NetApp Console入門（受限模式）

NetApp Console setup and administration

NetApp
February 11, 2026

This PDF was generated from https://docs.netapp.com/zh-tw/console-setup-admin/task-quick-start-restricted-mode.html on February 11, 2026. Always check docs.netapp.com for the latest.

目錄

NetApp Console入門（受限模式）

入門工作流程（受限模式）

透過準備環境和部署控制台代理，開始以受限模式使用NetApp Console。

受限模式通常由州和地方政府以及受監管的公司使用，包括在 AWS GovCloud 和 Azure Government 區域中的部署。在開始之前，請確保您了解"控制台代理"和"部署模式"。

1 "準備部署"

1. 準備一個符合 CPU、RAM、磁碟空間、容器編排工具等要求的專用 Linux 主機。
2. 設定提供對目標網路的存取、用於手動安裝的出站網路存取以及用於日常存取的出站網路的網路。
3. 在您的雲端提供者中設定權限，以便您可以在部署控制台代理程式實例後將這些權限與控制台代理程式實例關聯。

2 "部署控制台代理"

1. 從雲端提供者的市場安裝控制台代理，或在您自己的 Linux 主機上手動安裝該軟體。
2. 透過開啟 Web 瀏覽器並輸入 Linux 主機的 IP 位址來設定NetApp Console。
3. 向控制台代理提供您先前設定的權限。

3 "訂閱NetApp Intelligent Services（可選）"

可選：從雲端供應商的市場訂閱NetApp Intelligent Services，以按小時費率（PAYGO）或透過年度合約支付資料服務費用。 NetApp Intelligent Services包括NetApp Backup and Recovery、 Cloud Volumes ONTAP、 NetApp Cloud Tiering、 NetApp Ransomware Resilience和NetApp Disaster Recovery。 NetApp Data Classification包含在您的訂閱中，無需額外付費。

準備在受限模式下部署

在受限模式下部署NetApp Console之前，請準備好您的環境。您需要查看主機需求、準備網路、設定權限等。

步驟 1：了解限制模式的工作原理

在開始之前了解NetApp Console在受限模式下的工作方式。

使用已安裝的NetApp Console代理程式本機提供的基於瀏覽器的介面。您無法從透過 SaaS 層提供的基於 Web 的控制台存取NetApp Console。

此外，並非所有控制台功能和NetApp資料服務都可使用。

"了解限制模式的工作原理" 。

第 2 步：查看安裝選項

在受限模式下，您只能在雲端安裝控制台代理程式。有以下安裝選項可用：

- 來自 AWS Marketplace
- 來自 Azure 市場
- 在 AWS、Azure 或 Google Cloud 中執行的 Linux 主機上手動安裝控制台代理

第 3 步：查看主機需求

主機必須滿足特定的作業系統、RAM 和連接埠要求才能執行控制台代理。

當您從 AWS 或 Azure 市場部署控制台代理程式時，映像包含所需的作業系統和軟體元件。您只需選擇符合 CPU 和 RAM 要求的執行個體類型。

專用主機

控制台代理需要專用主機。只要滿足以下尺寸要求，任何架構都受支援：

- CPU：8 核心或 8 個 vCPU
- 記憶體：32 GB
- 磁碟空間：建議主機預留165GB空間，分割區需求如下：
  - `/opt`：必須有 120 GiB 可用空間

    代理使用 `/opt`安裝 `/opt/application/netapp`目錄及其內容。

  - `/var`：必須有 40 GiB 可用空間

    控制台代理需要此空間 `/var`因為 Podman 或 Docker 的設計初衷就是在這個目錄下建立容器。具體來說，他們將在以下位置建立容器： `/var/lib/containers/storage`目錄和 `/var/lib/docker`用於 Docker。外部安裝或符號連結不適用於此空間。

AWS EC2 執行個體類型

滿足 CPU 和 RAM 要求的實例類型。 NetApp推薦使用 t3.2xlarge。

Azure VM 大小

滿足 CPU 和 RAM 要求的實例類型。 NetApp推薦 Standard_D8s_v3。

Google Cloud 機器類型

滿足 CPU 和 RAM 要求的實例類型。NetApp推薦 n2-standard-8。

Google Cloud 虛擬機器實例上的控制台代理程式支援下列作業系統： "受防護的虛擬機器功能"

虛擬機器管理程序

需要經過認證可運行支援的作業系統的裸機或託管虛擬機器管理程式。

作業系統和容器要求

在標準模式或受限模式下使用控制台時，控制台代理程式支援下列作業系統。安裝代理之前需要一個容器編

排工具。

作業系統	支援的作業系統版本	支援的代理版本	所需的容器工具	**SELinux**
紅帽企業 Linux		9.6 • 僅限英文版本。 • 主機必須在 Red Hat 訂閱管理中註冊。如果未註冊，主機將無法在代理安裝期間存取儲存庫來更新所需的第三方軟體。	4.0.0 或更高版本，控制台處於標準模式或受限模式	Podman 版本 5.4.0，podman-compose 版本 1.5.0。 查看 Podman 設定要求 。
在強制模式或寬容模式下受支持		9.1 至 9.4 • 僅限英文版本。 • 主機必須在 Red Hat 訂閱管理中註冊。如果未註冊，主機將無法在代理安裝期間存取儲存庫來更新所需的第三方軟體。	3.9.50 或更高版本，控制台處於標準模式或受限模式	Podman 版本 4.9.4，podman-compose 版本 1.5.0。 查看 Podman 設定要求 。
在強制模式或寬容模式下受支持		8.6 至 8.10 • 僅限英文版本。 • 主機必須在 Red Hat 訂閱管理中註冊。如果未註冊，主機將無法在代理安裝期間存取儲存庫來更新所需的第三方軟體。	3.9.50 或更高版本，控制台處於標準模式或受限模式	Podman 版本 4.6.1 或 4.9.4，搭配 podman-compose 1.0.6。 查看 Podman 設定要求 。
在強制模式或寬容模式下受支持	Ubuntu		24.04 LTS	3.9.45 或更高版本，NetApp Console處於標準模式或受限模式
Docker Engine 23.06 至 28.0.0。	不支援		22.04 LTS	3.9.50 或更高版本

步驟 4：安裝 Podman 或 Docker Engine

若要手動安裝控制台代理，請透過安裝 Podman 或 Docker Engine 來準備主機。

根據您的作業系統，安裝代理程式之前需要 Podman 或 Docker Engine。

- Red Hat Enterprise Linux 8 和 9 需要 Podman。

  查看支援的 Podman 版本 。

- Ubuntu 需要 Docker 引擎。

  查看支援的 Docker Engine 版本 。

範例 **1.** 步驟

Podman

請依照以下步驟安裝和設定 Podman：

- 啟用並啟動 podman.socket 服務
- 安裝python3
- 安裝 podman-compose 套件版本 1.0.6
- 將 podman-compose 加入到 PATH 環境變量
- 如果使用 Red Hat Enterprise Linux，請驗證您的 Podman 版本使用的是 Netavark Aardvark DNS 而不是 CNI

> 安裝代理程式後調整 aardvark-dns 連接埠（預設值：53），以避免 DNS 連接埠衝突。按照說明配置連接埠。

步驟

1. 如果主機上安裝了 podman-docker 套件，請將其刪除。

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. 安裝 Podman。

   您可以從官方 Red Hat Enterprise Linux 儲存庫取得 Podman。

   a. 對於 Red Hat Enterprise Linux 9.6：

   ```
   sudo dnf install podman-5:<version>
   ```

   其中 <version> 是您正在安裝的 Podman 支援的版本。查看支援的 Podman 版本 。

   b. 適用於 Red Hat Enterprise Linux 9.1 至 9.4：

   ```
   sudo dnf install podman-4:<version>
   ```

   其中 <version> 是您正在安裝的 Podman 支援的版本。查看支援的 Podman 版本 。

   c. 對於 Red Hat Enterprise Linux 8：

   ```
   sudo dnf install podman-4:<version>
   ```

   其中 <version> 是您正在安裝的 Podman 支援的版本。查看支援的 Podman 版本 。

3. 啟用並啟動 podman.socket 服務。

```
sudo systemctl enable --now podman.socket
```

4. 安裝 python3。

```
sudo dnf install python3
```

5. 如果您的系統上還沒有 EPEL 儲存庫包，請安裝它。

   此步驟是必要的，因為 podman-compose 可從 Extra Packages for Enterprise Linux (EPEL) 儲存庫中取得。

6. 如果使用 Red Hat Enterprise 9：

   a. 安裝EPEL存儲庫軟體包。

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

   +

   a. 安裝 podman-compose 套件 1.5.0。

```
sudo dnf install podman-compose-1.5.0
```

7. 如果使用的是 Red Hat Enterprise Linux 8：

   a. 安裝EPEL存儲庫軟體包。

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

   b. 安裝 podman-compose 套件 1.0.6。

```
sudo dnf install podman-compose-1.0.6
```

   使用 `dnf install`指令滿足將 podman-compose 新增至 PATH 環境變數的要求。安裝指令將 podman-compose 新增至 /usr/bin，它已經包含在 `secure_path`主機上的選項。

   c. 如果使用 Red Hat Enterprise Linux 8，請驗證您的 Podman 版本是否使用具有 Aardvark DNS 的 NetAvark 而不是 CNI。

i. 透過執行以下命令檢查您的 networkBackend 是否設定為 CNI：

```
podman info | grep networkBackend
```

ii. 如果 networkBackend 設定為 `CNI`，你需要將其更改為 `netavark`。

iii. 安裝 `netavark`和 `aardvark-dns`使用以下命令：

```
dnf install aardvark-dns netavark
```

iv. 打開 `/etc/containers/containers.conf`檔案並修改 network_backend 選項以使用“netavark”而不是“cni”。

如果 `/etc/containers/containers.conf`不存在，請將配置變更為 `/usr/share/containers/containers.conf`。

v. 重新啟動 podman。

```
systemctl restart podman
```

vi. 使用以下命令確認 networkBackend 現在已更改為“netavark”：

```
podman info | grep networkBackend
```

Docker 引擎

依照 Docker 的文件安裝 Docker Engine。

步驟

1. "查看 Docker 的安裝說明"

   請依照步驟安裝支援的 Docker Engine 版本。請勿安裝最新版本，因為控制台不支援它。

2. 驗證 Docker 是否已啟用並正在運行。

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

步驟 5：準備網路訪問

設定網路訪問，以便控制台代理可以管理公有雲中的資源。除了為控制台代理提供虛擬網路和子網路之外，您還需要確保滿足以下要求。

連接到目標網絡

確保控制台代理程式與儲存位置有網路連線。例如，您計劃部署Cloud Volumes ONTAP 的VPC 或 VNet，或您的本機ONTAP叢集所在的資料中心。

準備網路以供使用者存取**NetApp Console**

在受限模式下，使用者從控制台代理 VM 存取控制台。控制台代理聯繫幾個端點來完成資料管理任務。當從控制台完成特定操作時，將從使用者的電腦聯繫這些端點。

4.0.0 版本之前的控制台代理需要額外的端點。如果您升級到 4.0.0 或更高版本，則可以從允許清單中刪除舊端點。"了解有關 4.0.0 之前版本所需的網路存取的更多資訊。"

+

端點	目的
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	在NetApp Console中提供功能和服務。
\ https://cdn.auth0.com \ https://services.cloud.netapp.com	您的 Web 瀏覽器透過NetApp Console連線到這些端點以進行集中使用者驗證。

用於日常運營的出站互聯網訪問

控制台代理程式的網路位置必須具有出站網際網路存取權限。它需要能夠存取NetApp Console的 SaaS 服務以及各自公有雲環境中的端點。

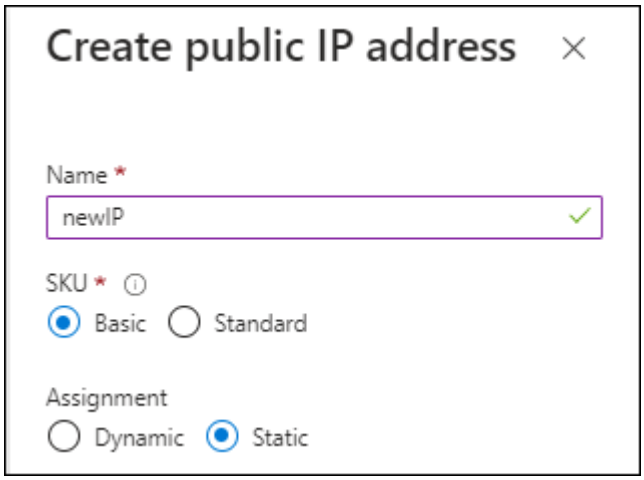
端點	目的
AWS 環境	AWS 服務（amazonaws.com）： • 雲形成 • 彈性運算雲（EC2） • 身分和存取管理 (IAM) • 金鑰管理服務（KMS） • 安全性令牌服務 (STS) • 簡單儲存服務（S3）
管理 AWS 資源。端點取決於您的 AWS 區域。 "有關詳細信息，請參閱 AWS 文檔"	Amazon FsX for NetApp ONTAP： • api.workloads.netapp.com
基於 Web 的控制台透過與 Workload Factory API 互動來管理和操作基於ONTAP 的FSx 工作負載。	Azure 環境

端點	目的
\ https://management.azure.com \ https://login.microsoftonline.com \ https://blob.core.windows.net \ https://core.windows.net	管理 Azure 公用區域中的資源。
\ https://management.usgovcloudapi.net \ https://login.microsoftonline.us \ https://blob.core.usgovcloudapi.net \ https://core.usgovcloudapi.net	管理 Azure 政府區域中的資源。
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	管理 Azure 中國區域的資源。
Google Cloud 環境	\ https://www.googleapis.com/compute/v1/ \ https://compute.googleapis.com/compute/v1 \ https://cloudresourcemanager.googleapis.com/v1/projects \ https://www.googleapis.com/compute/beta https://www.googleapis.com/storage/v1 https://storage.googleapis.com/storage/v1 https://iam.googleapis.com/v1 \ https://cloudkms.googleapis.com/v1 \ https://config.googleapis.com/v1/projects
管理 Google Cloud 中的資源。	• NetApp Console端點*
\ https://mysupport.netapp.com	取得許可資訊並向NetApp支援發送AutoSupport訊息。
\ https://signin.b2c.netapp.com	更新NetApp支援網站 (NSS) 憑證或將新的 NSS 憑證新增至NetApp Console。
\ https://support.netapp.com	取得許可資訊並向NetApp支援發送AutoSupport訊息以及接收Cloud Volumes ONTAP的軟體更新。
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	在NetApp Console中提供功能和服務。

端點	目的
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	取得控制台代理升級的影像。 • 當您部署新代理程式時，驗證檢查會測試與目前端點的連線。如果你使用"先前的端點"，驗證檢查失敗。為了避免此失敗，請跳過驗證檢查。 儘管先前的端點仍然受支持，但NetApp建議盡快將防火牆規則更新至目前端點。"了解如何更新終端節點列表"。 • 當您更新到防火牆中的目前端點時，您現有的代理程式將繼續運作。

Azure 中的公用 **IP** 位址

如果要在 Azure 中將公用 IP 位址與控制台代理程式 VM 一起使用，則該 IP 位址必須使用基本 SKU 以確保控制台使用此公用 IP 位址。



如果您使用標準 SKU IP 位址，則控制台將使用控制台代理程式的_私有_ IP 位址，而不是公用 IP。如果您用於存取控制台的機器無法存取該私人 IP 位址，則控制台中的操作將會失敗。

"Azure 文件：公用 IP SKU"

代理伺服器

NetApp支援顯式和透明代理配置。如果您使用透明代理，則只需要提供代理伺服器的憑證。如果您使用明確代理，您還需要 IP 位址和憑證。

- IP 位址
- 證書
- HTTPS 憑證

連接埠

除非您啟動它或將其用作代理將AutoSupport訊息從Cloud Volumes ONTAP發送到NetApp支持，否則控制台代理不會有傳入流量。

- HTTP（80）和 HTTPS（443）提供對本機 UI 的訪問，您會在極少數情況下使用它們。
- 僅當需要連接到主機進行故障排除時才需要 SSH（22）。
- 如果您在沒有外部網路連線的子網路中部署Cloud Volumes ONTAP系統，則需要透過連接埠 3128 建立入站連線。

  如果Cloud Volumes ONTAP系統沒有出站網路連線來傳送AutoSupport訊息，控制台會自動設定這些系統以使用控制台代理附帶的代理伺服器。唯一的要求是確保控制台代理的安全群組允許透過連接埠 3128 進行入站連線。部署控制台代理程式後，您需要開啟此連接埠。

啟用 **NTP**

如果您打算使用NetApp Data Classification來掃描公司資料來源，則應在控制台代理程式和NetApp Data Classification系統上啟用網路時間協定 (NTP) 服務，以便系統之間的時間同步。 "了解有關NetApp資料分類的更多信息"

如果您打算從雲端提供者的市場建立控制台代理，請在建立控制台代理後實現此網路需求。

步驟 6：準備雲端權限

控制台代理程式需要雲端提供者的權限才能在虛擬網路中部署Cloud Volumes ONTAP並使用NetApp資料服務。您需要在雲端提供者中設定權限，然後將這些權限與控制台代理程式關聯。

若要查看所需的步驟，請選擇用於雲端提供者的身份驗證選項。

AWS IAM 角色

使用 IAM 角色為控制台代理提供權限。

如果您從 AWS Marketplace 建立控制台代理，則在啟動 EC2 執行個體時系統會提示您選擇該 IAM 角色。

如果您在自己的 Linux 主機上手動安裝控制台代理，請將角色附加到 EC2 執行個體。

步驟

1. 登入 AWS 主控台並導覽至 IAM 服務。
2. 建立策略：
   a. 選擇“策略”>“建立策略”。
   b. 選擇 **JSON** 並複製並貼上內容"控制台代理的 IAM 策略"。
   c. 完成剩餘步驟以建立策略。
3. 建立 IAM 角色：
   a. 選擇*角色 > 建立角色*。
   b. 選擇 **AWS** 服務 **> EC2**。
   c. 透過附加剛剛建立的策略來新增權限。
   d. 完成剩餘步驟以建立角色。

結果

您現在擁有控制台代理 EC2 執行個體的 IAM 角色。

AWS 存取金鑰

為 IAM 使用者設定權限和存取金鑰。安裝控制台代理程式並設定控制台後，您需要向控制台提供 AWS 存取金鑰。

步驟

1. 登入 AWS 主控台並導覽至 IAM 服務。
2. 建立策略：
   a. 選擇“策略”>“建立策略”。
   b. 選擇 **JSON** 並複製並貼上內容"控制台代理的 IAM 策略"。
   c. 完成剩餘步驟以建立策略。

      根據您計劃使用的NetApp資料服務，您可能需要建立第二個策略。

   對於標準區域，權限分佈在兩個策略中。由於 AWS 中託管策略的最大字元大小限制，因此需要兩個策略。"了解有關控制台代理的 IAM 策略的更多信息" 。
3. 將策略附加到 IAM 使用者。
   - "AWS 文件：建立 IAM 角色"
   - "AWS 文件：新增和刪除 IAM 政策"

4. 確保使用者擁有存取金鑰，您可以在安裝控制台代理後將其新增至NetApp Console。

Azure 角色

建立具有所需權限的 Azure 自訂角色。您將把此角色指派給控制台代理 VM。

請注意，您可以使用 Azure 入口網站、Azure PowerShell、Azure CLI 或 REST API 建立 Azure 自訂角色。以下步驟展示如何使用 Azure CLI 建立角色。如果您希望使用其他方法，請參閱 "Azure 文件"

步驟

1. 如果您打算在自己的主機上手動安裝軟體，請在 VM 上啟用系統指派的託管標識，以便您可以透過自訂角色提供所需的 Azure 權限。

   "Microsoft Azure 文件：使用 Azure 入口網站為 VM 上的 Azure 資源配置託管標識"

2. 複製"連接器的自訂角色權限"並將它們保存在 JSON 檔案中。
3. 透過將 Azure 訂閱 ID 新增至可分配範圍來修改 JSON 檔案。

   您應該為想要與NetApp Console一起使用的每個 Azure 訂閱新增 ID。

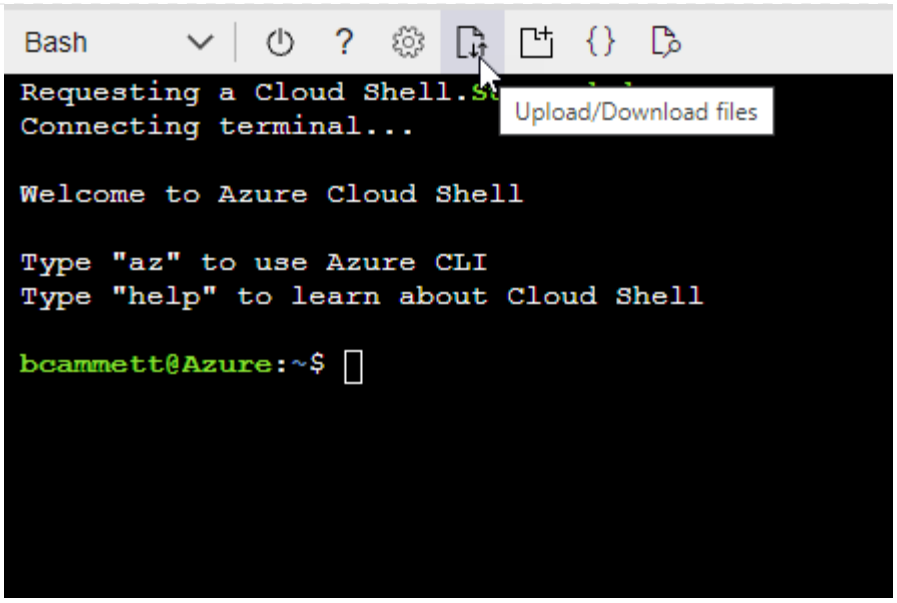
   例子

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

4. 使用 JSON 檔案在 Azure 中建立自訂角色。

   以下步驟說明如何使用 Azure Cloud Shell 中的 Bash 建立角色。

   a. 開始 "Azure 雲端外殼"並選擇 Bash 環境。
   b. 上傳 JSON 檔案。



c. 使用 Azure CLI 建立自訂角色：

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

Azure 服務主體

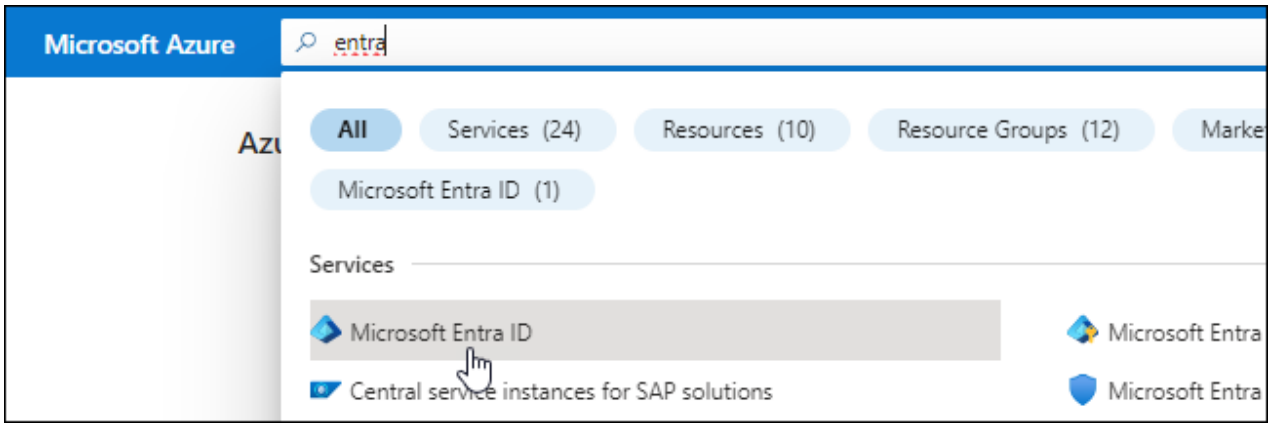
在 Microsoft Entra ID 中建立並設定服務主體，並取得控制台所需的 Azure 憑證。安裝控制台代理程式後，您需要向控制台提供這些憑證。

建立用於基於角色的存取控制的 **Microsoft Entra** 應用程式

1. 確保您在 Azure 中擁有建立 Active Directory 應用程式並將該應用程式指派給角色的權限。

   有關詳細信息，請參閱 "Microsoft Azure 文件：所需權限"

2. 從 Azure 入口網站開啟 **Microsoft Entra ID** 服務。



3. 在選單中，選擇*應用程式註冊*。
4. 選擇*新註冊*。
5. 指定有關應用程式的詳細資訊：

- 名稱：輸入應用程式的名稱。
- 帳戶類型：選擇帳戶類型（任何類型都可以與NetApp Console一起使用）。
- 重定向 **URI**：您可以將此欄位留空。

6. 選擇*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

1. 建立自訂角色：

請注意，您可以使用 Azure 入口網站、Azure PowerShell、Azure CLI 或 REST API 建立 Azure 自訂角色。以下步驟展示如何使用 Azure CLI 建立角色。如果您希望使用其他方法，請參閱 "Azure 文件"

a. 複製"控制台代理程式的自訂角色權限"並將它們保存在 JSON 檔案中。

b. 透過將 Azure 訂閱 ID 新增至可分配範圍來修改 JSON 檔案。

您應該為使用者將從中建立Cloud Volumes ONTAP系統的每個 Azure 訂閱新增 ID。

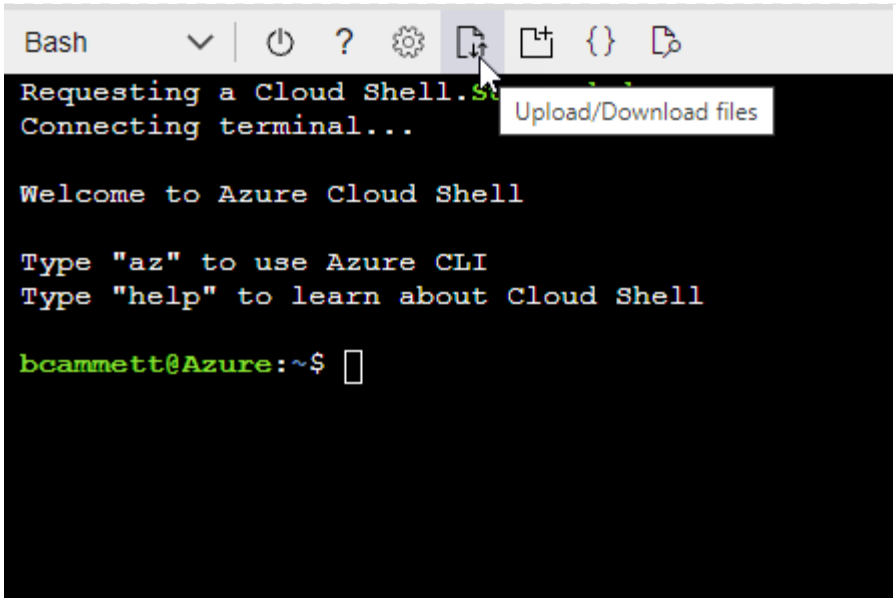
例子

```
"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。

以下步驟說明如何使用 Azure Cloud Shell 中的 Bash 建立角色。

- 開始 "Azure 雲端外殼"並選擇 Bash 環境。
- 上傳 JSON 檔案。



- 使用 Azure CLI 建立自訂角色：

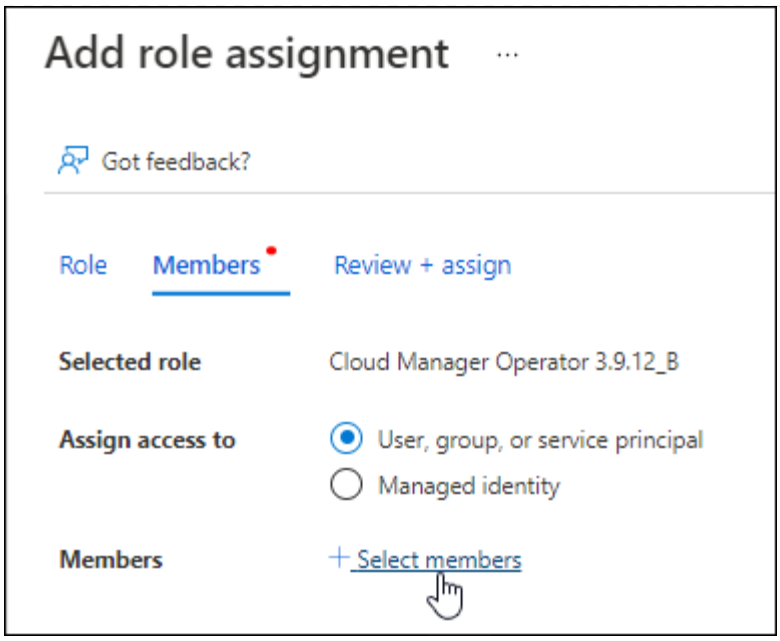
```
az role definition create --role-definition agent_Policy.json
```

現在您應該有一個名為「控制台操作員」的自訂角色，可以將其指派給控制台代理虛擬機器。

2. 將應用程式指派給角色：

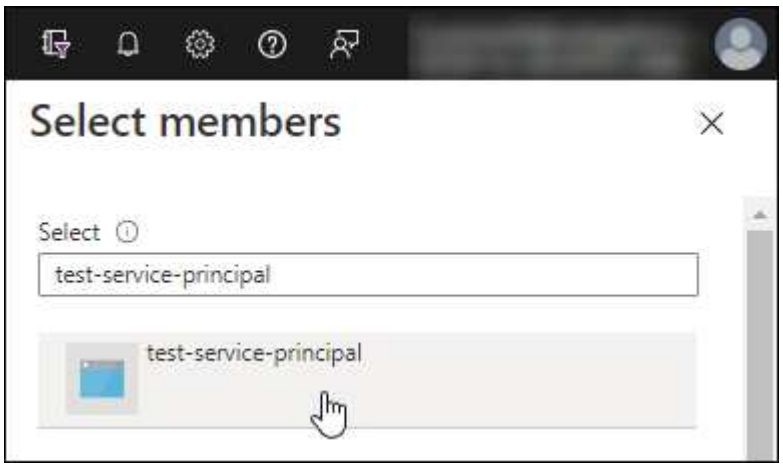
   a. 從 Azure 入口網站開啟 **Subscriptions** 服務。
   b. 選擇訂閱。
   c. 選擇“存取控制 (IAM)”>“新增”>“新增角色分配”。
   d. 在*角色*標籤中，選擇*控制台操作員*角色並選擇*下一步*。
   e. 在「成員」標籤中，完成以下步驟：

      - 保持選取「使用者、群組或服務主體」。
      - 選擇*選擇成員*。



- 搜尋應用程式的名稱。

  以下是一個例子：



- 選擇應用程式並選擇*選擇*。
- 選擇“下一步”。

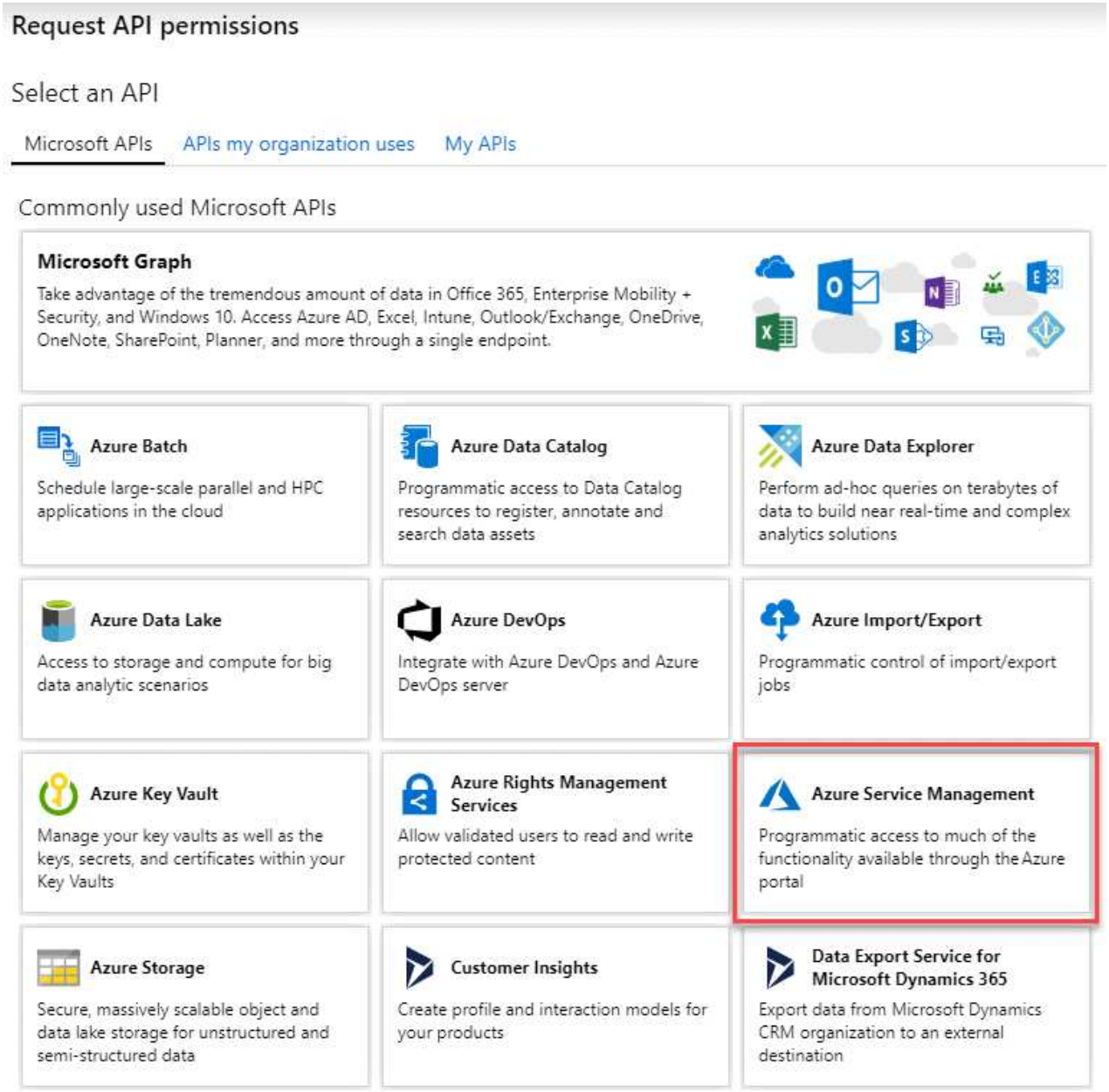
f. 選擇*審閱+分配*。

服務主體現在具有部署控制台代理程式所需的 Azure 權限。

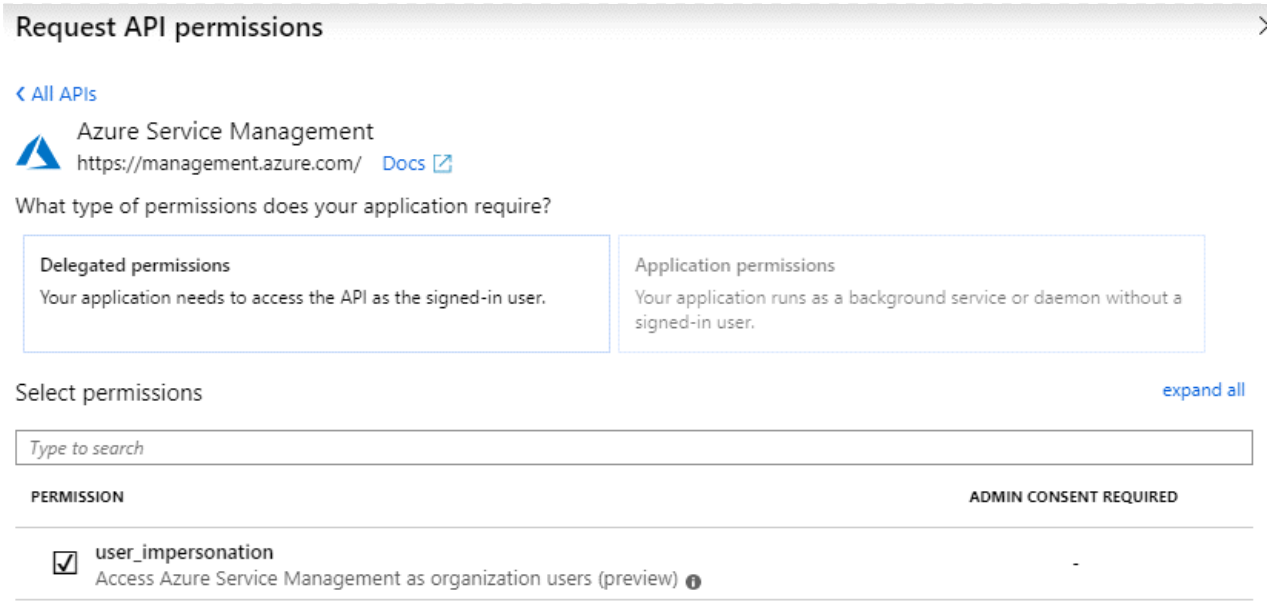
如果您想要從多個 Azure 訂閱部署Cloud Volumes ONTAP ，則必須將服務主體綁定到每個訂閱。在NetApp Console中，您可以選擇部署Cloud Volumes ONTAP時要使用的訂閱。

新增 **Windows Azure** 服務管理 **API** 權限

1. 在*Microsoft Entra ID*服務中，選擇*App Registrations*並選擇應用程式。
2. 選擇*API 權限 > 新增權限*。
3. 在「Microsoft API」下，選擇「Azure 服務管理」。

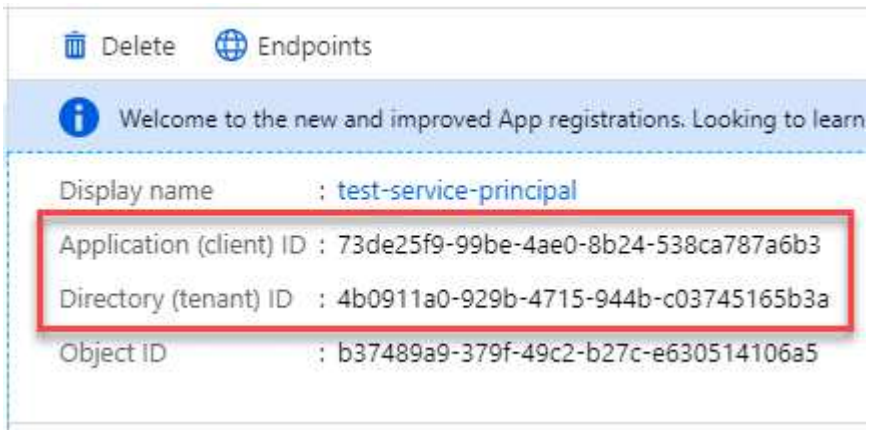


4. 選擇*以組織使用者身分存取 Azure 服務管理*，然後選擇*新增權限*。



取得應用程式的應用程式**ID**和目錄**ID**

1. 在*Microsoft Entra ID*服務中，選擇*App Registrations*並選擇應用程式。
2. 複製*應用程式（客戶端）ID*和*目錄（租用戶）ID*。



將 Azure 帳戶新增至控制台時，您需要提供應用程式（用戶端）ID 和應用程式的目錄（租用戶）ID。控制台使用 ID 以程式設計方式登入。

建立客戶端機密

1. 開啟*Microsoft Entra ID*服務。
2. 選擇*應用程式註冊*並選擇您的應用程式。
3. 選擇*憑證和機密>新客戶端機密*。
4. 提供秘密的描述和持續時間。
5. 選擇“新增”。
6. 複製客戶端機密的值。

結果

您的服務主體現已設定完畢，您應該已經複製了應用程式（客戶端）ID、目錄（租用戶）ID 和用戶端機密的值。新增 Azure 帳戶時，您需要在控制台中輸入此資訊。

Google Cloud 服務帳號

建立角色並將其套用至您將用於控制台代理 VM 執行個體的服務帳戶。

步驟

1. 在 Google Cloud 中建立自訂角色：

   a. 建立一個 YAML 文件，其中包含在"Google Cloud 的控制台代理政策"。

   b. 從 Google Cloud 啟動雲殼。

   c. 上傳包含控制台代理程式所需權限的 YAML 檔案。

   d. 使用建立自訂角色 `gcloud iam roles create`命令。

      以下範例在專案層級建立一個名為「agent」的角色：

```
gcloud iam roles create agent --project=myproject --file=agent.yaml
```

   +
   "Google Cloud 文件：建立和管理自訂角色"

2. 在 Google Cloud 中建立服務帳號：

   a. 從 IAM 和管理服務中，選擇 服務帳戶 > 建立服務帳戶。

   b. 輸入服務帳戶詳細資料並選擇*建立並繼續*。

   c. 選擇您剛剛建立的角色。

   d. 完成剩餘步驟以建立角色。

      "Google Cloud 文件：建立服務帳號"

步驟 7：啟用 Google Cloud API

在 Google Cloud 中部署Cloud Volumes ONTAP需要多個 API。

步

1. "在您的專案中啟用以下 Google Cloud API"
    - 雲端部署管理器 V2 API
    - 雲端基礎架構管理器 API
    - 雲端日誌 API
    - 雲端資源管理器 API
    - 計算引擎 API
    - 身分識別和存取管理 (IAM) API
    - Cloud Key Management Service (KMS) API（僅當您打算使用 NetApp Backup and Recovery 搭配客戶管理的加密金鑰（CMEK）時才需要）
    - Cloud Quotas API（使用 Infrastructure Manager 部署 Cloud Volumes ONTAP 時需要）

在限制模式下部署控制台代理

以受限模式部署控制台代理，以便您可以在有限的出站連線下使用NetApp Console。首先，安裝控制台代理，透過存取控制台代理上執行的使用者介面來設定控制台，然後提供您先前設定的雲端權限。

步驟 1：安裝控制台代理

從雲端提供者的市場安裝控制台代理程式或在 Linux 主機上手動安裝。

在安裝控制台代理之前，您需要先準備好環境。您可以從 AWS Marketplace、Azure Marketplace 安裝，也可以在您自己的執行於 AWS、Azure 或 Google Cloud 中的 Linux 主機上手動安裝。

AWS 商業市場

開始之前

需要以下物品：

- 滿足組網需求的VPC及子網路。

  "了解網路要求"

- 具有附加策略的 IAM 角色，其中包含控制台代理程式所需的權限。

  "了解如何設定 AWS 權限"

- 您的 IAM 使用者訂閱並取消訂閱 AWS Marketplace 的權限。
- 了解代理程式的 CPU 和 RAM 要求。

  "審查代理要求"。

- EC2 執行個體的金鑰對。

步驟

1. 前往 "AWS Marketplace 上的NetApp Console代理程式列表"
2. 在市場頁面上，選擇*繼續訂閱*。
3. 若要訂閱軟體，請選擇*接受條款*。

   訂閱過程可能需要幾分鐘。

4. 訂閱程序完成後，選擇*繼續配置*。
5. 在*配置此軟體*頁面上，確保您選擇了正確的區域，然後選擇*繼續啟動*。
6. 在*啟動此軟體*頁面的*選擇操作*下，選擇*透過 EC2 啟動*，然後選擇*啟動*。

   使用 EC2 控制台啟動執行個體並附加 IAM 角色。使用「從網站啟動」操作無法實現這一點。

7. 依照提示配置並部署實例：
   - 名稱和標籤：輸入實例的名稱和標籤。
   - 應用程式和作業系統映像：跳過此部分。控制台代理程式 AMI 已被選取。
   - 執行個體類型：根據區域可用性，選擇符合 RAM 和 CPU 要求的執行個體類型（預先選擇並建議 t3.2xlarge）。
   - 金鑰對（登入）：選擇您想要用來安全地連線到執行個體的金鑰對。
   - 網路設定：依需求編輯網路設定：
     - 選擇所需的 VPC 和子網路。
     - 指定執行個體是否應具有公用 IP 位址。
     - 指定安全性群組設置，為控制台代理實例啟用所需的連線方法：SSH、HTTP 和 HTTPS。

       "查看 AWS 的安全群組規則"。

- 配置儲存：保留根磁碟區的預設大小和磁碟類型。

  如果要在根磁碟區上啟用 Amazon EBS 加密，請選擇 進階，展開 磁碟區 **1**，選擇 加密，然後選擇 KMS 金鑰。

- 進階詳細資料：在 **IAM** 實例設定檔 下，選擇包含控制台代理程式所需權限的 IAM 角色。
- 摘要：查看摘要並選擇*啟動實例*。

結果

AWS 使用指定的設定啟動軟體。控制台代理大約需要五分鐘即可部署。

下一步是什麼？

設定NetApp Console。

AWS 政府市場

開始之前

需要以下物品：

- 滿足組網需求的VPC及子網路。

  "了解網路要求"

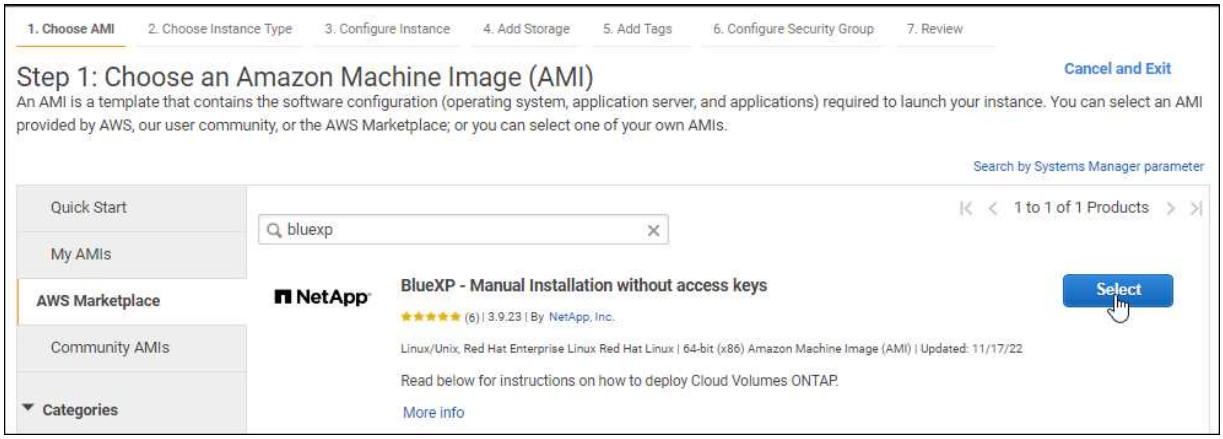
- 具有附加策略的 IAM 角色，其中包含控制台代理程式所需的權限。

  "了解如何設定 AWS 權限"

- 您的 IAM 使用者訂閱並取消訂閱 AWS Marketplace 的權限。
- EC2 執行個體的金鑰對。

步驟

1. 前往 AWS Marketplace 中提供的NetApp Console代理程式。
   a. 開啟 EC2 服務並選擇 啟動執行個體。
   b. 選擇 **AWS Marketplace**。
   c. 搜尋NetApp Console並選擇產品。



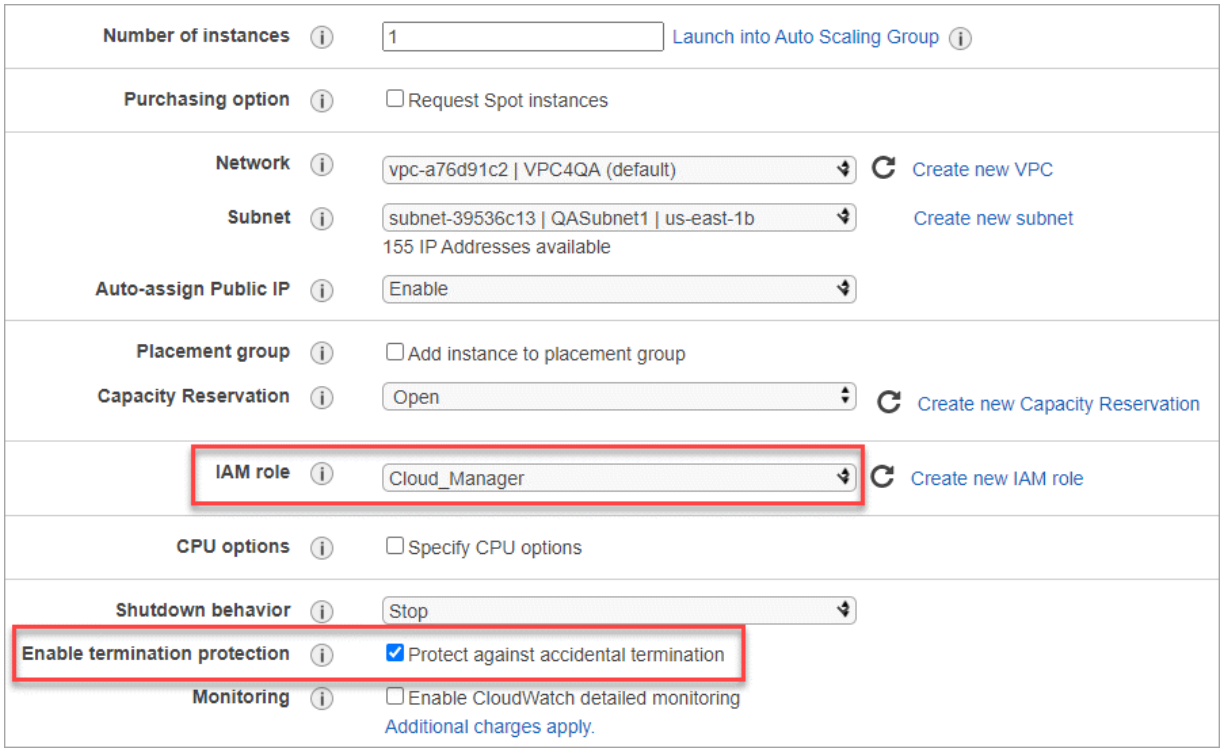
d. 選擇*繼續*。

2. 依照提示設定並啟動實例：

   - 選擇實例類型：根據區域可用性，選擇一種受支援的執行個體類型（建議使用 t3.2xlarge）。

     "查看實例要求"。

   - 設定實例詳細資料：選擇 VPC 和子網，選擇您在步驟 1 中建立的 IAM 角色，啟用終止保護（建議），並選擇任何其他符合您要求的設定選項。



   - 新增儲存：保留預設儲存選項。
   - 新增標籤：如果需要，輸入實例的標籤。
   - 設定安全群組：指定控制台代理實例所需的連線方法：SSH、HTTP 和 HTTPS。
   - 審查：審查您的選擇並選擇*啟動*。

結果

AWS 使用指定的設定啟動軟體。控制台代理大約需要五分鐘即可部署。

下一步是什麼？

設定控制台。

Azure 政府市場

開始之前

您應該具有以下內容：

- 滿足網路需求的 VNet 和子網路。

  "了解網路要求"

- 包含控制台代理程式所需權限的 Azure 自訂角色。

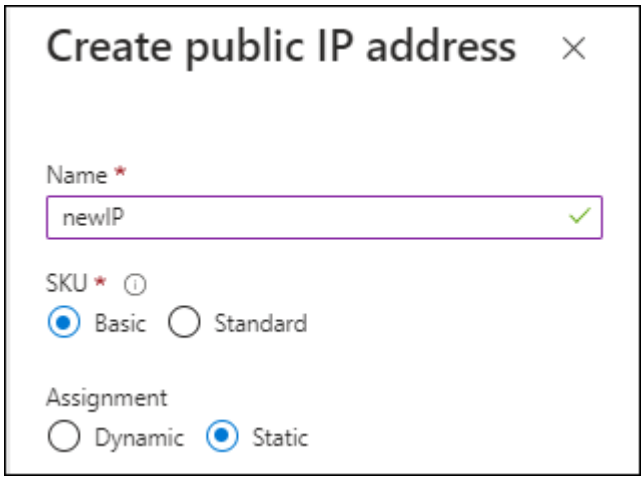
  "了解如何設定 Azure 權限"

步驟

1. 前往 Azure 市場中的NetApp Console代理 VM 頁面。
   - "商業區域的 Azure 市集頁面"
   - "Azure 政府區域的 Azure 市集頁面"
2. 選擇*立即取得*，然後選擇*繼續*。
3. 從 Azure 入口網站中，選擇「建立」並依照步驟設定虛擬機器。

   配置虛擬機器時請注意以下事項：

   - **VM** 大小：選擇符合 CPU 和 RAM 需求的 VM 大小。我們推薦 Standard_D8s_v3。
   - 磁碟：控制台代理可以透過 HDD 或 SSD 磁碟實現最佳效能。
   - 公網 **IP**：若要將公網 IP 位址與控制台代理 VM 一起使用，請選擇基本 SKU。



   如果您使用標準 SKU IP 位址，則控制台將使用控制台代理程式的_私有_ IP 位址，而不是公用 IP。如果用於存取控制台的電腦無法存取私人 IP 位址，則控制台將無法運作。

   "Azure 文件：公用 IP SKU"

   - 網路安全群組：控制台代理程式需要使用 SSH、HTTP 和 HTTPS 的入站連線。

     "查看 Azure 的安全性群組規則" 。

   - 身分：在*管理*下，選擇*啟用系統指派的託管身分*。

     託管識別允許控制台代理虛擬機器無需憑證即可向 Microsoft Entra ID 進行身份驗證。 "詳細了解 Azure 資源的託管標識" 。
4. 在「審查 + 建立」頁面上，檢視您的選擇並選擇「建立」以開始部署。

結果

Azure 使用指定的設定部署虛擬機器。虛擬機器和控制台代理軟體應在大約五分鐘內運作。

下一步是什麼？

設定NetApp Console。

手動安裝（必須用於 **Google Cloud**）

您可以將控制台代理程式手動安裝到執行在 AWS、Azure 或 Google Cloud 上的 Linux 主機上。

開始之前

您應該具有以下內容：

- 安裝控制台代理程式的 root 權限。
- 如果控制台代理需要代理才能存取互聯網，則提供有關代理伺服器的詳細資訊。

  您可以選擇在安裝後設定代理伺服器，但這樣做需要重新啟動控制台代理。

- 如果代理伺服器使用 HTTPS 或代理是攔截代理，則需要 CA 簽署的憑證。

> ⓘ 手動安裝控制台代理程式時，無法為透明代理伺服器設定憑證。如果需要為透明代理伺服器設定證書，則必須在安裝後使用維護控制台。詳細了解"代理維護控制台"。

- 您需要停用安裝期間驗證出站連線的設定檢查。如果未停用此檢查，手動安裝將失敗。"了解如何停用手動安裝的設定檢查。"
- 根據您的作業系統，在安裝控制台代理之前需要 Podman 或 Docker Engine。

關於此任務

安裝後，如果有新版本可用，控制台代理會自動更新。

步驟

1. 如果主機上設定了 *http_proxy* 或 *https_proxy* 系統變量，請將其刪除：

```
unset http_proxy
unset https_proxy
```

   如果不刪除這些系統變量，安裝將會失敗。

2. 下載控制台代理軟體，然後將其複製到 Linux 主機。您可以從NetApp Console或NetApp支援網站下載。
   - NetApp Console：前往*代理程式 > 管理 > 部署代理程式 > 本機部署 > 手動安裝*。

     選擇下載代理安裝程式檔案或檔案的 URL。

   - NetApp支援網站（如果您還沒有存取控制台的權限，則需要此網站） "NetApp支援站點" ，
3. 分配運行腳本的權限。

```
chmod +x NetApp_Console_Agent_Cloud_<version>
```

其中 <version> 是您下載的控制台代理的版本。

4. 如果在政府雲端環境中安裝，請停用設定檢查。"了解如何停用手動安裝的設定檢查。"
5. 運行安裝腳本。

```
./NetApp_Console_Agent_Cloud_<version> --proxy <HTTP or HTTPS proxy
server> --cacert <path and file name of a CA-signed certificate>
```

如果您的網路需要代理才能存取互聯網，則需要新增代理資訊。您可以在安裝過程中明確新增代理程式。 `--proxy`和 `--cacert`參數是可選的，系統不會提示您新增。如果您有明確的代理伺服器，則需要以所示方式輸入參數。

如果要設定透明代理，可以在安裝完成後進行設定。 "了解代理維護控制台"

+

以下是使用 CA 簽章憑證設定明確代理伺服器的範例：

+

```
./NetApp_Console_Agent_Cloud_v4.0.0--proxy
https://user:password@10.0.0.30:8080/ --cacert
/tmp/cacert/certificate.cer
```

+
`--proxy` 設定 Console 代理程式以使用下列格式之一的 HTTP 或 HTTPS 代理伺服器：

+ * http://address:port * http://user-name:password@address:port * http://domain-name%92user-name:password@address:port * https://address:port * https://user-name:password@address:port * https://domain-name%92user-name:password@address:port

+ 請注意以下事項：

+ 使用者可以是本機使用者或網域使用者。 對於網域使用者，您必須使用如上所示的 \ ASCII 碼。 **Console** 代理程式不支援包含 **@** 字元的使用者名稱或密碼。 如果密碼包含以下任何特殊字元，您必須在其前面加上反斜線以進行轉義：& 或 !

+ 例如：

+ http://bxpproxyuser:netapp1\!@address:3128

1. 如果您使用 Podman，則需要調整 aardvark-dns 連接埠。
   a. 透過 SSH 連接到控制台代理虛擬機器。

b. 開啟 podman */usr/share/containers/containers.conf* 檔案並修改 Aardvark DNS 服務的選定連接埠。例如，將其更改為54。

```
vi /usr/share/containers/containers.conf
```

例如：

```
# Port to use for dns forwarding daemon with netavark in rootful
bridge
# mode and dns enabled.
# Using an alternate port might be useful if other DNS services
should
# run on the machine.
#
dns_bind_port = 54
```

a. 重新啟動控制台代理虛擬機器。

結果

控制台代理現已安裝。安裝結束時，如果您指定了代理伺服器，控制台代理服務 (occm) 將重新啟動兩次。

下一步是什麼？

設定NetApp Console。

第 2 步：設定NetApp Console

首次存取控制台時，系統會提示您為控制台代理程式選擇一個組織，並需要啟用受限模式。

開始之前

設定控制台代理的人員必須使用尚不屬於控制台組織的登入名稱登入控制台。

如果您的登入資訊與另一個組織關聯，您需要註冊一個新的登入資訊。否則，您將在設定畫面上看不到啟用受限模式的選項。

步驟

1. 從與控制台代理程式執行個體有連線的主機開啟 Web 瀏覽器，然後輸入您安裝的控制台代理程式的下列 URL。
2. 註冊或登入NetApp Console。
3. 登入後，設定控制台：
   a. 輸入控制台代理的名稱。
   b. 輸入新控制台組織的名稱。
   c. 選擇*您是否在安全環境中運作？ *

d. 選擇*在此帳戶上啟用受限模式*。

請注意，帳戶建立後您無法變更此設定。您以後無法啟用受限模式，也無法停用它。

如果您在政府區域部署了控制台代理，則該核取方塊已啟用且無法變更。這是因為限制模式是政府區域唯一支持的模式。

a. 選擇*讓我們開始吧*。

結果

控制台代理現在已安裝並設定到您的控制台組織。所有使用者都需要使用控制台代理執行個體的 IP 位址存取控制台。

下一步是什麼？

向控制台提供您先前設定的權限。

步驟 3：向控制台代理提供權限

如果您是從 Azure Marketplace 或手動安裝的控制台代理，則需要授予您先前設定的權限。

如果您從 AWS Marketplace 部署了控制台代理，則這些步驟不適用，因為您在部署期間選擇了所需的 IAM 角色。

"了解如何準備雲端權限" 。

AWS IAM 角色

將您先前建立的 IAM 角色附加到安裝了控制台代理程式的 EC2 執行個體。

只有當您在 AWS 中手動安裝了控制台代理程式時，這些步驟才適用。對於 AWS Marketplace 部署，您已將控制台代理執行個體與包含所需權限的 IAM 角色關聯。

步驟

1. 前往 Amazon EC2 主控台。
2. 選擇*實例*。
3. 選擇控制台代理實例。
4. 選擇*操作>安全性>修改 IAM 角色*。
5. 選擇 IAM 角色並選擇 更新 **IAM** 角色。

AWS 存取金鑰

向NetApp Console提供具有所需權限的 IAM 使用者的 AWS 存取金鑰。

步驟

1. 選擇“管理 **>** 憑證”。
2. 選擇*組織憑證*。
3. 選擇“新增憑證”並按照精靈中的步驟操作。
   a. 憑證位置：選擇*Amazon Web Services > 代理程式。
   b. 定義憑證：輸入 AWS 存取金鑰和金鑰。
   c. 市場訂閱：透過立即訂閱或選擇現有訂閱將市場訂閱與這些憑證關聯。
   d. 審核：確認有關新憑證的詳細資訊並選擇*新增*。

Azure 角色

前往 Azure 入口網站並將 Azure 自訂角色指派給一個或多個訂閱的控制台代理虛擬機器。

步驟

1. 從 Azure 入口網站開啟「訂閱」服務並選擇您的訂閱。

   從*訂閱*服務分配角色很重要，因為這指定了訂閱等級的角色分配範圍。 _範圍_定義了存取適用的資源集。如果您在不同層級（例如，虛擬機器層級）指定範圍，則您在NetApp Console內完成操作的能力將受到影響。

   "Microsoft Azure 文件：了解 Azure RBAC 的範圍"

2. 選擇*存取控制 (IAM)* > 新增 > 新增角色分配。
3. 在*角色*標籤中，選擇*控制台操作員*角色並選擇*下一步*。

   控制台操作員是策略中提供的預設名稱。如果您為角色選擇了不同的名稱，請選擇該名稱。

4. 在「成員」標籤中，完成以下步驟：
    a. 指派對*託管身分*的存取權限。
    b. 選擇“選擇成員”，選擇建立控制台代理虛擬機器的訂閱，在“託管識別”下，選擇“虛擬機器”，然後選擇控制台代理虛擬機器。
    c. 選擇*選擇*。
    d. 選擇“下一步”。
    e. 選擇*審閱+分配*。
    f. 如果要管理其他 Azure 訂閱中的資源，請切換到該訂閱，然後重複這些步驟。

Azure 服務主體

向NetApp Console提供您先前設定的 Azure 服務主體的憑證。

步驟

1. 選擇“管理 **>** 憑證”。
2. 選擇“新增憑證”並按照精靈中的步驟操作。
    a. 憑證位置：選擇*Microsoft Azure > 代理程式*。
    b. 定義憑證：輸入有關授予所需權限的 Microsoft Entra 服務主體的資訊：
        - 應用程式（客戶端）ID
        - 目錄（租戶）ID
        - 客戶端密鑰
    c. 市場訂閱：透過立即訂閱或選擇現有訂閱將市場訂閱與這些憑證關聯。
    d. 審核：確認有關新憑證的詳細資訊並選擇*新增*。

結果

NetApp Console現在具有代表您在 Azure 中執行操作所需的權限。

Google Cloud 服務帳號

將服務帳戶與控制台代理 VM 關聯。

步驟

1. 前往 Google Cloud 入口網站並將服務帳戶指派給控制台代理程式 VM 執行個體。

    "Google Cloud 文件：變更執行個體的服務帳戶和存取範圍"

2. 如果您想管理其他專案中的資源，請透過將具有控制台代理角色的服務帳戶新增至該專案來授予存取權限。您需要對每個項目重複此步驟。

訂閱NetApp Intelligent Services（受限模式）

從雲端供應商的市場訂閱NetApp Intelligent Services，以按小時費率（PAYGO）或透過年度合約支付資料服務費用。如果您從NetApp （BYOL）購買了許可證，您還需要訂閱市場

產品。您的許可證始終會先被收費，但如果您超出許可容量或許可證期限到期，則會按小時費率向您收費。

市場訂閱支援以受限模式對以下數據服務收費：

- NetApp Backup and Recovery
- Cloud Volumes ONTAP
- NetApp Cloud Tiering
- NetApp Ransomware Resilience
- NetApp Disaster Recovery

NetApp Data Classification可透過您的訂閱啟用，但使用分類是免費的。

開始之前

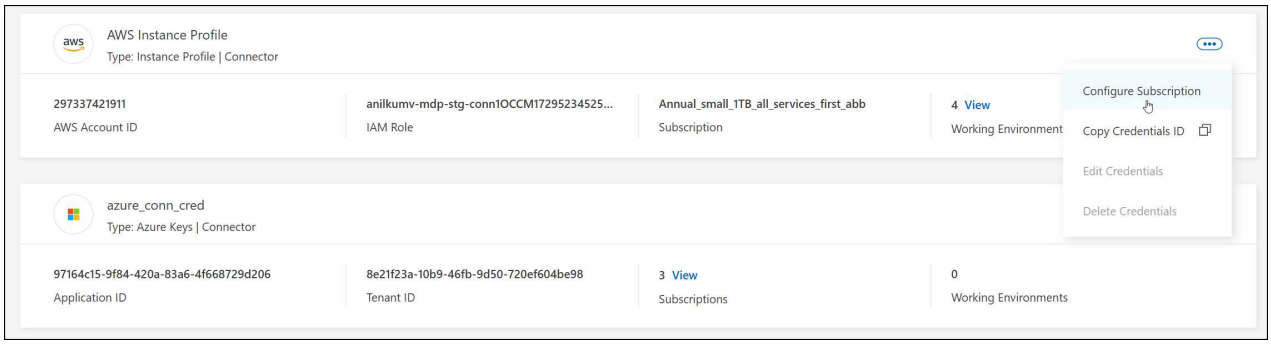
您必須已經部署控制台代理程式才能訂閱資料服務。您需要將市場訂閱與連接到控制台代理的雲端憑證關聯起來。

AWS

步驟

1. 選擇“管理 > 憑證”。
2. 選擇*組織憑證*。
3. 選擇與控制台代理程式關聯的一組憑證的操作選單，然後選擇*配置訂閱*。

   您必須選擇與控制台代理程式關聯的憑證。您無法將市場訂閱與與NetApp Console關聯的憑證關聯。



4. 若要將憑證與現有訂閱關聯，請從下拉清單中選擇訂閱並選擇*配置*。
5. 若要將憑證與新訂閱關聯，請選擇「新增訂閱」>「繼續」*，然後依照 AWS Marketplace 中的步驟：

   a. 選擇“查看購買選項”。

   b. 選擇*訂閱*。

   c. 選擇*設定您的帳戶*。

      您將被重新導向到NetApp Console。

   d. 從「訂閱分配」頁面：

      - 選擇您想要與此訂閱關聯的控制台組織或帳戶。
      - 在「取代現有訂閱」欄位中，選擇是否要用這個新訂閱自動取代一個組織或帳戶的現有訂閱。

        控制台將用這個新訂閱替換組織或帳戶中所有憑證的現有訂閱。如果一組憑證從未與訂閱關聯，那麼這個新訂閱將不會與這些憑證關聯。

   對於所有其他組織或帳戶，您需要重複這些步驟來手動關聯訂閱。

   ◦ 選擇*儲存*。

Azure

步驟

1. 選擇“管理 > 憑證”。
2. 選擇*組織憑證*。
3. 選擇與控制台代理程式關聯的一組憑證的操作選單，然後選擇*配置訂閱*。

   您必須選擇與控制台代理程式關聯的憑證。您無法將市場訂閱與與NetApp Console關聯的憑證關聯。

4. 若要將憑證與現有訂閱關聯，請從下拉清單中選擇訂閱並選擇*配置*。
5. 若要將憑證與新訂閱關聯，請選擇「新增訂閱」>「繼續」*，然後按照 Azure 市場中的步驟操作：

    a. 如果出現提示，請登入您的 Azure 帳戶。

    b. 選擇*訂閱*。

    c. 填寫表格並選擇*訂閱*。

    d. 訂閱程序完成後，選擇*立即配置帳戶*。

    您將被重新導向到NetApp Console。

    e. 從「訂閱分配」頁面：

    - 選擇您想要與此訂閱關聯的控制台組織或帳戶。
    - 在「取代現有訂閱」欄位中，選擇是否要用這個新訂閱自動取代一個組織或帳戶的現有訂閱。

    控制台將用這個新訂閱替換組織或帳戶中所有憑證的現有訂閱。如果一組憑證從未與訂閱關聯，那麼這個新訂閱將不會與這些憑證關聯。

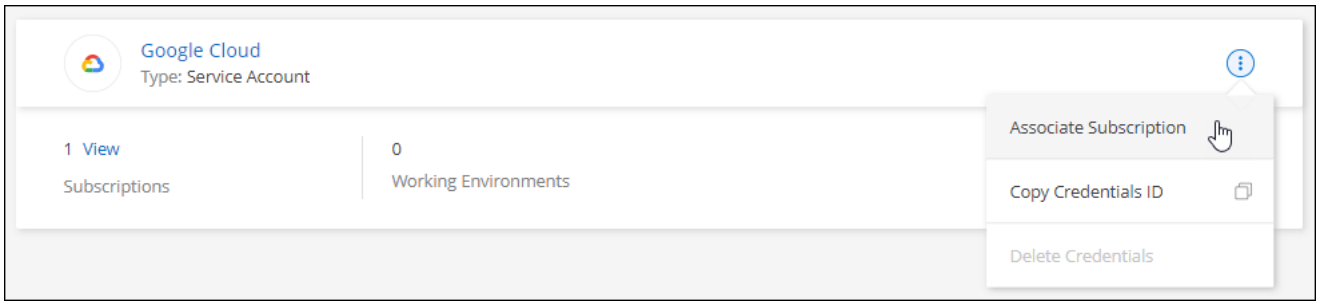
對於所有其他組織或帳戶，您需要重複這些步驟來手動關聯訂閱。

    。選擇*儲存*。

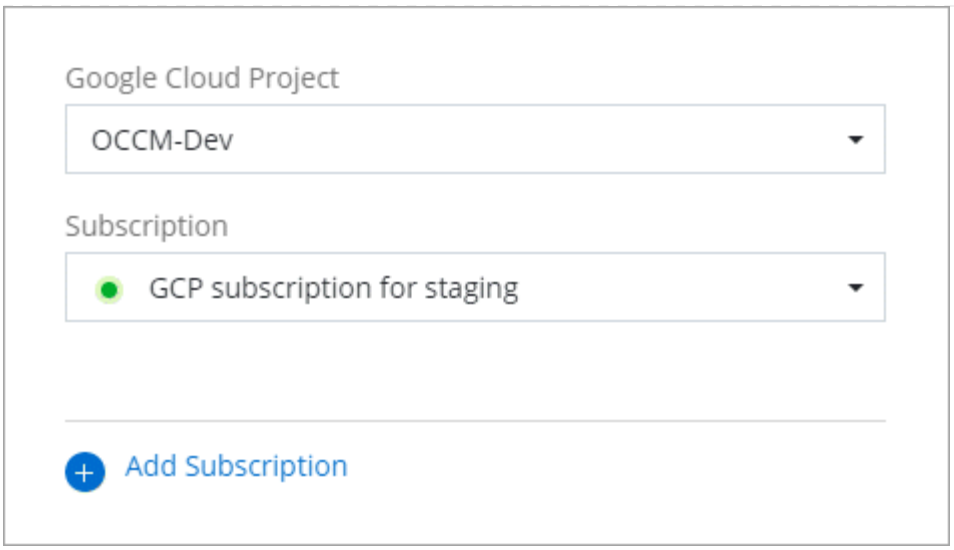
Google雲

步驟

1. 選擇“管理 > 憑證”。
2. 選擇*組織憑證*。
3. 選擇與控制台代理程式關聯的一組憑證的操作選單，然後選擇*配置訂閱*。



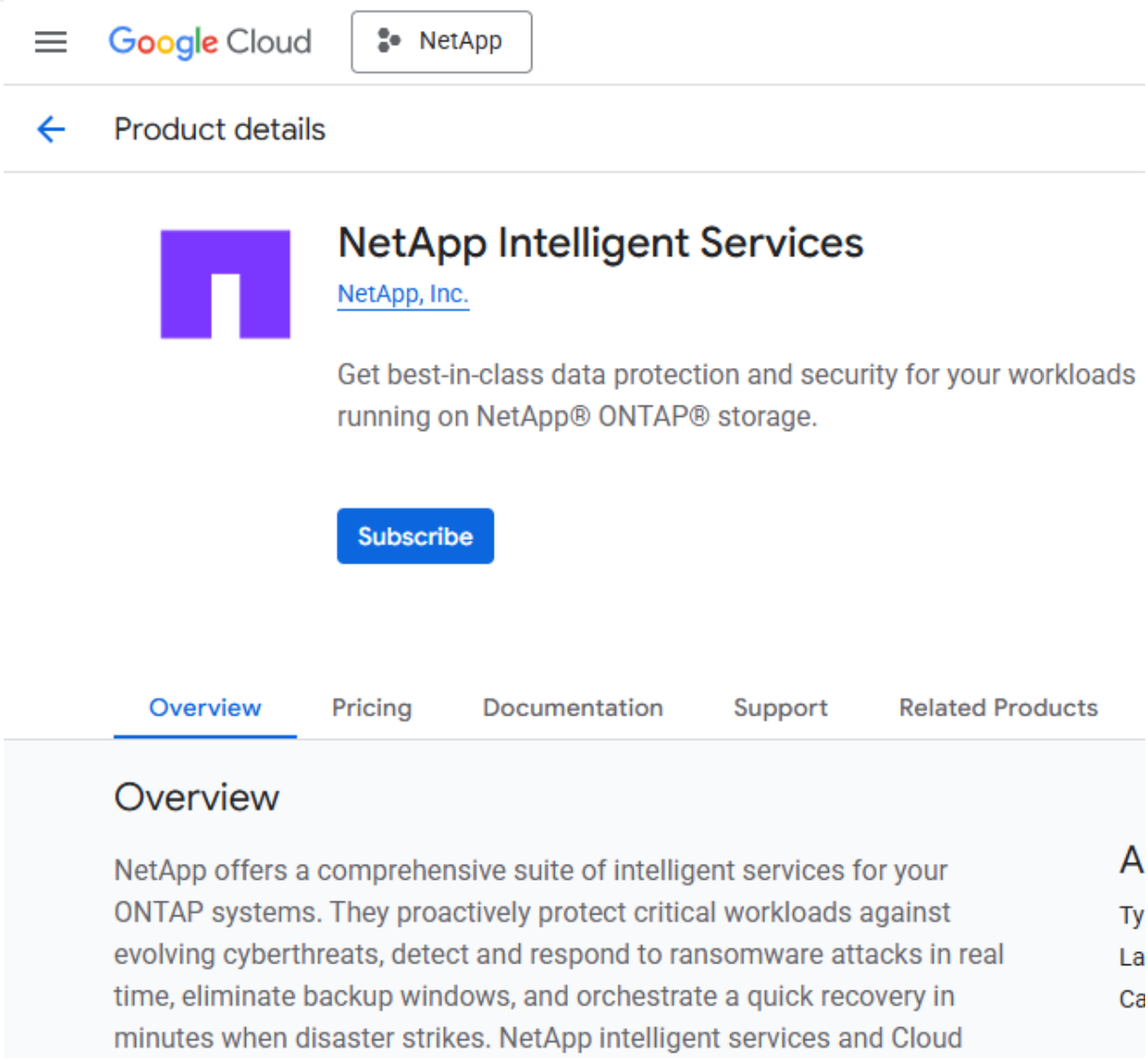
1. 若要使用選定的憑證設定現有訂閱，請從下拉清單中選擇一個 Google Cloud 專案和訂閱，然後選擇*設定*。



2. 如果您還沒有訂閱，請選擇*新增訂閱>繼續*並按照 Google Cloud Marketplace 中的步驟操作。

   在完成以下步驟之前，請確保您在 Google Cloud 帳戶中同時擁有 Billing Admin 權限以及NetApp Console登入權限。

   a. 在您被重定向到 "Google Cloud Marketplace 上的NetApp Intelligent Services頁面"，確保在頂部導航選單中選擇了正確的項目。



b. 選擇*訂閱*。

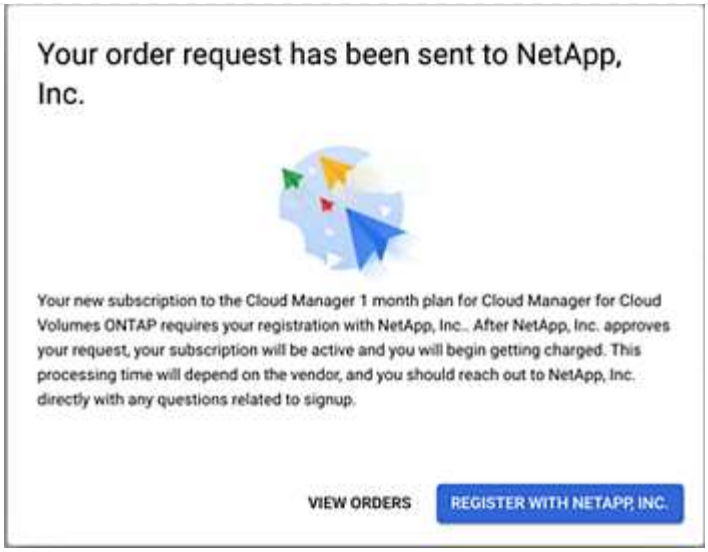
c. 選擇適當的結算帳戶並同意條款和條件。

d. 選擇*訂閱*。

   此步驟將您的轉移請求傳送給NetApp。

e. 在彈出的對話方塊中，選擇*向NetApp, Inc. 註冊*。

   必須完成此步驟才能將 Google Cloud 訂閱與您的控制台組織或帳戶關聯。直到您從此頁面重定向並登入控制台後，連結訂閱的過程才完成。



f. 完成「訂閱分配」頁面上的步驟：

> 如果您組織中的某人已經從您的結算帳戶訂閱了市場，那麼您將被重新導向到"NetApp Console中的Cloud Volumes ONTAP頁面"反而。如果這是意外情況，請聯絡您的NetApp銷售團隊。 Google 為每個 Google 結算帳戶僅啟用一項訂閱。

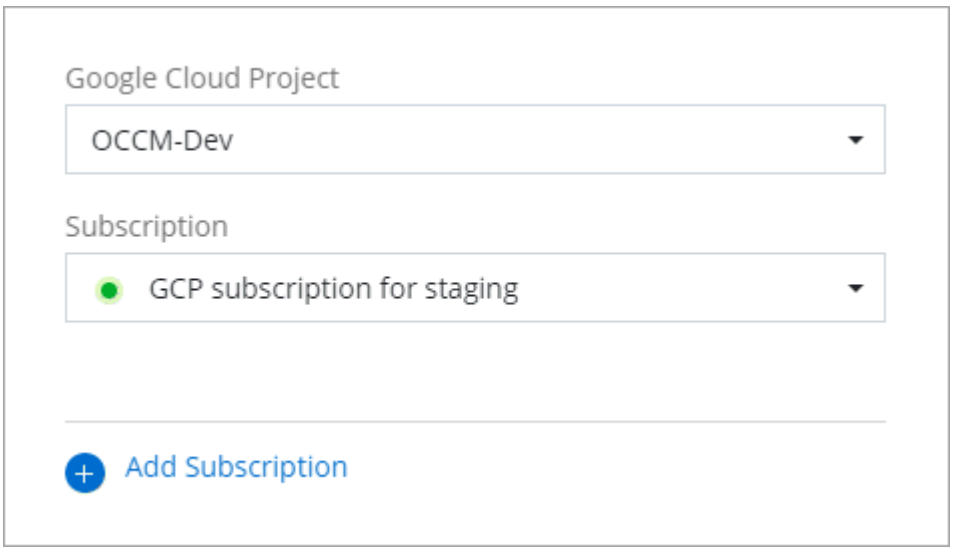
- 選擇您想要與此訂閱關聯的控制台組織。
- 在「取代現有訂閱」欄位中，選擇是否要用這個新訂閱自動取代組織的現有訂閱。

  控制台將用這個新訂閱替換組織中所有憑證的現有訂閱。如果一組憑證從未與訂閱關聯，那麼這個新訂閱將不會與這些憑證關聯。

對於所有其他組織或帳戶，您需要重複這些步驟來手動關聯訂閱。

◦ 選擇*儲存*。

3. 此過程完成後，導覽回控制台中的「憑證」頁面並選擇此新訂閱。



相關資訊

- "管理Cloud Volumes ONTAP 的BYOL 基於容量的許可證"
- "管理資料服務的 BYOL 許可證"
- "管理 AWS 憑證和訂閱"
- "管理 Azure 憑證和訂閱"
- "管理 Google Cloud 憑證和訂閱"

接下來可以做什麼（受限模式）

在限制模式下啟動並執行NetApp Console後，您可以開始使用限制模式支援的服務。

如需協助，請參閱以下服務的文件：

- "Azure NetApp Files文檔"
- "備份和恢復文檔"
- "分類文檔"
- "Cloud Volumes ONTAP文檔"
- "數位錢包文檔"
- "本地ONTAP集群文檔"
- "複製文檔"

相關資訊

"NetApp Console部署模式"

版權資訊

Copyright © 2026 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

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。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。 美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 http://www.netapp.com/TM 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。