也可以新增其

他認證資料。

初始 **AWS** 認證資料

從Cloud Manager部署Connector時、您需要為IAM使用者提供IAM角色或存取金鑰的ARN。您使用的驗證方法必須具有必要的權限、才能在AWS中部署Connector執行個體。所需權限列於 ["AWS 的連接器部署原則"](#)。

Cloud Manager 在 AWS 中啟動 Connector 執行個體時、會為執行個體建立 IAM 角色和執行個體設定檔。它也附加原則、讓Connector有權限管理該AWS帳戶內的資源和程序。 ["檢閱 Cloud Manager 如何使用權限"](#)。



Cloud Manager 會在您為 Cloud Volumes ONTAP 下列項目建立新的工作環境時、依預設選取這些 AWS 認證資料：

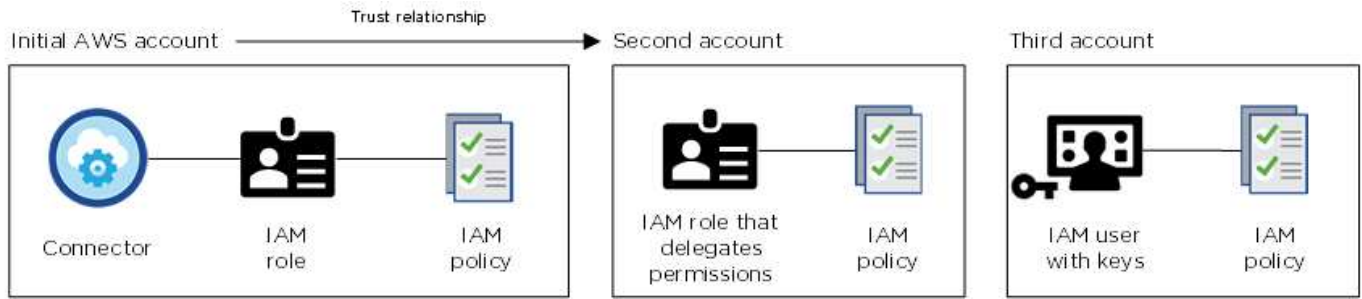
Details & Credentials			
Instance Profile		QA Subscription	Edit Credentials
Credentials	Account ID	Marketplace Subscription	

其他 **AWS** 認證資料

有兩種方法可以新增額外的AWS認證資料。

將**AWS**認證資料新增至現有的**Connector**

如果您想要在 Cloud Volumes ONTAP 不同的 AWS 帳戶中啟動功能、您也可以選擇 ["為 IAM 使用者或信任帳戶角色的 ARN 提供 AWS 金鑰"](#)。下圖顯示兩個額外的帳戶、一個透過信任帳戶中的 IAM 角色提供權限、另一個則透過 IAM 使用者的 AWS 金鑰提供權限：



您可以 "將帳戶認證新增至 [Cloud Manager](#)" 指定 IAM 角色的 Amazon 資源名稱（ARN）或 IAM 使用者的 AWS 金鑰。

新增一組認證資料之後、您可以在建立新的工作環境時切換至這些認證資料：

Edit Credentials & Add Subscription

Associate Subscription to Credentials ⓘ

Credentials

- keys | Account ID: [redacted]
- Instance Profile | Account ID: [redacted]
- casaba QA subscription

+ Add Subscription

Apply Cancel

直接將**AWS**認證資料新增至**Cloud Manager**

將新的AWS認證資料新增至Cloud Manager、可讓Cloud Manager擁有必要的權限、以建立和管理適用於ONTAP 整個作業環境的FSX、或是建立Connector。

Marketplace 部署和內部部署呢？

以上各節說明建議的連接器部署方法、該方法來自 Cloud Manager。您也可以從部署 AWS 中的 Connector ["AWS Marketplace"](#) 您也可以 ["在內部部署安裝連接器"](#)。

如果您使用 Marketplace、則會以相同方式提供權限。您只需要手動建立和設定 IAM 角色、然後為任何其他帳戶提供權限。

對於內部部署、您無法為 Cloud Manager 系統設定 IAM 角色、但您可以像提供額外 AWS 帳戶一樣提供權限。

我該如何安全地旋轉 **AWS** 認證資料？

如上所述、Cloud Manager 可讓您以幾種方式提供 AWS 認證資料：與 Connector 執行個體相關的 IAM 角色、在信任的帳戶中擔任 IAM 角色、或提供 AWS 存取金鑰。

Cloud Manager 採用前兩個選項、使用 AWS 安全性權杖服務取得持續循環的暫用認證資料。此程序是最佳實務做法、它是自動且安全的。

如果您為 Cloud Manager 提供 AWS 存取金鑰、您應該定期在 Cloud Manager 中更新金鑰、藉此旋轉金鑰。這是完全手動的程序。

管理**AWS**認證資料和**Cloud Manager**訂閱

新增及管理AWS認證資料、讓Cloud Manager擁有在AWS帳戶中部署及管理雲端資源所需的權限。如果您管理多個 AWS 訂閱、您可以從「認證」頁面將每個訂閱指派給不同的 AWS 認證資料。

總覽

您可以將AWS認證資料新增至現有的Connector、或直接新增至Cloud Manager：

- 將額外的AWS認證資料新增至現有的Connector

將新的AWS認證資料新增至現有的Connector、可讓您Cloud Volumes ONTAP 使用相同的Connector在另一個AWS帳戶中部署。 [瞭解如何將AWS認證資料新增至Connector](#)。

- 將AWS認證資料新增至Cloud Manager以建立Connector

將新的AWS認證資料新增至Cloud Manager、可讓Cloud Manager擁有建立Connector所需的權限。 [瞭解如何將AWS認證資料新增至Cloud Manager](#)。

- 將AWS認證資料新增至Cloud Manager for FSX ONTAP for S

將新的AWS認證資料新增至Cloud Manager、可讓Cloud Manager擁有必要的權限、以建立及管理FSX for ONTAP the S for。 ["瞭解如何設定FSX for ONTAP S for S for S for的權限"](#)

如何旋轉認證資料

Cloud Manager 可讓您以幾種方式提供 AWS 認證資料：與 Connector 執行個體相關的 IAM 角色、在信任的帳戶中擔任 IAM 角色、或提供 AWS 存取金鑰。 ["深入瞭解 AWS 認證與權限"](#)。

Cloud Manager 採用前兩個選項、使用 AWS 安全性權杖服務取得持續循環的暫用認證資料。此程序是最佳實務做法、因為它是自動且安全的。

如果您為 Cloud Manager 提供 AWS 存取金鑰、您應該定期在 Cloud Manager 中更新金鑰、藉此旋轉金鑰。這是完全手動的程序。

新增其他認證資料至**Connector**

將AWS認證資料新增至Connector、以便在Cloud Volumes ONTAP 其他AWS帳戶中部署及管理功能。您可以在其他帳戶中提供IAM角色的ARN、或是提供AWS存取金鑰。

授予權限

在您新增額外的AWS認證資料至Connector之前、您必須先提供必要的權限。這些權限可讓 Cloud Manager 管理該 AWS 帳戶內的資源和程序。您提供權限的方式取決於您是否要為Cloud Manager提供信任帳戶或AWS金鑰中角色的ARN。



當您從 Cloud Manager 部署 Connector 時、Cloud Manager 會自動為您部署 Connector 的帳戶新增 AWS 認證資料。如果您在現有系統上手動安裝 Connector 軟體、則不會新增此初始帳戶。"[深入瞭解 AWS 認證與權限](#)"。

- 選項 *
- [\[Grant permissions by assuming an IAM role in another account\]](#)
- [\[Grant permissions by providing AWS keys\]](#)

在另一個帳戶中擔任IAM角色、藉此授予權限

您可以使用 IAM 角色、在部署 Connector 執行個體的來源 AWS 帳戶與其他 AWS 帳戶之間建立信任關係。接著、您將從信任的帳戶中、為 Cloud Manager 提供 IAM 角色的 ARN。

步驟

1. 前往您要部署Cloud Volumes ONTAP 的目標帳戶中的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*、然後輸入連接器執行個體所在帳戶的ID。
 - 透過複製及貼上的內容來建立原則 "[連接器的IAM原則](#)"。
3. 複製IAM角色的角色ARN、以便稍後將其貼到Cloud Manager中。

帳戶現在擁有必要的權限。 [您現在可以將認證資料新增至Connector](#)。

提供AWS金鑰來授予權限

如果您想要為 IAM 使用者提供 AWS 金鑰給 Cloud Manager、則必須將必要的權限授予該使用者。Cloud Manager IAM 原則定義了允許 Cloud Manager 使用的 AWS 動作和資源。

步驟

1. 從IAM主控台複製並貼上的內容、以建立原則 "[連接器的IAM原則](#)"。

["AWS 文件：建立 IAM 原則"](#)

2. 將原則附加至 IAM 角色或 IAM 使用者。
 - ["AWS 文件：建立 IAM 角色"](#)
 - ["AWS 文件：新增和移除 IAM 原則"](#)

帳戶現在擁有必要的權限。 [您現在可以將認證資料新增至Connector](#)。

新增認證資料

在您提供具備所需權限的AWS帳戶之後、您可以將該帳戶的認證資料新增至現有的Connector。這可讓您Cloud Volumes ONTAP 使用相同的Connector在該帳戶中啟動支援功能。

如果您剛在雲端供應商中建立這些認證資料、可能需要幾分鐘的時間才能使用。請稍候幾分鐘、再將認證資料新增至Cloud Manager。

步驟

1. 請確定Cloud Manager目前已選取正確的Connector。
2. 在 Cloud Manager 主控台右上角、按一下「設定」圖示、然後選取 * 認證 *。



3. 按一下*「Add Credential*（新增認證*）」、然後依照精靈中的步驟進行。
 - a. 認證資料位置：選取* Amazon Web Services > Connector*。
 - b. 定義認證資料：提供可信IAM角色的ARN（Amazon資源名稱）、或輸入AWS存取金鑰和秘密金鑰。
 - c. 市場訂閱：立即訂閱或選取現有的訂閱、以建立Marketplace訂閱與這些認證的關聯。

若要以Cloud Volumes ONTAP 每小時費率（PAYGO）或是以年度合約支付、AWS認證資料必須與Cloud Volumes ONTAP 從AWS Marketplace訂閱的功能相關聯。

- d. 審查：確認新認證資料的詳細資料、然後按一下*新增*。

現在、您可以在建立新的工作環境時、從「詳細資料與認證」頁面切換至不同的認證資料集：

將認證資料新增至Cloud Manager以建立Connector

提供IAM角色的ARN、讓Cloud Manager擁有建立Connector所需的權限、藉此將AWS認證新增至Cloud Manager。您可以在建立新的Connector時選擇這些認證資料。

設定IAM角色

設定IAM角色、讓Cloud Manager SaaS能夠承擔角色。

步驟

1. 前往目標帳戶中的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的ID：952013314444。
- 建立包含建立Connector所需權限的原則。
 - ["檢視FSXfor ONTAP Sfor Sf哪些 權限"](#)
 - ["檢視Connector部署原則"](#)

3. 複製IAM角色的角色ARN、以便在下一步將其貼到Cloud Manager中。

IAM角色現在擁有所需的權限。 [您現在可以將它新增至 Cloud Manager](#)。

新增認證資料

在您提供IAM角色所需的權限之後、請將角色ARN新增至Cloud Manager。

如果您剛建立IAM角色、可能需要幾分鐘的時間才能使用。請稍候幾分鐘、再將認證資料新增至Cloud Manager。

步驟

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



2. 按一下*「Add Credential*（新增認證*）」、然後依照精靈中的步驟進行。
 - a. 認證資料位置：選取* Amazon Web Services > Cloud Manager*。
 - b. 定義認證資料：提供IAM角色的ARN（Amazon資源名稱）。
 - c. 審查：確認新認證資料的詳細資料、然後按一下*新增*。

您現在可以在建立新的Connector時使用認證資料。

建立AWS訂閱的關聯

將 AWS 認證資料新增至 Cloud Manager 之後、您可以將 AWS Marketplace 訂閱與這些認證資料建立關聯。訂閱可讓您以Cloud Volumes ONTAP 小時費率（PAYGO）或使用年度合約來支付報銷費用、並使用其他NetApp 雲端服務。

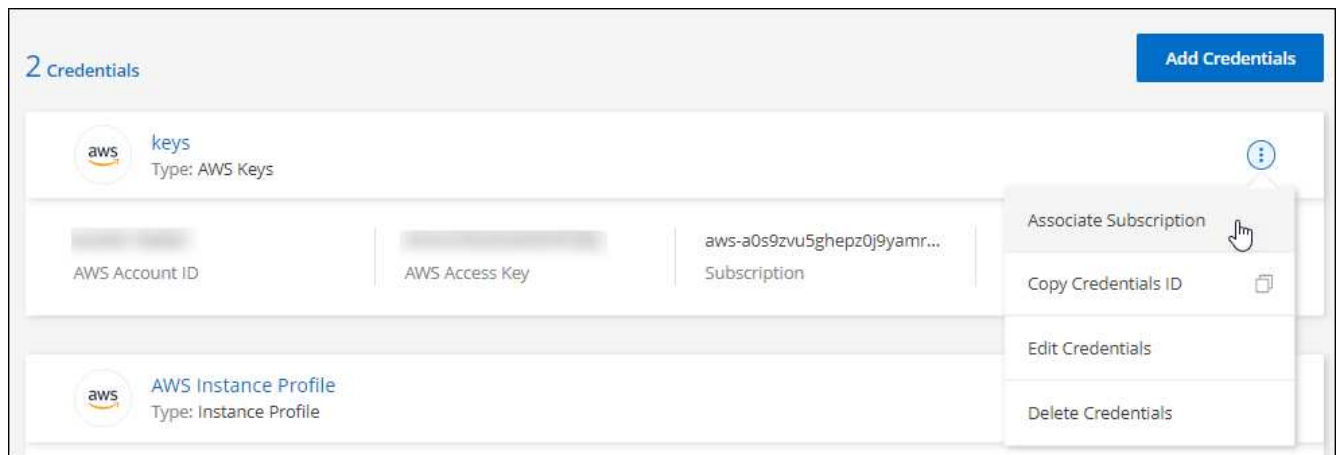
您可能會在將認證新增至 Cloud Manager 之後、在兩種情況下建立 AWS Marketplace 訂閱的關聯：

- 初次將認證新增至 Cloud Manager 時、您並未建立訂閱關聯。
- 您想要以新的訂閱取代現有的 AWS Marketplace 訂閱。

您必須先建立連接器、才能變更 Cloud Manager 設定。"瞭解如何建立連接器"。

步驟

1. 在 Cloud Manager 主控台右上角、按一下「設定」圖示、然後選取 * 認證 *。
2. 按一下動作功能表以取得一組認證資料、然後選取「建立訂閱關聯」。



3. 從下拉式清單中選取現有的訂閱、或按一下「新增訂閱」、然後依照步驟建立新的訂閱。

► https://docs.netapp.com/zh-tw/cloud-manager-setup-admin//media/video_subscribing_aws.mp4 (video)

編輯認證資料

在Cloud Manager中編輯AWS認證資料、方法是變更帳戶類型（AWS金鑰或承擔角色）、編輯名稱、或自行更新認證資料（金鑰或角色ARN）。



您無法編輯與Connector執行個體相關聯之執行個體設定檔的認證資料。

步驟

1. 在 Cloud Manager 主控台右上角、按一下「設定」圖示、然後選取 * 認證 *。
2. 按一下動作功能表以取得一組認證資料、然後選取*編輯認證*。
3. 進行必要的變更、然後按一下「套用」。

刪除認證資料

如果您不再需要一組認證資料、可以從Cloud Manager刪除。您只能刪除與工作環境無關的認證資料。



您無法刪除與連接器執行個體相關聯之執行個體設定檔的認證。

步驟

1. 在 Cloud Manager 主控台右上角、按一下「設定」圖示、然後選取 * 認證 * 。
2. 按一下動作功能表以取得一組認證資料、然後選取*刪除認證資料*。
3. 按一下*刪除*以確認。

Azure 認證

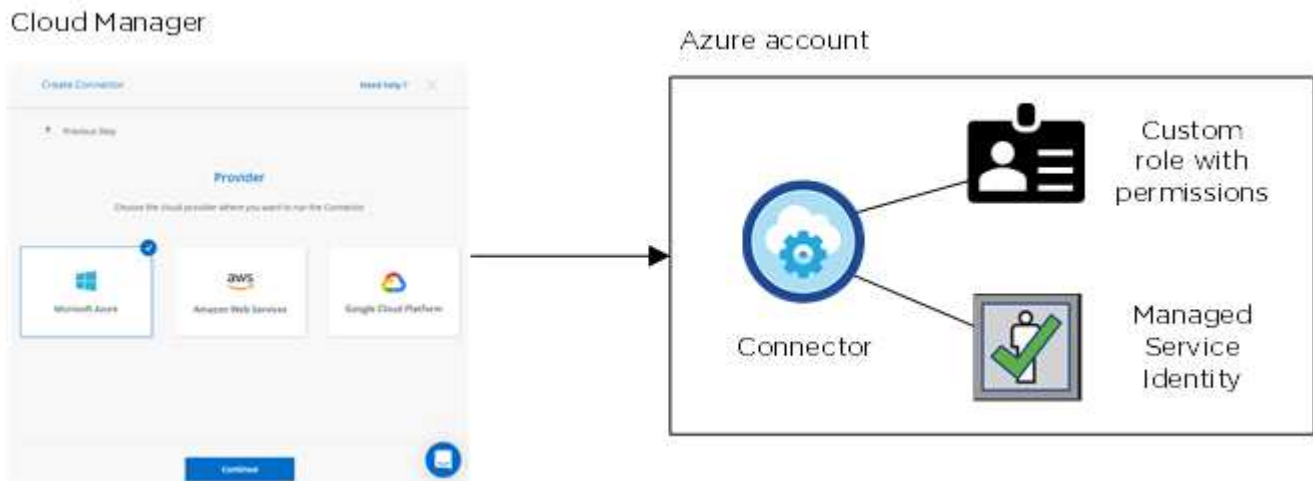
Azure 認證與權限

Cloud Manager 可讓您在部署 Cloud Volumes ONTAP 時選擇要使用的 Azure 認證資料。您可以 Cloud Volumes ONTAP 使用初始 Azure 認證來部署所有的整套系統、也可以新增其他認證資料。


Azure 初始認證

從Cloud Manager部署Connector時、您需要使用具備部署Connector虛擬機器權限的Azure帳戶或服務主體。所需權限列於 "[Azure 的連接器部署原則](#)" 。

當 Cloud Manager 在 Azure 中部署 Connector 虛擬機器時、就能實現 "[系統指派的託管身分識別](#)" 在虛擬機器上建立自訂角色、然後將其指派給虛擬機器。此角色可讓 Cloud Manager 在該 Azure 訂閱中管理資源和程序。 "[檢閱 Cloud Manager 如何使用權限](#)" 。



Cloud Manager 會在您為 Cloud Volumes ONTAP 下列項目建立新的工作環境時、依預設選取這些 Azure 認證資料：

Details & Credentials			
Managed Service Ide...	OCCM QA1	 No subscription is associated	Edit Credentials
Credential Name	Azure Subscription	Marketplace Subscription	

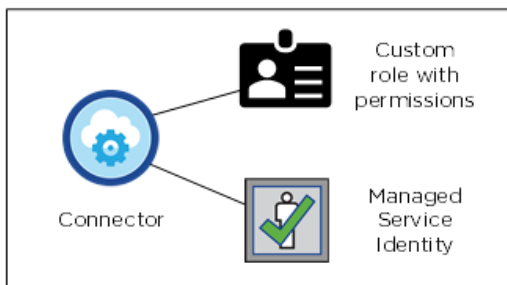
額外的 **Azure** 訂閱、提供託管身分識別

託管身分識別與您啟動 Connector 的訂閱相關聯。如果您想要選擇不同的 Azure 訂閱、則需要 ["將託管身分識別與這些訂閱建立關聯"](#)。

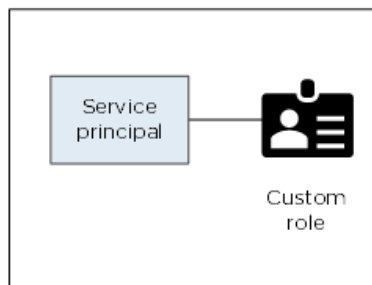
其他 **Azure** 認證資料

如果您要使用 Cloud Volumes ONTAP 不同的 Azure 認證資料來部署功能、則必須授予所需的權限 ["在 Azure Active Directory 中建立及設定服務主體"](#) 針對每個 Azure 帳戶。下圖顯示兩個額外的帳戶、每個帳戶都設有提供權限的服務主體和自訂角色：

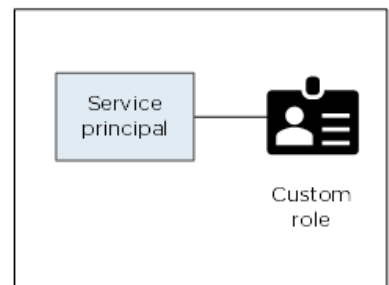
Initial Azure account



Second account



Third account



您可以 ["將帳戶認證新增至 Cloud Manager"](#) 提供 AD 服務主體的詳細資料。

新增一組認證資料之後、您可以在建立新的工作環境時切換至這些認證資料：

Edit Account & Add Subscription

Credentials

cloud-manager-app | Application ID: 57c42424-88a0-480a.

Managed Service Identity

OCCM QA1 (Default)

Marketplace 部署和內部部署呢？

以上各節說明推薦的 Connector 部署方法、該方法來自 NetApp Cloud Central。您也可以從部署連接器至 Azure ["Azure Marketplace"](#) 您也可以 ["在內部部署安裝連接器"](#)。

如果您使用 Marketplace、則會以相同方式提供權限。您只需要手動建立及設定 Connector 的託管身分識別、然後為任何其他帳戶提供權限。

對於內部部署、您無法設定 Connector 的託管身分識別、但您可以像使用服務主體一樣提供額外帳戶的權限。

管理 Azure 認證與 Cloud Manager 訂閱

當您建立 Cloud Volumes ONTAP 一個功能完善的系統時、您需要選取 Azure 認證資料、才能與該系統搭配使用。如果您使用隨用隨付授權、也需要選擇 Marketplace 訂閱。如果您需要使用多個 Azure 認證或多個 Azure Marketplace 訂閱 Cloud Volumes ONTAP 以供使用、請依照本頁的步驟進行。

有兩種方法可在 Cloud Manager 中新增額外的 Azure 訂閱和認證資料。

1. 將額外的 Azure 訂閱與 Azure 託管身分識別建立關聯。
2. 如果您要使用 Cloud Volumes ONTAP 不同的 Azure 認證資料來部署功能、請使用服務主體來授予 Azure 權限、並將其認證資料新增至 Cloud Manager。

將額外的 **Azure** 訂閱與託管身分識別建立關聯

Cloud Manager 可讓您選擇要部署 Cloud Volumes ONTAP 的 Azure 認證和 Azure 訂閱。除非您建立關聯、否則您無法為託管身分識別設定檔選取不同的 Azure 訂閱 ["託管身分識別"](#) 這些訂閱。

託管身分識別是 ["初始 Azure 帳戶"](#) 當您從 Cloud Manager 部署 Connector 時。部署 Connector 時、Cloud Manager 會建立 Cloud Manager 操作員角色、並將其指派給 Connector 虛擬機器。

步驟

1. 登入 Azure 入口網站。
2. 開啟 * 訂閱 * 服務、然後選取您要部署 Cloud Volumes ONTAP 的訂閱內容。
3. 按一下 * 存取控制 (IAM) *。
 - a. 按一下「* 新增 * > * 新增角色指派 *」、然後新增權限：
 - 選取 * Cloud Manager operator * 角色。



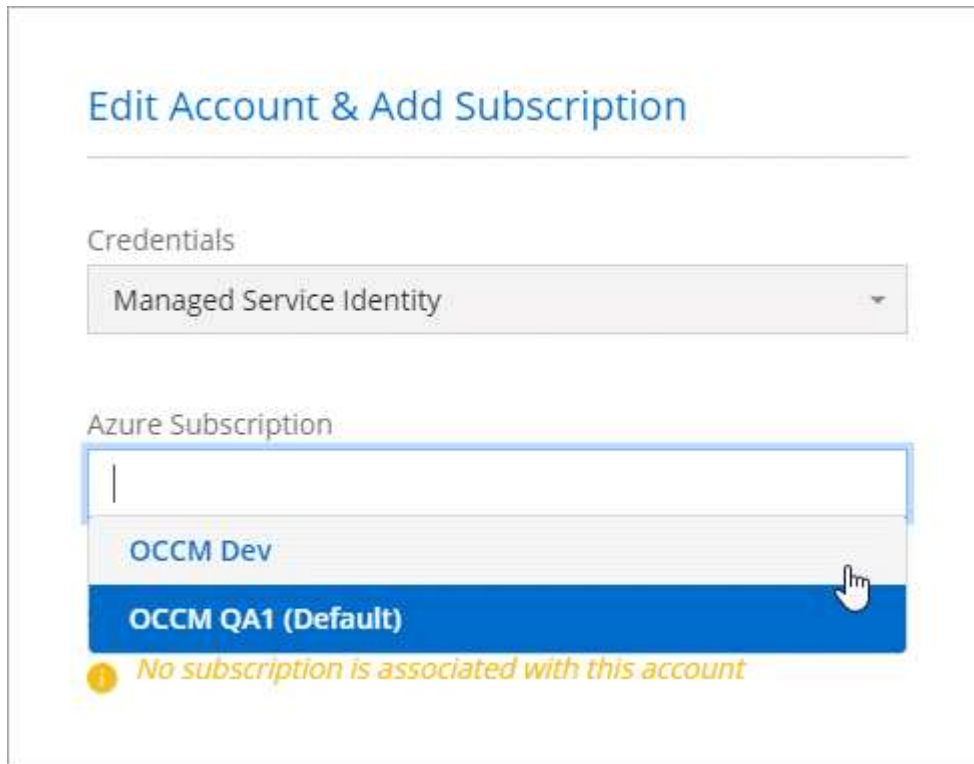
Cloud Manager 運算子是 Connector 原則中提供的預設名稱。如果您為角色選擇不同的名稱、請改為選取該名稱。

- 指派 * 虛擬機器 * 的存取權。
- 選取建立 Connector 虛擬機器的訂閱。
- 選取 Connector 虛擬機器。

- 按一下「* 儲存 *」。

4. 請重複這些步驟以取得額外訂閱內容。

當您建立新的工作環境時、現在應該能夠從多個 Azure 訂閱中選取託管身分識別設定檔。



將額外的Azure認證資料新增至Cloud Manager

當您從Cloud Manager部署Connector時、Cloud Manager會在擁有必要權限的虛擬機器上、啟用系統指派的託管身分識別。Cloud Manager會在您建立Cloud Volumes ONTAP 全新的作業系統以供參考時、依預設選取這些Azure認證資料。



如果您在現有系統上手動安裝Connector軟體、則不會新增一組初始認證資料。"[瞭解Azure認證與權限](#)"。

如果您要使用Cloud Volumes ONTAP _different_ Azure認證來部署功能、則必須在Azure Active Directory中為每個Azure帳戶建立及設定服務主體、以授予必要的權限。然後您可以將新認證新增至Cloud Manager。

使用服務主體授予 Azure 權限

Cloud Manager 需要權限才能在 Azure 中執行動作。您可以在 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、將必要的權限授予 Azure 帳戶。

下圖說明 Cloud Manager 如何取得在 Azure 中執行作業的權限。與一或多個 Azure 訂閱相關聯的服務主體物件、代表 Azure Active Directory 中的 Cloud Manager、並指派給允許必要權限的自訂角色。



步驟

1. 建立 Azure Active Directory 應用程式。
2. 將應用程式指派給角色。
3. 新增 Windows Azure Service Management API 權限。
4. 取得應用程式 ID 和目錄 ID。
5. 建立用戶端機密。

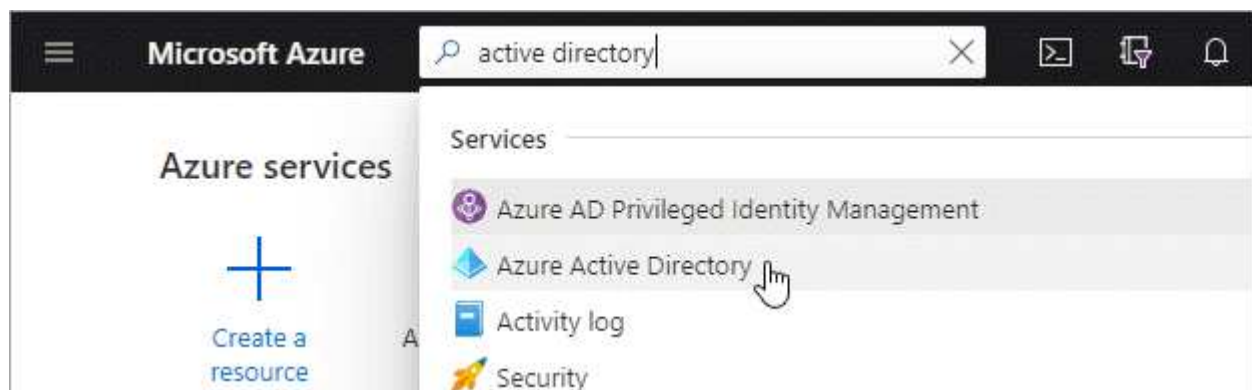
建立 Azure Active Directory 應用程式

建立 Azure Active Directory （AD）應用程式與服務主體、讓 Cloud Manager 可用於角色型存取控制。

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

您必須將服務委託人繫結至一或多個 Azure 訂閱、並指派自訂的「OnCommand 支援對象」角色給該委託人、以便 Cloud Manager 在 Azure 中擁有權限。

步驟

1. 建立自訂角色：
 - a. 複製的內容 "[Connector的自訂角色權限](#)" 並將它們儲存在Json檔案中。
 - b. 將 Azure 訂閱 ID 新增至可指派的範圍、以修改 Json 檔案。

您應該為使用者建立 Cloud Volumes ONTAP 的各個 Azure 訂閱新增 ID 。

▪ 範例 *

```
"AssignableScopes": [  
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",  
  "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",  
  "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
```

- c. 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。

- 開始 "[Azure Cloud Shell](#)" 並選擇Bash環境。
- 上傳Json檔案。



- 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 Cloud Manager 的自訂角色、可以指派給 Connector 虛擬機器。

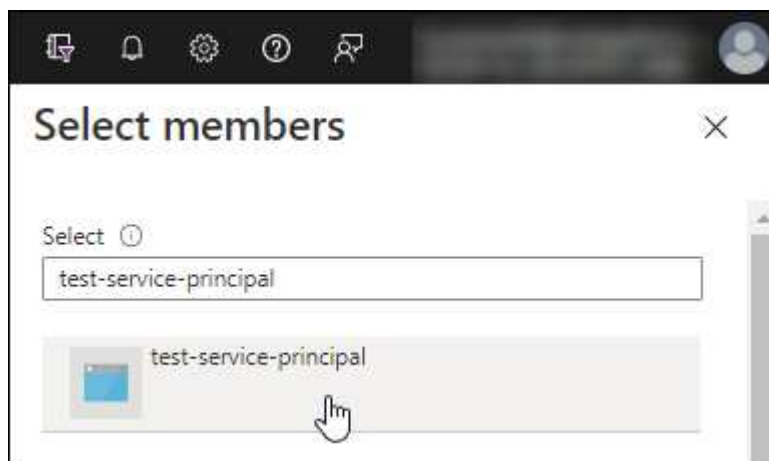
2. 將應用程式指派給角色：

- 從 Azure 入口網站開啟 * 訂閱 * 服務。
- 選取訂閱。
- 按一下 * 存取控制（IAM） > 新增 > 新增角色指派 *。
- 在「角色」索引標籤中、選取「* Cloud Manager operator*」角色、然後按一下「下一步」。
- 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*。



- 搜尋應用程式名稱。

範例如下：



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

服務主體現在擁有部署Connector所需的Azure權限。

如果您想要從 Cloud Volumes ONTAP 多個 Azure 訂閱中部署支援功能、則必須將服務授權對象繫結至每個訂閱項目。Cloud Manager 可讓您選擇部署 Cloud Volumes ONTAP 時要使用的訂閱。

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](#)

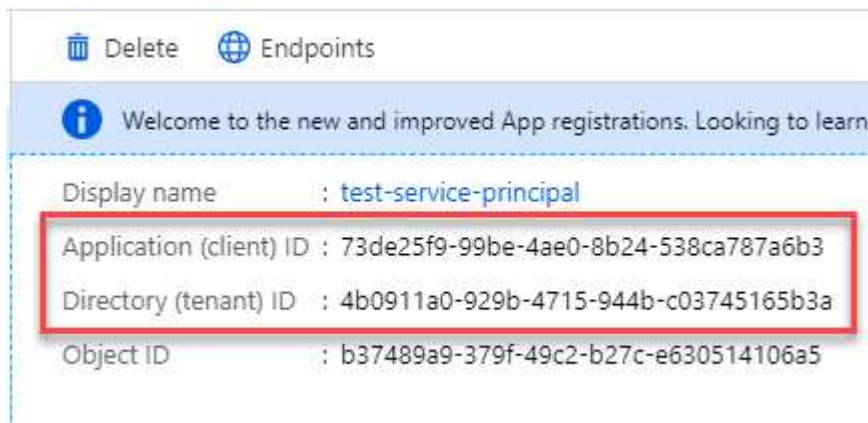
Type to search	
PERMISSION	ADMIN CONSENT REQUIRED
<input checked="" type="checkbox"/> user_impersonation Access Azure Service Management as organization users (preview) ⓘ	-

取得應用程式 ID 和目錄 ID

將 Azure 帳戶新增至 Cloud Manager 時、您必須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 。

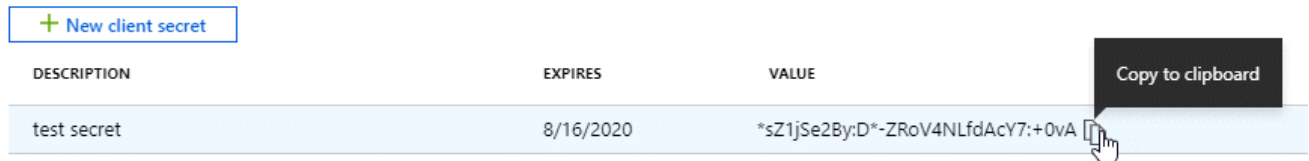
步驟

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.



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。新增 Azure 帳戶時、您必須在 Cloud Manager 中輸入此資訊。

將認證資料新增至Cloud Manager

在您提供 Azure 帳戶所需的權限之後、即可將該帳戶的認證資料新增至 Cloud Manager。完成此步驟可讓您 Cloud Volumes ONTAP 使用不同的 Azure 認證資料來啟動功能。

如果您剛在雲端供應商中建立這些認證資料、可能需要幾分鐘的時間才能使用。請稍候幾分鐘、再將認證資料新增至Cloud Manager。

您必須先建立連接器、才能變更 Cloud Manager 設定。"瞭解方法"。

步驟

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

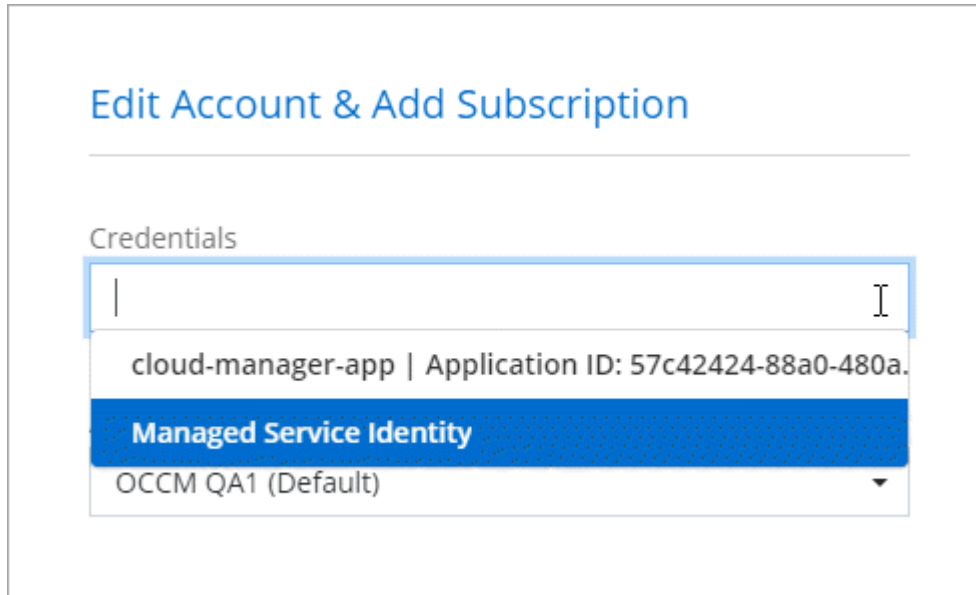


2. 按一下*「Add Credential*（新增認證*）」、然後依照精靈中的步驟進行。
 - a. 認證位置：選擇* Microsoft Azure > Connector*。
 - b. 定義認證：輸入Azure Active Directory服務主體的相關資訊、以授予必要的權限：
 - 應用程式（用戶端） ID：請參閱 [\[Getting the application ID and directory ID\]](#)。
 - 目錄（租戶） ID：請參閱 [\[Getting the application ID and directory ID\]](#)。
 - 用戶端機密：請參閱 [\[Creating a client secret\]](#)。
 - c. 市場訂閱：立即訂閱或選取現有的訂閱、以建立Marketplace訂閱與這些認證的關聯。

若要以Cloud Volumes ONTAP 每小時費率 (PAYGO) 支付
給 LW Y1 Y1 Y1 YGO Y1 Y1 Y1 Y1 Y1 Y1 Y1 Y1 Y1 Y1

- d. 審查：確認新認證資料的詳細資料、然後按一下*新增*。

您現在可以從「詳細資料與認證」頁面切換至不同的認證集合 "[在建立新的工作環境時](#)"



管理現有認證資料

透過建立Marketplace訂閱關聯、編輯認證資料及刪除認證、來管理您已新增至Cloud Manager的Azure認證資料。

將 **Azure Marketplace** 訂閱與認證資料建立關聯

將 Azure 認證資料新增至 Cloud Manager 之後、您可以將 Azure Marketplace 訂閱與這些認證資料建立關聯。訂閱可讓您建立隨用隨付 Cloud Volumes ONTAP 的功能、並使用其他 NetApp 雲端服務。

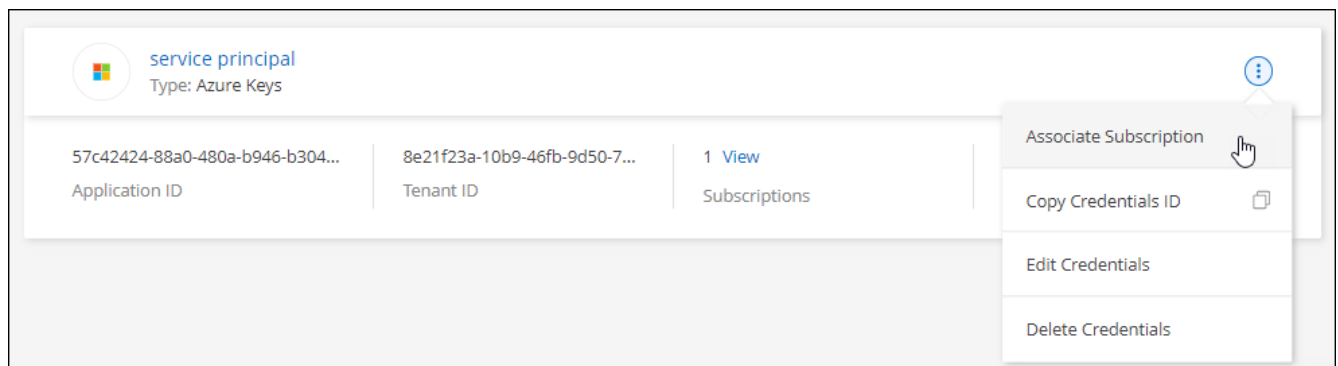
您可能會在將認證新增至 Cloud Manager 之後、在兩種情況下建立 Azure Marketplace 訂閱的關聯：

- 初次將認證新增至 Cloud Manager 時、您並未建立訂閱關聯。
- 您想要以新的訂閱取代現有的 Azure Marketplace 訂閱。

您必須先建立連接器、才能變更 Cloud Manager 設定。"[瞭解方法](#)"。

步驟

1. 在 Cloud Manager 主控台右上角、按一下「設定」圖示、然後選取 * 認證 *。
2. 按一下動作功能表以取得一組認證資料、然後選取「建立訂閱關聯」。



3. 從下拉式清單中選取訂閱、或按一下「* 新增訂閱 *」、然後依照步驟建立新的訂閱。

下列影片會從工作環境精靈的內容開始播放、但會在您按一下「* 新增訂閱 *」之後顯示相同的工作流程：

► https://docs.netapp.com/zh-tw/cloud-manager-setup-admin//media/video_subscribing_azure.mp4

(video)

編輯認證資料

修改Azure服務認證資料的詳細資料、即可在Cloud Manager中編輯Azure認證資料。例如、如果為服務主體應用程式建立新的密碼、您可能需要更新用戶端密碼。

步驟

1. 在 Cloud Manager 主控台右上角、按一下「設定」圖示、然後選取 * 認證 * 。
2. 按一下動作功能表以取得一組認證資料、然後選取*編輯認證*。
3. 進行必要的變更、然後按一下「套用」。

刪除認證資料

如果您不再需要一組認證資料、可以從Cloud Manager刪除。您只能刪除與工作環境無關的認證資料。

步驟

1. 在 Cloud Manager 主控台右上角、按一下「設定」圖示、然後選取 * 認證 * 。
2. 按一下動作功能表以取得一組認證資料、然後選取*刪除認證資料*。
3. 按一下*刪除*以確認。

Google Cloud認證資料

Google Cloud 專案、權限和帳戶

服務帳戶可讓Cloud Manager擁有部署和管理Cloud Volumes ONTAP 與Connector相同專案或不同專案中的各種系統的權限。

Cloud Manager 的專案與權限

在 Cloud Volumes ONTAP Google Cloud 中部署時、您必須先在 Google Cloud 專案中部署 Connector 。Connector 無法在您的內部環境或其他雲端供應商中執行。

直接從 Cloud Manager 部署 Connector 之前、必須先設定兩組權限：

1. 您需要使用具有從 Cloud Manager 啟動 Connector VM 執行個體權限的 Google 帳戶來部署 Connector 。
2. 部署 Connector 時、系統會提示您選取 **"服務帳戶"** 適用於 VM 執行個體。Cloud Manager 可從服務帳戶取得權限 Cloud Volumes ONTAP 、代表您建立及管理各種系統。將自訂角色附加至服務帳戶、即可提供權限。

我們已設定兩個 Y反 洗錢檔案、其中包含使用者和服務帳戶所需的權限。 ["瞭解如何使用 Yaml 檔案來設定權限"](#)。

下圖說明上述第 1 和第 2 項所述的權限要求：



適用於此產品的專案 **Cloud Volumes ONTAP**

可與 Connector 位於同一個專案中、或位於不同的專案中。Cloud Volumes ONTAP若要在 Cloud Volumes ONTAP 不同的專案中部署功能、您必須先將 Connector 服務帳戶和角色新增至該專案。

- ["瞭解如何設定服務帳戶"](#)
- ["瞭解如何在 Cloud Volumes ONTAP GCP 中部署功能、並選擇專案"](#)

管理 **Cloud Manager** 的 **GCP** 認證與訂閱

您可以管理與Connector VM執行個體相關的認證資料。

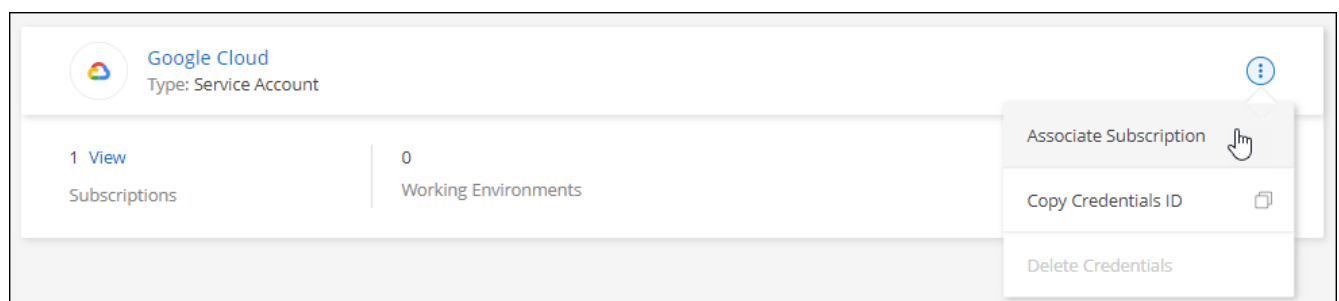
將 **Marketplace** 訂閱與 **GCP** 認證建立關聯

在 GCP 中部署 Connector 時、Cloud Manager 會建立一組與 Connector VM 執行個體相關的預設認證資料。這些是 Cloud Manager 用來部署 Cloud Volumes ONTAP 功能的認證資料。

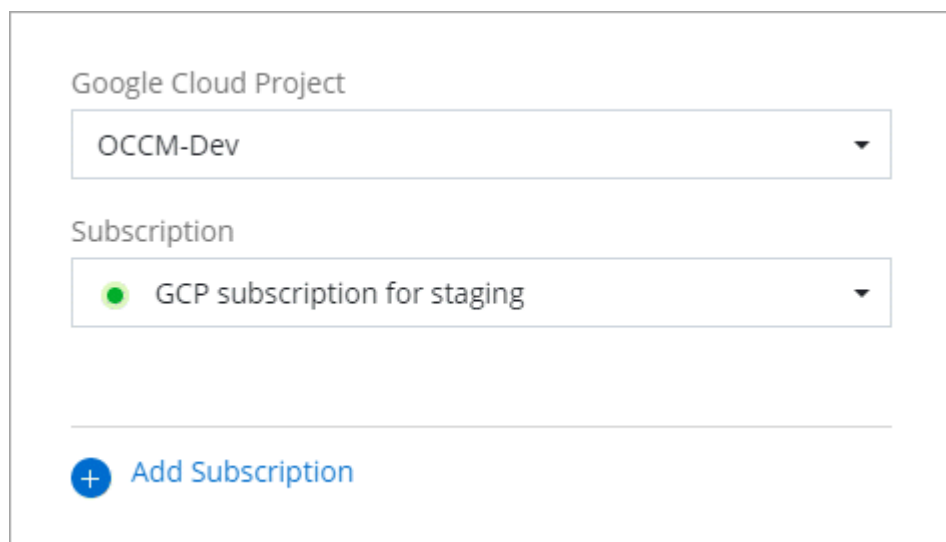
您可以隨時變更與這些認證資料相關的 Marketplace 訂閱。訂閱可讓您建立隨用隨付 Cloud Volumes ONTAP 的功能、並使用其他 NetApp 雲端服務。

步驟

1. 在 Cloud Manager 主控台右上角、按一下「設定」圖示、然後選取 * 認證 *。
2. 按一下動作功能表以取得一組認證資料、然後選取「建立訂閱關聯」。



3. 從下拉式清單中選取Google Cloud專案並訂閱。



The screenshot shows a web interface for selecting a Google Cloud Project and a Subscription. Under the heading "Google Cloud Project", there is a dropdown menu with "OCCM-Dev" selected. Below this, under the heading "Subscription", there is a dropdown menu with "GCP subscription for staging" selected, preceded by a small green circle icon. At the bottom of the form, there is a blue button with a plus sign and the text "Add Subscription".

4. 按一下「* 經銷 *」。
5. 如果您尚未訂閱、請按一下「新增訂閱」、然後依照下列步驟建立新的訂閱。




在您完成下列步驟之前、請先確認您在Google Cloud帳戶中擁有「帳單管理」權限、以及NetApp Cloud Central登入權限。

6. 查看訂購步驟、然後按一下*繼續*。

Add Subscription

Subscription Steps:

- 1 **Cloud Manager**
Clicking **Continue** to create your subscription from the Google Cloud Marketplace.
 - 2 **Google Cloud Marketplace**
Subscribe and then then click **Register With NetApp** to configure your account from Cloud Central.
 - 3 **Cloud Central**
Save your subscription.
 - 4 **Cloud Manager**
Associate the Marketplace subscription with your Google Cloud project.
-  View video instructions

Continue

Cancel

7. 重新導向至之後 "[Google Cloud Marketplace上的NetApp Cloud Manager頁面](#)"下、請確定在頂端導覽功能表中選取正確的專案。

 Google Cloud Platform 





Cloud Manager for Cloud Volumes ONTAP

NetApp, Inc.

Enterprise-grade data management and protection

[SUBSCRIBE](#)

[OVERVIEW](#) [PRICING](#) [SUPPORT](#)

Overview

Cloud Volumes ONTAP is a data-management layer that runs natively on Google Cloud infrastructure enabling enhanced control, data protection, mobility and agility for business application data. Get consistent enterprise-grade storage across your hybrid cloud platforms with built-in disaster recovery, backup and ransomware protection. Seamlessly migrate enterprise applications without reengineering. Create company-wide file shares with simultaneous NFS and CIFS/SMB access and iSCSI block storage for GCE instances with scalability up to 368TB. Automate persistent storage provisioning for your Kubernetes clusters. Accelerate CI/CD cycles with instant, zero-capacity data replication. Reduce storage costs by 70% with advanced storage efficiencies. Cloud Manager is the console used to deploy, manage and automate Cloud Volumes ONTAP instances across the hybrid multi-cloud.

[Learn more](#)

Additional details

Type: [APIs & services](#)

Last updated: 3/26/21

Category: [Storage](#)

Runs on: NetApp, Inc. Cloud Servers

8. 按一下*訂閱*。
9. 選擇適當的帳單帳戶、並同意條款與條件。

2. Purchase details

Select a billing account *
Secondary_Billing_Account ▼

3. Terms

Cancellation and change policy

- Usage fee is billed every month.
- You can cancel the service at any time and it will take effect immediately. You will be billed by the amount you used for that month.

Additional terms

- ☒ I understand this subscription will be automatically renewed at the end of the current term.
- ☒ I authorize Google LLC and its affiliates ("Google") to share my purchase, usage, operational (e.g., project lifecycle events), support ticket, and account information with NetApp, Inc., its affiliates and subcontractors, for the purposes of providing the service, sales attribution, and technical support. I represent that I have the authority to bind my company.
- ☒ By deploying the software or accessing the service you are agreeing to comply with the [End User License Agreement](#), [GCP Marketplace Terms of Service](#), and the terms of applicable open source software licenses bundled with the software or service. Please review these terms and licenses carefully for details about any obligations you may have related to the software or service. To the limited extent an open source software license related to the software or service expressly supersedes the GCP Marketplace Terms of Service, that open source software license governs your use of that software or service.
- By using this product, you understand that certain account and usage information may be shared with NetApp, Inc. for the purposes of financial accounting, sales attribution, performance analysis, and support. ⓘ
- Google is providing this software or service "as-is" and any support for this software or service will be provided by NetApp, Inc. under their terms of service.

SUBSCRIBE

10. 按一下*訂閱*。

此步驟會將您的轉帳要求傳送給NetApp。

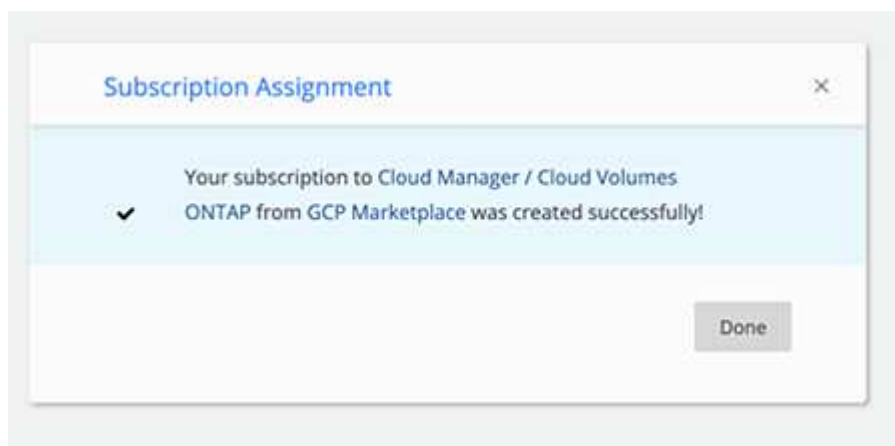
11. 在快顯對話方塊中、按一下*向NetApp註冊*、將其重新導向至NetApp Cloud Central。



必須完成此步驟、才能將GCP訂閱連結至您的NetApp帳戶。在您從本頁重新導向、然後登入NetApp Cloud Central之前、連結訂閱的程序並不完整。

12. 重新導向至Cloud Central之後、請登入NetApp Cloud Central或註冊、然後按一下「完成」繼續。

GCP訂閱會連結至您的使用者登入所關聯的所有NetApp帳戶。



如果貴組織的人員已從您的帳單帳戶訂閱NetApp Cloud Manager、您將會被重新導向至 "NetApp Cloud Central上的《銷售資料頁面Cloud Volumes ONTAP" 而是。如果這是意外情況、請聯絡您的NetApp銷售團隊。Google每個Google帳單帳戶只能啟用一次訂閱。

13. 完成此程序後、請瀏覽至Cloud Manager中的「認證」頁面、然後選取新的訂閱。

Google Cloud Project

OCCM-Dev

Subscription

GCP subscription for staging

+ Add Subscription

Marketplace訂閱程序疑難排解

有時候透過Cloud Volumes ONTAP Google Cloud Marketplace訂閱的功能可能會因為權限不正確或不小心不再重新導向至NetApp Cloud Central而變得零散。如果發生這種情況、請使用下列步驟完成訂購程序。

步驟

1. 瀏覽至 "[Google Cloud Marketplace上的NetApp Cloud Manager頁面](#)" 檢查訂單狀態。如果頁面顯示*管理供應商*、請向下捲動並按一下*管理訂單*。

Pricing

The product was purchased on 12/9/20.

MANAGE ORDERS

- a. 如果訂單顯示綠色勾選標記、但這是意外情況、則組織中使用相同帳單帳戶的其他人可能已經訂閱。如果這是意外情況、或您需要此訂閱的詳細資料、請聯絡您的NetApp銷售團隊。

Filter Enter property name or value										
Status	Order number	Plan	Discount	Start date ↓	Plan duration	End date	Payment Schedule	Auto-renew	Next plan	
	2eebbc...	Cloud Manager	-	10/21/21	1 month	-	Postpay	N/A	N/A	⋮

- b. 如果訂單顯示時鐘和*待處理*狀態、請返回市場頁面、選擇*管理供應商*以完成上述程序。

Filter Enter property name or value										
Status	Order number	Plan	Discount	Start date ↓	Plan duration	End date	Payment Schedule	Auto-renew	Next plan	
	d56c66...	Cloud Manager	-	Pending	1 month	Pending	Postpay	N/A	N/A	⋮

在Cloud Manager中新增及管理NetApp支援網站帳戶

提供您NetApp支援網站（NSS）帳戶的認證資料、以啟用Cloud Volumes ONTAP 關鍵的

流程來執行支援功能、並透過Active IQ 支援功能實現預測性分析和主動式支援。

總覽

若要執行下列工作、必須將NetApp Support Site帳戶新增至Cloud Manager：

- 在Cloud Volumes ONTAP 您自帶授權（BYOL）時部署

您必須提供您的NSS帳戶、Cloud Manager才能上傳授權金鑰、並啟用您所購買之期限的訂閱。這包括定期續約的自動更新。

- 註冊隨用隨付Cloud Volumes ONTAP 的功能不全的系統

您必須提供您的NSS帳戶、才能啟動系統支援、並取得NetApp技術支援資源的存取權。

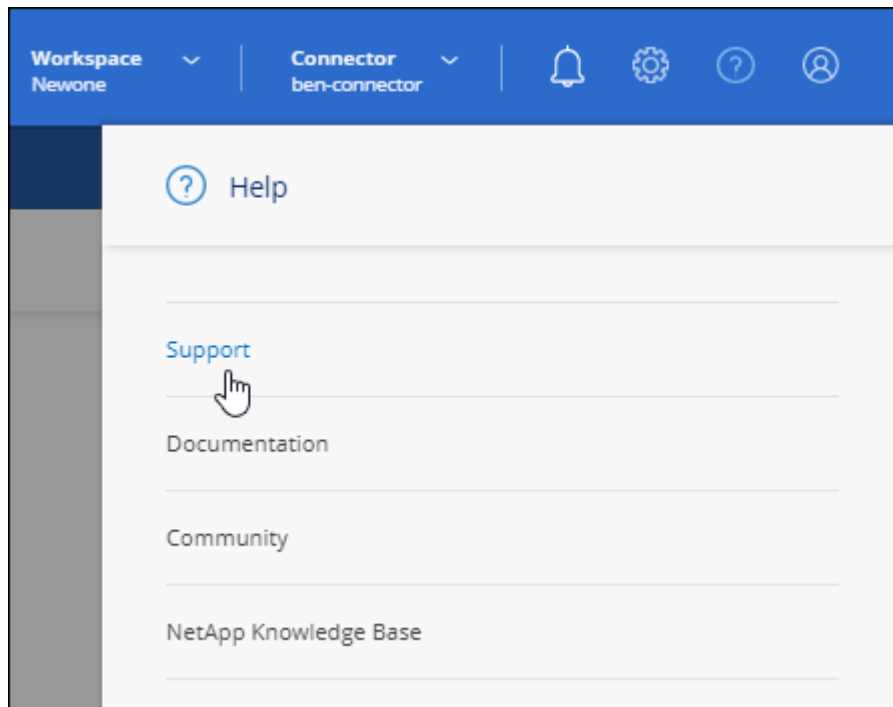
- 升級Cloud Volumes ONTAP 到最新版本的更新版
- 使用Active IQ Cloud Manager中的「解決方案」

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。

請注意帳戶的下列需求：

- 帳戶必須是客戶層級的帳戶（不是來賓帳戶或臨時帳戶）。
- 如果您打算部署節點型BYOL系統：
 - 帳戶必須獲得授權、才能存取 BYOL 系統的序號。
 - 如果您購買安全的 BYOL 訂閱、則需要安全的 NSS 帳戶。

現在、使用者可以在建立新Cloud Volumes ONTAP 的視覺系統、註冊現有Cloud Volumes ONTAP 的視覺系統、以及在Active IQ 使用效益資料時選擇帳戶。

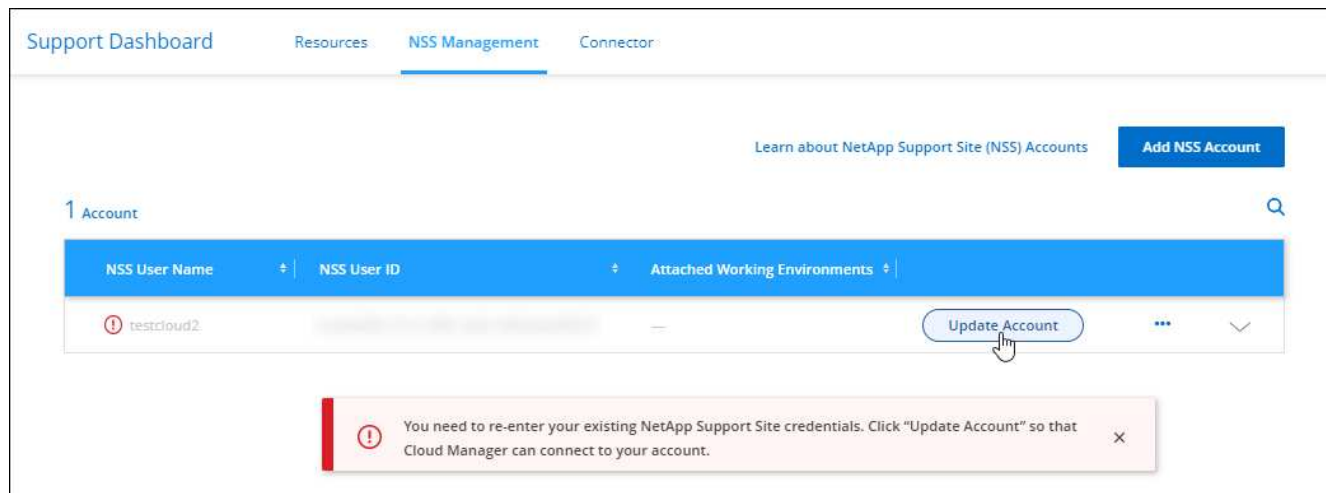
- ["在 Cloud Volumes ONTAP AWS 中啟動"](#)
- ["在 Cloud Volumes ONTAP Azure 中啟動"](#)
- ["在 Cloud Volumes ONTAP GCP 中啟動"](#)
- ["註冊隨用隨付系統"](#)

更新新驗證方法的NSS帳戶

自2021年11月起、NetApp現在使用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。此更新之後、Cloud Manager會提示您更新先前新增之任何現有帳戶的認證資料。

步驟

1. 如果您尚未這麼做、["建立Microsoft Azure Active Directory B2C帳戶、並連結至您目前的NetApp帳戶"](#)。
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"。
4. 針對您要更新的NSS帳戶、按一下*更新帳戶*。



5. 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。

6. 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。

完成此程序之後、您更新的帳戶現在應該會在表格中列為_new帳戶。此表中仍會列出_舊版_帳戶、以及任何現有的工作環境關聯。

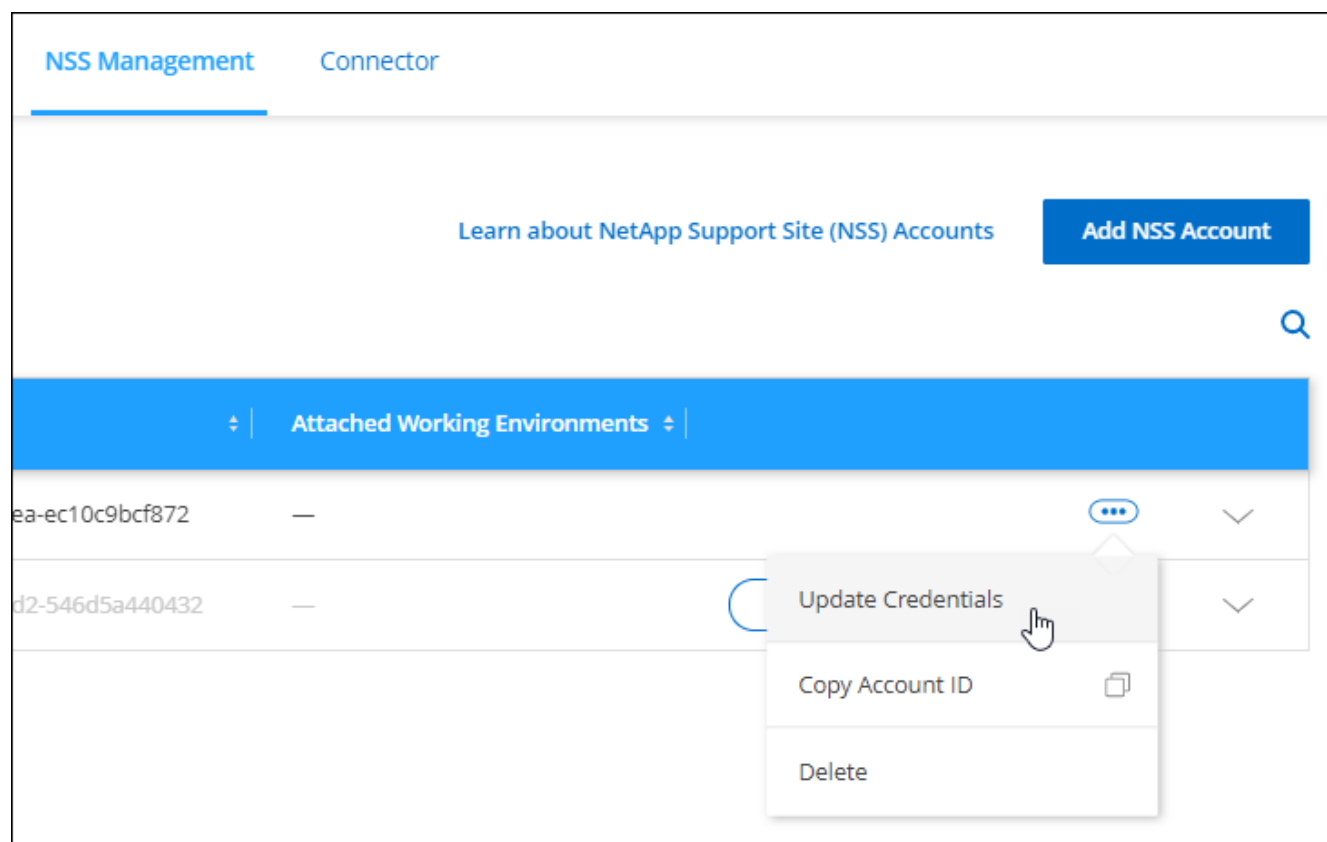
7. 如果Cloud Volumes ONTAP 現有的不工作環境附加至舊版帳戶、請依照下列步驟執行 [將這些工作環境附加至不同的NSS帳戶](#)。
8. 移至舊版的nss帳戶、按一下 ... 然後選取*刪除*。

更新NSS認證資料

每當您變更您的NSS帳戶認證資料時、都必須在Cloud Manager中更新。

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. 按一下*"nss管理"。
3. 針對您要更新的NSS帳戶、按一下 ... 然後選取*更新認證*。



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。

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。

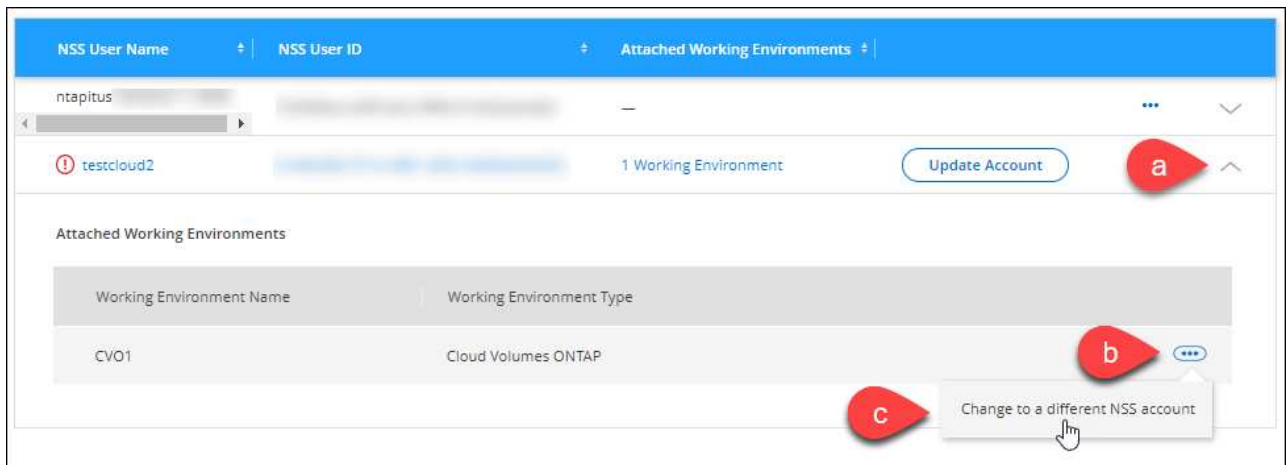
將工作環境附加至不同的NSS帳戶

如果您的組織有多個NetApp Support Site帳戶、您可以變更Cloud Volumes ONTAP 哪個帳戶與某個支援系統相關聯。

此功能僅適用於設定為使用NetApp採用的Microsoft Azure AD進行身分識別管理的NSS帳戶。在使用此功能之前、您需要按一下*「Add nssAccount」（新增nssAccount）或「Update Account」（更新帳戶）*。

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. 按一下*「nss管理」*。
3. 完成下列步驟以變更NSS帳戶：
 - a. 展開工作環境目前關聯的NetApp支援網站帳戶列。
 - b. 若要變更關聯的工作環境、請按一下 ...
 - c. 選擇*變更為不同的nss*帳戶。



- d. 選取帳戶、然後按一下*「Save（儲存）」*。

顯示NSS帳戶的電子郵件地址

由於NetApp Support Site帳戶使用Microsoft Azure Active Directory進行驗證服務、因此Cloud Manager中顯示的NSS使用者名稱通常是Azure AD所產生的識別碼。因此、您可能無法立即得知與該帳戶相關的電子郵件地址。但Cloud Manager可選擇顯示相關的電子郵件地址。

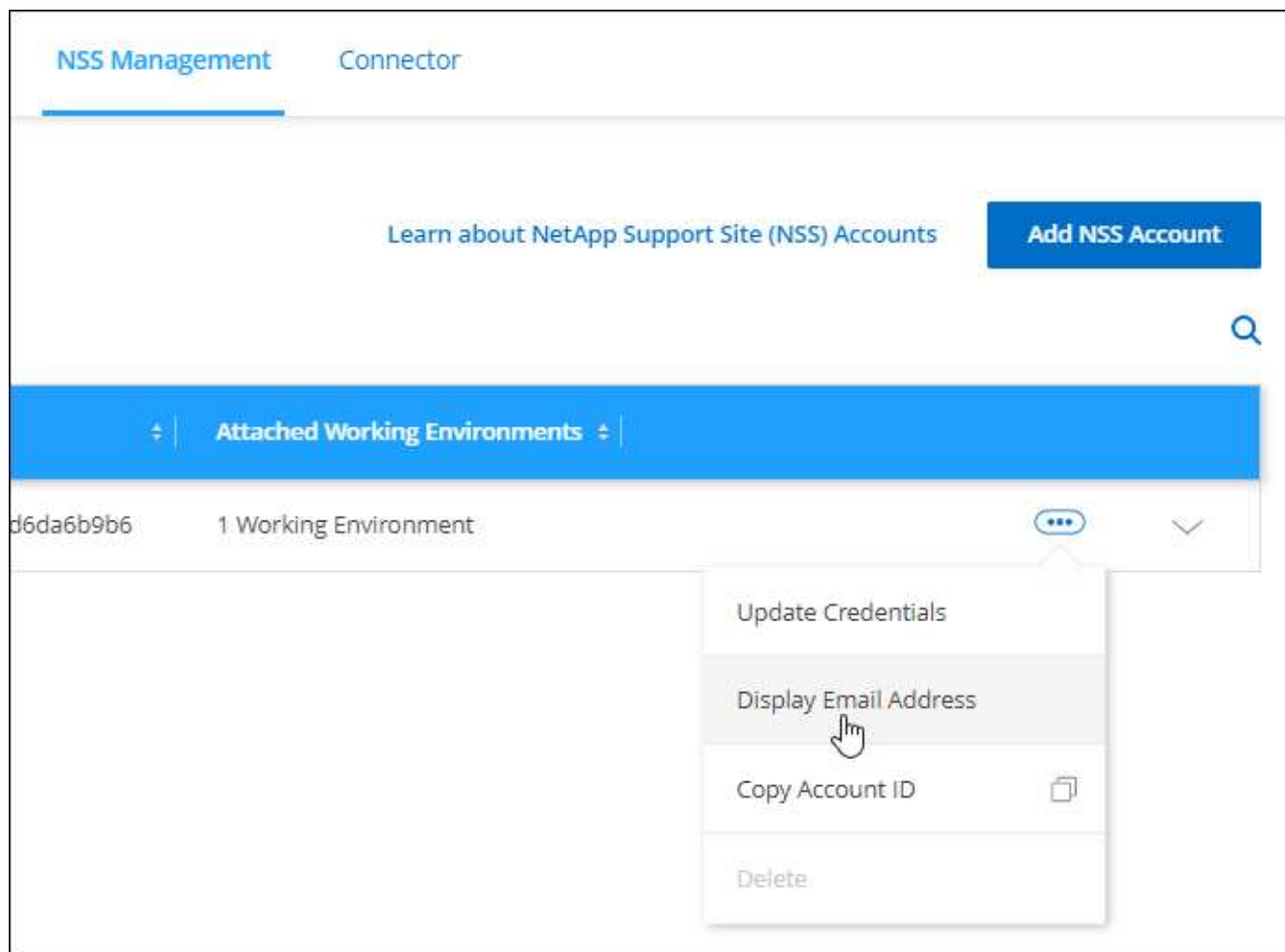


前往「NSS管理」頁面時、Cloud Manager會為表格中的每個帳戶產生權杖。該權杖包含相關電子郵件地址的相關資訊。當您離開頁面時、便會移除權杖。這些資訊永遠不會快取、有助於保護您的隱私。

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. 按一下"**nss管理**"。
3. 針對您要更新的NSS帳戶、按一下 **...** 然後選取***顯示電子郵件地址***。



Cloud Manager會顯示NetApp支援網站使用者名稱及相關的電子郵件地址。您可以使用複製按鈕來複製電子郵件地址。

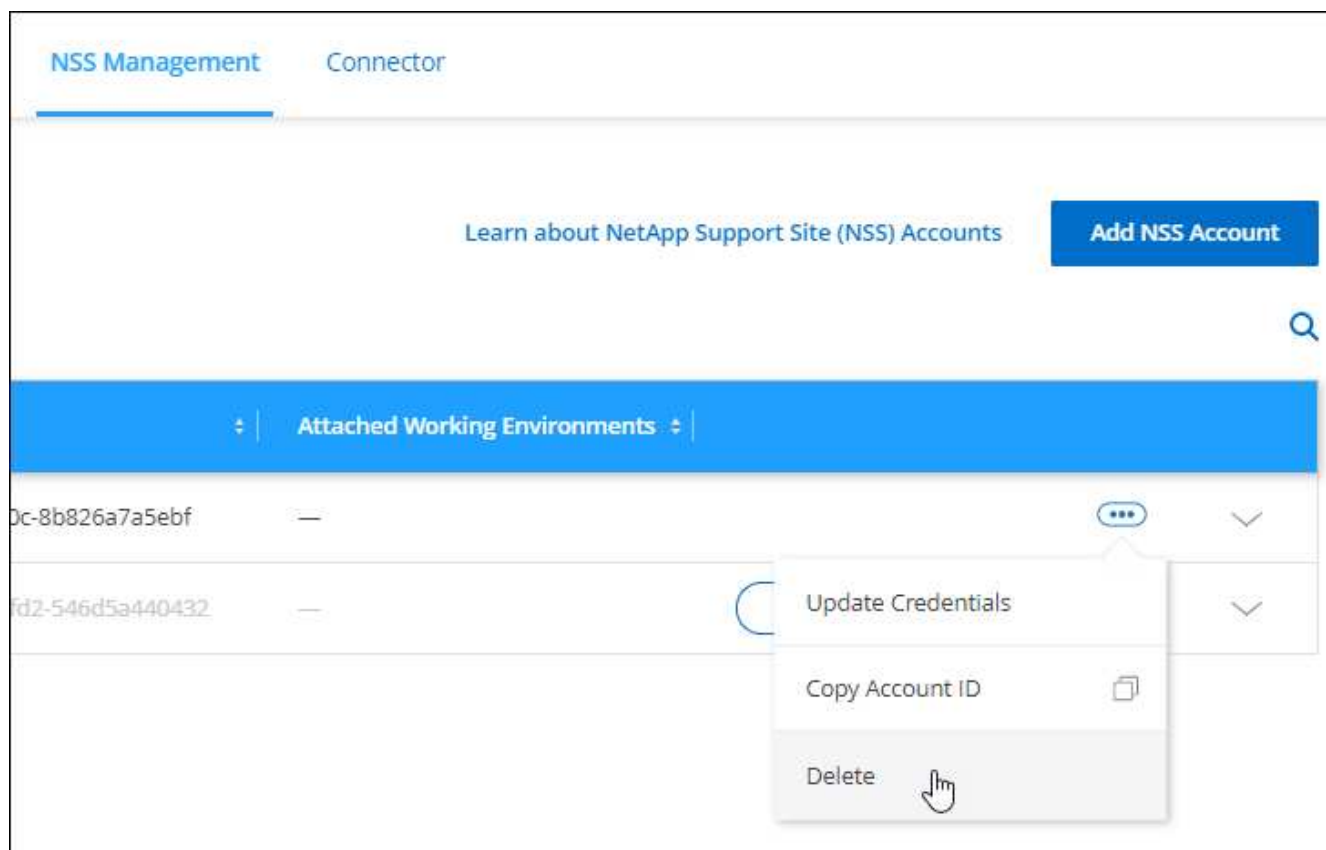
移除NSS.帳戶

刪除任何不再想與Cloud Manager搭配使用的NSS帳戶。

請注意、您無法刪除目前與Cloud Volumes ONTAP 某個運作環境相關聯的帳戶。您首先需要 [將這些工作環境附加至不同的NSS帳戶](#)。

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. 按一下"**nss管理**"。
3. 針對您要刪除的NSS帳戶、按一下 **...** 然後選取***刪除***。



4. 按一下*刪除*以確認。

參考資料

Cloud Manager的權限摘要

若要使用Cloud Manager中的功能和服務、您必須提供權限、以便Cloud Manager能在雲端環境中執行作業。使用此頁面上的連結、根據您的目標快速存取所需的權限。

AWS權限

目的	說明	連結
連接器部署	從Cloud Manager建立Connector的使用者需要特定權限、才能在AWS中部署執行個體。	"從Cloud Manager在AWS中建立連接器"
連接器操作	Cloud Manager啟動Connector時、會將原則附加至執行個體、以提供管理AWS帳戶中資源和程序所需的權限。您需要自行設定原則 "從市場推出Connector" 或是您 "將更多AWS認證資料新增至Connector" 。您也必須確保在後續版本中新增權限時、原則保持在最新狀態。	"Connector的AWS權限"
作業系統Cloud Volumes ONTAP	必須將IAM角色附加至Cloud Volumes ONTAP AWS中的每個節點。HA中介者也是如此。預設選項是讓Cloud Manager為您建立IAM角色、但您可以自行使用。	"瞭解如何自行設定IAM角色"

Azure權限

目的	說明	連結
連接器部署	當您從Cloud Manager部署Connector時、您需要使用Azure帳戶或服務主體、該用戶必須具有在Azure中部署Connector VM的權限。	"從Cloud Manager在Azure中建立Connector"
連接器操作	Cloud Manager在Azure中部署Connector VM時、會建立自訂角色、提供必要的權限來管理該Azure訂閱中的資源和程序。 您需要自行設定自訂角色（如果您） "從市場推出Connector" 或是您 "將更多Azure認證資料新增至Connector" 。 您也必須確保在後續版本中新增權限時、原則保持在最新狀態。	"連接器的Azure權限"

Google Cloud權限

目的	說明	連結
連接器部署	從Cloud Manager部署Connector的Google Cloud使用者需要特定權限、才能在Google Cloud中部署Connector。	"設定部署Connector的權限"
連接器操作	Connector VM執行個體的服務帳戶必須具有特定的日常作業權限。從Cloud Manager部署時、您需要將服務帳戶與Connector建立關聯。您也必須確保在後續版本中新增權限時、原則保持在最新狀態。	"設定Connector的服務帳戶"

Connector的AWS權限

Cloud Manager在AWS中啟動Connector執行個體時、會將原則附加至執行個體、讓Connector有權管理該AWS帳戶內的資源和程序。連接器使用權限來撥打API呼叫數個AWS服務、包括EC2、S3、CloudForecation、IAM、金鑰管理服務（KMS）等。

IAM原則

下列IAM原則提供Connector所需的權限、以便根據AWS區域管理公有雲環境中的資源和程序。

直接從Cloud Manager建立Connector時、Cloud Manager會自動將此原則套用至Connector。

如果您是從AWS Marketplace部署Connector、或是在Linux主機上手動安裝Connector、則必須自行設定原則。

您也必須確保在後續版本中新增權限時、原則保持在最新狀態。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "cvoServicePolicy",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeRouteTables",
        "ec2:DescribeImages",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DescribeVolumes",
        "ec2:ModifyVolumeAttribute",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:CreateSnapshot",
        "ec2:DescribeSnapshots",
        "ec2:GetConsoleOutput",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DescribeTags",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "iam:PassRole",
        "iam:CreateRole",
        "iam:PutRolePolicy",
```

```
"iam:CreateInstanceProfile",
"iam:AddRoleToInstanceProfile",
"iam:RemoveRoleFromInstanceProfile",
"iam:ListInstanceProfiles",
"sts:DecodeAuthorizationMessage",
"ec2:AssociateIamInstanceProfile",
"ec2:DescribeIamInstanceProfileAssociations",
"ec2:DisassociateIamInstanceProfile",
"s3:GetBucketTagging",
"s3:GetBucketLocation",
"s3:ListBucket",
"s3:CreateBucket",
"s3:GetLifecycleConfiguration",
"s3:ListBucketVersions",
"s3:GetBucketPolicyStatus",
"s3:GetBucketPublicAccessBlock",
"s3:GetBucketPolicy",
"s3:GetBucketAcl",
"kms:List*",
"kms:ReEncrypt*",
"kms:Describe*",
"kms:CreateGrant",
"ce:GetReservationUtilization",
"ce:GetDimensionValues",
"ce:GetCostAndUsage",
"ce:GetTags",
"ec2:CreatePlacementGroup",
"ec2:DescribeReservedInstancesOfferings",
"sts:AssumeRole",
"ec2:AssignPrivateIpAddresses",
"ec2:CreateRoute",
"ec2:DescribeVpcs",
"ec2:ReplaceRoute",
"ec2:UnassignPrivateIpAddresses",
"s3:PutObjectTagging",
"s3:GetObjectTagging",
"fsx:Describe*",
"fsx:List*",
"ec2:DeleteSecurityGroup",
"ec2:DeleteNetworkInterface",
"ec2:DeleteSnapshot",
"ec2:DeleteTags",
"ec2:DeleteRoute",
"ec2:DeletePlacementGroup",
"iam:DeleteRole",
"iam:DeleteRolePolicy",
```

```

        "iam:DeleteInstanceProfile",
        "cloudformation:DeleteStack",
        "ec2:DescribePlacementGroups",
        "iam:GetRolePolicy",
        "s3:ListAllMyBuckets",
        "s3:GetObject",
        "iam:GetRole",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:PutObject",
        "ec2:ModifyVolume",
        "ec2:DescribeVolumesModifications"
    ],
    "Resource": "*"
},
{
    "Sid": "backupPolicy",
    "Effect": "Allow",
    "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeImages",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "kms:List*",
        "kms:Describe*",
        "ec2:describeVpcEndpoints",
        "kms:ListAliases",
        "athena:StartQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryExecution",
        "athena:StopQueryExecution",
        "glue:CreateDatabase",
        "glue:CreateTable",
    ]
}

```

```

        "glue:BatchDeletePartition"
    ],
    "Resource": "*"
},
{
    "Sid": "backupS3Policy",
    "Effect": "Allow",
    "Action": [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:CreateBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions",
        "s3:GetBucketAcl",
        "s3:PutBucketPublicAccessBlock",
        "s3:GetObject",
        "s3:PutEncryptionConfiguration",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject",
        "s3:PutBucketAcl",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts",
        "s3:DeleteBucket"
    ],
    "Resource": [
        "arn:aws:s3:::netapp-backup-*"
    ]
},
{
    "Sid": "tagServicePolicy",
    "Effect": "Allow",
    "Action": [
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:DescribeTags",
        "tag:getResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "tag:TagResources",
        "tag:UntagResources"
    ],

```

```

    "Resource": "*"
  },
  {
    "Sid": "fabricPoolS3Policy",
    "Effect": "Allow",
    "Action": [
      "s3:CreateBucket",
      "s3:GetLifecycleConfiguration",
      "s3:PutLifecycleConfiguration",
      "s3:PutBucketTagging",
      "s3:ListBucketVersions",
      "s3:GetBucketPolicyStatus",
      "s3:GetBucketPublicAccessBlock",
      "s3:GetBucketAcl",
      "s3:GetBucketPolicy",
      "s3:PutBucketPublicAccessBlock",
      "s3:DeleteBucket"
    ],
    "Resource": [
      "arn:aws:s3:::fabric-pool*"
    ]
  },
  {
    "Sid": "fabricPoolPolicy",
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeRegions"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:StartInstances",
      "ec2:StopInstances",
      "ec2:TerminateInstances"
    ],
    "Condition": {
      "StringLike": {
        "ec2:ResourceTag/netapp-adc-manager": "*"
      }
    },
    "Resource": [
      "arn:aws:ec2:*:*:instance/*"
    ]
  },
},

```

```

{
  "Effect": "Allow",
  "Action": [
    "ec2:StartInstances",
    "ec2:TerminateInstances",
    "ec2:AttachVolume",
    "ec2:DetachVolume"
  ],
  "Condition": {
    "StringLike": {
      "ec2:ResourceTag/GFCInstance": "*"
    }
  },
  "Resource": [
    "arn:aws:ec2:*:*:instance/*"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:StartInstances",
    "ec2:TerminateInstances",
    "ec2:AttachVolume",
    "ec2:DetachVolume",
    "ec2:StopInstances",
    "ec2>DeleteVolume"
  ],
  "Condition": {
    "StringLike": {
      "ec2:ResourceTag/WorkingEnvironment": "*"
    }
  },
  "Resource": [
    "arn:aws:ec2:*:*:instance/*"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:AttachVolume",
    "ec2:DetachVolume"
  ],
  "Resource": [
    "arn:aws:ec2:*:*:volume/*"
  ]
},

```

```

    {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteVolume"
      ],
      "Condition": {
        "StringLike": {
          "ec2:ResourceTag/WorkingEnvironment": "*"
        }
      },
      "Resource": [
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Sid": "K8sServicePolicy",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeRegions",
        "iam:ListInstanceProfiles",
        "eks:ListClusters",
        "eks:DescribeCluster"
      ],
      "Resource": "*"
    },
    {
      "Sid": "GFCservicePolicy",
      "Effect": "Allow",
      "Action": [
        "cloudformation:DescribeStacks",
        "cloudwatch:GetMetricStatistics",
        "cloudformation:ListStacks"
      ],
      "Resource": "*"
    }
  ]
}

```

GovCloud (美國) 地區

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [

```



```
"iam:ListInstanceProfiles",
"iam:CreateRole",
"iam:DeleteRole",
"iam:PutRolePolicy",
"iam:CreateInstanceProfile",
"iam:DeleteRolePolicy",
"iam:AddRoleToInstanceProfile",
"iam:RemoveRoleFromInstanceProfile",
"iam:DeleteInstanceProfile",
"ec2:ModifyVolumeAttribute",
"sts:DecodeAuthorizationMessage",
"ec2:DescribeImages",
"ec2:DescribeRouteTables",
"ec2:DescribeInstances",
"iam:PassRole",
"ec2:DescribeInstanceState",
"ec2:RunInstances",
"ec2:ModifyInstanceAttribute",
"ec2:CreateTags",
"ec2:CreateVolume",
"ec2:DescribeVolumes",
"ec2:DeleteVolume",
"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:CreateSnapshot",
"ec2:DeleteSnapshot",
"ec2:DescribeSnapshots",
"ec2:StopInstances",
"ec2:GetConsoleOutput",
"ec2:DescribeKeyPairs",
"ec2:DescribeRegions",
"ec2:DeleteTags",
"ec2:DescribeTags",
"cloudformation:CreateStack",
```

```

        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:CreateBucket",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "kms:List*",
        "kms:ReEncrypt*",
        "kms:Describe*",
        "kms:CreateGrant",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DescribeInstanceAttribute",
        "ce:GetReservationUtilization",
        "ce:GetDimensionValues",
        "ce:GetCostAndUsage",
        "ce:GetTags",
        "ec2:CreatePlacementGroup",
        "ec2>DeletePlacementGroup"
    ],
    "Resource": "*"
},
{
    "Sid": "fabricPoolPolicy",
    "Effect": "Allow",
    "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:PutBucketPublicAccessBlock"
    ],

```

```

        "Resource": [
            "arn:aws-us-gov:s3:::fabric-pool*"
        ]
    },
    {
        "Sid": "backupPolicy",
        "Effect": "Allow",
        "Action": [
            "s3:DeleteBucket",
            "s3:GetLifecycleConfiguration",
            "s3:PutLifecycleConfiguration",
            "s3:PutBucketTagging",
            "s3:ListBucketVersions",
            "s3:GetObject",
            "s3:ListBucket",
            "s3:ListAllMyBuckets",
            "s3:GetBucketTagging",
            "s3:GetBucketLocation",
            "s3:GetBucketPolicyStatus",
            "s3:GetBucketPublicAccessBlock",
            "s3:GetBucketAcl",
            "s3:GetBucketPolicy",
            "s3:PutBucketPublicAccessBlock"
        ],
        "Resource": [
            "arn:aws-us-gov:s3:::netapp-backup-*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:StartInstances",
            "ec2:TerminateInstances",
            "ec2:AttachVolume",
            "ec2:DetachVolume"
        ],
        "Condition": {
            "StringLike": {
                "ec2:ResourceTag/WorkingEnvironment": "*"
            }
        },
        "Resource": [
            "arn:aws-us-gov:ec2:*:*:instance/*"
        ]
    },
    {

```

```

    "Effect": "Allow",
    "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
    ],
    "Resource": [
        "arn:aws-us-gov:ec2:*:*:volume/*"
    ]
}
]
}

```

C2S環境

```

{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "ec2:DescribeInstances",
            "ec2:DescribeInstanceStatus",
            "ec2:RunInstances",
            "ec2:ModifyInstanceAttribute",
            "ec2:DescribeRouteTables",
            "ec2:DescribeImages",
            "ec2:CreateTags",
            "ec2:CreateVolume",
            "ec2:DescribeVolumes",
            "ec2:ModifyVolumeAttribute",
            "ec2>DeleteVolume",
            "ec2:CreateSecurityGroup",
            "ec2>DeleteSecurityGroup",
            "ec2:DescribeSecurityGroups",
            "ec2:RevokeSecurityGroupEgress",
            "ec2:RevokeSecurityGroupIngress",
            "ec2:AuthorizeSecurityGroupEgress",
            "ec2:AuthorizeSecurityGroupIngress",
            "ec2:CreateNetworkInterface",
            "ec2:DescribeNetworkInterfaces",
            "ec2>DeleteNetworkInterface",
            "ec2:ModifyNetworkInterfaceAttribute",
            "ec2:DescribeSubnets",
            "ec2:DescribeVpcs",
            "ec2:DescribeDhcpOptions",
            "ec2:CreateSnapshot",
            "ec2>DeleteSnapshot",

```

```

        "ec2:DescribeSnapshots",
        "ec2:GetConsoleOutput",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DeleteTags",
        "ec2:DescribeTags",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "iam:PassRole",
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "kms:List*",
        "kms:Describe*",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DescribeInstanceAttribute",
        "ec2:CreatePlacementGroup",
        "ec2:DeletePlacementGroup",
        "iam:ListInstanceProfiles"
    ],
    "Resource": "*"
},
{
    "Sid": "fabricPoolPolicy",
    "Effect": "Allow",
    "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions"
    ]
}

```

```

    ],
    "Resource": [
        "arn:aws-iso:s3:::fabric-pool*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:AttachVolume",
        "ec2:DetachVolume"
    ],
    "Condition": {
        "StringLike": {
            "ec2:ResourceTag/WorkingEnvironment": "*"
        }
    },
    "Resource": [
        "arn:aws-iso:ec2:*:*:instance/*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
    ],
    "Resource": [
        "arn:aws-iso:ec2:*:*:volume/*"
    ]
}
]
}

```

= AWS權限的使用方式

以下各節說明如何將權限用於每項NetApp雲端服務。如果您的企業原則規定只有在需要時才提供權限、此資訊就很有幫助。

==應用程式範本標記

當您使用應用程式範本標記服務時、Connector會發出下列API要求來管理AWS資源上的標記：

- EC2：建立標記

- EC2：刪除標記
- EC2：取消標示
- 標記：getResources
- 標記：getTagKeys
- 標記：getTagValues
- 標記：TagResources
- 標記：取消標記資源

=雲端備份

Connector會提出下列API要求、以部署Cloud Backup的還原執行個體：

- EC2：啟動安裝
- EC2：停止執行
- EC2：資料說明
- EC2：取消訂閱即時狀態
- EC2：RunInstances
- EC2：終端安裝
- EC2：取消訂閱實例屬性
- EC2：取消影像
- EC2：建立標記
- EC2：建立磁碟區
- EC2：建立安全性群組
- EC2：無資料子網路
- EC2：取消功能Vpcs
- EC2：取消註冊
- 雲端：建立堆疊
- 雲端：刪除堆疊
- 雲端：無標準堆疊

Connector會提出下列API要求、以管理Amazon S3中的備份：

- S3：GetBucketLocation
- S3：ListAllMyb桶
- S3：清單庫
- S3：建立桶
- S3：Get生命週期組態
- S3：Put升降器組態

- S3 : PuttBucketting
- S3 : listBucketVerions
- S3 : GetBucketAcl
- S3 : PuttBucketPublicAccessBlock
- 公里：清單*
- 公里：描述*
- S3 : GetObject
- EC2：已描述VpcEndpoints
- kms：清單別名
- S3 : PuttEncryptionConfiguration

當您使用搜尋與還原方法還原磁碟區和檔案時、Connector會發出下列API要求：

- S3：建立桶
- S3：刪除物件
- S3：刪除ObjectVersion
- S3：GetBucketAcl
- S3：清單庫
- S3：listBucketVerions
- S3：listBucketMultiPartUploads
- S3：PuttObject
- S3：PuttBucketAcl
- S3：Putt升降 器組態
- S3：PuttBucketPublicAccessBlock
- S3：中止多重角色上傳
- S3：列出多個零件上傳零件
- Athena：StartQueryExecutionc
- Athena：GetQueryResults
- Athena：GetQueryExecution
- Athena：停止查詢執行
- 黏著劑：建立資料庫
- 黏著劑：CreateTable
- 黏著劑：批字刪除分割區

==雲端資料感測

Connector會提出下列API要求來部署Cloud Data Sense執行個體：

- EC2：資料說明
- EC2：取消訂閱即時狀態
- EC2：RunInstances
- EC2：終端安裝
- EC2：建立標記
- EC2：建立磁碟區
- EC2：AttachVolume
- EC2：建立安全性群組
- EC2：刪除安全性群組
- EC2：取消安全性群組
- EC2：建立網路介面
- EC2：網路介面
- EC2：刪除網路介面
- EC2：無資料子網路
- EC2：取消功能Vpcs
- EC2：建立Snapshot
- EC2：取消註冊
- 雲端：建立堆疊
- 雲端：刪除堆疊
- 雲端：無標準堆疊
- 雲端：取消功能堆疊事件
- IAM：AddRoleToInstanceProfile
- EC2：Associate IamInstanceProfile
- EC2：解讀IamInstanceProfileAssociations

使用Cloud Data Sense時、Connector會發出下列API要求來掃描S3儲存區：

- IAM：AddRoleToInstanceProfile
- EC2：Associate IamInstanceProfile
- EC2：解讀IamInstanceProfileAssociations
- S3：GetBucketting
- S3：GetBucketLocation
- S3：ListAllMyb桶
- S3：清單庫
- S3：GetBucketPolicyStatus
- S3：GetBucketPolicy

- S3：GetBucketAcl
- S3：GetObject
- IAM：GetRole
- S3：刪除物件
- S3：刪除ObjectVersion
- S3：PutObject
- STS: AssumeRole

=雲端分層

連接器會在您使用雲端分層時、提出下列API要求、將資料分層至Amazon S3。

行動	用於設定？	用於日常營運？
S3：建立桶	是的	否
S3：PutObject 器組態	是的	否
S3：GetObject 週期組態	是的	是的
EC2：取消註冊	是的	是的

== Cloud Volumes ONTAP 不一樣

Connector會提出下列API要求、要求在Cloud Volumes ONTAP AWS中部署及管理功能。

目的	行動	用於部署？	用於日常營運？	用於刪除？
建立及管理IAM角色及Cloud Volumes ONTAP 執行個體設定檔以利執行個體	IAM：清單執行設定檔	是的	是的	否
	IAM：建立角色	是的	否	否
	IAM：刪除角色	否	是的	是的
	IAM：Putt角色 原則	是的	否	否
	IAM：CreatanceProfile	是的	否	否
	IAM：刪除角色原則	否	是的	是的
	IAM：AddRoleToInstanceProfile	是的	否	否
	IAM：RemoveRoleFromInstanceProfile	否	是的	是的
	IAM：刪除InstanceProfile	否	是的	是的
	IAM：密碼	是的	否	否
	EC2：AssociateIamInstanceProfile	是的	是的	否
	EC2：解讀IamInstanceProfileAssociations	是的	是的	否
	EC2：中斷IamInstanceProfile	否	是的	否
解碼授權狀態訊息	STS:解碼授權訊息	是的	是的	否
說明帳戶可使用的指定映像（Amis）	EC2：取消影像	是的	是的	否
描述VPC中的路由表（僅HA配對需要）	EC2：取消功能表	是的	否	否

目的	行動	用於部署？	用於日常營運？	用於刪除？
停止、啟動及監控執行個體	EC2：啟動安裝	是的	是的	否
	EC2：停止執行	是的	是的	否
	EC2：資料說明	是的	是的	否
	EC2：取消訂閱即時狀態	是的	是的	否
	EC2：RunInstances	是的	否	否
	EC2：終端安裝	否	否	是的
	EC2：修改實例屬性	否	是的	否
確認已針對支援的執行個體類型啟用增強式網路功能	EC2：取消訂閱實例屬性	否	是的	否
使用「WorkingEnvironment」和「WorkingEnvironmentId」標記來標記資源、這些標記用於維護和成本分配	EC2：建立標記	是的	是的	否
管理Cloud Volumes ONTAP EBS磁碟區、這些磁碟區可作為後端儲存設備使用	EC2：建立磁碟區	是的	是的	否
	EC2：減量磁碟區	是的	是的	是的
	EC2：修改Volume屬性	否	是的	是的
	EC2：AttachVolume	是的	是的	否
	EC2：刪除Volume	否	是的	是的
	EC2：分離Volume	否	是的	是的

目的	行動	用於部署？	用於日常營運？	用於刪除？
建立及管理安全性群組Cloud Volumes ONTAP 以利執行	EC2：建立安全性群組	是的	否	否
	EC2：刪除安全性群組	否	是的	是的
	EC2：取消安全性群組	是的	是的	是的
	EC2：RevokeSecurityGroupEgress	是的	否	否
	EC2：授權安全性群組出口	是的	否	否
	EC2：授權安全性群組入口	是的	否	否
	EC2：RevokeSecurityGroupIngress	是的	是的	否
在Cloud Volumes ONTAP 目標子網路中建立及管理用於實現效能不中斷的網路介面	EC2：建立網路介面	是的	否	否
	EC2：網路介面	是的	是的	否
	EC2：刪除網路介面	否	是的	是的
	EC2：修改網路互連屬性	否	是的	否
取得目的地子網路和安全性群組清單	EC2：無資料子網路	是的	是的	否
	EC2：取消功能Vpcs	是的	是的	否
取得DNS伺服器 和Cloud Volumes ONTAP 預設的網域名稱以供執行個體使用	EC2：取消功能DhcpOptions	是的	否	否
拍攝EBS Volume的快照Cloud Volumes ONTAP 以供其使用	EC2：建立Snapshot	是的	是的	否
	EC2：刪除Snapshot	否	是的	是的
	EC2：取消快照	否	是的	否
擷取Cloud Volumes ONTAP 附加於AutoSupport 資訊畫面的功能	EC2：GetConsole輸出	是的	是的	否

目的	行動	用於部署？	用於日常營運？	用於刪除？
取得可用金鑰組的清單	EC2：評量會議	是的	否	否
取得可用AWS區域的清單	EC2：取消註冊	是的	是的	否
管理Cloud Volumes ONTAP 與實例相關的資源標記	EC2：刪除標記	否	是的	是的
	EC2：取消標示	否	是的	否
建立及管理AWS CloudFormation範本的堆疊	雲端：建立堆疊	是的	否	否
	雲端：刪除堆疊	是的	否	否
	雲端：無標準堆疊	是的	是的	否
	雲端：取消功能堆疊事件	是的	否	否
	cloudformation：驗證範本	是的	否	否

目的	行動	用於部署？	用於日常營運？	用於刪除？
建立並管理Cloud Volumes ONTAP S3儲存區、讓整個系統做為資料分層的容量層	S3：建立桶	是的	是的	否
	S3：刪除資源桶	否	是的	是的
	S3：Get生命週期組態	否	是的	否
	S3：Putt升降器組態	否	是的	否
	S3：PuttBucketting	否	是的	否
	S3：listBucketVerions	否	是的	否
	S3：GetBucketPolicy Status	否	是的	否
	S3：GetBucketPublic AccessBlock	否	是的	否
	S3：GetBucketAcl	否	是的	否
	S3：GetBucketPolicy	否	是的	否
	S3：PuttBucketPublic AccessBlock	否	是的	否
	S3：GetBucketting	否	是的	否
	S3：GetBucketLocati on	否	是的	否
	S3：ListAllMyb桶	否	否	否
	S3：清單庫	否	是的	否
使用Cloud Volumes ONTAP AWS金鑰管理服務（KMS）啟用資料加密功能	公里：清單*	是的	是的	否
	公里：ReEncrypt *	是的	否	否
	公里：描述*	是的	是的	否
	公里：建立授予	是的	是的	否

目的	行動	用於部署？	用於日常營運？	用於刪除？
取得AWS成本資料Cloud Volumes ONTAP 以供使用	CE : GetReservationUtilization	否	是的	否
	CE : GetDimensionValues	否	是的	否
	CE : GetCostAndusage	否	是的	否
	CE : GetTags	否	是的	否
在單一AWS可用性區域中、為兩個HA節點建立並管理AWS分散放置群組、以及協調器	EC2：建立位置群組	是的	否	否
	EC2：刪除位置群組	否	是的	是的
建立報告	FSX：說明*	否	是的	否
	FSX：清單*	否	是的	否
建立及管理可支援Amazon EBS彈性Volume功能的集合體	EC2：說明體積修改	否	是的	否
	EC2：修改Volume	否	是的	否

==全域檔案快取

Connector會在部署期間提出下列API要求、以部署全域檔案快取執行個體：

- 雲端：無標準堆疊
- cloudwatch：GetMetricStatistics
- 雲端：清單堆疊

== Kubernetes

Connector會提出下列API要求、以探索及管理Amazon EKS叢集：

- EC2：取消註冊
- EKS：清單叢集
- EKS：取消叢集
- IAM：GetInstanceProfile

連接器的**Azure**權限

Cloud Manager在Azure中啟動Connector VM時、會將自訂角色附加至VM、讓Connector

有權管理該Azure訂閱中的資源和程序。Connector會使用權限來撥打API呼叫數個Azure服務。

自訂角色權限

下列自訂角色提供Connector管理Azure網路中資源與程序所需的權限。

直接從Cloud Manager建立Connector時、Cloud Manager會自動將此自訂角色套用至Connector。

如果您從Azure Marketplace部署Connector、或是在Linux主機上手動安裝Connector、則必須自行設定自訂角色。

您也必須確保在後續版本中新增權限時、該角色是最新的。

```
{
  "Name": "Cloud Manager Operator",
  "Actions": [
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/disks/read",
    "Microsoft.Compute/disks/write",
    "Microsoft.Compute/locations/operations/read",
    "Microsoft.Compute/locations/vmSizes/read",

    "Microsoft.Resources/subscriptions/locations/read",
    "Microsoft.Compute/operations/read",

    "Microsoft.Compute/virtualMachines/instanceView/read",

    "Microsoft.Compute/virtualMachines/powerOff/action",
    "Microsoft.Compute/virtualMachines/read",

    "Microsoft.Compute/virtualMachines/restart/action",

    "Microsoft.Compute/virtualMachines/deallocate/action",
    "Microsoft.Compute/virtualMachines/start/action",
    "Microsoft.Compute/virtualMachines/vmSizes/read",
    "Microsoft.Compute/virtualMachines/write",
    "Microsoft.Compute/images/write",
    "Microsoft.Compute/images/read",

    "Microsoft.Network/locations/operationResults/read",
    "Microsoft.Network/locations/operations/read",
    "Microsoft.Network/networkInterfaces/read",
    "Microsoft.Network/networkInterfaces/write",
    "Microsoft.Network/networkInterfaces/join/action",
    "Microsoft.Network/networkSecurityGroups/read",
    "Microsoft.Network/networkSecurityGroups/write",
```

```
"Microsoft.Network/networkSecurityGroups/join/action",
    "Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
    "Microsoft.Network/virtualNetworks/subnets/read",
    "Microsoft.Network/virtualNetworks/subnets/write",

"Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",

"Microsoft.Network/virtualNetworks/virtualMachines/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",
    "Microsoft.Resources/deployments/operations/read",
    "Microsoft.Resources/deployments/read",
    "Microsoft.Resources/deployments/write",
    "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.Storage/checknameavailability/read",
    "Microsoft.Storage/operations/read",

"Microsoft.Storage/storageAccounts/listkeys/action",
    "Microsoft.Storage/storageAccounts/read",
    "Microsoft.Storage/storageAccounts/delete",

"Microsoft.Storage/storageAccounts/regeneratekey/action",
    "Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/storageAccounts/blobServices/containers/read",
    "Microsoft.Storage/usages/read",
    "Microsoft.Compute/snapshots/write",
    "Microsoft.Compute/snapshots/read",
    "Microsoft.Compute/availabilitySets/write",
    "Microsoft.Compute/availabilitySets/read",
    "Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements"
```

```

ts/read",

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

    "Microsoft.Network/loadBalancers/read",
    "Microsoft.Network/loadBalancers/write",
    "Microsoft.Network/loadBalancers/delete",

"Microsoft.Network/loadBalancers/backendAddressPools/read",

"Microsoft.Network/loadBalancers/backendAddressPools/join/action",

"Microsoft.Network/loadBalancers/frontendIPConfigurations/read",

"Microsoft.Network/loadBalancers/loadBalancingRules/read",
    "Microsoft.Network/loadBalancers/probes/read",

"Microsoft.Network/loadBalancers/probes/join/action",
    "Microsoft.Authorization/locks/*",
    "Microsoft.Network/routeTables/join/action",
    "Microsoft.NetApp/netAppAccounts/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",
    "Microsoft.Network/privateEndpoints/write",

"Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/action",

"Microsoft.Storage/storageAccounts/privateEndpointConnections/read",

"Microsoft.Storage/storageAccounts/managementPolicies/read",

"Microsoft.Storage/storageAccounts/managementPolicies/write",
    "Microsoft.Network/privateEndpoints/read",
    "Microsoft.Network/privateDnsZones/write",

"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
    "Microsoft.Network/virtualNetworks/join/action",
    "Microsoft.Network/privateDnsZones/A/write",
    "Microsoft.Network/privateDnsZones/read",

```

```

"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",

"Microsoft.Resources/deployments/operationStatuses/read",
    "Microsoft.Insights/Metrics/Read",

"Microsoft.Compute/virtualMachines/extensions/write",

"Microsoft.Compute/virtualMachines/extensions/delete",

"Microsoft.Compute/virtualMachines/extensions/read",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Network/networkInterfaces/delete",
    "Microsoft.Network/networkSecurityGroups/delete",
    "Microsoft.Resources/deployments/delete",
    "Microsoft.Compute/diskEncryptionSets/read",
    "Microsoft.Compute/snapshots/delete",
    "Microsoft.Network/privateEndpoints/delete",
    "Microsoft.Compute/availabilitySets/delete",
    "Microsoft.Network/loadBalancers/delete",
    "Microsoft.KeyVault/vaults/read",
    "Microsoft.KeyVault/vaults/accessPolicies/write",
    "Microsoft.Compute/diskEncryptionSets/write",
    "Microsoft.KeyVault/vaults/deploy/action",
    "Microsoft.Compute/diskEncryptionSets/delete",
    "Microsoft.Resources/tags/read",
    "Microsoft.Resources/tags/write",
    "Microsoft.Resources/tags/delete",

"Microsoft.Network/applicationSecurityGroups/write",

"Microsoft.Network/applicationSecurityGroups/read",

"Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action",

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

"Microsoft.Network/applicationSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/securityRules/delete"
],
    "NotActions": [],
    "AssignableScopes": [],
    "Description": "Cloud Manager Permissions",
    "IsCustom": "true"
}

```

Azure 權限的使用方式

行動	目的
Microsoft.Compute/locations/operations/read" 、 「 Microsoft.Compute/locations/vmSizes/read" 、 Microsoft.Compute/operations/read" 、 Microsoft.Compute/virtualMachines/instanceView/read " 、 「 Microsoft.Compute/virtualMachines/powerOff/action" 、 Microsoft.Compute/virtualMachines/read" 、 「 Microsoft.Compute/virtualMachines/restart/action" 、 Microsoft.Compute/virtualMachines/start/action" 、 Microsoft.Compute/virtualMachines/deallocate/action" 、 「 Microsoft.Compute/virtualMachines/vmSizes/read" 、 「 Microsoft.Compute/virtualMachines/write" 、	建立 Cloud Volumes ONTAP 不同時停止、啟動、刪除 及取得系統狀態。
「 Microsoft.Compute/images/write" 、 Microsoft.Compute/images/read" 、	可 Cloud Volumes ONTAP 從 VHD 進行支援功能性部 署。
Microsoft.Compute/disks/delete" 、 "Microsoft.Compute/disks/read" 、 "Microsoft.Compute/disks/write" 、 "microsoft.Storage/checkamed可用度 / 讀取 " 、 "microsoft.Storage/operations / 讀取 " 、 "Microsoft.Storage/storageAccounts/listkeys/action" 、 "Microsoft.Storage/storageAccounts/read" 、 "Microsoft.Storage/storageAccounts/再生金鑰 / 行動 " 、 "Microsoft.Storage/storageAccounts/write" 、 "Microsoft.Storage/storageAccounts/storageAccounts/ delete" 、 "Microsoft.Storage/改用 / 讀取 " 、	管理 Azure 儲存帳戶和磁碟、並將磁碟附加 Cloud Volumes ONTAP 至
"Microsoft.Storage/storageAccounts/blobServices/con tains/read" 、 "Microsoft.KeyVault/Vaults/read" 、 "Micro soft.KeyVault/Vaults/accessPolicys/write	可備份至 Azure Blob 儲存設備、並加密儲存帳戶
「 Microsoft.Network/networkInterfaces/read" 、 Microsoft.Network/networkInterfaces/write" 、 「 Microsoft.Network/networkInterfaces/join/action" 、	建立並管理 Cloud Volumes ONTAP 目標子網路中的網 路介面以供其使用。
「 Microsoft.Network/networkSecurityGroups/read" 、 Microsoft.Network/networkSecurityGroups/write" 、 「 Microsoft.Network/networkSecurityGroups/join/action" 、	建立預先定義 Cloud Volumes ONTAP 的網路安全群組 以供使用。

行動	目的
"Microsoft.Resources/訂購 / 位置 / 讀取 " 、 "Microsoft.Network/locations/operationResults/read" 、 "Microsoft.Network/locations/operations/read" 、 "Microsoft.Network/virtualNetworks/read" 、 "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read" 、 「 Microsoft.Network/virtualNetworks/subnets/read" 、 Microsoft.Network/virtualNetworks/subnets/virtualMachines/read" 、 「 Microsoft.Network/virtualNetworks/virtualMachines/read" 、 Microsoft.Network/virtualNetworks/subnets/join/action" 、	取得區域、目標 Vnet 和子網路的網路資訊、並將 Cloud Volumes ONTAP 之新增至 VNets 。
「 Microsoft.Network/virtualNetworks/subnets/write" 、 Microsoft.Network/routeTables/join/action" 、	啟用 vnet 服務端點以進行資料分層。
"microsoft.Resources/edges/operations / read" 、 "microsoft.Resources/edges/read" 、 "microsoft.Resources/edges/write" 、	從 Cloud Volumes ONTAP 範本部署功能。
"microsoft.Resources/editions/operations/read" 、 "microsoft.Resources/editions/read" 、 "microsoft.Resources/dations/read" 、 "microsoft.Resources/read" 、 "microsoft.Resources/dations/operations/read" 、 "Microsoft.Resources / 訂閱 / 資源群組 / 刪除 " 、 "Microsoft.Resources / 訂閱 / 資源群組 / 讀取 " 、 "Microsoft.Resources / 訂閱 / 資源群組 / 資源 / 讀取 " 、 "Microsoft.Resources / 訂閱 / 資源群組 / 寫入 " 、	建立及管理 Cloud Volumes ONTAP 資源群組以供參考。
「Microsoft.Compute/snapshots/write" 、 Microsoft.Compute/snapshots/read" 、 「Microsoft.Compute/snapshots/delete" 、 Microsoft.Compute/disks/beginGetAccess/action" 、	建立及管理 Azure 託管快照。
「 Microsoft.Compute/availabilitySets/write" 、 Microsoft.Compute/availabilitySets/read" 、	建立及管理 Cloud Volumes ONTAP 可用度集以供使用。
"Microsoft.MarketplaceOrdnation/offersTypes / 出版商 / 服務 / 方案 / 協議 / 讀取" 、 "Microsoft.MarketplaceOrdnations/offersTypes / 出版商 / 服務 / 計畫 / 協議 / 寫入" 、	可從 Azure Marketplace 進程式化部署。

行動	目的
Microsoft.Network/loadBalancers/read" 、 「 Microsoft.Network/loadBalancers/write" 、 Microsoft.Network/loadBalancers/delete" 、 Microsoft.Network/loadBalancers/backendAddressPools/read" 、 「 Microsoft.Network/loadBalancers/backendAddressPools/join/action" 、 「 Microsoft.Network/loadBalancers/frontendIPConfigurations/read" 、 Microsoft.Network/loadBalancers/loadBalancingRules/read" 、 「 Microsoft.Network/loadBalancers/probes/read" 、 Microsoft.Network/loadBalancers/probes/join/action" 、	管理 Azure 負載平衡器以供 HA 配對使用。
"Microsoft.Authorization/Locks/* 、	可管理 Azure 磁碟上的鎖定。
"Microsoft.Authorization/RoleDefinitions/write (Microsoft 授權 / 角色指派 / 寫入) " 、 "Microsoft.Web/sites/* (Microsoft 網站 / 網站 / *) "	管理 HA 配對的容錯移轉。
Microsoft.Network/privateEndpoints/write" 、 "Microsoft.Storage/storageAccounts/privateEndpointConnectionsApproval / AC 巨集指令 " 、 "Microsoft.Storage/storageAccounts/privateEndpointConnections/read" 、 "Microsoft.Network/privateEndpoints/read" 、 "Microsoft.Network/privateDnsZones/write" 、 Microsoft.Network/privateDnsZones/virtualNetworkLinks/write" 、 「 Microsoft.Network/virtualNetworks/join/action" 、 Microsoft.Network/privateDnsZones/A/write" 、 Microsoft.Network/privateDnsZones/read" 、 「 Microsoft.Network/privateDnsZones/virtualNetworkLinks/read" 、	可管理私有端點。未將連線提供給子網路外部時、會使用私有端點。Cloud Manager 會為 HA 建立儲存帳戶、但僅在子網路內建立內部連線功能。
「 Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete" 、	讓 Cloud Manager 能夠刪除 Volume 以 Azure NetApp Files 供使用。
"Microsoft.Resources / 部署 / 作業狀態 / 讀取 "	Azure 在某些虛擬機器部署中需要此權限（視部署期間所使用的基礎實體硬體而定）。
"microsoft.Resources/edges/operationStatuses/read" 、 "microsoft.Insights / Metrics / read" 、 "Microsoft.Compute/virtualMachines/extensions/write" 、 "Microsoft.Compute/virtualMachines/extensions/read" 、 "Microsoft.Compute/virtualMachines/extensions/delete" 、 Microsoft.Compute/virtualMachines/delete" 、 "Microsoft.Network/networkInterfaces/delete" 、 "Microsoft.Network/networkSecurityGroups/delete" 、 "microsoft.Resources/edges/delete" 、	可讓您使用全域檔案快取。

行動	目的
「Microsoft.Network/privateEndpoints/delete"、Microsoft.Compute/availabilitySets/delete"、	可讓Cloud Manager在Cloud Volumes ONTAP 部署失敗或刪除時、從屬於支援的資源群組移除資源。
Microsoft.Compute/diskEncryptionSets/read"「Microsoft.Compute/diskEncryptionSets/write"」、「Microsoft.Compute/diskEncryptionSets/delete""microsoft.KeyVault/Vaults/Deploy / action」、「microsoft.KeyVault/Vaults/read」、「microsoft.KeyVault/Vaults/accesss/write」、	可搭配Cloud Volumes ONTAP 使用客戶管理的加密金鑰。API 支援此功能。
"Microsoft.Resources/標記/讀取"、 "Microsoft.Resources/標記/寫入" "Microsoft.Resources/標記/刪除"	可讓您使用Cloud Manager標記服務來管理Azure資源上的標記。
Microsoft.Network/applicationSecurityGroups/write"、 「Microsoft.Network/applicationSecurityGroups/read"、 Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action"、 Microsoft.Network/networkSecurityGroups/securityRules/write"、 「Microsoft.Network/applicationSecurityGroups/delete"、 「Microsoft.Network/networkSecurityGroups/securityRules/delete"	可讓Cloud Manager設定HA配對的應用程式安全群組、隔離HA互連和叢集網路NIC。

Connector的Google Cloud權限

Cloud Manager需要權限才能在Google Cloud中執行動作。這些權限包含在NetApp提供的自訂角色中。您可能想要瞭解 Cloud Manager 使用這些權限的功能。

服務帳戶權限

下方顯示的自訂角色提供Connector在Google Cloud網路中管理資源和程序所需的權限。

您必須將此自訂角色套用至連接器VM的服務帳戶。 [檢視逐步指示](#)。

您也必須確保在後續版本中新增權限時、該角色是最新的。

```

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

如何使用Google Cloud權限

行動	目的
- compute 、 disks.create - compute 、 disks.createSnapshot - compute.disks.delete - compute 、 disks.Get - compute 、 disks.list - compute.disks.setLabels - compute.disks.use	建立及管理 Cloud Volumes ONTAP 磁碟以供使用。

行動	目的
- compute 、防火牆、 create - compute.firewalls.delete - compute 、防火牆、 Get - compute 、防火牆、 list	建立 Cloud Volumes ONTAP 防火牆規則以供使用。
運算： globalOperations 。 Get	以取得作業狀態。
- compiler.images.Get - compile.images.getFromFamily - compile.images.list - compute.images.useReadOnly	取得 VM 執行個體的映像。
- compute.instances.attachDisk - compute.instances.detachDisk	可將磁碟安裝到 Cloud Volumes ONTAP 實體上、並將其拆離。
- compute.instances.create - compute.instances.delete	建立及刪除 Cloud Volumes ONTAP 不顯示的 VM 執行個體。
- compute.instances.get	列出 VM 執行個體。
- compute.instances.getSerialPortOutput	以取得主控台記錄。
- compute.instances.list	可檢索區域中的實例列表。
- compute.instances.setDeletionProtection	設定執行個體的刪除保護。
- compute.instances.setLabels	以新增標籤。
- compute.instances.setMachineType - compute.instances.setMinCpuPlatform	變更 Cloud Volumes ONTAP 機器類型以供使用。
- compute.instances.setMetadata	新增中繼資料。
- compute.instances.setTags	新增防火牆規則的標記。
- compute.instances.start - compute.instances.stop - compute.instances.updateDisplayDevice	開始和停止 Cloud Volumes ONTAP 功能。
- compute 。 machineTypes 。 Get	取得要檢查 qoutas 的核心數量。
- compute.projects.get	支援多個專案。
- compute 、 snapshots.create - compute.snapshots.delete - compute 、 snapshots.Get - compute 、 snapshots.list - compute.snapshots.setLabels	以建立及管理持續磁碟快照。
- compute.networks.get - compute.networks.list - compute .regions.Get - compute .regions.list - compute .subnetworks .Get - compute .subnetworks .list - compute .zonewores.Get - compute .zones.list	取得建立全新 Cloud Volumes ONTAP 的物件虛擬機器執行個體所需的網路資訊。

行動	目的
deploymentmanager.compositeTypes.get - deploymentmanager.compositeTypes.list - deploymentmanager.deployments.create - deploymentmanager.deployments.delete - deploymentmanager.deployments.get - deploymentmanager.deployments.list - deploymentmanager.in清單 - deploymentmanager.in 清單 - deploymentmanager.in清單 - deploymentmanager.operations - deploymentmanager.operations .list - deploymentmanager.sepairs.Get - deploymentmanager.operations - deploymentmanager.types.list - deploymentmanager.list	使用 Cloud Volumes ONTAP Google Cloud Deployment Manager 部署物件虛擬機器執行個體。
- logging.logEntries .list - logging.privateLogEntries .list	以取得堆疊記錄磁碟機。
- resourceManager.projects.get	支援多個專案。
- storage 、 buckets 、 create - storage.buckets.delete - storage 、 buckets 、 storage 、 buckets 、 list - storage 、 buckets 、 update	建立及管理 Google Cloud Storage 儲存庫以進行資料分層。
- cloudkms.cryptoKeyVersions.useToEncrypt - cloudkms.cryptoKeys.Get - cloudkms.cryptoKeys.list - cloudkms.keycycles.list	搭配 Cloud Volumes ONTAP 使用 Cloud Key Management Service 的客戶管理加密金鑰。
- compute.instances.setServiceAccount - iam.serviceAccounts.actAs - iam.serviceAccounts.getIamPolicy - iam.serviceAccounts.list - 儲存空間 .objects.Get - 儲存 空間 .objects.list	在 Cloud Volumes ONTAP 整個過程中設定服務帳戶。此服務帳戶提供資料分層至 Google Cloud Storage 儲存庫的權限。
- compute 、 addresses.list - compute 、 backendServices.create - compute.networks.updatePolicy - compute 、 Region. 、 BackendServices.create - compute 、 Region. 、 BackendServices.list	部署 HA 配對。
- compute.subnetworks.use - compute.subnetworks.useExternallp - compute.instances.addAccessConfig	以實現Cloud Data Sense。
- container 。叢集 。Get - container 。叢集 。清單	探索在Google Kubernetes Engine中執行的Kubernetes叢集。
- compute.instanceGroups.get - compute 、 addresses.Get	在HA配對上建立及管理儲存VM。

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> [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。

- ["Cloud Manager 3.9 注意事項"](#)

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。