# 管理和監測

## NetApp Console setup and administration

NetApp
February 11, 2026

# 目錄

# 管理和監測

## NetApp支援帳戶

### 管理與NetApp Console關聯的 NSS 憑證

將NetApp支援網站帳號與您的控制台組織關聯，以啟用儲存管理的關鍵工作流程。這些 NSS 憑證與整個組織相關。

控制台也支援每個使用者帳戶關聯一個 NSS 帳戶。"了解如何管理使用者級憑證" 。

概況

需要將NetApp支援網站憑證與您的特定控制台帳戶序號關聯才能啟用下列任務：

- 自帶授權 (BYOL) 時部署Cloud Volumes ONTAP

  需要提供您的 NSS 帳戶，以便控制台可以上傳您的許可證金鑰並啟用您購買的期限的訂閱。這包括期限續訂的自動更新。

- 註冊即用即付Cloud Volumes ONTAP系統

  需要提供您的 NSS 帳戶才能啟動對您的系統的支援並獲得NetApp技術支援資源的存取權限。

- 將Cloud Volumes ONTAP軟體升級至最新版本

這些憑證與您的特定控制台帳戶序號相關聯。使用者可以從*支援 > NSS 管理*存取這些憑證。

新增 **NSS** 帳戶

您可以從控制台中的支援資訊板新增和管理用於控制台的NetApp支援網站帳戶。

當您新增了 NSS 帳戶後，控制台會使用此資訊進行許可證下載、軟體升級驗證和未來支援註冊等。

您可以將多個 NSS 帳戶與您的組織關聯；但是，您無法在同一個組織內擁有客戶帳戶和合作夥伴帳戶。

NetApp使用 Microsoft Entra ID 作為特定於支援和授權的身份驗證服務的身份提供者。

步驟

1. 在*管理 > 支援*中。
2. 選擇*NSS 管理*。
3. 選擇*新增 NSS 帳戶*。
4. 選擇“繼續”以重定向到 Microsoft 登入頁面。
5. 在登入頁面，提供您的NetApp支援網站註冊的電子郵件地址和密碼。

   成功登入後， NetApp將儲存 NSS 使用者名稱。

這是系統產生的映射到您的電子郵件的 ID。在*NSS 管理*頁面上，您可以顯示來自 ••• 菜單。

- 如果您需要刷新登入憑證令牌，還有一個*更新憑證*選項 ••• 菜單。

  使用此選項會提示您再次登入。請注意，這些帳戶的令牌將在 90 天後過期。我們將發布通知來提醒您此事。

下一步是什麼？

使用者現在可以在建立新的Cloud Volumes ONTAP系統和註冊現有Cloud Volumes ONTAP系統時選擇帳戶。

- "在 AWS 中啟動Cloud Volumes ONTAP"
- "在 Azure 中啟動Cloud Volumes ONTAP"
- "在 Google Cloud 啟動Cloud Volumes ONTAP"
- "註冊現收現付系統"

更新 **NSS** 憑證

出於安全原因，您必須每 90 天更新一次您的 NSS 憑證。如果您的 NSS 憑證已過期，您將在控制台通知中心收到通知。"了解通知中心" 。

過期的憑證可能會影響以下情況，但不限於：

- 許可證更新，這意味著您將無法利用新購買的容量。
- 能夠提交和追蹤支援案例。

此外，如果您想變更與您的組織關聯的 NSS 帳戶，您可以更新與您的組織關聯的 NSS 憑證。例如，如果與您的 NSS 帳戶關聯的人員已離開您的公司。

步驟

1. 在*管理 > 支援*中。
2. 選擇*NSS 管理*。
3. 對於要更新的 NSS 帳戶，選擇 ••• 然後選擇*更新憑證*。
4. 當出現提示時，選擇「繼續」以重新導向至 Microsoft 登入頁面。

   NetApp使用 Microsoft Entra ID 作為與支援和授權相關的身份驗證服務的身份提供者。

5. 在登入頁面，提供您的NetApp支援網站註冊的電子郵件地址和密碼。

將系統附加到不同的 **NSS** 帳戶

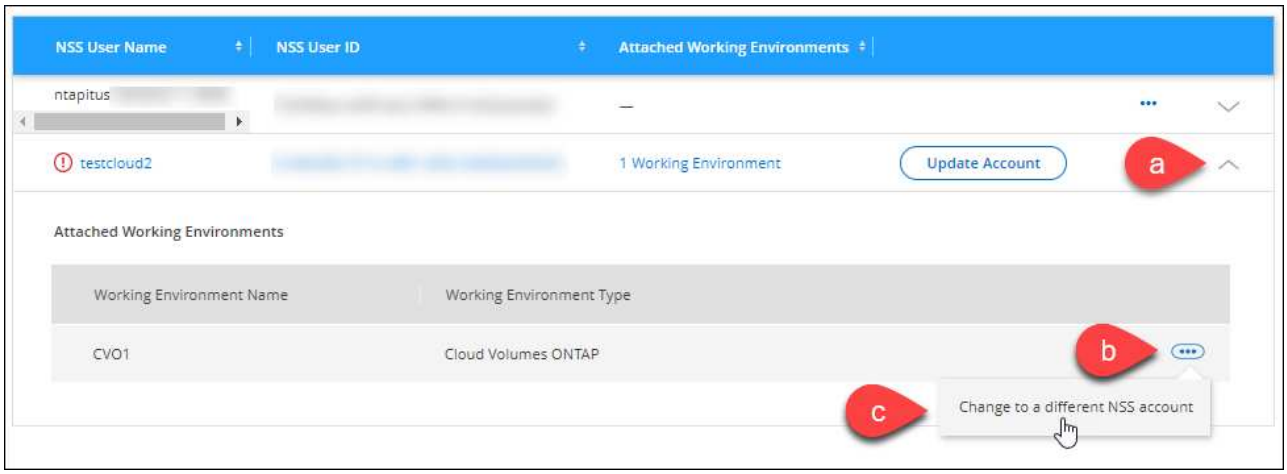
如果您的組織有多個NetApp支援網站帳戶，您可以變更與Cloud Volumes ONTAP系統關聯的帳戶。

您必須先將帳戶與控制台關聯。

步驟

1. 在*管理 > 支援*中。
2. 選擇*NSS 管理*。

3. 完成以下步驟來變更 NSS 帳戶：
   a. 展開系統目前關聯的NetApp支援網站帳戶的行。
   b. 對於要變更關聯的系統，選擇 •••
   c. 選擇*變更為不同的 NSS 帳戶*。




   d. 選擇帳戶，然後選擇*儲存*。

顯示 **NSS** 帳號的電子郵件地址

為了安全起見，預設不會顯示與 NSS 帳戶關聯的電子郵件地址。您可以查看 NSS 帳戶的電子郵件地址和關聯的使用者名稱。

當您前往 NSS 管理頁面時，控制台會為表中的每個帳戶產生一個令牌。此令牌包含有關關聯電子郵件地址的資訊。當您離開頁面時，令牌將被刪除。資訊永遠不會被緩存，這有助於保護您的隱私。

步驟

1. 在*管理 > 支援*中。
2. 選擇*NSS 管理*。
3. 對於要更新的 NSS 帳戶，選擇 ••• 然後選擇*顯示電子郵件地址*。您可以使用複製按鈕複製電子郵件地址。

刪除 **NSS** 帳戶

刪除不再想在控制台中使用的所有 NSS 帳戶。

您無法刪除目前與Cloud Volumes ONTAP系統關聯的帳戶。你首先需要將這些系統附加到不同的 NSS 帳戶。

步驟

1. 在*管理 > 支援*中。
2. 選擇*NSS 管理*。
3. 對於要刪除的 NSS 帳戶，選擇 ••• 然後選擇*刪除*。
4. 選擇*刪除*進行確認。

# 管理與您的NetApp Console登入關聯的憑證

根據您在控制台中執行的操作，您可能已將ONTAP憑證和NetApp支援網站 (NSS) 憑證與您的使用者登入關聯。關聯這些憑證後，您可以檢視和管理它們。例如，如果您變更這些憑證的密碼，則需要在控制台中更新密碼。

## ONTAP憑證

使用者需要ONTAP管理員憑證才能在控制台中發現ONTAP叢集。但是， ONTAP系統管理員存取取決於您是否使用控制台代理。

### 無需控制台代理

系統會提示使用者輸入其ONTAP憑證以存取叢集的ONTAP系統管理員。使用者可以選擇將這些憑證保存在控制台中，這意味著他們不必每次都輸入這些憑證。使用者憑證僅對對應使用者可見，並且可以從使用者憑證頁面進行管理。

### 使用控制台代理

預設情況下，不會提示使用者輸入其ONTAP憑證來存取ONTAP系統管理員。但是，控制台管理員（具有組織管理員角色）可以設定控制台以提示使用者輸入其ONTAP憑證。啟用此設定後，使用者每次都需要輸入其ONTAP憑證。

"了解更多。"

## NSS 憑證

與您的NetApp Console登入關聯的 NSS 憑證可支援註冊、案例管理和存取Digital Advisor。

- 當您造訪*支援>資源*並註冊支援時，系統會提示您將 NSS 憑證與您的登入名稱關聯。

  這將註冊您的組織或帳戶以獲得支持並啟動支持權利。您的組織中只有一個使用者必須將NetApp支援網站帳戶與其登入名稱關聯，以註冊支援並啟動支援權利。完成後，「資源」頁面將顯示您的帳戶已註冊支援。

  "了解如何註冊以獲得支持"

- 當您存取*管理 > 支援 > 案例管理*時，如果您還沒有輸入 NSS 憑證，系統會提示您輸入。此頁面使您能夠建立和管理與您的 NSS 帳戶和公司相關的支援案例。
- 當您在控制台中造訪Digital Advisor時，系統會提示您輸入 NSS 憑證登入Digital Advisor 。

請注意與您的登入關聯的 NSS 帳戶的以下事項：

- 該帳戶在使用者層級進行管理，這意味著其他登入的使用者無法查看該帳戶。
- 每個使用者只能有一個與Digital Advisor和支援案例管理關聯的 NSS 帳戶。
- 如果您嘗試將NetApp支援網站帳號與Cloud Volumes ONTAP系統關聯，則只能從新增至您所屬組織的 NSS 帳戶中進行選擇。

  NSS 帳戶級憑證與與您的登入關聯的 NSS 帳戶不同。 NSS 帳戶級憑證可讓您使用 BYOL 部署Cloud Volumes ONTAP 、註冊 PAYGO 系統並升級其軟體。

  "了解有關將 NSS 憑證與您的NetApp Console組織或帳戶結合使用的更多信息" 。

管理您的使用者憑證

透過更新使用者名稱和密碼或刪除憑證來管理您的使用者憑證。

步驟

1. 選擇“管理 > 憑證”。
2. 選擇*使用者憑證*。
3. 如果您還沒有任何使用者憑證，您可以選擇*新增 NSS 憑證*來新增您的NetApp支援網站帳戶。
4. 透過從「操作」功能表中選擇以下選項來管理現有憑證：
   - 更新憑證：更新帳戶的使用者名稱和密碼。
   - 刪除憑證：刪除與您的控制台登入關聯的 NSS 帳戶。

# 控制台代理

## 了解**NetApp Console**代理

### 您可以使用控制台代理將NetApp Console連接到您的基礎架構，並安全地協調跨 AWS、Azure、Google Cloud 或本地環境的儲存解決方案，以及使用資料保護服務。

控制台代理程式可讓您：

- 透過NetApp Console協調儲存管理任務，例如設定Cloud Volumes ONTAP、設定儲存磁碟區、使用資料分類等等。
- 使用雲端提供者的 IAM 角色進行身份驗證，以實現訂閱計費整合。
- 使用進階資料服務（NetApp Backup and Recovery、 NetApp Disaster Recovery、 NetApp Ransomware Resilience和NetApp Cloud Tiering）
- 以受限模式使用控制台。

如果您不需要進階編排或資料保護，則可以集中管理本機ONTAP叢集和雲端原生儲存服務，而無需部署代理程式。此外，也提供監控和資料傳輸工具。

下表顯示了您可以使用和不使用控制台代理時可以使用的功能和服務。

| | 可聯絡經紀人獲取資訊 | 無需代理即可購買 |
|---|---|---|
| 支援的儲存系統： | | |
| 適用於ONTAP 的Amazon FSx | 是的（發現和管理功能） | 是的（僅限探索） |
| Amazon S3 存儲 | 是的 | 不 |
| Azure Blob 儲存 | 是的 | 是的 |
| Azure NetApp Files | 是的 | 是的 |

| | 可聯絡經紀人獲取資訊 | 無需代理即可購買 |
|---|---|---|
| Cloud Volumes ONTAP | 是的 | 不 |
| E系列系統 | 是的 | 不 |
| Google Cloud NetApp Volumes | 是的 | 是的 |
| Google Cloud 儲存桶 | 是的 | 不 |
| StorageGRID系統 | 是的 | 不 |
| 本地部署ONTAP叢集（高階管理和發現） | 是的（高階管理和發現） | 否（僅限基本發現） |
| 可用的儲存管理服務： | | |
| 警報 | 是的 | 不 |
| 自動化中心 | 是的 | 是的 |
| Digital Advisor（Active IQ） | 是的 | 不 |
| 授權和訂閱管理 | 是的 | 不 |
| 經濟效益 | 是的 | 不 |
| 首頁儀錶板指標 | 是的[2] | 不 |
| 生命週期規劃 | 是的 | 1號 |
| 永續性 | 是的 | 不 |
| 軟體更新 | 是的 | 是的 |
| NetApp工作負載 | 是的 | 是的 |
| 可用資料服務： | | |
| NetApp Backup and Recovery | 是的 | 不 |
| 資料分類 | 是的 | 不 |
| NetApp Cloud Tiering | 是的 | 不 |

| | 可聯絡經紀人獲取資訊 | 無需代理即可購買 |
|---|---|---|
| NetApp Copy and Sync | 是的 | 不 |
| NetApp Disaster Recovery | 是的 | 不 |
| NetApp Ransomware Resilience | 是的 | 不 |
| NetApp Volume Caching | 是的 | 不 |

[1] 無需控制台代理即可查看生命週期規劃，但需要控制台代理才能啟動操作。

[2] 主頁上的準確指標需要大小合適且配置正確的控制台代理。

控制台代理程式必須始終處於執行狀態

控制台代理程式是NetApp Console的基本組成部分。您（客戶）有責任確保相關代理商隨時處於正常運作和可存取狀態。控制台可以處理短暫的代理程式中斷，但您必須快速修復基礎架構故障。

本文檔受 EULA 管轄。按照文件以外的方式操作產品可能會影響其功能和您的 EULA 權利。

支援的位置

您可以在以下位置安裝代理：

- 亞馬遜網路服務
- 微軟 Azure

  在 Azure 中與其管理的Cloud Volumes ONTAP系統位於相同區域的控制台代理。或者，將其部署在 "Azure 區域對"。這可確保Cloud Volumes ONTAP及其關聯的儲存帳戶之間使用 Azure Private Link 連線。 "了解Cloud Volumes ONTAP如何使用 Azure Private Link"

- Google雲

  若要將控制台和資料服務與 Google Cloud 一起使用，請在 Google Cloud 中部署您的代理程式。

- 在您的場所

與雲端提供者的溝通

該代理程式使用 TLS 1.3 與 AWS、Azure 和 Google Cloud 進行所有通訊。

限制模式

若要在受限模式下使用控制台，請安裝控制台代理程式並存取在控制台代理程式上本機執行的控制台介面。

"了解NetApp Console部署模式" 。

如何安裝控制台代理

您可以直接從控制台、雲端提供者的市場安裝控制台代理，也可以在您自己的 Linux 主機或 VCenter 環境中手動安裝軟體。

- "了解NetApp Console部署模式"
- "開始在標準模式下使用NetApp Console"
- "開始在受限模式下使用NetApp Console"

雲端提供者權限

您需要特定權限才能直接從NetApp Console建立控制台代理，並且需要另一組權限來建立控制台代理本身。如果您直接從控制台在 AWS 或 Azure 中建立控制台代理，則控制台將使用其所需的權限建立控制台代理。

在標準模式下使用控制台時，如何提供權限取決於您計劃如何建立控制台代理。

若要了解如何設定權限，請參閱以下內容：

- 標準模式
  - "AWS 中的代理安裝選項"
  - "Azure 中的代理程式安裝選項"
  - "Google Cloud 中的代理程式安裝選項"
  - "為本地部署設定雲端權限"
- "設定限制模式的權限"

若要查看控制台代理日常操作所需的確切權限，請參閱以下頁面：

- "了解控制台代理程式如何使用 AWS 權限"
- "了解控制台代理程式如何使用 Azure 權限"
- "了解控制台代理程式如何使用 Google Cloud 權限"

您有責任在後續版本中新增權限時更新控制台代理程式策略。發行說明列出了新的權限。

代理升級

NetApp每月更新代理軟體以新增功能並提高穩定性。某些控制台功能（如Cloud Volumes ONTAP和本機ONTAP叢集管理）依賴控制台代理程式版本和設定。

當您在雲端安裝代理程式時，如果控制台代理可以存取互聯網，則會自動更新。

作業系統和虛擬機器維護

維護控制台代理主機上的作業系統是您（客戶）的責任。例如，您（客戶）應按照貴公司的作業系統分發標準程序，對控制台代理主機上的作業系統套用安全性更新。

請注意，您（客戶）在套用次要安全性更新時不需要停止控制台主機上的任何服務。

如果您（客戶）需要停止然後啟動控制台代理虛擬機，您應該從雲端提供者的控制台或使用標準的內部管理程序

來執行此操作。

控制台代理程式必須始終處於執行狀態 。

多系統和代理

一個代理可以在控制台中管理多個系統並支援資料服務。您可以根據部署規模和使用的資料服務使用單一代理程式來管理多個系統。

對於大規模部署，請與您的NetApp代表合作來確定您的環境規模。如果遇到問題，請聯絡NetApp支援。

以下是代理部署的一些範例：

- 您有一個多雲環境（例如，AWS 和 Azure），並且您希望在 AWS 中有一個代理，在 Azure 中有一個代理程式。每個系統都管理在這些環境中執行的Cloud Volumes ONTAP系統。
- 服務提供者可能使用一個控制台組織為其客戶提供服務，同時使用另一個組織為其某個業務部門提供災難復原。每個組織都需要自己的代理人。

# 部署控制台代理

## AWS

### AWS 中的控制台代理安裝選項

有幾種不同的方法可以在 AWS 中建立控制台代理。直接從NetApp Console是最常見的方式。

有以下安裝選項可用：

- "直接從控制台建立控制台代理"（這是標準選項）

  此操作將在您選擇的 VPC 中啟動執行 Linux 和控制台代理軟體的 EC2 執行個體。

- "從 AWS Marketplace 建立控制台代理"

  此操作也會啟動執行 Linux 和控制台代理軟體的 EC2 實例，但部署直接從 AWS Marketplace 啟動，而不是從控制台啟動。

- "在您自己的Linux主機上下載並手動安裝軟體"

您選擇的安裝選項會影響您如何準備安裝。這包括如何向控制台提供驗證和管理 AWS 中的資源所需的權限。

### 透過NetApp Console在 AWS 中建立控制台代理

您可以直接從NetApp Console在 AWS 中建立控制台代理程式。在從控制台建立 AWS 中的控制台代理之前，您需要設定網路並準備 AWS 權限。

開始之前

- 你應該有一個"了解控制台代理"。
- 你應該回顧一下"控制台代理限制"。

## 步驟 1：設定網路以在 AWS 中部署控制台代理

確保您打算安裝控制台代理的網路位置支援以下要求。這些要求使控制台代理程式能夠管理混合雲中的資源和流程。

**VPC** 和子網

建立控制台代理程式時，您需要指定它所在的 VPC 和子網路。

連接到目標網絡

控制台代理程式需要與您計劃建立和管理系統的位置建立網路連線。例如，您計劃在本機環境中建立Cloud Volumes ONTAP系統或儲存系統的網路。

出站互聯網訪問

部署控制台代理程式的網路位置必須具有出站網路連線才能聯絡特定端點。

從控制台代理聯繫的端點

控制台代理需要外部網路存取來聯繫以下端點，以管理公有雲環境中的資源和流程以進行日常操作。

下面列出的端點都是 CNAME 條目。

| 端點 | 目的 |
| --- | --- |
| AWS 服務（amazonaws.com）：<br>• 雲形成<br>• 彈性運算雲（EC2）<br>• 身分和存取管理 (IAM)<br>• 金鑰管理服務（KMS）<br>• 安全性令牌服務 (STS)<br>• 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：<br>• 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。 |
| \ 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。 |

| 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://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io | 取得控制台代理升級的影像。<br><br>• 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。<br><br>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"。<br><br>• 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。 |

從**NetApp**控制台聯繫的端點

當您使用透過 SaaS 層提供的基於 Web 的NetApp Console時，它會聯絡多個端點來完成資料管理任務。這包括從控制台聯繫以部署控制台代理的端點。

"查看從NetApp控制台聯繫的端點列表"。

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"

建立控制台代理程式後，您需要實作此網路要求。

步驟 **2**：為控制台代理程式設定 **AWS** 權限

控制台需要透過 AWS 進行身份驗證，然後才能在您的 VPC 中部署控制台代理程式。您可以選擇以下身份驗證方法之一：

- 讓控制台承擔具有所需權限的 IAM 角色
- 為具有所需權限的 IAM 使用者提供 AWS 存取金鑰和金鑰

無論選擇哪種方式，第一步都是建立 IAM 策略。此原則僅包含從控制台啟動 AWS 中的控制台代理程式所需的權限。

如果需要，您可以使用 IAM 限制 IAM 策略 `Condition`元素。 "AWS 文件：條件元素"

步驟

1. 前往 AWS IAM 主控台。
2. 選擇“策略”>“建立策略”。
3. 選擇 **JSON**。
4. 複製並貼上以下策略：

此原則僅包含從控制台啟動 AWS 中的控制台代理程式所需的權限。當控制台建立控制台代理時，它會將一組新權限套用至控制台代理，使控制台代理程式能夠管理 AWS 資源。"查看控制台代理本身所需的權限"。

```
{
  "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",
```

```
        "iam:ListRoles",
        "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",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeLaunchTemplates",
        "ec2:CreateLaunchTemplate",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "iam:GetRole",
        "iam:TagRole",
        "kms:ListAliases",
        "cloudformation:ListStacks"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:TerminateInstances"
      ],
```

```
        "Condition": {
          "StringLike": {
            "ec2:ResourceTag/OCCMInstance": "*"
          }
        },
        "Resource": [
          "arn:aws:ec2:*:*:instance/*"
        ]
      }
    ]
}
```

5. 選擇*下一步*並新增標籤（如果需要）。
6. 選擇*下一步*並輸入名稱和描述。
7. 選擇*建立策略*。
8. 將政策附加到控制台可以承擔的 IAM 角色或 IAM 用戶，以便您可以為控制台提供存取金鑰：
   - （選項 1）設定控制台可以承擔的 IAM 角色：
     i. 前往目標帳戶中的 AWS IAM 主控台。
     ii. 在存取管理下，選擇*角色>建立角色*並依照步驟建立角色。
     iii. 在 受信任實體類型 下，選擇 **AWS** 帳戶。
     iv. 選擇*另一個 AWS 帳戶*並輸入控制台 SaaS 帳戶的 ID：952013314444
     v. 選擇您在上一節中建立的策略。
     vi. 建立角色後，複製角色 ARN，以便在建立控制台代理時將其貼到控制台中。
   - （選項 2）為 IAM 使用者設定權限，以便您可以向控制台提供存取金鑰：
     i. 從 AWS IAM 控制台中，選擇 使用者，然後選擇使用者名稱。
     ii. 選擇*新增權限>直接附加現有策略*。
     iii. 選擇您建立的策略。
     iv. 選擇*下一步*，然後選擇*新增權限*。
     v. 確保您擁有 IAM 使用者的存取金鑰和金鑰。

結果

現在您應該擁有一個具有所需權限的 IAM 角色或一個具有所需權限的 IAM 使用者。從控制台建立控制台代理時，您可以提供有關角色或存取金鑰的資訊。

步驟 **3**：建立控制台代理

直接從基於 Web 的控制台建立控制台代理程式。

關於此任務

- 從控制台建立控制台代理程式使用預設配置在 AWS 中部署 EC2 執行個體。建立控制台代理程式後，請勿切換到具有較少 CPU 或較少 RAM 的較小 EC2 執行個體。"了解控制台代理的預設配置"。

- 當控制台建立控制台代理時，它會為代理程式建立一個 IAM 角色和一個設定檔。此角色包括使控制台代理程式能夠管理 AWS 資源的權限。確保在未來版本中新增權限時更新角色。"了解有關控制台代理的 IAM 策略的更多信息"。

開始之前

您應該具有以下內容：

- AWS 驗證方法：具有所需權限的 IAM 角色或 IAM 使用者的存取金鑰。
- 滿足組網需求的VPC及子網路。
- EC2 執行個體的金鑰對。
- 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。
- 設定"網路需求"。
- 設定"AWS 權限"。

步驟

1. 選擇“管理 **>** 代理”。
2. 在“概覽”頁面上，選擇“部署代理”>“AWS”
3. 依照精靈中的步驟建立控制台代理：
4. 在「簡介」頁面上提供了該過程的概述
5. 在 **AWS Credentials** 頁面上，指定您的 AWS 區域，然後選擇一種驗證方法，該方法可以是控制台可以承擔的 IAM 角色，也可以是 AWS 存取金鑰和金鑰。

   如果您選擇*承擔角色*，您可以從控制台代理部署精靈建立第一組憑證。任何附加憑證集都必須從憑證頁面建立。然後，它們將從嚮導的下拉清單中提供。"了解如何新增其他憑證" 。

6. 在「詳細資料」頁面上，提供有關控制台代理的詳細資訊。
   - 輸入名稱。
   - 新增自訂標籤（元資料）。
   - 選擇是否希望控制台建立具有所需權限的新角色，或是否要選擇您設定的現有角色"所需的權限"。
   - 選擇是否要加密控制台代理的 EBS 磁碟。您可以選擇使用預設加密金鑰或使用自訂金鑰。
7. 在*網路*頁面上，為代理指定 VPC、子網路和金鑰對，選擇是否啟用公用 IP 位址，並選擇性地指定代理程式配置。

   確保您擁有正確的金鑰對來存取控制台代理虛擬機器。如果沒有密鑰對，您就無法存取它。

8. 在「安全群組」頁面上，選擇是否建立新的安全性群組或是否選擇允許所需入站和出站規則的現有安全性群組。

   "查看 AWS 的安全群組規則" 。

9. 檢查您的選擇以驗證您的設定是否正確。
   a. 預設情況下，*驗證代理程式設定*複選框處於選取狀態，以便控制台在您部署時驗證網路連線要求。如果控制台無法部署代理，它會提供一份報告來幫助您排除故障。如果部署成功，則不會提供報告。

如果您仍在使用"先前的端點"用於代理升級，驗證失敗並出現錯誤。為了避免這種情況，請取消選取核取方塊以跳過驗證檢查。

10. 選擇“新增”。

    控制台大約需要 10 分鐘即可部署代理程式。停留在該頁面上，直到過程完成。

結果

過程完成後，即可從控制台使用控制台代理。

如果部署失敗，您可以從控制台下載報告和日誌來幫助您解決問題。"了解如何解決安裝問題。"

如果您在建立控制台代理程式的相同 AWS 帳戶中擁有 Amazon S3 儲存桶，您將看到 Amazon S3 工作環境自動出現在 系統 頁面上。 "了解如何從NetApp Console管理 S3 儲存桶"

### 從 **AWS Marketplace** 建立控制台代理

## 您可以直接從 AWS Marketplace 在 AWS 中建立控制台代理程式。若要從 AWS Marketplace 建立控制台代理，您需要設定網路、準備 AWS 權限、檢視執行個體要求，然後建立控制台代理。

開始之前

- 你應該有一個"了解控制台代理"。
- 你應該回顧一下"控制台代理限制"。

步驟 **1**：設定網絡

確保控制台代理程式的網路位置符合以下要求以管理混合雲資源。

**VPC** 和子網

建立控制台代理程式時，您需要指定它所在的 VPC 和子網路。

連接到目標網絡

控制台代理程式需要與您計劃建立和管理系統的位置建立網路連線。例如，您計劃在本機環境中建立Cloud Volumes ONTAP系統或儲存系統的網路。

出站互聯網訪問

部署控制台代理程式的網路位置必須具有出站網路連線才能聯絡特定端點。

從控制台代理聯繫的端點

控制台代理需要外部網路存取來聯繫以下端點，以管理公有雲環境中的資源和流程以進行日常操作。

下面列出的端點都是 CNAME 條目。

| 端點 | 目的 |
| --- | --- |
| AWS 服務（amazonaws.com）：<br>• 雲形成<br>• 彈性運算雲（EC2）<br>• 身分和存取管理 (IAM)<br>• 金鑰管理服務（KMS）<br>• 安全性令牌服務 (STS)<br>• 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：<br>• 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。 |
| \ 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。<br><br>• 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。<br><br>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"。<br><br>• 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。 |

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"

建立控制台代理程式後實現此網路存取。

### 步驟 2：設定 AWS 權限

為了準備市場部署，請在 AWS 中建立 IAM 策略並將其附加到 IAM 角色。當您從 AWS Marketplace 建立控制台代理程式時，系統會提示您選擇該 IAM 角色。

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。

      您可能需要根據計劃使用的NetApp資料服務建立第二個策略。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. 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

現在，您擁有一個 IAM 角色，可以在從 AWS Marketplace 部署期間將其與 EC2 執行個體關聯。

### 步驟 3：檢視實例要求

建立控制台代理程式時，您需要選擇符合下列要求的 EC2 執行個體類型。

中央處理器
: 8 個核心或 8 個 vCPU

記憶體
: 32GB

**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。

### 步驟 4：建立控制台代理

直接從 AWS Marketplace 建立控制台代理。

關於此任務

從 AWS Marketplace 建立控制台代理程式會使用預設配置在 AWS 中部署 EC2 執行個體。"了解控制台代理的預設配置" 。

開始之前

您應該具有以下內容：

- 滿足組網需求的VPC及子網路。
- 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。
- 您的 IAM 使用者訂閱並取消訂閱 AWS Marketplace 的權限。
- 了解執行個體的 CPU 和 RAM 需求。
- 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*。

     AWS 使用指定的設定啟動控制台代理，控制台代理將在大約十分鐘內運作。

如果安裝失敗，您可以查看日誌和報告來幫助您排除故障。"了解如何解決安裝問題。"

8. 從連接到控制台代理虛擬機器並具有控制台代理 URL 的主機開啟 Web 瀏覽器。
9. 登入後，設定控制台代理：
   a. 指定與控制台代理程式關聯的控制台組織。
   b. 輸入系統的名稱。
   c. 在*您是否在安全環境中運作？ *下保持限制模式為停用。

      保持限制模式處於停用狀態以便在標準模式下使用控制台。只有當您擁有安全的環境並希望中斷此帳戶與控制台後端服務的連線時，才應啟用受限模式。如果真是這樣的話，"依照步驟在受限模式下開始使用NetApp Console" 。

   d. 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。

開啟 Web 瀏覽器並前往 "NetApp Console"開始將控制台代理與控制台一起使用。

如果您在建立控制台代理程式的相同 AWS 帳戶中擁有 Amazon S3 儲存桶，您將看到 Amazon S3 工作環境自動出現在 系統 頁面上。 "了解如何從NetApp Console管理 S3 儲存桶"

在 **AWS** 中手動安裝控制台代理

## 您可以在 AWS 中執行的 Linux 主機上手動安裝控制台代理程式。要在您自己的 Linux 主機上手動安裝控制台代理，您需要查看主機要求、設定網路、準備 AWS 權限、安裝控制台代理，然後提供您準備好的權限。

開始之前

- 你應該有一個"了解控制台代理"。
- 你應該回顧一下"控制台代理限制"。

步驟 **1**：查看主機需求

確保運行控制台代理軟體的主機符合作業系統、記憶體和連接埠要求。

控制台代理保留 19000 到 19200 的 UID 和 GID 範圍。這個範圍是固定的，不能修改。如果主機上的任何第三方軟體使用此範圍內的 UID 或 GID，則代理安裝將會失敗。 NetApp建議使用沒有第三方軟體的主機以避免衝突。

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。

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<br>• 僅限英文版本。<br>• 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。<br>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<br>• 僅限英文版本。<br>• 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。<br>查看 Podman 設定要求 。 |

| 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** |
| --- | --- | --- | --- | --- |
| 在強制模式或寬容模式下受支持 | | 8.6 至 8.10<br>• 僅限英文版本。<br>• 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。<br>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 |

密鑰對

建立控制台代理程式時，您需要選擇一個 EC2 金鑰對來與執行個體一起使用。

使用 **IMDSv2** 時的 **PUT** 響應跳數限制

如果啟用了 IMDSv2（新 EC2 執行個體的預設設定），請將 PUT 回應跳數限制設為 3。否則，系統會在代理設定期間顯示 UI 初始化錯誤。

- "要求在 Amazon EC2 執行個體上使用 IMDSv2"
- "AWS 文件：變更 PUT 回應跳數限制"

### 步驟 2：安裝 **Podman** 或 **Docker Engine**

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 **3**：設定網絡

請確保網路位置符合以下要求，以便控制台代理程式能夠管理混合雲中的資源。

連接到目標網絡

控制台代理程式需要與您計劃建立和管理系統的位置建立網路連線。例如，您計劃在本機環境中建立Cloud Volumes ONTAP系統或儲存系統的網路。

出站互聯網訪問

部署控制台代理程式的網路位置必須具有出站網路連線才能聯絡特定端點。

使用基於 **Web** 的**NetApp Console**時從電腦聯繫的端點

從 Web 瀏覽器存取控制台的電腦必須能夠聯絡多個端點。您需要使用控制台來設定控制台代理並進行控制台的日常使用。

"為NetApp控制台準備網絡" 。

從控制台代理聯繫的端點

控制台代理需要外部網路存取來聯繫以下端點，以管理公有雲環境中的資源和流程以進行日常操作。

下面列出的端點都是 CNAME 條目。

| 端點 | 目的 |
| --- | --- |
| AWS 服務（amazonaws.com）：<br>• 雲形成<br>• 彈性運算雲（EC2）<br>• 身分和存取管理 (IAM)<br>• 金鑰管理服務（KMS）<br>• 安全性令牌服務 (STS)<br>• 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：<br>• 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。 |
| \ 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。 |

| 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://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io | 取得控制台代理升級的影像。<br><br>• 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。<br><br>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" 。<br><br>• 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。 |

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"

步驟 **4**：設定控制台的 **AWS** 權限

請使用下列選項之一為NetApp Console提供 AWS 權限：

- 選項 1：建立 IAM 原則並將政策附加到可與 EC2 執行個體關聯的 IAM 角色。
- 選項 2：向控制台提供具有所需權限的 IAM 使用者的 AWS 存取金鑰。

依照步驟準備控制台的權限。

**IAM** 角色

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. 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

安裝控制台代理程式後，您現在擁有一個可以與 EC2 執行個體關聯的 IAM 角色。

**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。

結果

現在，您擁有一個具有所需權限的 IAM 使用者和一個可以提供給控制台的存取金鑰。

步驟 **5**：安裝控制台代理

完成所有先決條件後，請在您的 Linux 主機上手動安裝軟體。

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"。

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。

2. 等待安裝完成。

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。

如果安裝失敗，您可以查看安裝報告和日誌來協助您解決問題。"了解如何解決安裝問題。"

1. 從連接到控制台代理虛擬機器的主機開啟 Web 瀏覽器並輸入以下 URL：

<a href="https://<em>ipaddress</em>" class="bare">https://<em>ipaddress</em></a>

2. 登入後，設定控制台代理：

a. 指定與控制台代理程式關聯的組織。

b. 輸入系統的名稱。

c. 在*您是否在安全環境中運作？ *下保持限制模式為停用。

您應該保持限制模式處於停用狀態，因為這些步驟描述如何在標準模式下使用控制台。只有當您擁有安全的環境並希望中斷此帳戶與後端服務的連線時，才應啟用受限模式。如果真是這樣的話，"依照步驟在受限模式下開始使用NetApp Console" 。

d. 選擇*讓我們開始吧*。

如果您在建立控制台代理程式的相同 AWS 帳戶中擁有 Amazon S3 儲存桶，您將看到 Amazon S3 儲存系統自動出現在 系統 頁面上。 "了解如何透過NetApp ConsoleP 管理 S3 儲存桶"

步驟 **6**：提供對**NetApp Console**的權限

安裝控制台代理程式後，提供您設定的 AWS 權限，以便控制台代理程式可以管理您在 AWS 中的資料和儲存基礎架構。

**IAM** 角色

將建立的 IAM 角色附加到控制台代理 EC2 執行個體。

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。

前往 "NetApp Console"開始使用控制台代理。

**AWS** 存取金鑰

向控制台提供具有所需權限的 IAM 使用者的 AWS 存取金鑰。

步驟

1. 確保目前在控制台中選擇了正確的控制台代理。
2. 選擇“管理 **>** 憑證”。
3. 選擇*組織憑證*。
4. 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*。

前往 "NetApp Console"開始使用控制台代理。

## Azure

### **Azure** 中的控制台代理安裝選項

有幾種不同的方法可以在 Azure 中建立控制台代理程式。直接從NetApp Console是最常見的方式。

有以下安裝選項可用：

- "直接從NetApp Console建立控制台代理"（這是標準選項）

  此操作將在您選擇的 VNet 中啟動運行 Linux 和控制台代理軟體的 VM。

- "從 Azure 市集建立控制台代理"

  此操作也會啟動執行 Linux 和控制台代理軟體的 VM，但部署直接從 Azure 市場啟動，而不是從控制台啟

動。

- "在您自己的Linux主機上下載並手動安裝軟體"

您選擇的安裝選項會影響您如何準備安裝。這包括如何為控制台代理程式提供在 Azure 中驗證和管理資源所需的權限。

從**NetApp Console**在 **Azure** 中建立控制台代理

# 若要從NetApp Console在 Azure 中建立控制台代理，您需要設定網路、準備 Azure 權限，然後建立控制台代理程式。

開始之前

- 你應該有一個"了解控制台代理"。
- 你應該回顧一下"控制台代理限制"。

步驟 **1**：設定網絡

確保您打算安裝控制台代理的網路位置支援以下要求。這些要求允許控制台代理管理混合雲資源。

**Azure** 區域

如果您使用Cloud Volumes ONTAP，則控制台代理程式應部署在與其管理的Cloud Volumes ONTAP系統相同的 Azure 區域中，或部署在 "Azure 區域對"適用於Cloud Volumes ONTAP系統。此要求可確保在Cloud Volumes ONTAP及其關聯的儲存帳戶之間使用 Azure Private Link 連線。

"了解Cloud Volumes ONTAP如何使用 Azure Private Link"

**VNet** 與子網路

建立控制台代理程式時，您需要指定它所在的 VNet 和子網路。

連接到目標網絡

控制台代理程式需要與您計劃建立和管理系統的位置建立網路連線。例如，您計劃在本機環境中建立Cloud Volumes ONTAP系統或儲存系統的網路。

出站互聯網訪問

部署控制台代理程式的網路位置必須具有出站網路連線才能聯絡特定端點。

從控制台代理聯繫的端點

控制台代理需要外部網路存取來聯繫以下端點，以管理公有雲環境中的資源和流程以進行日常操作。

下面列出的端點都是 CNAME 條目。

| 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.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。 |

| 端點 | 目的 |
| --- | --- |
| \ 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。 |
| \ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io | 取得控制台代理升級的影像。<br>• 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。<br>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" 。<br>• 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。 |

從**NetApp**控制台聯繫的端點

當您使用透過 SaaS 層提供的基於 Web 的NetApp Console時，它會聯絡多個端點來完成資料管理任務。這包括從控制台聯繫以部署控制台代理的端點。

"查看從NetApp控制台聯繫的端點列表" 。

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"

您需要在建立控制台代理程式後實現此網路要求。

步驟 **2**：建立控制台代理部署策略（自訂角色）

您需要建立一個具有在 Azure 中部署控制台代理程式的權限的自訂角色。

建立 Azure 自訂角色，您可以將其指派給您的 Azure 帳戶或 Microsoft Entra 服務主體。控制台透過 Azure 進行驗證，並使用這些權限代表您建立控制台代理程式。

控制台在 Azure 中部署控制台代理虛擬機，啟用 "系統分配的託管標識"，建立所需的角色，並將其指派給虛擬機器。"查看控制台如何使用權限" 。

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. 複製 Azure 中新自訂角色所需的權限並將其保存在 JSON 檔案中。

   此自訂角色僅包含從控制台啟動 Azure 中的控制台代理程式 VM 所需的權限。請勿將此政策用於其他情況。當控制台建立控制台代理程式時，它會將一組新權限套用至控制台代理程式 VM，使控制台代理程式能夠管理 Azure 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. 透過將 Azure 訂閱 ID 新增至可分配範圍來修改 JSON。

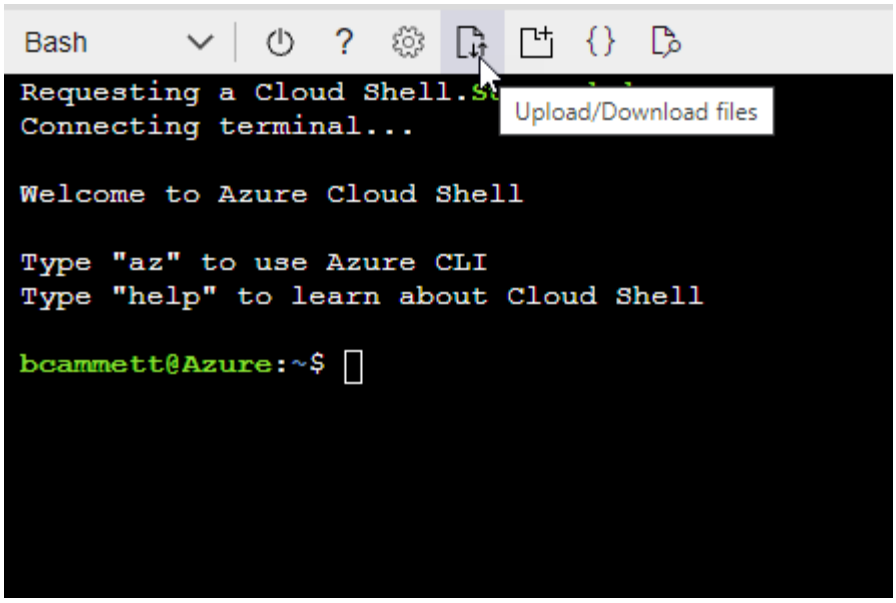
   例子

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

3. 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. 輸入以下 Azure CLI 指令：

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

您現在有一個名為“Azure SetupAsService”的自訂角色。您可以將此自訂角色套用到您的使用者帳戶或服務主體。

步驟 **3**：設定身份驗證

從控制台建立控制台代理程式時，您需要提供登入名，以使控制台能夠透過 Azure 進行驗證並部署 VM。您有兩個選擇：

1. 出現提示時使用您的 Azure 帳戶Sign in。此帳戶必須具有特定的 Azure 權限。這是預設選項。
2. 提供有關 Microsoft Entra 服務主體的詳細資訊。此服務主體也需要特定的權限。

請依照下列步驟準備其中一種驗證方法以供控制台使用。

**Azure** 帳戶

將自訂角色指派給將從控制台部署控制台代理程式的使用者。

步驟

1. 在 Azure 入口網站中，開啟 **Subscriptions** 服務並選擇使用者的訂閱。
2. 點選*存取控制 (IAM)*。
3. 按一下*新增*>*新增角色分配*，然後新增權限：
   a. 選擇 **Azure SetupAsService** 角色並點選 下一步。

      Azure SetupAsService 是 Azure 控制台代理程式部署原則中提供的預設名稱。如果您為角色選擇了不同的名稱，請選擇該名稱。

   b. 保持選取「使用者、群組或服務主體」 。
   c. 按一下*選擇成員*，選擇您的使用者帳戶，然後按一下*選擇*。
   d. 按一下“下一步”。
   e. 按一下*審閱+分配*。

服務主體

您無需使用 Azure 帳戶登錄，而是可以向控制台提供具有所需權限的 Azure 服務主體的憑證。

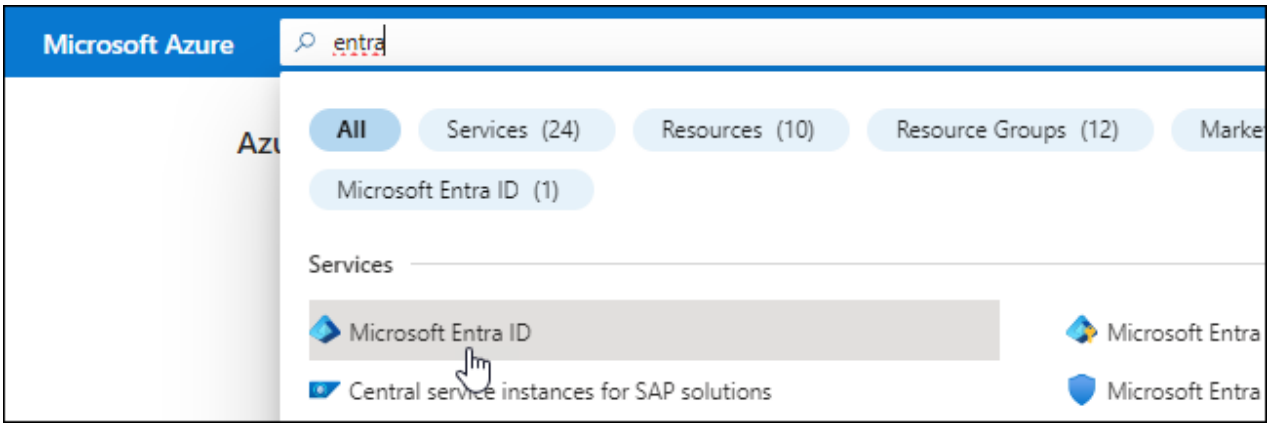
在 Microsoft Entra ID 中建立並設定服務主體，並取得控制台所需的 Azure 憑證。

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*。

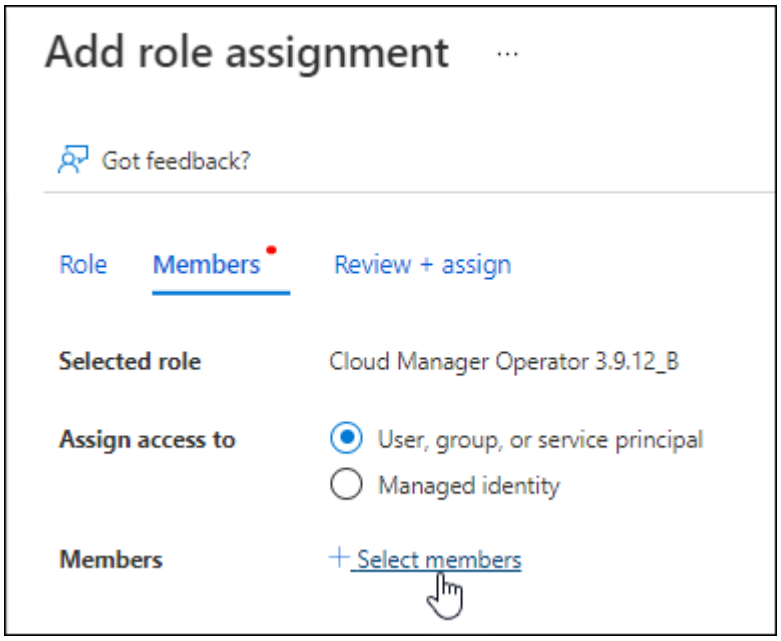
您已建立 AD 應用程式和服務主體。

將自訂角色指派給應用程式

1. 從 Azure 入口網站開啟 **Subscriptions** 服務。
2. 選擇訂閱。
3. 點選*存取控制 (IAM) > 新增 > 新增角色分配*。
4. 在「角色」標籤中，選擇「控制台操作員」角色，然後按一下「下一步」。
5. 在「成員」標籤中，完成以下步驟：

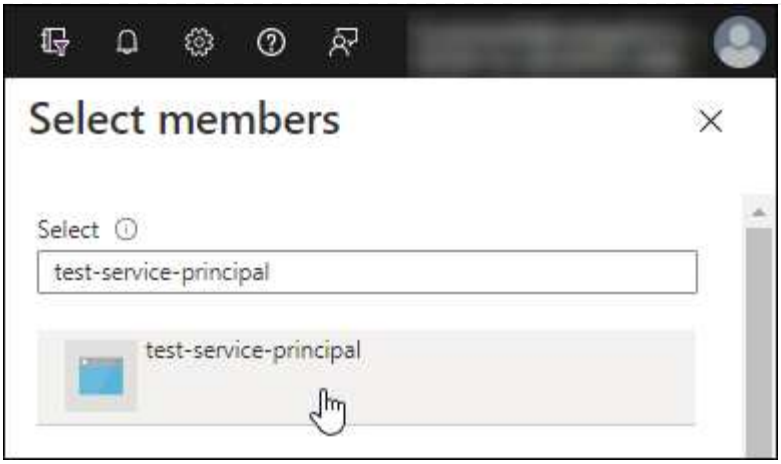
a. 保持選取「使用者、群組或服務主體」。

b. 按一下“選擇成員”。




c. 搜尋應用程式的名稱。

以下是一個例子：




a. 選擇應用程式並點擊*選擇*。

b. 按一下“下一步”。

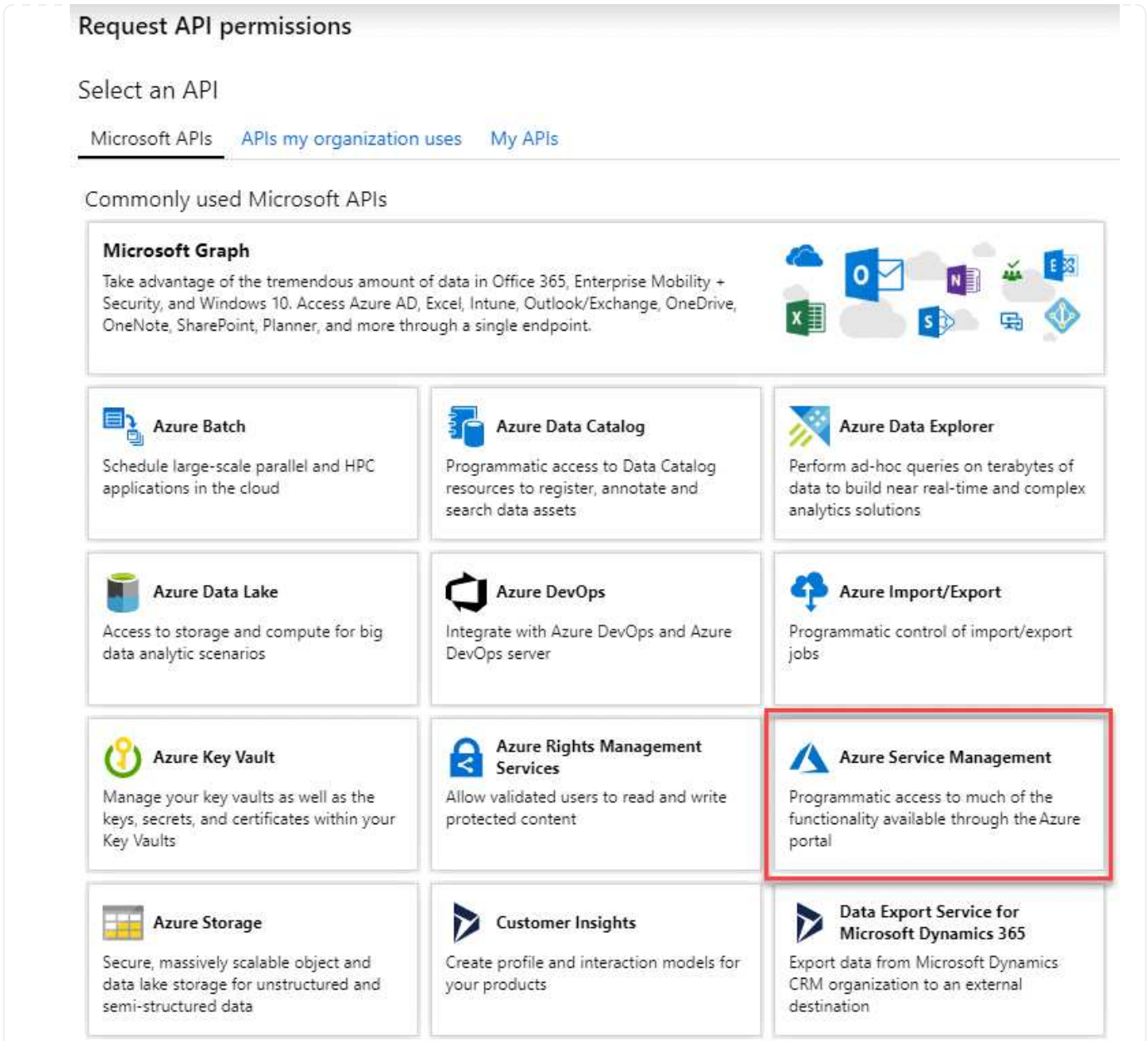
6. 按一下*審閱+分配*。

服務主體現在具有部署控制台代理程式所需的 Azure 權限。

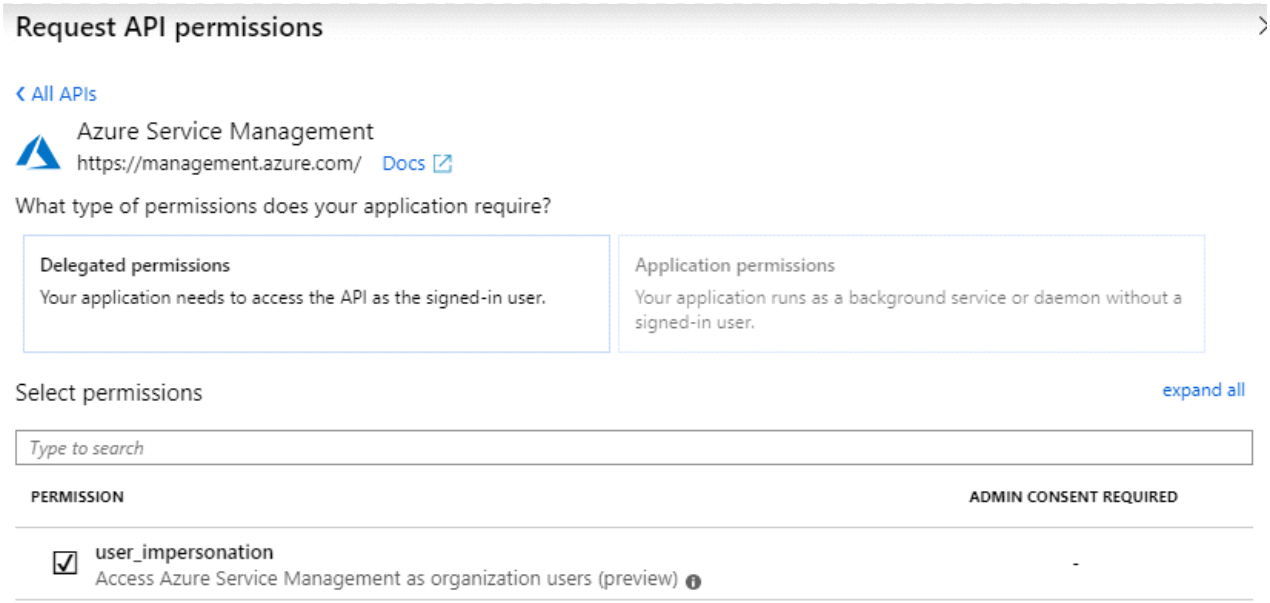
如果您想要管理多個 Azure 訂閱中的資源，則必須將服務主體繫結至每個訂閱。例如，控制台允許您選擇部署Cloud Volumes ONTAP時要使用的訂閱。

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」。

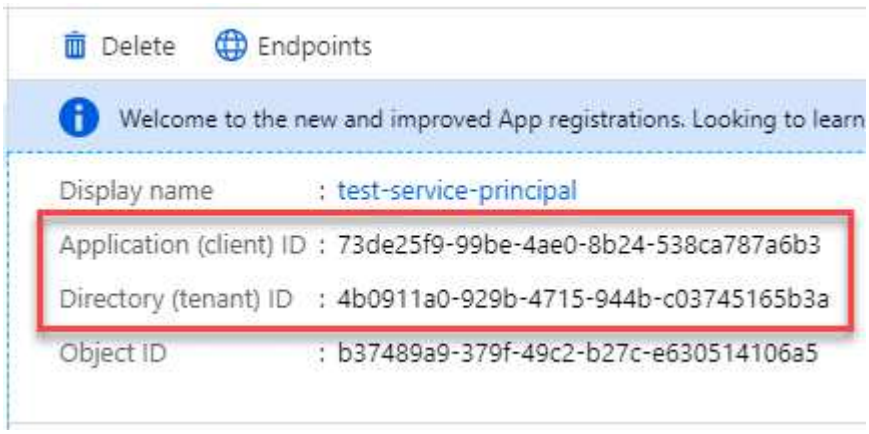



4. 選擇*以組織使用者身分存取 Azure 服務管理*，然後選擇*新增權限*。




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置，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。建立控制台代理時，您需要在控制台中輸入此資訊。

步驟 **4**：建立控制台代理

直接從NetApp Console建立控制台代理程式。

關於此任務

- 從控制台建立控制台代理程式會使用預設配置在 Azure 中部署虛擬機器。建立控制台代理程式後，請勿切換到具有較少 CPU 或較少 RAM 的較小 VM 執行個體。"了解控制台代理的預設配置" 。
- 當控制台部署控制台代理程式時，它會建立一個自訂角色並將其指派給控制台代理 VM。此角色包括使控制台代理程式能夠管理 Azure 資源的權限。您需要確保角色保持最新，因為在後續版本中新增了新的權限。"了解有關控制台代理的自訂角色的更多信息" 。

開始之前

您應該具有以下內容：

- Azure 訂閱。
- 您選擇的 Azure 區域中的 VNet 和子網路。
- 如果您的組織需要代理來處理所有傳出的網路流量，請提供關於代理伺服器的詳細資訊：
  - IP 位址
  - 證書
  - HTTPS 憑證
- 如果您想要對控制台代理虛擬機器使用該驗證方法，則需要 SSH 公鑰。身份驗證方法的另一種選擇是使用密碼。

  "了解如何連接到 Azure 中的 Linux VM"

- 如果您不希望控制台自動為控制台代理程式建立 Azure 角色，則需要建立自己的"使用此頁面上的政策"。

  這些權限適用於控制台代理本身。這與您先前為部署控制台代理虛擬機器而設定的權限不同。

步驟

1. 選擇“管理 **>** 代理”。
2. 在“概述”頁面上，選擇“部署代理”>“Azure”

3. 在*審核*頁面上，審核部署代理程式的要求。這些要求也在本頁上方詳細說明。
4. 在「虛擬機器驗證」頁面上，選擇與您設定 Azure 權限的方式相符的驗證選項：
   - 選擇*登入*登入您的 Microsoft 帳戶，該帳戶應具有所需的權限。

     該表單由 Microsoft 擁有並託管。您的憑證未提供給NetApp。

     如果您已經登入 Azure 帳戶，則控制台會自動使用該帳戶。如果您有多個帳戶，那麼您可能需要先登出以確保您使用的是正確的帳戶。
   - 選擇「**Active Directory** 服務主體」以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

   了解如何取得服務主體的這些值 。
5. 在「虛擬機器驗證」頁面上，選擇 Azure 訂閱、位置、新資源群組或現有資源群組，然後為您正在建立的控制台代理虛擬機器選擇驗證方法。

   虛擬機器的身份驗證方法可以是密碼或 SSH 公鑰。

   "了解如何連接到 Azure 中的 Linux VM"
6. 在「詳細資料」頁面上，輸入代理的名稱，指定標籤，並選擇是否希望控制台建立具有所需權限的新角色，或是否要選擇您設定的現有角色"所需的權限"。

   請注意，您可以選擇與此角色關聯的 Azure 訂閱。您選擇的每個訂閱都會為控制台代理提供管理該訂閱中的資源的權限（例如， Cloud Volumes ONTAP）。
7. 在「網路」頁面上，選擇 VNet 和子網，是否啟用公用 IP 位址，並可選擇指定代理設定。
   - 在「安全群組」頁面上，選擇是否建立新的安全性群組或是否選擇允許所需入站和出站規則的現有安全性群組。

     "查看 Azure 的安全性群組規則" 。
8. 檢查您的選擇以驗證您的設定是否正確。
   a. 預設情況下，*驗證代理程式設定*複選框處於選取狀態，以便控制台在您部署時驗證網路連線要求。如果控制台無法部署代理，它會提供一份報告來幫助您排除故障。如果部署成功，則不會提供報告。

   如果您仍在使用"先前的端點"用於代理升級，驗證失敗並出現錯誤。為了避免這種情況，請取消選取核取方塊以跳過驗證檢查。
9. 選擇“新增”。

   控制台大約需要 10 分鐘才能準備好代理。停留在該頁面上，直到過程完成。

結果

過程完成後，即可從控制台使用控制台代理。

如果部署失敗，您可以從控制台下載報告和日誌來幫助您解決問題。"了解如何解決安裝問題。"

如果您在建立控制台代理程式的相同 Azure 帳戶中擁有 Azure Blob 存儲，您將看到 Azure Blob 儲存體會自動出現在 系統 頁面上。 "了解如何透過NetApp Console管理 Azure Blob 儲存"

從 **Azure** 市集建立控制台代理

# 您可以直接從 Azure 市場在 Azure 中建立控制台代理程式。若要從 Azure 市集建立控制台代理，您需要設定網路、準備 Azure 權限、檢視執行個體要求，然後建立控制台代理程式。

開始之前

- 你應該有一個"了解控制台代理"。
- 審查"控制台代理限制"。

步驟 **1**：設定網絡

確保您打算安裝控制台代理的網路位置支援以下要求。這些要求使控制台代理程式能夠管理混合雲中的資源。

**Azure** 區域

如果您使用Cloud Volumes ONTAP，則控制台代理程式應部署在與其管理的Cloud Volumes ONTAP系統相同的 Azure 區域中，或部署在 "Azure 區域對"適用於Cloud Volumes ONTAP系統。此要求可確保在Cloud Volumes ONTAP及其關聯的儲存帳戶之間使用 Azure Private Link 連線。

"了解Cloud Volumes ONTAP如何使用 Azure Private Link"

**VNet** 與子網路

建立控制台代理程式時，您需要指定它所在的 VNet 和子網路。

連接到目標網絡

控制台代理程式需要與您計劃建立和管理系統的位置建立網路連線。例如，您計劃在本機環境中建立Cloud Volumes ONTAP系統或儲存系統的網路。

出站互聯網訪問

部署控制台代理程式的網路位置必須具有出站網路連線才能聯絡特定端點。

從控制台代理聯繫的端點

控制台代理需要外部網路存取來聯繫以下端點，以管理公有雲環境中的資源和流程以進行日常操作。

下面列出的端點都是 CNAME 條目。

| 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。 |

| 端點 | 目的 |
| --- | --- |
| \ 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。 |
| \ 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。 |
| \ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io | 取得控制台代理升級的影像。<br><br>• 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。<br><br>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" 。<br><br>• 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。 |

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"

建立控制台代理程式後實現網路要求。

步驟 **2**：查看 **VM** 需求

建立控制台代理程式時，請選擇符合下列要求的虛擬機器類型。

中央處理器

8 個核心或 8 個 vCPU

記憶體

32GB

**Azure VM** 大小

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

步驟 **3**：設定權限

您可以透過以下方式提供權限：

- 選項 1：使用系統指派的託管識別為 Azure VM 指派自訂角色。
- 選項 2：提供控制台具有所需權限的 Azure 服務主體的憑證。

請依照下列步驟設定控制台的權限。

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"

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。

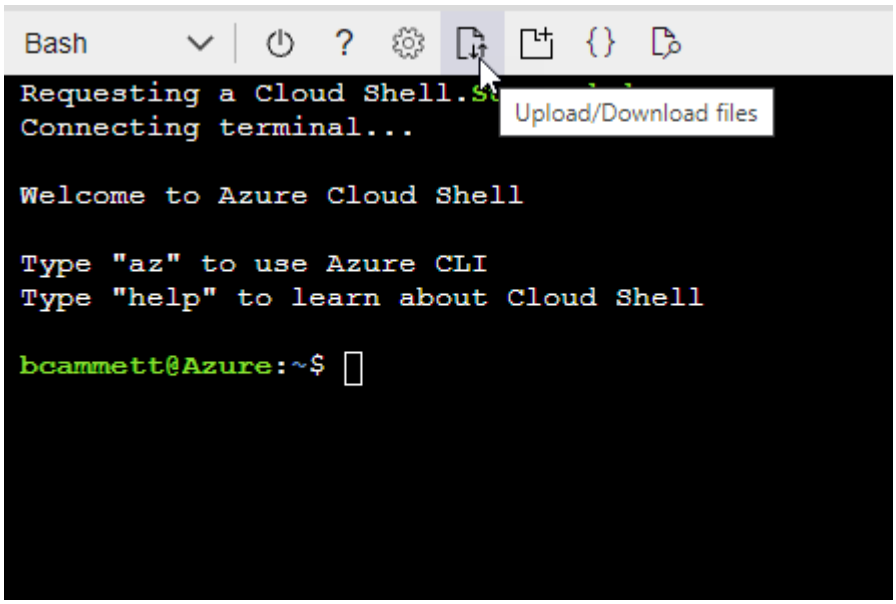
   例子

   ```
   "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
```

服務主體

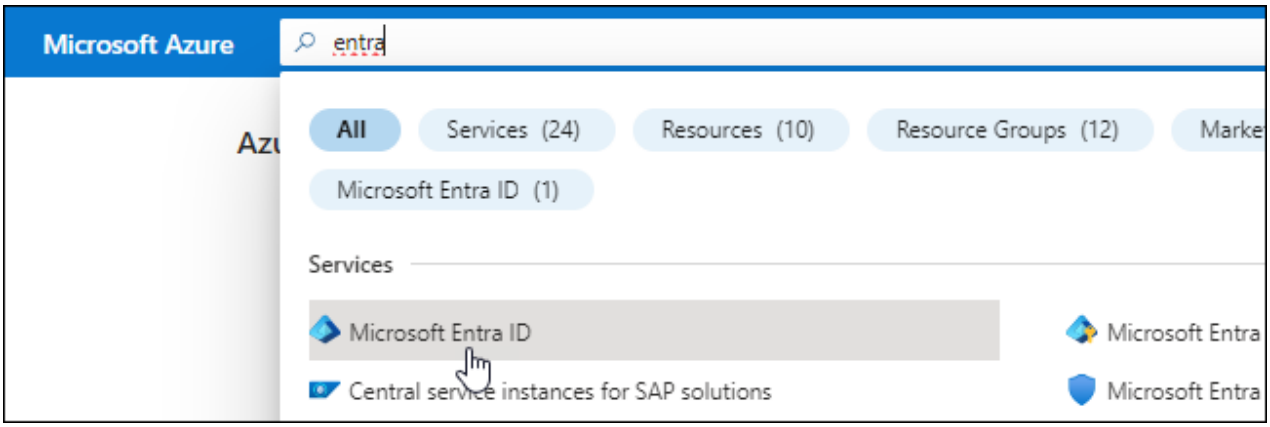
在 Microsoft Entra ID 中建立並設定服務主體，並取得控制台所需的 Azure 憑證。

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。

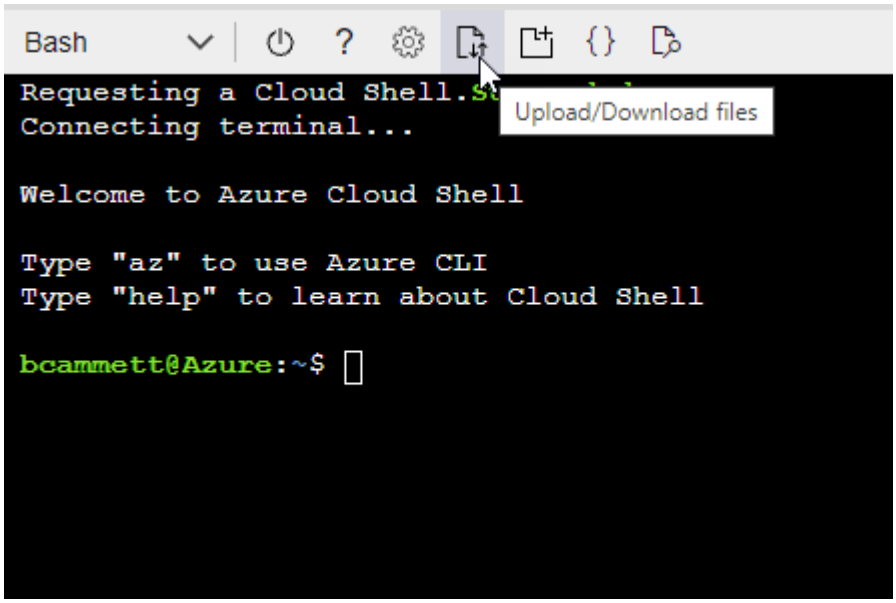
例子

```
"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。

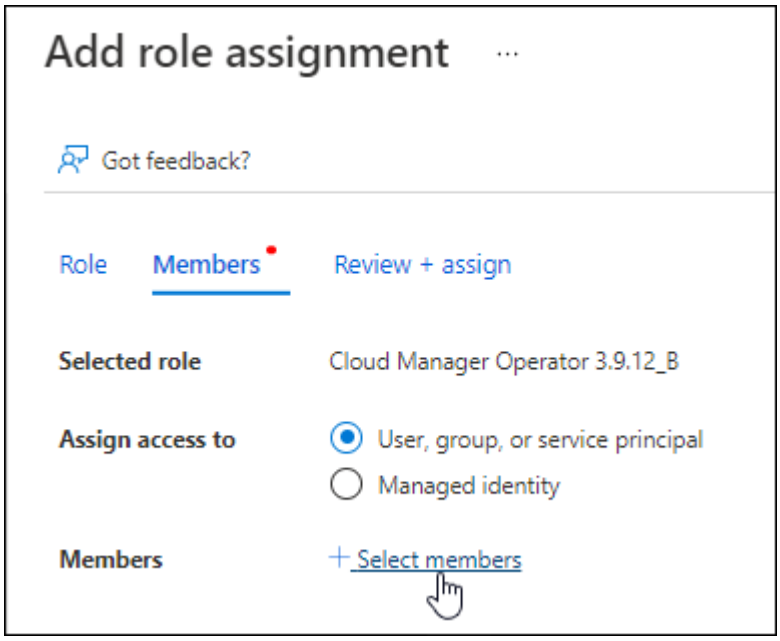
b. 選擇訂閱。

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*。

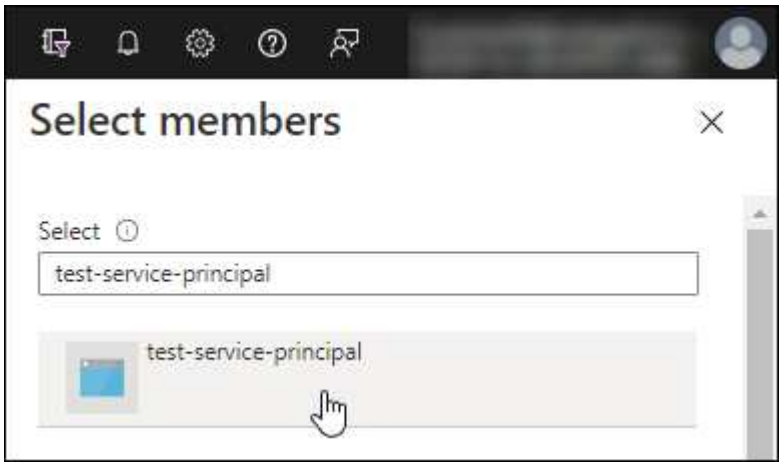
e. 在「成員」標籤中，完成以下步驟：

- 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”。

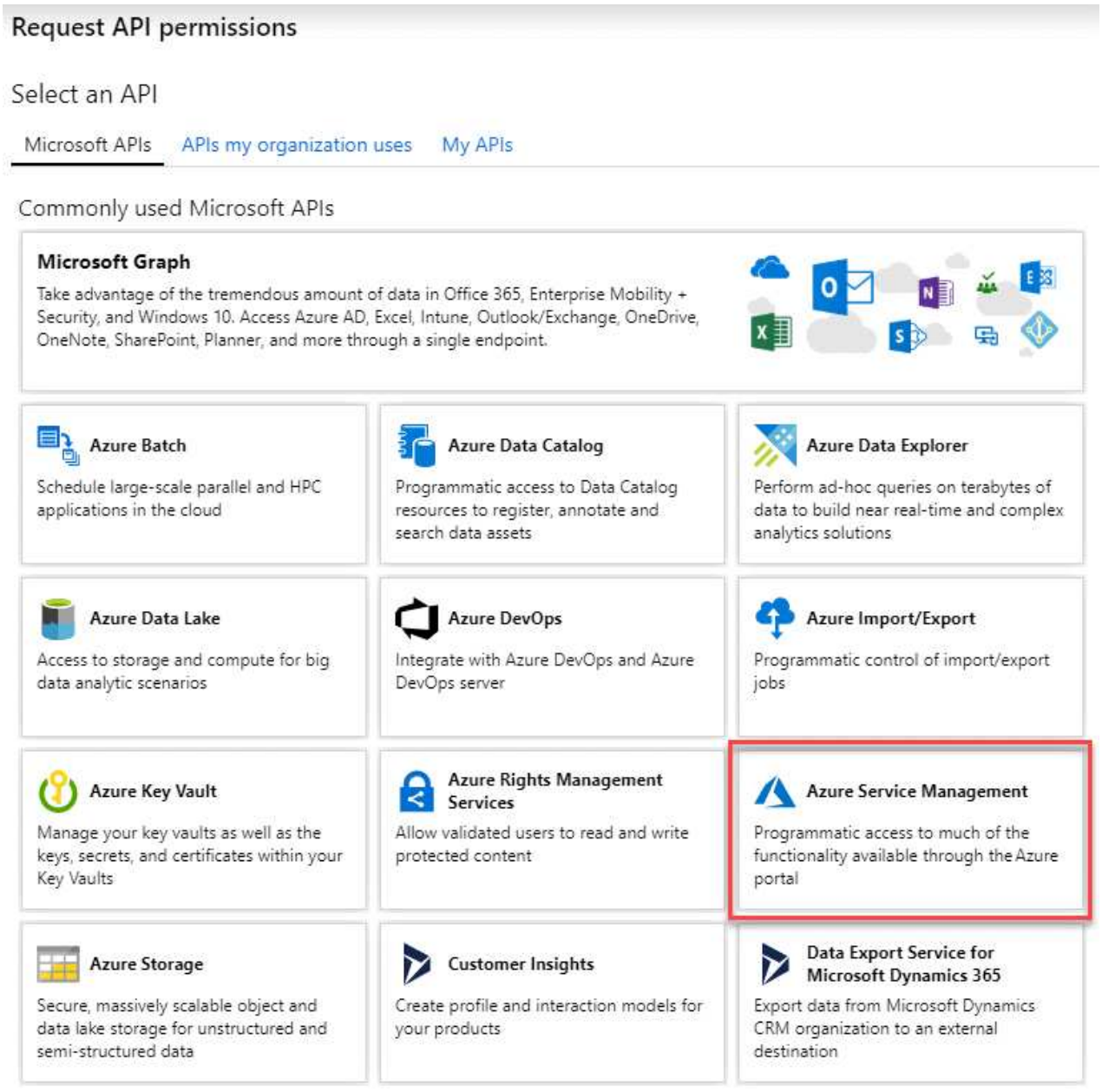
f. 選擇*審閱+分配*。

服務主體現在具有部署控制台代理程式所需的 Azure 權限。

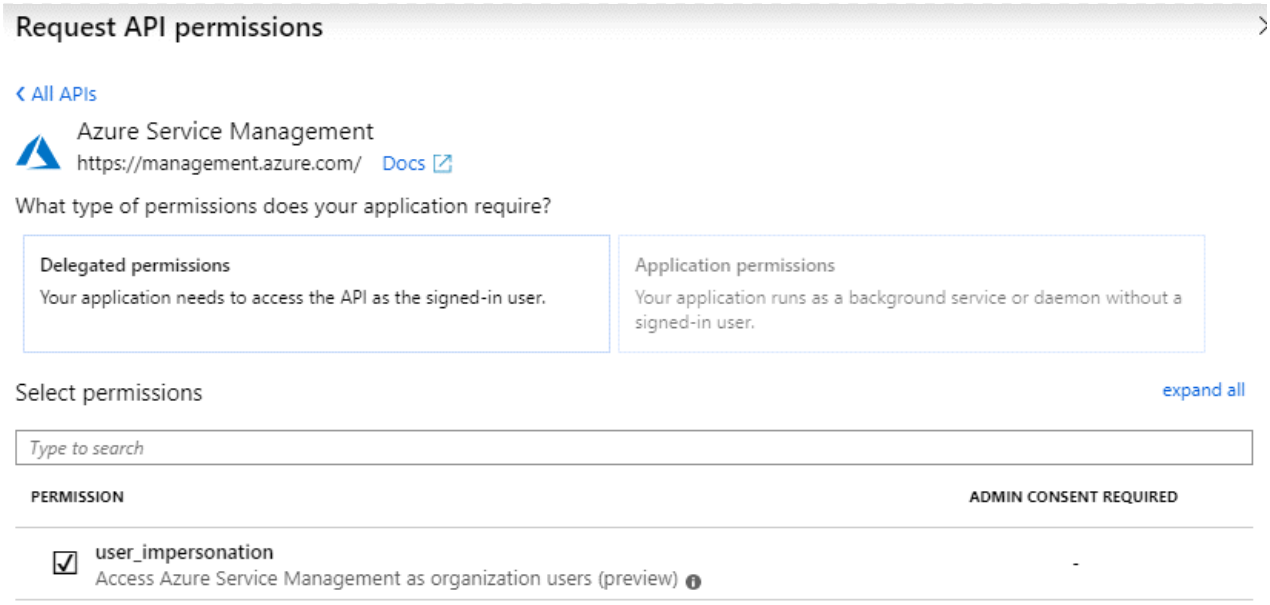
如果您想要從多個 Azure 訂閱部署Cloud Volumes ONTAP ，則必須將服務主體綁定到每個訂閱。在NetApp Console中，您可以選擇部署Cloud Volumes ONTAP時要使用的訂閱。

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」。

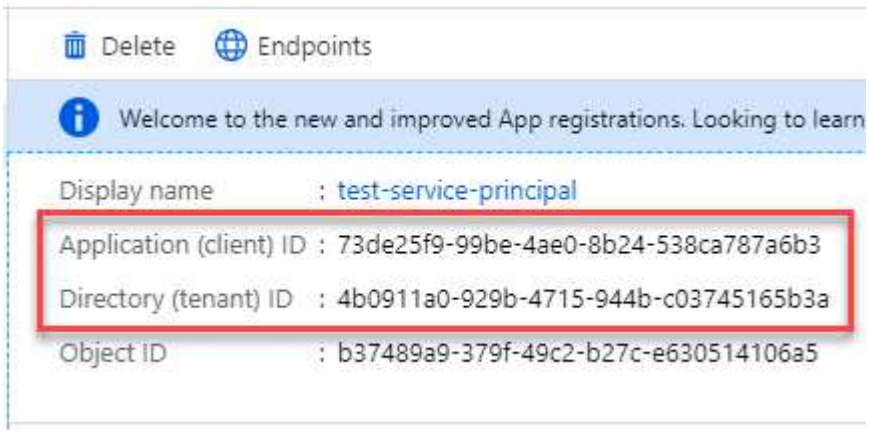



4. 選擇*以組織使用者身分存取 Azure 服務管理*，然後選擇*新增權限*。




取得應用程式的應用程式**ID**和目錄**ID**

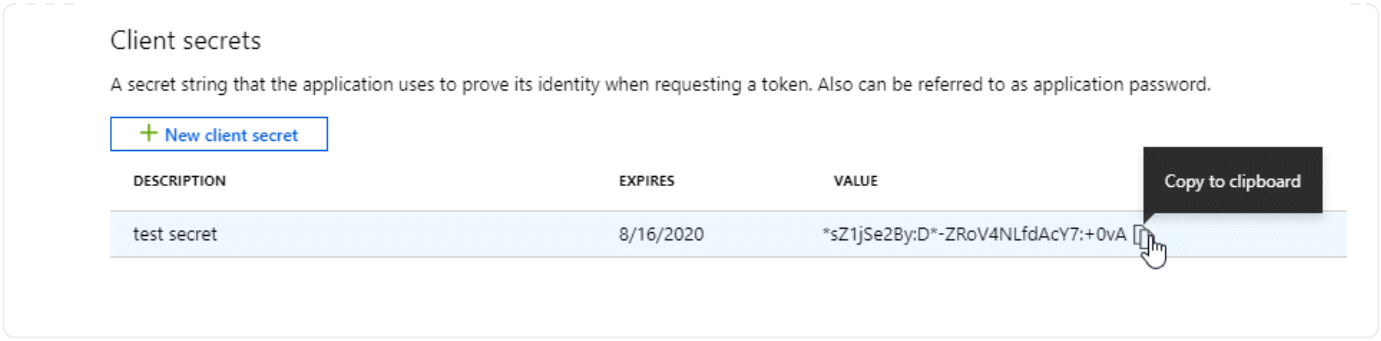
1. 在*Microsoft Entra ID*服務中，選擇*App Registrations*並選擇應用程式。
2. 複製*應用程式（客戶端）ID*和*目錄（租用戶）ID*。




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。




步驟 **4**：建立控制台代理

直接從 Azure 市集啟動控制台代理程式。

關於此任務

從 Azure 市場建立控制台代理程式會設定具有預設配置的虛擬機器。"了解控制台代理的預設配置" 。

開始之前

您應該具有以下內容：

- Azure 訂閱。
- 您選擇的 Azure 區域中的 VNet 和子網路。
- 如果您的組織需要代理來處理所有傳出的網路流量，請提供關於代理伺服器的詳細資訊：
  - IP 位址
  - 證書
  - HTTPS 憑證
- 如果您想要對控制台代理虛擬機器使用該驗證方法，則需要 SSH 公鑰。身份驗證方法的另一種選擇是使用密碼。

  "了解如何連接到 Azure 中的 Linux VM"

- 如果您不希望控制台自動為控制台代理程式建立 Azure 角色，則需要建立自己的"使用此頁面上的政策"。

  這些權限適用於控制台代理實例本身。這與您先前為部署控制台代理虛擬機器而設定的權限不同。

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"

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。
- 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*。

  此設定很重要，因為託管身分允許控制台代理虛擬機器向 Microsoft Entra ID 標識自己，而無需提供任何憑證。 "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。

   Azure 使用指定的設定部署虛擬機器。您應該會在大約十分鐘內看到虛擬機器和控制台代理軟體運作。

   如果安裝失敗，您可以查看日誌和報告來幫助您排除故障。"了解如何解決安裝問題。"

5. 從連接到控制台代理虛擬機器的主機開啟 Web 瀏覽器並輸入以下 URL：

   <a href="https://<em>ipaddress</em>" class="bare">https://<em>ipaddress</em></a>

6. 登入後，設定控制台代理：
   a. 指定與控制台代理程式關聯的控制台組織。
   b. 輸入系統的名稱。
   c. 在*您是否在安全環境中運作？ *下保持限制模式為停用。

      保持限制模式處於停用狀態以便在標準模式下使用控制台。只有當您擁有安全的環境並希望中斷此帳戶與控制台後端服務的連線時，才應啟用受限模式。如果真是這樣的話，"依照步驟開始在受限模式下使用控制台" 。

   d. 選擇*讓我們開始吧*。

結果

現在您已經安裝了控制台代理並將其與您的控制台組織一起設定。

如果您在建立控制台代理程式的相同 Azure 訂閱中擁有 Azure Blob 存儲，您將看到 Azure Blob 儲存系統自動出現在「系統」頁面上。 "了解如何從控制台管理 Azure Blob 存儲"

步驟 **5**：向控制台代理提供權限

現在您已經建立了控制台代理，您需要為其提供先前設定的權限。提供權限使控制台代理程式能夠管理 Azure 中的資料和儲存基礎結構。

自訂角色

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。

下一步是什麼？

前往 "NetApp Console"開始使用控制台代理。

服務主體

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

控制台現在具有代表您在 Azure 中執行操作所需的權限。

在 **Azure** 中手動安裝控制台代理

# 要在您自己的 Linux 主機上手動安裝控制台代理，您需要查看主機要求、設定網路、準備 Azure 權限、安裝控制台代理，然後提供您準備好的權限。

開始之前

- 你應該有一個"了解控制台代理"。
- 你應該回顧一下"控制台代理限制"。

步驟 **1**：查看主機需求

控制台代理軟體必須在滿足特定作業系統要求、RAM 要求、連接埠要求等的主機上執行。

控制台代理保留 19000 到 19200 的 UID 和 GID 範圍。這個範圍是固定的，不能修改。如果主機上的任何第三方軟體使用此範圍內的 UID 或 GID，則代理安裝將會失敗。 NetApp建議使用沒有第三方軟體的主機以避免衝突。

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。

**Azure VM** 大小

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

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<br>• 僅限英文版本。<br>• 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。<br>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<br>• 僅限英文版本。<br>• 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。<br>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<br>• 僅限英文版本。<br>• 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。<br>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 **2**：安裝 **Podman** 或 **Docker Engine**

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 **2.** 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 **3**：設定網絡

確保您打算安裝控制台代理的網路位置支援以下要求。滿足這些要求使控制台代理程式能夠管理混合雲環境中的資源和流程。

**Azure** 區域

如果您使用Cloud Volumes ONTAP，則控制台代理程式應部署在與其管理的Cloud Volumes ONTAP系統相同的 Azure 區域中，或部署在 "Azure 區域對"適用於Cloud Volumes ONTAP系統。此要求可確保在Cloud Volumes ONTAP及其關聯的儲存帳戶之間使用 Azure Private Link 連線。

"了解Cloud Volumes ONTAP如何使用 Azure Private Link"

連接到目標網絡

控制台代理程式需要與您計劃建立和管理系統的位置建立網路連線。例如，您計劃在本機環境中建立Cloud Volumes ONTAP系統或儲存系統的網路。

出站互聯網訪問

部署控制台代理程式的網路位置必須具有出站網路連線才能聯絡特定端點。

使用基於 **Web** 的**NetApp Console**時從電腦聯繫的端點

從 Web 瀏覽器存取控制台的電腦必須能夠聯絡多個端點。您需要使用控制台來設定控制台代理並進行控制台的日常使用。

"為NetApp控制台準備網絡" 。

從控制台代理聯繫的端點

控制台代理需要外部網路存取來聯繫以下端點，以管理公有雲環境中的資源和流程以進行日常操作。

下面列出的端點都是 CNAME 條目。

| 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.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。 |
| \ 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。<br><br>• 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。<br><br>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"。<br><br>• 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。 |

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"

步驟 **4**：設定控制台代理部署權限

您需要使用下列選項之一向控制台代理提供 Azure 權限：

- 選項 1：使用系統指派的託管識別為 Azure VM 指派自訂角色。
- 選項 2：向控制台代理程式提供具有所需權限的 Azure 服務主體的憑證。

依照步驟為控制台代理程式準備權限。

為控制台代理部署建立自訂角色

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"

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。

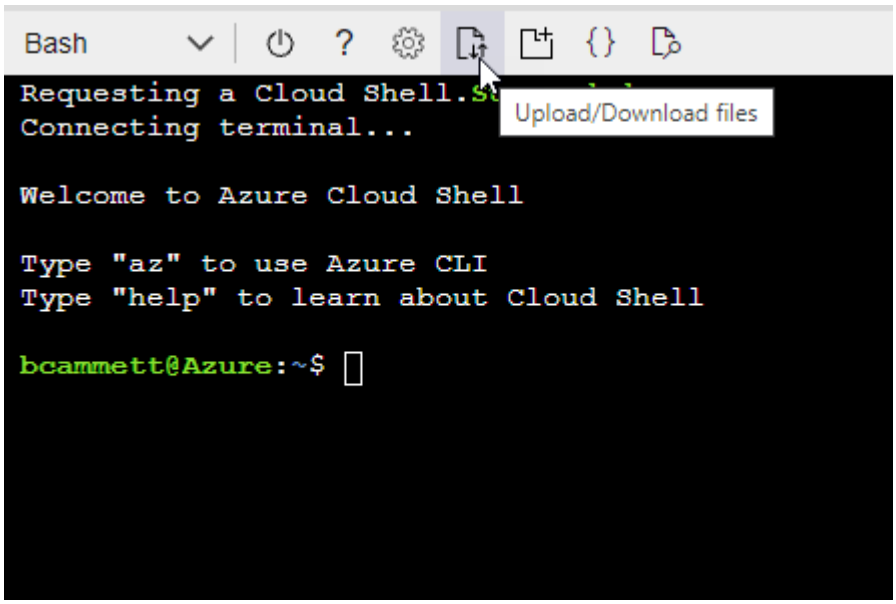
   例子

   ```
   "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
```

服務主體

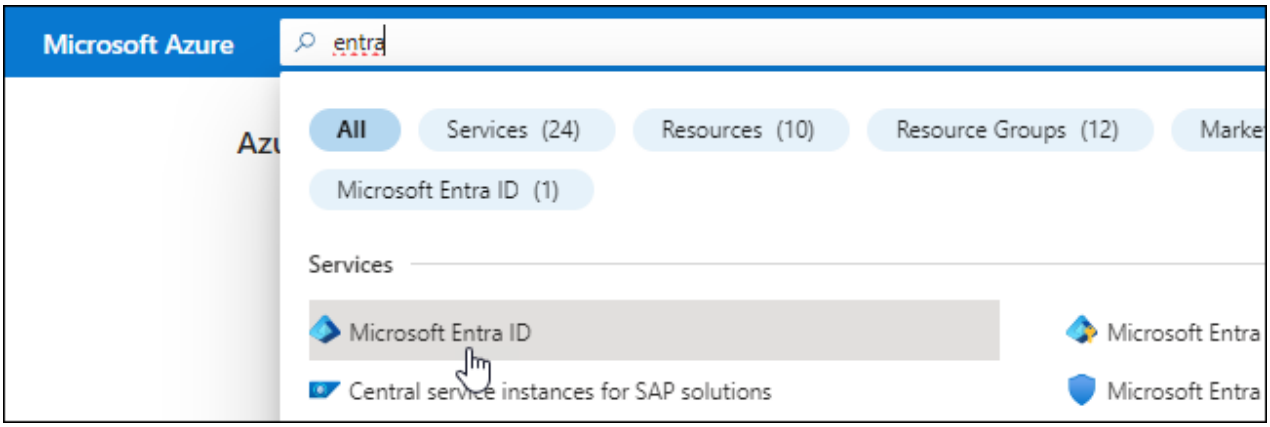
在 Microsoft Entra ID 中建立並設定服務主體，並取得控制台代理程式所需的 Azure 憑證。

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。

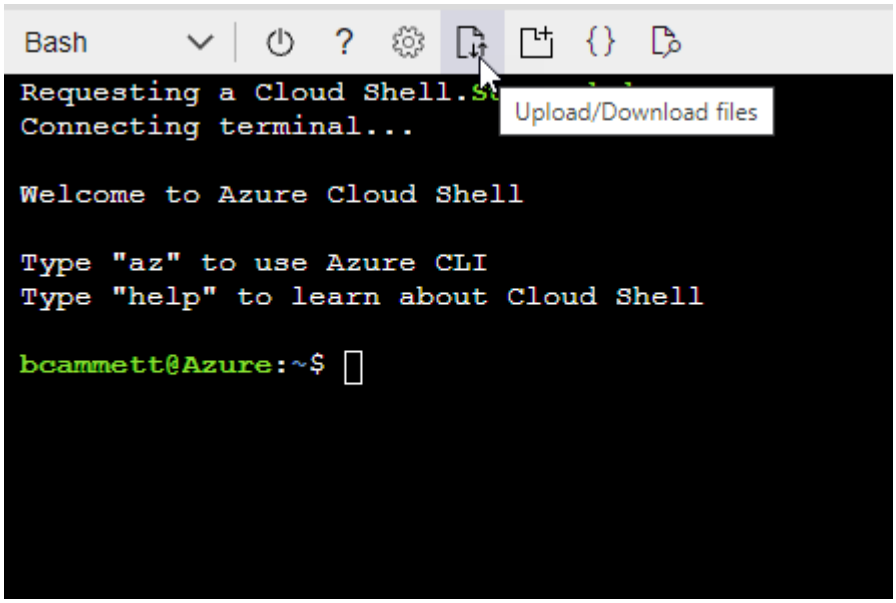
例子

```
"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。

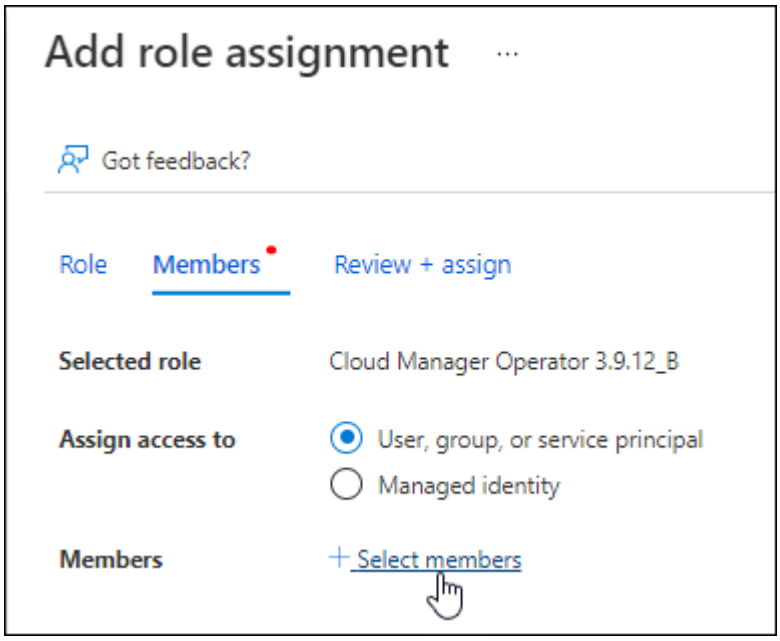
b. 選擇訂閱。

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*。

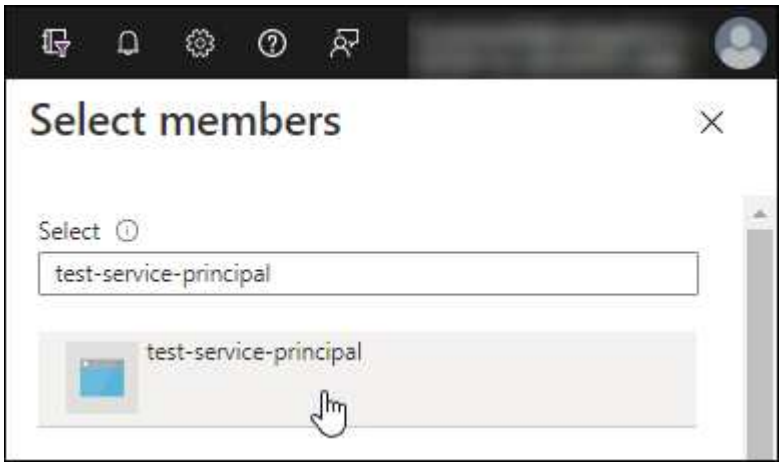
e. 在「成員」標籤中，完成以下步驟：

- 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”。

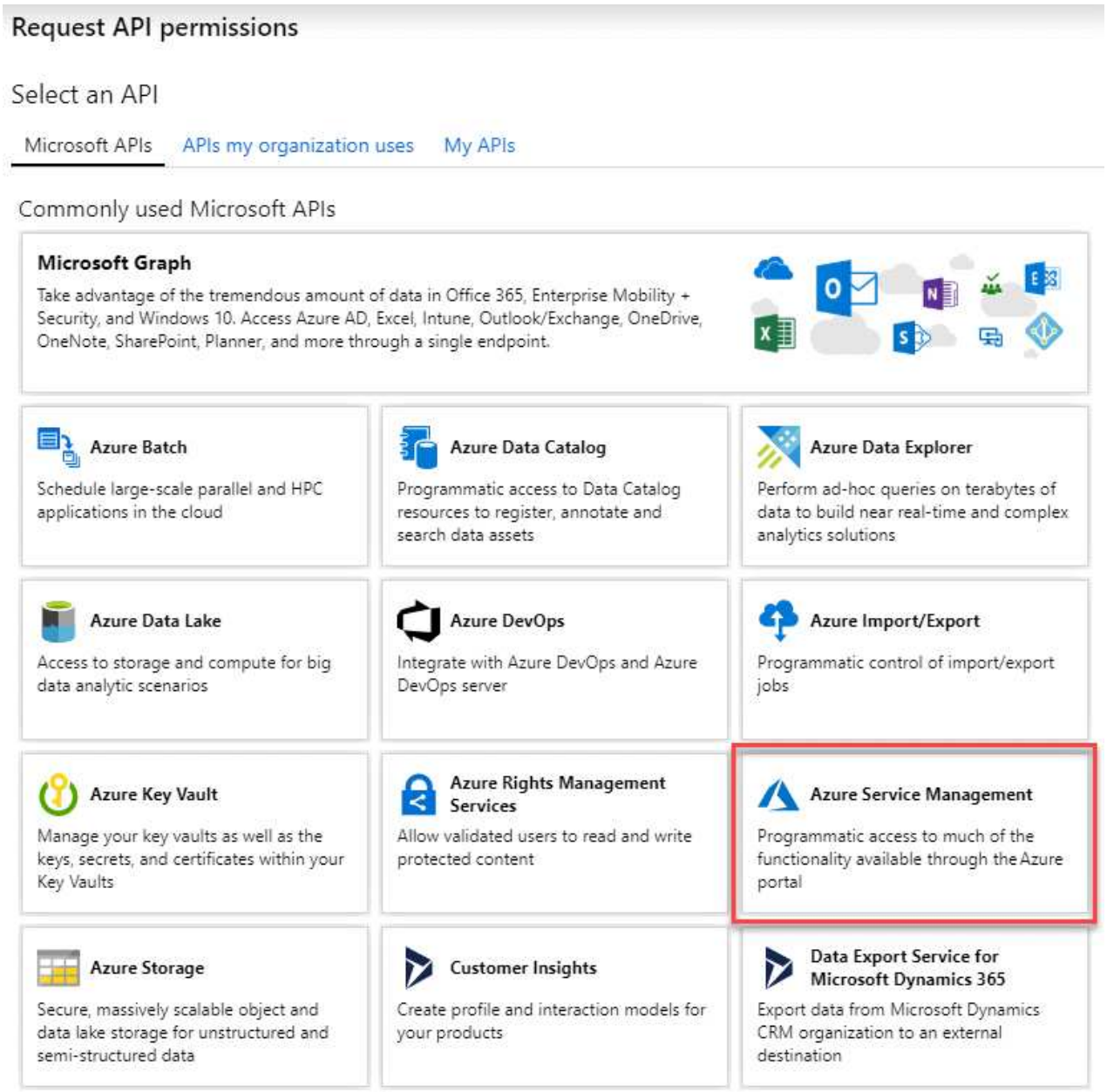
f. 選擇*審閱+分配*。

服務主體現在具有部署控制台代理程式所需的 Azure 權限。

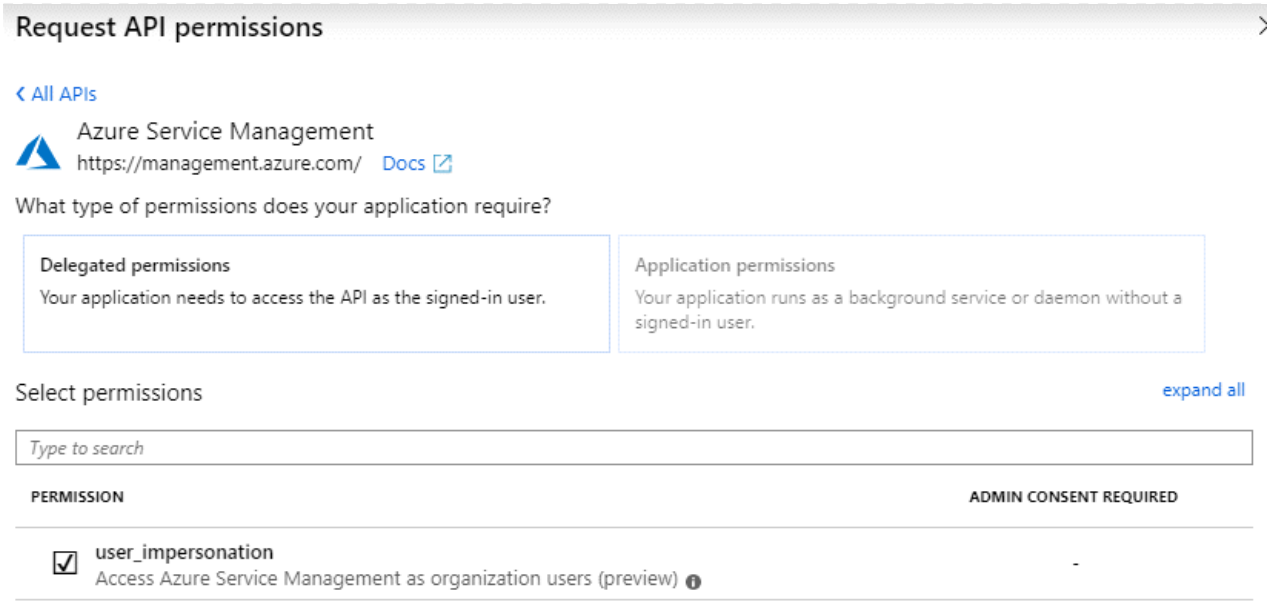
如果您想要從多個 Azure 訂閱部署Cloud Volumes ONTAP ，則必須將服務主體綁定到每個訂閱。在NetApp Console中，您可以選擇部署Cloud Volumes ONTAP時要使用的訂閱。

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」。

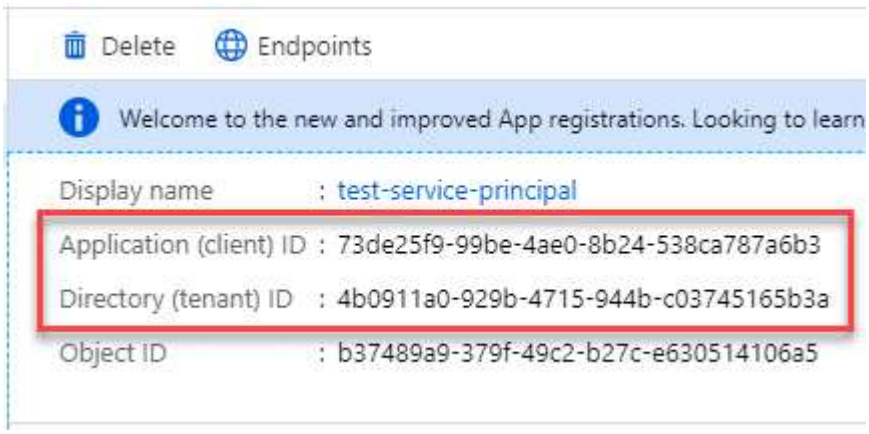



4. 選擇*以組織使用者身分存取 Azure 服務管理*，然後選擇*新增權限*。




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置，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。

步驟 **5**：安裝控制台代理

完成先決條件後，您可以在自己的 Linux 主機上手動安裝軟體。

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"。

- 在 Azure 中的 VM 上啟用託管標識，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"

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。

2. 等待安裝完成。

   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。

   如果安裝失敗，您可以查看安裝報告和日誌來協助您解決問題。"了解如何解決安裝問題。"

1. 從連接到控制台代理虛擬機器的主機開啟 Web 瀏覽器並輸入以下 URL：

   <a href="https://<em>ipaddress</em>" class="bare">https://<em>ipaddress</em></a>

2. 登入後，設定控制台代理：

   a. 指定與控制台代理程式關聯的組織。

   b. 輸入系統的名稱。

   c. 在*您是否在安全環境中運作？ *下保持限制模式為停用。

      您應該保持限制模式處於停用狀態，因為這些步驟描述如何在標準模式下使用控制台。只有當您擁有安全的環境並希望中斷此帳戶與後端服務的連線時，才應啟用受限模式。如果真是這樣的話，"依照步驟在受限模式下開始使用NetApp Console" 。

   d. 選擇*讓我們開始吧*。

如果您在建立控制台代理程式的相同 Azure 訂閱中擁有 Azure Blob 存儲，您將看到 Azure Blob 儲存系統自動出現在「系統」頁面上。 "了解如何透過NetApp Console管理 Azure Blob 儲存"

## 步驟 6：提供對NetApp Console的權限

現在您已經安裝了控制台代理，您需要為控制台代理提供您先前設定的 Azure 權限。提供權限使控制台能夠管理 Azure 中的資料和儲存基礎結構。

自訂角色

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。

下一步是什麼？

前往 "NetApp Console"開始使用控制台代理。

服務主體

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

控制台代理現在具有代表您在 Azure 中執行操作所需的權限。

## Google雲

### Google Cloud 中的控制台代理安裝選項

有幾種不同的方法可以在 Google Cloud 中建立控制台代理。直接從NetApp Console是最常見的方式。

有以下安裝選項可用：

- "直接從控制台建立控制台代理"（這是標準選項）

  此操作將在您選擇的 VPC 中啟動運行 Linux 和控制台代理軟體的 VM 執行個體。

- "使用 Google Platform 建立控制台代理"

  此操作也會啟動執行 Linux 和控制台代理軟體的 VM 實例，但部署直接從 Google Cloud 啟動，而不是從控制台啟動。

- "在您自己的Linux主機上下載並手動安裝軟體"

您選擇的安裝選項會影響您如何準備安裝。這包括如何向控制台提供驗證身分和管理 Google Cloud 中的資源所需的權限。

### 透過NetApp Console在 Google Cloud 中建立控制台代理

您可以從控制台在 Google Cloud 中建立控制台代理程式。您需要設定網路、準備 Google Cloud 權限、啟用 Google Cloud API，然後建立控制台代理。

開始之前

- 你應該有一個"了解控制台代理"。
- 你應該回顧一下"控制台代理限制"。

步驟 1：設定網絡

設定網路以確保控制台代理可以管理資源，並連接到目標網路和出站網路存取。

**VPC** 和子網

建立控制台代理程式時，您需要指定它所在的 VPC 和子網路。

連接到目標網絡

控制台代理程式需要與您計劃建立和管理系統的位置建立網路連線。例如，您計劃在本機環境中建立Cloud Volumes ONTAP系統或儲存系統的網路。

出站互聯網訪問

部署控制台代理程式的網路位置必須具有出站網路連線才能聯絡特定端點。

從控制台代理聯繫的端點

控制台代理需要外部網路存取來聯繫以下端點，以管理公有雲環境中的資源和流程以進行日常操作。

下面列出的端點都是 CNAME 條目。

| 端點 | 目的 |
| --- | --- |
| \ 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。 |
| \ 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。 |
| \ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io | 取得控制台代理升級的影像。<br><br>• 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。<br><br>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" 。<br><br>• 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。 |

從**NetApp**控制台聯繫的端點

當您使用透過 SaaS 層提供的基於 Web 的NetApp Console時，它會聯絡多個端點來完成資料管理任務。這包括從控制台聯繫以部署控制台代理的端點。

"查看從NetApp控制台聯繫的端點列表" 。

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"

建立控制台代理程式後實現此網路需求。

步驟 **2**：設定權限以建立控制台代理

在從控制台部署控制台代理程式之前，您需要為部署控制台代理程式 VM 的 Google 平台使用者設定權限。

步驟

1. 在 Google 平台中建立自訂角色：

   a. 建立包含以下權限的 YAML 檔案：

```
title: Console agent deployment policy
description: Permissions for the user who deploys the Console agent
stage: GA
includedPermissions:
```

```
- cloudbuild.builds.get
- 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
- config.deployments.create
- config.operations.get
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getState
- config.deployments.list
```

```
- config.deployments.update
- config.deployments.updateState
- config.previews.get
- config.previews.list
- config.revisions.get
- config.resources.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.actAs
- iam.serviceAccounts.create
- iam.serviceAccounts.list
- iam.serviceAccountKeys.create
- storage.buckets.create
- storage.buckets.get
- storage.objects.create
- storage.folders.create
- storage.objects.list
```

b. 從 Google Cloud 啟動雲殼。

c. 上傳包含所需權限的 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「agentDeployment」的角色：

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

"Google Cloud 文件：建立和管理自訂角色"

2. 將此自訂角色指派給將從控制台或使用 gcloud 部署控制台代理程式的使用者。

"Google Cloud 文件：授予單一角色"

步驟 **3**：建立 **Google Cloud** 服務帳戶以與代理程式一起使用。

需要一個 Google Cloud 服務帳號來向控制台代理提供控制台管理 Google Cloud 中的資源所需的權限。建立控制台代理程式時，您需要將此服務帳戶與控制台代理 VM 關聯。

在後續版本中新增權限時，您有責任更新自訂角色。如果需要新的權限，它們將在發行說明中列出。

步驟

1. 在 Google Cloud 中建立自訂角色：

   a. 建立一個包含以下內容的 YAML 文件"控制台代理程式的服務帳戶權限"。

   b. 從 Google Cloud 啟動雲殼。

   c. 上傳包含所需權限的 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 connector --project=myproject --file=agent.yaml
      ```

   "Google Cloud 文件：建立和管理自訂角色"

2. 在 Google Cloud 中建立服務帳號並將角色指派給該服務帳號：

   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"

3. 如果您打算在與控制台代理程式所在專案不同的專案中部署Cloud Volumes ONTAP系統，則需要為控制台代理程式的服務帳戶提供這些項目的存取權限。

   例如，假設控制台代理程式位於專案 1 中，而您想要在專案 2 中建立Cloud Volumes ONTAP系統。您需要授予項目 2 中的服務帳戶存取權限。

   a. 從 IAM 和管理服務中，選擇您想要建立Cloud Volumes ONTAP系統的 Google Cloud 專案。

   b. 在 **IAM** 頁面上，選擇 授予存取權限 並提供所需的詳細資訊。

      - 輸入控制台代理服務帳戶的電子郵件。
      - 選擇控制台代理程式的自訂角色。
      - 選擇*儲存*。

   有關詳細信息，請參閱 "Google Cloud 文件"

步驟 **4**：設定共享 **VPC** 權限

如果您使用共用 VPC 將資源部署到服務項目中，則需要準備好您的權限。

此表僅供參考，當 IAM 配置完成時，您的環境應該反映權限表。

查看共用 **VPC** 權限

| 身分 | 創造者 | 主辦地點 | 服務項目權限 | 宿主專案權限 | 目的 |
|---|---|---|---|---|---|
| Google 帳戶部署代理 | 風俗 | 服務項目 | "代理部署策略" | 計算.網路用戶 | 在服務項目中部署代理 |
| 代理服務帳戶 | 風俗 | 服務項目 | "代理服務帳號策略" | 計算.網路使用者<br>部署管理員.編輯器 | 部署和維護服務項目中的Cloud Volumes ONTAP和服務 |
| Cloud Volumes ONTAP 服務帳戶 | 風俗 | 服務項目 | storage.admin 成員： NetApp Console服務帳號作為 serviceAccount.user | 不適用 | （選購）適用於NetApp Cloud Tiering和NetApp Backup and Recovery |
| Google API 服務代理 | Google 雲 | 服務項目 | （預設）編輯器 | 計算.網路用戶 | 代表部署與 Google Cloud API 互動。允許控制台使用共用網路。 |
| Google Compute Engine 預設服務帳戶 | Google 雲 | 服務項目 | （預設）編輯器 | 計算.網路用戶 | 代表部署部署 Google Cloud 執行個體和運算基礎架構。允許控制台使用共用網路。 |

筆記：

1. 如果您沒有將防火牆規則傳遞給部署並選擇讓控制台為您建立規則，則僅主機專案才需要 deploymentmanager.editor。如果未指定規則， NetApp Console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給部署並選擇讓控制台為您建立它們時，才需要firewall.create 和firewall.delete。這些權限位於控制台帳戶 .yaml 檔案中。如果您使用共用 VPC 部署 HA 對，這些權限將用於為 VPC1、2 和 3 建立防火牆規則。對於所有其他部署，這些權限也將用於為 VPC0 建立規則。
3. 對於 Cloud Tiering，分層服務帳戶必須在服務帳戶上具有 serviceAccount.user 角色，而不僅僅是在專案層級。目前，如果您在專案層級指派 serviceAccount.user，則使用 getIAMPolicy 查詢服務帳號時不會顯示權限。

步驟 **5**：啟用 **Google Cloud API**

在部署控制台代理程式和Cloud Volumes ONTAP之前，您必須啟用多個 Google Cloud 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）

"Google Cloud 文件：啟用 API"

步驟 **6**：建立控制台代理

直接從控制台建立控制台代理。

建立控制台代理程式會使用預設配置在 Google Cloud 中部署虛擬機器執行個體。建立控制台代理程式後，請勿切換到具有較少 CPU 或較少 RAM 的較小 VM 執行個體。"了解控制台代理的預設配置"。

在 Google Cloud 中部署代理程式時，代理程式會建立一個儲存桶來儲存部署文件。

開始之前

您應該具有以下內容：

- 建立控制台代理程式所需的 Google Cloud 權限以及控制台代理虛擬機器的服務帳號。
- 滿足組網需求的VPC及子網路。
- 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。

步驟

1. 選擇“管理 **>** 代理”。
2. 在“概覽”頁面上，選擇“部署代理”>“Google Cloud”
3. 在*部署代理*頁面上，查看您需要的詳細資訊。您有兩個選擇：
   a. 選擇“繼續”以使用產品內指南準備部署。產品內指南中的每個步驟都包含文件此頁面上的資訊。
   b. 如果您已按照此頁面上的步驟做好準備，請選擇「跳至部署」。
4. 依照精靈中的步驟建立控制台代理：
   - 如果出現提示，請登入您的 Google 帳戶，該帳戶應該具有建立虛擬機器實例所需的權限。

     該表單由 Google 擁有並託管。您的憑證未提供給NetApp。
   - 詳細資訊：輸入虛擬機器實例的名稱，指定標籤，選擇項目，然後選擇具有所需權限的服務帳戶（有關詳細信息，請參閱上面的部分）。

- 位置：指定實例的區域、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代理程式配置。
- 網路標籤：如果使用透明代理，則向控制台代理實例新增網路標籤。網路標籤必須以小寫字母開頭，並且可以包含小寫字母、數字和連字號。標籤必須以小寫字母或數字結尾。例如，您可以使用標籤“console-agent-proxy”。
- 防火牆策略：選擇是否建立新的防火牆策略，或是否選擇允許所需入站和出站規則的現有防火牆策略。

  "Google Cloud 中的防火牆規則"

5. 檢查您的選擇以驗證您的設定是否正確。

   a. 預設情況下，*驗證代理程式設定*複選框處於選取狀態，以便控制台在您部署時驗證網路連線要求。如果控制台無法部署代理，它會提供一份報告來幫助您排除故障。如果部署成功，則不會提供報告。

   如果您仍在使用"先前的端點"用於代理升級，驗證失敗並出現錯誤。為了避免這種情況，請取消選取核取方塊以跳過驗證檢查。

6. 選擇“新增”。

   代理大約需要 10 分鐘才能準備就緒；請停留在頁面上直到過程完成。

結果

過程完成後，控制台代理即可使用。

如果部署失敗，您可以從控制台下載報告和日誌來幫助您解決問題。"了解如何解決安裝問題。"

如果您在建立控制台代理程式的相同 Google Cloud 帳戶中擁有 Google Cloud Storage 儲存桶，您將看到 Google Cloud Storage 系統自動出現在 **Systems** 頁面上。 "了解如何透過控制台管理 Google 雲端存儲"

從 **Google Cloud** 建立控制台代理

## 若要使用 Google Cloud 在 Google Cloud 中建立控制台代理，您需要設定網路、準備 Google Cloud 權限、啟用 Google Cloud API，然後建立控制台代理。

開始之前

- 你應該有一個"了解控制台代理"。
- 你應該回顧一下"控制台代理限制"。

步驟 **1**：設定網絡

設定網路以使控制台代理程式能夠管理資源並連接到目標網路和網際網路。

**VPC** 和子網

建立控制台代理程式時，您需要指定它所在的 VPC 和子網路。

連接到目標網絡

控制台代理程式需要與您計劃建立和管理系統的位置建立網路連線。例如，您計劃在本機環境中建立Cloud Volumes ONTAP系統或儲存系統的網路。

出站互聯網訪問

部署控制台代理程式的網路位置必須具有出站網路連線才能聯絡特定端點。

從控制台代理聯繫的端點

控制台代理需要外部網路存取來聯繫以下端點，以管理公有雲環境中的資源和流程以進行日常操作。

下面列出的端點都是 CNAME 條目。

| 端點 | 目的 |
| --- | --- |
| \ 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。 |
| \ 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。<br><br>• 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。<br><br>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"。<br><br>• 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。 |

從**NetApp**控制台聯繫的端點

當您使用透過 SaaS 層提供的基於 Web 的NetApp Console時，它會聯絡多個端點來完成資料管理任務。這包括從控制台聯繫以部署控制台代理的端點。

"查看從NetApp控制台聯繫的端點列表"。

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"

建立控制台代理程式後實現此網路需求。

步驟 **2**：設定權限以建立控制台代理

為 Google Cloud 使用者設定權限以從 Google Cloud 部署控制台代理虛擬機器。

步驟

1. 在 Google 平台中建立自訂角色：

    a. 建立包含以下權限的 YAML 檔案：

```
title: Console agent deployment policy
description: Permissions for the user who deploys the Console
agent
stage: GA
includedPermissions:

- cloudbuild.builds.get
- 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
- config.deployments.create
```

```
- config.operations.get
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getState
- config.deployments.list
- config.deployments.update
- config.deployments.updateState
- config.previews.get
- config.previews.list
- config.revisions.get
- config.resources.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.actAs
- iam.serviceAccounts.create
- iam.serviceAccounts.list
- iam.serviceAccountKeys.create
- storage.buckets.create
- storage.buckets.get
- storage.objects.create
- storage.folders.create
- storage.objects.list
```

b. 從 Google Cloud 啟動雲殼。

c. 上傳包含所需權限的 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「connectorDeployment」的角色：

gcloud iam 角色建立 connectorDeployment --project=myproject --file=connector-deployment.yaml

"Google Cloud 文件：建立和管理自訂角色"

2. 將此自訂角色指派給從 Google Cloud 部署控制台代理程式的使用者。

"Google Cloud 文件：授予單一角色"

步驟 **3**：設定控制台代理操作的權限

需要一個 Google Cloud 服務帳號來向控制台代理提供控制台管理 Google Cloud 中的資源所需的權限。建立控制台代理程式時，您需要將此服務帳戶與控制台代理 VM 關聯。

在後續版本中新增權限時，您有責任更新自訂角色。如果需要新的權限，它們將在發行說明中列出。

步驟

1. 在 Google Cloud 中建立自訂角色：

   a. 建立一個包含以下內容的 YAML 文件"控制台代理程式的服務帳戶權限"。

   b. 從 Google Cloud 啟動雲殼。

   c. 上傳包含所需權限的 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 connector --project=myproject --file=agent.yaml
   ```

   "Google Cloud 文件：建立和管理自訂角色"

2. 在 Google Cloud 中建立服務帳號並將角色指派給該服務帳號：

   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"

3. 如果您打算在與控制台代理程式所在專案不同的專案中部署Cloud Volumes ONTAP系統，則需要為控制台代理程式的服務帳戶提供這些項目的存取權限。

   例如，假設控制台代理程式位於專案 1 中，而您想要在專案 2 中建立Cloud Volumes ONTAP系統。您需要授予項目 2 中的服務帳戶存取權限。

   a. 從 IAM 和管理服務中，選擇您想要建立Cloud Volumes ONTAP系統的 Google Cloud 專案。

   b. 在 **IAM** 頁面上，選擇 授予存取權限 並提供所需的詳細資訊。

- 輸入控制台代理服務帳戶的電子郵件。
- 選擇控制台代理程式的自訂角色。
- 選擇*儲存*。

有關詳細信息，請參閱 "Google Cloud 文件"

步驟 **4**：設定共享 **VPC** 權限

如果您使用共用 VPC 將資源部署到服務項目中，則需要準備好您的權限。

此表僅供參考，當 IAM 配置完成時，您的環境應該反映權限表。

查看共用 **VPC** 權限

| 身分 | 創造者 | 主辦地點 | 服務項目權限 | 宿主專案權限 | 目的 |
|---|---|---|---|---|---|
| Google 帳戶部署代理 | 風俗 | 服務項目 | "代理部署策略" | 計算.網路用戶 | 在服務項目中部署代理 |
| 代理服務帳戶 | 風俗 | 服務項目 | "代理服務帳號策略" | 計算.網路使用者<br>部署管理員.編輯器 | 部署和維護服務項目中的Cloud Volumes ONTAP和服務 |
| Cloud Volumes ONTAP 服務帳戶 | 風俗 | 服務項目 | storage.admin 成員： NetApp Console服務帳號作為 serviceAccount.user | 不適用 | （選購）適用於NetApp Cloud Tiering和NetApp Backup and Recovery |
| Google API 服務代理 | Google 雲 | 服務項目 | （預設）編輯器 | 計算.網路用戶 | 代表部署與 Google Cloud API 互動。允許控制台使用共用網路。 |
| Google Compute Engine 預設服務帳戶 | Google 雲 | 服務項目 | （預設）編輯器 | 計算.網路用戶 | 代表部署部署 Google Cloud 執行個體和運算基礎架構。允許控制台使用共用網路。 |

筆記：

1. 如果您沒有將防火牆規則傳遞給部署並選擇讓控制台為您建立規則，則僅主機專案才需要 deploymentmanager.editor。如果未指定規則， NetApp Console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給部署並選擇讓控制台為您建立它們時，才需要firewall.create 和firewall.delete。這些權限位於控制台帳戶 .yaml 檔案中。如果您使用共用 VPC 部署 HA 對，這些權限將用於為 VPC1、2 和 3 建立防火牆規則。對於所有其他部署，這些權限也將用於為 VPC0 建立規則。
3. 對於 Cloud Tiering，分層服務帳戶必須在服務帳戶上具有 serviceAccount.user 角色，而不僅僅是在專案層級。目前，如果您在專案層級指派 serviceAccount.user，則使用 getIAMPolicy 查詢服務帳號時不會顯示權限。

### 步驟 **5**：啟用 **Google Cloud API**

在部署控制台代理程式和Cloud Volumes ONTAP之前，先啟用多個 Google Cloud 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）

"Google Cloud 文件：啟用 API"

步驟 **6**：建立控制台代理

使用 Google Cloud 建立控制台代理程式。

建立控制台代理程式會使用預設配置在 Google Cloud 中部署虛擬機器執行個體。建立控制台代理程式後，請勿切換到具有較少 CPU 或較少 RAM 的較小 VM 執行個體。"了解控制台代理的預設配置" 。

開始之前

您應該具有以下內容：

- 建立控制台代理程式所需的 Google Cloud 權限以及控制台代理虛擬機器的服務帳號。
- 滿足組網需求的VPC及子網路。
- 了解 VM 實例要求。
  - **CPU**：8 核心或 8 個 vCPU
  - 記憶體：32 GB
  - 機器類型：我們推薦 n2-standard-8。

    Google Cloud 在具有支援 Shielded VM 功能的作業系統的 VM 執行個體上支援控制台代理。

步驟

1. 使用您喜歡的方法登入 Google Cloud SDK。

   此範例使用安裝了 gcloud SDK 的本機 shell，但您也可以使用 Google Cloud Shell。

   有關 Google Cloud SDK 的更多信息，請訪問"Google Cloud SDK 文件頁面"。

2. 驗證您是否以具有上述部分定義的所需權限的使用者身分登入：

   ```
   gcloud auth list
   ```

   輸出應顯示以下內容，其中 * 使用者帳戶是要登入的使用者帳戶：

```
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. 運行 `gcloud compute instances create`命令：

```
gcloud compute instances create <instance-name>
  --machine-type=n2-standard-8
  --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>
```

實例名稱
: VM 實例所需的實例名稱。

專案
: （可選）您想要部署虛擬機器的專案。

服務帳戶
: 步驟 2 的輸出中指定的服務帳戶。

區
: 您想要部署虛擬機器的區域

無地址
: （可選）不使用外部 IP 位址（您需要雲端 NAT 或代理將流量路由到公用網際網路）

網路標籤
: （可選）新增網路標記，使用標記將防火牆規則連結到控制台代理實例

網路路徑

（可選）新增要部署控制台代理程式的網路名稱（對於共用 VPC，您需要完整路徑）

子網路路徑

（可選）新增要部署控制台代理程式的子網路名稱（對於共用 VPC，您需要完整路徑）

**kms** 金鑰路徑

（可選）新增 KMS 金鑰來加密控制台代理的磁碟（還需要套用 IAM 權限）

有關這些標誌的更多信息，請訪問"Google Cloud 運算 SDK 文件"。

運行該命令將部署控制台代理程式。控制台代理實例和軟體應在大約五分鐘內運行。

4. 開啟 Web 瀏覽器並輸入控制台代理主機 URL：

   控制台主機 URL 可以是本機主機、私人 IP 位址或公用 IP 位址，取決於主機的配置。例如，如果控制台代理程式位於沒有公用 IP 位址的公有雲中，則必須輸入與控制台代理主機有連接的主機的私人 IP 位址。

5. 登入後，設定控制台代理：

   a. 指定與控制台代理程式關聯的控制台組織。

      "了解身分和存取管理" 。

   b. 輸入系統的名稱。

結果

控制台代理現在已安裝並設定到您的控制台組織。

開啟 Web 瀏覽器並前往 "NetApp Console"開始使用控制台代理。

#### 在 **Google Cloud** 中手動安裝控制台代理

## 要在您自己的 Linux 主機上手動安裝控制台代理，您需要查看主機要求、設定網路、準備 Google Cloud 權限、啟用 Google Cloud API、安裝控制台，然後提供您準備好的權限。

開始之前

- 你應該有一個"了解控制台代理"。
- 你應該回顧一下"控制台代理限制"。

步驟 **1**：查看主機需求

控制台代理軟體必須在滿足特定作業系統要求、RAM 要求、連接埠要求等的主機上執行。

控制台代理保留 19000 到 19200 的 UID 和 GID 範圍。這個範圍是固定的，不能修改。如果主機上的任何第三方軟體使用此範圍內的 UID 或 GID，則代理安裝將會失敗。 NetApp建議使用沒有第三方軟體的主機以避免衝突。

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。

**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<br>• 僅限英文版本。<br>• 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。<br>查看 Podman 設定要求 。 |

| 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** |
| --- | --- | --- | --- | --- |
| 在強制模式或寬容模式下受支持 | | 9.1 至 9.4<br>• 僅限英文版本。<br>• 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。<br>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<br>• 僅限英文版本。<br>• 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。<br>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 |

**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"

步驟 **2**：安裝 **Podman** 或 **Docker Engine**

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 3. 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 **3**：設定網絡

設定您的網絡，以便控制台代理可以管理混合雲環境中的資源和流程。例如，您需要確保可以連接到目標網路並且可以進行外部網路存取。

連接到目標網絡

控制台代理程式需要與您計劃建立和管理系統的位置建立網路連線。例如，您計劃在本機環境中建立Cloud Volumes ONTAP系統或儲存系統的網路。

出站互聯網訪問

部署控制台代理程式的網路位置必須具有出站網路連線才能聯絡特定端點。

使用基於 **Web** 的**NetApp Console**時從電腦聯繫的端點

從 Web 瀏覽器存取控制台的電腦必須能夠聯絡多個端點。您需要使用控制台來設定控制台代理並進行控制台的日常使用。

"為NetApp控制台準備網絡" 。

從控制台代理聯繫的端點

控制台代理需要外部網路存取來聯繫以下端點，以管理公有雲環境中的資源和流程以進行日常操作。

下面列出的端點都是 CNAME 條目。

| 端點 | 目的 |
| --- | --- |
| \ 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。 |
| \ 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。<br><br>• 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。<br><br>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"。<br><br>• 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。 |

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"

步驟 **4**：設定控制台代理的權限

需要一個 Google Cloud 服務帳號來向控制台代理提供控制台管理 Google Cloud 中的資源所需的權限。建立控制台代理程式時，您需要將此服務帳戶與控制台代理 VM 關聯。

在後續版本中新增權限時，您有責任更新自訂角色。如果需要新的權限，它們將在發行說明中列出。

步驟

1. 在 Google Cloud 中建立自訂角色：

   a. 建立一個包含以下內容的 YAML 文件"控制台代理程式的服務帳戶權限"。

   b. 從 Google Cloud 啟動雲殼。

   c. 上傳包含所需權限的 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 connector --project=myproject --file=agent.yaml
      ```

   "Google Cloud 文件：建立和管理自訂角色"

2. 在 Google Cloud 中建立服務帳號並將角色指派給該服務帳號：

   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"

3. 如果您打算在與控制台代理程式所在專案不同的專案中部署Cloud Volumes ONTAP系統，則需要為控制台代理程式的服務帳戶提供這些項目的存取權限。

   例如，假設控制台代理程式位於專案 1 中，而您想要在專案 2 中建立Cloud Volumes ONTAP系統。您需要授予項目 2 中的服務帳戶存取權限。

   a. 從 IAM 和管理服務中，選擇您想要建立Cloud Volumes ONTAP系統的 Google Cloud 專案。

   b. 在 **IAM** 頁面上，選擇 授予存取權限 並提供所需的詳細資訊。

      - 輸入控制台代理服務帳戶的電子郵件。
      - 選擇控制台代理程式的自訂角色。
      - 選擇*儲存*。

   有關詳細信息，請參閱 "Google Cloud 文件"

步驟 **5**：設定共享 **VPC** 權限

如果您使用共用 VPC 將資源部署到服務項目中，則需要準備好您的權限。

此表僅供參考，當 IAM 配置完成時，您的環境應該反映權限表。

查看共用 **VPC** 權限

| 身分 | 創造者 | 主辦地點 | 服務項目權限 | 宿主專案權限 | 目的 |
|---|---|---|---|---|---|
| Google 帳戶部署代理 | 風俗 | 服務項目 | "代理部署策略" | 計算.網路用戶 | 在服務項目中部署代理 |
| 代理服務帳戶 | 風俗 | 服務項目 | "代理服務帳號策略" | 計算.網路使用者<br>部署管理員.編輯器 | 部署和維護服務項目中的Cloud Volumes ONTAP和服務 |
| Cloud Volumes ONTAP 服務帳戶 | 風俗 | 服務項目 | storage.admin 成員： NetApp Console服務帳號作為 serviceAccount.user | 不適用 | （選購）適用於NetApp Cloud Tiering和NetApp Backup and Recovery |
| Google API 服務代理 | Google 雲 | 服務項目 | （預設）編輯器 | 計算.網路用戶 | 代表部署與 Google Cloud API 互動。允許控制台使用共用網路。 |
| Google Compute Engine 預設服務帳戶 | Google 雲 | 服務項目 | （預設）編輯器 | 計算.網路用戶 | 代表部署部署 Google Cloud 執行個體和運算基礎架構。允許控制台使用共用網路。 |

筆記：

1. 如果您沒有將防火牆規則傳遞給部署並選擇讓控制台為您建立規則，則僅主機專案才需要 deploymentmanager.editor。如果未指定規則， NetApp Console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給部署並選擇讓控制台為您建立它們時，才需要firewall.create 和firewall.delete。這些權限位於控制台帳戶 .yaml 檔案中。如果您使用共用 VPC 部署 HA 對，這些權限將用於為 VPC1、2 和 3 建立防火牆規則。對於所有其他部署，這些權限也將用於為 VPC0 建立規則。
3. 對於 Cloud Tiering，分層服務帳戶必須在服務帳戶上具有 serviceAccount.user 角色，而不僅僅是在專案層級。目前，如果您在專案層級指派 serviceAccount.user，則使用 getIAMPolicy 查詢服務帳號時不會顯示權限。

## 第 **6** 步：啟用 **Google Cloud API**

在 Google Cloud 中部署控制台代理程式之前，必須啟用多個 Google Cloud 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）

"Google Cloud 文件：啟用 API"

步驟 **7**：安裝控制台代理

完成先決條件後，您可以在自己的 Linux 主機上手動安裝軟體。

部署代理程式時，系統也會建立一個 Google Cloud 儲存桶來儲存部署檔案。

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"。

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。

2. 等待安裝完成。

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。

如果安裝失敗，您可以查看安裝報告和日誌來協助您解決問題。"了解如何解決安裝問題。"

1. 從連接到控制台代理虛擬機器的主機開啟 Web 瀏覽器並輸入以下 URL：

<a href="https://<em>ipaddress</em>" class="bare">https://<em>ipaddress</em></a>

2. 登入後，設定控制台代理：

a. 指定與控制台代理程式關聯的組織。

b. 輸入系統的名稱。

c. 在*您是否在安全環境中運作？ *下保持限制模式為停用。

您應該保持限制模式處於停用狀態，因為這些步驟描述如何在標準模式下使用控制台。只有當您擁有安全的環境並希望中斷此帳戶與後端服務的連線時，才應啟用受限模式。如果真是這樣的話，"依照步驟在受限模式下開始使用NetApp Console" 。

d. 選擇*讓我們開始吧*。

如果安裝失敗，您可以查看日誌和報告來幫助您排除故障。"了解如何解決安裝問題。"

如果您在建立控制台代理程式的相同 Google Cloud 帳戶中擁有 Google Cloud Storage 儲存桶，您將看到 Google Cloud Storage 系統自動出現在 **Systems** 頁面上。 "了解如何透過NetApp Console管理 Google Cloud Storage"

步驟 8：向控制台代理提供權限

您需要向控制台代理提供您先前設定的 Google Cloud 權限。提供權限可使控制台代理程式管理 Google Cloud 中的資料和儲存基礎架構。

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 Google Cloud 專案中的資源，請透過將具有控制台代理角色的服務帳號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。

在本地安裝代理

在本機手動安裝控制台代理

# 在本地安裝控制台代理，然後登入並設定它以與您的控制台組織協同工作。

如果您是 VMWare 用戶，您可以使用 OVA 在您的 VCenter 中安裝控制台代理程式。"了解有關在 VCenter 中安裝代理程式的更多資訊。"

在安裝之前，您需要確保您的主機（VM 或 Linux 主機）符合要求，並確保控制台代理可以存取網際網路以及目標網路。如果您打算使用NetApp資料服務或Cloud Volumes ONTAP），則需要在雲端提供者中建立憑證以新增至控制台，以便控制台代理可以代表您在雲端執行操作。

準備安裝控制台代理

在安裝控制台代理之前，您應該確保您擁有一台符合安裝要求的主機。您還需要與網路管理員合作，以確保控制台代理程式具有所需端點的出站存取權限以及與目標網路的連線。

查看控制台代理主機需求

在符合作業系統、RAM 和連接埠要求的 x86 主機上執行控制台代理。在安裝控制台代理之前，請確保您的主機符合這些要求。

控制台代理保留 19000 到 19200 的 UID 和 GID 範圍。這個範圍是固定的，不能修改。如果主機上的任何第三方軟體使用此範圍內的 UID 或 GID，則代理安裝將會失敗。 NetApp建議使用沒有第三方軟體的主機以避免衝突。

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。

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<br>• 僅限英文版本。<br>• 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。<br>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<br>• 僅限英文版本。<br>• 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。<br>查看 Podman 設定要求 。 |

| 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** |
| --- | --- | --- | --- | --- |
| 在強制模式或寬容模式下受支持 | | 8.6 至 8.10<br>• 僅限英文版本。<br>• 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。<br>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 |

為控制台代理設定網路訪問

設定網路存取以確保控制台代理可以管理資源。它需要連接到目標網路並存取特定端點的出站互聯網。

連接到目標網絡

控制台代理程式需要與您計劃建立和管理系統的位置建立網路連線。例如，您計劃在本機環境中建立Cloud Volumes ONTAP系統或儲存系統的網路。

出站互聯網訪問

部署控制台代理程式的網路位置必須具有出站網路連線才能聯絡特定端點。

使用基於 **Web** 的**NetApp Console**時從電腦聯繫的端點

從 Web 瀏覽器存取控制台的電腦必須能夠聯絡多個端點。您需要使用控制台來設定控制台代理並進行控制台的日常使用。

"為NetApp控制台準備網絡" 。

從控制台代理聯繫的端點

控制台代理需要外部網路存取來聯繫以下端點，以管理公有雲環境中的資源和流程以進行日常操作。

下面列出的端點都是 CNAME 條目。

安裝在您場所的控制台代理無法管理 Google Cloud 中的資源。如果您想管理 Google Cloud 資源，則需要在 Google Cloud 中安裝代理程式。

**AWS**

當控制台代理程式安裝在本機時，它需要對以下 AWS 端點進行網路訪問，以便管理部署在 AWS 中的NetApp系統（例如Cloud Volumes ONTAP）。

從控制台代理聯繫的端點

控制台代理需要外部網路存取來聯繫以下端點，以管理公有雲環境中的資源和流程以進行日常操作。

下面列出的端點都是 CNAME 條目。

| 端點 | 目的 |
| --- | --- |
| AWS 服務（amazonaws.com）：<br>• 雲形成<br>• 彈性運算雲（EC2）<br>• 身分和存取管理 (IAM)<br>• 金鑰管理服務（KMS）<br>• 安全性令牌服務 (STS)<br>• 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：<br>• 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。 |
| \ 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。<br><br>• 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。<br><br>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"。<br><br>• 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**

當控制台代理程式安裝在本機時，它需要對以下 Azure 端點進行網路訪問，以便管理部署在 Azure 中的NetApp系統（例如Cloud Volumes ONTAP）。

| 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.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。 |
| \ 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。<br><br>• 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。<br><br>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"。<br><br>• 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。 |

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"

## 為 **AWS** 或 **Azure** 建立控制台代理雲端權限

如果您想透過本機控制台代理程式使用 AWS 或 Azure 中的NetApp資料服務，則需要在雲端提供者中設定權限，然後在安裝控制台代理程式後將憑證新增至控制台代理程式。

您必須在 Google Cloud 中安裝控制台代理程式來管理駐留在那裡的任何資源。

**AWS**

當控制台代理程式安裝在本機時，您需要透過為具有所需權限的 IAM 使用者新增存取金鑰來為控制台提供 AWS 權限。

如果控制台代理程式安裝在本機，則必須使用此驗證方法。您不能使用 IAM 角色。

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。

結果

您現在應該擁有具有所需權限的 IAM 使用者的存取金鑰。安裝控制台代理程式後，從控制台將這些憑證與控制台代理程式關聯。

**Azure**

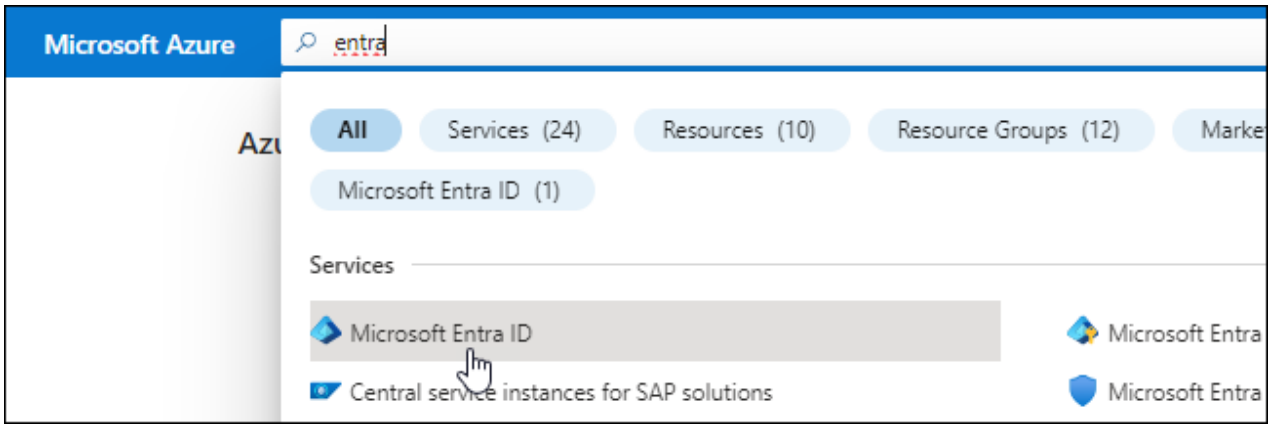
當控制台代理程式安裝在本機時，您需要透過在 Microsoft Entra ID 中設定服務主體並取得控制台代理程式所需的 Azure 憑證來為控制台代理程式提供 Azure 權限。

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。

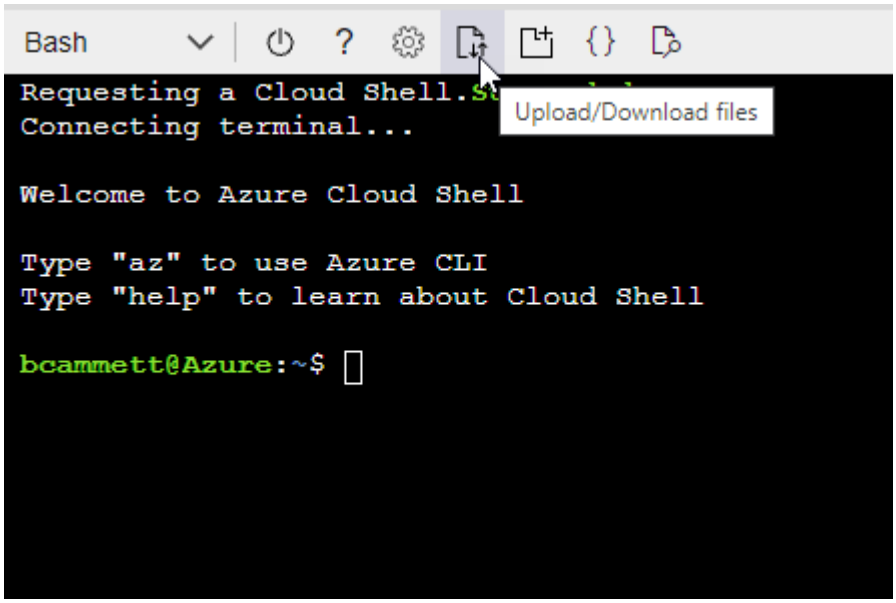
      例子

      ```
      "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：

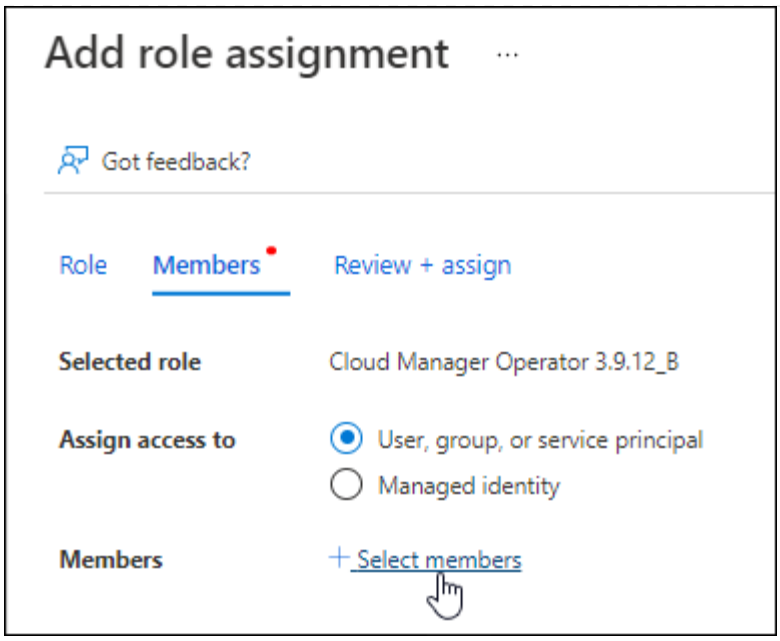
```
az role definition create --role-definition agent_Policy.json
```

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：

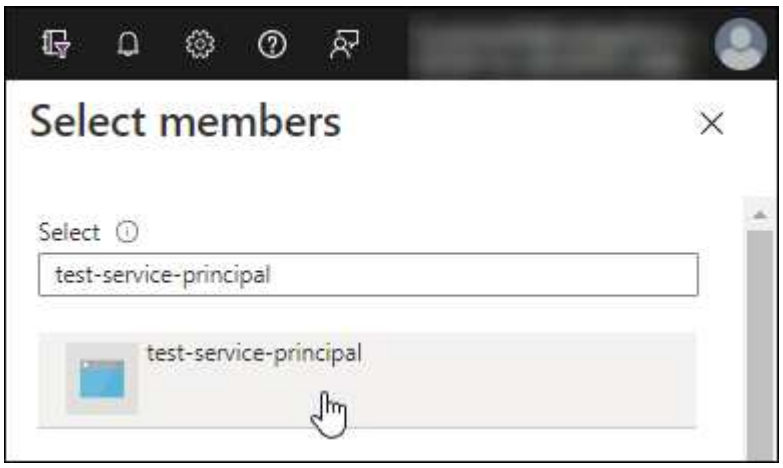
a. 從 Azure 入口網站開啟 **Subscriptions** 服務。
b. 選擇訂閱。
c. 選擇“存取控制 (IAM)”>“新增”>“新增角色分配”。
d. 在*角色*標籤中，選擇*控制台操作員*角色並選擇*下一步*。
e. 在「成員」標籤中，完成以下步驟：

- 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”。

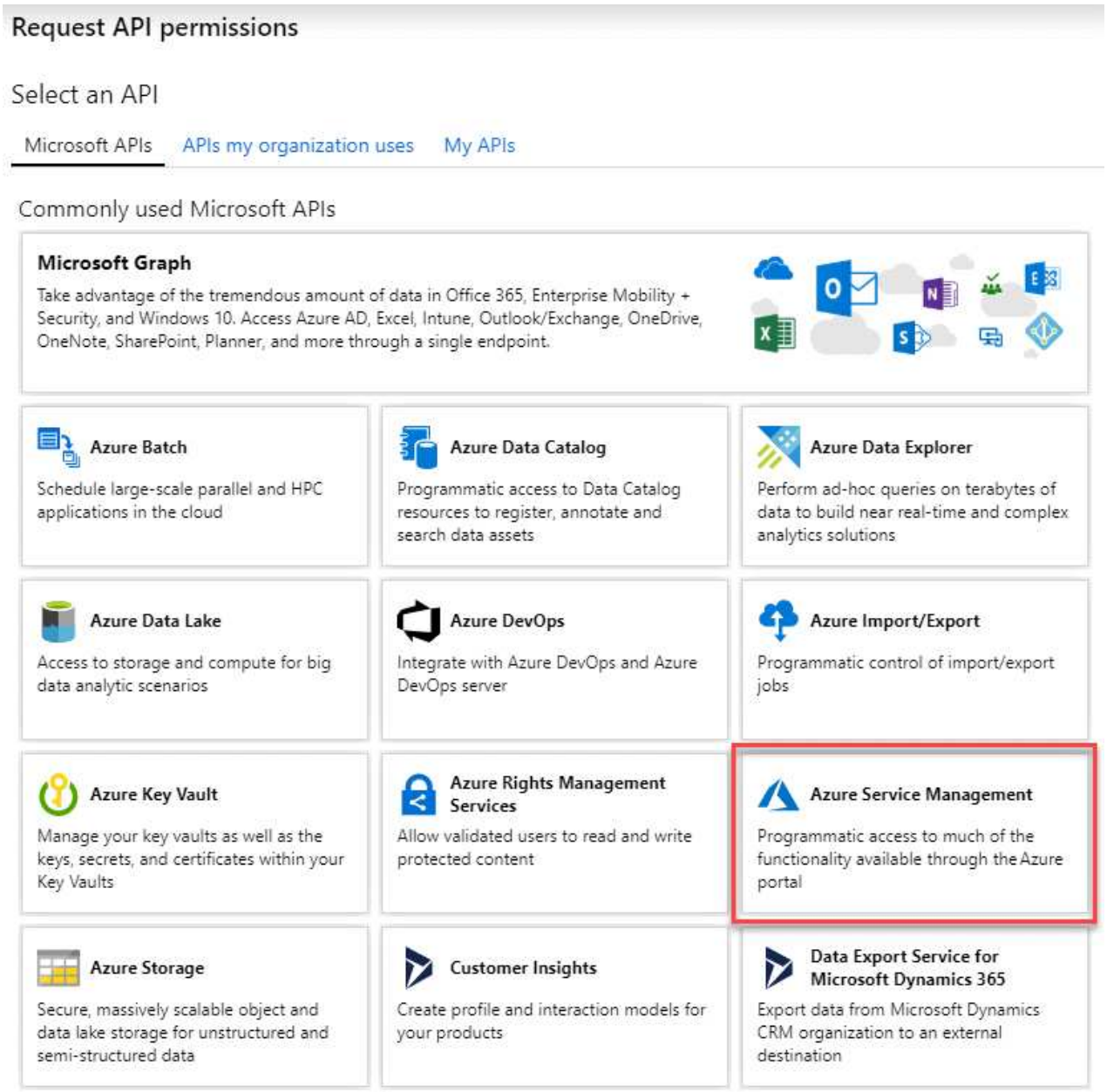
f. 選擇*審閱+分配*。

服務主體現在具有部署控制台代理程式所需的 Azure 權限。

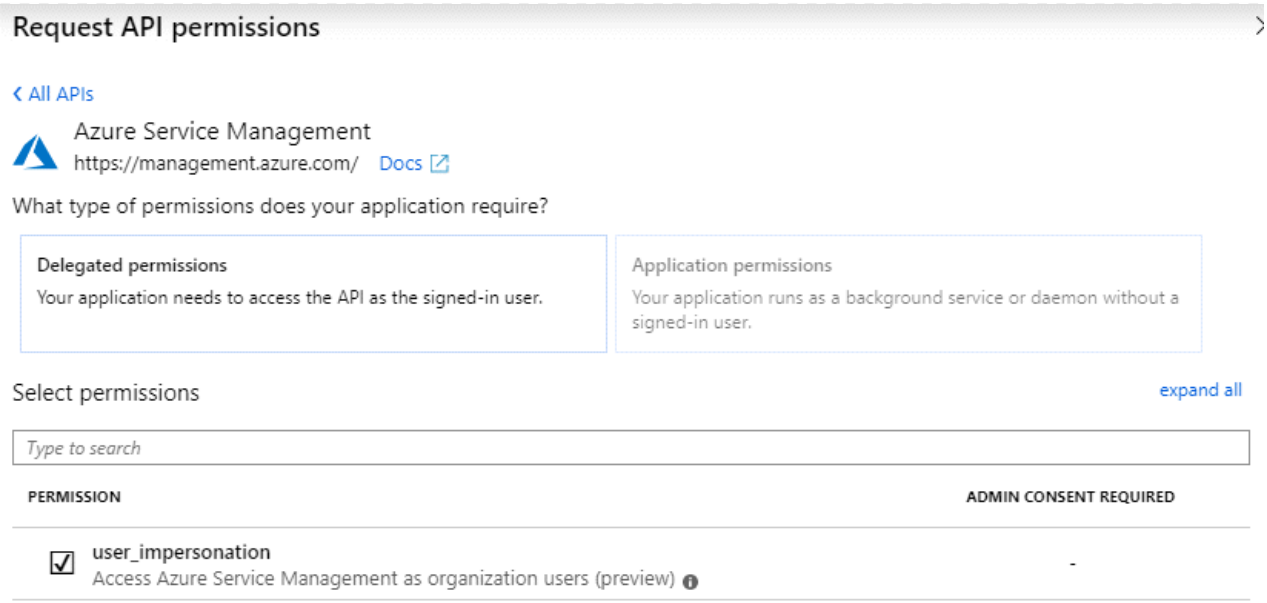
如果您想要從多個 Azure 訂閱部署Cloud Volumes ONTAP ，則必須將服務主體綁定到每個訂閱。在NetApp Console中，您可以選擇部署Cloud Volumes ONTAP時要使用的訂閱。

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」。

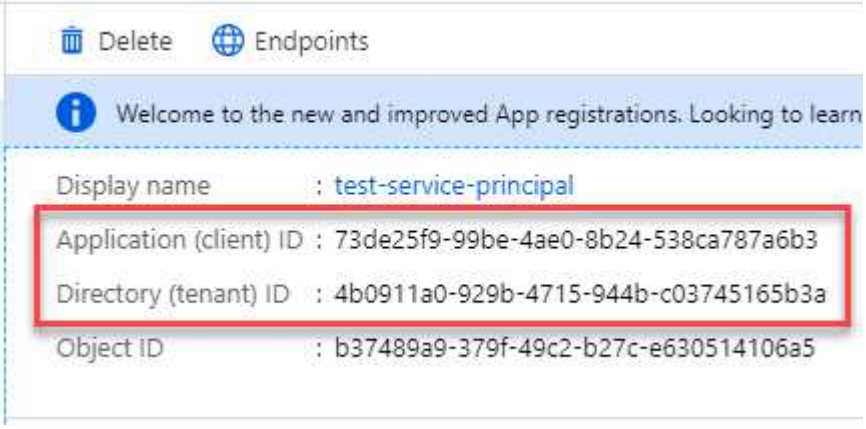



4. 選擇*以組織使用者身分存取 Azure 服務管理*，然後選擇*新增權限*。




取得應用程式的應用程式**ID**和目錄**ID**

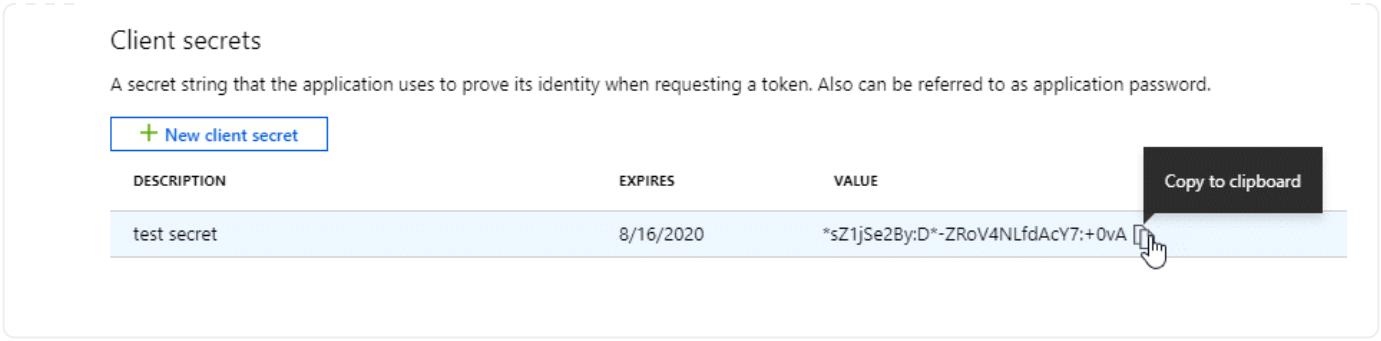
1. 在*Microsoft Entra ID*服務中，選擇*App Registrations*並選擇應用程式。
2. 複製*應用程式（客戶端）ID*和*目錄（租用戶）ID*。




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。




手動安裝控制台代理

當您手動安裝控制台代理時，您需要準備您的機器環境以使其滿足要求。您需要一台 Linux 機器，並且需要安裝 Podman 或 Docker，這取決於您的 Linux 作業系統。

### 安裝 **Podman** 或 **Docker Engine**

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 **4.** 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
```

手動安裝控制台代理

在本機現有 Linux 主機上下載並安裝控制台代理軟體。

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"。

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。

下一步是什麼？

您需要在NetApp Console中註冊控制台代理程式。

## 使用**NetApp Console**註冊控制台代理

登入控制台並將控制台代理與您的組織關聯。登入方式取決於您使用控制台的模式。如果您在標準模式下使用控制台，則可以透過 SaaS 網站登入。如果您在受限模式下使用控制台，則可以從控制台代理主機本機登入。

步驟

1. 開啟 Web 瀏覽器並輸入控制台代理主機 URL：

   控制台主機 URL 可以是本機主機、私人 IP 位址或公用 IP 位址，取決於主機的配置。例如，如果控制台代理程式位於沒有公用 IP 位址的公有雲中，則必須輸入與控制台代理主機有連接的主機的私人 IP 位址。

2. 註冊或登入。
3. 登入後，設定控制台：
   a. 指定與控制台代理程式關聯的控制台組織。
   b. 輸入系統的名稱。
   c. 在*您是否在安全環境中運作？ *下保持限制模式為停用。

      當控制台代理安裝在本機時，不支援限制模式。

   d. 選擇*讓我們開始吧*。

## 向**NetApp Console**提供雲端提供者憑證

安裝並設定控制台代理程式後，新增您的雲端憑證，以便控制台代理程式具有在 AWS 或 Azure 中執行操作所需的權限。

**AWS**

開始之前

如果您剛剛建立了這些 AWS 憑證，它們可能需要幾分鐘才能生效。等待幾分鐘，然後將憑證新增至控制台。

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*。

您現在可以前往 "NetApp Console"開始使用控制台代理。

**Azure**

開始之前

如果您剛剛建立了這些 Azure 憑證，它們可能需要幾分鐘才能使用。等待幾分鐘，然後再新增控制台代理的憑證。

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

控制台代理現在具有代表您在 Azure 中執行操作所需的權限。您現在可以前往 "NetApp Console"開始使用控制台代理。

使用 **VCenter** 在本機安裝控制台代理

# 如果您是 VMWare 用戶，您可以使用 OVA 在您的 VCenter 中安裝控制台代理程式。可透過NetApp Console取得 OVA 下載或 URL。

當您使用 VCenter 工具安裝控制台代理程式時，您可以使用 VM Web 控制台執行維護任務。"了解有關代理的 VM 控制台的更多資訊。"

## 準備安裝控制台代理

安裝之前，請確保您的 VM 主機符合要求並且控制台代理程式可以存取網際網路和目標網路。若要使用NetApp資料服務或Cloud Volumes ONTAP，請為控制台代理程式建立雲端提供者憑證以代表您執行操作。

### 查看控制台代理主機需求

在安裝控制台代理之前，請確保您的主機符合安裝要求。

- CPU：8 核心或 8 個 vCPU
- 記憶體：32 GB
- 磁碟空間：165 GB（厚置備）
- vSphere 7.0 或更高版本
- ESXi 主機 7.03 或更高版本

在 vCenter 環境中安裝代理，而不是直接在 ESXi 主機上安裝。

### 為控制台代理設定網路訪問

與您的網路管理員合作，確保控制台代理具有所需端點的出站存取權限以及與目標網路的連線。

#### 連接到目標網絡

控制台代理程式需要與您計劃建立和管理系統的位置建立網路連線。例如，您計劃在本機環境中建立Cloud Volumes ONTAP系統或儲存系統的網路。

#### 出站互聯網訪問

部署控制台代理程式的網路位置必須具有出站網路連線才能聯絡特定端點。

#### 使用基於 **Web** 的**NetApp Console**時從電腦聯繫的端點

從 Web 瀏覽器存取控制台的電腦必須能夠聯絡多個端點。您需要使用控制台來設定控制台代理並進行控制台的日常使用。

"為NetApp控制台準備網絡" 。

#### 從控制台代理聯繫的端點

控制台代理需要外部網路存取來聯繫以下端點，以管理公有雲環境中的資源和流程以進行日常操作。

下面列出的端點都是 CNAME 條目。

您無法使用安裝在本機的控制台代理程式來管理 Google Cloud 中的資源。若要管理 Google Cloud 資源，請在 Google Cloud 中安裝代理程式。

**AWS**

當控制台代理程式安裝在本機時，它需要對以下 AWS 端點進行網路訪問，以便管理部署在 AWS 中的NetApp系統（例如Cloud Volumes ONTAP）。

從控制台代理聯繫的端點

控制台代理需要外部網路存取來聯繫以下端點，以管理公有雲環境中的資源和流程以進行日常操作。

下面列出的端點都是 CNAME 條目。

| 端點 | 目的 |
| --- | --- |
| AWS 服務（amazonaws.com）：<br>• 雲形成<br>• 彈性運算雲（EC2）<br>• 身分和存取管理 (IAM)<br>• 金鑰管理服務（KMS）<br>• 安全性令牌服務 (STS)<br>• 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：<br>• 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。 |
| \ 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。<br><br>• 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。<br><br>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"。<br><br>• 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**

當控制台代理程式安裝在本機時，它需要對以下 Azure 端點進行網路訪問，以便管理部署在 Azure 中的NetApp系統（例如Cloud Volumes ONTAP）。

| 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.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。 |
| \ 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。<br><br>• 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。<br><br>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"。<br><br>• 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。 |

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"

## 為 **AWS** 或 **Azure** 建立控制台代理雲端權限

如果您想將 AWS 或 Azure 中的NetApp資料服務與本機控制台代理程式一起使用，則需要在雲端提供者中設定權限，以便在安裝控制台代理程式後將憑證新增至控制台代理程式。

您無法使用安裝在本機的控制台代理程式來管理 Google Cloud 中的資源。如果您想管理 Google Cloud 資源，則需要在 Google Cloud 中安裝代理程式。

**AWS**

對於本機控制台代理，透過新增 IAM 使用者存取金鑰來提供 AWS 權限。

對本機控制台代理程式使用 IAM 使用者存取金鑰；本機控制台代理程式不支援 IAM 角色。

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。

結果

您現在應該擁有具有所需權限的 IAM 使用者存取金鑰。安裝控制台代理程式後，從控制台將這些憑證與控制台代理程式關聯。

**Azure**

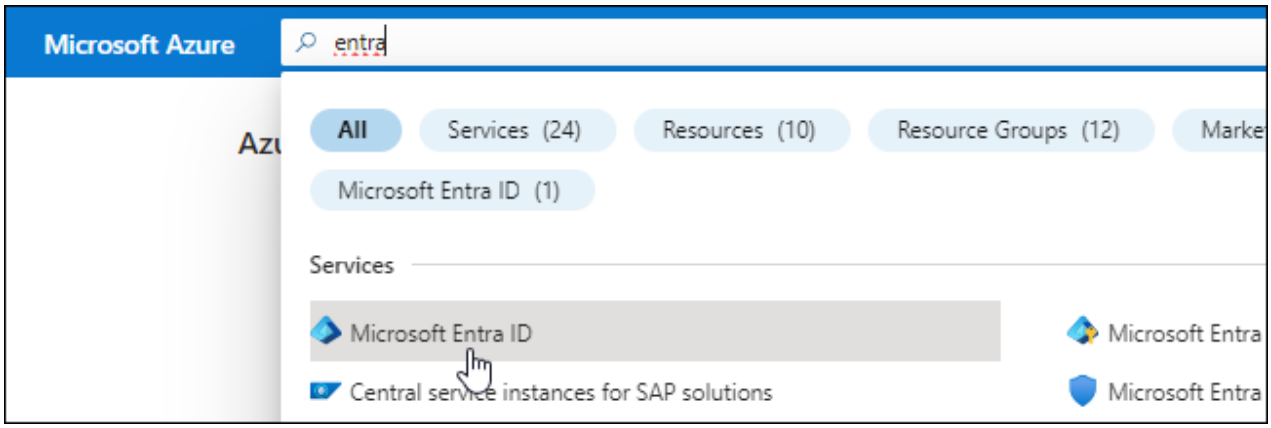
當控制台代理程式安裝在本機時，您需要透過在 Microsoft Entra ID 中設定服務主體並取得控制台代理程式所需的 Azure 憑證來授予控制台代理 Azure 權限。

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。

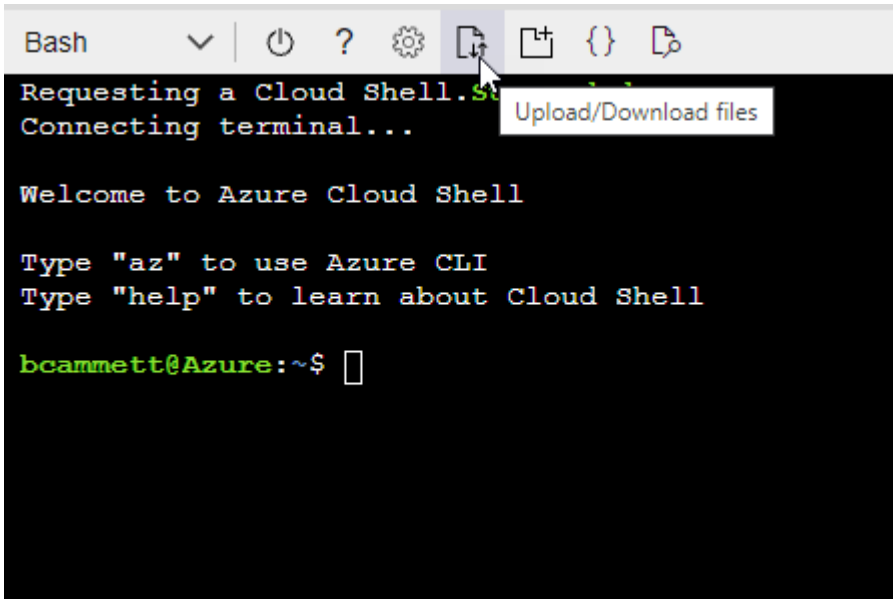
      例子

      ```
      "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。

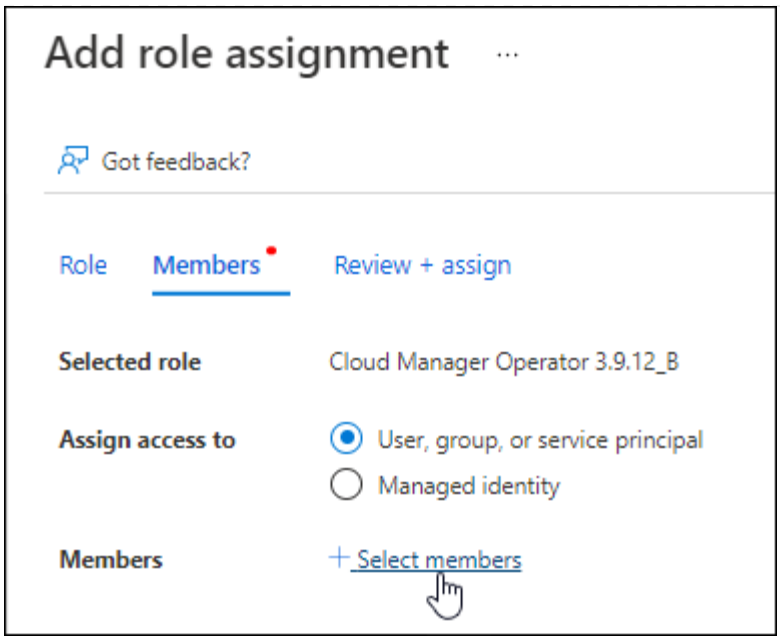
b. 選擇訂閱。

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*。

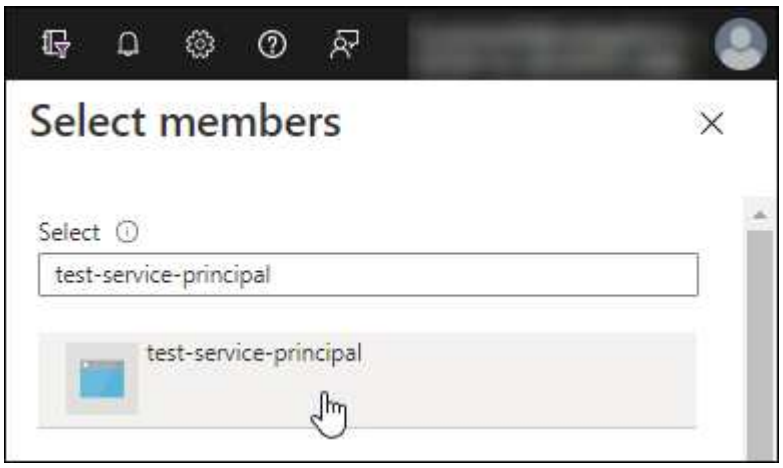
e. 在「成員」標籤中，完成以下步驟：

- 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”。

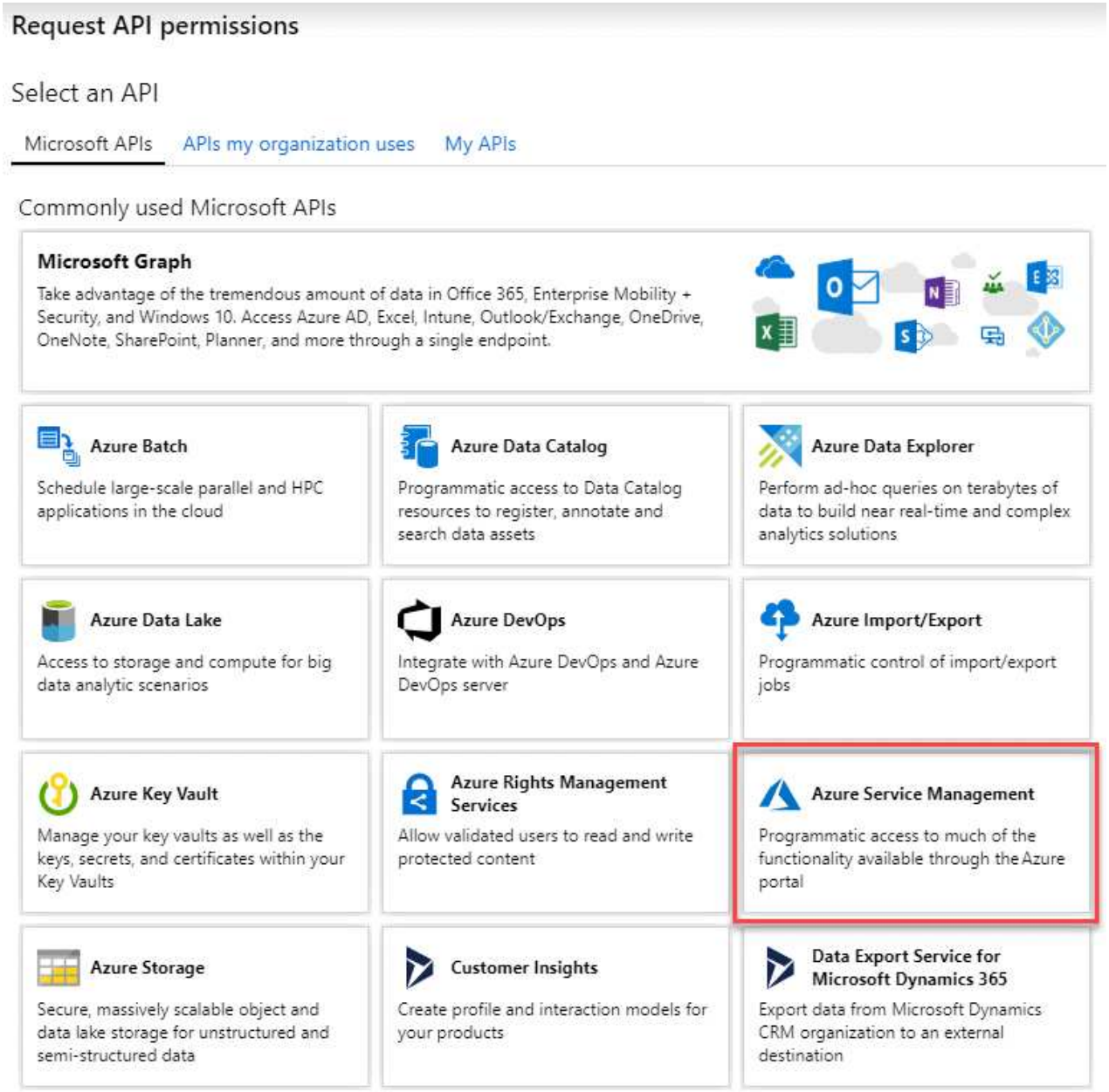
f. 選擇*審閱+分配*。

服務主體現在具有部署控制台代理程式所需的 Azure 權限。

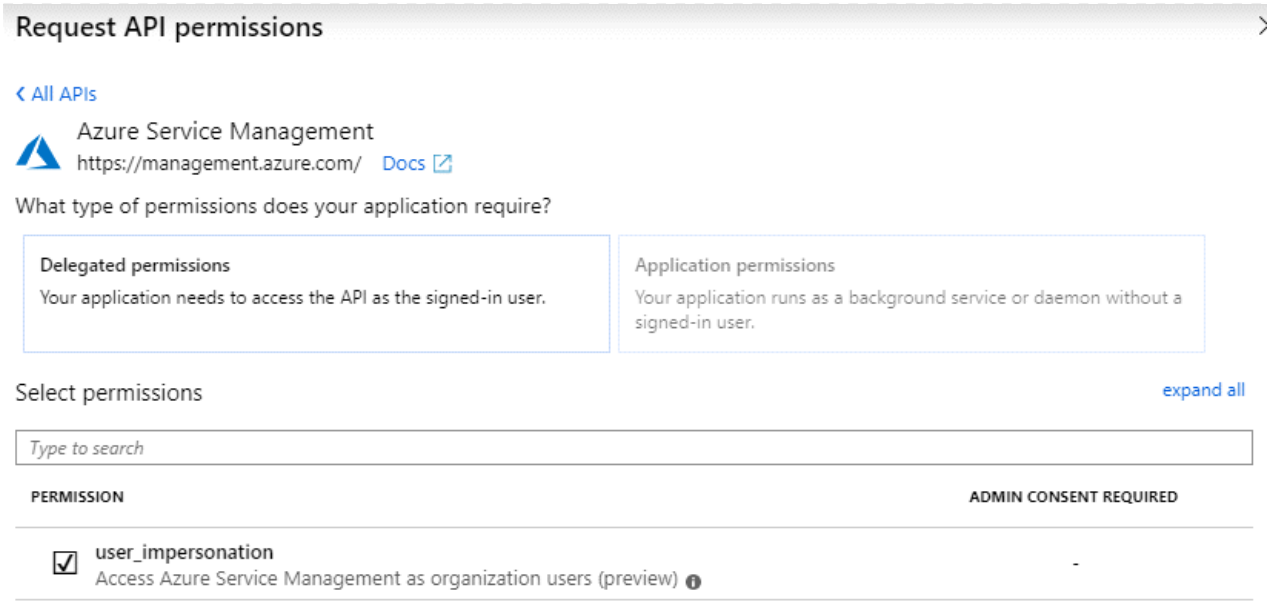
如果您想要從多個 Azure 訂閱部署Cloud Volumes ONTAP ，則必須將服務主體綁定到每個訂閱。在NetApp Console中，您可以選擇部署Cloud Volumes ONTAP時要使用的訂閱。

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」。

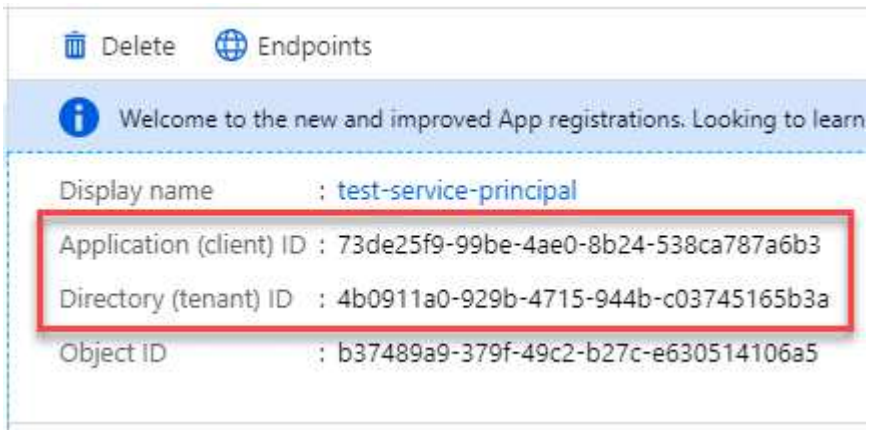



4. 選擇*以組織使用者身分存取 Azure 服務管理*，然後選擇*新增權限*。




取得應用程式的應用程式**ID**和目錄**ID**

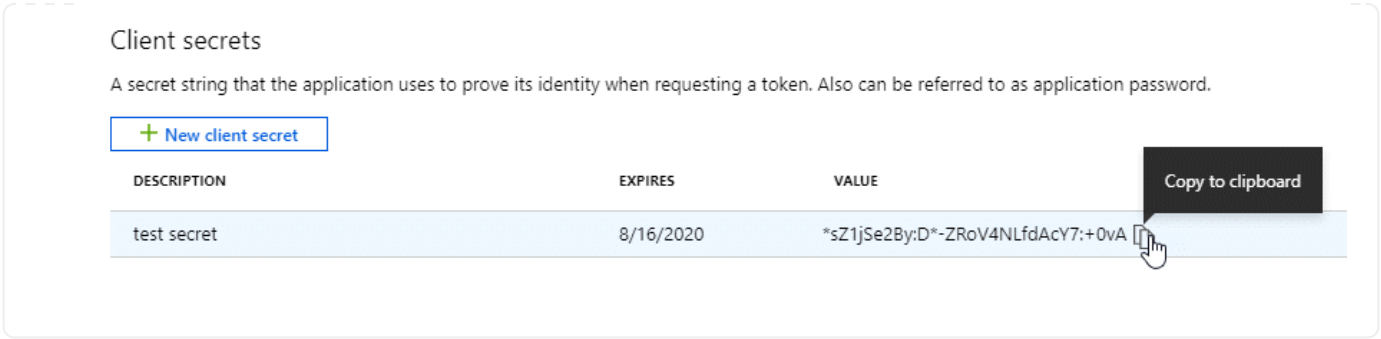
1. 在*Microsoft Entra ID*服務中，選擇*App Registrations*並選擇應用程式。
2. 複製*應用程式（客戶端）ID*和*目錄（租用戶）ID*。




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。




### 在 **VCenter** 環境中安裝控制台代理

NetApp支援在您的 VCenter 環境中安裝控制台代理程式。 OVA 檔案包含一個預先設定的 VM 映像，您可以在 VMware 環境中部署該映像。可直接從NetApp Console下載檔案或部署 URL。它包括控制台代理軟體和自簽名證書。

#### 下載 **OVA** 或複製 **URL**

直接從NetApp Console下載 OVA 或複製 OVA URL。

1. 選擇“管理 **>** 代理”。
2. 在「概覽」頁面上，選擇「部署代理程式**>**本機」。
3. 選擇*使用 OVA*。
4. 選擇下載 OVA 或複製 URL 以在 VCenter 中使用。

#### 在您的 **VCenter** 中部署代理

登入您的 VCenter 環境以部署代理程式。

步驟

1. 如果您的環境需要，請將自簽名憑證上傳到您的受信任憑證。安裝後，您可以替換此證書。"了解如何替換自簽名憑證。"
2. 從內容庫或本機系統部署 OVA。

| 從本地系統 | 來自內容庫 |
| --- | --- |
| a. 右鍵點選並選擇 部署 **OVF** 範本...。 b. 從 URL 中選擇 OVA 檔案或瀏覽到其位置，然後選擇 下一步。 | a. 前往您的內容庫並選擇控制台代理 OVA。 b. 選擇“操作”>“從此範本新虛擬機器” |

3. 完成部署 OVF 範本精靈以部署控制台代理程式。
4. 為虛擬機器選擇名稱和資料夾，然後選擇“下一步”。
5. 選擇一個計算資源，然後選擇*下一步*。
6. 查看範本的詳細信息，然後選擇*下一步*。
7. 接受許可協議，然後選擇*下一步*。
8. 選擇要使用的代理配置類型：明確代理、透明代理或無代理。
9. 選擇要部署虛擬機器的資料存儲，然後選擇*下一步*。確保它滿足主機要求。

10. 選擇您想要連接虛擬機器的網絡，然後選擇*下一步*。確保網路為 IPv4 並且具有對所需端點的出站網路存取權限。
11. 在*自訂範本*視窗中，填寫以下欄位：
    - 代理資訊
      - 如果選擇了明確代理，請輸入代理伺服器主機名稱或 IP 位址和連接埠號，以及使用者名稱和密碼。
      - 如果您選擇了透明代理，請上傳對應的憑證。
    - 虛擬機器配置
      - 跳過配置檢查：預設未選取此複選框，這表示代理程式執行配置檢查以驗證網路存取。
        - NetApp建議不要選取此框，以便安裝包含代理程式的設定檢查。配置檢查驗證代理是否具有對所需端點的網路存取權限。如果由於連線問題導致部署失敗，您可以從代理主機存取驗證報告和日誌。在某些情況下，如果您確信代理程式具有網路存取權限，則可以選擇跳過檢查。例如，如果您仍在使用"先前的端點"用於代理升級，驗證失敗並出現錯誤。為了避免這種情況，請勾選複選框以在不進行驗證檢查的情況下進行安裝。"了解如何更新終端節點列表" 。
      - 維修密碼：設定維修密碼 `maint`允許存取代理維護控制台的使用者。
      - **NTP** 伺服器：指定一個或多個 NTP 伺服器進行時間同步。
      - 主機名稱：設定此虛擬機器的主機名稱。它不能包含搜尋域。例如，FQDN console10.searchdomain.company.com 應輸入為 console10。
      - 主 **DNS**：指定用於名稱解析的主 DNS 伺服器。
      - 輔助 **DNS**：指定用於名稱解析的輔助 DNS 伺服器。
      - 搜尋域：指定解析主機名稱時所使用的搜尋網域名稱。例如，如果 FQDN 是 console10.searchdomain.company.com，則輸入 searchdomain.company.com。
      - **IPv4** 位址：對應到主機名稱的 IP 位址。
      - **IPv4** 子網路遮罩：IPv4 位址的子網路遮罩。
      - **IPv4** 網關位址：IPv4 位址的網關位址。
12. 選擇“下一步”。
13. 查看“準備完成”視窗中的詳細信息，選擇“完成”。

    vSphere 工作列顯示控制台代理部署的進度。
14. 啟動虛擬機器。

如果部署失敗，您可以從代理主機存取驗證報告和日誌。"了解如何解決安裝問題。"

### 使用NetApp Console註冊控制台代理

登入控制台並將控制台代理與您的組織關聯。登入方式取決於您使用控制台的模式。如果您在標準模式下使用控制台，則可以透過 SaaS 網站登入。如果您在受限或私人模式下使用控制台，則可以從控制台代理主機本機登入。

步驟

1. 開啟 Web 瀏覽器並輸入控制台代理主機 URL：

控制台主機 URL 可以是本機主機、私人 IP 位址或公用 IP 位址，取決於主機的配置。例如，如果控制台代理程式位於沒有公用 IP 位址的公有雲中，則必須輸入與控制台代理主機有連接的主機的私人 IP 位址。

2. 註冊或登入。
3. 登入後，設定控制台：
   a. 指定與控制台代理程式關聯的控制台組織。
   b. 輸入系統的名稱。
   c. 在*您是否在安全環境中運作？ *下保持限制模式為停用。

      當控制台代理安裝在本機時，不支援限制模式。

   d. 選擇*讓我們開始吧*。

將雲端提供者憑證新增至控制台

安裝並設定控制台代理程式後，新增您的雲端憑證，以便控制台代理程式具有在 AWS 或 Azure 中執行操作所需的權限。

**AWS**

開始之前

如果您剛剛建立了這些 AWS 憑證，它們可能需要幾分鐘才能生效。等待幾分鐘，然後將憑證新增至控制台。

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*。

您現在可以前往 "NetApp Console"開始使用控制台代理。

**Azure**

開始之前

如果您剛剛建立了這些 Azure 憑證，它們可能需要幾分鐘才能使用。等待幾分鐘，然後再新增控制台代理的憑證。

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

控制台代理現在具有代表您在 Azure 中執行操作所需的權限。您現在可以前往 "NetApp Console"開始使用控制台代理。

本機控制台代理的連接埠

## 當在本機 Linux 主機上手動安裝時，控制台代理使用_入站_連接埠。請參考這些連接埠以進行規劃。

這些入站規則適用於所有NetApp Console部署模式。

| 協定 | 港口 | 目的 |
| --- | --- | --- |
| HTTP | 80 | • 提供從客戶端 Web 瀏覽器到本機使用者介面的 HTTP 訪問<br>• 在Cloud Volumes ONTAP升級過程中使用 |
| HTTPS | 443 | 提供從客戶端 Web 瀏覽器到本機使用者介面的 HTTPS 訪問 |

## 維護控制台代理

為控制台代理程式維護 **VCenter** 或 **ESXi** 主機

部署控制台代理程式後，您可以對現有的 VCenter 或 ESXi 主機進行變更。例如，您可以增加託管控制台代理程式的 VM 執行個體的 CPU 或 RAM。

使用 VM Web 控制台執行下列維護任務：

- 增加磁碟大小
- 重啟代理
- 更新靜態路由
- 更新搜尋域

限制

尚不支援透過控制台升級代理程式。此外，您只能查看有關 IP 位址、DNS 和網關的資訊。

存取虛擬機器維護控制台

您可以從 VSphere 用戶端存取維護控制台。

步驟

1. 開啟 VSphere 用戶端並登入您的 VCenter。
2. 選擇託管控制台代理程式的 VM 執行個體。
3. 選擇*啟動 Web 控制台*。
4. 使用建立 VM 實例時指定的使用者名稱和密碼登入 VM 實例。使用者名稱是 `maint`密碼是您在建立 VM 實例時指定的密碼。

修改主用戶密碼

您可以更改 `maint`用戶。

步驟

1. 開啟 VSphere 用戶端並登入您的 VCenter。
2. 選擇託管控制台代理程式的 VM 執行個體。
3. 選擇*啟動 Web 控制台*。

4. 使用建立 VM 實例時指定的使用者名稱和密碼登入 VM 實例。使用者名稱是 `maint`密碼是您在建立 VM 實例時指定的密碼。
5. 進入 `1`查看 `System Configuration`菜單。
6. 進入 `1`變更維護使用者密碼並按照螢幕上的指示進行操作。

### 增加虛擬機器執行個體的 **CPU** 或 **RAM**

您可以增加託管控制台代理程式的 VM 執行個體的 CPU 或 RAM。

在您的 VCenter 或 ESXi 主機中編輯 VM 實例設置，然後使用維護控制台套用變更。

**VSphere** 用戶端中的步驟

1. 開啟 VSphere 用戶端並登入您的 VCenter。
2. 選擇託管控制台代理程式的 VM 執行個體。
3. 右鍵點選 VM 實例並選擇*編輯設定*。
4. 增加用於 /opt 或 /var 分區的硬碟空間。
   a. 選擇“硬碟 **2**”以增加用於 /opt 的硬碟空間。
   b. 選擇*硬碟 3* 來增加 /var 所使用的硬碟空間。
5. 儲存更改。

維護控制台中的步驟

1. 開啟 VSphere 用戶端並登入您的 VCenter。
2. 選擇託管控制台代理程式的 VM 執行個體。
3. 選擇*啟動 Web 控制台*。
4. 使用建立 VM 實例時指定的使用者名稱和密碼登入 VM 實例。使用者名稱是 `maint`密碼是您在建立 VM 實例時指定的密碼。
5. 進入 `1 to view the `System Configuration`菜單。
6. 進入 `2`並按照螢幕上的指示進行操作。控制台掃描新設定並增加分割區的大小。

### 查看代理虛擬機器的網路設置

查看 VSphere 用戶端中代理 VM 的網路設定以確認或排除網路問題。您只能查看（不能更新）以下網路設定：IP 位址和 DNS 詳細資訊。

步驟

1. 開啟 VSphere 用戶端並登入您的 VCenter。
2. 選擇託管控制台代理程式的 VM 執行個體。
3. 選擇*啟動 Web 控制台*。
4. 使用建立 VM 實例時指定的使用者名稱和密碼登入 VM 實例。使用者名稱是 `maint`密碼是您在建立 VM 實例時指定的密碼。
5. 進入 `2`查看 `Network Configuration`菜單。
6. 輸入 1 到 6 之間的數字以查看相應的網路設定。

## 更新代理虛擬機器的靜態路由

根據需要新增、更新或刪除代理虛擬機器的靜態路由。

步驟

1. 開啟 VSphere 用戶端並登入您的 VCenter。
2. 選擇託管控制台代理程式的 VM 執行個體。
3. 選擇*啟動 Web 控制台*。
4. 使用建立 VM 實例時指定的使用者名稱和密碼登入 VM 實例。使用者名稱是 `maint`密碼是您在建立 VM 實例時指定的密碼。
5. 進入 `2`查看 `Network Configuration`菜單。
6. 進入 `7`更新靜態路由並依照螢幕上的指示進行操作。
7. 按 Enter 鍵。
8. 或者，進行其他更改。
9. 進入 `9`提交您的更改。

## 更新代理虛擬機器的網域搜尋設置

您可以更新代理虛擬機器的搜尋域設定。

步驟

1. 開啟 VSphere 用戶端並登入您的 VCenter。
2. 選擇託管控制台代理程式的 VM 執行個體。
3. 選擇*啟動 Web 控制台*。
4. 使用建立 VM 實例時指定的使用者名稱和密碼登入 VM 實例。使用者名稱是 `maint`密碼是您在建立 VM 實例時指定的密碼。
5. 進入 `2``查看 `Network Configuration`菜單。
6. 進入 `8`更新網域搜尋設定並按照螢幕上的指示進行操作。
7. 按 Enter 鍵。
8. 或者，進行其他更改。
9. 進入 `9`提交您的更改。

## 存取代理診斷工具

存取診斷工具來解決控制台代理的問題。 NetApp支援可能會在解決問題時要求您執行此操作。

步驟

1. 開啟 VSphere 用戶端並登入您的 VCenter。
2. 選擇託管控制台代理程式的 VM 執行個體。
3. 選擇*啟動 Web 控制台*。
4. 使用建立 VM 實例時指定的使用者名稱和密碼登入 VM 實例。使用者名稱是 `maint`密碼是您在建立 VM 實

例時指定的密碼。

5. 進入 `3`查看支援和診斷選單。
6. 進入 `1`存取診斷工具並按照螢幕上的指示進行操作。 + 例如，您可以驗證所有代理服務是否正在執行。"檢查控制台代理狀態" 。

遠端存取代理診斷工具

您可以使用 Putty 等工具遠端存取診斷工具。透過指派一次性密碼啟用對代理 VM 的 SSH 存取。

SSH 存取支援複製和貼上等進階終端功能。

步驟

1. 開啟 VSphere 用戶端並登入您的 VCenter。
2. 選擇託管控制台代理程式的 VM 執行個體。
3. 選擇*啟動 Web 控制台*。
4. 使用建立 VM 實例時指定的使用者名稱和密碼登入 VM 實例。使用者名稱是 `maint`密碼是您在建立 VM 實例時指定的密碼。
5. 進入 `3`查看 `Support and Diagnostics`菜單。
6. 進入 `2`存取診斷工具並依照螢幕上的指示配置 24 小時後過期的一次性密碼。
7. 使用 SSH 工具（例如 Putty）透過使用者名稱連接到代理虛擬機 `diag`以及您設定的一次性密碼。

安裝 **CA** 簽署的憑證以進行基於 **Web** 的控制台訪問

## 當您在受限模式下使用NetApp Console時，可以從部署在雲端區域或本機的控制台代理虛擬機器存取使用者介面。預設情況下，控制台使用自簽名 SSL 憑證為控制台代理程式上執行的基於 Web 的控制台提供安全的 HTTPS 存取。

如果您的業務需要，您可以安裝由憑證授權單位 (CA) 簽署的證書，它比自簽名憑證提供更好的安全保護。安裝憑證後，當使用者存取基於 Web 的控制台時，控制台將使用 CA 簽署的憑證。

### 安裝 **HTTPS** 憑證

安裝由 CA 簽署的證書，以便安全地存取在控制台代理上執行的基於 Web 的控制台。

關於此任務

您可以使用以下選項之一安裝憑證：

- 從控制台產生憑證簽署要求 (CSR)，將憑證要求提交給 CA，然後在控制台代理程式上安裝 CA 簽署的憑證。

  控制台用於產生 CSR 的金鑰對儲存在控制台代理程式內部。當您在控制台代理程式上安裝憑證時，控制台會自動擷取相同的金鑰對（私密金鑰）。

- 安裝您已有的 CA 簽章憑證。

  使用此選項，CSR 不會透過控制台產生。您單獨產生 CSR 並將私鑰儲存於外部。安裝憑證時，您需要向控制台提供私鑰。

步驟

1. 選擇“管理 **>** 代理”。
2. 在*概述*頁面上，選擇控制台代理的操作選單並選擇*HTTPS 設定*。

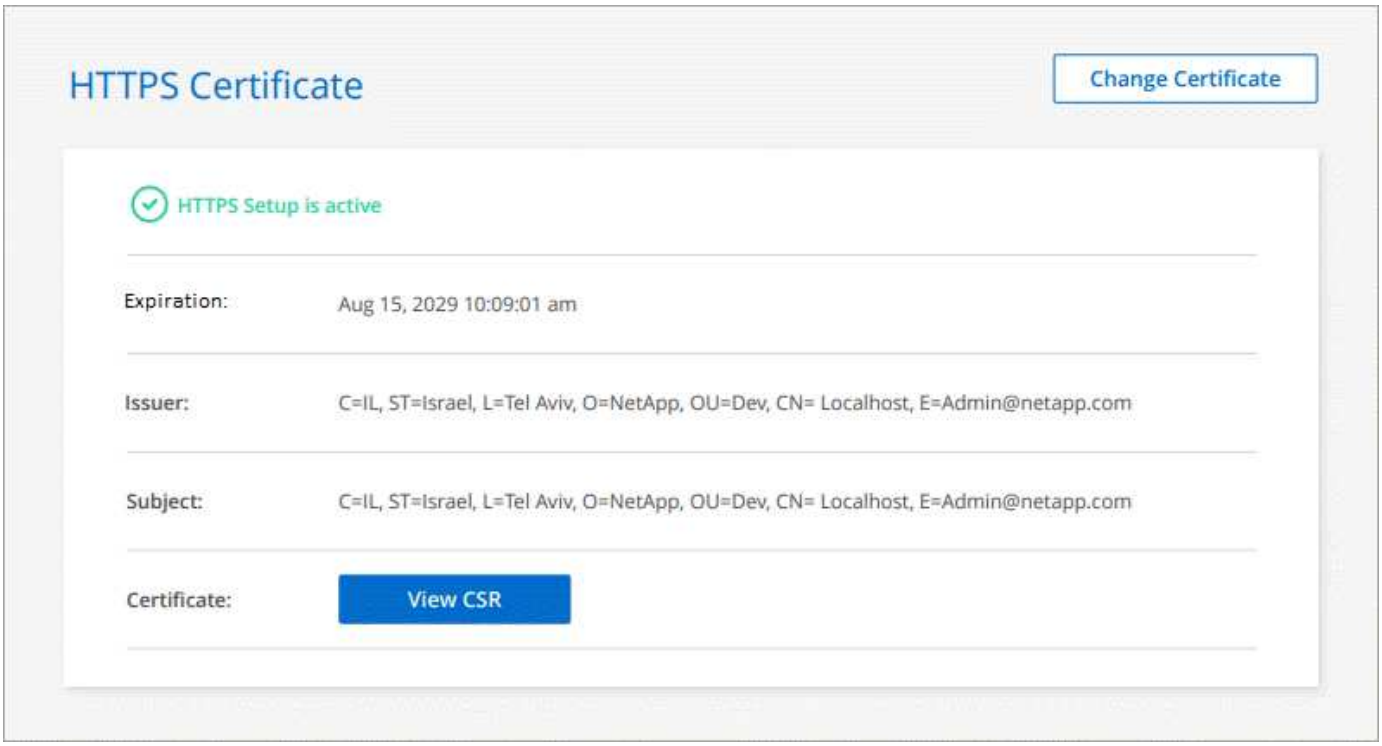
   必須連接控制台代理才能進行編輯。

3. 在 HTTPS 設定頁面中，透過產生憑證簽章要求 (CSR) 或安裝您自己的 CA 簽章憑證來安裝憑證：

| 選項 | 描述 |
| --- | --- |
| 產生 CSR | a. 輸入控制台代理主機的主機名稱或 DNS（其通用名稱），然後選擇 產生 **CSR**。<br><br>控制台顯示憑證簽署要求。<br><br>b. 使用 CSR 向 CA 提交 SSL 憑證請求。<br><br>憑證必須使用隱私增強郵件 (PEM) Base-64 編碼的 X.509 格式。<br><br>c. 上傳證書文件，然後選擇*安裝*。 |
| 安裝您自己的 CA 簽名證書 | a. 選擇*安裝 CA 簽章憑證*。<br>b. 載入憑證檔案和私鑰，然後選擇*安裝*。<br><br>憑證必須使用隱私增強郵件 (PEM) Base-64 編碼的 X.509 格式。 |

結果

控制台代理現在使用 CA 簽署的憑證來提供安全的 HTTPS 存取。下圖顯示了配置為安全存取的代理程式：




續訂控制台 **HTTPS** 憑證

您應該在代理程式的 HTTPS 憑證到期之前更新它，以確保安全存取。如果您未在憑證到期前續訂，則當使用者使用 HTTPS 存取 Web 控制台時會出現警告。

步驟

1. 選擇“管理 **>** 代理”。
2. 在*概述*頁面上，選擇控制台代理的操作選單並選擇*HTTPS 設定*。

   顯示有關證書的詳細信息，包括到期日期。

3. 選擇*變更憑證*並依照步驟產生 CSR 或安裝您自己的 CA 簽章憑證。

配置控制台代理以使用代理伺服器

如果您的公司政策要求您使用代理伺服器進行所有與互聯網的通信，那麼您需要設定您的代理以使用該代理伺服器。如果您在安裝期間沒有將控制台代理程式設定為使用代理伺服器，那麼您可以隨時將控制台代理程式設定為使用該代理伺服器。

代理程式的代理伺服器無需公用 IP 或 NAT 閘道即可實現出站網際網路存取。代理伺服器僅為控制台代理提供出站連接，而不為Cloud Volumes ONTAP系統提供出站連接。

如果Cloud Volumes ONTAP系統缺少出站互聯網訪問，控制台會將其配置為使用控制台代理的代理伺服器。您必須確保控制台代理程式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開啟此連接埠。

如果控制台代理本身沒有出站互聯網連接， Cloud Volumes ONTAP系統將無法使用已設定的代理伺服器。

支援的配置

- 為Cloud Volumes ONTAP系統提供服務的代理支援透明代理伺服器。如果您將NetApp資料服務與Cloud Volumes ONTAP一起使用，請為Cloud Volumes ONTAP建立專用代理，您可以在其中使用透明代理伺服器。
- 所有代理程式都支援明確代理伺服器，包括管理Cloud Volumes ONTAP系統的代理程式和管理NetApp資料服務的代理程式。
- HTTP 和 HTTPS。
- 代理伺服器可以位於雲端或您的網路。

一旦配置了代理，您就無法變更代理類型。如果需要變更代理類型，請刪除控制台代理並新增具有新代理類型的新代理程式。

在控制台代理上啟用明確代理

當您將控制台代理程式設定為使用代理伺服器時，該代理程式及其管理的Cloud Volumes ONTAP系統（包括任何 HA 中介）都會使用代理伺服器。

此操作將重新啟動控制台代理程式。在繼續之前，請先確認控制台代理是否空閒。

步驟

1. 選擇“管理 **>** 代理”。
2. 在*概覽*頁面上，選擇控制台代理程式的操作選單，然後選擇*編輯代理*。

   控制台代理程式必須處於活動狀態才能對其進行編輯。

3. 選擇*HTTP 代理程式配置*。
4. 在配置類型欄位中選擇*明確代理*。
5. 選擇*啟用代理*。
6. 使用語法指定伺服器 <a href="http://<em>address:port</em>" class="bare">http://<em>address:port</em></a>或者 <a href="https://<em>address:port</em>" class="bare">https://<em>address:port</em></a>
7. 如果伺服器需要基本驗證，請指定使用者名稱和密碼。

   請注意以下事項：

   - 使用者可以是本機使用者或網域使用者。
   - 對於網域用戶，您必須輸入 \ 的 ASCII 代碼，如下所示：domain-name%92user-name

     例如：netapp%92proxy

   - 控制台不支援包含 @ 字元的密碼。
8. 選擇*儲存*。

為控制台代理啟用透明代理

僅Cloud Volumes ONTAP支援在控制台代理上使用透明代理。如果您除了Cloud Volumes ONTAP之外還使用NetApp資料服務，則應建立一個單獨的代理來用於資料服務或用於Cloud Volumes ONTAP。

啟用透明代理前，請確保滿足以下要求：

- 代理與透明代理伺服器安裝在同一網路上。
- 代理伺服器上啟用了 TLS 檢查。
- 您有一個 PEM 格式的證書，與透明代理伺服器上使用的證書相符。
- 您不要將控制台代理用於除Cloud Volumes ONTAP之外的任何NetApp資料服務。

若要將現有代理程式設定為使用透明代理伺服器，請使用可透過控制台代理主機上的命令列取得的控制台代理維護工具。

當您設定代理伺服器時，控制台代理將重新啟動。在繼續之前，請先確認控制台代理是否空閒。

步驟

確保您擁有代理伺服器的 PEM 格式的憑證檔案。如果您沒有證書，請聯絡您的網路管理員以取得證書。

1. 在控制台代理主機上開啟命令列介面。
2. 導覽至控制台代理維護工具目錄： `/opt/application/netapp/service-manager-2/agent-maint-console`
3. 運行以下命令啟用透明代理，其中 `/home/ubuntu/<certificate-file>.pem`是您擁有的代理伺服器憑證檔案的目錄和名稱：

   ```
   ./agent-maint-console proxy add -c /home/ubuntu/<certificate-file>.pem
   ```

   確保證書檔案為 PEM 格式並與命令位於同一目錄中，或指定證書檔案的完整路徑。

   ```
   ./agent-maint-console proxy add -c /home/ubuntu/<certificate-file>.pem
   ```

修改控制台代理的透明代理

您可以使用下列方法更新控制台代理現有的透明代理伺服器： `proxy update`透過使用命令來移除透明代理伺服器 `proxy remove`命令。更多信息，請查閱相關文件。"代理維護控制台" 。

> 一旦配置了代理，您就無法變更代理類型。如果需要變更代理類型，請刪除控制台代理並新增具有新代理類型的新代理程式。

如果控制台代理無法存取互聯網，請更新它

如果您的網路代理程式配置發生變化，您的代理程式可能會失去對網際網路的存取權限。例如，如果有人更改了代理伺服器的密碼或更新了憑證。在這種情況下，您需要直接從控制台代理主機存取 UI 並更新設定。確保您可以透過網路存取控制台代理主機，並且可以登入控制台。

啟用直接 **API** 流量

如果您已將控制台代理程式配置為使用代理伺服器，則可以在控制台代理上啟用直接 API 流量，以便直接向雲端提供者服務發送 API 呼叫，而無需透過代理程式。在 AWS、Azure 或 Google Cloud 中執行的代理程式支援

此選項。

如果您停用帶有Cloud Volumes ONTAP 的Azure Private Links 並使用服務端點，請啟用直接 API 流量。否則，流量將無法正確路由。

"了解有關將 Azure Private Link 或服務端點與Cloud Volumes ONTAP結合使用的更多信息"

步驟

1. 選擇“管理 > 代理”。
2. 在*概覽*頁面上，選擇控制台代理程式的操作選單，然後選擇*編輯代理*。

   控制台代理程式必須處於活動狀態才能對其進行編輯。

3. 選擇*支援直接 API 流量*。
4. 選取核取方塊以啟用該選項，然後選擇*儲存*。

控制台代理故障排除

## 要解決控制台代理的問題，您可以自行驗證問題或與NetApp支援人員合作，他們可能會詢問您的系統 ID、代理程式版本或最新的AutoSupport訊息。

如果您有NetApp支援網站帳戶，您也可以查看"NetApp知識庫。"

常見錯誤訊息和解決方法

此表列出了常見的錯誤訊息以及解決方法：

| 錯誤訊息 | 解釋 | 該怎麼辦 |
| --- | --- | --- |
| 無法載入控制台代理 UI | 代理安裝失敗 | • 驗證服務管理員服務是否處於活動狀態。<br>• 驗證所有容器是否正在運作。<br>• 確保您的防火牆允許存取連接埠 8888 的服務。<br>• 如果仍有問題，請聯絡客服。 |
| 無法存取NetApp代理程式 UI | 嘗試存取代理程式的 IP 位址時會出現此訊息。如果代理沒有正確的網路存取權限或不穩定，則代理程式可能無法初始化。 | • 連接到控制台代理。<br>• 驗證 Service Manager 服務<br>• 驗證代理是否具有所需的網路存取權限。"了解有關所需網路存取端點的更多資訊。" |
| 無法載入代理設定 | 當您嘗試造訪代理設定頁面時，控制台會顯示此訊息。 | • 檢查 OCCM 容器是否正在運作並正常運作。<br>• 如果問題仍然存在，請聯絡支援人員。 |

| 錯誤訊息 | 解釋 | 該怎麼辦 |
| --- | --- | --- |
| 無法載入代理的支援資訊。 | 如果代理無法存取您的支援帳戶，則會顯示此訊息。 | • 確認代理程式擁有所需端點的出站存取權。"了解有關所需網路存取端點的更多資訊。" |

檢查控制台代理狀態

使用以下命令之一來驗證您的控制台代理。所有服務的狀態都應為「正在運作」。如果不是這種情況，請聯絡NetApp支援。

有關訪問控制台代理診斷的詳細信息，請參閱以下主題：

- "檢查控制台代理程式狀態（適用於 Linux 主機部署）"
- "檢查控制台代理程式狀態（針對 VCenter 部署）"

**Docker**（用於 **Ubuntu** 和 **VCenter** 部署）

```
docker ps -a
```

**Podman**（用於 **RedHat Enterprise Linux** 部署）

```
podman ps -a
```

查看控制台代理版本

查看控制台代理版本以確認升級或與您的NetApp代表共用。

步驟

1. 選擇*管理>支援>代理*。

   控制台在頁面頂部顯示版本。

驗證網路存取

確保控制台代理程式具有所需的網路存取權限。"了解有關所需網路存取點的更多資訊。"

對控制台代理運行配置檢查

從控制台或代理程式維護控制台對控制台代理程式執行設定檢查，以確保它們已連線。

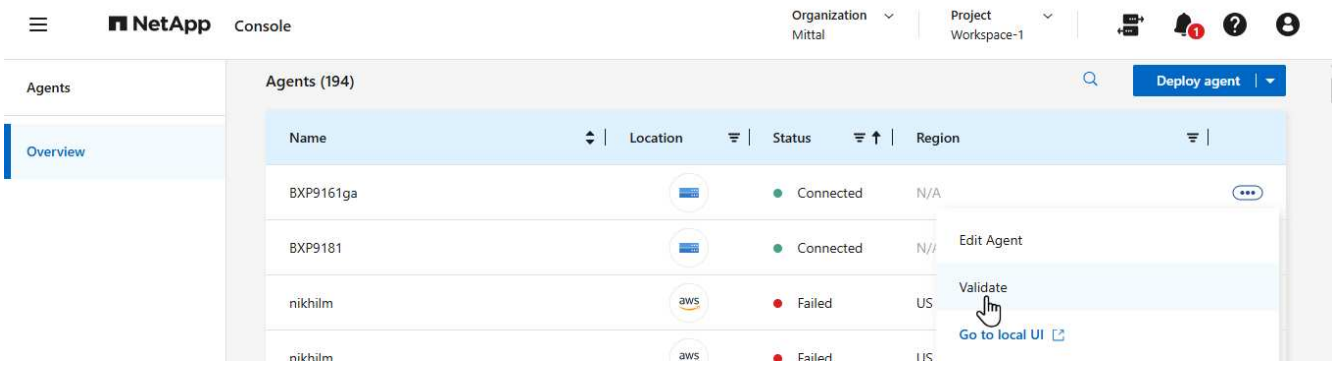
您也可以使用代理維護控制台執行設定檢查。"了解更多關於使用 config-checker validate 命令的資訊。"

您只能驗證狀態為「已連線」的代理程式。

控制台操作步驟

1. 選擇“管理 > 代理”。

2. 選擇要檢查的控制台代理程式的操作選單，然後選擇「驗證」。




驗證過程可能需要長達 15 分鐘。結果會在完成後顯示。

控制台代理安裝問題

如果安裝失敗，請查看報告和日誌以解決問題。

您也可以直接從下列目錄中的控制台代理主機存取 JSON 格式的驗證報表和設定日誌：

```
/tmp/netapp-console-agents/logs

/tmp/netapp-console-agents/results.json
```

- 對於新代理部署， NetApp會檢查以下端點："此處列出" 。如果您使用先前用於升級的端點，則此組態檢查將會失敗並出現錯誤，"此處列出" 。 NetApp建議您盡快更新防火牆規則，以允許存取目前端點並阻止存取先前的端點"了解如何更新您的網絡"。
- 如果您更新防火牆中的端點，您現有的代理程式將繼續運作。

停用手動安裝的設定檢查

有時您可能需要停用在安裝期間驗證出站連線的設定檢查。例如，在政府雲端環境中手動安裝代理程式時，需要停用設定檢查，否則安裝將失敗。

步驟

您可以透過在 *com/opt/application/netapp/service-manager-2/config.json* 檔案中設定 *skipConfigCheck* 標誌來停用設定檢查。預設情況下，此標誌設定為 false，且設定檢查會驗證代理程式的出站存取。將此標誌設為 true 以停用檢查。在完成此步驟之前，請先熟悉 JSON 語法。

若要重新啟用設定檢查，請使用下列步驟並將_skipConfigCheck_標誌設為false。

步驟

1. 以 root 身分或使用 sudo 權限存取控制台代理主機。
2. 建立 */opt/application/netapp/service-manager-2/config.json* 檔案的備份副本，以確保您可以還原變更。
3. 透過執行以下命令停止服務管理員 2 服務：

```
systemctl stop netapp-service-manager.service
```

1. 編輯 */opt/application/netapp/service-manager-2/config.json* 檔案並將 *skipConfigCheck* 標誌的值變更為 true。

```
  "skipConfigCheck": true
```

2. 儲存您的文件。
3. 透過執行以下命令重新啟動服務管理員 2 服務：

```
systemctl restart netapp-service-manager.service
```

#### 與NetApp支援部門合作

如果您無法解決控制台代理的問題，您可能需要聯絡NetApp支援。 NetApp支援人員可能會要求您提供控制台代理 ID，或者如果他們還沒有控制台代理程式日誌，則要求您將控制台代理程式日誌傳送給他們。

### 尋找控制台代理 ID

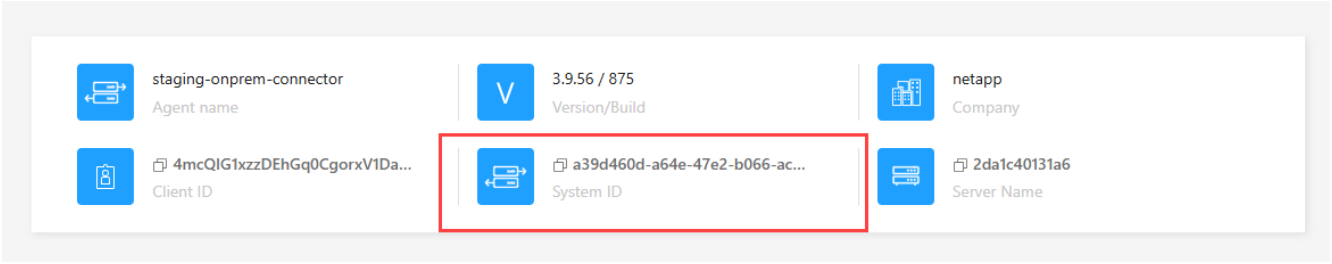
為了幫助您入門，您可能需要控制台代理的系統 ID。此 ID 通常用於許可和故障排除目的。

步驟

1. 選擇*管理>支援>代理*。

   您可以在頁面頂部找到系統 ID。

   例子




2. 將滑鼠懸停在 ID 上並單擊即可複製它。

### 下載或發送AutoSupport訊息

如果您遇到問題， NetApp可能會要求您向NetApp支援發送AutoSupport訊息以進行故障排除。

由於負載平衡， NetApp Console最多需要五個小時才能發送AutoSupport訊息。對於緊急通信，請下載文件並手動發送。

步驟

1. 選擇*管理>支援>代理*。
2. 根據您需要向NetApp支援發送訊息的方式，選擇以下選項之一：
   a. 選擇將AutoSupport訊息下載到本機的選項。然後，您可以使用首選方法將其傳送給NetApp支援。
   b. 選擇「發送AutoSupport」以將訊息直接傳送給NetApp支援。

#### 修復使用 **Google Cloud NAT** 閘道時下載失敗的問題

控制台代理程式會自動下載Cloud Volumes ONTAP 的軟體更新。如果您的設定使用 Google Cloud NAT 網關，可能會導致下載失敗。您可以透過限制軟體映像劃分的部分數來解決此問題。此步驟必須使用 API 完成。

步

1. 向 /occm/config 提交 PUT 請求，並將以下 JSON 作為正文：

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

   *maxDownloadSessions* 的值可以是 1 或任何大於 1 的整數。如果值為1，則下載的影像不會被分割。

   請注意，32 是一個範例值。該值取決於您的 NAT 配置和同時會話的數量。

"了解有關 /occm/config API 呼叫的更多信息"

#### 從**NetApp**知識庫取得協助

"查看NetApp支援團隊所建立的故障排除訊息" 。

### 解除安裝並刪除控制台代理

卸載控制台代理程式以解決問題或將其從主機中永久刪除。您需要使用的步驟取決於您使用的部署模式。從環境中刪除控制台代理程式後，您可以將其從控制台中刪除。

"了解NetApp Console部署模式" 。

#### 使用標準或受限模式時卸載代理

如果您使用的是標準模式或受限模式（換句話說，代理主機具有出站連線），那麼您應該按照下列步驟卸載代理程式。

步驟

1. 連接到代理程式的 Linux VM。
2. 從 Linux 主機執行卸載腳本：

   ```
   /opt/application/netapp/service-manager-2/uninstall.sh [silent]
   ```

   *silent* 運行腳本而不提示您確認。

從控制台中刪除控制台代理

如果您刪除了代理虛擬機器或卸載了代理，則應將其從控制台的代理清單中刪除。刪除代理虛擬機器或卸載代理軟體後，代理程式在控制台中顯示狀態為「已中斷連線」。

刪除控制台代理程式時請注意以下事項：

- 此操作不會刪除虛擬機器。
- 此操作無法恢復 - 一旦刪除控制台代理，就無法將其加回。

步驟

1. 選擇“管理 > 代理”。
2. 在「概覽」頁面上，選擇已中斷連線的代理程式的操作選單，然後選擇「移除代理程式」。
3. 輸入代理人的姓名進行確認，然後選擇*刪除*。

# 管理雲端提供者憑證

## AWS

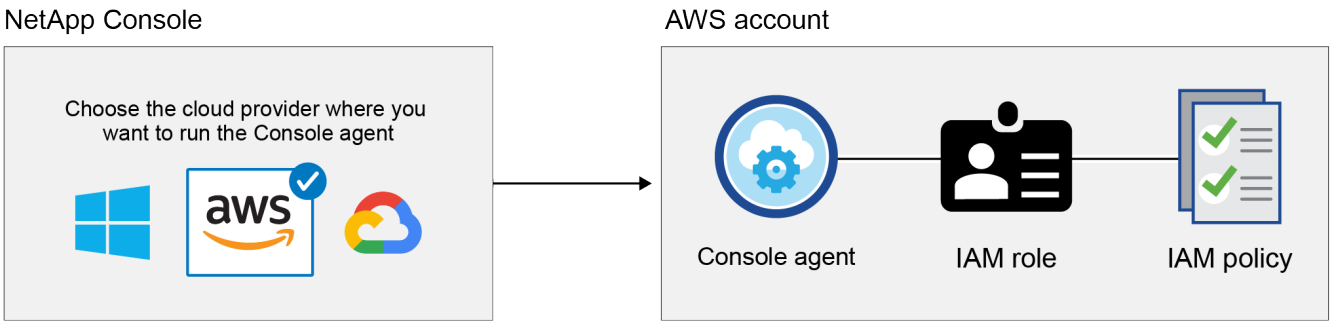
### 了解NetApp Console中的 AWS 憑證和權限

您可以透過NetApp Console直接管理 AWS 憑證和市集訂閱，透過在控制台代理部署期間提供適當的 IAM 憑證並將其與 AWS Marketplace 訂閱關聯以進行計費，來確保Cloud Volumes ONTAP和其他資料服務的安全部署。

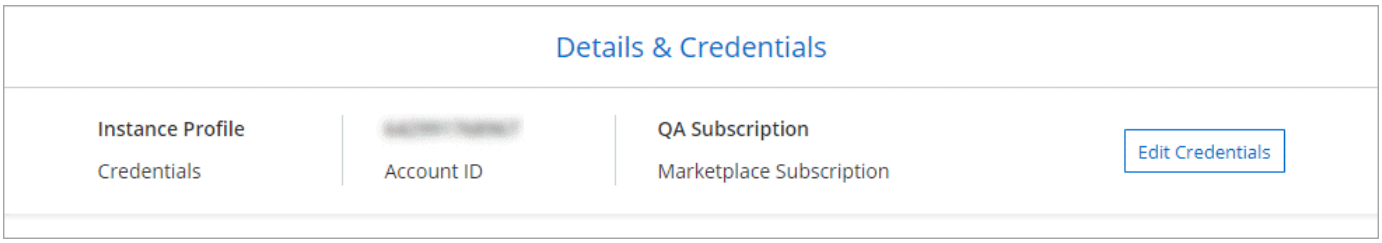
#### 初始 AWS 憑證

從控制台部署控制台代理程式時，您需要提供 IAM 角色的 ARN 或 IAM 使用者的存取金鑰。身份驗證方法必須具有在 AWS 中部署控制台代理程式的權限。所需權限列於表中"AWS代理部署策略"。

當控制台在 AWS 中啟動控制台代理時，它會為代理程式建立一個 IAM 角色和一個設定檔。它還附加了一項策略，為控制台代理提供管理該 AWS 帳戶內的資源和流程的權限。"查看代理如何使用權限"。




如果您新增的Cloud Volumes ONTAP系統，控制台將預設選擇以下 AWS 憑證：




使用初始 AWS 憑證部署所有Cloud Volumes ONTAP系統，或者您可以新增其他憑證。

額外的 **AWS** 憑證

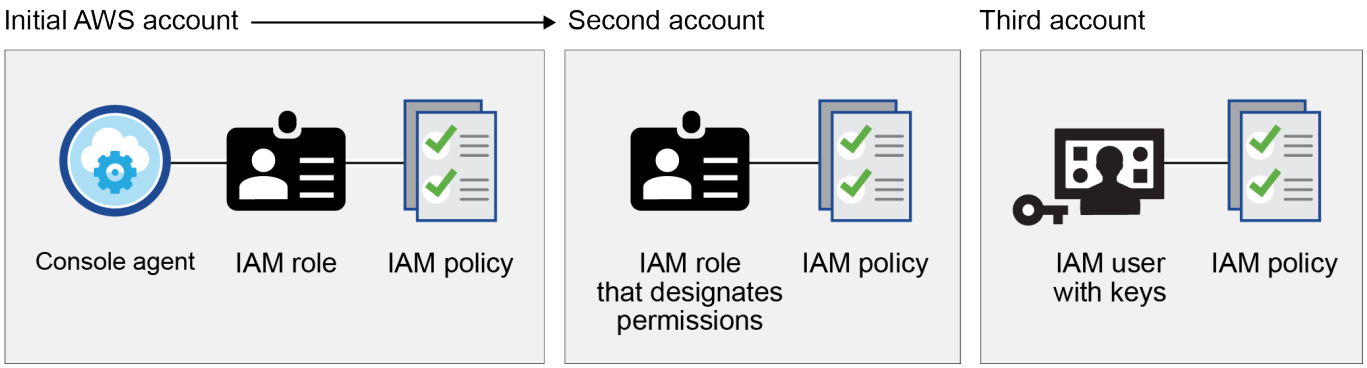
在下列情況下，您可能會為控制台新增其他 AWS 憑證：

- 若要將您現有的控制台代理程式與額外的 AWS 帳戶一起使用，請執行下列操作：
- 在特定 AWS 帳戶中建立新代理
- 建立和管理 FSx for ONTAP檔案系統

請參閱以下部分以了解更多詳細資訊。

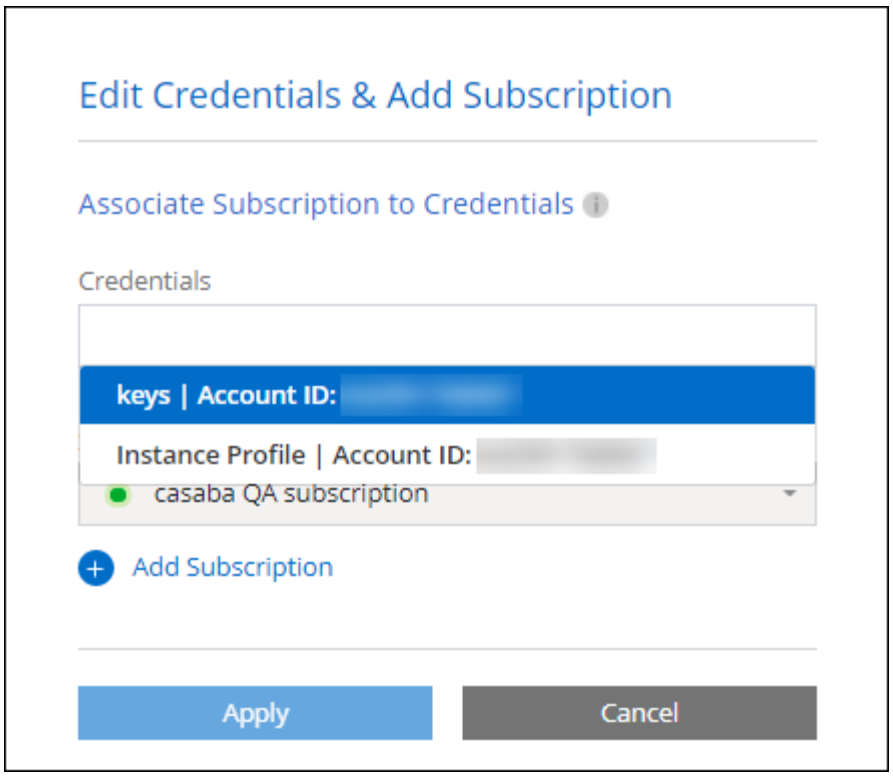
新增 **AWS** 憑證以將控制台代理程式與另一個 **AWS** 帳戶一起使用

若要將控制台與額外的 AWS 帳戶一起使用，請提供 AWS 金鑰或受信任帳戶中角色的 ARN。下圖顯示了兩個附加帳戶，一個透過受信任帳戶中的 IAM 角色提供權限，另一個透過 IAM 使用者的 AWS 金鑰提供權限：




您可以透過指定 IAM 角色的 Amazon 資源名稱 (ARN) 或 IAM 使用者的 AWS 金鑰，將帳戶憑證新增至控制台。

例如，您可以在建立新的Cloud Volumes ONTAP系統時在憑證之間切換：




"了解如何將 AWS 憑證新增至現有代理程式。"

新增 **AWS** 憑證以建立控制台代理

新增 AWS 憑證即可取得建立控制台代理的權限。

"了解如何將 AWS 憑證新增至控制台以建立控制台代理"

為 **FSx for ONTAP**新增 **AWS** 憑證

將 AWS 憑證新增至控制台以提供建立和管理 FSx for ONTAP系統所需的權限。

"了解如何將 AWS 憑證新增至Amazon FSx for ONTAP控制台"

憑證和市場訂閱

您必須將新增至控制台代理的憑證與 AWS Marketplace 訂閱關聯起來，才能按小時費率 (PAYGO) 支付Cloud Volumes ONTAP費用，並透過年度合約支付其他NetApp資料服務費用。"了解如何關聯 AWS 訂閱"。

請注意以下有關 AWS 憑證和市場訂閱的事項：

- 您只能將一個 AWS Marketplace 訂閱與一組 AWS 憑證關聯
- 您可以使用新的訂閱替換現有的市場訂閱

常問問題

以下問題與憑證和訂閱有關。

如何安全地輪換我的 **AWS** 憑證？

如上文所述，控制台可讓您透過幾種方式提供 AWS 憑證：與控制台代理程式關聯的 IAM 角色、在受信任的帳戶中承擔 IAM 角色或提供 AWS 存取金鑰。

對於前兩個選項，控制台使用 AWS 安全性令牌服務來取得不斷輪換的臨時憑證。這個流程是最佳實踐——它既自動化又安全。

如果您向控制台提供 AWS 存取金鑰，則應透過定期在控制台中更新金鑰來輪替金鑰。這是一個完全手動的過程。

我可以更改**Cloud Volumes ONTAP**系統的 **AWS Marketplace** 訂閱嗎？

是的，你可以。當您變更與一組憑證關聯的 AWS Marketplace 訂閱時，所有現有和新的Cloud Volumes ONTAP系統都會根據新訂閱收費。

"了解如何關聯 AWS 訂閱" 。

我可以新增多個 **AWS** 憑證，每個憑證都有不同的市場訂閱嗎？

屬於相同 AWS 帳戶的所有 AWS 憑證都將與相同 AWS Marketplace 訂閱相關聯。

如果您擁有屬於不同 AWS 帳戶的多個 AWS 憑證，則這些憑證可以與相同 AWS Marketplace 訂閱或不同的訂閱相關聯。

我可以將現有的**Cloud Volumes ONTAP**系統移至不同的 **AWS** 帳號嗎？

不可以，無法將與您的Cloud Volumes ONTAP系統關聯的 AWS 資源移至其他 AWS 帳戶。

憑證如何用於市場部署和本地部署？

以上部分描述了控制台代理的建議部署方法，即從控制台部署。您也可以從 AWS Marketplace 在 AWS 部署代理，也可以在您自己的 Linux 主機或 VCenter 中手動安裝控制台代理軟體。

如果您使用市場，則權限以相同的方式提供。您只需手動建立和設定 IAM 角色，然後為任何其他帳戶提供權限。

對於本機部署，您無法為控制台設定 IAM 角色，但可以使用 AWS 存取金鑰提供權限。

若要了解如何設定權限，請參閱以下頁面：

- 標準模式
  - "設定 AWS Marketplace 部署的權限"
  - "設定本地部署的權限"
- 限制模式
  - "設定限制模式的權限"

#### 管理**NetApp Console**的 **AWS** 憑證和市集訂閱

新增和管理 AWS 憑證，以便您從NetApp Console部署和管理 AWS 帳戶中的雲端資源。

# 如果您管理多個 AWS Marketplace 訂閱，則可以從「憑證」頁面將每個訂閱指派給不同的 AWS 憑證。

## 概況

您可以將 AWS 憑證新增至現有的控制台代理或直接新增至控制台：

- 為現有代理程式新增額外的 AWS 憑證

  將 AWS 憑證新增至控制台代理程式以管理雲端資源。了解如何將 AWS 憑證新增至控制台代理 。

- 將 AWS 憑證新增至控制台以建立控制台代理

  在控制台新增的 AWS 憑證可提供建立控制台代理程式所需的權限。了解如何將 AWS 憑證新增至NetApp Console 。

- 將 AWS 憑證新增至 FSx for ONTAP控制台

  將新的 AWS 憑證新增至控制台以建立和管理 FSx for ONTAP。 "了解如何設定 FSx for ONTAP 的權限"

## 如何輪換憑證

NetApp Console可讓您透過幾種方式提供 AWS 憑證：與代理程式實例關聯的 IAM 角色、在受信任的帳戶中承擔 IAM 角色或提供 AWS 存取金鑰。"了解有關 AWS 憑證和權限的更多信息" 。

對於前兩個選項，控制台使用 AWS 安全性令牌服務來取得不斷輪換的臨時憑證。這個過程是最佳實踐，因為它是自動的並且是安全的。

透過在控制台中更新來手動輪換 AWS 存取金鑰。

## 向控制台代理程式新增附加憑證

為控制台代理程式新增額外的 AWS 憑證，以便它具有管理公有雲環境中的資源和流程所需的權限。您可以提供另一個帳戶中的 IAM 角色的 ARN，也可以提供 AWS 存取金鑰。

"了解NetApp Console如何使用 AWS 憑證和權限"。

## 授予權限

在將 AWS 憑證新增至控制台代理之前授予權限。這些權限允許控制台代理程式管理該 AWS 帳戶內的資源和流程。您可以使用受信任帳戶或 AWS 金鑰中角色的 ARN 來提供權限。

如果您從控制台部署了控制台代理，它會自動為您部署控制台代理的帳戶新增 AWS 憑證。這確保了管理資源所需的必要權限。

## 選擇

- 透過承擔另一個帳戶中的 IAM 角色來授予權限
- 透過提供 AWS 金鑰授予權限

### 透過承擔另一個帳戶中的 **IAM** 角色來授予權限

您可以使用 IAM 角色在部署控制台代理程式的來源 AWS 帳戶與其他 AWS 帳戶之間建立信任關係。然後，您將向控制台提供來自受信任帳戶的 IAM 角色的 ARN。

如果控制台代理程式安裝在本機，則無法使用此驗證方法。您必須使用 AWS 金鑰。

步驟

1. 前往您想要為控制台代理提供權限的目標帳戶中的 IAM 控制台。
2. 在存取管理下，選擇*角色>建立角色*並依照步驟建立角色。

   請務必執行以下操作：

   - 在 受信任實體類型 下，選擇 **AWS** 帳戶。
   - 選擇“其他 AWS 帳戶”，並輸入控制台代理執行個體所在帳戶的 ID。
   - 透過複製並貼上以下內容來創建所需的策略"控制台代理的 IAM 策略"。
3. 複製 IAM 角色的角色 ARN，以便稍後將其貼上到控制台中。

結果

該帳戶具有所需的權限。現在您可以將憑證新增至控制台代理 。

### 透過提供 **AWS** 金鑰授予權限

如果您想要為 IAM 使用者提供具有 AWS 金鑰的控制台，則需要向該使用者授予所需的權限。控制台 IAM 政策定義了控制台允許使用的 AWS 操作和資源。

如果本機安裝了控制台代理，則必須使用此驗證方法。您不能使用 IAM 角色。

步驟

1. 從 IAM 控制台，透過複製並貼上以下內容來建立策略"控制台代理的 IAM 策略"。

   "AWS 文件：建立 IAM 原則"

2. 將策略附加到 IAM 角色或 IAM 使用者。
   - "AWS 文件：建立 IAM 角色"
   - "AWS 文件：新增和刪除 IAM 政策"

### 將憑證新增至現有代理

為 AWS 帳戶提供所需權限後，您可以將該帳戶的憑證新增至現有代理程式。這使您可以使用相同的代理程式在該帳戶中啟動Cloud Volumes ONTAP系統。

您的雲端提供者中的新憑證可能需要幾分鐘才能生效。

步驟

1. 使用頂部導覽列選擇要新增憑證的控制台代理程式。
2. 在左側導覽列中，選擇“管理”>“憑證”。

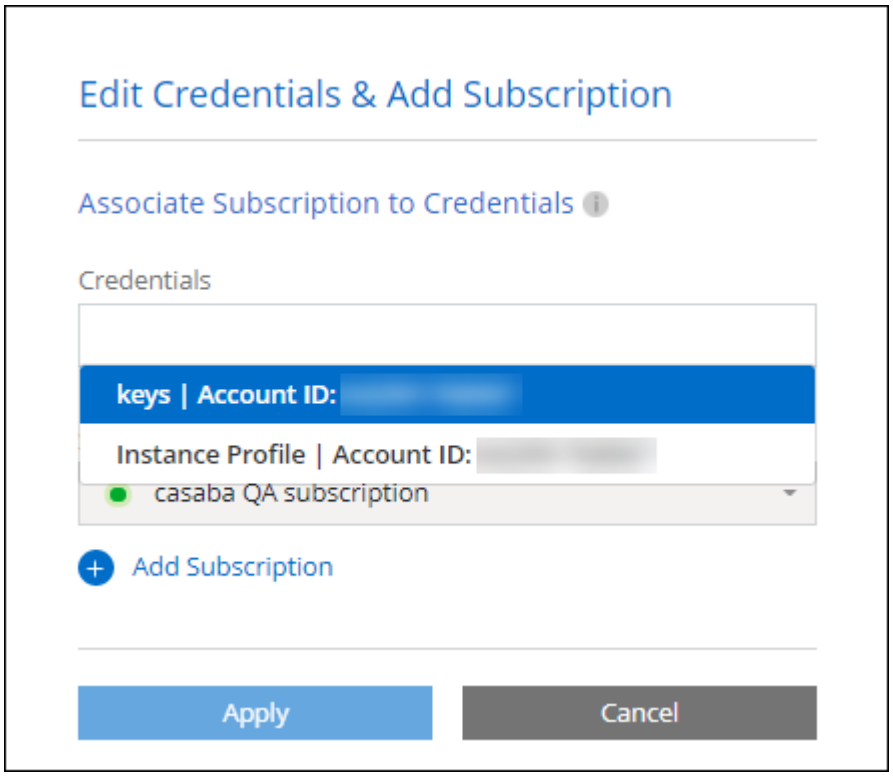
3. 在*組織憑證*頁面上，選擇*新增憑證*並按照精靈中的步驟進行操作。
   a. 憑證位置：選擇*Amazon Web Services > 代理*。
   b. 定義憑證：提供受信任的 IAM 角色的 ARN（Amazon 資源名稱），或輸入 AWS 存取金鑰和金鑰。
   c. 市場訂閱：透過立即訂閱或選擇現有訂閱將市場訂閱與這些憑證關聯。

      若要以小時費率（PAYGO）或年度合約支付服務費用，您必須將 AWS 憑證與您的 AWS Marketplace 訂閱關聯起來。

   d. 審核：確認有關新憑證的詳細資訊並選擇*新增*。

結果

現在，您可以在向控制台新增訂閱時從「詳細資料和憑證」頁面切換到不同的憑證集。




將憑證新增至控制台以建立控制台代理

透過提供 IAM 角色的 ARN 來新增 AWS 憑證，該角色授予建立控制台代理程式所需的權限。您可以在建立新代理時選擇這些憑證。

### 設定 **IAM** 角色

設定一個 IAM 角色，使NetApp Console軟體即服務 (SaaS) 層能夠承擔該角色。

步驟

1. 前往目標帳戶中的 IAM 控制台。
2. 在存取管理下，選擇*角色>建立角色*並依照步驟建立角色。

   請務必執行以下操作：

- 在 受信任實體類型 下，選擇 **AWS** 帳戶。
- 選擇「另一個 AWS 帳戶」並輸入NetApp Console SaaS 的 ID：9520133144444
- 具體來說，對於Amazon FSx for NetApp ONTAP ，編輯 信任關係 策略以包含「AWS」：「arn:aws:iam::952013314444:root」。

  例如，該策略應如下所示：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::952013314444:root",
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

+
參考"AWS 身分和存取管理 (IAM) 文檔"有關 IAM 中跨帳戶資源存取的詳細資訊。

- 建立一個包含建立控制台代理程式所需權限的策略。
  - "查看 FSx for ONTAP所需的權限"
  - "查看代理部署策略"

3. 複製 IAM 角色的角色 ARN，以便您可以在下一步中將其貼上到控制台中。

結果

IAM 角色現在具有所需的權限。現在您可以將其新增至控制台。

新增憑證

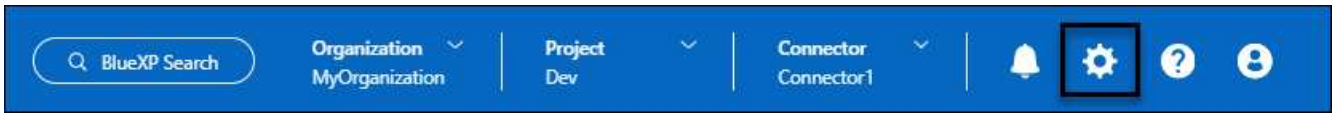
為 IAM 角色提供所需的權限後，將角色 ARN 新增至控制台。

開始之前

如果您剛剛建立了 IAM 角色，則可能需要幾分鐘才能使用它們。等待幾分鐘，然後將憑證新增至控制台。

步驟

1. 選擇“管理 > 憑證”。



2. 在*組織憑證*頁面上，選擇*新增憑證*並按照精靈中的步驟進行操作。
   a. 憑證位置：選擇*Amazon Web Services > 控制台*。
   b. 定義憑證：提供 IAM 角色的 ARN（Amazon 資源名稱）。
   c. 審核：確認有關新憑證的詳細資訊並選擇*新增*。

在**Amazon FSx for ONTAP**控制台新增憑證

有關詳細信息，請參閱 "Amazon FSx for ONTAP 的控制台文檔"

配置 **AWS** 訂閱

新增 AWS 憑證後，您可以使用這些憑證設定 AWS Marketplace 訂閱。透過訂閱，您可以按小時費率（PAYGO）或使用年度合約支付NetApp資料服務和Cloud Volumes ONTAP 的費用。

在新增憑證後，您可以在兩種情況下設定 AWS Marketplace 訂閱：

- 最初新增憑證時您沒有配置訂閱。
- 您想要變更已配置為 AWS 憑證的 AWS Marketplace 訂閱。

  用新的訂閱取代目前的市場訂閱會更改任何現有Cloud Volumes ONTAP系統和所有新系統的市場訂閱。

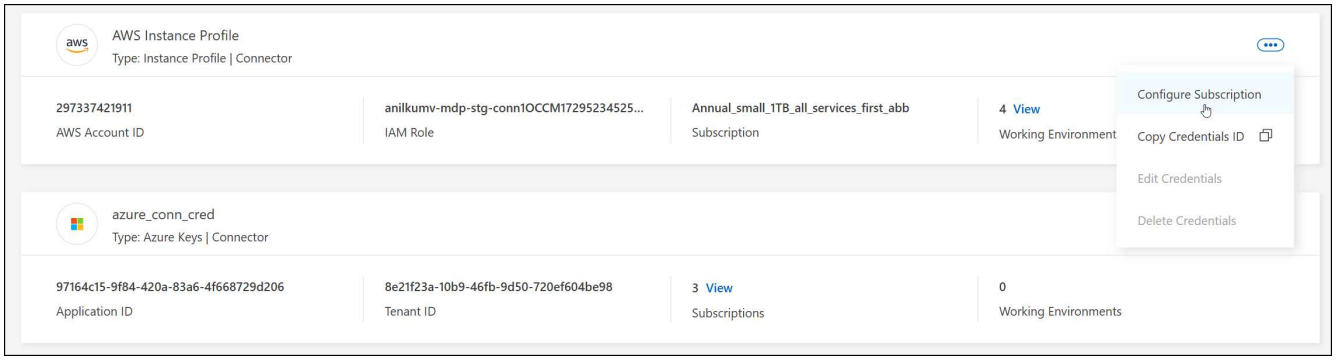
開始之前

您需要先建立控制台代理，然後才能設定訂閱。"了解如何建立控制台代理"。

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*。

將現有訂閱與您的組織關聯

當您從 AWS Marketplace 訂閱時，流程的最後一步是將訂閱與您的組織關聯。如果您沒有完成此步驟，那麼您就無法在您的組織中使用該訂閱。

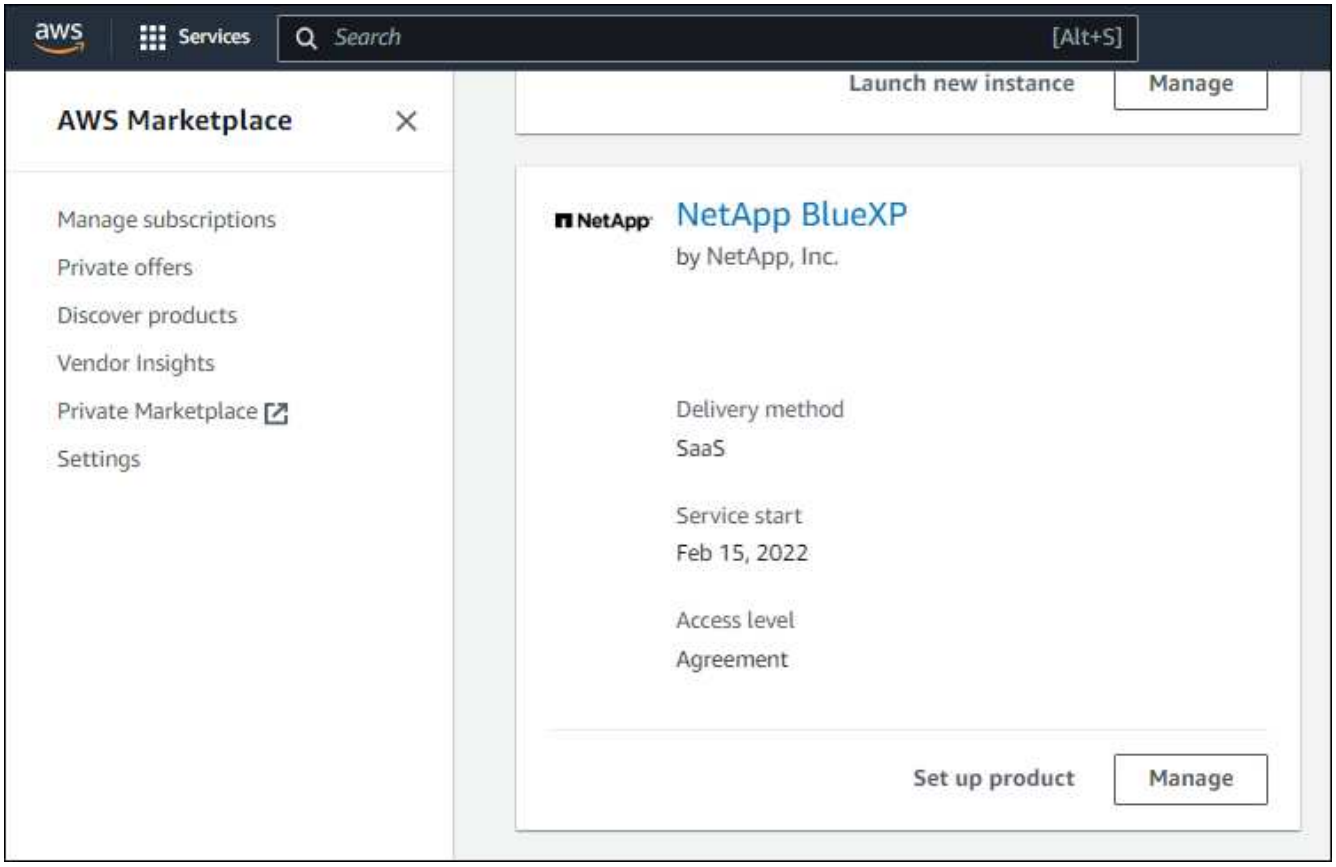
- "了解控制台部署模式"
- "了解控制台身分和存取管理"

如果您從 AWS Marketplace 訂閱了NetApp Intelligent Services，但錯過了將訂閱與您的帳戶關聯的步驟，請按照以下步驟操作。

步驟

1. 確認您沒有將您的訂閱與您的控制台組織關聯。
   a. 從導覽選單中，選擇*管理>Licenses and subscriptions*。
   b. 選擇*訂閱*。
   c. 確認您的訂閱沒有出現。

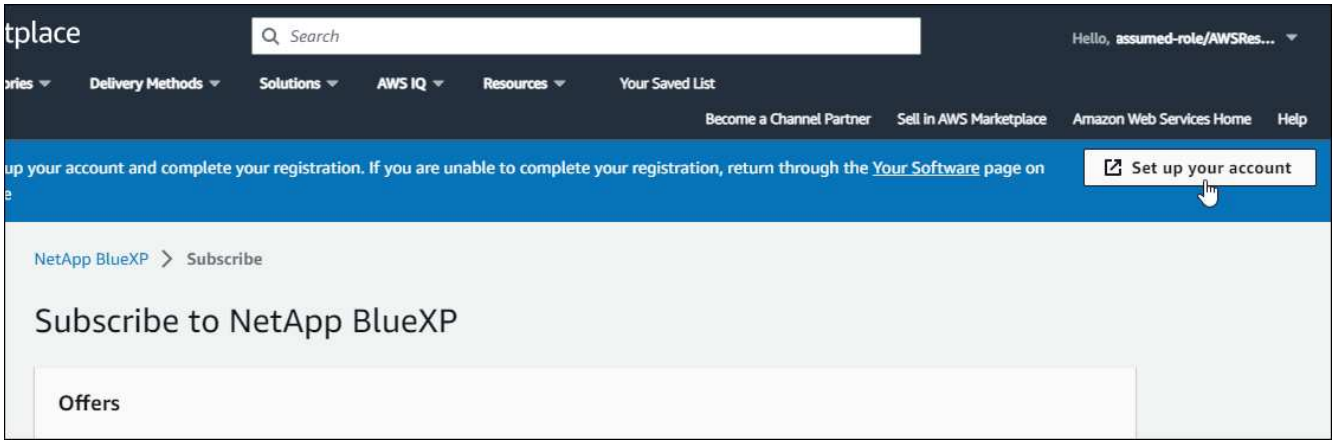
   您只會看到與您目前正在查看的組織或帳戶相關的訂閱。如果您沒有看到您的訂閱，請繼續執行以下步驟。
2. 登入 AWS 主控台並導覽至 **AWS Marketplace** 訂閱。
3. 尋找訂閱。




4. 選擇*設定產品*。

   訂閱優惠頁面應在新的瀏覽器標籤或視窗中載入。

5. 選擇*設定您的帳戶*。




   netapp.com 上的 **Subscription Assignment** 頁面應在新瀏覽器標籤或視窗中載入。

   請注意，系統可能會提示您先登入控制台。

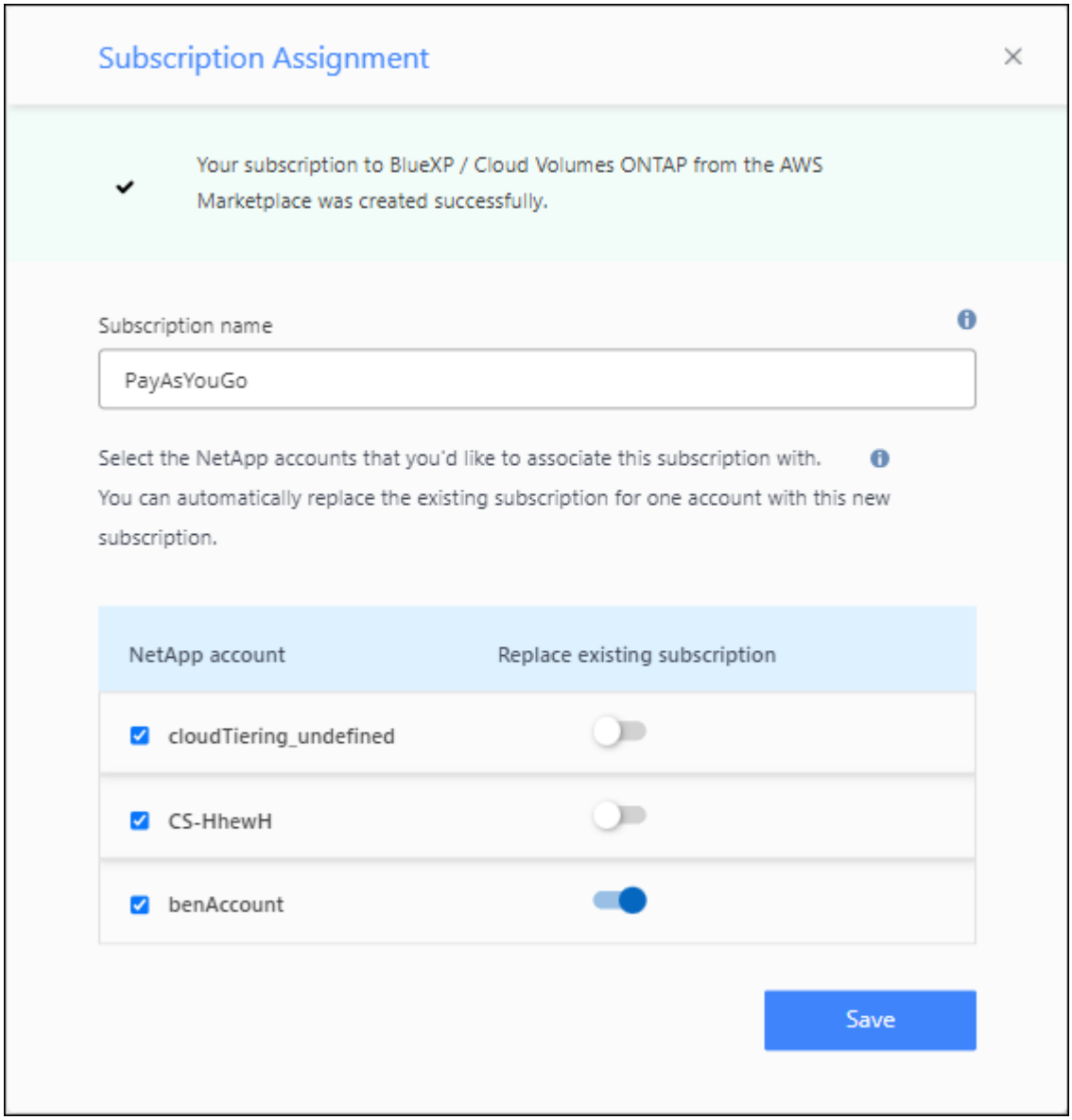
6. 從「訂閱分配」頁面：

   ◦ 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。

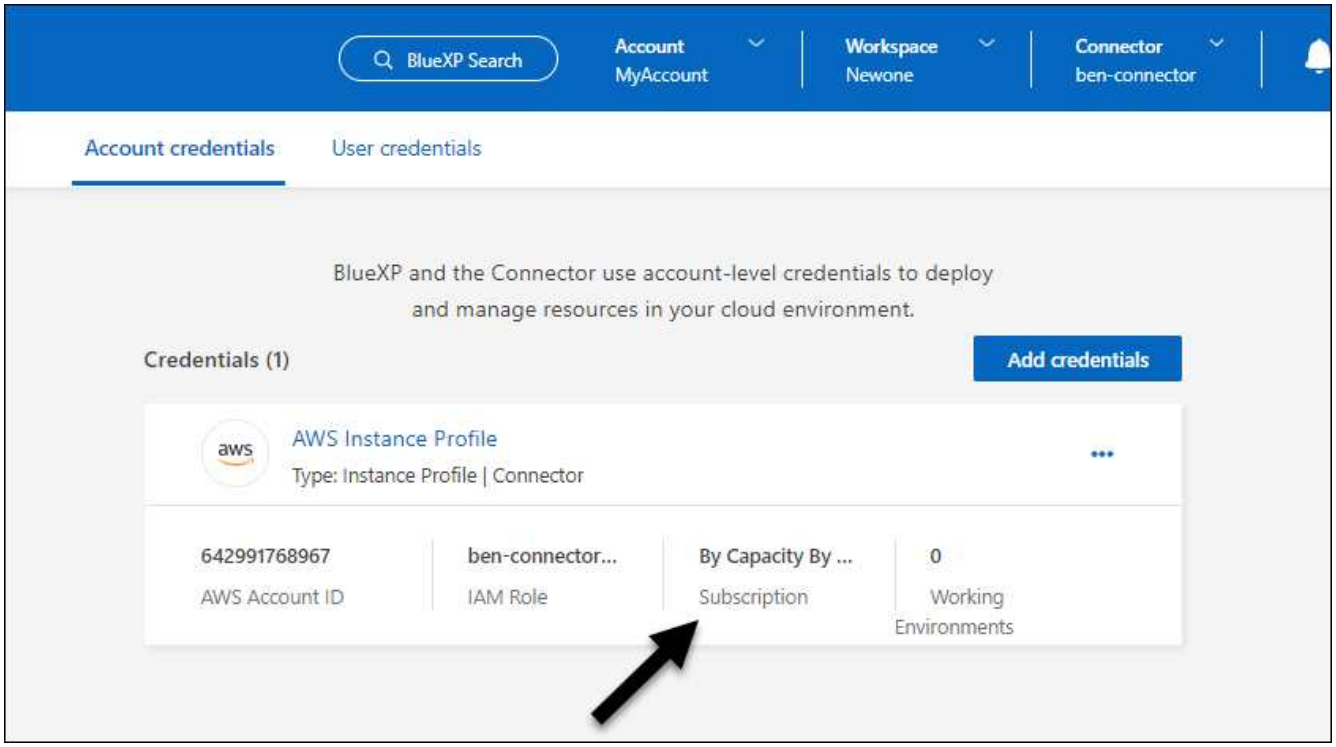
控制台將用這個新訂閱替換組織或帳戶中所有憑證的現有訂閱。如果一組憑證從未與訂閱關聯，那麼這個新訂閱將不會與這些憑證關聯。

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。




7. 確認訂閱與您的組織相關聯。
   a. 從導覽選單中，選擇*管理>許可證和訂閱*。
   b. 選擇*訂閱*。
   c. 驗證您的訂閱是否出現。
8. 確認訂閱與您的 AWS 憑證相關聯。
   a. 選擇“管理 > 憑證”。
   b. 在「組織憑證」頁面上，驗證訂閱是否與您的 AWS 憑證關聯。

這是一個例子。




編輯憑證

透過變更帳戶類型（AWS 金鑰或承擔角色）、編輯名稱或更新憑證本身（金鑰或角色 ARN）來編輯您的 AWS 憑證。

您無法編輯與控制台代理實例或Amazon FSx for ONTAP實例關聯的實例設定檔的憑證。您只能重新命名 FSx for ONTAP實例的憑證。

步驟

1. 選擇“管理 > 憑證”。
2. 在*組織憑證*頁面上，選擇一組憑證的操作選單，然後選擇*編輯憑證*。
3. 進行所需的更改，然後選擇*應用*。

刪除憑證

如果您不再需要一組憑證，您可以刪除它們。您只能刪除與系統無關的憑證。

您無法刪除與控制台代理程式關聯的實例設定檔的憑證。

步驟

1. 選擇“管理 > 憑證”。
2. 在*組織憑證*或*帳戶憑證*頁面上，選擇一組憑證的操作選單，然後選擇*刪除憑證*。
3. 選擇*刪除*進行確認。

## Azure

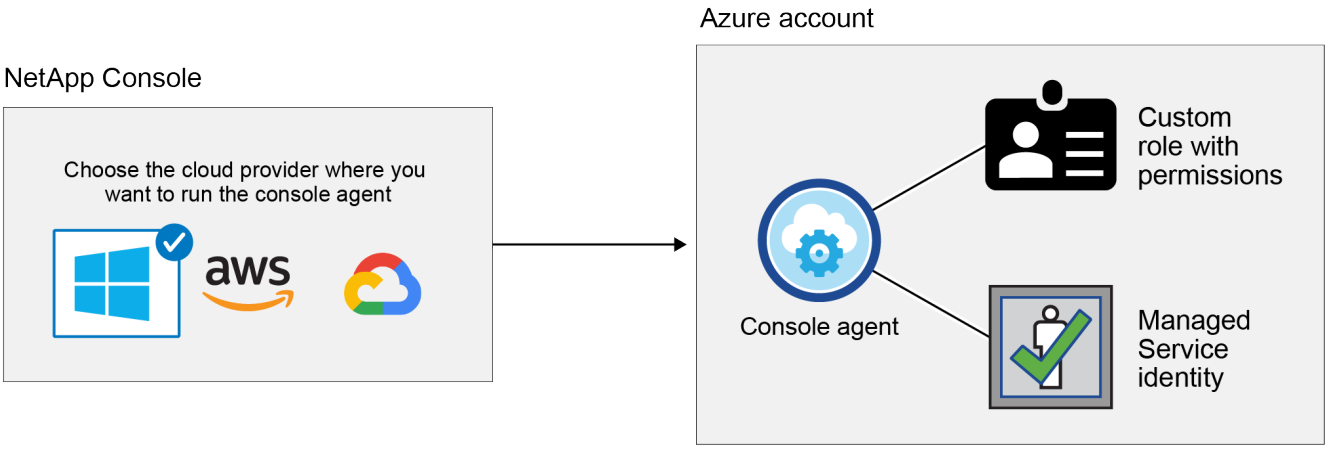
了解NetApp Console中的 Azure 憑證和權限

# 了解NetApp Console如何使用 Azure 憑證代表您執行操作以及這些憑證如何與市場訂閱相關聯。了解這些詳細資訊有助於您管理一個或多個 Azure 訂閱的憑證。例如，您可能想了解何時在控制台新增其他 Azure 憑證。

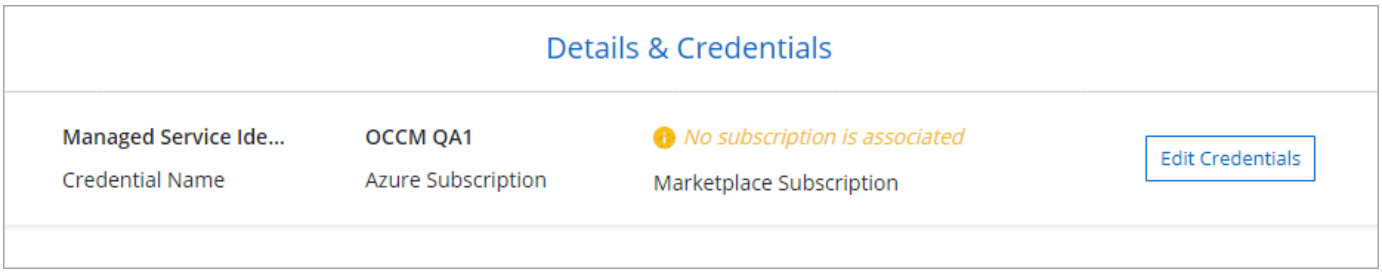
### 初始 Azure 憑證

從控制台部署控制台代理程式時，您需要使用具有部署控制台代理虛擬機器權限的 Azure 帳戶或服務主體。所需權限列於"Azure 的代理程式部署策略"。

當控制台在 Azure 中部署控制台代理虛擬機器時，它會啟用 "系統分配的託管標識"在虛擬機器上，建立自訂角色，並將其指派給虛擬機器。此角色為控制台提供管理該 Azure 訂閱內的資源和流程所需的權限。"查看控制台如何使用權限" 。




如果您為Cloud Volumes ONTAP建立新系統，控制台將預設選擇以下 Azure 憑證：




您可以使用初始 Azure 憑證部署所有Cloud Volumes ONTAP系統，也可以新增其他憑證。

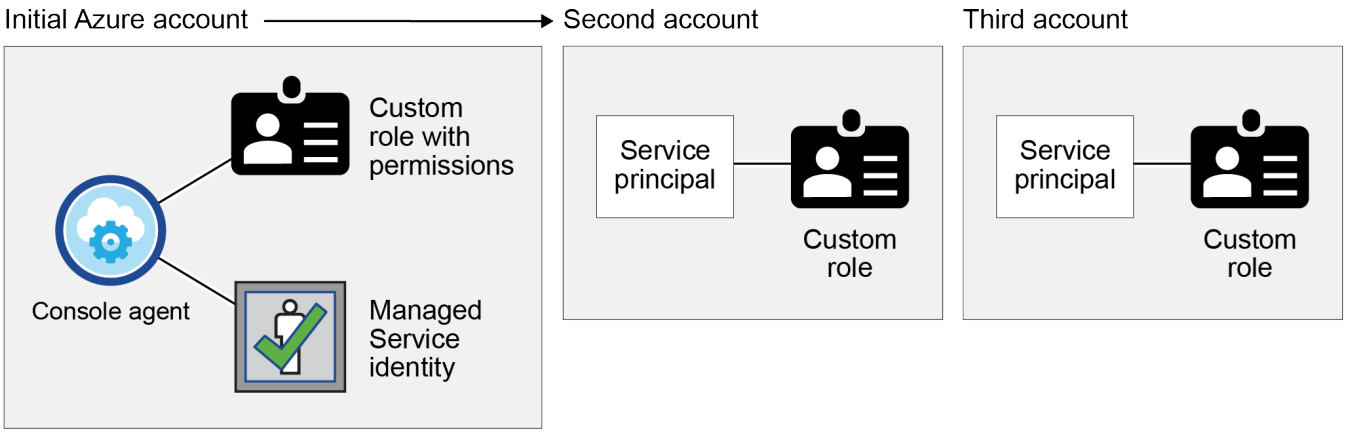
### 託管識別碼的其他 Azure 訂閱

指派給控制台代理程式 VM 的系統指派託管識別碼與您啟動控制台代理程式的訂閱相關聯。如果您想要選擇不同的 Azure 訂閱，則需要"將託管識別碼與這些訂閱關聯"。

### 其他 Azure 憑證

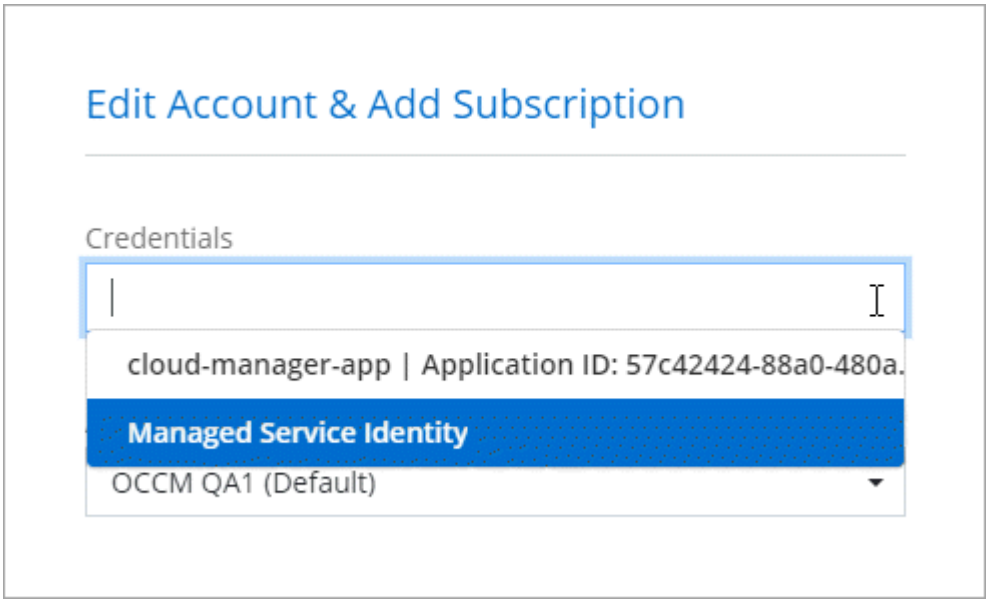
如果要在控制台中使用不同的 Azure 憑證，則必須透過以下方式授予所需的權限"在 Microsoft Entra ID 中建立和

設定服務主體"對於每個 Azure 帳戶。下圖顯示了另外兩個帳戶，每個帳戶都設定了服務主體和提供權限的自訂角色：




那你會"將帳戶憑證新增至控制台"透過提供有關 AD 服務主體的詳細資訊。

例如，您可以在建立新的Cloud Volumes ONTAP系統時在憑證之間切換：




憑證和市場訂閱

您新增至控制台代理程式的憑證必須與 Azure Marketplace 訂閱相關聯，以便您可以按小時費率（PAYGO）或NetApp資料服務或透過年度合約支付Cloud Volumes ONTAP費用。

"了解如何關聯 Azure 訂閱" 。

請注意有關 Azure 憑證和市集訂閱的以下事項：

- 只能將一個 Azure 市集訂閱與一組 Azure 憑證關聯
- 您可以使用新的訂閱替換現有的市場訂閱

常問問題

以下問題與憑證和訂閱有關。

我可以更改**Cloud Volumes ONTAP**系統的 **Azure Marketplace** 訂閱嗎？

是的，你可以。當您變更與一組 Azure 憑證關聯的 Azure 市場訂閱時，所有現有和新的Cloud Volumes ONTAP系統都會根據新訂閱收費。

"了解如何關聯 Azure 訂閱" 。

我可以新增多個 **Azure** 憑證，每個憑證都有不同的市場訂閱嗎？

屬於相同 Azure 訂閱的所有 Azure 憑證都將與相同 Azure 市場訂閱相關聯。

如果您有屬於不同 Azure 訂閱的多個 Azure 憑證，則這些憑證可以與同一個 Azure 市場訂閱或不同的市集訂閱相關聯。

我可以將現有的**Cloud Volumes ONTAP**系統移至不同的 **Azure** 訂閱嗎？

不可以，無法將與您的Cloud Volumes ONTAP系統關聯的 Azure 資源移至其他 Azure 訂閱。

憑證如何用於市場部署和本地部署？

以上部分描述了控制台代理的建議部署方法，即從控制台部署。您也可以從 Azure 市場在 Azure 中部署控制台代理，並且可以在自己的 Linux 主機上安裝控制台代理軟體。

如果您使用 Marketplace，您可以透過向控制台代理 VM 和系統指派的託管身分指派自訂角色來提供權限，或者您可以使用 Microsoft Entra 服務主體。

對於本機部署，您無法為控制台代理程式設定託管標識，但可以使用服務主體提供權限。

若要了解如何設定權限，請參閱以下頁面：

- 標準模式
  - "設定 Azure 市場部署的權限"
  - "設定本地部署的權限"
- 限制模式
  - "設定限制模式的權限"

管理**NetApp Console**的 **Azure** 憑證和市集訂閱

# 新增和管理 Azure 憑證，以便NetApp Console具有在 Azure 訂閱中部署和管理雲端資源所需的權限。如果您管理多個 Azure 市場訂閱，則可以從「憑證」頁面將每個訂閱指派給不同的 Azure 憑證。

概況

有兩種方法可以在控制台中新增額外的 Azure 訂閱和憑證。

1. 將其他 Azure 訂閱與 Azure 託管識別碼關聯。
2. 若要使用不同的 Azure 憑證部署Cloud Volumes ONTAP ，請使用服務主體授予 Azure 權限並將其憑證新增至控制台。

### 將其他 **Azure** 訂閱與託管識別關聯**Associate additional Azure subscriptions with a managed identity**

控制台可讓您選擇要部署Cloud Volumes ONTAP 的Azure 憑證和 Azure 訂閱。除非關聯 "託管識別"透過這些訂閱。

#### 關於此任務

託管身分"初始 Azure 帳戶"當您從控制台部署控制台代理程式時。部署控制台代理程式時，控制台會將控制台操作員角色指派給控制台代理虛擬機器。

#### 步驟

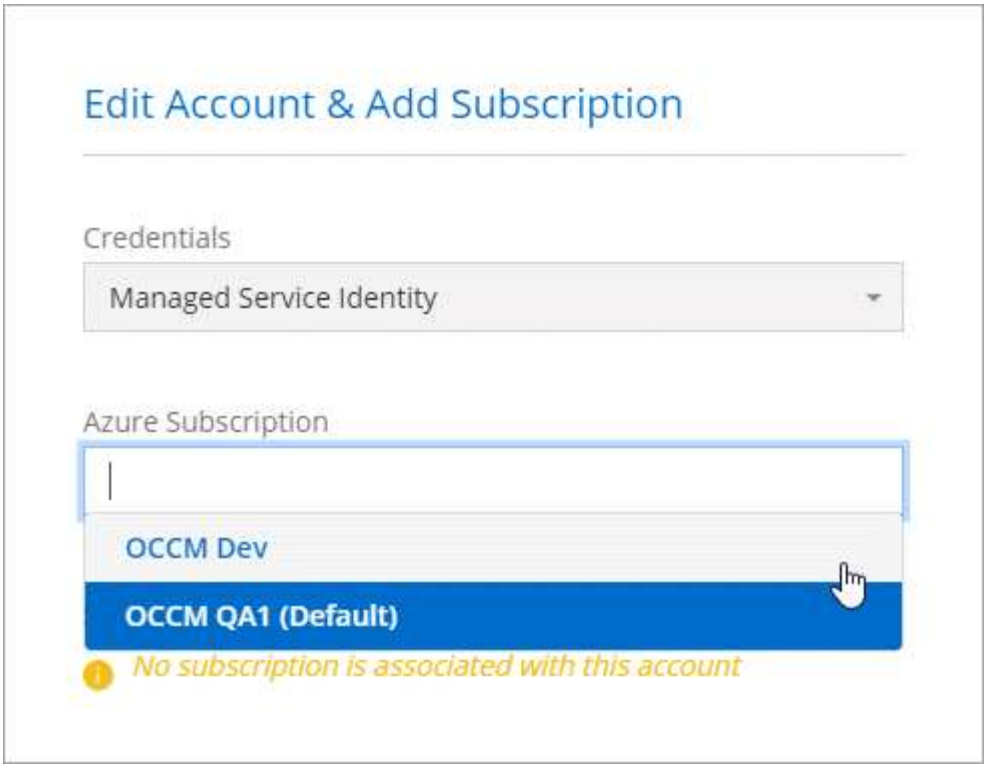
1. 登入 Azure 入口網站。
2. 開啟*訂閱*服務，然後選擇要部署Cloud Volumes ONTAP 的訂閱。
3. 選擇*存取控制 (IAM)*。
   a. 選擇 新增 > 新增角色分配，然後新增權限：
      - 選擇*控制台操作員*角色。

        控制台操作員是控制台代理程式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。

      - 分配對*虛擬機器*的存取權限。
      - 選擇建立控制台代理虛擬機器的訂閱。
      - 選擇一個控制台代理虛擬機器。
      - 選擇*儲存*。
4. 重複這些步驟以獲得更多訂閱。

#### 結果

建立新系統時，您現在可以從多個 Azure 訂閱中選擇託管識別設定檔。




### 為**NetApp Console**新增其他 **Azure** 憑證

從控制台部署控制台代理程式時，控制台會在具有所需權限的虛擬機器上啟用系統指派的託管識別碼。當您為Cloud Volumes ONTAP建立新系統時，控制台會預設選擇這些 Azure 憑證。

如果您在現有系統上手動安裝了控制台代理軟體，則不會新增初始憑證集。"了解 Azure 憑證和權限" 。

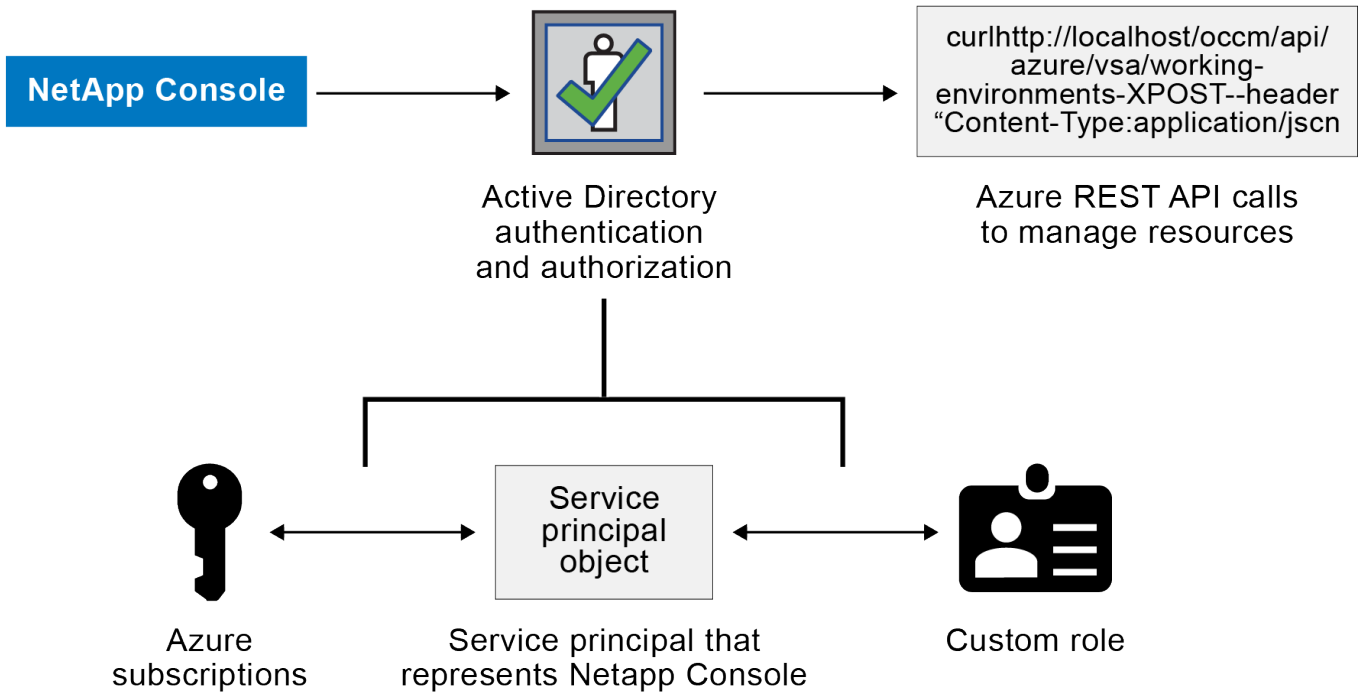
如果您想要使用不同的 Azure 憑證部署Cloud Volumes ONTAP ，則必須透過在 Microsoft Entra ID 中為每個 Azure 帳戶建立和設定服務主體來授予所需的權限。然後，您可以將新憑證新增至控制台。

#### 使用服務主體授予 **Azure** 權限

控制台需要權限才能在 Azure 中執行操作。您可以透過在 Microsoft Entra ID 中建立和設定服務主體並取得控制台所需的 Azure 憑證來授予 Azure 帳戶所需的權限。

##### 關於此任務

下圖描述了控制台如何取得在 Azure 中執行操作的權限。服務主體物件與一個或多個 Azure 訂閱綁定，代表 Microsoft Entra ID 中的控制台，並指派給允許所需權限的自訂角色。




步驟

1. 建立 Microsoft Entra 應用程式 。
2. [將應用程式指派給角色] 。
3. 新增 Windows Azure 服務管理 API 權限 。
4. 取得應用程式ID和目錄ID 。
5. [建立客戶端機密] 。

建立 **Microsoft Entra** 應用程式

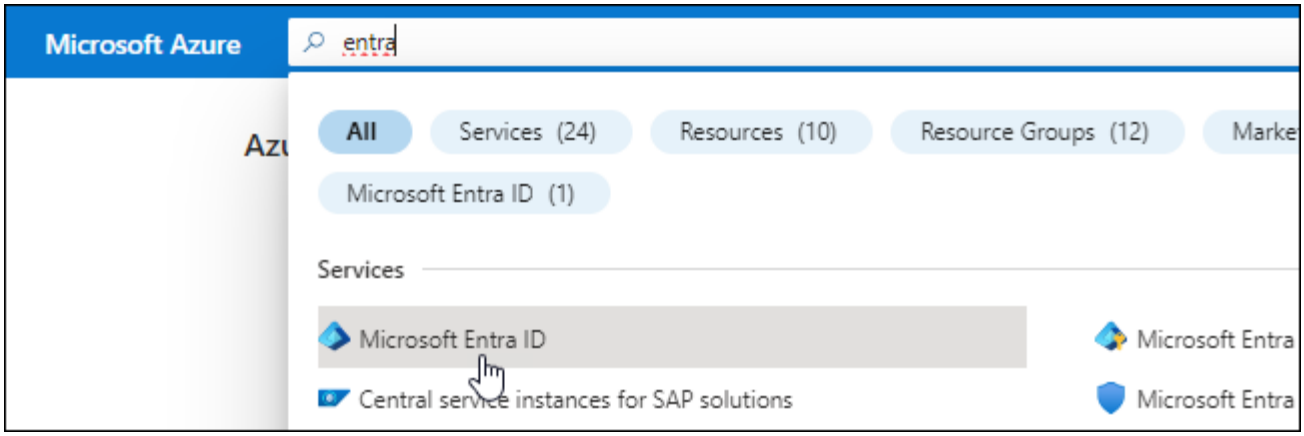
建立控制台可用於基於角色的存取控制的 Microsoft Entra 應用程式和服務主體。

步驟

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

您必須將服務主體綁定至一個或多個 Azure 訂閱，並為其指派自訂「控制台操作員」角色，以便控制台在 Azure 中擁有權限。

步驟

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。

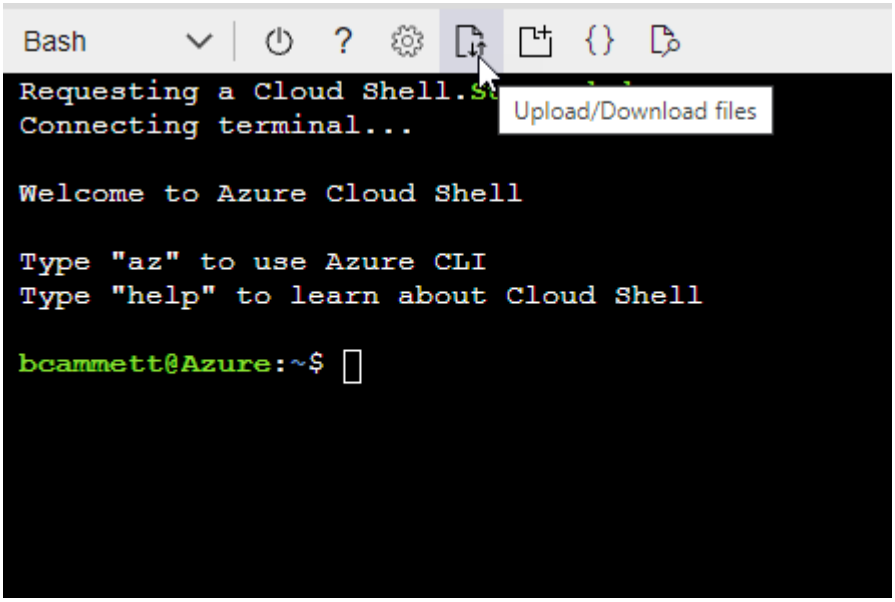
      例子

```
"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。

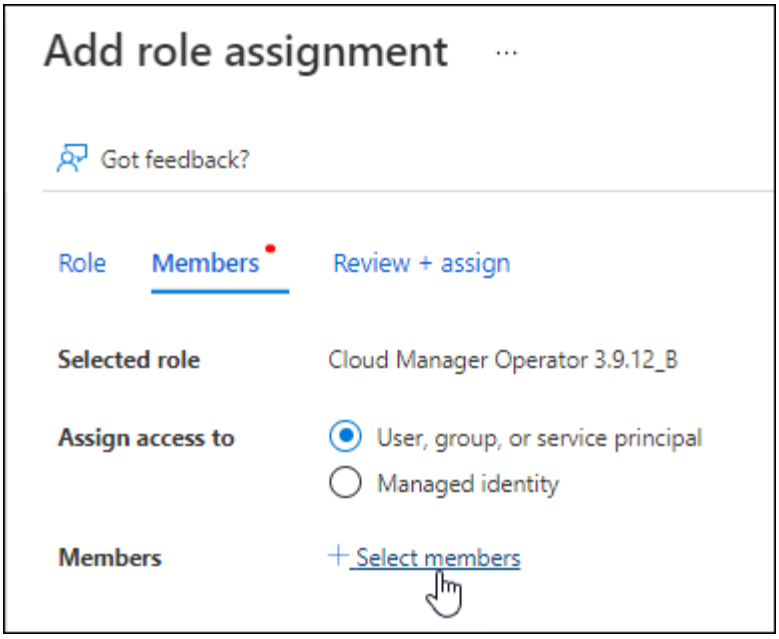
b. 選擇訂閱。

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*。

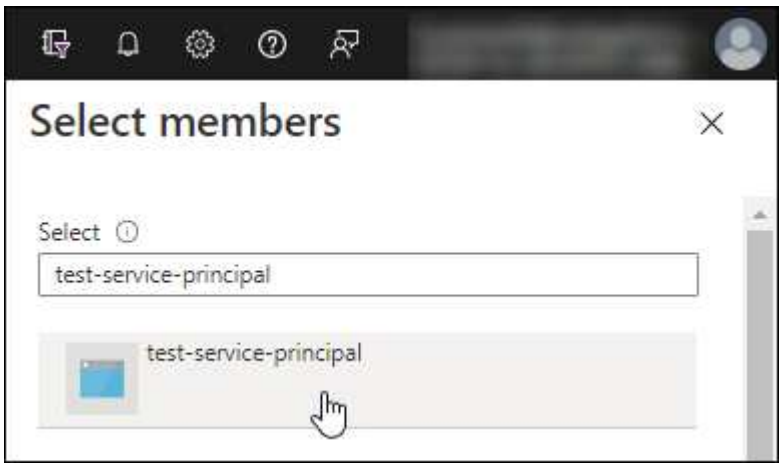
e. 在「成員」標籤中，完成以下步驟：

- 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。

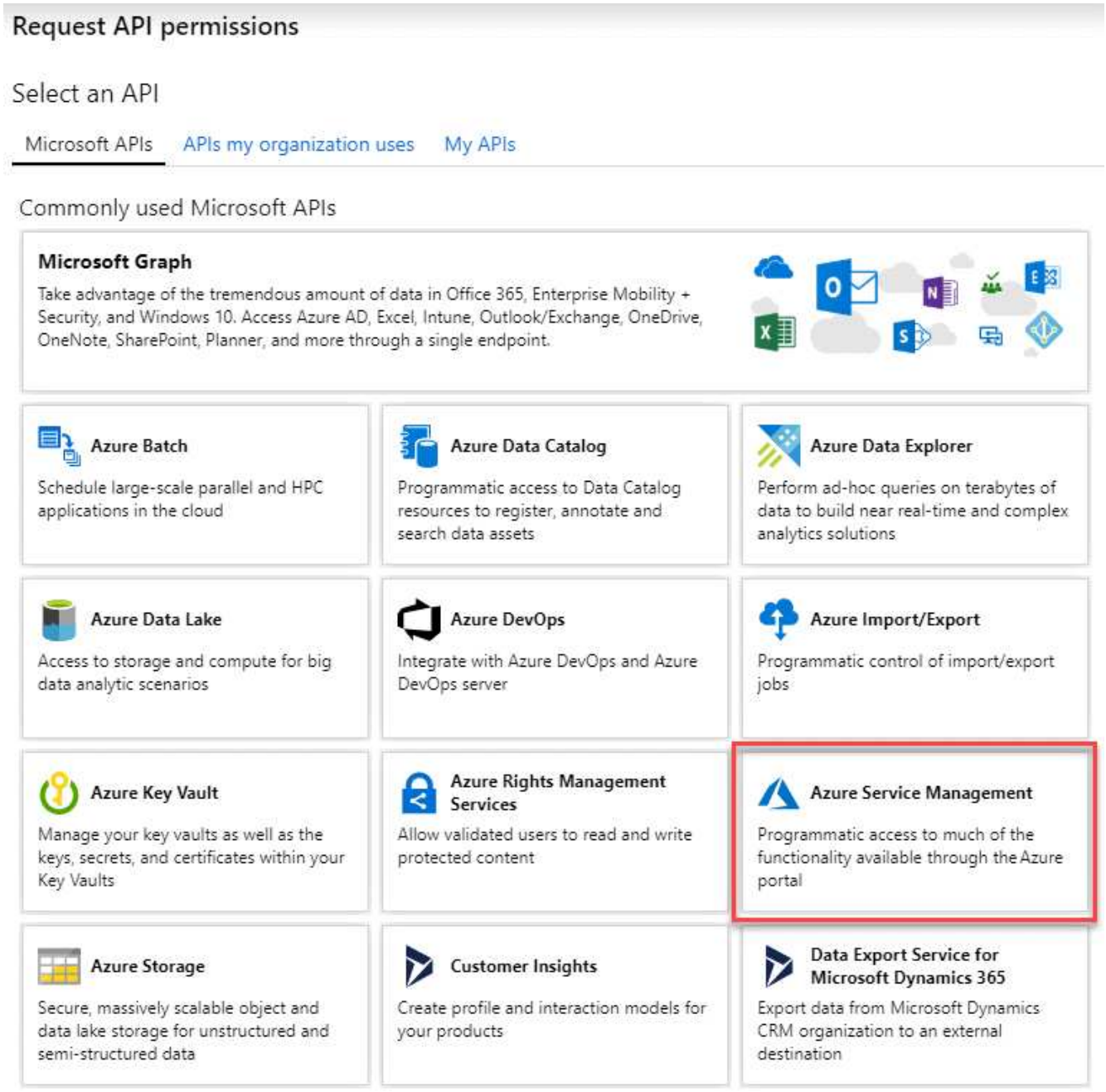
如果您想要從多個 Azure 訂閱部署Cloud Volumes ONTAP ，則必須將服務主體綁定到每個訂閱。在NetApp Console中，您可以選擇部署Cloud Volumes ONTAP時要使用的訂閱。

新增 **Windows Azure** 服務管理 **API** 權限

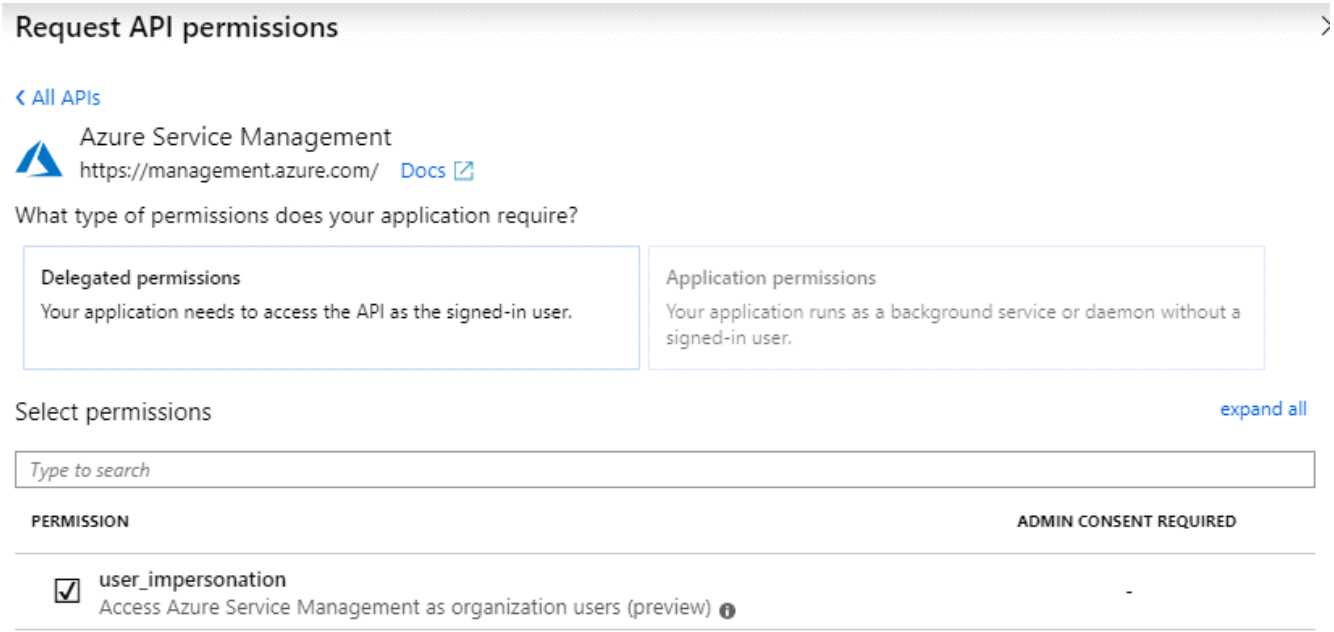
您必須為服務主體指派「Windows Azure 服務管理 API」權限。

步驟

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*。

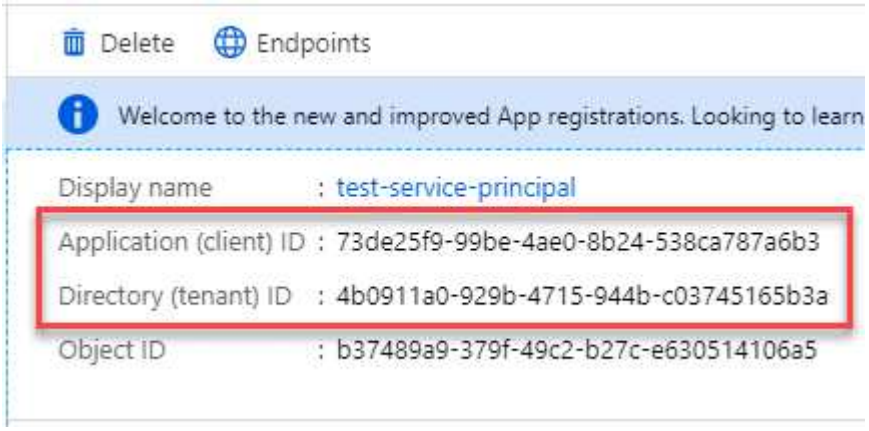



取得應用程式**ID**和目錄**ID**

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。

步驟

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

建立客戶端金鑰並將其值提供給控制台以使用 Microsoft Entra ID 進行身份驗證。

步驟

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置，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。

將憑證新增至控制台

為 Azure 帳戶提供所需權限後，您可以將該帳戶的憑證新增至控制台。完成此步驟後，您可以使用不同的 Azure 憑證啟動Cloud Volumes ONTAP 。

開始之前

如果您剛剛在雲端提供者中建立了這些憑證，則可能需要幾分鐘才能使用它們。等待幾分鐘，然後將憑證新增至控制台。

開始之前

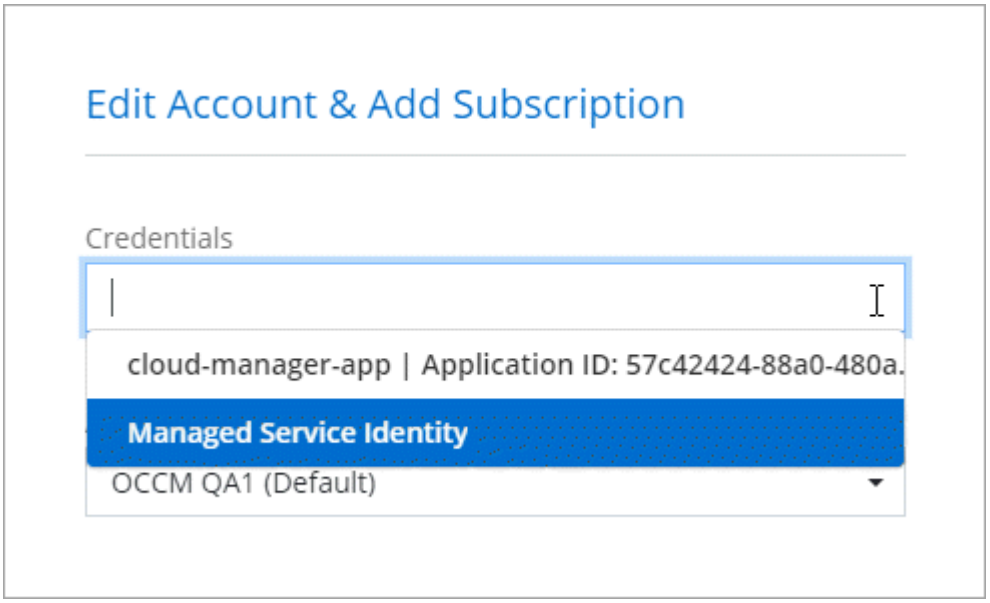
您需要先建立控制台代理，然後才能變更控制台設定。"了解如何建立控制台代理" 。

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

您可以從「詳細資料和憑證」頁面切換到另一組憑證 "將系統新增至控制台時"




管理現有憑證

透過關聯 Marketplace 訂閱、編輯憑證和刪除憑證來管理已新增至控制台的 Azure 憑證。

將 **Azure** 市場訂閱關聯到憑證

將 Azure 憑證新增至控制台後，您可以將 Azure 市集訂閱與這些憑證關聯。您可以使用訂閱來建立按使用量付費的Cloud Volumes ONTAP系統並存取NetApp資料服務。

將憑證新增至控制台後，可以在兩種情況下關聯 Azure 市集訂閱：

- 當您最初將憑證新增至控制台時，您沒有關聯訂閱。
- 您想要變更與 Azure 憑證關聯的 Azure 市集訂閱。

  取代目前的市場訂閱會針對現有和新的Cloud Volumes ONTAP系統進行更新。

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*。

編輯憑證

在控制台中編輯您的 Azure 憑證。例如，如果為服務主體應用程式建立了新的金鑰，您可以更新客戶端金鑰。

步驟

1. 選擇“管理 **>** 憑證”。
2. 選擇*組織憑證*。
3. 選擇一組憑證的操作選單，然後選擇*編輯憑證*。
4. 進行所需的更改，然後選擇*應用*。

刪除憑證

如果您不再需要一組憑證，您可以刪除它們。您只能刪除與系統無關的憑證。

步驟

1. 選擇“管理 **>** 憑證”。
2. 選擇*組織憑證*。
3. 在*組織憑證*頁面上，選擇一組憑證的操作選單，然後選擇*刪除憑證*。
4. 選擇*刪除*進行確認。

## Google雲

### 了解 Google Cloud 專案和權限

了解NetApp Console如何使用 Google Cloud 憑證代表您執行操作以及這些憑證如何與市場訂閱相關聯。了解這些詳細資訊有助於您管理一個或多個 Google Cloud 專案的憑證。例如，您可能想要了解與控制台代理 VM 關聯的服務帳戶。

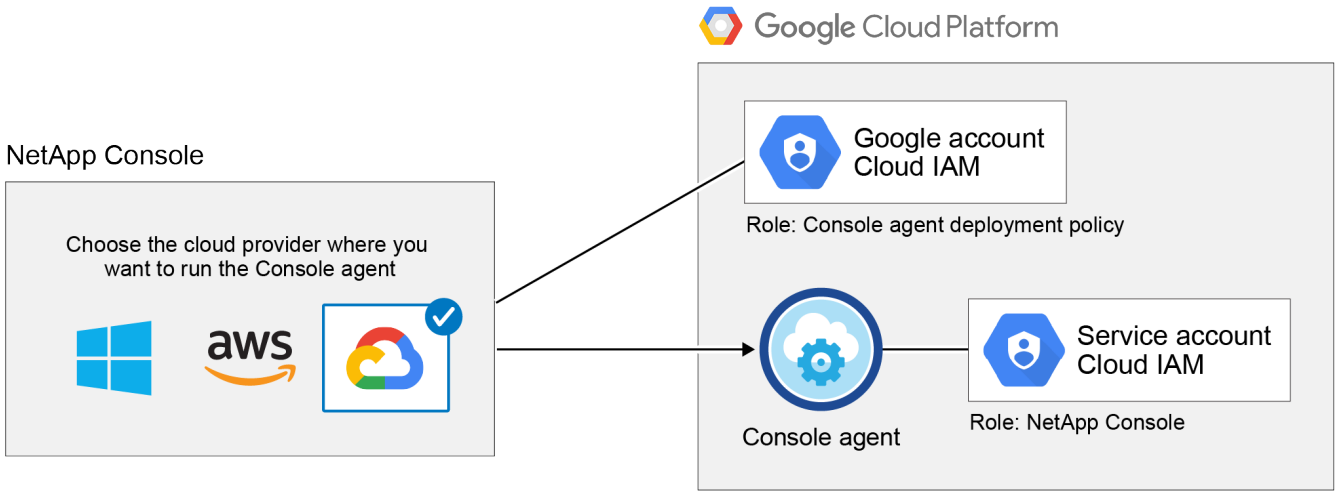
#### NetApp Console的專案和權限

您必須先部署控制台代理，然後才能使用控制台管理 Google Cloud 專案中的資源。代理程式不能在您的場所或不同的雲端提供者中運作。

直接從控制台部署控制台代理程式之前，必須具備兩組權限：

1. 您需要使用具有從控制台啟動控制台代理權限的 Google 帳戶部署控制台代理程式。
2. 部署控制台代理程式時，系統會提示您選擇 "服務帳戶"對於代理控制台從服務帳戶取得權限來建立和管理Cloud Volumes ONTAP系統、使用NetApp備份和還原管理備份等等。透過將自訂角色附加到服務帳戶來提供權限。

下圖描述了上面第 1 項和第 2 項中所述的權限要求：




若要了解如何設定權限，請參閱以下頁面：

- "設定標準模式的 Google Cloud 權限"
- "設定限制模式的權限"

憑證和市場訂閱

當您在 Google Cloud 中部署控制台代理程式時，控制台會為控制台代理程式所在專案中的 Google Cloud 服務帳號建立一組預設憑證。這些憑證必須與 Google Cloud Marketplace 訂閱相關聯，以便您可以支付Cloud Volumes ONTAP和NetApp資料服務的費用。

"了解如何關聯 Google Cloud Marketplace 訂閱" 。

請注意以下有關 Google Cloud 憑證和市場訂閱的事項：

- 一個控制台代理只能關聯一組 Google Cloud 憑證
- 您只能將一個 Google Cloud Marketplace 訂閱與憑證關聯
- 您可以使用新的訂閱替換現有的市場訂閱

**Cloud Volumes ONTAP項目**

Cloud Volumes ONTAP可以與控制台代理程式位於同一專案中，也可以位於不同的專案中。要在不同的專案中部署Cloud Volumes ONTAP ，您需要先將控制台代理服務帳戶和角色新增至該專案。

- "了解如何設定服務帳戶"

- "了解如何在 Google Cloud 中部署Cloud Volumes ONTAP並選擇項目"

管理 **Google Cloud** 的憑證和訂閱以使用 **NetApp Console**

您可以透過關聯市場訂閱並對訂閱流程進行故障排除，來管理與 Console 代理虛擬機器執行個體關聯的 Google Cloud 憑證。這兩項操作可確保您可以使用市場訂閱來支付資料服務費用。

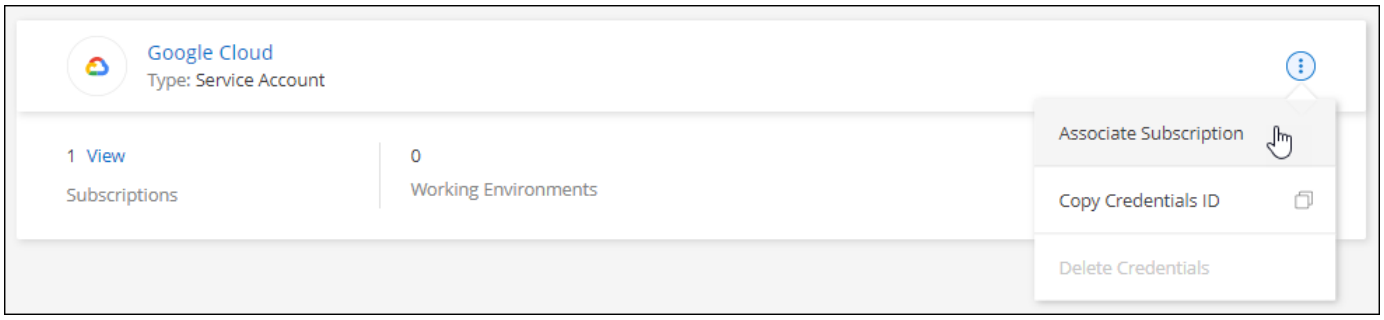
將 **Marketplace** 訂閱與 **Google Cloud** 憑證建立關聯

在 Google Cloud 中部署 Console 代理程式時，Console 會建立一組預設憑證，這些憑證與 Console 代理程式 VM 執行個體相關聯。您可以隨時變更與這些憑證相關聯的 Google Cloud Marketplace 訂閱。此訂閱可讓您建立隨用隨付的 Cloud Volumes ONTAP 系統，並使用其他資料服務。

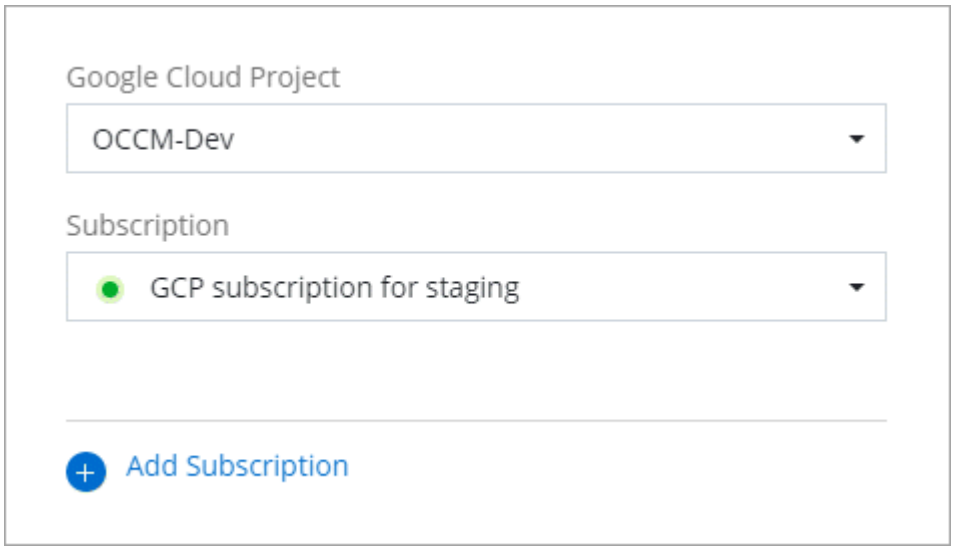
用新的訂閱取代目前的市場訂閱會更改任何現有Cloud Volumes ONTAP系統和所有新系統的市場訂閱。

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*。



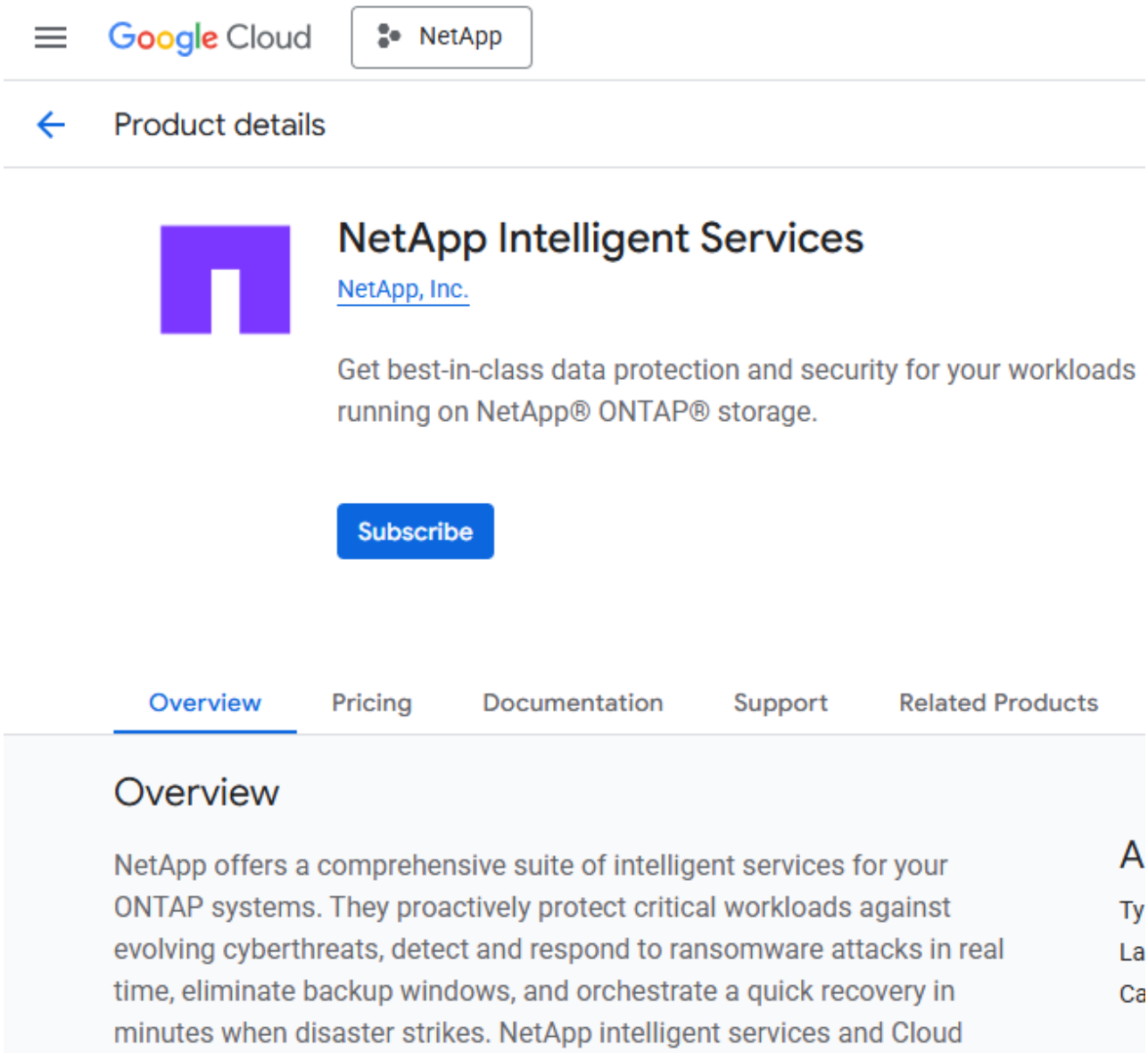

1. 若要使用選定的憑證設定現有訂閱，請從下拉清單中選擇一個 Google Cloud 專案和訂閱，然後選擇*設定*。



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。

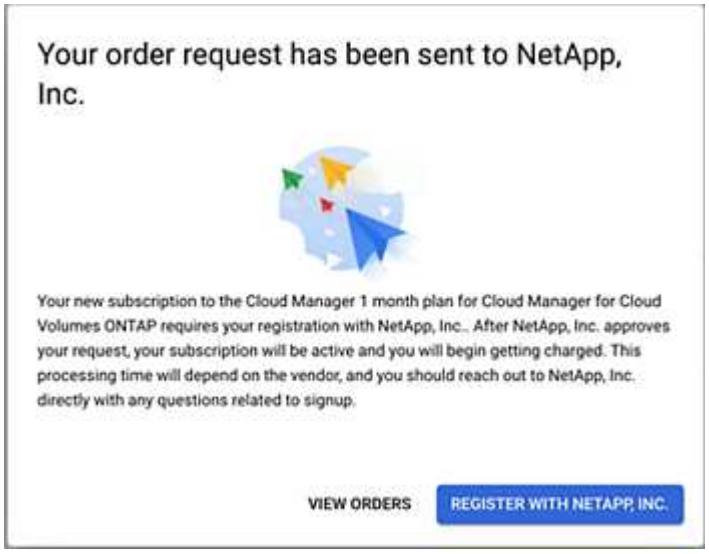
   d. 選擇*訂閱*。

      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。

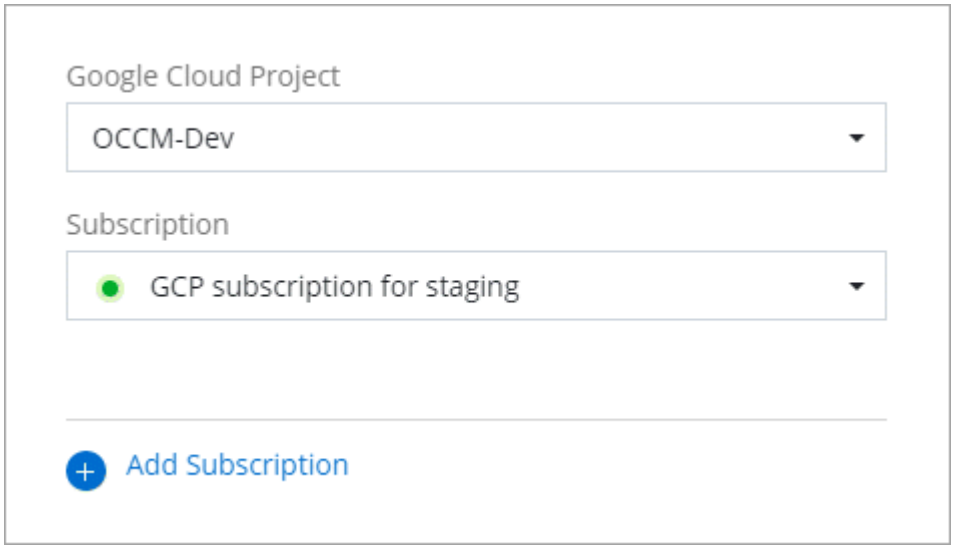
- 選擇您想要與此訂閱關聯的控制台組織。
- 在「取代現有訂閱」欄位中，選擇是否要用這個新訂閱自動取代組織的現有訂閱。

  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。

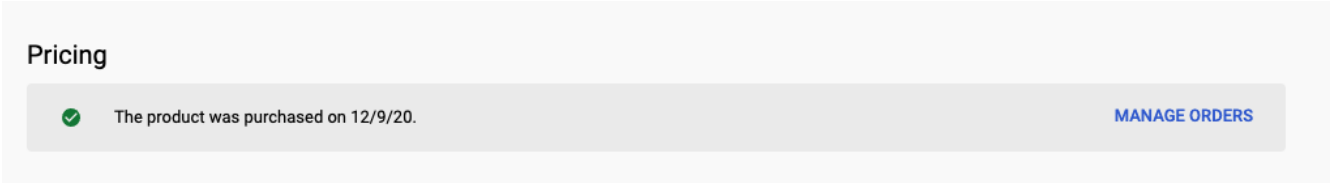


排解 **Marketplace** 訂閱程序問題

有時透過 Google Cloud Marketplace 訂閱 NetApp 資料服務可能會因為權限不正確或意外未遵循重新導向至 Console 而變得分散。如果發生這種情況，請使用以下步驟完成訂閱流程。

步驟

1. 導航至 "Google Cloud Marketplace 上的 NetApp 頁面"以查看訂單狀態。如果頁面顯示 **Manage on Provider**，請向下捲動並選擇 **Manage Orders**。




   - 如果訂單顯示綠色對勾，而這並非預期結果，則可能是組織內其他使用相同帳單帳戶的使用者已經訂閱了該服務。如果您對此感到意外或需要了解此訂閱的詳細資訊，請聯繫您的 NetApp 銷售團隊。


   - 如果訂單顯示時鐘和 **Pending** 狀態，請返回市場頁面並選擇 **Manage on Provider** 以按照上述說明完成流程。


# 身分和存取管理

## 了解**NetApp Console**身分和存取管理

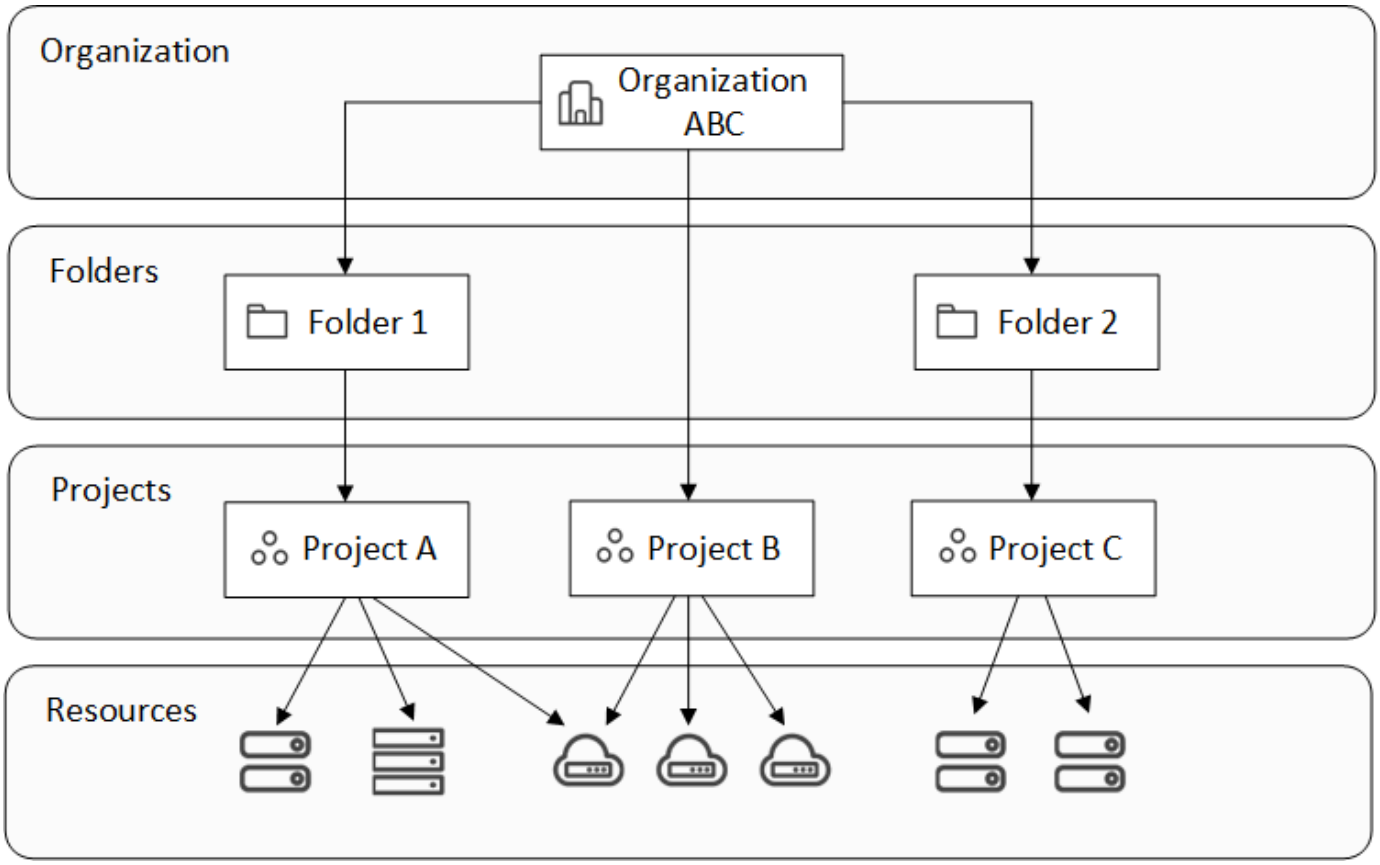
使用NetApp控制台的身分和存取管理 (IAM) 來組織您的NetApp資源，並根據您的業務結構（按位置、部門或專案）控制存取權限。

資源按層級排列：組織位於頂層，其次是資料夾（可以包含其他資料夾或項目），然後是項目，項目包含儲存系統、工作負載和代理。

在組織、資料夾或專案層級指派存取角色，以便使用者擁有對資源的正確存取權限。

> 您必須擁有_超級管理員_、_組織管理員_或_資料夾或專案管理員_角色才能在NetApp Console中管理 IAM。

下圖從基本層面說明了這個層次結構。




]

身分和存取管理元件

在NetApp Console中，您可以使用三個主要元件來組織儲存資源：組織元件、資源元件和使用者存取元件。

組織內的專案和資料夾

在您的 IAM 架構中，您使用三個組織元件：組織、專案和資料夾。您可以透過為使用者指派以下任何層級的角色來授予他們存取權限。

組織

_組織_是控制台 IAM 系統的頂層，通常代表您的公司。您的組織由資料夾、專案、成員、角色和資源組成。代理與組織內的特定項目相關聯。

專案

項目用於提供對儲存資源的存取。必須先將資源分配給項目，其他人才能存取這些資源。您可以將多個資源指派給一個項目，也可以建立多個項目。然後，您可以為使用者指派專案權限，使他們能夠存取專案中的資源。

例如，您可以根據需要，將本機ONTAP系統與單一專案或組織中的所有專案關聯起來。

"了解如何為您的組織新增項目。"

資料夾

將相關項目分組到_資料夾_中，以便按位置、站點或業務部門進行組織。您無法直接將資源與資料夾關聯，但將使用者指派到資料夾層級的角色，即可使其存取該資料夾中的所有項目。

"了解如何為您的組織新增資料夾。"

資源

資源 是指 NetApp Console 可識別並可指派給專案的實體。資源 包括儲存系統、Keystone 訂閱、部分 NetApp Backup and Recovery 工作負載以及 NetApp Console 代理。

+ 必須先將資源與項目關聯，其他人才能存取該資源。

+

例如，您可以將Cloud Volumes ONTAP系統與一個專案或組織中的所有專案關聯起來。資源的分配方式取決於貴組織的需求。

+

"了解如何將資源關聯到專案。"

儲存系統和**Keystone**訂閱

儲存系統是您在 NetApp Console 中管理的主要資源。NetApp Console 支援管理內部部署和雲端儲存系統。您必須將儲存系統新增至專案，以便指派給該專案的人員可以存取它。

儲存系統

儲存系統會自動關聯到新增它們的專案，但您也可以在 **Resources** 頁面中將它們關聯到其他專案或資料夾。您無法將 FSx for NetApp ONTAP 儲存系統關聯到專案或資料夾，但可以在 **Systems** 頁面或 Workloads 中查看它們。

**Keystone**訂閱

Keystone訂閱也是您可以與專案關聯的資源，以便授予使用者在NetApp Console中存取訂閱的權限。

備份與還原工作負載（**Oracle** 和 **Microsoft SQL Server**）

某些 Backup and Recovery 工作負載也被視為資源。您可以為使用者指派存取 Backup and Recovery 的權限。

控制台代理

組織管理員建立控制台代理來管理儲存系統並啟用NetApp資料服務。代理最初與創建它們的項目關聯，但管理員可以從“代理”頁面將它們添加到其他項目或資料夾。

將代理程式與專案關聯起來，可以管理該專案中的資源；而將代理程式與資料夾關聯起來，可以讓資料夾或專案管理員決定哪些專案應該使用該代理程式。代理人必須與特定項目關聯才能提供管理能力。

"了解如何將代理商與項目關聯起來。"

成員及角色

成員

您的組織的成員是使用者帳戶或服務帳戶。應用程式通常使用服務帳戶來完成指定的任務，而無需人工幹預。

成員註冊NetApp Console後，您需要將他們新增至您的組織。添加完成後，您可以為他們指派角色，以便授予他們存取資源的權限。您可以手動從控制台新增服務帳戶，也可以透過NetApp ConsoleIAM API 自動建立和管理服務帳戶。

"了解如何為您的組織新增成員。"

訪問角色

控制台提供您可以指派給組織成員的存取角色。

將成員與角色關聯時，您可以為整個組織、特定資料夾或特定專案授予該角色。您選擇的角色賦予成員對層次結構中選取部分的資源的權限。

NetApp Console提供細粒度的角色控制，遵循「最小權限」原則，這表示存取角色旨在僅向使用者授予其所需的權限。

這意味著隨著使用者職責的增加，他們可能會被分配多個角色。

"了解訪問角色"。

**IAM** 策略範例

小型組織策略

對於使用者少於 50 人且採用集中式儲存管理的組織，可以考慮使用超級管理員和超級查看者角色的簡化方法。

範例：**ABC**公司（**5**人團隊）

- 組織架構： 單一組織，下設 3 個項目（生產、開發、備份）
- 角色：
  - 2 位高階成員：擁有*超級管理員*角色，可取得完整的管理權限
  - 3 位團隊成員：*超級檢視者*角色，擁有監控權限但無修改權限
- 代理策略：所有項目都關聯一個代理，以實現資源共享存取。
- 優勢：簡化管理，降低角色複雜性，適合需要廣泛存取權限的團隊

多區域企業策略

對於擁有區域營運和專業團隊的大型組織，應採用層級式方法，並以資料夾表示地理或業務單元邊界。

例如：**XYZ**公司（跨國公司）

- 結構： 組織結構 > 區域資料夾（北美、歐洲、亞太） > 每個區域的專案資料夾
- 平台角色：
  - 1 組織管理：全球監督與政策管理
  - 3 資料夾或專案管理員：區域控制（每個區域一個）
  - 1 聯盟管理員：企業身分提供者集成
- 按區域劃分的儲存角色：
  - 9 儲存管理員：發現並管理指定區域中的儲存系統
  - 2 儲存檢視器：監控跨區域的儲存資源
  - 1 系統健康專家：無需修改系統即可管理儲存健康狀況

- 數據服務角色：
  - 備份與復原管理員：按項目依備份職責而定
  - 勒索軟體復原管理員：負責跨專案的安全團隊監控
- 代理策略：與相應地理項目相關的區域代理
- 優勢： 透過角色分離、區域自主權和遵守當地法規來增強安全性

部門專業化策略

對於擁有需要特定資料服務存取權限的專業團隊的組織，應根據職能職責進行有針對性的角色分配。

例如：**TechCorp**（一家中型科技公司）

- 結構： 組織 > 部門資料夾（IT、安全、開發） > 專案特定資源
- 專業職缺：
  - 安全團隊：*勒索軟體復原管理員*和*分類檢視器*角色
  - 備份團隊：備份與還原超級管理員，負責全面的備份作業
  - 開發團隊：測試環境管理儲存管理員
  - 合規團隊：營運支援分析師，負責監控與支援個案管理
- 代理策略： 根據資源所有權將代理與部門項目關聯起來
- 優勢： 可自訂的存取控制、更高的營運效率以及明確的專案任務責任劃分

**NetApp Console**中 **IAM** 的後續步驟

- "開始使用NetApp Console中的 IAM"
- "監控或稽核 IAM 活動"
- "了解NetApp Console IAM 的 API"

## 開始在**NetApp Console**中使用身分和存取權限

當您註冊NetApp Console時，系統會提示您建立一個新的組織。該組織包括一名成員（組織管理員）和一個預設項目。要設定身分和存取管理 (IAM) 來滿足您的業務需求，您需要自訂組織的層次結構、新增其他成員、新增或發現資源，並在整個層次結構中關聯這些資源。

您需要擁有*組織管理員*或*超級管理員*權限才能管理組織的身分和存取權限。擁有*資料夾或專案管理員*權限，您只能管理您有權存取的資料夾和專案。

請依照以下步驟建立一個新組織。該順序可能會根據您組織的需求而有所不同。

1 編輯預設項目或加入組織的層次結構

使用預設項目或建立與您的業務層次結構相符的其他項目和資料夾。

"了解如何使用資料夾和項目來組織資源" 。

2 將成員與您的組織關聯

當使用者註冊NetApp Console後，您必須明確地將他們新增至您的 Console 組織。您也可以選擇為您的組織新增服務帳戶。

"了解如何管理成員及其權限" 。

3 新增或發現資源

在控制台新增或發現資源（系統）。組織成員從專案內部管理系統。

了解如何建立或發現資源：

- "Amazon FSx for NetApp ONTAP"
- "Azure NetApp Files"
- "Cloud Volumes ONTAP"
- "E系列系統"
- "本地ONTAP集群"
- "StorageGRID"

4 將資源與其他項目關聯

在控制台中新增或發現系統會自動將資源與目前選定的項目關聯。若要使該資源可供組織中的另一個專案使用，請將其與對應的專案關聯。如果使用控制台代理程式來管理資源，請將控制台代理程式與對應的項目關聯。

- "了解如何管理組織的資源層次結構" 。
- "了解如何將控制台代理與資料夾或項目關聯" 。

相關資訊

- "了解NetApp Console中的身分和存取管理"
- "了解身分和存取 API"

## 設定您的控制台組織

### 將資料夾和專案新增至**NetApp Console**組織

新增資料夾和項目，以符合您的業務結構。建立資料夾和專案後，您可以將資源與它們關聯起來，並管理成員對這些項目的存取權。

建立新組織時，控制台會自動為您建立專案。大多數組織都需要多個項目，以及資料夾來保持井然有序。"了解NetApp Console中的資源層次結構"。

#### 使用資料夾和項目來組織資源

在NetApp Console中，組織包含資料夾和項目，可協助您組織資源。資料夾可以幫助您將相關項目分組，專案可以幫助您管理資源和成員存取權限。

資料夾

資料夾可以幫助您整理相關項目。您可以建立嵌套資料夾來表示組織結構的不同層級。例如，您可以為每個業務部門建立一個頂級資料夾，然後在該業務部門內為不同的團隊建立子資料夾。然後，您可以在資料夾內建立項目。

資料夾還可以透過角色繼承更有效地管理成員存取權。在資料夾層級為成員指派角色時，他們將繼承所有子項目和資料夾的權限。

資料夾是一種組織工具，對於沒有 IAM 權限的成員（例如組織管理員、資料夾或專案管理員或超級管理員角色）是不可見的。成員存取的是項目，而不是資料夾。

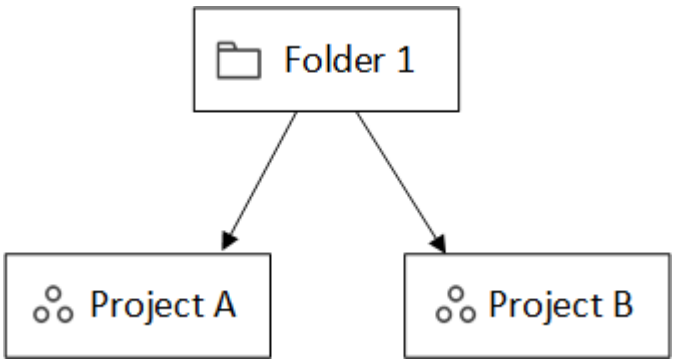
組織管理員可以透過建立資料夾來委派管理職責。建立資料夾後，組織管理員可以為特定資料夾指派資料夾管理員或專案管理員角色。這些成員無需訪問整個組織即可管理該資料夾內的所有項目。

資料夾可以包含其他資料夾或項目作為子資料夾，但不能直接關聯資源。資源必須與項目關聯。

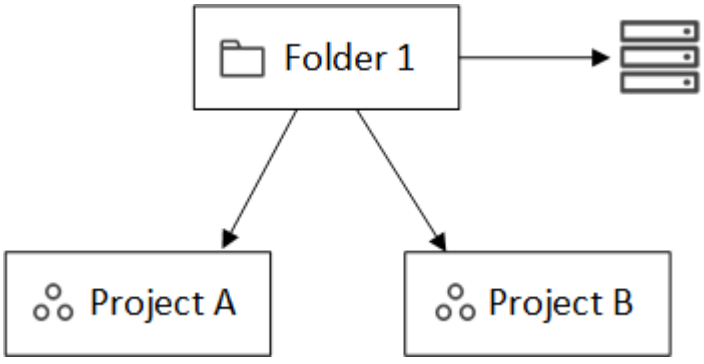
何時將資源與資料夾關聯

_組織管理員_可以將資源與資料夾關聯，以便_資料夾或專案管理員_可以將其連結到資料夾中的相應項目。

例如，假設您有一個包含兩個項目的資料夾：

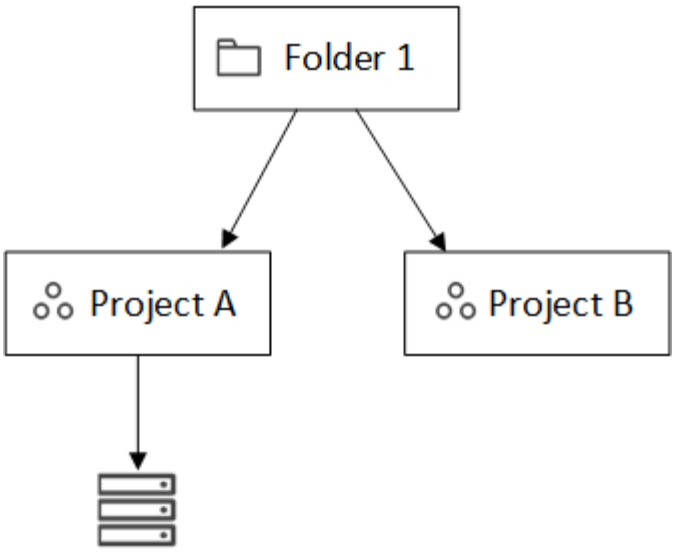



_組織管理員_可以將資源與資料夾關聯：




將資源與資料夾關聯並不會使所有項目都可以存取它；只有資料夾或專案管理員可以看到它。 _資料夾或專案管理員_決定哪些項目可以存取它，並將資源與適當的專案關聯。

在此範例中，管理員將資源與專案 A 關聯：




擁有專案 A 權限的成員現在可以存取該資源。

專案

將資源與專案關聯起來，以便成員進行管理。資源必須與專案關聯才能進行管理和使用者存取。

一個組織可以有一個或多個專案。項目可以直接位於組織下，也可以位於資料夾內。如果使用代理程式來發現專案中的資源，則也必須將該代理與該專案關聯起來。

使用者可在「系統」頁面上瀏覽已指派的項目，以管理與每個項目相關的資源。

新增資料夾或項目

新增專案以管理資源，新增資料夾以對相關項目進行分組。建立新組織時，控制台會包含一個項目。

您可以在組織的資源結構中建立最多七層的資料夾和項目。根據需要建立嵌套資料夾來整理資源。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇*組織*。
3. 從*組織*頁面中，選擇*新增資料夾或項目*。
4. 選擇*資料夾*或*項目*。
5. 請輸入資料夾或項目詳細資料：
   - 名稱和位置：輸入資料夾或項目的名稱並選擇其位置。您可以將資料夾或項目放置在組織下，也可以放置在其他資料夾內。
   - 資源：選擇要與此資料夾或項目關聯的資源。如果您尚未向主機新增儲存系統，您可以稍後執行此步驟。

只有當資料夾中的資源被指派給某個專案後，成員才能存取這些資源。使用資料夾暫時存放資源，直到建立必要的項目為止。這可以幫助組織管理員將資源分配委派給資料夾或專案管理員，然後由該管理員將資源指派給資料夾內的專案。

- 存取權限：選擇*新增成員*以指派存取權限和角色。您可以隨時在專案或資料夾中新增或刪除成員。

  "了解訪問角色" 。

6. 選擇“新增”。

#### 重新命名資料夾或項目

根據需要重新命名資料夾或項目。重新命名不會影響相關資源或成員存取權限。

步驟

1. 從「組織」頁面，導覽至表中的項目或資料夾，選擇 ••• 然後選擇*編輯資料夾*或*編輯項目*。
2. 在*編輯*頁面上，輸入新名稱並選擇*應用*。

#### 刪除資料夾或項目

刪除不再需要的資料夾和項目，例如團隊重組或專案完成後。

刪除資料夾或項目之前，請確保其中不包含任何資源。了解如何移除資源。

步驟

1. 從「組織」頁面，導覽至表中的項目或資料夾，選擇 ••• 然後選擇*刪除*。
2. 確認您要刪除資料夾或項目。

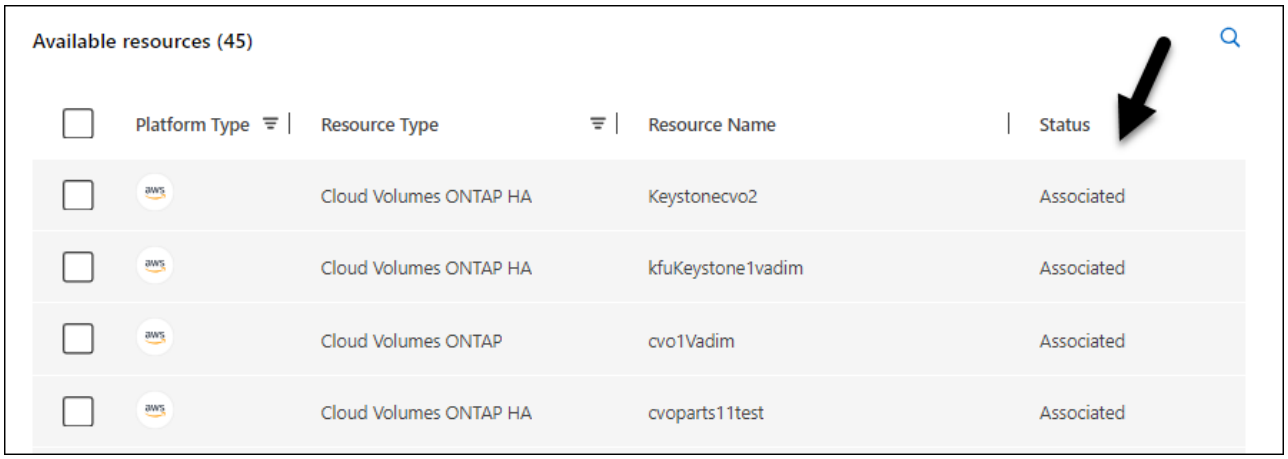
#### 查看與資料夾或項目關聯的資源

查看哪些資源和成員與資料夾或項目相關聯。

步驟

1. 從「組織」頁面，導覽至表中的項目或資料夾，選擇 ••• 然後選擇*編輯資料夾*或*編輯項目*。


2. 在*編輯*頁面上，您可以透過展開*資源*或*存取*部分來查看有關所選資料夾或項目的詳細資訊。
   - 選擇“資源”來查看相關資源。在表中，「狀態」列標識與資料夾或項目相關的資源。




更改與資料夾或項目關聯的資源

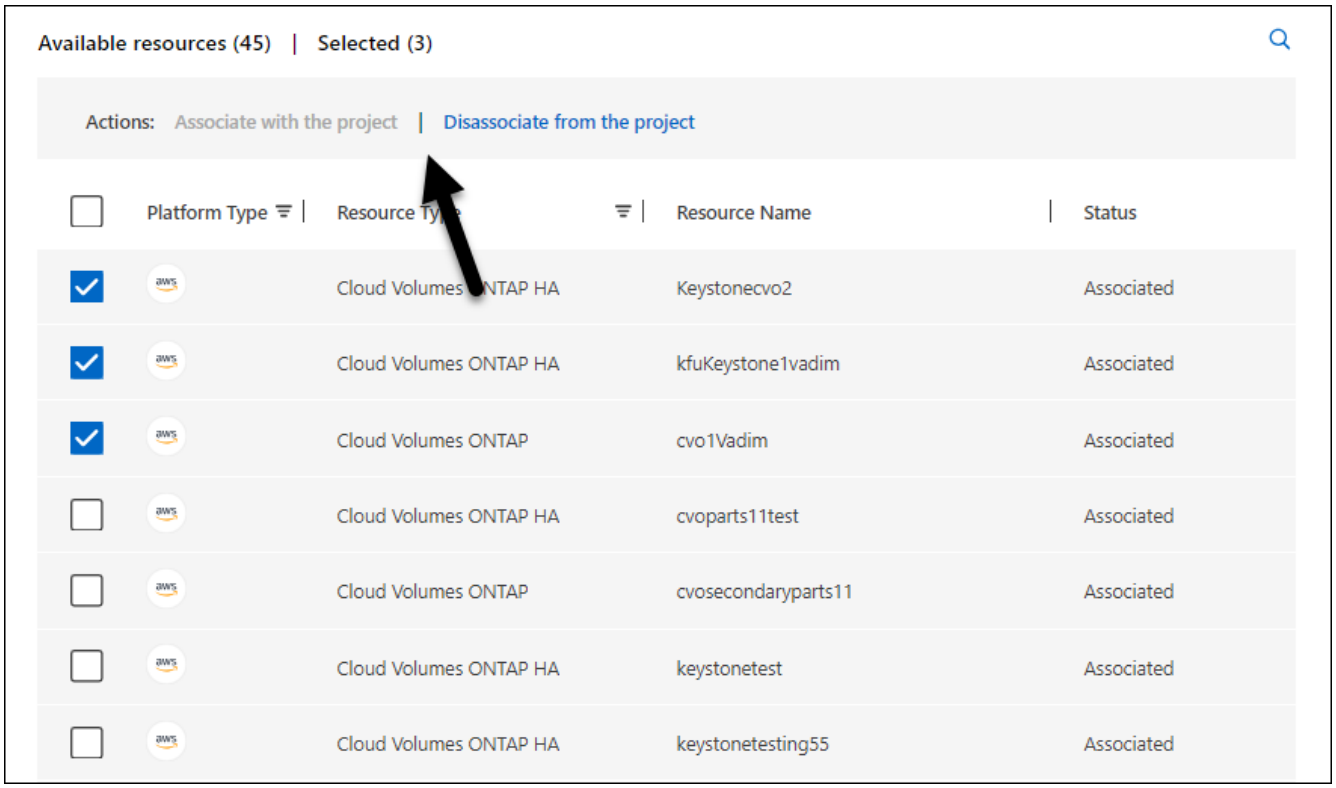
您可以根據組織的需求變更與資料夾或項目相關的資源變更。

步驟

1. 從「組織」頁面，導覽至表中的項目或資料夾，選擇 ••• 然後選擇*編輯資料夾*或*編輯項目*。
2. 在*編輯*頁面上，選擇*資源*。

   在表中，「狀態」列標識與資料夾或項目相關的資源。

3. 選擇您想要關聯或取消關聯的資源。
4. 根據您選擇的資源，選擇「與項目關聯」或「與項目取消關聯」。



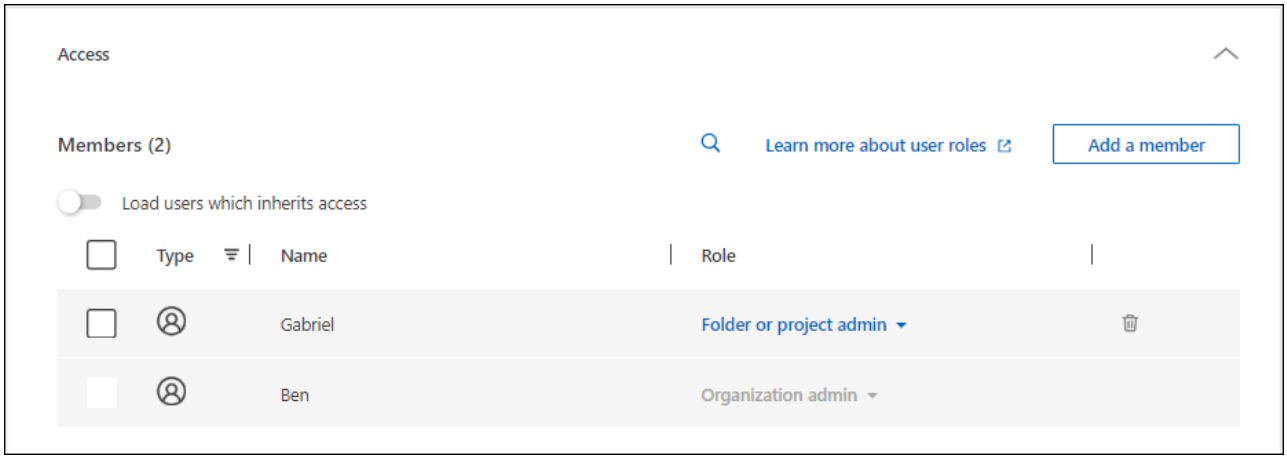

5. 選擇*應用*。

查看與資料夾或項目關聯的成員

您可以從「組織」頁面查看與資料夾或項目關聯的成員。

步驟

1. 從「組織」頁面，導覽至表中的項目或資料夾，選擇 ••• 然後選擇*編輯資料夾*或*編輯項目*。
2. 在*編輯*頁面上，選擇*存取*以查看有權存取所選資料夾或項目的成員清單。
   - 選擇*存取*來查看有權存取該資料夾或項目的成員。




修改成員對資料夾或項目的存取權限

修改成員存取權限以控制資源存取。請記住，在資料夾層級分配的角色將被所有子項目和資料夾繼承。

如果成員存取權限是從資料夾或組織層級繼承的，則無法在較低層級變更成員存取權限。變更較高層級成員的權限以變更存取權限。或者，您可以 "從「會員」頁面管理權限"。

步驟

1. 從「組織」頁面，導覽至表中的項目或資料夾，選擇 ••• 然後選擇*編輯資料夾*或*編輯項目*。
2. 在*編輯*頁面上，選擇*存取*以查看有權存取所選資料夾或項目的成員清單。
3. 修改會員存取權限：
   - 新增成員：選擇您想要新增至資料夾或專案的成員並為他們指派角色。
   - 變更成員的角色：對於具有組織管理員以外角色的任何成員，選擇其現有角色，然後選擇新角色。
   - 刪除成員存取權限：對於在您正在查看的資料夾或專案中定義了角色的成員，您可以刪除他們的存取權限。
4. 選擇*應用*。

相關資訊

- "了解NetApp Console中的身分和存取權限"
- "開始使用身分和存取權限"
- "了解身分和存取 API"

在**NetApp Console**中新增資源

# 透過將使用者新增至NetApp Console組織中的專案和資料夾來控制使用者對資源的存取權限。授予專案級使用者存取權限。

資源是指控制台所感知到的實體，例如儲存資源、控制台代理程式或備份和還原工作負載。

您可以在控制台的「資源」頁面中檢視和管理資源。

## 控制台資源類型

您可以將多種類型的資源關聯到NetApp Console組織中的專案：

### 儲存資源

儲存資源是組織中最常見的資源類型，包括本地儲存系統和雲端儲存系統。在控制台中新增儲存系統時，您可以將其新增至資料夾或專案。在此之前，控制台會將其標記為未發現，並且不會在「資源」頁面上顯示它。

### 控制台代理

如果您使用控制台代理程式來發現儲存系統，請將該代理程式新增至相同資料夾或專案。這允許使用者執行代理啟用的功能，例如資料服務或控制台原生儲存管理。您可以從控制台的「代理」頁面新增代理程式到資料夾或專案。"了解如何將控制台代理與資料夾或項目關聯"。

### **Keystone**訂閱

如果您的組織擁有Keystone訂閱，您可以在「資源」頁面上查看它們。您可以將Keystone訂閱與資料夾或項目關聯起來，以便提供擁有這些資料夾或專案權限的成員存取權限。

## 查看組織中的資源

您可以查看與您的組織相關的已發現和未發現的資源。系統會尋找儲存資源，並將其標記為未發現，直到您將其新增至控制台為止。

控制台會將Amazon FSx for NetApp ONTAP資源從「資源」頁面中排除，因為使用者無法將其與角色關聯。您可以在「系統」頁面或「工作負載」中查看這些資源。

### 步驟

1. 選擇*管理>身分和存取*。
2. 選擇*資源*。
3. 選擇*進階搜尋和過濾*。
4. 利用現有選項尋找資源：
   - 按資源名稱搜尋：輸入文字字串並選擇*新增*。
   - 平台：選擇一個或多個平台，例如 Amazon Web Services。
   - 資源：選擇一個或多個資源，例如Cloud Volumes ONTAP。
   - 組織、資料夾或專案：選擇整個組織、特定資料夾或特定專案。
5. 選擇*搜尋*。

### 將資源與資料夾和項目關聯

將資源關聯到資料夾或項目，使其可供具有該資料夾或項目權限的成員使用。

步驟

1. 從「資源」頁面，導覽到表中的資源，選擇 ••• 然後選擇*關聯到資料夾或項目*。
2. 選擇一個資料夾或項目，然後選擇*接受*。
3. 若要關聯其他資料夾或項目，請選擇*新增資料夾或項目*，然後選擇該資料夾或項目。

   請注意，您只能從您擁有管理員權限的資料夾和項目中進行選擇。

4. 選擇*關聯資源*。
   - 如果您將資源與項目關聯，則擁有這些項目權限的成員現在可以從控制台存取該資源。
   - 如果您將資源與資料夾關聯，則_資料夾或專案管理員_現在可以存取該資源並將其與資料夾內的項目關聯。"了解如何將資源與資料夾關聯"。

完成後

如果您使用控制台代理程式發現資源，請將控制台代理程式與專案關聯以授予存取權限。否則，沒有「組織管理員」角色的成員將無法存取控制台代理程式及其相關資源。

"了解如何將控制台代理與資料夾或項目關聯"。

### 查看與資源關聯的資料夾和項目

您可以查看與特定資源關聯的資料夾和項目。

如果您需要了解哪些組織成員有權存取該資源，您可以"查看有權存取與資源關聯的資料夾和項目的成員"。

步驟

1. 從「資源」頁面，導覽到表中的資源，選擇 ••• 然後選擇*查看詳細資訊*。

以下範例顯示了與一個項目關聯的資源。


要查看哪些組織成員有權存取該資源，"查看有權存取關聯資料夾和項目的成員"。

從資料夾或項目中刪除資源

若要從資料夾或項目中刪除資源，請刪除其關聯。這樣可以防止成員管理該資料夾或專案中的資源。

若要從整個組織中刪除已發現的資源，請前往「系統」頁面並刪除該系統。

步驟

1. 從「資源」頁面，導覽到表中的資源，選擇 ••• 然後選擇*查看詳細資訊*。
2. 若要從資料夾或項目移除資源，請選擇 在資料夾或項目旁邊。
3. 選擇“刪除”以移除關聯。

相關資訊

- "了解NetApp Console中的身分和存取權限"
- "開始在NetApp Console中使用身分和存取權限"
- "了解身分和存取 API"

將控制台代理程式與其他資料夾和項目關聯

## 將控制台代理與特定項目關聯，以啟用資源管理和資料服務存取。透過控制台代理程式發現的資源需要資源和代理程式都與同一個專案關聯，才能實現團隊存取。

超級管理員和組織管理員可以建立代理，並將任何代理與任何專案或資料夾關聯起來。資料夾或專案管理員只能將現有代理與他們擁有權限的資料夾和項目關聯起來。"詳細了解資料夾或專案管理員可以完成的操作"。

步驟

1. 選擇*管理>身分和存取*>*代理*。
2. 從表中，找到要關聯的控制台代理程式。

   使用表格上方的搜尋功能尋找特定的控制台代理程式或依資源層次結構篩選表格。

3. 若要查看連結到控制台代理的資料夾和項目，請選擇 ••• 然後選擇*查看詳細資訊*。

   此頁面顯示與控制台代理程式關聯的資料夾和項目的詳細資訊。

4. 選擇*關聯到資料夾或項目*。
5. 選擇一個資料夾或項目，然後選擇*接受*。
6. 若要將控制台代理程式與其他資料夾或項目關聯，請選擇*新增資料夾或項目*，然後選擇該資料夾或項目。
7. 選擇*關聯代理*。

完成後

將控制台代理程式的資源與「資源」頁面中的相同資料夾和項目關聯。

"了解如何將資源與資料夾和項目關聯" 。

相關資訊

- "了解NetApp Console代理"
- "了解NetApp Console身分和存取管理"
- "開始使用身分和存取權限"
- "了解身分和存取管理的 API"

## 將使用者新增至您的控制台組織

### 將使用者新增至**NetApp Console**組織

在控制台中，您可以根據存取角色授予使用者對專案或資料夾的存取權限。_存取角色_包含一組權限，使成員（使用者或服務帳戶）能夠在資源層次結構的指定層級執行特定操作。

#### 所需存取權限

超級管理員、組織管理員或資料夾或專案管理員（對於他們管理的資料夾和專案）。"了解訪問角色"。

#### 了解如何在**NetApp Console**中授予存取權限

NetApp Console使用基於角色的存取控制 (RBAC) 來管理權限。可以單獨為使用者指派角色，也可以透過聯合群組為使用者指派角色。每個角色都定義了對特定資源允許的操作。

請注意以下關於在NetApp Console中授予存取權限的事項：

- 所有使用者必須先註冊NetApp Console，然後才能取得資源存取權限。
- 即使使用者是已指派角色的聯合群組的成員，也必須在控制台中明確地為每個使用者指派角色，然後他們才能存取資源。
- 您可以直接從控制台新增服務帳戶並為其指派角色。

#### 在您的組織中加入成員

NetApp Console支援三種類型的成員：使用者帳戶、服務帳戶和聯合群組。

即使使用者屬於聯合群組，也必須先註冊NetApp Console，然後才能新增他們並指派角色。直接在控制台中建立服務帳戶。

所有成員必須至少被明確分配一個角色才能存取資源。

新增成員時，選擇資源層級（組織、資料夾或專案），並指派一個或多個具有所需權限的角色。

#### 新增用戶

使用者註冊NetApp Console，但組織管理員、資料夾管理員或專案管理員必須將他們新增至組織、資料夾或專案中，以便他們能夠存取資源。

開始之前：

使用者必須已經註冊了NetApp Console。如果他們還沒有註冊，請引導他們... "註冊NetApp Console。"

如果要新增屬於聯合群組的用戶，請確保該用戶已註冊NetApp Console，並在控制台中明確指派了角色。NetApp建議指派最低存取權限角色，例如組織檢視者。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇*成員*。
3. 選擇*新增成員*。
4. 對於*會員類型*，保持選擇*使用者*。
5. 對於*使用者的電子郵件*，輸入與其建立的登入相關聯的使用者的電子郵件地址。
6. 使用「選擇組織、資料夾或項目」部分來選擇成員應具有權限的資源層次結構層級。

   請注意以下事項：

   - 您只能選擇您擁有權限的資料夾和項目。
   - 選擇組織或資料夾時，即授予該成員對其所有內容的存取權限。
   - 您只能在組織層級指派*組織管理員*角色。
7. 選擇一個類別，然後選擇一個*角色*，該角色為成員提供與您選擇的組織、資料夾或專案相關的資源的權限。

   "了解訪問角色" 。
8. 若要授予對更多資料夾、項目或角色的存取權限，請選擇“新增角色”，選擇資料夾、項目或角色類別，然後選擇角色。
9. 選擇“新增”。

   控制台會透過電子郵件向使用者發送操作說明。

新增服務帳戶

服務帳戶可讓您自動執行任務並安全地連接到控制台 API。對於簡單的設置，可以選擇客戶端 ID 和金鑰；對於自動化或雲端原生環境，可以選擇 JWT（JSON Web Token）以獲得更強的安全性。選擇符合您安全要求的方法。

開始之前：

對於 JWT 身份驗證，請準備您的公鑰或憑證。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇*成員*。
3. 選擇*新增成員*。
4. 對於*會員類型*，選擇*服務帳戶*。
5. 輸入服務帳戶的名稱。
6. 若要使用 JWT 驗證，請選擇“使用私鑰 JWT 驗證”，然後上傳您的 RSA 公鑰或憑證。如果使用客戶端 ID 和

金鑰，則跳過此步驟。

您的 X.509 證書。它必須是 PEM、CRT 或 CER 格式。

a. 設定證書到期通知。您可以選擇七天或三十天。到期通知將透過電子郵件發送給具有超級管理員或組織管理員角色的用戶，並在控制台中顯示。

7. 使用「選擇組織、資料夾或項目」部分來選擇成員應具有權限的資源層次結構層級。

   請注意以下事項：

   - 您只能從您有權限的資料夾和項目中進行選擇。
   - 選擇一個組織或資料夾將授予成員對其所有內容的權限。
   - 您只能在組織層級指派*組織管理員*角色。

8. 選擇一個*類別*，然後選擇一個*角色*，授予成員對所選組織、資料夾或專案中的資源的權限。

   "了解訪問角色" 。

9. 若要授予對更多資料夾、項目或角色的存取權限，請選擇“新增角色”，選擇資料夾、項目或角色類別，然後選擇角色。

10. 如果您沒有選擇使用 JWT 驗證，請下載或複製用戶端 ID 和用戶端金鑰。

    控制台只會顯示一次客戶端金鑰。請妥善備份；如果遺失，您可以稍後重新建立。

11. 如果您選擇 JWT 驗證，請下載或複製用戶端 ID 和 JWT 受眾群體。控制台只會顯示此資訊一次，之後無法再檢索。

12. 選擇*關閉*。

在您的組織中新增聯合組

您可以將身分提供者 (IdP) 中的聯合群組新增至您的組織，並為其指派一個或多個角色。聯合群組的成員將繼承您在控制台中指派給該群組的角色。

在為聯合組分配角色之前，請確保以下事項：

- 在身分識別提供者 (IdP) 和控制台之間建立聯盟。 "了解如何建立聯邦。"
- 該群組必須已存在於您的身分提供者 (IdP) 中，並且已被指派對控制台的應用程式存取權。
- 屬於該群組的使用者必須已經註冊了NetApp Console，並且已明確指派了控制台中的角色。NetApp建議指派最低存取權限角色，例如組織檢視者。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇*成員*。
3. 選擇*新增成員*。
4. 對於“成員類型”，請選擇“聯合群組”。
5. 選擇該團體所屬的聯邦。
6. 對於“群組名稱”，請輸入您身分提供者 (IdP) 中群組的確切名稱。

7. 使用「選擇組織、資料夾或項目」部分來選擇成員應具有權限的資源層次結構層級。

   請注意以下事項：

   - 您只能從您有權限的資料夾和項目中進行選擇。
   - 選擇一個組織或資料夾將授予成員對其所有內容的權限。
   - 您只能在組織層級指派*組織管理員*角色。

8. 選擇一個*類別*，然後選擇一個*角色*，授予成員對所選組織、資料夾或專案中的資源的權限。

   "了解訪問角色" 。

9. 若要授予對更多資料夾、項目或角色的存取權限，請選擇“新增角色”，選擇資料夾、項目或角色類別，然後選擇角色。

相關資訊

- "了解NetApp Console中的身分和存取管理"
- "開始使用身分和存取權限"
- "NetApp Console存取角色"
- "了解身分和存取 API"

# 管理使用者存取權限和安全

## 了解**NetApp Console**基於角色的存取控制 **(RBAC)**

使用基於角色的存取控制 (RBAC) 管理使用者對NetApp Console的訪問，在組織、資料夾或專案層級指派預先定義角色。每個角色都授予特定的權限，定義使用者在其指派的權限範圍內可以執行哪些操作。

NetApp在設計控制台角色時遵循最小權限原則，因此每個角色僅包含其任務所需的權限。這種方法透過限制每個成員所需的存取權限來增強安全性。

將資源整理成資料夾和專案後，為組織成員指派特定資料夾或專案的角色，使他們只能履行自己的職責。

例如，您可以為特定專案層級的成員指派勒索軟體復原管理員角色，允許他們對該專案內的資源執行勒索軟體復原操作，而無需授予他們對整個組織的更廣泛存取權限。同一使用者可以被授予組織內多個專案的角色。

您可以根據使用者的職責，為相同範圍或不同範圍的使用者指派多個角色。例如，規模較小的組織可能會讓同一用戶在組織層級管理勒索軟體復原和備份與復原任務，而規模較大的組織可能會在專案層級為每個角色分配不同的使用者。

### 控制台組織成員的類型

NetApp Console組織中有三種類型的成員：* 使用者帳號：登入NetApp Console以管理資源的個人使用者。使用者必須先註冊NetApp Console，然後才能被加入到組織中。* 服務帳戶：應用程式或服務透過 API 與NetApp Console互動時使用的非人類帳戶。您可以將服務帳戶直接新增至您的控制台組織。* 聯合群組：從您的身分提供者 (IdP) 同步的群組，可讓您集中管理多個使用者的存取權限。聯合群組中的每個使用者都必須先註冊NetApp Console，並被新增到您的組織中，並且擁有相應的存取角色，然後才能存取授予該群組的資源。

"了解如何為您的組織新增成員。"

### NetApp Console中的預先定義角色

NetApp Console包含預先定義角色，您可以將其指派給組織成員。每個角色都包含權限，用於指定成員在其指派的範圍（組織、資料夾或專案）內可以執行哪些操作。

NetApp Console角色採用最小權限原則，確保成員僅擁有完成任務所需的權限，並按角色提供的存取權限類型對其進行分類：

- 平台角色：提供控制台管理權限
- 資料服務角色：提供管理特定資料服務的權限，例如勒索軟體復原和備份與復原。
- 應用程式角色：提供管理儲存以及審核控制台事件和警報的權限

您可以根據成員的職責為其指派多個角色。例如，您可以為特定項目為一名成員指派勒索軟體復原管理員角色和備份與復原管理員角色。

"了解NetApp Console中可用的預先定義角色"。

## 在NetApp Console中管理成員存取權限

管理您在控制台組織中的成員存取權限。分配角色以設定權限。成員離開時將其移除。

### 所需存取權限

超級管理員、組織管理員或資料夾或專案管理員（對於他們管理的資料夾和專案）。連結：reference-iam-predefined-roles.html[了解訪問角色]。

您可以按項目或資料夾指派存取角色。例如，可以為使用者指派兩個特定項目的角色，或在資料夾層級指派角色，從而授予使用者對資料夾中所有項目的勒索軟體復原管理員角色。

請先新增資料夾和項目，然後再分配使用者存取權限。 "了解如何新增資料夾和項目。"

### 了解如何在NetApp Console中授予存取權限

NetApp Console使用基於角色的存取控制 (RBAC) 模型來管理使用者權限。您可以單獨或透過聯合群組為成員指派預先定義的角色。您可以為服務帳戶以及聯合群組新增和指派角色。每個角色都定義了成員可以在相關資源上執行哪些動作。

請注意以下關於在NetApp Console中授予存取權限的事項：

- 所有使用者必須先註冊NetApp Console，然後才能取得資源存取權限。
- 即使使用者是已指派角色的聯合群組的成員，也必須在控制台中明確地為每個使用者指派角色，然後他們才能存取資源。
- 您可以直接從控制台新增服務帳戶並為其指派角色。

### 使用角色繼承

在NetApp Console中，當您在組織、資料夾或專案層級指派角色時，所選範圍內的所有資源都會自動繼承該角色。例如，資料夾級角色適用於所有包含的項目，而專案級角色適用於該項目內的所有資源。

查看組織成員

若要了解成員可用的資源和權限，您可以查看在組織資源層級結構的不同層級指派給該成員的角色。"了解如何使用角色來控制對控制台資源的存取。"

步驟

1. 選擇*管理>身分和存取*。
2. 選擇*成員*。

   *成員*表格列出了您組織的成員。

3. 從「成員」頁面，導覽至表中的成員，選擇 ••• 然後選擇*查看詳細資訊*。

查看指派給成員的角色

您可以查看他們目前被指派的角色。

如果您具有_資料夾或專案管理員_角色，則該頁面將顯示組織中的所有成員。但是，您只能查看和管理您擁有權限的資料夾和專案的成員權限。"詳細了解資料夾或專案管理員可以完成的操作" 。

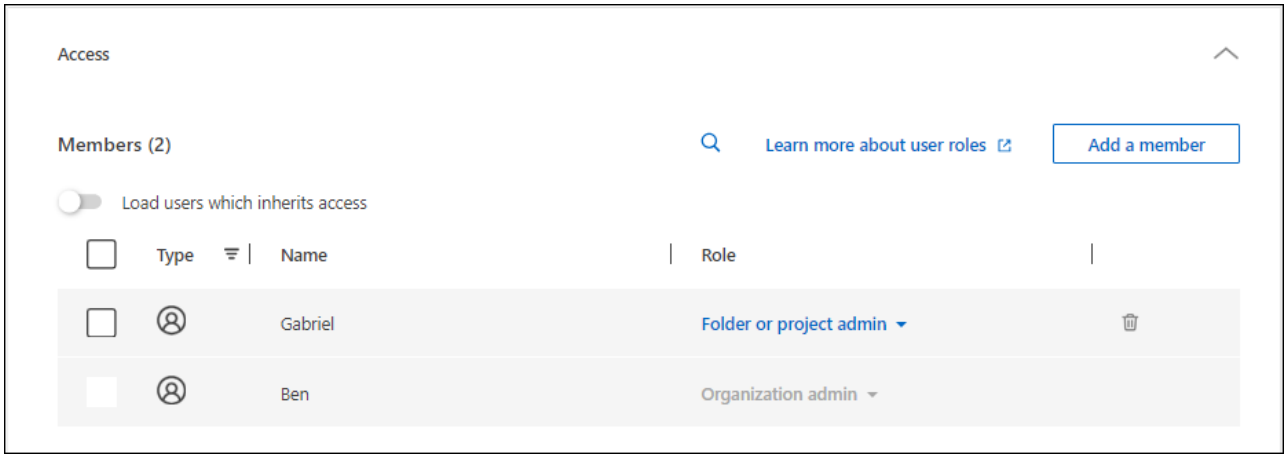
1. 在「成員」頁面中，導覽至表格中的某個成員，然後選擇 ••• 然後選擇“查看詳情”。
2. 在表格中，展開您想要查看成員指派角色的組織、資料夾或專案的對應行，然後在「角色」欄位中選擇「檢視」。

查看與資料夾或項目關聯的成員

您可以查看哪些成員有權存取特定資料夾或項目。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇*組織*。
3. 從「組織」頁面，導覽至表中的項目或資料夾，選擇 ••• 然後選擇*編輯資料夾*或*編輯項目*。
   - 選擇*存取*來查看有權存取該資料夾或項目的成員。



## 分配或修改成員存取權限

使用者註冊NetApp Console後，您可以將他們新增至您的組織並指派角色，以便向他們提供資源存取權。 "了解如何為您的組織新增成員。"

您可以根據需要新增或刪除角色來調整成員的存取權限。

### 為成員新增存取角色

您通常在為組織新增成員時指派角色，但您可以隨時透過刪除或新增角色來更新它。

您可以為使用者指派組織、資料夾或專案的存取角色。

成員可以在同一個專案內或不同的專案中擔任多個角色。例如，規模較小的組織可能會將所有可用的存取角色分配給相同用戶，而規模較大的組織可能會讓用戶執行更專業的任務。或者，您也可以在組織層級為一名使用者指派勒索軟體復原管理員角色。在這個例子中，使用者可以對組織內的所有項目執行勒索軟體復原任務。

您的存取角色策略應與您組織NetApp資源的方式保持一致。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇*成員*。
3. 選擇成員標籤之一：使用者、服務帳戶*或*聯合群組。
4. 選擇操作選單 ••• 在您想要指派角色的成員旁邊，選擇「新增角色」。
5. 若要新增角色，請完成對話方塊中的步驟：
   - 選擇組織、資料夾或專案：選擇成員應具有權限的資源層次結構層級。

     如果您選擇組織或資料夾，則該成員將擁有該組織或資料夾內所有內容的權限。
   - 選擇類別：選擇角色類別。"了解訪問角色"。
   - 選擇*角色*：選擇一個角色，該角色為成員提供與您選擇的組織、資料夾或專案相關的資源的權限。
   - 新增角色：如果您想提供組織內其他資料夾或項目的存取權限，請選擇*新增角色*，指定另一個資料夾或項目或角色類別，然後選擇一個角色類別和對應的角色。
6. 選擇*新增角色*。

### 更改成員的指定角色

更改成員角色以更新其存取權限。

必須為使用者指派至少一個角色。您無法刪除使用者的所有角色。如果您需要刪除所有角色，則必須從組織中刪除該使用者。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇*成員*。
3. 選擇成員標籤之一：使用者、服務帳戶*或*聯合群組。

4. 從「成員」頁面，導覽至表中的成員，選擇 ••• 然後選擇*查看詳細資訊*。
5. 在表格中，展開要變更成員指派角色的組織、資料夾或專案的對應行，然後在「角色」欄位中選擇「檢視」以查看指派給該成員的角色。
6. 您可以變更成員的現有角色或刪除角色。
   a. 若要變更成員的角色，請選擇要變更的角色旁邊的「變更」。您只能將角色變更為同一角色類別內的角色。例如，您可以從一個資料服務角色變更為另一個資料服務角色。確認更改。
   b. 若要取消指派成員的角色，請選擇 🗑 在角色旁邊，點擊即可從成員中移除對應的角色。您將被要求確認刪除操作。

從您的組織中移除成員

如果成員離開您的組織，則將其從組織中移除。

刪除成員時，系統會撤銷其控制台權限，但保留其控制台和NetApp支援網站帳號。

聯邦成員

- 當聯合使用者從您的身分提供者 (IdP) 中移除時，他們將自動失去對NetApp Console的存取權限。但您仍然應該將它們從您的控制台組織中刪除，以保持您的成員清單是最新的。
- 如果您從身分提供者 (IdP) 中的聯合群組中移除用戶，他們將失去與該群組關聯的控制台存取權限。但是，他們仍然保留在控制台中分配給他們的明確角色所關聯的任何存取權限。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇*成員*。
3. 選擇成員標籤之一：使用者、服務帳戶*或*聯合群組。
4. 從「成員」頁面，導覽至表中的成員，選擇 ••• 然後選擇*刪除使用者*。
5. 確認您要從組織中刪除該成員。

使用者安全

## 透過管理成員安全設置，確保使用者對NetApp Console組織的存取權限。您可以重設使用者密碼、管理多因素身份驗證 (MFA) 以及重新建立服務帳戶憑證。

所需存取權限

超級管理員、組織管理員或資料夾或專案管理員（對於他們管理的資料夾和專案）。連結：reference-iam-predefined-roles.html[了解訪問角色]。

重設使用者密碼（僅限本地用戶）

組織管理員無法重設本機使用者的使用者密碼。但是，他們可以指導用戶重置自己的密碼。

指示使用者透過選擇「忘記密碼？」從控制台登入頁面重設密碼。

此選項不適用於聯合組織中的使用者。

管理用戶的多重身份驗證 **(MFA)**

如果使用者失去對其 MFA 設備的存取權限，您可以刪除或停用其 MFA 配置。

多因素身份驗證僅適用於本機用戶。聯合身份驗證使用者無法啟用多因素身份驗證 (MFA)。

使用者移除多因素身份驗證後，登入時必須重新設定多因素身份驗證。如果使用者暫時無法存取其 MFA 設備，他們可以使用已儲存的復原代碼登入。

如果他們沒有恢復代碼，請暫時停用 MFA 以允許登入。當您為使用者停用 MFA 時，它只會停用八個小時，然後自動重新啟用。在此期間，用戶無需 MFA 即可登入一次。八小時後，使用者必須使用 MFA 才能登入。

若要管理使用者的多重身分驗證，您必須擁有與受影響使用者位於相同網域的電子郵件地址。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇*成員*。

   *成員*表格列出了您組織的成員。

3. 從「成員」頁面，導覽至表中的成員，選擇 ••• 然後選擇*管理多重身份驗證*。
4. 選擇是否刪除或停用使用者的 MFA 配置。

重新建立服務帳戶的憑證

如果您遺失或需要更新服務憑證，可以建立新的憑證。

建立新憑證會刪除舊憑證。您不能使用舊的憑證。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇*成員*。
3. 在「成員」表中，導覽至服務帳戶，選擇 ••• 然後選擇*重新建立秘密*。
4. 選擇*重新建立*。
5. 下載或複製客戶端 ID 和客戶端金鑰。

   控制台只會顯示一次客戶端金鑰。請務必複製或下載並妥善保存。

## NetApp Console存取角色

### 了解**NetApp Console**存取角色

NetApp Console中的身分和存取管理 (IAM) 提供了預先定義的角色，您可以將這些角色指派給組織中不同資源層級的成員。在指派這些角色之前，您應該了解每個角色包含的權限。角色分為以下類別：平台、應用程式和資料服務。

平台角色

平台角色授予NetApp Console管理權限，包括角色指派和使用者管理。控制台具有多種平台角色。

| 平台角色 | 職責 |
| --- | --- |
| "組織管理員" | 允許使用者不受限制地存取組織內的所有項目和資料夾，為任何項目或資料夾添加成員，以及執行任何任務和使用任何沒有明確關聯角色的資料服務。具有此角色的使用者可以透過建立資料夾和專案、分配角色、新增使用者以及管理系統（如果他們擁有適當的憑證）來管理您的組織。這是唯一可以建立控制台代理的存取角色。 |
| "資料夾或專案管理員" | 允許使用者不受限制地存取已指派的項目和資料夾。可以將成員新增到他們管理的資料夾或專案中，以及執行任何任務並在他們被指派的資料夾或專案內的資源上使用任何資料服務或應用程式。資料夾或專案管理員無法建立控制台代理。 |
| "聯盟管理員" | 允許使用者使用控制台建立和管理聯合，從而實現單一登入 (SSO)。 |
| "聯邦檢視器" | 允許使用者使用控制台查看現有的聯合。無法建立或管理聯盟。 |
| "合作夥伴管理員" | 允許使用者創建和管理合作關係。 |
| "合作夥伴檢視器" | 允許用戶查看現有的合作關係。無法創建或管理合作關係。 |
| "超管理員" | 為使用者提供管理員角色的子集。此角色專為可能不需要在多個使用者之間分配控制台職責的小型組織而設計。 |
| "超觀眾" | 為使用者提供子集查看者角色。此角色專為可能不需要在多個使用者之間分配控制台職責的小型組織而設計。 |

應用程式角色

以下是應用程式類別中的角色清單。每個角色在其指定範圍內授予特定的權限。沒有所需應用程式或平台角色的使用者無法存取相應的應用程式。

| 應用程式角色 | 職責 |
| --- | --- |
| "Google Cloud NetApp Volumes管理員" | 具有Google Cloud NetApp Volumes角色的使用者可以發現和管理Google Cloud NetApp Volumes。 |
| "Google Cloud NetApp Volumes檢視器" | 具有Google Cloud NetApp Volumes使用者角色的使用者可以查看Google Cloud NetApp Volumes。 |
| "Keystone管理員" | 具有Keystone管理員角色的使用者可以建立服務請求。允許使用者監控和查看他們正在存取的Keystone租戶內的使用情況、資源和管理詳細資訊。 |
| "Keystone檢視器" | 具有Keystone檢視者角色的使用者不能建立服務請求。允許使用者監控和查看他們正在存取的Keystone租戶內的消費、資產和管理資訊。 |
| ONTAP調解器設定角色 | 具有ONTAP調解器設定角色的服務帳戶可以建立服務請求。服務帳戶中需要此角色來配置"ONTAP雲端調解器"。 |
| "營運支援分析師" | 提供對警報和監控工具的存取以及輸入和管理支援案例的能力。 |
| "儲存管理員" | 管理儲存健康和治理功能，發現儲存資源，以及修改和刪除現有系統。 |
| "儲存檢視器" | 查看儲存健康和治理功能，以及查看先前發現的儲存資源。無法發現、修改或刪除現有的儲存系統。 |

| 應用程式角色 | 職責 |
| --- | --- |
| "系統健康專家" | 管理儲存和健康和治理功能，儲存管理員的所有權限，但不能修改或刪除現有系統。 |

數據服務角色

以下是資料服務類別中的角色清單。每個角色在其指定範圍內授予特定的權限。沒有所需資料服務角色或平台角色的使用者將無法存取資料服務。

| 數據服務角色 | 職責 |
| --- | --- |
| "備份和恢復超級管理員" | 在NetApp Backup and Recovery中執行任何操作。 |
| "備份和復原管理員" | 執行本機快照備份、複製到二級儲存以及備份到物件儲存。 |
| "備份和還原復原管理員" | 恢復備份和復原中的工作負載。 |
| "備份和還原克隆管理員" | 在備份和復原中克隆應用程式和資料。 |
| "備份和還原檢視器" | 查看備份和復原資訊。 |
| "災難復原管理員" | 在NetApp Disaster Recovery服務中執行任何操作。 |
| "災難復原故障轉移管理員" | 執行故障轉移和遷移。 |
| "災難復原應用程式管理員" | 建立複製計劃、變更複製計劃並啟動測試故障轉移。 |
| "災難復原檢視器" | 僅查看資訊。 |
| 分類檢視器 | 允許使用者查看NetApp Data Classification掃描結果。具有此角色的使用者可以查看合規性資訊並產生他們有權存取的資源的報告。這些使用者無法啟用或停用磁碟區、儲存桶或資料庫模式的掃描。分類功能沒有管理員角色。 |
| "勒索軟體抵禦能力管理員" | 管理NetApp Ransomware Resilience的「保護」、「警報」、「復原」、「設定」和「報告」標籤上的操作。 |
| "勒索軟體復原力檢視器" | 在 Ransomware Resilience 中查看工作負載資料、查看警報資料、下載復原資料和下載報告。 |
| "勒索軟體復原力用戶行為管理員" | 在勒索軟體復原中設定、管理和查看可疑使用者行為偵測、警報和監控。 |
| "勒索軟體恢復用戶行為檢視器" | 查看勒索軟體復原中的可疑使用者行為警報和見解。 |
| SnapCenter管理員 | 提供使用NetApp Backup and Recovery從本機ONTAP叢集備份應用程式快照的功能。具有此角色的成員可以完成以下操作：* 從“備份和恢復”>“應用程式”完成任何操作* 管理他們具有權限的項目和資料夾中的所有系統* 使用所有NetApp Console服務SnapCenter沒有查看者角色。 |

相關連結

- "了解NetApp Console身分和存取管理"
- "開始使用NetApp Console IAM"
- "管理NetApp Console成員及其權限"
- "了解NetApp Console IAM 的 API"

# 為使用者指派平台角色，以授予管理NetApp Console、指派角色、新增使用者、建立控制台代理程式和管理聯合的權限。

大型跨國組織的組織角色範例

XYZ 公司按地區（北美、歐洲和亞太地區）組織資料儲存訪問，從而提供區域控制和集中監督。

XYZ 公司控制台中的*組織管理員*為每個區域建立一個初始組織和單獨的資料夾。每個區域的*資料夾或專案管理員*在該區域的資料夾中組織專案（及相關資源）。

具有「資料夾或專案管理員」角色的區域管理員透過新增資源和使用者來主動管理他們的資料夾。這些區域管理員還可以新增、刪除或重新命名他們管理的資料夾和項目。*組織管理員*繼承任何新資源的權限，保持整個組織的儲存使用情況的可見性。

在同一個組織內，一名使用者被指派了*共同管理員*角色來管理該組織與其企業 IdP 的聯合。該使用者可以新增或刪除聯合組織，但不能管理組織內的使用者或資源。*組織管理員*為使用者指派*共同檢視者*角色，以檢查聯合狀態並查看聯合組織。

下表列出了每個控制台平台角色可以執行的操作。

組織管理角色

| 任務 | 組織管理員 | 資料夾或專案管理員 |
|---|---|---|
| 創建代理 | 是的 | 不 |
| 從控制台建立、修改或刪除系統（新增或發現系統） | 是的 | 是的 |
| 建立資料夾和項目，包括刪除 | 是的 | 不 |
| 重新命名現有資料夾和項目 | 是的 | 是的 |
| 分配角色並新增用戶 | 是的 | 是的 |
| 將資源與資料夾和項目關聯 | 是的 | 是的 |
| 將代理程式與資料夾和項目關聯 | 是的 | 不 |
| 從資料夾和項目中刪除代理 | 是的 | 不 |
| 管理代理程式（編輯證書、設定等） | 是的 | 不 |
| 從管理 > 憑證管理憑證 | 是的 | 是的 |
| 建立、管理和檢視聯合 | 是的 | 不 |
| 透過控制台註冊支援並提交案例 | 是的 | 是的 |
| 使用與明確存取角色無關的資料服務 | 是的 | 是的 |
| 查看審核頁面和通知 | 是的 | 是的 |

聯盟角色

| 任務 | 聯盟管理員 | 聯邦檢視器 |
|---|---|---|
| 創建聯盟 | 是的 | 不 |

| 任務 | 聯盟管理員 | 聯邦檢視器 |
| --- | --- | --- |
| 驗證域名 | 是的 | 不 |
| 將網域新增至聯合 | 是的 | 不 |
| 禁用和刪除聯盟 | 是的 | 不 |
| 測驗聯盟 | 是的 | 不 |
| 查看聯盟及其詳細信息 | 是的 | 是的 |

合作夥伴角色

| 任務 | 合作夥伴管理員 | 合作夥伴檢視器 |
| --- | --- | --- |
| 可以建立合作關係 | 是的 | 不 |
| 為合作夥伴成員指派角色 | 是的 | 不 |
| 可以為合作關係加入成員 | 是的 | 不 |
| 可以查看組織合作關係詳細信息 | 是的 | 是的 |

超級管理員和查看者角色

*超級管理員*角色提供管理控制台功能、儲存和資料服務的完全存取權限。這個角色適合那些監督行政和治理的人。相較之下，「超級查看者」角色提供唯讀存取權限，非常適合需要查看資訊而不進行更改的審計員或利害關係人。

組織應謹慎使用*超級管理員*存取權限，以最大限度地降低安全風險並符合最小特權原則。大多數組織應該分配具有必要權限的細粒度角色，以降低風險並提高可審計性。

超級角色範例

ABC 公司擁有一個由五人組成的小團隊，利用NetApp Console進行資料服務和儲存管理。他們沒有分配多個角色，而是將「超級管理員」角色分配給兩名高階團隊成員，由他們負責所有管理任務，包括使用者管理和資源配置。其餘三名團隊成員被分配了*超級查看者*角色，允許他們監控儲存健康和數據服務狀態，但無法修改設定。

| 角色 | 繼承的角色 |
| --- | --- |
| 超管理員 | • 組織管理員<br>• 資料夾或專案管理員<br>• 聯盟管理員<br>• 合作夥伴管理員<br>• 勒索軟體抵禦能力管理員<br>• 災難復原管理員<br>• 備份超級管理員<br>• 儲存管理員<br>• Keystone管理員<br>• Google Cloud NetApp Volumes管理員 |
| 超觀眾 | • 組織檢視器<br>• 聯邦檢視器<br>• 合作夥伴檢視器<br>• 勒索軟體復原力檢視器<br>• 災難復原檢視器<br>• 備份檢視器<br>• 儲存檢視器<br>• Keystone檢視器<br>• Google Cloud NetApp Volumes檢視器 |

應用程式角色

#### NetApp Console中的Google Cloud NetApp Volumes角色

## 您可以為使用者指派以下角色，以便他們能夠存取NetApp Console中的Google Cloud NetApp Volumes。

Google Cloud NetApp Volumes使用下列角色：

- * Google Cloud NetApp Volumes管理員*：在控制台中發現並管理Google Cloud NetApp Volumes 。
- * Google Cloud NetApp Volumes檢視器*：在控制台中檢視Google Cloud NetApp Volumes 。

#### NetApp Console中的Keystone存取角色

## Keystone角色提供對Keystone儀表板的存取權限，並允許使用者查看和管理他們的Keystone訂閱。 Keystone角色有兩種： Keystone管理員和Keystone檢視者。這兩個角

色的主要區別在於他們在Keystone中可以採取的行動。 Keystone管理員角色是唯一允許建立服務要求或修改訂閱的角色。

**NetApp Console**中的**Keystone**角色範例

XYZ 公司有四名來自不同部門的儲存工程師查看Keystone訂閱資訊。雖然所有這些用戶都需要監控Keystone訂閱，但只有團隊負責人才被允許提出服務要求。團隊中的三名成員被賦予 * Keystone查看者* 角色，而團隊負責人被賦予 * Keystone管理員* 角色，以便對公司的服務請求進行控制。

下表列出了每個Keystone角色可以執行的操作。

| 特徵和動作 | **Keystone**管理員 | **Keystone**檢視器 |
|---|---|---|
| 查看以下選項卡：訂閱、資產、監控和管理 | 是的 | 是的 |
| * Keystone訂閱頁面*： | | |
| 查看訂閱 | 是的 | 是的 |
| 修改或續訂 | 是的 | 不 |
| * Keystone資產頁面*： | | |
| 查看資產 | 是的 | 是的 |
| 管理資產 | 是的 | 不 |
| * Keystone警報頁面*： | | |
| 查看警報 | 是的 | 是的 |
| 管理警報 | 是的 | 不 |
| 為自己創建提醒 | 是的 | 是的 |
| **Licenses and subscriptions**： | | |
| 可以查看授權和訂閱 | 是的 | 是的 |
| * Keystone報告頁面*： | | |
| 下載報告 | 是的 | 是的 |
| 管理報告 | 是的 | 是的 |
| 為自己建立報告 | 是的 | 是的 |
| 服務請求： | | |
| 建立服務請求 | 是的 | 不 |

| 特徵和動作 | Keystone管理員 | Keystone檢視器 |
| --- | --- | --- |
| 查看組織內任何使用者建立的服務請求 | 是的 | 是的 |

### NetApp Console的營運支援分析師存取角色

您可以將營運支援分析師角色指派給用戶，以便他們能夠存取警報和監控功能。具有此角色的使用者還可以開啟支援案例。

營運支援分析師

| 任務 | 可以執行 |
| --- | --- |
| 從「設定」>「憑證」管理自己的使用者憑證 | 是的 |
| 查看發現的資源 | 是的 |
| 透過控制台註冊支援並提交案例 | 是的 |
| 查看審核頁面和通知 | 是的 |
| 查看、下載和設定警報 | 是的 |

### NetApp Console的儲存存取角色

您可以為使用者指派以下角色，以便他們存取NetApp Console中的儲存管理功能。您可以為使用者指派管理角色來管理儲存或指派檢視者角色來監控。

NetApp Console合作夥伴 API 不會提供這些角色。

管理員可以為使用者指派以下儲存資源和功能的儲存角色：

儲存資源：

- 本地ONTAP集群
- StorageGRID
- E系列

控制台服務和功能：

- 數位顧問
- 軟體更新
- 生命週期規劃
- 永續性

### NetApp Console中的儲存角色範例

XYZ 公司是一家跨國公司，擁有龐大的儲存工程師和儲存管理員團隊。它們允許該團隊管理其所在地區的儲存資產，同時限制對核心控制台任務（如使用者管理、代理建立和許可證管理）的存取。

在一個由 12 人組成的團隊中，有兩名使用者被賦予「儲存檢視者」角色，這使他們能夠監控與他們被分配到的控制台專案相關的儲存資源。其餘九人被賦予*儲存管理員*角色，包括管理軟體更新、透過控制台存取ONTAP系統管理員以及發現儲存資源（新增系統）的能力。團隊中的一名成員被賦予*系統健康專家*角色，以便他們可以管理其所在區域的儲存資源的健康狀況，但不能修改或刪除任何系統。此人還可以對其所分配項目的儲存資源執行軟體更新。

該組織還有兩個具有「組織管理員」角色的用戶，他們可以管理控制台的所有方面，包括用戶管理、代理創建和許可證管理，還有幾個具有「資料夾或專案管理員」角色的用戶，他們可以對分配到的資料夾和專案執行控制台管理任務。

下表顯示了每個儲存角色執行的操作。

| 特徵和動作 | 儲存管理員 | 系統健康專家 | 儲存檢視器 |
|---|---|---|---|
| 儲存管理： | | | |
| 發現新資源（創建系統） | 是的 | 是的 | 不 |
| 查看發現的系統 | 是的 | 是的 | 不 |
| 從控制台刪除系統 | 是的 | 不 | 不 |
| 修改系統 | 是的 | 不 | 不 |
| 建立代理 | 不 | 不 | 不 |
| 數位顧問 | | | |
| 查看所有頁面和功能 | 是的 | 是的 | 是的 |
| **Licenses and subscriptions** | | | |
| 查看所有頁面和功能 | 不 | 不 | 不 |
| 軟體更新 | | | |
| 查看登陸頁面和建議 | 是的 | 是的 | 是的 |
| 審查潛在的版本建議和主要優點 | 是的 | 是的 | 是的 |
| 查看叢集的更新詳細信息 | 是的 | 是的 | 是的 |
| 執行更新前檢查並下載升級計劃 | 是的 | 是的 | 是的 |
| 安裝軟體更新 | 是的 | 是的 | 不 |
| 生命週期規劃 | | | |
| 審查容量規劃狀態 | 是的 | 是的 | 是的 |

| 特徵和動作 | 儲存管理員 | 系統健康專家 | 儲存檢視器 |
| --- | --- | --- | --- |
| 選擇下一步行動（最佳實踐、層級） | 是的 | 不 | 不 |
| 將冷數據分層到雲端儲存並釋放儲存空間 | 是的 | 是的 | 不 |
| 設定提醒 | 是的 | 是的 | 是的 |
| 永續性 | | | |
| 查看儀表板和建議 | 是的 | 是的 | 是的 |
| 下載報告數據 | 是的 | 是的 | 是的 |
| 編輯碳減排百分比 | 是的 | 是的 | 不 |
| 修復建議 | 是的 | 是的 | 不 |
| 延後建議 | 是的 | 是的 | 不 |
| 系統管理員存取 | | | |
| 可以輸入憑證 | 是的 | 是的 | 不 |
| 證書 | | | |
| 使用者憑證 | 是的 | 是的 | 不 |

數據服務角色

#### NetApp Console中的NetApp Backup and Recovery角色

## 您可以為使用者指派以下角色，以便他們存取控制台內的NetApp Backup and Recovery。備份和復原角色可讓您靈活地為使用者指派特定於他們需要在組織內完成的任務的角色。如何分配角色取決於您自己的業務和儲存管理實踐。

該服務使用特定於NetApp Backup and Recovery 的以下角色。

- 備份和還原超級管理員：在NetApp Backup and Recovery中執行任何操作。
- 備份和還原備份管理員：在NetApp Backup and Recovery中執行備份到本機快照、複製到二級儲存以及備份到物件儲存作業。
- 備份和還原復原管理員：使用NetApp Backup and Recovery復原工作負載。
- 備份和還原克隆管理：使用NetApp Backup and Recovery應用程式和資料。
- 備份和還原檢視器：查看NetApp Backup and Recovery中的信息，但不執行任何操作。

有關所有NetApp Console訪問角色的詳細信息，請參閱 "控制台設定和管理文檔"。

用於常見操作的角色

下表列出了每個NetApp Backup and Recovery角色可以針對所有工作負載執行的操作。

| 特徵和動作 | 備份和恢復超級管理員 | 備份和還原備份管理員 | 備份和還原復原管理員 | 備份和還原克隆管理員 | 備份和還原檢視器 |
|---|---|---|---|---|---|
| 新增、編輯或刪除主機 | 是的 | 不 | 不 | 不 | 不 |
| 安裝插件 | 是的 | 不 | 不 | 不 | 不 |
| 新增憑證（主機、實例、vCenter） | 是的 | 不 | 不 | 不 | 不 |
| 查看儀表板和所有選項卡 | 是的 | 是的 | 是的 | 是的 | 是的 |
| 開始免費試用 | 是的 | 不 | 不 | 不 | 不 |
| 啟動工作負載發現 | 不 | 是的 | 是的 | 是的 | 不 |
| 查看許可證資訊 | 是的 | 是的 | 是的 | 是的 | 是的 |
| 啟動許可證 | 是的 | 不 | 不 | 不 | 不 |
| 查看主機 | 是的 | 是的 | 是的 | 是的 | 是的 |
| 時間表： | | | | | |
| 啟動計劃 | 是的 | 是的 | 是的 | 是的 | 不 |
| 暫停時間表 | 是的 | 是的 | 是的 | 是的 | 不 |
| 政策與保護： | | | | | |
| 查看保護計劃 | 是的 | 是的 | 是的 | 是的 | 是的 |
| 建立、修改或刪除保護計劃 | 是的 | 是的 | 不 | 不 | 不 |
| 恢復工作負載 | 是的 | 不 | 是的 | 不 | 不 |
| 建立、拆分或刪除克隆 | 是的 | 不 | 不 | 是的 | 不 |
| 建立、修改或刪除策略 | 是的 | 是的 | 不 | 不 | 不 |
| 報告： | | | | | |
| 查看報告 | 是的 | 是的 | 是的 | 是的 | 是的 |

| 特徵和動作 | 備份和恢復超級管理員 | 備份和還原備份管理員 | 備份和還原復原管理員 | 備份和還原克隆管理員 | 備份和還原檢視器 |
|---|---|---|---|---|---|
| 建立報告 | 是的 | 是的 | 是的 | 是的 | 不 |
| 刪除報告 | 是的 | 不 | 不 | 不 | 不 |
| 從**SnapCenter**匯入並管理主機： | | | | | |
| 查看導入的SnapCenter數據 | 是的 | 是的 | 是的 | 是的 | 是的 |
| 從SnapCenter匯入數據 | 是的 | 是的 | 不 | 不 | 不 |
| 管理（遷移）主機 | 是的 | 是的 | 不 | 不 | 不 |
| 配置設定： | | | | | |
| 配置日誌目錄 | 是的 | 是的 | 是的 | 不 | 不 |
| 關聯或刪除實例憑證 | 是的 | 是的 | 是的 | 不 | 不 |
| 桶： | | | | | |
| 查看儲存桶 | 是的 | 是的 | 是的 | 是的 | 是的 |
| 建立、編輯或刪除儲存桶 | 是的 | 是的 | 不 | 不 | 不 |

用於特定於工作負載的操作的角色

下表列出了每個NetApp Backup and Recovery角色可以針對特定工作負載執行的動作。

**Kubernetes** 工作負載

此表顯示了每個NetApp Backup and Recovery角色可以針對特定於 Kubernetes 工作負載的操作執行的操作。

| 特徵和動作 | 備份和恢復超級管理員 | 備份和還原備份管理員 | 備份和還原復原管理員 | 備份和還原檢視器 |
|---|---|---|---|---|
| 查看叢集、命名空間、儲存類別和 API 資源 | 是的 | 是的 | 是的 | 是的 |
| 新增的 Kubernetes 集群 | 是的 | 是的 | 不 | 不 |
| 更新叢集配置 | 是的 | 不 | 不 | 不 |
| 從管理中刪除集群 | 是的 | 不 | 不 | 不 |
| 查看應用程式 | 是的 | 是的 | 是的 | 是的 |

| 特徵和動作 | 備份和恢復超級管理員 | 備份和還原備份管理員 | 備份和還原復原管理員 | 備份和還原檢視器 |
| --- | --- | --- | --- | --- |
| 建立和定義新的應用程式 | 是的 | 是的 | 不 | 不 |
| 更新應用程式配置 | 是的 | 是的 | 不 | 不 |
| 從管理中刪除應用程式 | 是的 | 是的 | 不 | 不 |
| 查看受保護的資源和備份狀態 | 是的 | 是的 | 是的 | 是的 |
| 建立備份並使用策略保護應用程式 | 是的 | 是的 | 不 | 不 |
| 取消保護應用程式並刪除備份 | 是的 | 是的 | 不 | 不 |
| 查看恢復點和資源檢視器結果 | 是的 | 是的 | 是的 | 是的 |
| 從復原點還原應用程式 | 是的 | 不 | 是的 | 不 |
| 查看 Kubernetes 備份策略 | 是的 | 是的 | 是的 | 是的 |
| 建立 Kubernetes 備份策略 | 是的 | 是的 | 是的 | 不 |
| 更新備份策略 | 是的 | 是的 | 是的 | 不 |
| 刪除備份策略 | 是的 | 是的 | 是的 | 不 |
| 查看執行鉤子和鉤子來源 | 是的 | 是的 | 是的 | 是的 |
| 建立執行鉤子和鉤子來源 | 是的 | 是的 | 是的 | 不 |
| 更新執行鉤子和鉤子來源 | 是的 | 是的 | 是的 | 不 |
| 刪除執行鉤子和鉤子來源 | 是的 | 是的 | 是的 | 不 |
| 查看執行鉤子模板 | 是的 | 是的 | 是的 | 是的 |
| 建立執行鉤子模板 | 是的 | 是的 | 是的 | 不 |
| 更新執行鉤子模板 | 是的 | 是的 | 是的 | 不 |
| 刪除執行鉤子模板 | 是的 | 是的 | 是的 | 不 |

| 特徵和動作 | 備份和恢復超級管理員 | 備份和還原備份管理員 | 備份和還原復原管理員 | 備份和還原檢視器 |
|---|---|---|---|---|
| 查看工作負載摘要和分析儀表板 | 是的 | 是的 | 是的 | 是的 |
| 查看StorageGRID儲存桶和儲存目標 | 是的 | 是的 | 是的 | 是的 |

#### NetApp Console中的NetApp Disaster Recovery角色

## 您可以為使用者指派以下角色，以便他們存取控制台內的NetApp Disaster Recovery。災難復原角色可讓您靈活地為使用者指派特定於他們需要在組織內完成的任務的角色。如何分配角色取決於您自己的業務和儲存管理實踐。

災難復原使用以下角色：

- 災難復原管理員：執行任何動作。
- 災難復原故障轉移管理：執行故障轉移和遷移。
- 災難復原應用程式管理員：建立複製計劃。修改複製計劃。開始測試故障轉移。
- 災難復原檢視器：僅查看資訊。

下表列出了每個角色可以執行的操作。

| 特徵和動作 | 災難復原管理員 | 災難復原故障轉移管理員 | 災難復原應用程式管理員 | 災難復原檢視器 |
|---|---|---|---|---|
| 查看儀表板和所有選項卡 | 是的 | 是的 | 是的 | 是的 |
| 開始免費試用 | 是的 | 不 | 不 | 不 |
| 啟動工作負載發現 | 是的 | 不 | 不 | 不 |
| 查看許可證資訊 | 是的 | 是的 | 是的 | 是的 |
| 啟動許可證 | 是的 | 不 | 是的 | 不 |
| 在「網站」標籤上： | | | | |
| 查看網站 | 是的 | 是的 | 是的 | 是的 |
| 新增、修改或刪除站點 | 是的 | 不 | 不 | 不 |
| 在複製計劃標籤上： | | | | |
| 查看複製計劃 | 是的 | 是的 | 是的 | 是的 |
| 查看複製計劃詳細信息 | 是的 | 是的 | 是的 | 是的 |

| 特徵和動作 | 災難復原管理員 | 災難復原故障轉移管理員 | 災難復原應用程式管理員 | 災難復原檢視器 |
|---|---|---|---|---|
| 建立或修改複製計劃 | 是的 | 是的 | 是的 | 不 |
| 建立報告 | 是的 | 不 | 不 | 不 |
| 查看快照 | 是的 | 是的 | 是的 | 是的 |
| 執行故障轉移測試 | 是的 | 是的 | 是的 | 不 |
| 執行故障轉移 | 是的 | 是的 | 不 | 不 |
| 執行故障回復 | 是的 | 是的 | 不 | 不 |
| 執行遷移 | 是的 | 是的 | 不 | 不 |
| 在資源組標籤上： | | | | |
| 查看資源組 | 是的 | 是的 | 是的 | 是的 |
| 建立、修改或刪除資源組 | 是的 | 不 | 是的 | 不 |
| 在「作業監控」標籤上： | | | | |
| 查看職位 | 是的 | 不 | 是的 | 是的 |
| 取消作業 | 是的 | 是的 | 是的 | 不 |

**NetApp Console**的勒索軟體恢復存取角色

## 勒索軟體復原角色為使用者提供對NetApp Ransomware Resilience的存取權限。勒索軟體復原能力支援以下角色：

基線角色

- 勒索軟體復原管理員 - 配置勒索軟體復原設定；調查並回應加密警報
- 勒索軟體復原力檢視器 - 查看加密事件、報告和發現設置

使用者行為活動角色"可疑用戶活動偵測"警報提供對檔案活動事件等資料的可見性；這些警報包括檔案名稱和使用者執行的檔案操作（例如讀取、寫入、刪除、重新命名）。為了限制這些資料的可見性，只有具有這些角色的使用者才能管理或查看這些警報。

- 勒索軟體恢復用戶行為管理員 - 啟動可疑用戶活動檢測，調查並響應可疑用戶活動警報
- 勒索軟體恢復用戶行為檢視器 - 查看可疑用戶活動警報

使用者行為角色不是獨立角色；它們旨在添加到勒索軟體復原管理員或查看者角色中。有關詳細信息，請參閱 [使用者行為角色]。

有關每個角色的詳細描述，請參閱下表。

基線角色

下表描述了勒索軟體復原管理員和檢視者角色可執行的操作。

| 特徵和動作 | 勒索軟體抵禦能力管理員 | 勒索軟體復原力檢視器 |
|---|---|---|
| 查看儀表板和所有選項卡 | 是的 | 是的 |
| 在儀表板上更新推薦狀態 | 是的 | 不 |
| 開始免費試用 | 是的 | 不 |
| 啟動工作負載發現 | 是的 | 不 |
| 啟動工作負載的重新發現 | 是的 | 不 |
| 在「保護」標籤上： | | |
| 新增、修改或刪除加密策略的保護計劃 | 是的 | 不 |
| 保護工作負載 | 是的 | 不 |
| 透過資料分類識別敏感資料的暴露 | 是的 | 不 |
| 列出保護計劃和細節 | 是的 | 是的 |
| 列出保護組 | 是的 | 是的 |
| 查看保護組詳細信息 | 是的 | 是的 |
| 建立、編輯或刪除保護群組 | 是的 | 不 |
| 下載數據 | 是的 | 是的 |
| 在「警報」標籤上： | | |
| 查看加密警報和警報詳細信息 | 是的 | 是的 |
| 編輯加密事件狀態 | 是的 | 不 |

| 特徵和動作 | 勒索軟體抵禦能力管理員 | 勒索軟體復原力檢視器 |
| --- | --- | --- |
| 標記加密警報以供恢復 | 是的 | 不 |
| 查看加密事件詳細信息 | 是的 | 是的 |
| 解除或解決加密事件 | 是的 | 不 |
| 取得加密事件中受影響文件的完整列表 | 是的 | 不 |
| 下載加密事件警報數據 | 是的 | 是的 |
| 封鎖使用者（使用工作負載安全代理程式配置） | 是的 | 不 |
| 在「恢復」標籤上： | | |
| 下載加密事件中受影響的文件 | 是的 | 不 |
| 從加密事件中恢復工作負載 | 是的 | 不 |
| 從加密事件下載恢復數據 | 是的 | 是的 |
| 下載加密事件報告 | 是的 | 是的 |
| 在「設定」標籤上： | | |
| 新增或修改備份目標 | 是的 | 不 |
| 列出備份目的地 | 是的 | 是的 |
| 查看已連接的 SIEM 目標 | 是的 | 是的 |
| 新增或修改 SIEM 目標 | 是的 | 不 |
| 配置準備演練 | 是的 | 不 |
| 開始、重置或編輯準備情況演練 | 是的 | 不 |
| 審查準備演習狀態 | 是的 | 是的 |
| 更新發現配置 | 是的 | 不 |
| 查看發現配置 | 是的 | 是的 |
| 在「報告」標籤上： | | |

| 特徵和動作 | 勒索軟體抵禦能力管理員 | 勒索軟體復原力檢視器 |
| --- | --- | --- |
| 下載報告 | 是的 | 是的 |

使用者行為角色

若要配置可疑使用者行為設定並回應警報，使用者必須具有勒索軟體復原使用者行為管理員角色。要僅查看可疑用戶行為警報，用戶應具有勒索軟體恢復用戶行為查看者角色。

應將使用者行為角色授予具有現有勒索軟體復原管理員或檢視者權限且需要存取"可疑用戶活動設定和警報"。例如，具有勒索軟體復原管理員角色的使用者應該獲得勒索軟體復原使用者行為管理員角色來配置使用者活動代理並封鎖或解除封鎖使用者。不應將勒索軟體復原使用者行為管理員角色授予勒索軟體復原檢視者。

若要啟動可疑使用者活動偵測，您必須具有控制台組織管理員角色。

下表描述了勒索軟體復原使用者行為管理員和檢視者角色可執行的操作。

| 特徵和動作 | 勒索軟體復原力用戶行為管理員 | 勒索軟體恢復用戶行為檢視器 |
| --- | --- | --- |
| 在「設定」標籤上： | | |
| 建立、修改或刪除用戶活動代理 | 是的 | 不 |
| 建立或刪除使用者目錄連接器 | 是的 | 不 |
| 暫停或恢復資料收集器 | 是的 | 不 |
| 進行資料外洩準備演習 | 是的 | 不 |
| 在「保護」標籤上： | | |
| 新增、修改或刪除可疑使用者行為策略的保護計劃 | 是的 | 不 |
| 在「警報」標籤上： | | |
| 查看用戶活動警報和警報詳細信息 | 是的 | 是的 |
| 編輯使用者活動事件狀態 | 是的 | 不 |
| 標記用戶活動警報以供恢復 | 是的 | 不 |
| 查看用戶活動事件詳細信息 | 是的 | 是的 |
| 解除或解決使用者活動事件 | 是的 | 不 |
| 取得可疑使用者受影響文件的完整列表 | 是的 | 是的 |

| 特徵和動作 | 勒索軟體復原力用戶行為管理員 | 勒索軟體恢復用戶行為檢視器 |
| --- | --- | --- |
| 下載用戶活動事件警報數據 | 是的 | 是的 |
| 封鎖或取消封鎖用戶 | 是的 | 不 |
| 在「恢復」標籤上： | | |
| 下載使用者活動事件受影響的文件 | 是的 | 不 |
| 從使用者活動事件恢復工作負載 | 是的 | 不 |
| 從用戶活動事件下載恢復數據 | 是的 | 是的 |
| 從用戶活動事件下載報告 | 是的 | 是的 |

# 身分和存取 API

## 組織和專案 ID

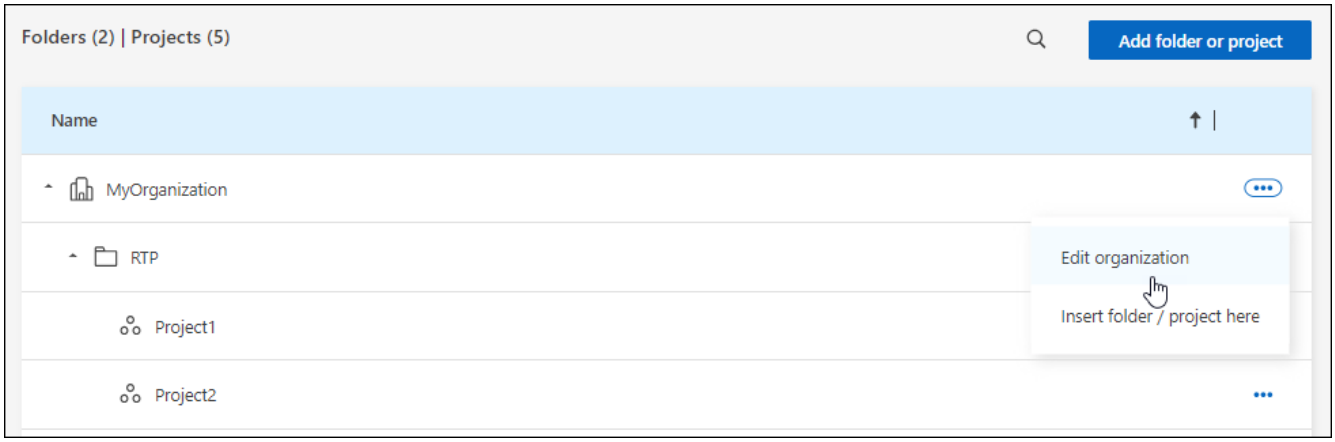
您的NetApp Console組織有一個名稱和一個 ID。您可以為您的組織選擇一個名稱以幫助識別它。您可能還需要檢索某些整合的組織 ID。

### 重新命名您的組織

您可以重新命名您的組織。如果您支持的不僅僅是組織，這將很有幫助。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇*組織*。
3. 從「組織」頁面，導覽至表格的第一行，選擇 ••• 然後選擇*編輯組織*。




4. 輸入新的組織名稱並選擇*套用*。

#### 取得組織 ID

組織 ID 用於與控制台的某些整合。

您可以從組織頁面查看組織 ID，並根據需要將其複製到剪貼簿。

步驟

1. 選擇*管理>身分和存取*>*組織*。
2. 在*組織*頁面上，在摘要欄中尋找您的組織 ID 並將其複製到剪貼簿。您可以保存它以供以後使用，或直接將其複製到需要使用它的地方。

#### 取得專案ID

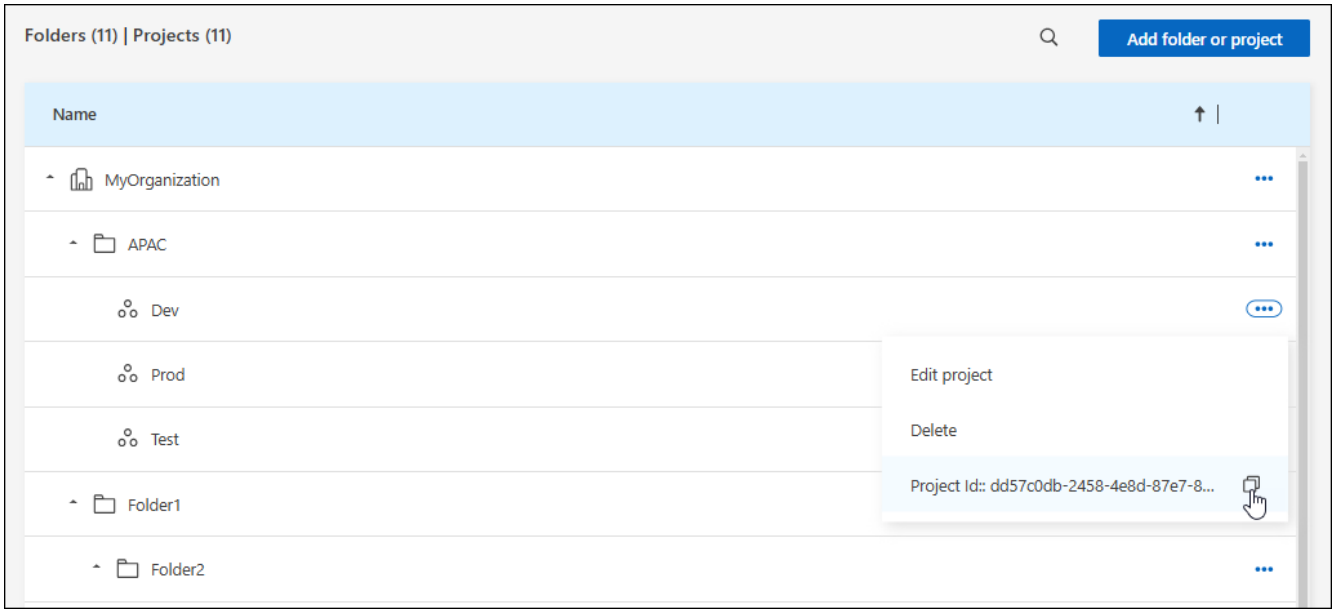
如果您使用 API，則需要取得項目的 ID。例如，在建立Cloud Volumes ONTAP系統時。

步驟

1. 從“組織”頁面，導航到表中的項目並選擇 •••

   顯示項目 ID。

2. 若要複製 ID，請選擇複製按鈕。




相關資訊

- "了解身分和存取管理"
- "開始使用身分和存取權限"
- "了解身分和存取 API"

# 安全與合規

# 身分聯合

## 使用NetApp Console的身份聯合實作單一登入

單一登入（聯合）允許使用者使用其公司憑證登入NetApp Console，從而簡化了登入流程並增強了安全性。您可以使用身分識別提供者 (IdP) 或NetApp支援網站啟用單一登入 (SSO)。

### 所需角色

組織管理員、聯盟管理員、聯盟檢視器。"了解有關訪問角色的更多資訊。"

### 透過 NetApp Support Site 進行單一登入

與NetApp支援網站聯合允許使用者使用相同的憑證登入控制台、 Active IQ Digital Advisor和其他相關應用程式。

如果您與NetApp支援網站聯合，則您不能與您的企業身分管理提供者聯合。選擇最適合您組織的一種。

### 步驟

1. 下載並完成 "NetApp聯合申請表"。
2. 將表格提交至表格中指定的電子郵件地址。

   NetApp支援團隊將審核並處理您的請求。

### 使用身分提供者進行單一登入

您可以與身分識別提供者建立聯合連接，以便為控制台啟用單一登入 (SSO)。這個過程涉及配置您的身分提供者以信任NetApp作為服務提供者，然後在控制台中建立連線。

如果您之前使用NetApp Cloud Central（控制台的外部應用程式）配置了聯合，則需要使用聯合頁面匯入聯合以在控制台內進行管理。"了解如何導入您的聯盟。"

### 支援的身份提供者

NetApp支援以下聯合協定和身分提供者：

協定

- 安全性斷言標記語言 (SAML) 身分提供者
- Active Directory 聯合驗證服務 (AD FS)

身分提供者

- 微軟Entra ID
- Ping聯邦

## 與NetApp Console聯合工作流程

NetApp僅支援服務供應商發起的（SP發起的） SSO。您需要先配置身分提供者以信任NetApp作為服務提供者。然後，您可以在控制台中建立使用身分提供者配置的連線。

您可以與您的電子郵件網域或您擁有的其他網域聯合。若要與不同於您的電子郵件網域的網域聯合，請先驗證您擁有該網域。

### 1 驗證您的網域名稱（如果不使用您的電子郵件網域）

若要與不同於您的電子郵件網域的網域聯合，請驗證您擁有該網域。您無需任何額外步驟即可聯合您的電子郵件網域。

### 2 配置您的 IdP 以信任NetApp作為服務提供者

透過建立新應用程式並提供 ACS URL、實體 ID 或其他憑證資訊等詳細信息，將您的身分提供者配置為信任NetApp 。服務提供者資訊因身分提供者而異，因此請參閱特定身分提供者的文件以了解詳細資訊。您需要與您的 IdP 管理員合作來完成此步驟。

### 3 在控制台中建立聯合連接

提供來自身分提供者的 SAML 元資料 URL 或檔案以建立連線。此資訊用於建立控制台和您的身分提供者之間的信任關係。您提供的資訊取決於您使用的 IdP。例如，如果您使用 Microsoft Entra ID，則需要提供用戶端 ID、金鑰和網域。

### 4 在控制台中測試您的聯盟

在啟用聯合連線之前對其進行測試。使用控制台中聯合頁面上的測試選項來驗證您的測試使用者是否可以成功進行身份驗證。如果測試成功，則可以啟用連線。

### 5 在控制台中啟用您的連接

啟用連線後，使用者可以使用其公司憑證登入控制台。

查看對應協議或 IdP 的主題以開始：

- "與 AD FS 設定聯合連接"
- "與 Microsoft Entra ID 建立聯合連接"
- "使用 PingFederate 設定聯合連接"
- "與 SAML 身分提供者建立聯合連接"

## 網域驗證

### 驗證聯合連線的電子郵件網域

如果您想要與不同於您的電子郵件網域的網域聯合，您必須先驗證您擁有該網域。您只能使用已驗證的網域進行聯合。

必備角色

需要聯盟管理員角色來創建和管理聯盟。聯盟檢視者可以查看聯盟頁面。"了解有關訪問角色的更多資訊。"

驗證您的網域名稱涉及向您的網域的 DNS 設定新增 TXT 記錄。此記錄用於證明您擁有該網域並允許NetApp Console信任該網域進行聯合。您可能需要與您的 IT 或網路管理員協調來完成此步驟。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇“**Federation**”以查看“**Federations**”頁面。
3. 選擇*配置新聯合*。
4. 選擇*驗證網域所有權*。
5. 輸入您要驗證的網域並選擇*繼續*。
6. 複製提供的 TXT 記錄。
7. 轉到您網域的 DNS 設定並配置作為您網域的 TXT 記錄提供的 TXT 值。如果需要，請與您的 IT 或網路管理員合作。
8. 新增TXT記錄後，返回控制台並選擇*驗證*。

配置聯合

#### 將**NetApp Console**與 **Active Directory** 聯合服務 **(AD FS)** 聯合起來

## 將您的 Active Directory 聯合驗證服務 (AD FS) 與NetApp Console聯合起來，以便為NetApp Console啟用單一登入 (SSO)。這允許用戶使用他們的公司憑證登入控制台。

必備角色

需要聯盟管理員角色來創建和管理聯盟。聯盟檢視者可以查看聯盟頁面。"了解有關訪問角色的更多資訊。"

您可以與您的企業 IdP 或NetApp支援網站聯合。 NetApp建議選擇其中一個，但不要同時選擇兩者。

NetApp僅支援服務供應商發起的（SP發起的） SSO。首先，配置身分提供者以信任NetApp Console作為服務提供者。然後，使用您的身分提供者的配置在控制台中建立連線。

您可以與 AD FS 伺服器建立聯合，以啟用NetApp Console的單一登入 (SSO)。這個過程涉及配置您的 AD FS 以信任控制台作為服務提供者，然後在NetApp Console中建立連線。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇“**Federation**”以查看“**Federations**”頁面。
3. 選擇*配置新聯合*。
4. 輸入您的網域詳細資料：
    a. 選擇您是否要使用已驗證的網域或您的電子郵件網域。電子郵件網域是與您登入的帳戶關聯的網域。
    b. 輸入您正在設定的聯盟的名稱。

c. 如果您選擇已驗證的網域，請從清單中選擇該網域。

5. 選擇“下一步”。
6. 對於您的連線方法，選擇*協定*，然後選擇*Active Directory 聯合驗證服務 (AD FS)*。
7. 選擇“下一步”。
8. 在您的 AD FS 伺服器中建立依賴方信任。您可以使用 PowerShell 或在 AD FS 伺服器上手動設定它。有關如何建立信賴方信任的詳細信息，請參閱 AD FS 文件。

   a. 使用以下腳本透過 PowerShell 建立信任：

   ```
   (new-object Net.WebClient -property @{Encoding = [Text.Encoding]
   ::UTF8}).DownloadString("https://raw.github.com/auth0/AD FS-
   auth0/master/AD FS.ps1") | iex
   AddRelyingParty "urn:auth0:netapp-cloud-account" "https://netapp-
   cloud-account.auth0.com/login/callback"
   ```

   b. 或者，您可以在 AD FS 管理控制台中手動建立信任。建立信任時使用以下NetApp Console值：

      - 建立依賴信任識別碼時，使用 **YOUR_TENANT** 值： `netapp-cloud-account`
      - 當您選擇 啟用對 **WS-Federation** 的支援 時，請使用 **YOUR_AUTH0_DOMAIN** 值： `netapp-cloud-account.auth0.com`

   c. 建立信任後，從 AD FS 伺服器複製元資料 URL 或下載聯合元資料檔。您需要此 URL 或檔案來完成控制台中的連線。

   NetApp建議使用元資料 URL 讓NetApp Console自動擷取最新的 AD FS 設定。如果您下載聯合元資料文件，則每當 AD FS 配置發生變更時，都需要在NetApp Console中手動更新它。

9. 返回控制台，然後選擇「下一步」來建立連線。
10. 建立與 AD FS 的連線。

    a. 輸入您在上一個步驟中從 AD FS 伺服器複製的 **AD FS URL** 或上傳您從 AD FS 伺服器下載的聯合元資料檔案。

11. 選擇*建立連線*。建立連線可能需要幾秒鐘。
12. 選擇“下一步”。
13. 選擇*測試連線*來測試您的連線。您將被引導至 IdP 伺服器的登入頁面。使用您的身分提供者憑證登入。登入後，返回控制台啟用連線。

    在受限模式下使用控制台時，請將 URL 複製到隱身瀏覽器視窗或單獨的瀏覽器中，以登入您的身分提供者 (IdP)。

14. 在控制台中，選擇「下一步」以查看摘要頁面。
15. 設定通知。

    您可以選擇七天或三十天。系統會透過電子郵件向具有以下角色的任何使用者發送到期通知，並在控制台中顯示這些通知：超級管理員、組織管理員、聯盟管理員和聯盟檢視者。

16. 查看聯盟詳細信息，然後選擇“啟用聯盟”。
17. 選擇“完成”以完成該過程。

啟用聯合身份驗證後，使用者可以使用其企業憑證登入NetApp Console。

#### 將**NetApp Console**與 **Microsoft Entra ID** 聯合起來

## 與您的 Microsoft Entra ID IdP 提供者聯合，為NetApp Console啟用單一登入 (SSO)。這允許用戶使用他們的公司憑證登入。

### 必備角色

需要聯盟管理員角色來創建和管理聯盟。聯盟檢視者可以查看聯盟頁面。"了解有關訪問角色的更多資訊。"

您可以與您的企業 IdP 或NetApp支援網站聯合。 NetApp建議選擇其中一個，但不要同時選擇兩者。

NetApp僅支援服務供應商發起的（SP發起的） SSO。您需要先配置身分提供者以信任NetApp作為服務提供者。然後，您可以在控制台中建立使用身分提供者配置的連線。

您可以與 Microsoft Entra ID 建立聯合連接，以啟用控制台的單一登入 (SSO)。這個過程涉及配置您的 Microsoft Entra ID 以信任控制台作為服務提供者，然後在控制台中建立連線。

### 步驟

1. 選擇*管理>身分和存取*。
2. 選擇“**Federation**”以查看“**Federations**”頁面。
3. 選擇*配置新聯合*。

### 域名詳細資訊

1. 輸入您的網域詳細資料：
   a. 選擇您是否要使用已驗證的網域或您的電子郵件網域。電子郵件網域是與您登入的帳戶關聯的網域。
   b. 輸入您正在設定的聯盟的名稱。
   c. 如果您選擇已驗證的網域，請從清單中選擇該網域。
2. 選擇“下一步”。

### 連接方法

1. 對於您的連線方法，選擇*提供者*，然後選擇*Microsoft Entra ID*。
2. 選擇“下一步”。

### 配置說明

1. 配置您的 Microsoft Entra ID 以信任NetApp為服務提供者。您需要在 Microsoft Entra ID 伺服器上執行此步驟。
   a. 註冊 Microsoft Entra ID 應用程式以信任控制台時，請使用下列值：

- 對於 重定向 **URL** ，使用 `https://services.cloud.netapp.com`
- 對於 回覆 **URL**，使用 `https://netapp-cloud-account.auth0.com/login/callback`

b. 為您的 Microsoft Entra ID 應用程式建立客戶端機密。您需要提供客戶端 ID、客戶端金鑰和 Entra ID 網域來完成聯合。

2. 返回控制台，然後選擇「下一步」來建立連線。

建立連接

1. 使用 Microsoft Entra ID 建立連接
   a. 輸入您在上一個步驟中建立的客戶端 ID 和客戶端金鑰。
   b. 輸入 Microsoft Entra ID 網域。
2. 選擇*建立連線*。系統在幾秒鐘內建立連線。

測試並啟用連接

1. 選擇“下一步”。
2. 選擇*測試連線*來測試您的連線。您將被引導至 IdP 伺服器的登入頁面。使用您的身分提供者憑證登入。登入後，返回控制台啟用連線。

> 在受限模式下使用控制台時，請將 URL 複製到隱身瀏覽器視窗或單獨的瀏覽器中，以登入您的身分提供者 (IdP)。

3. 在控制台中，選擇「下一步」以查看摘要頁面。
4. 設定通知。

   您可以選擇七天或三十天。系統會透過電子郵件向具有以下角色的任何使用者發送到期通知，並在控制台中顯示這些通知：超級管理員、組織管理員、聯盟管理員和聯盟檢視者。

5. 查看聯盟詳細信息，然後選擇“啟用聯盟”。
6. 選擇“完成”以完成該過程。

啟用聯合身份驗證後，使用者可以使用其企業憑證登入NetApp Console。

#### 使用 **PingFederate** 聯合**NetApp Console**

與您的 PingFederate IdP 提供者聯合，為NetApp Console啟用單一登入 (SSO)。這允許用戶使用他們的公司憑證登入。

必備角色

需要聯盟管理員角色來創建和管理聯盟。聯盟檢視者可以查看聯盟頁面。"了解有關訪問角色的更多資訊。"

> 您可以與您的企業 IdP 或NetApp支援網站聯合。 NetApp建議選擇其中一個，但不要同時選擇兩者。

NetApp僅支援服務供應商發起的（SP發起的） SSO。您需要先配置身分提供者以信任NetApp作為服務提供者。然後，您可以在控制台中建立使用身分提供者配置的連線。

您可以使用 PingFederate 設定聯合連接，以啟用控制台的單一登入 (SSO)。這個過程涉及配置您的 PingFederate 伺服器以信任控制台作為服務提供者，然後在控制台中建立連線。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇“**Federation**”以查看“**Federations**”頁面。
3. 選擇*配置新聯合*。
4. 輸入您的網域詳細資料：
   a. 選擇您是否要使用已驗證的網域或您的電子郵件網域。電子郵件網域是與您登入的帳戶關聯的網域。
   b. 輸入您正在設定的聯盟的名稱。
   c. 如果您選擇已驗證的網域，請從清單中選擇該網域。
5. 選擇“下一步”。
6. 對於您的連線方法，選擇*提供者*，然後選擇*PingFederate*。
7. 選擇“下一步”。
8. 設定您的 PingFederate 伺服器以信任NetApp為服務提供者。您需要在 PingFederate 伺服器上執行此步驟。
   a. 設定 PingFederate 以信任NetApp Console時，請使用下列值：
      - 對於 回覆 **URL** 或 斷言消費者服務 **(ACS) URL**，使用 `https://netapp-cloud-account.auth0.com/login/callback`
      - 對於*登出 URL*，使用 `https://netapp-cloud-account.auth0.com/logout`
      - 對於*受眾/實體 ID*，使用 `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>`其中 `<fed-domain-name-pingfederate>` 是聯合的網域名稱。例如，如果您的網域是 `example.com`，受眾/實體 ID 將是 `urn:auth0:netappcloud-account:fed-example-com-pingfederate`。
   b. 複製 PingFederate 伺服器 URL。在控制台中建立連線時，您將需要此 URL。
   c. 從您的 PingFederate 伺服器下載 X.509 憑證。它需要採用 Base64 編碼的 PEM 格式（.pem、.crt、.cer）。
9. 返回控制台，然後選擇「下一步」來建立連線。
10. 使用 PingFederate 建立連接
    a. 輸入您在上一個步驟中複製的 PingFederate 伺服器 URL。
    b. 上傳 X.509 簽署憑證。證書必須採用 PEM、CER 或 CRT 格式。
11. 選擇*建立連線*。系統在幾秒鐘內建立連線。
12. 選擇“下一步”。
13. 選擇*測試連線*來測試您的連線。您將被引導至 IdP 伺服器的登入頁面。使用您的身分提供者憑證登入。登入後，返回控制台啟用連線。

> 在受限模式下使用控制台時，請將 URL 複製到隱身瀏覽器視窗或單獨的瀏覽器中，以登入您的身分提供者 (IdP)。

14. 在控制台中，選擇「下一步」以查看摘要頁面。
15. 設定通知。

    您可以選擇七天或三十天。系統會透過電子郵件向具有以下角色的任何使用者發送到期通知，並在控制台中顯示這些通知：超級管理員、組織管理員、聯盟管理員和聯盟檢視者。

16. 查看聯盟詳細信息，然後選擇“啟用聯盟”。
17. 選擇“完成”以完成該過程。

啟用聯合身份驗證後，使用者可以使用其企業憑證登入NetApp Console。

與 **SAML** 身分提供者聯合

# 與您的 SAML 2.0 IdP 提供者聯合，為 NEtApp 控制台啟用單一登入 (SSO)。這允許用戶使用他們的公司憑證登入。

所需角色

需要聯盟管理員角色來創建和管理聯盟。聯盟檢視者可以查看聯盟頁面。"了解有關訪問角色的更多資訊。"

您可以與您的企業 IdP 或NetApp支援網站聯合。你不能與兩者結盟。

NetApp僅支援服務供應商發起的（SP發起的） SSO。您需要先配置身分提供者以信任NetApp作為服務提供者。然後，您可以在控制台中建立使用身分提供者配置的連線。

您可以與 SAML 2.0 提供者建立聯合連接，以便為控制台啟用單一登入 (SSO)。該過程涉及配置您的提供者以信任NetApp作為服務提供者，然後在控制台中建立連接。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇“**Federation**”以查看“**Federations**”頁面。
3. 選擇*配置新聯合*。
4. 輸入您的網域詳細資料：
   a. 選擇您是否要使用已驗證的網域或您的電子郵件網域。電子郵件網域是與您登入的帳戶關聯的網域。
   b. 輸入您正在設定的聯盟的名稱。
   c. 如果您選擇已驗證的網域，請從清單中選擇該網域。
5. 選擇“下一步”。
6. 對於您的連線方法，選擇*協定*，然後選擇*SAML 身分提供者*。
7. 選擇“下一步”。
8. 配置您的 SAML 身分提供者以信任NetApp作為服務提供者。您需要在 SAML 提供者伺服器上執行此步驟。
   a. 確保您的 IdP 具有屬性 `email`設定為使用者的電子郵件地址。這是控制台正確識別使用者所必需的：

```
<saml:AttributeStatement
xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <saml:Attribute Name="email"
NameFormat="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
        <saml:AttributeValue
xsi:type="xs:string">email@domain.com</saml:AttributeValue>
    </saml:Attribute>
</saml:AttributeStatement>
```

1. 在控制台中註冊 SAML 應用程式時，請使用下列值：
   - 對於 回覆 **URL** 或 斷言消費者服務 **(ACS) URL**，使用 `https://netapp-cloud-account.auth0.com/login/callback`
   - 對於*登出 URL*，使用 `https://netapp-cloud-account.auth0.com/logout`
   - 對於*受眾/實體 ID*，使用 `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>`其中 `<fed-domain-name-saml>` 是您想要用於聯合的網域名稱。例如，如果您的網域是 `example.com`，受眾/實體 ID 將是 `urn:auth0:netapp-cloud-account:fed-example-com-samlp`。
2. 建立信任後，從 SAML 提供者伺服器複製以下值：
   - 登入網址
   - 退出 URL（可選）
3. 從您的 SAML 提供者伺服器下載 X.509 憑證。它需要採用 PEM、CER 或 CRT 格式。
   a. 返回控制台，然後選擇「下一步」來建立連線。
   b. 使用 SAML 建立連線。
4. 輸入您的 SAML 伺服器的 登入 **URL**。
5. 上傳從 SAML 提供者伺服器下載的 X.509 憑證。
6. 或者，輸入您的 SAML 伺服器的 退出 **URL**。
   a. 選擇*建立連線*。系統在幾秒鐘內建立連線。
   b. 選擇“下一步”。
   c. 選擇*測試連線*來測試您的連線。您將被引導至 IdP 伺服器的登入頁面。使用您的身分提供者憑證登入。登入後，返回控制台啟用連線。

      在受限模式下使用控制台時，請將 URL 複製到隱身瀏覽器視窗或單獨的瀏覽器中，以登入您的身分提供者 (IdP)。

   d. 在控制台中，選擇「下一步」以查看摘要頁面。
   e. 設定通知。

      您可以選擇七天或三十天。系統會透過電子郵件向具有以下角色的任何使用者發送到期通知，並在控制

台中顯示這些通知：超級管理員、組織管理員、聯盟管理員和聯盟檢視者。

f. 查看聯盟詳細信息，然後選擇“啟用聯盟”。

g. 選擇“完成”以完成該過程。

啟用聯合身份驗證後，使用者可以使用其企業憑證登入NetApp Console。

管理聯盟

在**NetApp Console**中管理聯合

# 您可以在NetApp Console中管理您的聯合。您可以停用它，更新過期的憑證，以及在不再需要它時停用它。

必備角色

需要聯盟管理員角色來創建和管理聯盟。聯盟檢視者可以查看聯盟頁面。"了解有關訪問角色的更多資訊。"

您也可以為現有聯盟新增額外的已驗證網域，從而允許您為聯盟連線使用多個網域。

- 如果您使用NetApp Cloud Central 設定了聯合，請透過 **Federation** 頁面匯入它以在控制台中進行管理。"了解如何匯入您的聯盟"
- 您可以在「審核」頁面上查看聯盟管理事件，例如啟用、停用和更新聯盟。 "了解有關在NetApp Console中監控操作的更多資訊。"

啟用聯盟

如果您已經建立了聯盟但尚未啟用，您可以透過*聯盟*頁面啟用它。啟用聯合允許與聯合關聯的使用者使用其公司憑證登入控制台。在啟用聯合之前，請先成功建立並測試聯合。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇“**Federation**”選項卡。
3. 選擇操作選單 ••• 旁邊的您想要啟用的聯盟並選擇*啟用*。

將已驗證的網域新增至現有聯合

您可以在控制台中將已驗證的網域新增至現有聯合，以便使用具有相同身分提供者 (IdP) 的多個網域。

您必須先在控制台中驗證該網域，然後才能將其新增至聯合中。如果您尚未驗證域名，可以按照以下步驟進行驗證"在控制台中驗證您的網域"。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇“**Federation**”選項卡。
3. 選擇操作選單 ⋮ 在您要新增已驗證網域的聯盟旁邊，然後選擇*更新網域*。 *更新網域*對話方塊顯示已與此聯合關聯的網域。
4. 從可用網域清單中選擇一個已驗證的網域。

5. 選擇*更新*。新網域使用者可以在 30 秒內獲得聯合控制台存取權限。

### 更新即將到期的聯合連接

您可以在控制台中更新聯合的詳細資訊。例如，如果憑證或用戶端機密等憑證過期，則需要更新聯合。在需要時，更新通知日期以提醒您在連線到期之前更新連線。

在更新 IdP 之前，請先更新控制台以避免登入問題。在此過程中保持登入控制台。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇“**Federation**”選項卡。
3. 選擇要更新的聯合旁邊的操作選單（三個垂直點），然後選擇*更新聯合*。
4. 根據需要更新聯盟的詳細資訊。
5. 選擇*更新*。

### 測試現有的聯盟

測試現有聯合的連線以驗證其是否有效。這可以幫助您識別聯盟中的任何問題並進行故障排除。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇“**Federation**”選項卡。
3. 選擇操作選單旁邊的您想要新增已驗證網域的聯盟，然後選擇*測試連線*。
4. 選擇*測試*。系統提示您使用公司憑證登入。如果連線成功，您將被重新導向到NetApp Console。如果連線失敗，您會看到錯誤訊息，表示聯合存在問題。
5. 選擇“完成”返回“聯合”選項卡。

### 禁用聯合

如果您不再需要聯合，您可以停用它。這可以防止與聯盟關聯的使用者使用其公司憑證登入控制台。如果需要，您可以稍後重新啟用聯合。

在刪除聯合之前，請先停用它，例如在停用 IdP 或停止聯合時。如果需要的話，您可以稍後重新啟用它。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇“**Federation**”選項卡。
3. 選擇操作選單在您要新增已驗證網域的聯盟旁邊，然後選擇*停用*。

### 刪除聯盟

如果您不再需要聯盟，您可以將其刪除。這將刪除聯合併阻止與聯合關聯的任何使用者使用其公司憑證登入控制台。例如，如果 IdP 被停用或不再需要聯合。

刪除聯合後，您將無法恢復它。您必須創建一個新的聯盟。

您必須先停用聯合，然後才能刪除它。一旦刪除聯盟，就無法恢復刪除。

步驟

1. 選擇“管理”>“身份和存取”。
2. 選擇“**Federations**”以查看“**Federations**”頁面。
3. 選擇操作選單：在您要新增已驗證網域的聯盟旁邊，然後選擇*刪除*。

將您的聯合匯入**NetApp Console**

## 如果您先前已透過NetApp Cloud Central（ NetApp Console的外部應用程式）設定聯合，則聯合頁面會提示您將現有的聯合連接匯入控制台，以便您可以在新介面中對其進行管理。然後，您可以利用最新的增強功能，而無需重新建立聯合連接。

匯入現有聯盟後，您可以從「聯盟」頁面管理該聯盟。"了解有關管理聯盟的更多資訊。"

所需角色

組織管理員或聯盟管理員。"了解有關訪問角色的更多資訊。"

步驟

1. 選擇*管理>身分和存取*。
2. 選擇“**Federation**”選項卡。
3. 選擇*導入聯合*。

## 強制實施**ONTAP Advanced View**（**ONTAP**系統管理員）的**ONTAP**權限

## 預設情況下，控制台代理程式憑證允許使用者存取進階視圖（ONTAP系統管理員）。您可以提示使用者輸入他們的ONTAP憑證。這可確保使用者在Cloud Volumes ONTAP和ONTAP本地叢集中使用ONTAP叢集時套用其ONTAP權限。

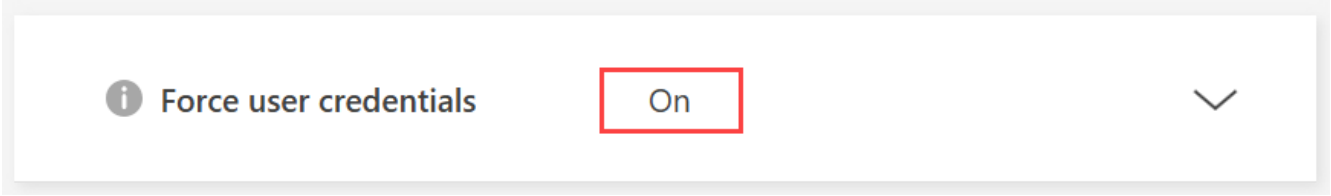
您必須具有組織管理員角色才能編輯控制台代理設定。

步驟

1. 選擇“管理 **>** 代理”。
2. 在*概覽*頁面上，選擇控制台代理程式的操作選單，然後選擇*編輯代理*。

   控制台代理程式必須處於活動狀態才能對其進行編輯。

3. 展開*強制憑證*選項。
4. 選取核取方塊以啟用*強制憑證*選項，然後選擇*儲存*。
5. 驗證「強制憑證」選項是否已啟用。




## 為NetApp Console組織啟用唯讀模式

為安全起見，您可以為NetApp Console組織啟用唯讀模式。在唯讀模式下，使用者可以查看資源和設置，但不能進行任何更改。

在唯讀模式下，具有管理員角色的使用者必須手動提升權限才能進行更改，這確保了更改是有意為之的。

所需存取權限

超級管理員或組織管理員。

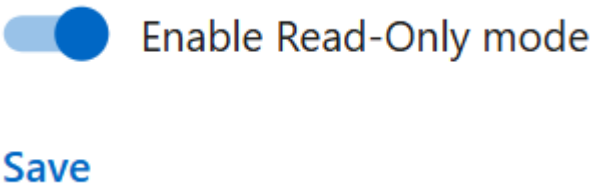
為您的控制台組織啟用唯讀模式

啟用唯讀模式以限制控制台組織的變更。所有用戶仍然可以查看資源。擁有管理員角色的用戶，如果不手動提升權限，則無法在控制台中執行任何操作。

啟用唯讀模式後，使用者會看到一個橫幅，通知他們該組織處於唯讀模式。用戶必須前往用戶設定來提升其角色。

步驟

1. 選擇*管理>身分和存取*。
2. 在「組織」標籤中，選擇要設定為唯讀模式的組織的「編輯組織設定」。
3. 在「唯讀模式」部分，將開關撥到「開」位置啟用唯讀模式，然後選擇「儲存」。




以初始組織管理員身分註冊**NetApp Console**

如果貴公司還沒有NetApp Console組織，請註冊建立一個。第一個使用者是管理員，負責管理帳號和權限。您可以稍後更新角色並新增管理員。

步驟

1. 開啟 Web 瀏覽器並前往 "NetApp Console"
2. 如果您擁有NetApp支援網站帳戶，請直接在「登入」頁面上輸入與您的帳戶關聯的電子郵件地址。

   控制台會在您首次登入時使用您的NetApp支援網站憑證進行註冊。

3. 如果您想透過建立控制台登入來註冊，請選擇*註冊*。
   a. 在*註冊*頁面上，輸入所需資訊並選擇*下一步*。

      註冊表格中只允許使用英文字元。

   b. 檢查您的收件箱，尋找來自NetApp的電子郵件，其中包含驗證您的電子郵件地址的說明。

      請驗證您的電子郵件地址以完成註冊。

4. 登入後，請閱讀並接受最終用戶許可協議。
5. 在「歡迎」頁面上，建立一個組織。
6. 選擇*讓我們開始吧*。

+ 作為首次擔任管理員的用戶，請依照引導流程新增儲存空間、建立控制台代理程式等。 "了解如何使用控制台助手。"

下一步

作為管理員，在完成控制台助手中包含的步驟後，您應該規劃身分和存取策略，將使用者新增至您的組織，並指派角色。 "了解NetApp Console的身份和存取管理"

如果組織已存在，請註冊或登入**NetApp Console**。

如果貴公司已有NetApp Console組織，請註冊或登入以存取它。您的註冊或登入方式取決於您的公司是否使用身分聯合或擁有NetApp支援網站憑證。如果還沒有，請建立NetApp Console登入帳號。

步驟

1. 開啟 Web 瀏覽器並前往 "NetApp Console"
2. 如果您擁有NetApp支援網站帳戶，或您的公司已設定單一登入 (SSO)，請在「登入」頁面上輸入您關聯的電子郵件地址或 SSO 憑證。依照提示完成登入。

   在這兩種情況下，您都會在初始登入時註冊控制台。

3. 如果您想透過建立控制台登入來註冊，請選擇*註冊*。
   a. 在*註冊*頁面上，輸入所需資訊並選擇*下一步*。

      註冊表格中只允許使用英文字元。

   b. 檢查您的收件箱，尋找來自NetApp的電子郵件，其中包含驗證您的電子郵件地址的說明。

      請驗證您的電子郵件地址以完成註冊。

4. 登入後，請閱讀並接受最終用戶許可協議。
5. 如果系統提示您建立組織，請關閉對話方塊並告知控制台管理員，以便他們可以將您新增至控制台組織並授予您存取權限。 "了解如何聯絡組織管理員。"

下一步

取得組織存取權限後，即可開始管理儲存空間並使用指派給您的資料服務。

# 管理組織夥伴關係

## NetApp Console 中的組織合作夥伴關係

在NetApp Console中建立組織間的合作夥伴關係，可讓合作夥伴安全地跨組織邊界管理NetApp資源，從而簡化協作並增強安全性。

必備角色

合作夥伴管理員"了解有關訪問角色的更多資訊。"

合作夥伴關係允許使用控制台中的角色驅動關係跨組織安全地管理NetApp資源。發起組織授予對其資源的存取權限，而接受組織提供被授予存取權限的使用者或服務帳戶。合作夥伴關係是透過自助服務工作流程建立的，使發起組織能夠完全控制共享的資源、分配的角色以及根據需要加入、管理或撤銷合作夥伴存取權限的能力。

客戶可以授權 MSP 或經銷商來管理NetApp環境，而無需複雜的設定。客戶可以控制合作夥伴可以存取哪些叢集以及他們擁有哪些角色，並且可以隨時撤銷存取權限以維護安全性和合規性。

作為合作夥伴，您可以獲得跨客戶環境的集中可見性和控制力。您可以輕鬆切換到客戶的組織來管理資源、運行數據服務並在定義的邊界內監控健康狀況，從而減少自訂工具並確保與每個客戶的政策保持一致。

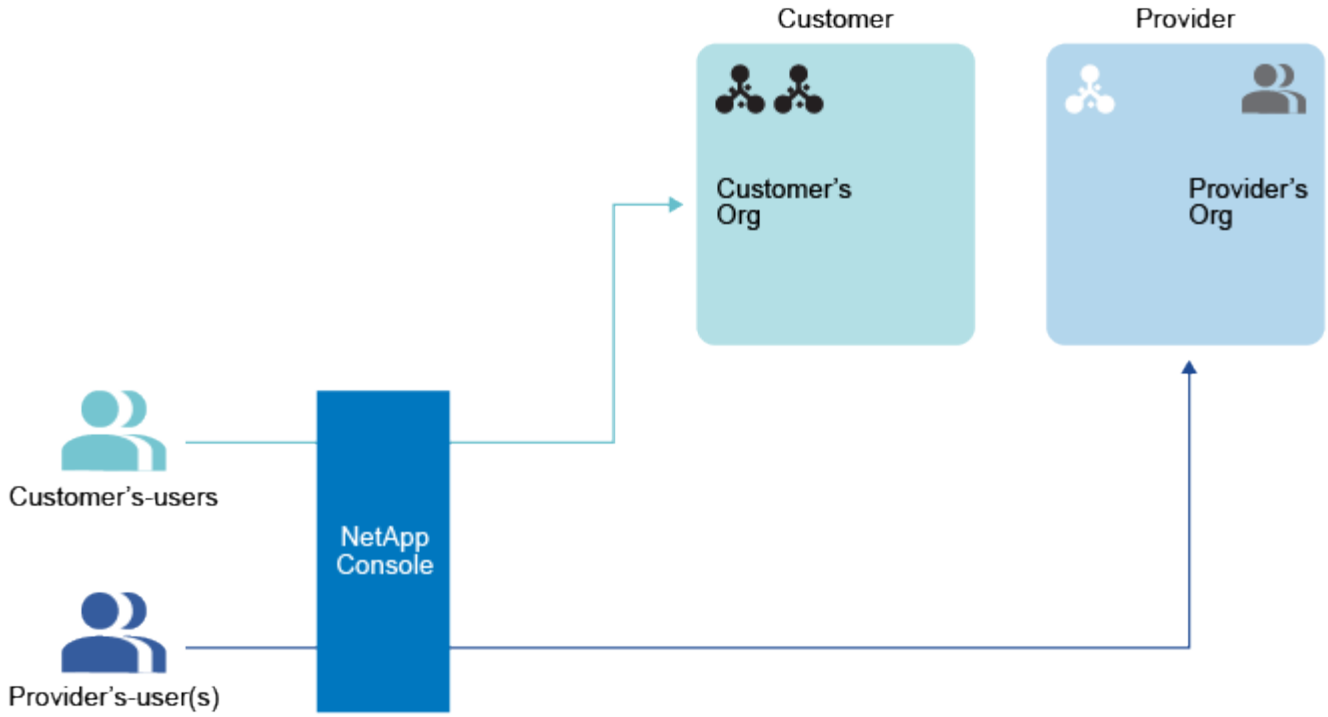
1. 為一個或多個使用者指派合作夥伴管理員角色

在發起組織和接收組織中，分別分配一個或多個使用者 Partnership admin 角色，以便他們建立和管理合作夥伴關係。您可以將 Partnership viewer 角色指派給只需要查看合作夥伴關係而無需管理的使用者。

2. 與發起組織共用您的組織 **ID**

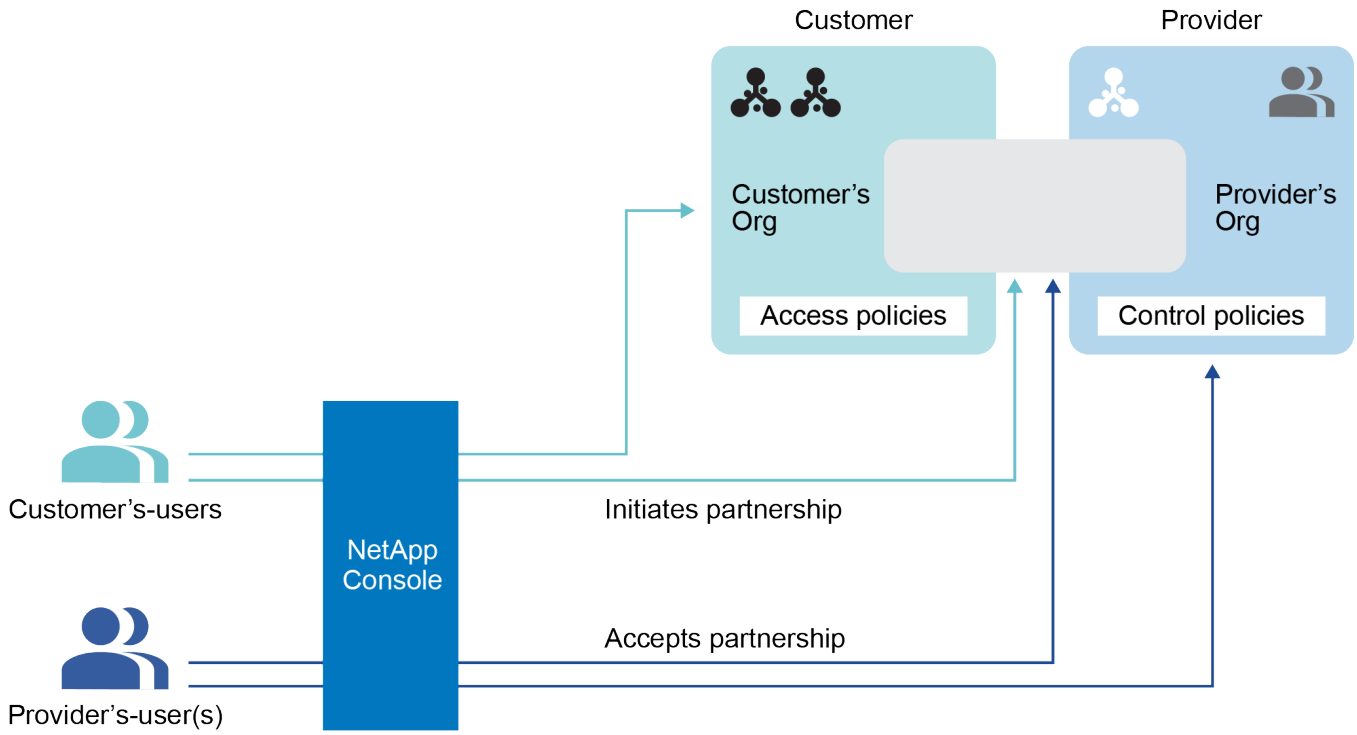
要發起合作關係，發起者必須知道目標組織的組織 ID。只有相應的組織可以存取此組織 ID。透過電子郵件或其他方式直接與NetApp Console以外的發起組織共用。

發起組織是授予其資源存取權限的組織。




3 在**NetApp Console**內建立合作關係

發起合作關係的組織透過從NetApp Console發送合作關係請求來發起合作關係。



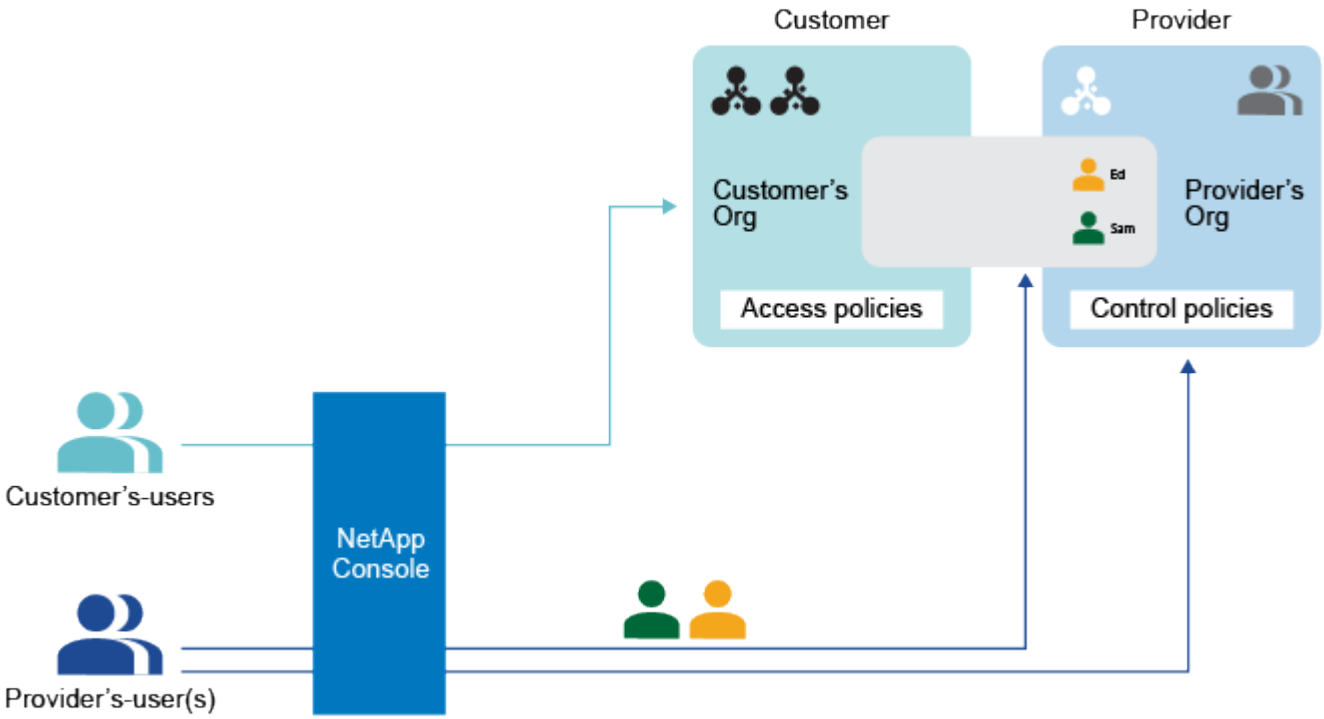
4 批准合作

接收組織必須接受該請求。

接收組織是被授予資源存取權限的組織。

5 將用戶分配到合作關係

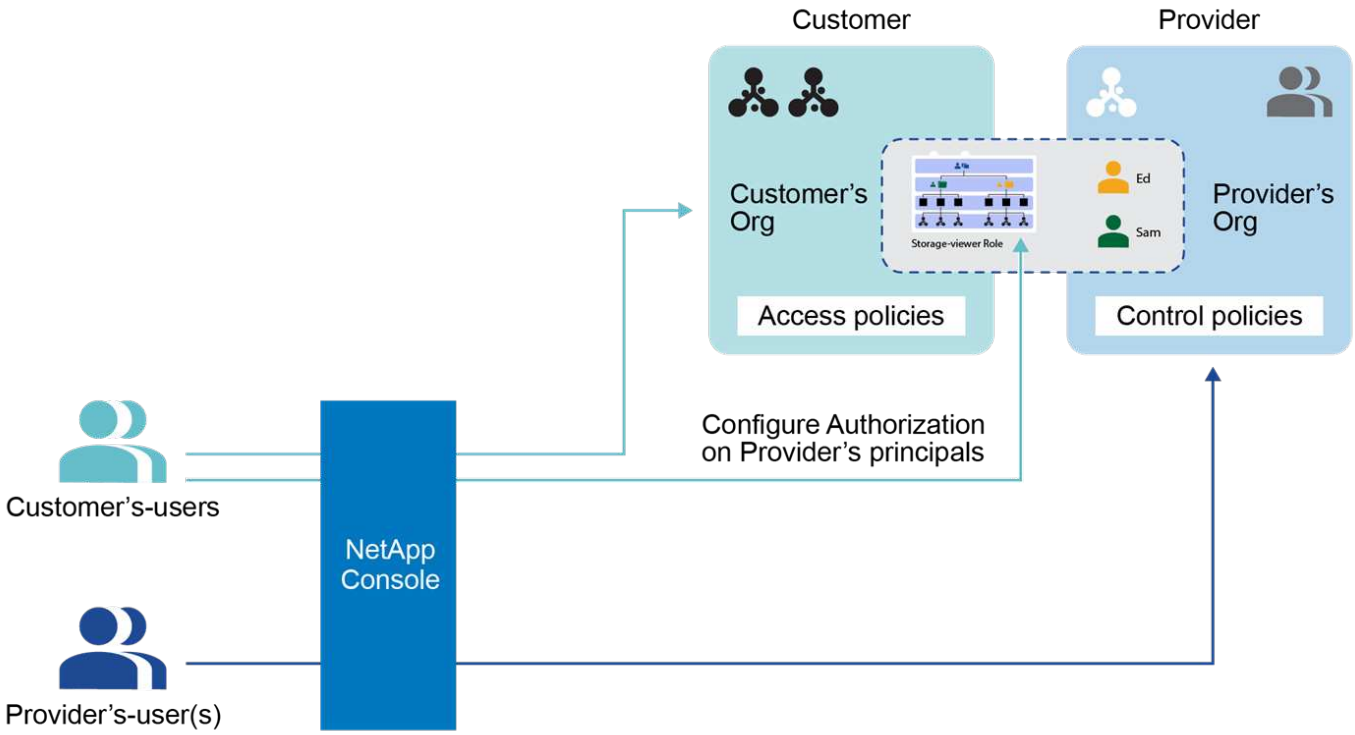
接收組織將您組織中的特定使用者或服務帳戶指派給合作夥伴關係。發起組織為這些使用者指派角色。




6 授予指定使用者對資源的存取權限

如果您是發起組織，您可以向指派給合作關係的使用者授予特定資源的存取權限。您可以隨時撤銷存取權限。

您可以透過為組織內的特定項目或資料夾分配角色來實現此目的。




# 在NetApp Console中管理合作夥伴關係

建立合作夥伴關係，在您的組織和值得信賴的合作夥伴之間建立安全、可管理的連接，以實現協作式NetApp資源管理。

透過合作夥伴關係，您可以透過控制台中的角色驅動關係安全地跨邊界管理NetApp資源。發起組織授予對其資源的存取權限，而接受組織提供被授予存取權限的使用者或服務帳戶。合作夥伴關係是透過自助服務工作流程建立的，使發起組織能夠完全控制共享的資源、分配的角色以及根據需要加入、管理或撤銷合作夥伴存取權限的能力。

## 必備角色

需要「合作夥伴關係管理員」角色來建立和管理合作夥伴關係。 *合作夥伴檢視者*可以查看合作夥伴頁面。"了解有關訪問角色的更多資訊。"

## 建立組織夥伴關係

如果您知道其他組織的組織 ID，您可以要求與其建立合作關係。接收組織必須批准該請求，合作關係才能繼續進行。

在開始之前，請確保您擁有合作夥伴組織的組織 ID，並且已被指派 合作夥伴管理員 角色。

### 步驟

1. 選擇*管理>身分和存取*。
2. 選擇“合作夥伴關係”標籤。
3. 選擇*新增合作夥伴關係*。
4. 在*建立合作夥伴關係*對話方塊中，輸入請求合作夥伴的合作夥伴組織 ID，然後選擇*新增*。

合作請求被發送給合作夥伴組織以供批准。您可以在*合作夥伴關係*頁面上查看合作請求的狀態。

### 批准組織合作關係

接收組織必須接受組織合作請求，合作才能繼續進行。您必須具有*合作夥伴關係管理員*角色才能批准和管理合作夥伴關係。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇*合作關係*。
3. 選擇“已收到合作關係”標籤。
4. 導航至您想要批准的合作關係並選擇 ••• 然後選擇*批准*。
5. 查看合作關係的詳細信息，包括請求合作關係的組織的名稱和組織 ID，然後選擇「下一步」。
6. 可選，將組織成員新增至合作夥伴關係並選擇*應用*。

   您可以隨時透過*合作夥伴*頁面新增其他成員。

   您新增的任何成員都會在合作夥伴的組織中可見，合作夥伴可以在其中將他們指派給資源。

結果

您批准的合作關係現在顯示狀態為*已建立*。任一組織中具有 **Partnership admim** 或 **Partnership viewer** 角色的使用者都可以查看合作關係。

### 查看合作關係狀態

查看您的合作關係狀態。

所需角色

合作夥伴關係管理員、合作夥伴關係查看者。"了解有關訪問角色的更多資訊。"

步驟

1. 選擇*管理>身分和存取*。
2. 選擇*合作關係*。
3. 選擇「已發起的合作關係」或「已接收的合作關係」標籤。
4. 查看顯示合作關係及其狀態的對應表格。

### 禁用組織合作關係

您必須是發起組織的成員才能停用合作關係。停用合作關係將立即撤銷您組織中與合作夥伴組織共享的任何資源的存取權限。

所需角色

合夥管理人。"了解有關訪問角色的更多資訊。"

步驟

1. 選擇*管理>身分和存取*。
2. 選擇*合作關係*。
3. 選擇“已啟動的合作夥伴關係”標籤。
4. 查看顯示合作關係及其狀態的對應表格。
5. 導航至您想要停用的已啟動合作關係並選擇 ••• 然後選擇*停用*。

## 管理合作組織的成員

您可以透過將使用者新增至合作夥伴組織來將使用者新增至合作夥伴關係。新增使用者後，合作夥伴組織負責為他們分配組織中特定資源的角色。

### 必備角色

需要「合作夥伴關係管理員」角色來建立和管理合作夥伴關係。 *合作夥伴檢視者*可以查看合作夥伴頁面。"了解有關訪問角色的更多資訊。"

您可以隨時從合作關係中移除使用者。從合作關係中移除使用者會立即撤銷其對合作夥伴組織中任何資源的存取權。

### 在合作關係中加入成員

當您在合作夥伴關係中新增成員時，合作夥伴組織的*合作夥伴關係管理員*必須為他們指派組織中特定資源的角色，然後他們才能存取這些資源。

將成員新增至合作夥伴關係後，這些成員將顯示為合作夥伴組織中的成員，合作夥伴可以在其中為他們指派資源。

### 步驟

1. 選擇*管理>身分和存取*。
2. 選擇*合作關係*。
3. 選擇“已收到合作關係”標籤。
4. 選擇操作選單 ••• 在您想要新增成員的已建立的合作關係旁邊，選擇「新增成員」。
5. 選擇一個或多個要新增至合作關係中的成員，然後選擇*新增*。

### 從合作關係中移除成員

您可以隨時從合作關係中移除成員。從合作關係中移除使用者會立即撤銷其對合作夥伴組織中任何資源的存取權。

如果您想調整成員擁有的角色或他們可以存取的資源，合作夥伴組織的合作夥伴管理員必須進行這些變更。

### 步驟

1. 選擇*管理>身分和存取*。
2. 選擇*合作關係*。
3. 選擇“已收到合作關係”標籤。
4. 選擇操作選單 ••• 在您想要刪除的成員旁邊，選擇「刪除關聯」。

5. 在對話方塊中選擇“刪除”來確認該操作。

查看使用者的角色訊息

您可以查看已指派給使用者的角色以及相關資源。

您不能變更與使用者關聯的角色。如果您對所提供的資源或角色有任何疑問，請聯絡合作夥伴組織的管理員。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇*合作關係*。
3. 選擇“已收到合作關係”標籤。
4. 從「成員」頁面，導覽至表中的成員，選擇 ••• 然後選擇*查看詳細資訊*。
5. 在表格中，展開您想要查看成員指派角色的組織、資料夾或專案的對應行，然後選擇「角色」欄位中的數字。

## 為合作夥伴用戶提供資源訪問

您可以透過為合作夥伴使用者指派組織內資料夾和專案的特定角色來授予他們存取權限。

必備角色

合夥管理人。"了解有關訪問角色的更多資訊。"

合作夥伴組織必須先將成員加入合作關係中，然後您才能為他們指派組織中資源的角色。"了解如何在合作關係中加入成員。"

了解合作夥伴使用者的角色

您可以按照管理自己的角色的方式來管理合作夥伴組織成員的角色。然而，並非所有角色都適合合作夥伴使用者。特別是，您不能授予合作夥伴使用者允許軟體更新的角色。更新ONTAP軟體通常需要直接網路存取。

您可以為合作夥伴使用者指派以下角色：

- "組織管理員"
- "資料夾或專案管理員"
- "聯盟管理員"
- "聯邦檢視器"
- "備份和復原管理員"
- "備份檢視器"
- "復原管理員"
- "複製管理員"
- "災難復原管理員"
- "災難復原故障轉移管理員"
- "災難復原應用程式管理員"

- "災難復原檢視器"
- "營運支援分析師"
- "分類檢視器"

"了解有關預定義角色的更多信息"

為合作夥伴使用者新增角色

您可以透過向成員新增角色來提供對組織資源的存取權。指派角色時，您指定一個資源和一個角色。您可以為一個使用者指派多個角色。

例如，如果您有兩個項目，並且希望同一個使用者同時擁有這兩個項目的備份和還原管理員角色，則您需要為每個項目的使用者提供該角色。同樣，如果您想為同一個專案的使用者提供兩個不同的角色，則需要分別分配每個角色。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇*合作關係*。
3. 選擇*合作夥伴關係已啟動*選項卡。
4. 選擇操作選單 ••• 在您想要查看的已建立的合作關係旁邊，選擇「查看詳細資訊」。

   *成員*清單顯示合作夥伴組織已新增至合作夥伴關係的成員。

5. 選擇操作選單 ••• 在您想要指派角色的成員旁邊，選擇「新增角色」。
6. 若要新增角色，請完成對話方塊中的步驟：
   - 選擇組織、資料夾或專案：選擇成員應具有權限的資源層次結構層級。

     如果您選擇組織或資料夾，則該成員將擁有該組織或資料夾內所有內容的權限。

   - 選擇類別：選擇角色類別。"了解訪問角色"。
   - 選擇*角色*：選擇一個角色，該角色為成員提供與您選擇的組織、資料夾或專案相關的資源的權限。
   - 新增角色：如果您想提供組織內其他資料夾或項目的存取權限，請選擇*新增角色*，指定另一個資料夾或項目或角色類別，然後選擇一個角色類別和對應的角色。
7. 選擇*新增角色*。

更改或刪除合作夥伴使用者的角色

您可以變更或刪除指派給合作夥伴組織成員的角色。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇*合作關係*。
3. 選擇*合作夥伴關係已啟動*選項卡。
4. 選擇操作選單 ••• 在您想要查看的已建立的合作關係旁邊，選擇「查看詳細資訊」。

*成員*清單顯示合作夥伴組織已新增至合作夥伴關係的成員。

5. 從「成員」頁面，導覽至表中的成員，選擇 ••• 然後選擇*查看詳細資訊*。
6. 在表格中，展開要變更成員指派角色的組織、資料夾或專案的對應行，然後在「角色」欄位中選擇「檢視」以查看指派給該成員的角色。
7. 您可以變更成員的現有角色或刪除角色。
   a. 若要變更成員的角色，請選擇要變更的角色旁邊的「變更」。您只能將角色變更為同一角色類別內的角色。例如，您可以從一個資料服務角色變更為另一個資料服務角色。確認更改。
   b. 若要取消指派成員的角色，請選擇 🗑 在角色旁邊，點擊即可從成員中移除對應的角色。您將被要求確認刪除操作。

### 在合作組織工作

一旦您在合作夥伴組織中被賦予角色，您就可以切換到該組織並執行您有權執行的操作。

使用組織選單在您的組織和您有權存取的任何合作夥伴組織之間切換。"了解有關切換組織和專案的更多資訊。"

您將能夠看到合作夥伴組織中與您共享的資源，並根據分配給您的角色執行操作。與您的合作夥伴管理員合作，確保您擁有需要存取的資源的適當角色。

# 監控NetApp Console操作

您可以監視控制台正在執行的操作的狀態，以查看是否有需要解決的問題。您可以從審核頁面、通知中心查看狀態，或將通知傳送到您的電子郵件。

此表透過比較突顯了審計頁面和通知中心的功能。

| 通知中心 | 審計頁面 |
| --- | --- |
| 顯示事件和動作的高級狀態 | 提供每個事件或行動的詳細資訊以進行進一步調查 |
| 顯示目前登入工作階段的狀態（登出後，該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發起的操作 | 顯示來自 UI 或 API 的所有操作 |
| 顯示用戶發起的操作 | 顯示所有操作，無論是使用者發起的還是系統發起的 |
| 依重要性過濾結果 | 依服務、操作、使用者、狀態等過濾 |
| 提供向使用者和其他人發送電子郵件通知的功能 | 沒有電子郵件功能 |

### 從審核頁面審核用戶活動

使用審計頁面來識別誰執行了操作或其狀態。

審計頁面顯示使用者為管理您的組織或帳戶而完成的操作。這包括關聯用戶、建立系統、建立代理等管理操作。

您也可以核實是誰向組織新增了成員，或者專案是否已成功刪除。

步驟

1. 選擇“管理”>“審計”。
2. 使用表格上方的篩選器來變更表格中顯示的操作。

   例如，您可以使用*服務*篩選器顯示與特定服務相關的操作，或可以使用*使用者*篩選器顯示與特定使用者帳戶相關的操作。

從審計頁面下載審計日誌

您可以將稽核日誌從稽核頁面下載到 CSV 檔案。這使您能夠記錄使用者在您的組織中執行的操作。 CSV 檔案包含下載的 CSV 檔案中的所有列，無論審計頁面上的篩選器或顯示的列為何。

步驟

1. 在*審計*頁面中，選擇表格右上角的下載圖示。

## 使用通知中心監控活動

通知追蹤控制台操作以確認成功。它們使您能夠查看在目前登入工作階段期間啟動的許多控制台操作的狀態。並非所有控制台服務都會將資訊報告到通知中心。

您可以選擇通知鈴來顯示通知（ ) 在選單列中。鈴鐺中小氣泡的顏色表示處於活動狀態的最高等級嚴重性通知。因此，如果您看到紅色氣泡，表示有重要的通知需要您查看。

您也可以設定控制台透過電子郵件傳送某些類型的通知，這樣即使您未登入系統也可以了解重要的系統活動。電子郵件可以發送給您組織中的任何用戶，或任何其他需要了解某些類型的系統活動的收件者。了解如何設定電子郵件通知設定。

比較通知中心和警報

通知中心使您能夠查看已啟動的操作的狀態並為某些類型的系統活動設定警報通知。同時，警報可讓您查看ONTAP儲存環境中與容量、可用性、效能、保護和安全性相關的問題或潛在風險。

"了解有關NetApp Console警報的更多信息"

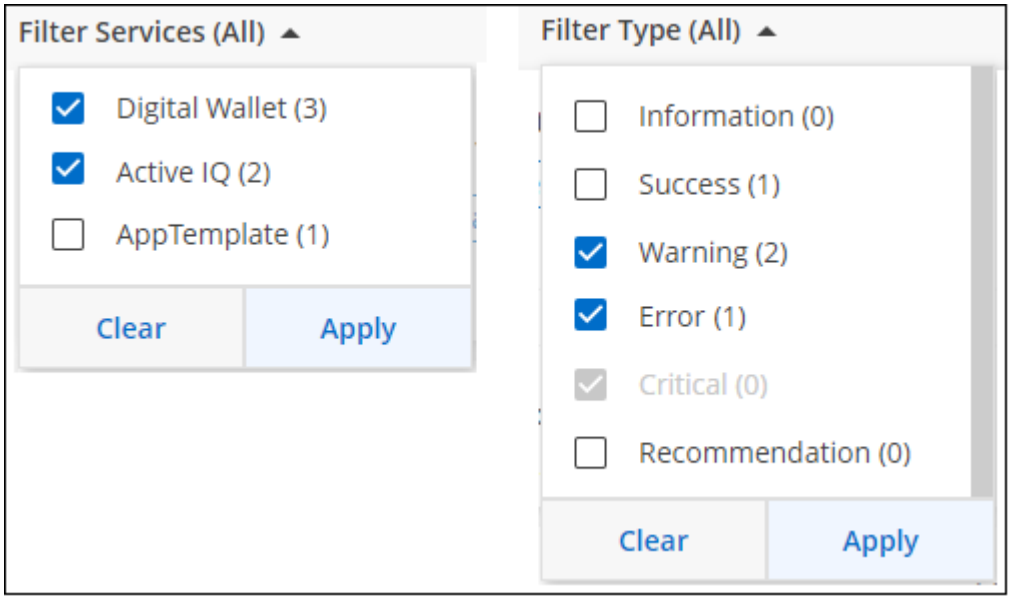
通知類型

控制台將通知分為以下類別：

| 通知類型 | 描述 |
| --- | --- |
| 批判的 | 出現問題，如果不立即採取糾正措施，可能會導致服務中斷。 |
| 錯誤 | 一項行動或過程以失敗告終，或如果不採取糾正措施則可能導致失敗。 |
| 警告 | 您應該注意這個問題，以確保其不會達到嚴重程度。這種嚴重程度的通知不會導致服務中斷，並且可能不需要立即採取糾正措施。 |
| 推薦 | 系統建議您採取行動來改善系統或某項服務；例如：節省成本、新服務建議、建議安全配置等。 |
| 資訊 | 提供有關操作或過程的附加資訊的訊息。 |
| 成功 | 動作或過程成功完成。 |

過濾通知

預設情況下，您會在通知中心看到所有活動通知。您可以過濾看到的通知，以僅顯示對您重要的通知。您可以按「服務」和通知「類型」進行篩選。




例如，如果您只想查看控制台操作的「錯誤」和「警告」通知，請選擇這些條目，您將只看到這些類型的通知。

關閉通知

如果您不再需要查看通知，可以從頁面中刪除它們。您可以單獨或一次關閉所有通知。

若要關閉所有通知，請在通知中心選擇並選擇*全部關閉*。

若要關閉單一通知，請將遊標停留在通知上並選擇*關閉*。

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，這樣即使您未登入也可以獲知重要的系統活動。電子郵件可以發送給您組織或帳戶中的任何用戶，或任何其他需要了解某些類型的系統活動的收件者。

- 控制台發送代理、許可證和訂閱、 NetApp Copy and Sync以及NetApp Backup and Recovery的電子郵件通知。
- 當控制台代理安裝在沒有網路存取的網站時，不支援發送電子郵件通知。

您在通知中心設定的篩選器不會決定您透過電子郵件收到的通知類型。預設情況下，任何組織管理員都會收到所有「關鍵」和「建議」通知的電子郵件。這些通知涵蓋所有服務 - 您無法選擇僅接收某些服務的通知，例如代理或NetApp Backup and Recovery。

所有其他使用者和收件者都配置為不接收任何通知電子郵件 - 因此您需要為任何其他使用者設定通知設定。

您必須具有組織管理員角色才能自訂通知設定。

步驟

1. 選擇*管理>通知設定*。
2. 選擇*組織使用者*或*其他收件者*。

   *其他收件者*頁面可讓您設定控制台以通知控制台組織的成員。

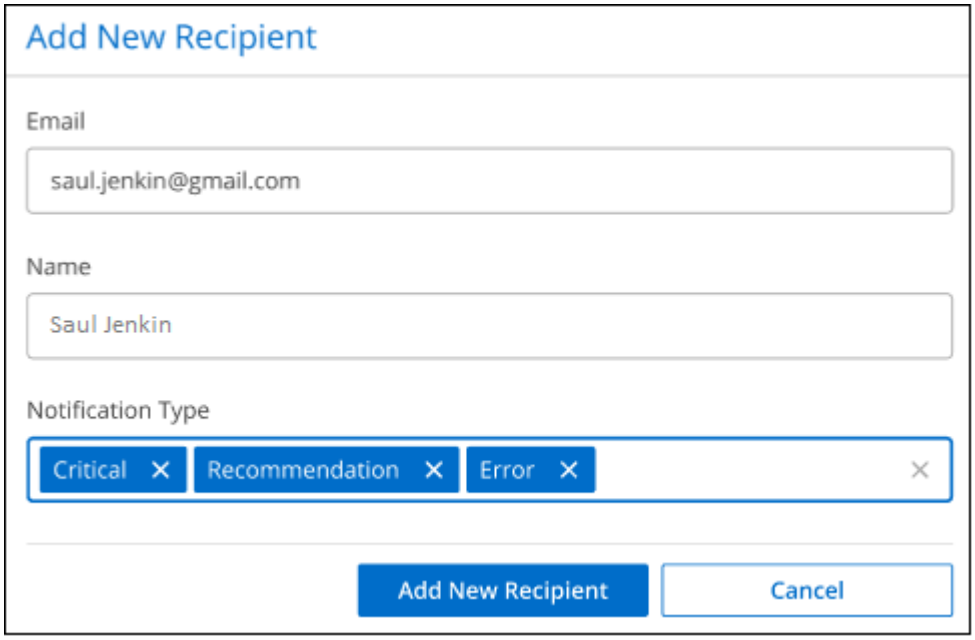
3. 從「組織用戶」頁面或「其他收件者」頁面中選擇一個或多個用戶，然後選擇要傳送的通知類型：
   - 若要對單一使用者進行更改，請選擇該使用者的通知列中的選單，檢查要傳送的通知類型，然後選擇*套用*。
   - 若要對多個使用者進行更改，請選取每個使用者的複選框，選擇*管理電子郵件通知*，檢查要傳送的通知類型，然後選擇*應用*。

新增其他電子郵件收件人

_組織使用者_頁面中顯示的使用者是從您的組織或帳戶中的使用者自動填入的。您可以在「其他收件者」頁面中為其他無權存取控制台但需要收到某些類型的警報和通知的個人或團體新增電子郵件地址。

步驟

1. 從*通知設定*頁面中，選擇*新增收件者*。




2. 輸入姓名、電子郵件地址，選擇收件者將收到的通知類型，然後選擇*新增收件者*。