開始

NetApp Console setup and administration

NetApp
February 09, 2026

目錄

開始

學習基礎知識

了解NetApp Console

該控制台透過整合資料服務統一混合多雲的儲存管理和保護，以保護和最佳化資料。

它既可以作為軟體即服務 (SaaS) 平台使用，也可以作為自託管選項安裝在您自己的主權雲端中。它提供儲存管理、資料移動性、資料保護以及資料分析和控制。管理功能透過基於 Web 的控制台和 API 提供。

集中儲存管理

使用控制台發現、部署和管理雲端和本地儲存。

支援的雲端和本地存儲

您可以從控制台管理以下類型的儲存空間：

雲端儲存解決方案

- Amazon FSx for NetApp ONTAP
- Azure NetApp Files
- Cloud Volumes ONTAP
- Google Cloud NetApp Volumes

本地閃存和對象存儲

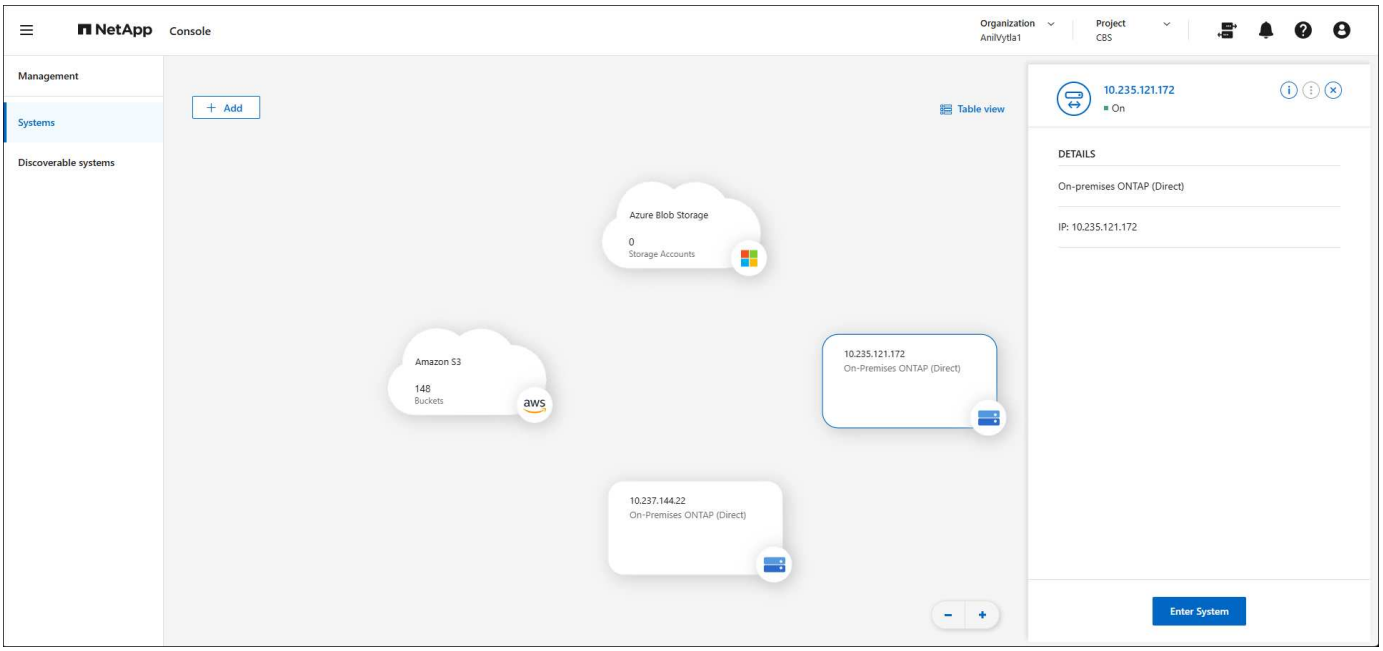
- E系列系統
- ONTAP叢集
- StorageGRID系統

雲端物件儲存

- Amazon S3 存儲
- Azure Blob 儲存
- Google 雲端儲存

儲存管理

在控制台中，*systems* 代表已發現或已部署的儲存空間。您可以選擇一個系統將其與NetApp資料服務整合或管理存儲，例如新增磁碟區。



整合數據服務和儲存管理，以保護、保障和最佳化數據

控制台提供資料服務以保護和維護儲存可用性。

儲存警報
: 查看與ONTAP環境中的容量、可用性、效能、保護和安全性相關的問題。

自動化中心
: 使用腳本解決方案來自動化NetApp產品和服務的部署和整合。

NetApp Backup and Recovery
: 備份和還原雲端和本地資料。

NetApp Data Classification
: 讓您的應用程式資料和雲端環境隱私做好準備。

NetApp Copy and Sync
: 在本地端和雲端資料儲存之間同步資料。

NetApp數位顧問 (Active IQ)
: 使用預測分析和主動支援來優化您的資料基礎架構。

Licenses and subscriptions
: 管理和監控您的許可證和訂閱。

NetApp Disaster Recovery
: 使用 VMware Cloud on Amazon FSx for ONTAP作為災難復原站點來保護本機 VMware 工作負載。

生命週期規劃
: 識別目前或預測容量較低的群集並實施資料分層或額外容量建議。

NetApp Ransomware Resilience

偵測可能導致勒索軟體攻擊的異常。保護和恢復工作負載。

NetApp Replication

在儲存系統之間複製資料以支援備份和災難復原。

軟體更新

自動評估、規劃和執行ONTAP升級。

永續性儀表板

分析儲存系統的可持續性。

NetApp Cloud Tiering

將您的本機ONTAP儲存擴展到雲端。

NetApp Volume Caching

建立可寫入的快取磁碟區以加快資料存取速度或卸載存取量大的磁碟區的流量。

NetApp工作負載

使用Amazon FSx for NetApp ONTAP設計、設定和執行關鍵工作負載。

"了解有關NetApp Console和可用資料服務的更多信息"

支援的雲端提供者

此控制台可讓您管理雲端儲存並使用 Amazon Web Services、Microsoft Azure 和 Google Cloud 中的雲端服務。

成本

NetApp Console是免費的。如果您在雲端中部署控制台代理程式或使用在雲端中部署的受限模式，則會產生費用。某些NetApp資料服務會產生相關費用。https://bluexp.netapp.com/pricing["了解NetApp數據服務定價"^]

NetApp Console的工作原理

NetApp Console是一個基於 Web 的控制台，透過 SaaS 層、資源和存取管理系統、管理儲存系統和啟用NetApp資料服務的控制台代理程式以及不同的部署模式提供，以滿足您的業務需求。

軟體即服務

您可以透過 "網路為基礎的介面"和 API。這種 SaaS 體驗使您能夠在最新功能發佈時自動存取它們。

身分和存取管理 (IAM)

控制台為資源和存取管理提供身分和存取管理 (IAM)。此 IAM 模型提供資源和權限的細粒度管理：

- 頂級組織使您能夠管理各個專案之間的存取權限
- 資料夾 使您可以將相關項目分組在一起
- 資源管理可讓您將資源與一個或多個資料夾或項目關聯

- 存取管理可讓您為組織層次結構中不同層級的成員指派角色
- "了解有關NetApp Console中的 IAM 的更多信息"

控制台代理

一些附加功能和資料服務需要控制台代理。它使您能夠管理本地和雲端環境中的資源和流程。您需要它來管理一些系統（例如， Cloud Volumes ONTAP）並使用一些NetApp資料服務。

"了解有關控制台代理的更多信息"。

SaaS 與主權雲端部署

您可以透過註冊 SaaS 服務或部署在您的主權雲端來開始使用NetApp Console 。在主權雲端部署NetApp Console時， NetApp會限制出站連接，以滿足您組織的安全性和合規性要求。當控制台部署在主權雲端時，並非所有功能和服務都可用。

NetApp持續為不需要出站連線的站點提供BlueXP 。BlueXP可以安裝在您的網路上，無需任何出站連線。"了解沒有網路連線的站點的BlueXP （私人模式）。"

"了解有關部署模式的更多信息"。

SOC 2 類型 **2** 認證

一家獨立的註冊會計師事務所和服務審計師審查了控制台，並確認其根據適用的信託服務標準實現了 SOC 2 類型 2 報告。

"查看 NetApp 的 SOC 2 報告"

了解**NetApp Console**部署模式

NetApp Console提供多種部署模式，讓您能夠滿足您的業務和安全需求。

- _標準模式_利用軟體即服務 (SaaS) 層來提供完整的功能。使用者透過基於 Web 的託管介面存取控制台
- _限制模式_適用於有連線限制並希望在自己的公有雲中安裝NetApp Console的組織。使用者透過託管在其雲端環境中的控制台代理程式上的基於 Web 的介面存取控制台。

  NetApp Console在受限模式下限制流量、通訊和數據，您必須確保您的環境（本地端和雲端）符合所需的規定。

概況

每種部署模式在出站連線、位置、安裝、驗證、資料服務和收費方法方面有所不同。

標準模式

您可以從基於 Web 的控制台使用 SaaS 服務。根據您計劃使用的資料服務和功能，控制台組織管理員將建立一個或多個控制台代理來管理混合雲環境中的資料。

此模式使用公共網際網路上的加密資料傳輸。

限制模式

您在雲端（在政府、主權或商業區域）安裝控制台代理，並且它與NetApp ConsoleSaaS 層的出站連接有限。

這種模式通常由州和地方政府以及受監管的公司使用。

了解有關 SaaS 層的出站連接的更多信息 。

BlueXP私人模式（僅限舊版**BlueXP**介面）

BlueXP私有模式（傳統BlueXP介面）通常用於沒有網路連線的本機環境和安全雲端區域，其中包括 AWS Secret Cloud、AWS Top Secret Cloud 和 Azure IL6。 NetApp繼續透過傳統的BlueXP介面支援這些環境。"BlueXP私人模式的 PDF 文檔"

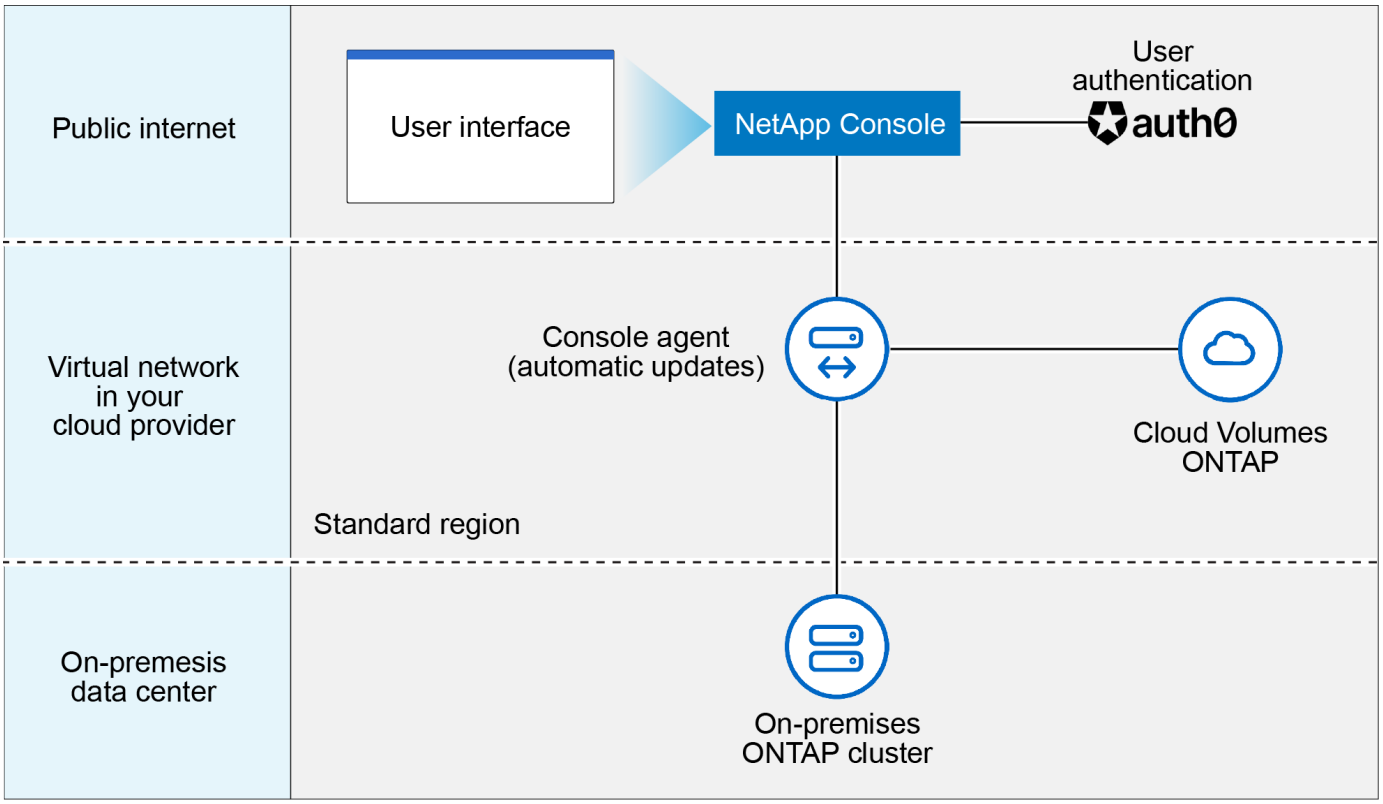
下表提供了NetApp控制台的比較。

	標準模式	限制模式
需要連接到**NetApp Console SaaS** 層嗎？	是的	僅限出站
需要連接到您的雲端提供者嗎？	是的	是的，在該地區
控制台代理安裝	從控制台、雲端市場或手動安裝	雲端市場或手動安裝
控制台代理升級	自動升級	自動升級
UI 訪問	從控制台 SaaS 層	從代理虛擬機器本地
API 端點	控制台 SaaS 層	控制台代理
驗證	透過使用 auth0、NSS 登入或身分聯合的 SaaS	透過使用 auth0 或身分聯合的 SaaS
多因素身份驗證	適用於本地用戶	無法使用
儲存和資料服務	全部支持	許多人受到支持
資料服務許可選項	市場訂閱和 BYOL	市場訂閱和 BYOL

閱讀以下部分以了解有關這些模式的更多信息，包括支援哪些NetApp Console功能和服務。

標準模式

下圖是標準模式部署的範例。



控制台在標準模式下的運作方式如下：

出站溝通

需要從控制台代理到控制台 SaaS 層、到雲端提供者的公開可用資源以及到日常操作的其他基本元件的連接。

- "代理在 AWS 中聯繫的終端節點"
- "代理程式在 Azure 中聯繫的終點"
- "代理在 Google Cloud 中聯繫的端點"

代理支援的位置

在標準模式下，代理在雲端或您的場所受支援。

控制台代理安裝

您可以使用以下方法之一安裝代理：

- 從控制台
- 來自 AWS 或 Azure 市場
- 來自 Google Cloud SDK
- 在資料中心或雲端中的 Linux 主機上手動使用安裝程序
- 在您的 VCenter 環境中使用提供的 OVA。

控制台代理升級

NetApp每月自動升級您的代理程式。

使用者介面存取

可以透過 SaaS 層提供的基於 Web 的控制台存取使用者介面。

API 端點

API 呼叫針對以下端點：\ https://api.bluexp.netapp.com

驗證

使用 auth0 或NetApp支援網站 (NSS) 登入進行驗證。身份聯合可用。

支援的數據服務

支援所有NetApp資料服務。"了解有關NetApp數據服務的更多信息" 。

支援的許可選項

標準模式支援市場訂閱和 BYOL；但是，支援的授權選項取決於您使用的NetApp資料服務。查看每項服務的文件以了解有關可用許可選項的更多資訊。

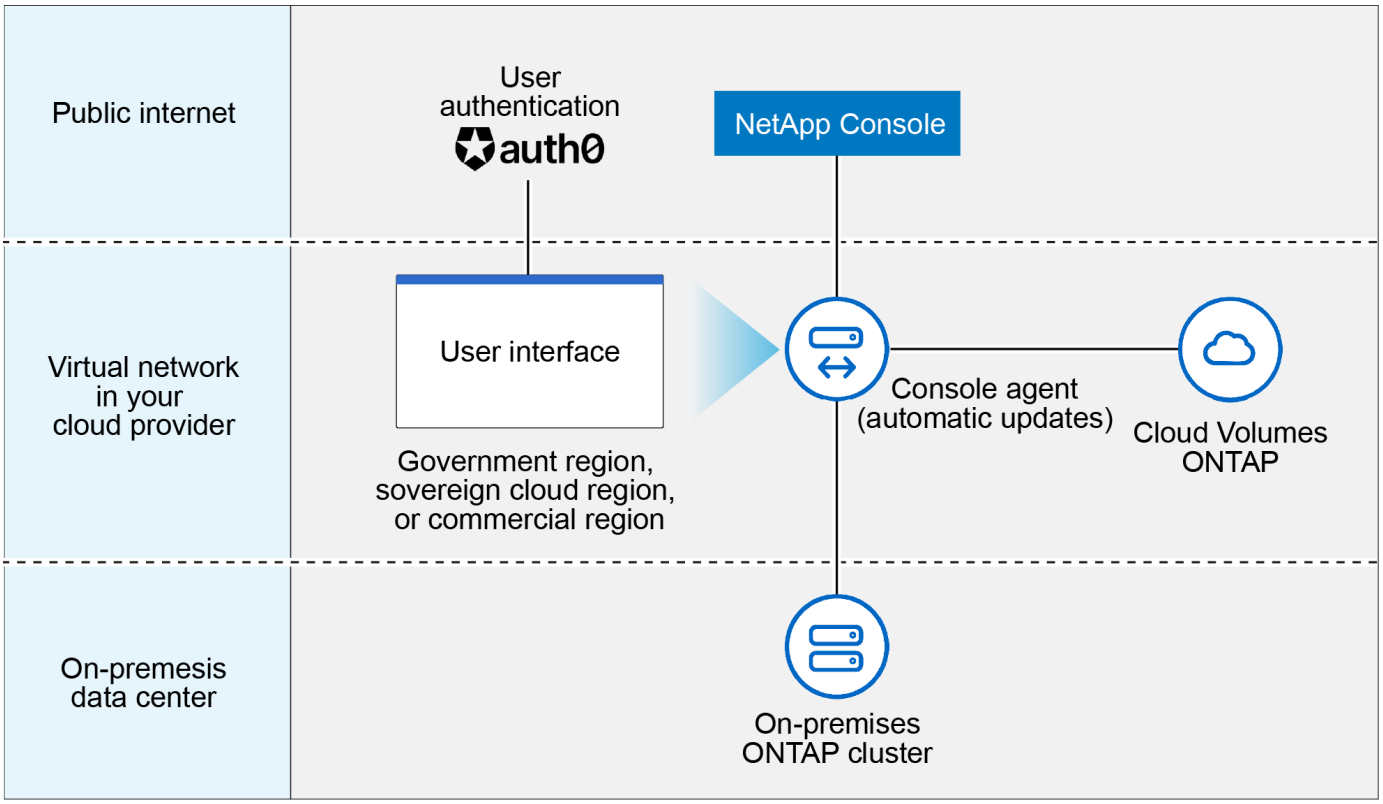
如何開始使用標準模式

前往 "NetApp Console"並註冊。

"了解如何開始使用標準模式" 。

限制模式

下圖是限制模式部署的範例。



控制台在限制模式下的工作方式如下：

出站溝通

代理程式需要與控制台 SaaS 層建立出站連接，以實現資料服務、軟體升級、身份驗證和元資料傳輸。

控制台 SaaS 層不會發起與代理程式的通訊。代理啟動與控制台 SaaS 層的所有通信，根據需要提取或推送資料。

還需要與區域內的雲端提供者資源建立連線。

代理支援的位置

在受限模式下，代理商在雲端中支援：在政府區域、主權區域或商業區域。

控制台代理安裝

您可以從 AWS 或 Azure 市場安裝，也可以在您自己的 Linux 主機上手動安裝，或在您的 VCenter 環境中使用可下載的 OVA。

控制台代理升級

NetApp每月自動更新您的代理程式軟體。

使用者介面存取

您可以從部署在雲端區域中的代理虛擬機器存取使用者介面。

API 端點

對代理虛擬機器進行 API 呼叫。

驗證

透過 auth0 提供身份驗證。身份聯合也可用。

支援的儲存管理和資料服務

以下儲存和資料服務具有受限模式：

支援的服務	筆記
Azure NetApp Files	全力支持
備份和復原	在政府區域和商業區域受限制模式支持。不支援在具有限制模式的主權區域使用。在受限模式下，NetApp Backup and Recovery and Recovery僅支援ONTAP磁碟區資料的備份和復原。 "查看ONTAP資料支援的備份目標列表"不支援應用程式資料和虛擬機器資料的備份和還原。
NetApp Data Classification	在政府區域內受限制模式支持。不支援商業區域或具有限制模式的主權區域。
Cloud Volumes ONTAP	全力支持
Licenses and subscriptions	您可以使用下面列出的受限模式支援的許可選項存取許可證和訂閱資訊。
本地ONTAP集群	使用控制台代理的發現和不使用控制台代理的發現（直接發現）均受支援。當您發現沒有控制台代理程式的本機叢集時，進階視圖（系統管理員）不受支援。

支援的服務	筆記
複製	在政府區域內受限制模式支持。不支援商業區域或具有限制模式的主權區域。

支援的許可選項

限制模式支援以下許可選項：

- 市場訂閱（按小時和按年合約）

  請注意以下事項：

  - 對於Cloud Volumes ONTAP，僅支援基於容量的許可。
  - 在 Azure 中，不支援與政府區域簽訂年度合約。
- BYOL

  對於Cloud Volumes ONTAP，BYOL 支援基於容量的授權和基於節點的授權。

如何開始使用受限模式

建立NetApp Console組織時，您需要啟用受限模式。

如果您還沒有組織，當您第一次從手動安裝的控制台代理或從雲端提供者的市場建立的控制台代理登入控制台時，系統會提示您建立組織並啟用受限模式。

建立組織後，您無法變更限制模式設定。

"了解如何開始使用受限模式" 。

服務和功能比較

下表可以幫助您快速識別受限模式支援哪些服務和功能。

請注意，某些服務可能會受到限制。有關如何在受限模式下支援這些服務的更多詳細信息，請參閱上面的部分。

產品領域	**NetApp**資料服務或功能	限制模式
儲存 表格的此部分列出了從控制台管理儲存系統的支援。它沒有指明NetApp Backup and Recovery支援的備份目標。	適用於ONTAP 的Amazon FSx	不
	亞馬遜 S3	不
	Azure Blob	不
	Azure NetApp Files	是的
	Cloud Volumes ONTAP	是的
	Google Cloud NetApp Volumes	不
	Google 雲端儲存	不
	本地ONTAP集群	是的
	E系列	不
	StorageGRID	不
數據服務	NetApp備份與復原	是的https://docs.netapp.com/us-en/data-services-backup-recovery/prev-ontap-protect-journey.html#support-for-sites-with-limited-internet-connectivity["查看ONTAP磁碟區資料支援的備份目標列表"^]
	NetApp Data Classification	是的
	NetApp Copy and Sync	不
	NetApp Disaster Recovery	不
	NetApp Ransomware Resilience	不
	NetApp Replication	是的
	NetApp Cloud Tiering	不
	NetApp磁碟區快取	不
	NetApp工作負載工廠	不

產品領域	NetApp資料服務或功能	限制模式
特徵	警報	不
	Digital Advisor	不
	授權和訂閱管理	是的
	身分和存取管理	是的
	證書	是的
	聯邦	是的
	生命週期規劃	不
	多因素身份驗證	是的
	NSS 帳戶	是的
	通知	是的
	搜尋	是的
	軟體更新	不
	永續性	不
	審計	是的

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。

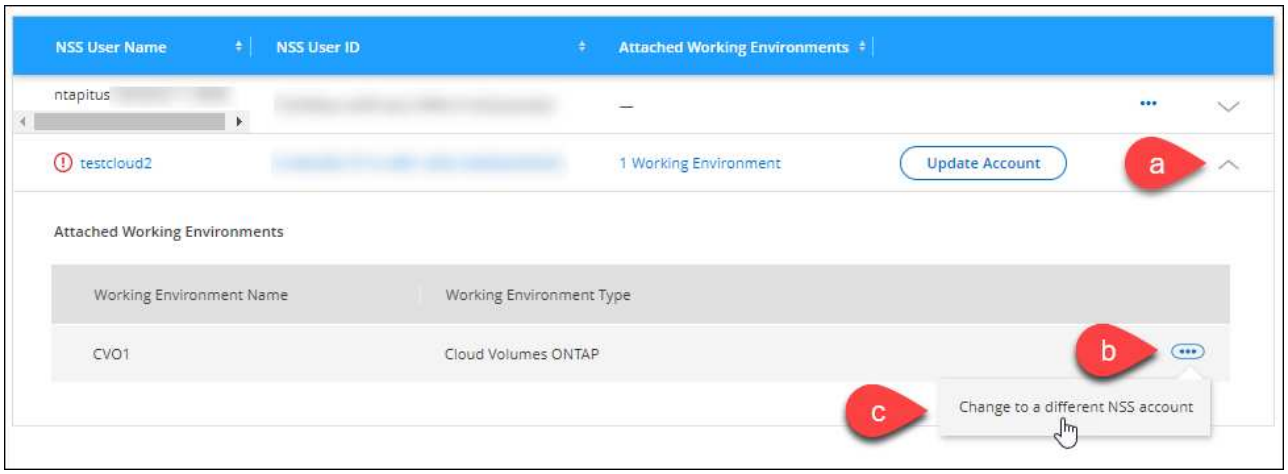
將系統附加到不同的 **NSS** 帳戶

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。

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。

了解NetApp Console身分和存取管理

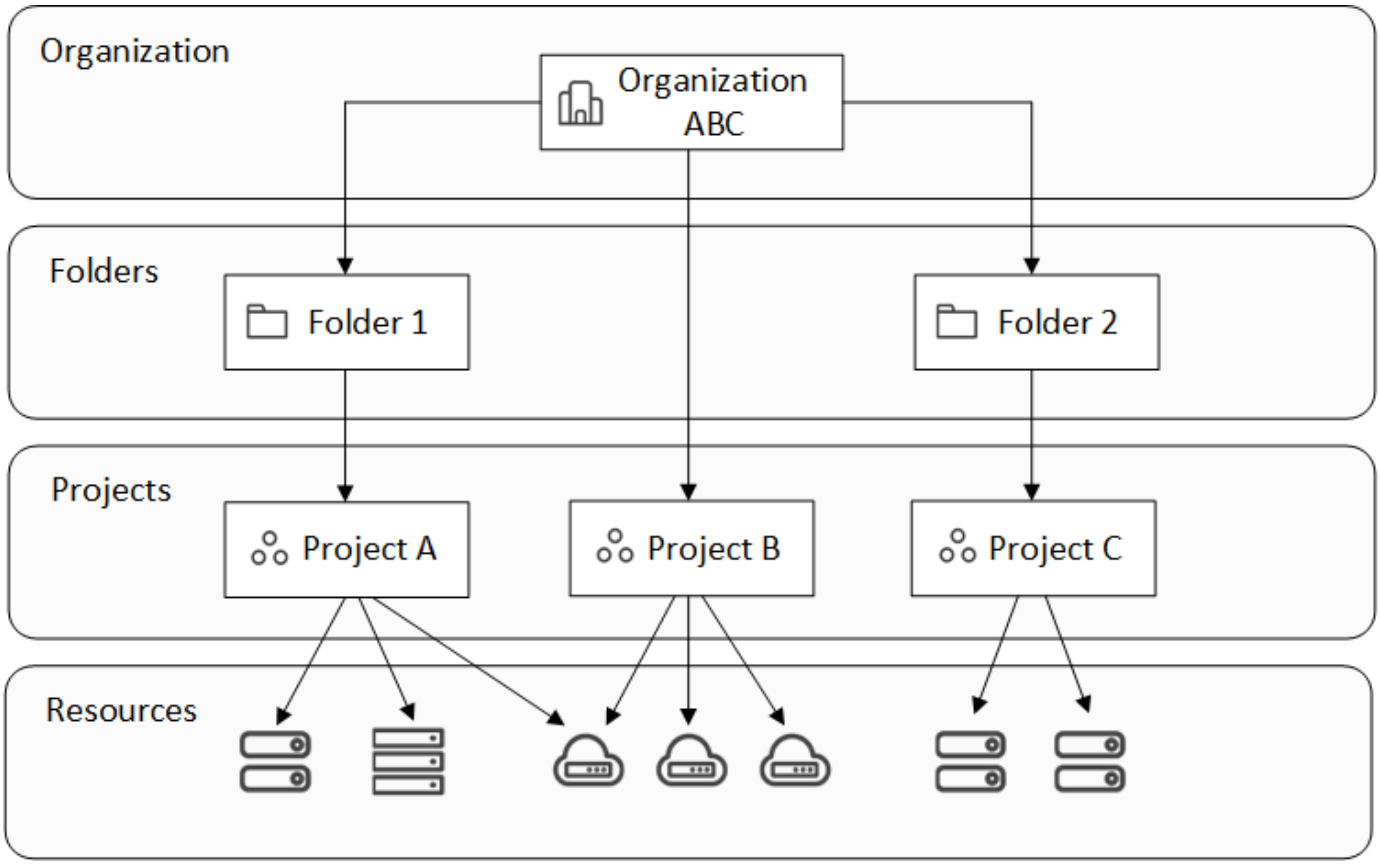
使用NetApp控制台的身分和存取管理 (IAM) 來組織您的NetApp資源，並根據您的業務結構（按位置、部門或專案）控制存取權限。

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"

NetApp Console (SaaS) 入門

入門工作流程（SaaS）

要開始使用NetApp Console(SaaS)，請先準備控制台的網絡，註冊並建立帳戶，然後使用控制台助手設定初始功能。

您可以存取由NetApp提供的基於 Web 的控制台，該控制台是軟體即服務 (SaaS) 產品。您可以使用控制台管理混合雲儲存環境並使用NetApp資料服務。

1 "準備使用**NetApp**控制台的網絡"

確保存取NetApp控制台的電腦能夠透過網路存取所需的端點。

"了解如何為NetApp控制台配置網路。"

2 "註冊並建立組織"

前往 "NetApp控制台" 並註冊。如果系統提示您建立組織，而您認為您的公司已經存在組織，請關閉對話方塊並告知您的組織管理員。如果貴公司目前沒有組織管理員，您可以認領此角色。 "了解如何聯絡組織管理員。"

此時，您已登錄，可以使用NetApp助理開始設定控制台。首先，請將您的NetApp支援帳號與控制台代理程式關聯，以啟用全部功能。

如果您選擇不使用NetApp助理或安裝控制台代理，您可以開始管理儲存體並使用Digital Advisor、 Amazon FSx for ONTAP、 Azure NetApp Files等服務。"了解沒有控制台代理您可以做什麼"。

3 關聯您的**NetApp**支援網站 **(NSS)** 帳戶

將您的NetApp支援網站 (NSS) 帳戶與控制台關聯，可以更輕鬆地管理您的授權和訂閱，並直接從控制台存取支援資源。

4 建立控制台代理

進階儲存管理功能和某些NetApp資料服務要求您安裝控制台代理程式。控制台代理程式使控制台能夠管理混合雲環境中的資源和流程。

您可以在雲端或本機網路中建立控制台代理程式。

- "詳細了解何時需要控制台代理以及它們如何運作"
- "了解如何在 AWS 中建立控制台代理"
- "了解如何在 Azure 中建立控制台代理"
- "了解如何在 Google Cloud 中建立控制台代理"
- "了解如何在本機建立控制台代理"

5 為主機新增儲存系統

在NetApp Console中，您可以新增或發現儲存系統來管理您的混合雲端儲存環境。使用NetApp助理新增您的第一個儲存系統。

如果在 AWS、Microsoft Azure 或 Google Cloud 中安裝控制台代理，則控制台會自動發現代理安裝位置的 Amazon S3 儲存桶、Azure Blob 儲存體或 Google Cloud Storage 儲存桶的相關資訊。這些系統會自動加入到「系統」頁面。

- "了解如何發現ONTAP系統"
- "了解如何發現StorageGRID系統"
- "了解如何發現 E 系列系統"

6 "訂閱**NetApp Intelligent Services**（可選）"

透過您的雲端供應商註冊NetApp Intelligent Services ，即可按小時（按需求付費）或按年計費。訂閱包

含NetApp Backup and Recovery、 Cloud Volumes ONTAP、 NetApp Cloud Tiering、 NetApp Ransomware Resilience、 NetApp Disaster Recovery和NetApp Data Classification。

準備NetApp Console的網路訪問

NetApp Console、 NetApp Console代理和NetApp資料服務需要出站網路存取以及聯繫必要端點的能力。

您需要為以下操作設定網路存取：

- 以軟體即服務 (SaaS) 形式存取NetApp Console的計算機
- 您在本機或雲端安裝的控制台代理程式。控制台代理。

> ⓘ 在 4.0.0 中， NetApp減少了控制台和控制台代理程式所需的網路端點，增強了安全性並簡化了部署。重要的是，4.0.0 版本之前的所有部署都將繼續全面支援。雖然先前的端點仍然可供現有代理程式使用，但NetApp強烈建議在確認代理程式升級成功後將防火牆規則更新到目前端點。"了解如何更新您的端點清單。"

NetApp Console和控制台代理程式聯繫的端點

您部署的每個代理程式和存取NetApp Console的每台電腦都必須連接到下面列出的端點。

部署在您的雲端提供者中的控制台代理程式需要存取該雲端提供者各自的端點。

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

雲端提供者端點聯繫了控制台代理

如果控制台代理程式部署在您的雲端提供者中，則它們必須能夠存取其他端點。

在安裝控制台代理之前設定雲端提供者網路端點存取。

- "為控制台代理程式設定 AWS 網路訪問"
- "為控制台代理程式設定 Azure 網路訪問"
- "為控制台代理設定 Google Cloud 網路訪問"

控制台代理聯繫的資料服務端點

一些NetApp資料服務以及Cloud Volumes ONTAP要求代理程式具有額外的出站網路存取權限。

Cloud Volumes ONTAP的端點

- "AWS 中的Cloud Volumes ONTAP端點"
- "Azure 中的Cloud Volumes ONTAP端點"
- "Google Cloud 中Cloud Volumes ONTAP的端點"

工作負載端點

控制台代理程式必須能夠存取以下NetApp工作負載端點。

端點	目的
https://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。

註冊或登入**NetApp Console**

若要使用控制台，請註冊或使用您的NetApp支援網站憑證登錄，或建立NetApp Console登入。如果您是公司第一個註冊的人，您將建立一個新的組織並擔任管理員。如果貴公司已有組織，請使用您現有的NetApp支援網站憑證或公司單一登入 (SSO) 註冊或登入。

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。第一個使用者將成為組織管理員，並管理使用者帳戶和權限。您可以稍後更新角色並新增更多管理員。

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*。

+ 身為首次使用者和組織管理員，您可以按照引導流程新增儲存資源、建立控制台代理程式等等。 "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。

開始使用NetApp Console助手

如果您是首次使用NetApp Console(SaaS) 並擁有組織管理員角色的用戶，則可以使用控制台助理來引導您完成初始設定程序。此助手可協助您新增NetApp支援網站 (NSS) 帳戶、新增控制台代理程式、新增叢集以及新增授權或訂閱，以便更輕鬆地開始管理您的資料。

存取控制台助手所需的角色

控制台助理僅對具有組織管理員角色的使用者可用。

預設情況下，對於具有組織管理員角色的首次用戶， NetApp Console會在主頁上顯示控制台助理。在您完成建立控制台代理程式和新增系統的必要任務之前，它將一直可用。

使用助手完成以下任務，這些任務將為您的NetApp Console環境提供最基本的設定：

- 新增NetApp支援網站 (NSS) 帳戶。

  "了解如何新增 NSS 帳戶"。

- 透過部署控制台代理程式連接到您的儲存環境。

  "了解如何在本機安裝控制台代理程式。"

- 透過新增或發現叢集來管理儲存系統
- 新增市場訂閱或 PAYGO 授權。

  "了解如何新增授權和訂閱"。

- 查看數據服務資訊。

NetApp Console入門（受限模式）

入門工作流程（受限模式）

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

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

1 "準備部署"

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

2 "部署控制台代理"

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

3 "訂閱NetApp Intelligent Services（可選）"

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

準備在受限模式下部署

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

步驟 **1**：了解限制模式的工作原理

在開始之前了解NetApp Console在受限模式下的工作方式。

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

此外，並非所有控制台功能和NetApp資料服務都可使用。

"了解限制模式的工作原理" 。

第 **2** 步：查看安裝選項

在受限模式下，您只能在雲端安裝控制台代理程式。有以下安裝選項可用：

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

第 **3** 步：查看主機需求

主機必須滿足特定的作業系統、RAM 和連接埠要求才能執行控制台代理。

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

專用主機

控制台代理需要專用主機。只要滿足以下尺寸要求，任何架構都受支援：

- CPU：8 核心或 8 個 vCPU
- 記憶體：32 GB

- 磁碟空間：建議主機預留165GB空間，分割區需求如下：
  - `/opt`：必須有 120 GiB 可用空間

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

  - `/var`：必須有 40 GiB 可用空間

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

AWS EC2 執行個體類型

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

Azure VM 大小

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

Google Cloud 機器類型

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

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

虛擬機器管理程序

需要經過認證可運行支援的作業系統的裸機或託管虛擬機器管理程式。

作業系統和容器要求

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

作業系統	支援的作業系統版本	支援的代理版本	所需的容器工具	**SELinux**
紅帽企業 Linux		9.6 • 僅限英文版本。 • 主機必須在 Red Hat 訂閱管理中註冊。如果未註冊，主機將無法在代理安裝期間存取儲存庫來更新所需的第三方軟體。	4.0.0 或更高版本，控制台處於標準模式或受限模式	Podman 版本 5.4.0 ，podman-compose 版本 1.5.0。 查看 Podman 設定要求 。

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

步驟 **4**：安裝 **Podman** 或 **Docker Engine**

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

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

- Red Hat Enterprise Linux 8 和 9 需要 Podman。

  查看支援的 Podman 版本 。

- Ubuntu 需要 Docker 引擎。

  查看支援的 Docker Engine 版本 。

範例 **1.** 步驟

Podman

請依照以下步驟安裝和設定 Podman：

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

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

步驟

1. 如果主機上安裝了 podman-docker 套件，請將其刪除。

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

2. 安裝 Podman。

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

   a. 對於 Red Hat Enterprise Linux 9.6：

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

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

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

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

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

   c. 對於 Red Hat Enterprise Linux 8：

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

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

3. 啟用並啟動 podman.socket 服務。

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

4. 安裝 python3。

```
sudo dnf install python3
```

5. 如果您的系統上還沒有 EPEL 儲存庫包，請安裝它。

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

6. 如果使用 Red Hat Enterprise 9：

   a. 安裝EPEL存儲庫軟體包。

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

   +

   a. 安裝 podman-compose 套件 1.5.0。

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

7. 如果使用的是 Red Hat Enterprise Linux 8：

   a. 安裝EPEL存儲庫軟體包。

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

   b. 安裝 podman-compose 套件 1.0.6。

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

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

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

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

```
podman info | grep networkBackend
```

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

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

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

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

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

v. 重新啟動 podman。

```
systemctl restart podman
```

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

```
podman info | grep networkBackend
```

Docker 引擎

依照 Docker 的文件安裝 Docker Engine。

步驟

1. "查看 Docker 的安裝說明"

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

2. 驗證 Docker 是否已啟用並正在運行。

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

步驟 **5**：準備網路訪問

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

連接到目標網絡

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

準備網路以供使用者存取**NetApp Console**

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

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

+

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

用於日常運營的出站互聯網訪問

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

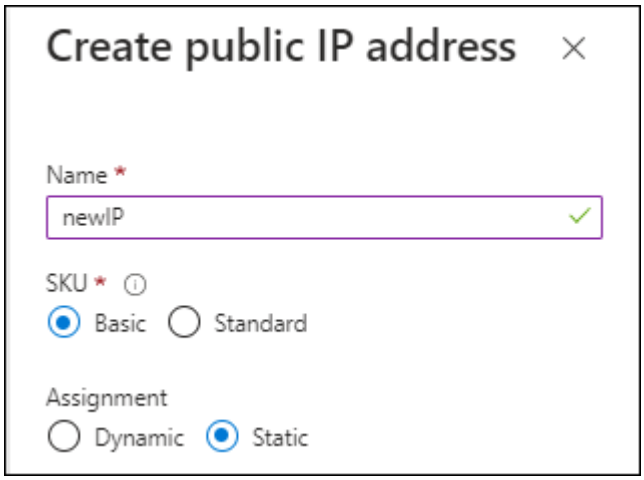
端點	目的
AWS 環境	AWS 服務（amazonaws.com）： • 雲形成 • 彈性運算雲（EC2） • 身分和存取管理 (IAM) • 金鑰管理服務（KMS） • 安全性令牌服務 (STS) • 簡單儲存服務（S3）
管理 AWS 資源。端點取決於您的 AWS 區域。 "有關詳細信息，請參閱 AWS 文檔"	Amazon FsX for NetApp ONTAP： • api.workloads.netapp.com
基於 Web 的控制台透過與 Workload Factory API 互動來管理和操作基於ONTAP 的FSx 工作負載。	Azure 環境

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

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

Azure 中的公用 **IP** 位址

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



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

"Azure 文件：公用 IP SKU"

代理伺服器

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

- IP 位址
- 證書
- HTTPS 憑證

連接埠

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

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

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

啟用 **NTP**

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

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

步驟 **6**：準備雲端權限

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

若要查看所需的步驟，請選擇用於雲端提供者的身份驗證選項。

AWS IAM 角色

使用 IAM 角色為控制台代理提供權限。

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

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

步驟

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

結果

您現在擁有控制台代理 EC2 執行個體的 IAM 角色。

AWS 存取金鑰

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

步驟

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

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

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

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

Azure 角色

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

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

步驟

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

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

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

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

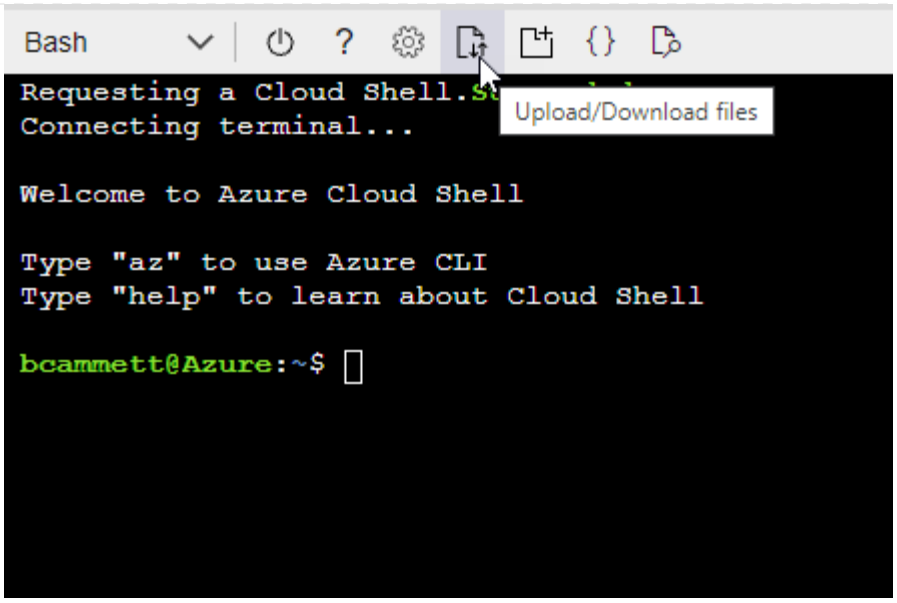
   例子

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

4. 使用 JSON 檔案在 Azure 中建立自訂角色。

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

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



c. 使用 Azure CLI 建立自訂角色：

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

Azure 服務主體

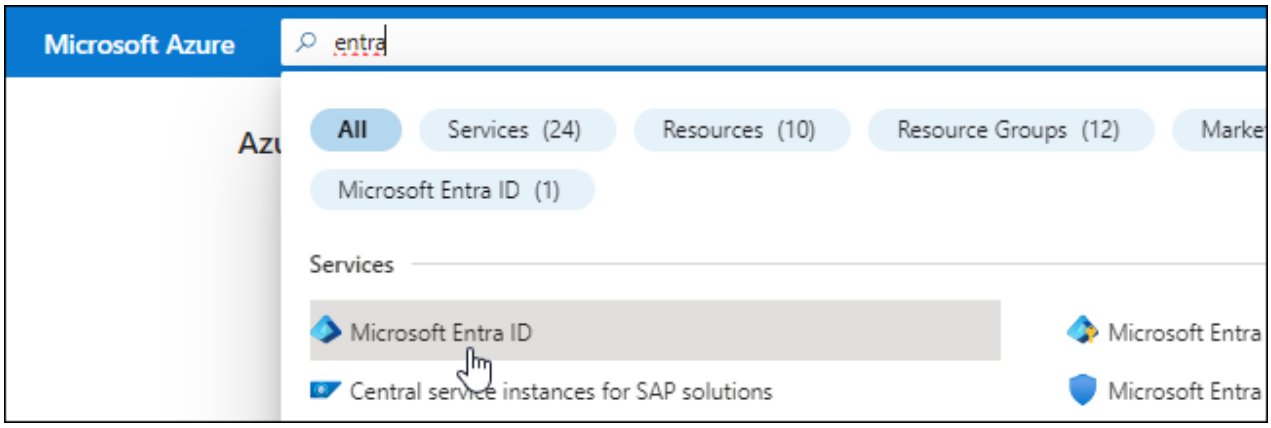
在 Microsoft Entra ID 中建立並設定服務主體，並取得控制台所需的 Azure 憑證。安裝控制台代理程式後，您需要向控制台提供這些憑證。

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

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

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

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



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

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

6. 選擇*註冊*。

您已建立 AD 應用程式和服務主體。

將應用程式指派給角色

1. 建立自訂角色：

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

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

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

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

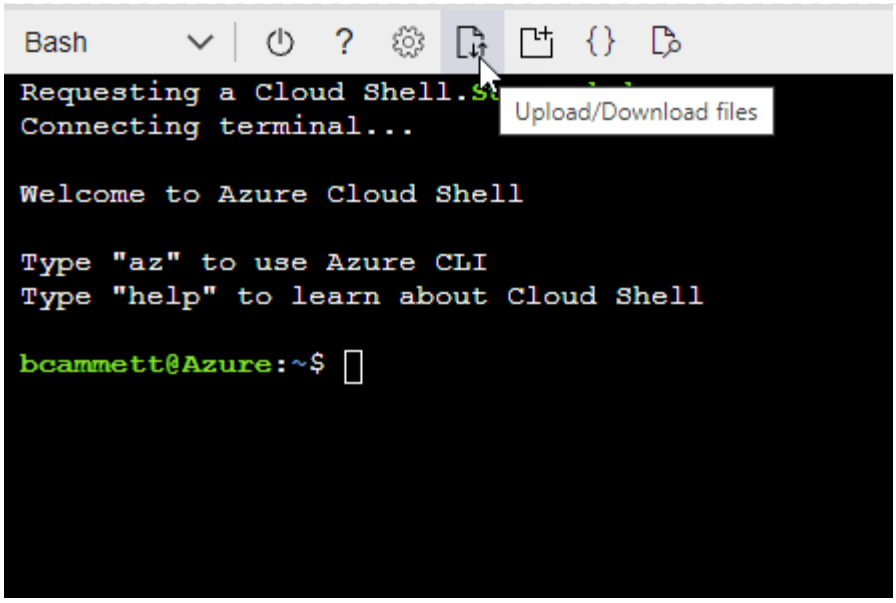
例子

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

c. 使用 JSON 檔案在 Azure 中建立自訂角色。

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

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



- 使用 Azure CLI 建立自訂角色：

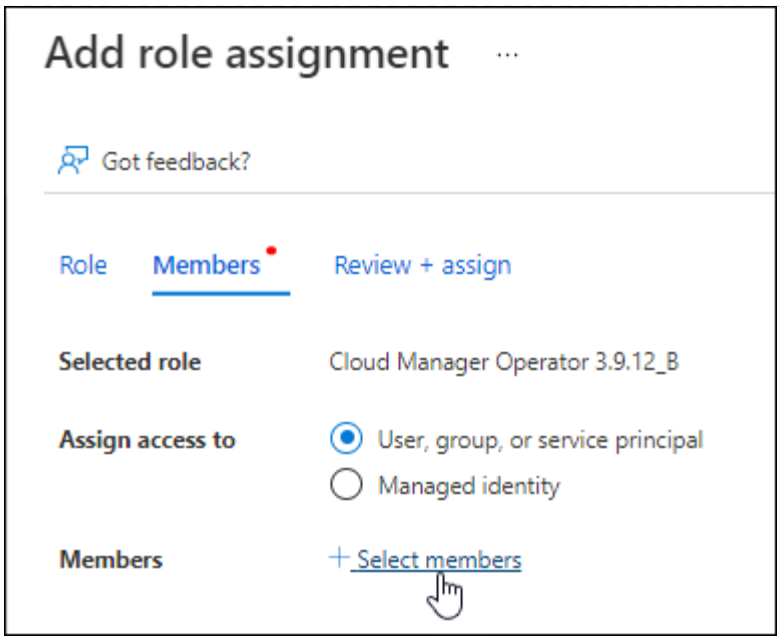
```
az role definition create --role-definition agent_Policy.json
```

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

2. 將應用程式指派給角色：

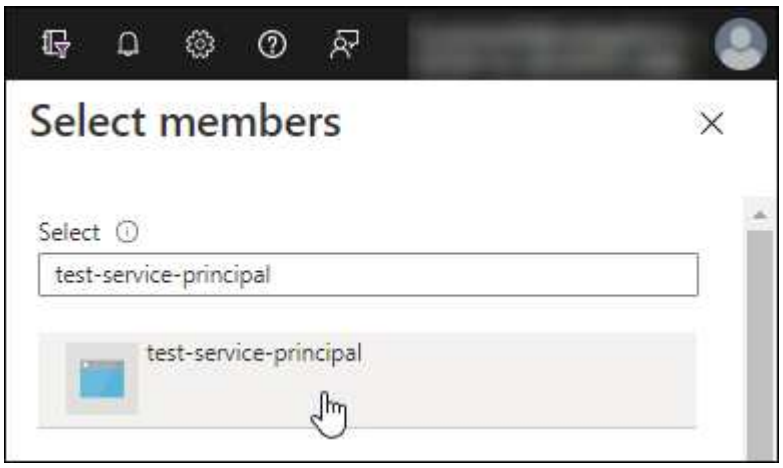
   a. 從 Azure 入口網站開啟 **Subscriptions** 服務。
   b. 選擇訂閱。
   c. 選擇“存取控制 (IAM)”>“新增”>“新增角色分配”。
   d. 在*角色*標籤中，選擇*控制台操作員*角色並選擇*下一步*。
   e. 在「成員」標籤中，完成以下步驟：

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



- 搜尋應用程式的名稱。

  以下是一個例子：



- 選擇應用程式並選擇*選擇*。
- 選擇“下一步”。

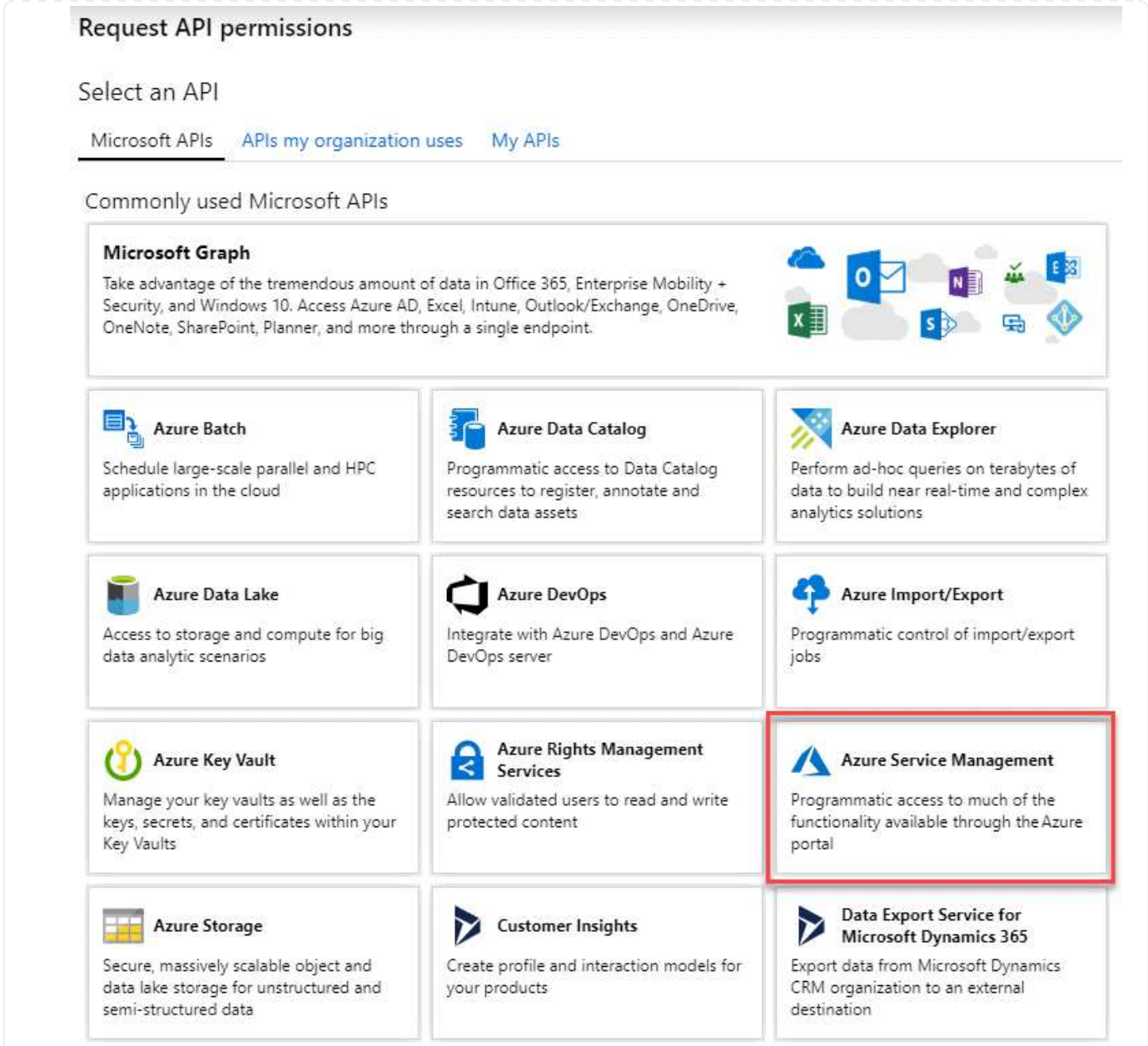
f. 選擇*審閱+分配*。

服務主體現在具有部署控制台代理程式所需的 Azure 權限。

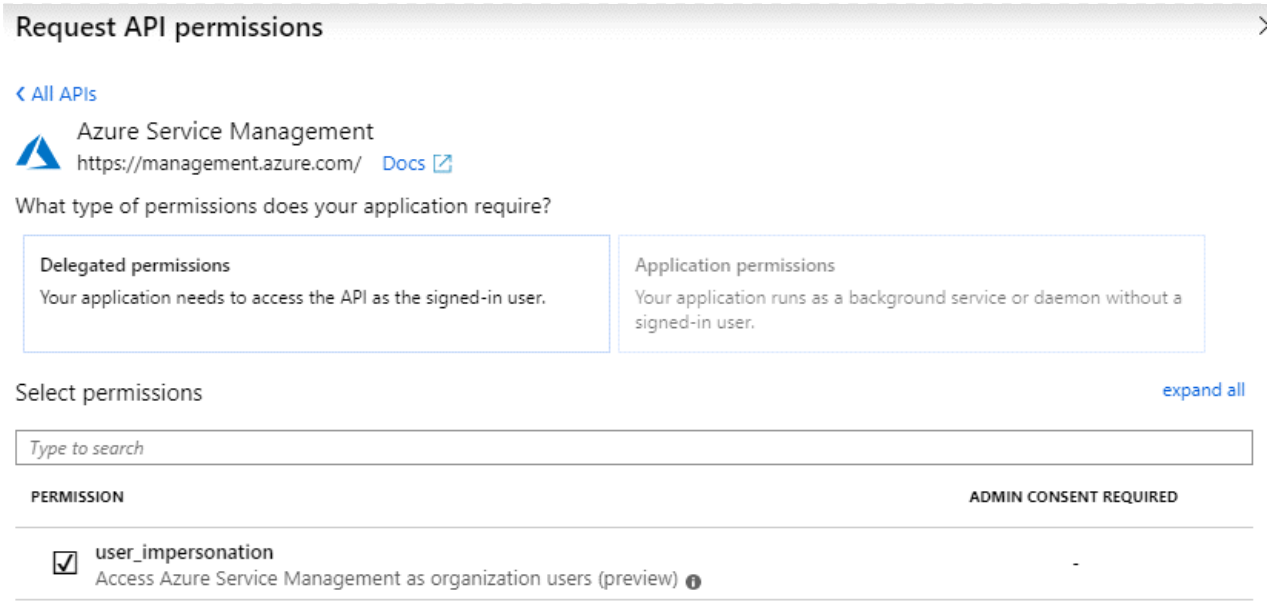
如果您想要從多個 Azure 訂閱部署Cloud Volumes ONTAP ，則必須將服務主體綁定到每個訂閱。在NetApp Console中，您可以選擇部署Cloud Volumes ONTAP時要使用的訂閱。

新增 **Windows Azure** 服務管理 **API** 權限

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

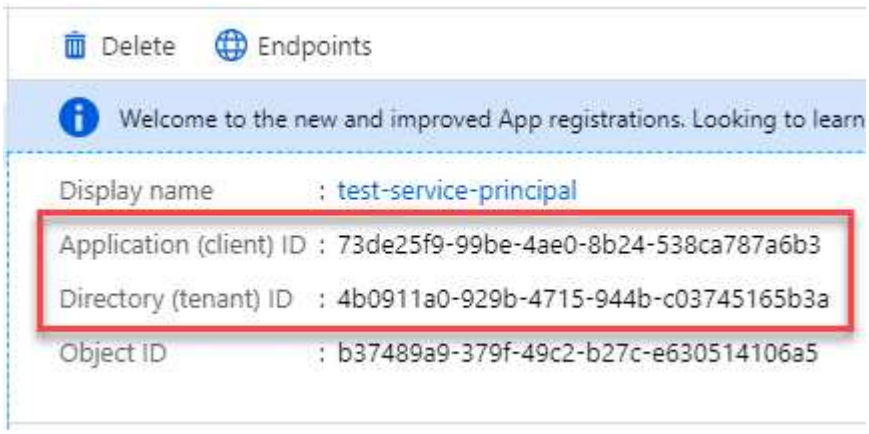


4. 選擇*以組織使用者身分存取 Azure 服務管理*，然後選擇*新增權限*。



取得應用程式的應用程式**ID**和目錄**ID**

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



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

建立客戶端機密

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

結果

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

Google Cloud 服務帳號

建立角色並將其套用至您將用於控制台代理 VM 執行個體的服務帳戶。

步驟

1. 在 Google Cloud 中建立自訂角色：

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

   b. 從 Google Cloud 啟動雲殼。

   c. 上傳包含控制台代理程式所需權限的 YAML 檔案。

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

      以下範例在專案層級建立一個名為「agent」的角色：

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

   +
   "Google Cloud 文件：建立和管理自訂角色"

2. 在 Google Cloud 中建立服務帳號：

   a. 從 IAM 和管理服務中，選擇 服務帳戶 > 建立服務帳戶。

   b. 輸入服務帳戶詳細資料並選擇*建立並繼續*。

   c. 選擇您剛剛建立的角色。

   d. 完成剩餘步驟以建立角色。

      "Google Cloud 文件：建立服務帳號"

步驟 **7**：啟用 **Google Cloud API**

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

步

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

在限制模式下部署控制台代理理

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

步驟 1：安裝控制台代理

從雲端提供者的市場安裝控制台代理程式或在 Linux 主機上手動安裝。

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

AWS 商業市場

開始之前

需要以下物品：

- 滿足組網需求的VPC及子網路。

  "了解網路要求"

- 具有附加策略的 IAM 角色，其中包含控制台代理程式所需的權限。

  "了解如何設定 AWS 權限"

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

  "審查代理要求"。

- EC2 執行個體的金鑰對。

步驟

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

   訂閱過程可能需要幾分鐘。

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

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

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

       "查看 AWS 的安全群組規則"。

- 配置儲存：保留根磁碟區的預設大小和磁碟類型。

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

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

結果

AWS 使用指定的設定啟動軟體。控制台代理大約需要五分鐘即可部署。

下一步是什麼？

設定NetApp Console。

AWS 政府市場

開始之前

需要以下物品：

- 滿足組網需求的VPC及子網路。

  "了解網路要求"

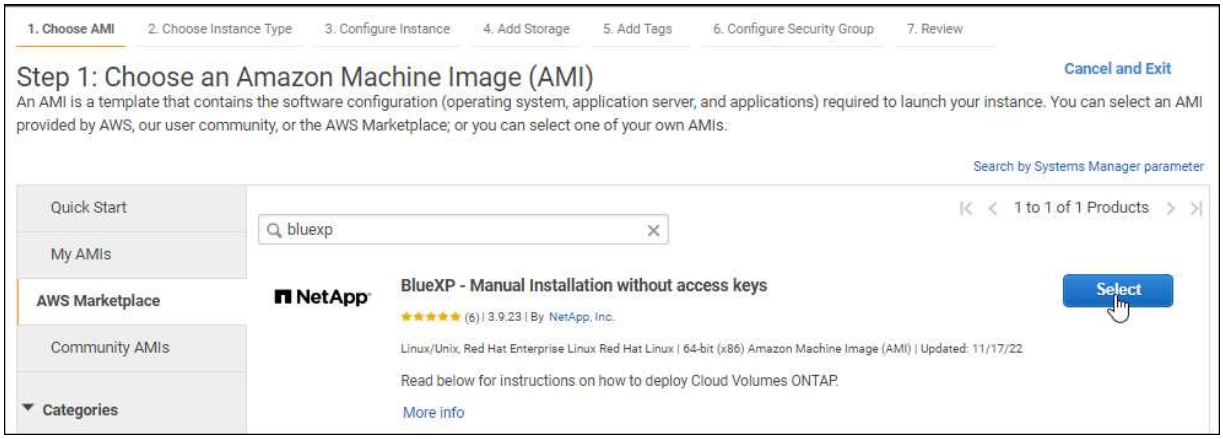
- 具有附加策略的 IAM 角色，其中包含控制台代理程式所需的權限。

  "了解如何設定 AWS 權限"

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

步驟

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



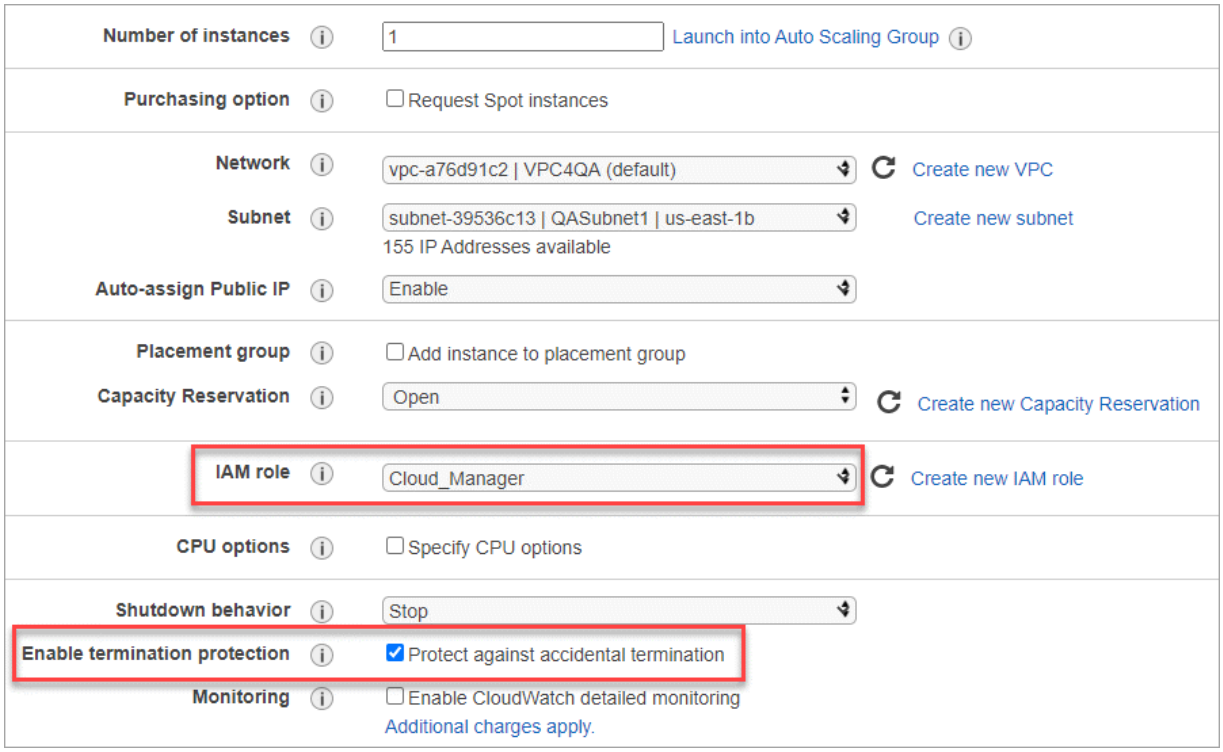
d. 選擇*繼續*。

2. 依照提示設定並啟動實例：

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

     "查看實例要求"。

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



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

結果

AWS 使用指定的設定啟動軟體。控制台代理大約需要五分鐘即可部署。

下一步是什麼？

設定控制台。

Azure 政府市場

開始之前

您應該具有以下內容：

- 滿足網路需求的 VNet 和子網路。

  "了解網路要求"

- 包含控制台代理程式所需權限的 Azure 自訂角色。

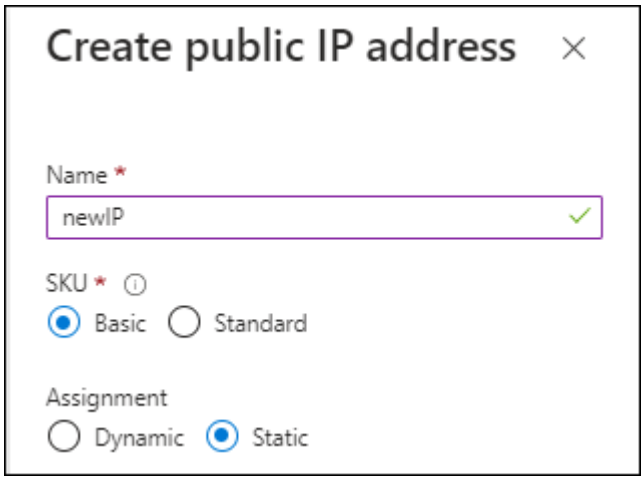
  "了解如何設定 Azure 權限"

步驟

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

   配置虛擬機器時請注意以下事項：

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



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

   "Azure 文件：公用 IP SKU"

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

     "查看 Azure 的安全性群組規則" 。

   - 身分：在*管理*下，選擇*啟用系統指派的託管身分*。

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

結果

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

下一步是什麼？

設定NetApp Console。

手動安裝（必須用於 **Google Cloud**）

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

開始之前

您應該具有以下內容：

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

  您可以選擇在安裝後設定代理伺服器，但這樣做需要重新啟動控制台代理。

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

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

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

關於此任務

安裝後，如果有新版本可用，控制台代理會自動更新。

步驟

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

```
unset http_proxy
unset https_proxy
```

   如果不刪除這些系統變量，安裝將會失敗。

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

     選擇下載代理安裝程式檔案或檔案的 URL。

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

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

其中 <version> 是您下載的控制台代理的版本。

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

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

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

如果要設定透明代理，可以在安裝完成後進行設定。 "了解代理維護控制台"

+

以下是使用 CA 簽章憑證設定明確代理伺服器的範例：

+

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

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

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

+ 請注意以下事項：

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

+ 例如：

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

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

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

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

例如：

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

a. 重新啟動控制台代理虛擬機器。

結果

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

下一步是什麼？

設定NetApp Console。

第 **2** 步：設定**NetApp Console**

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

開始之前

設定控制台代理的人員必須使用尚不屬於控制台組織的登入名稱登入控制台。

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

步驟

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

d. 選擇*在此帳戶上啟用受限模式*。

請注意，帳戶建立後您無法變更此設定。您以後無法啟用受限模式，也無法停用它。

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

a. 選擇*讓我們開始吧*。

結果

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

下一步是什麼？

向控制台提供您先前設定的權限。

步驟 **3**：向控制台代理提供權限

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

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

"了解如何準備雲端權限" 。

AWS IAM 角色

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

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

步驟

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

AWS 存取金鑰

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

步驟

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

Azure 角色

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

步驟

1. 從 Azure 入口網站開啟「訂閱」服務並選擇您的訂閱。

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

   "Microsoft Azure 文件：了解 Azure RBAC 的範圍"

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

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

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

Azure 服務主體

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

步驟

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

結果

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

Google Cloud 服務帳號

將服務帳戶與控制台代理 VM 關聯。

步驟

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

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

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

訂閱**NetApp Intelligent Services**（受限模式）

從雲端供應商的市場訂閱NetApp Intelligent Services，以按小時費率（PAYGO）或透過年度合約支付資料服務費用。如果您從NetApp （BYOL）購買了許可證，您還需要訂閱市場產品。您的許可證始終會先被收費，但如果您超出許可容量或許可證期限到期，則會按小

時費率向您收費。

市場訂閱支援以受限模式對以下數據服務收費：

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

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

開始之前

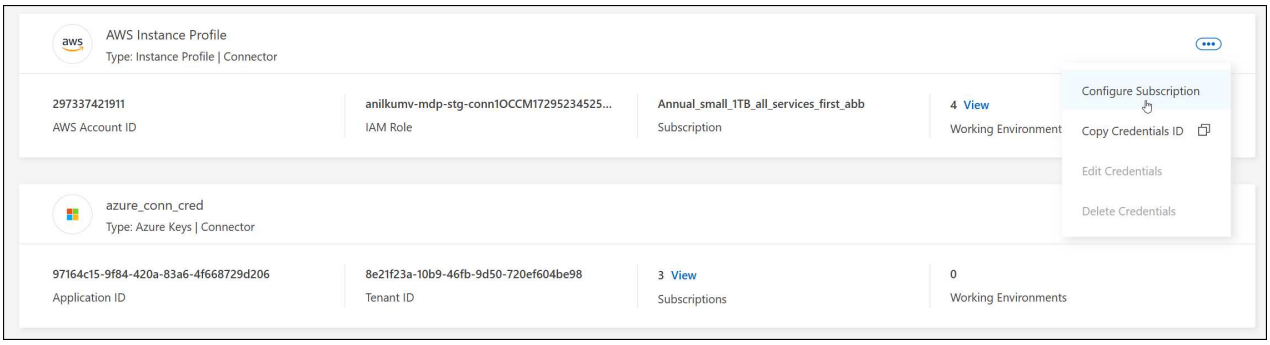
您必須已經部署控制台代理程式才能訂閱資料服務。您需要將市場訂閱與連接到控制台代理的雲端憑證關聯起來。

AWS

步驟

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

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



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

   a. 選擇“查看購買選項”。

   b. 選擇*訂閱*。

   c. 選擇*設定您的帳戶*。

      您將被重新導向到NetApp Console。

   d. 從「訂閱分配」頁面：

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

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

   對於所有其他組織或帳戶，您需要重複這些步驟來手動關聯訂閱。

   ◦ 選擇*儲存*。

Azure

步驟

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

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

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

    a. 如果出現提示，請登入您的 Azure 帳戶。

    b. 選擇*訂閱*。

    c. 填寫表格並選擇*訂閱*。

    d. 訂閱程序完成後，選擇*立即配置帳戶*。

    您將被重新導向到NetApp Console。

    e. 從「訂閱分配」頁面：

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

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

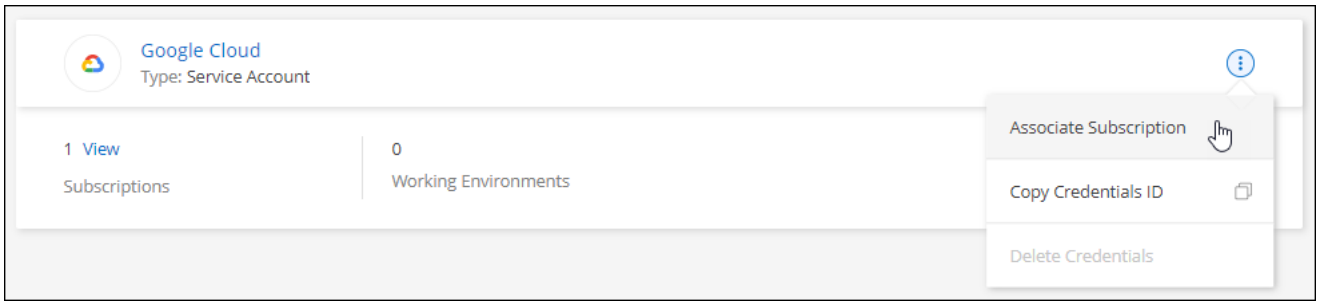
對於所有其他組織或帳戶，您需要重複這些步驟來手動關聯訂閱。

    。選擇*儲存*。

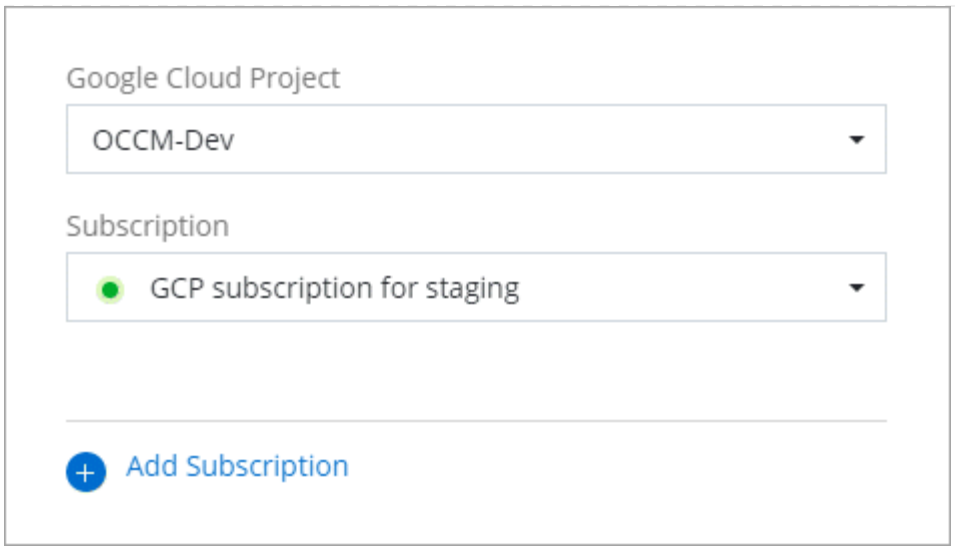
Google雲

步驟

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



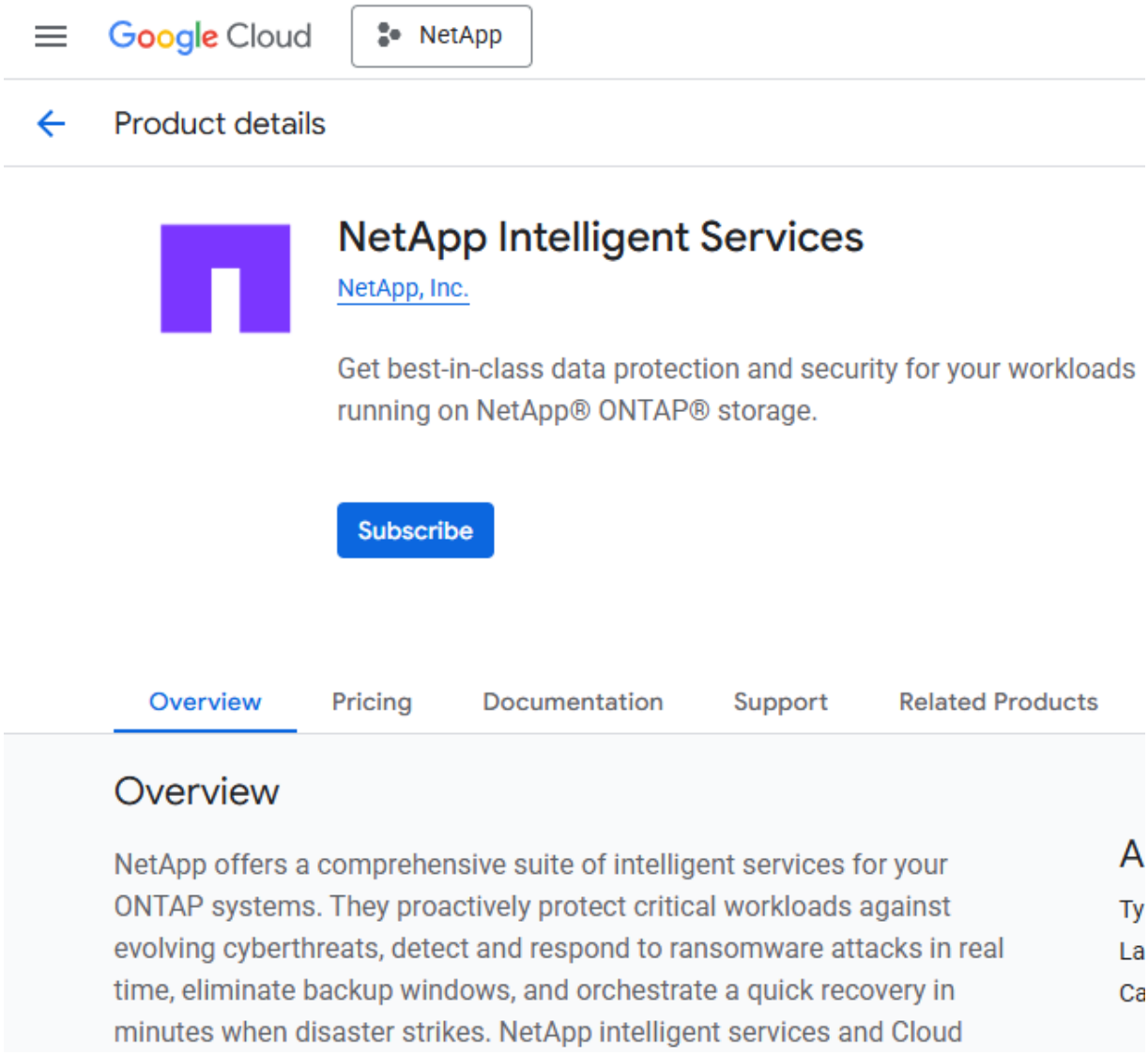
1. 若要使用選定的憑證設定現有訂閱，請從下拉清單中選擇一個 Google Cloud 專案和訂閱，然後選擇*設定*。



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

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

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



b. 選擇*訂閱*。

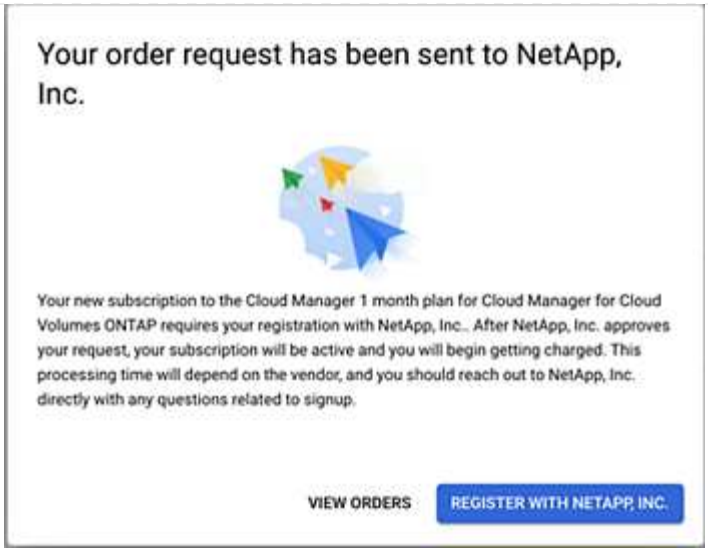
c. 選擇適當的結算帳戶並同意條款和條件。

d. 選擇*訂閱*。

   此步驟將您的轉移請求傳送給NetApp。

e. 在彈出的對話方塊中，選擇*向NetApp, Inc. 註冊*。

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



f. 完成「訂閱分配」頁面上的步驟：

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

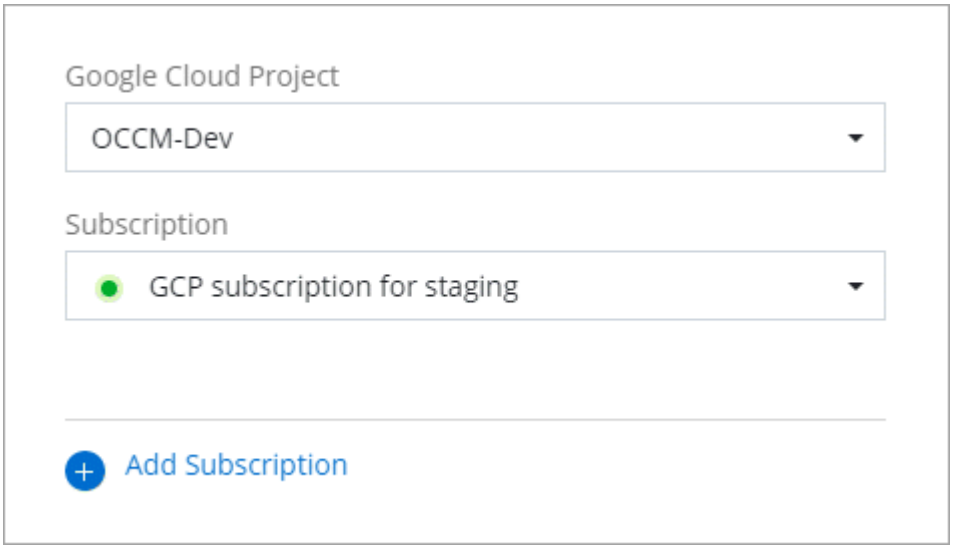
- 選擇您想要與此訂閱關聯的控制台組織。
- 在「取代現有訂閱」欄位中，選擇是否要用這個新訂閱自動取代組織的現有訂閱。

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

對於所有其他組織或帳戶，您需要重複這些步驟來手動關聯訂閱。

◦ 選擇*儲存*。

3. 此過程完成後，導覽回控制台中的「憑證」頁面並選擇此新訂閱。



相關資訊

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

接下來可以做什麼（受限模式）

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

如需協助，請參閱以下服務的文件：

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

相關資訊

"NetApp Console部署模式"

開始使用私密模式

入門工作流程（**BlueXP**私人模式）

BlueXP私有模式（傳統BlueXP介面）通常用於沒有網路連線的本機環境和安全雲端區域，其中包括 AWS Secret Cloud、AWS Top Secret Cloud 和 Azure IL6。 NetApp繼續透過傳統的BlueXP介面支援這些環境。

"BlueXP私人模式的 PDF 文檔"

私有模式支援的功能和資料服務

下表可以幫助您快速識別哪些BlueXP服務和功能支援私人模式。

請注意，某些服務可能會受到限制。

產品領域	**BlueXP**服務或功能	私人模式
工作環境 表格的這一部分列出了對BlueXP畫布的工作環境管理的支援。它沒有指出BlueXP backup and recovery所支援的備份目的地。	適用於ONTAP 的Amazon FSx	不
	亞馬遜 S3	不
	Azure Blob	不
	Azure NetApp Files	不
	Cloud Volumes ONTAP	是的
	Google Cloud NetApp Volumes	不
	Google 雲端儲存	不
	本地ONTAP集群	是的
	E系列	不
	StorageGRID	不
服務	警報	不
	備份和復原	是的https://docs.netapp.com/us-en/data-services-backup-recovery/prev-ontap-protect-journey.html#support-for-sites-with-no-internet-connectivity["查看ONTAP磁碟區資料支援的備份目標列表"^]
	分類	是的
	複製和同步	不
	數位顧問	不
	數位錢包	是的
	災難復原	不
	經濟效益	不
	勒索軟體抵禦能力	不
	複製	是的
	軟體更新	不
	永續性	不
	分層	不
	卷緩存	不
	工作負載工廠	不

產品領域	**BlueXP**服務或功能	私人模式
特徵	身分和存取管理	是的
	證書	是的
	聯邦	不
	多因素身份驗證	不
	NSS 帳戶	不
	通知	不
	搜尋	不
	時間軸	是的