



控制台代理

NetApp Console setup and administration

NetApp

January 27, 2026

目錄

控制台代理	1
了解NetApp Console代理	1
控制台代理程式必須始終處於執行狀態	3
支援的位置	3
與雲端提供者的溝通	3
限制模式	3
如何安裝控制台代理	3
雲端提供者權限	3
代理升級	4
作業系統和虛擬機器維護	4
多系統和代理	4
部署控制台代理	5
AWS	5
Azure	30
Google雲	76
在本地安裝代理	107
維護控制台代理	143
為控制台代理程式維護 VCenter 或 ESXi 主機	143
安裝 CA 簽署的憑證以進行基於 Web 的控制台訪問	146
配置控制台代理以使用代理伺服器	148
控制台代理故障排除	151
解除安裝並刪除控制台代理	155
管理雲端提供者憑證	156
AWS	156
Azure	169
Google雲	182

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
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）

	可聯絡經紀人獲取資訊	無需代理即可購買
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
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。

連接到目標網路

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) : • 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。
\ 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.bluelxp.netapp.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluelxp.netapp.com \ https://cdn.auth0.com	在NetApp Console中提供功能和服務。

端點	目的
https://bluexpinfraproduct.eastus2.data.azurecr.io \ https://bluexpinfraproduct.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。

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：設定網路

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。

連接到目標網路

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) : • 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。
\ 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.bluelxp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluelxp.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。

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 • 僅限英文版本。 • 主機必須在 Red Hat 訂閱管理中註冊。如果未註冊，主機將無法在代理安裝期間存取儲存庫來更新所需的第三方軟體。	4.0.0 或更高版本，控制台處於標準模式或受限模式	Podman 版本 5.4.0，podman-compose 版本 1.5.0。 查看 Podman 設定要求 。
在強制模式或寬容模式下受支持		9.1 至 9.4 • 僅限英文版本。 • 主機必須在 Red Hat 訂閱管理中註冊。如果未註冊，主機將無法在代理安裝期間存取儲存庫來更新所需的第三方軟體。	3.9.50 或更高版本，控制台處於標準模式或受限模式	Podman 版本 4.9.4，podman-compose 版本 1.5.0。 查看 Podman 設定要求 。

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 • 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

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)： • 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。
\ 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.blueexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.blueexp.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。

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：設定網路

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。

連接到目標網路

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.blueexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.blueexp.netapp.com \ https://cdn.auth0.com	在NetApp Console中提供功能和服務。
\ https://blueexpinfraprod.eastus2.data.azurecr.io \ https://blueexpinfraprod.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。

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/read",
"Microsoft.Network/networkInterfaces/ipConfigurations/read",
"Microsoft.Resources/deployments/operations/read",
"Microsoft.Resources/deployments/read",
"Microsoft.Resources/deployments/delete",
"Microsoft.Resources/deployments/cancel/action",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Resources/resources/read",
"Microsoft.Resources/subscriptions/operationresults/read",
"Microsoft.Resources/subscriptions/resourceGroups/delete",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Authorization/roleDefinitions/write",
"Microsoft.Authorization/roleAssignments/write",

```

```

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

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

```

2. 透過將 Azure 訂閱 ID 新增至可分配範圍來修改 JSON。

例子

```

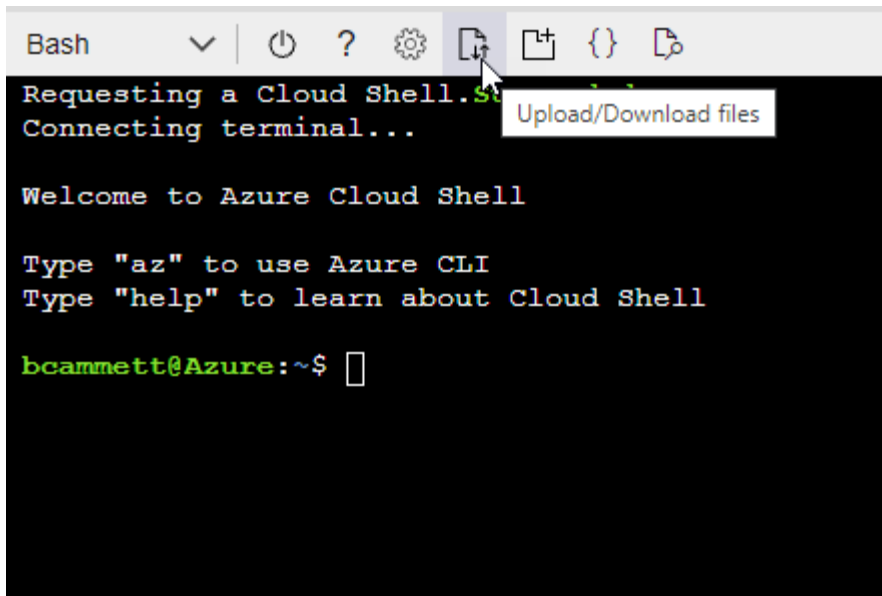
"AssignableScopes": [
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzzz"
]

```

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。

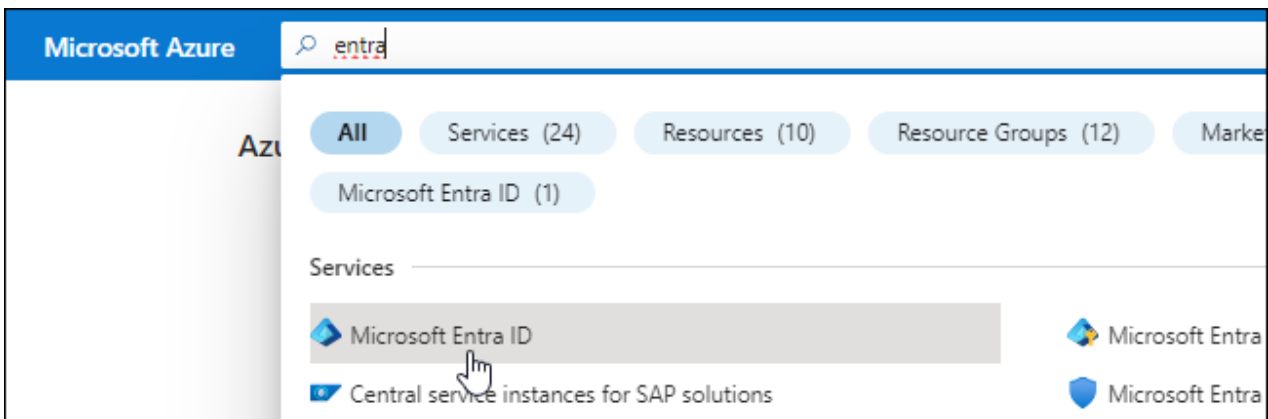
在 Microsoft Entra ID 中建立並設定服務主體，並取得控制台所需的 Azure 憑證。

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：

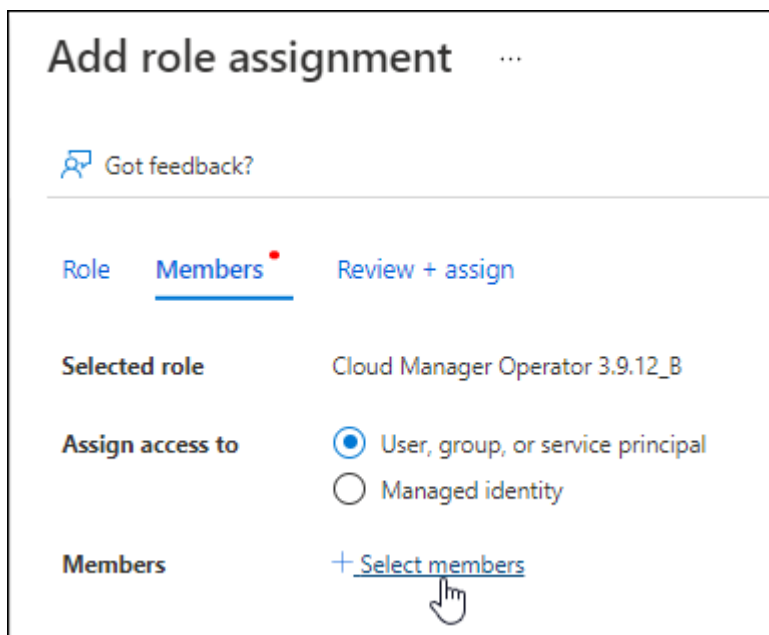
- 名稱：輸入應用程式的名稱。
- 帳戶類型：選擇帳戶類型（任何類型都可以與NetApp Console一起使用）。
- 重定向 **URI**：您可以將此欄位留空。

6. 選擇*註冊*。

您已建立 AD 應用程式和服務主體。

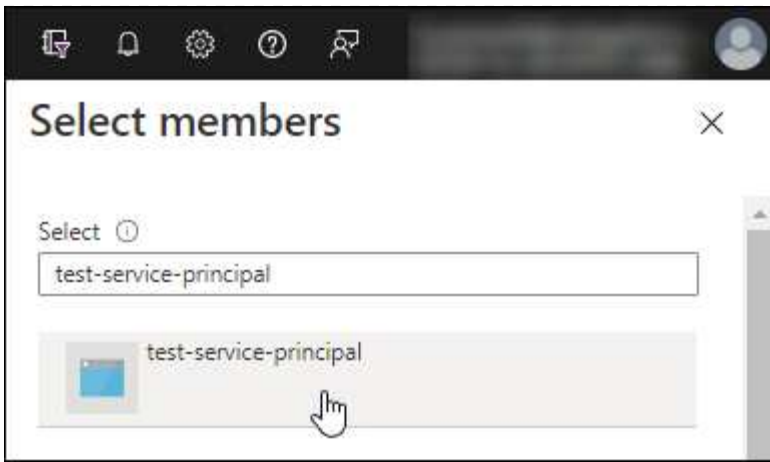
將自訂角色指派給應用程式

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」。

Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

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



**Azure Batch**
Schedule large-scale parallel and HPC applications in the cloud

**Azure Data Catalog**
Programmatic access to Data Catalog resources to register, annotate and search data assets

**Azure Data Explorer**
Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

**Azure Data Lake**
Access to storage and compute for big data analytic scenarios

**Azure DevOps**
Integrate with Azure DevOps and Azure DevOps server

**Azure Import/Export**
Programmatic control of import/export jobs

**Azure Key Vault**
Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

**Azure Rights Management Services**
Allow validated users to read and write protected content

**Azure Service Management**
Programmatic access to much of the functionality available through the Azure portal

**Azure Storage**
Secure, massively scalable object and data lake storage for unstructured and semi-structured data

**Customer Insights**
Create profile and interaction models for your products

**Data Export Service for Microsoft Dynamics 365**
Export data from Microsoft Dynamics CRM organization to an external destination

4. 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*。

Request API permissions

[← All APIs](#)



Azure Service Management

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

What type of permissions does your application require?

Delegated permissions

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

Application permissions

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

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED

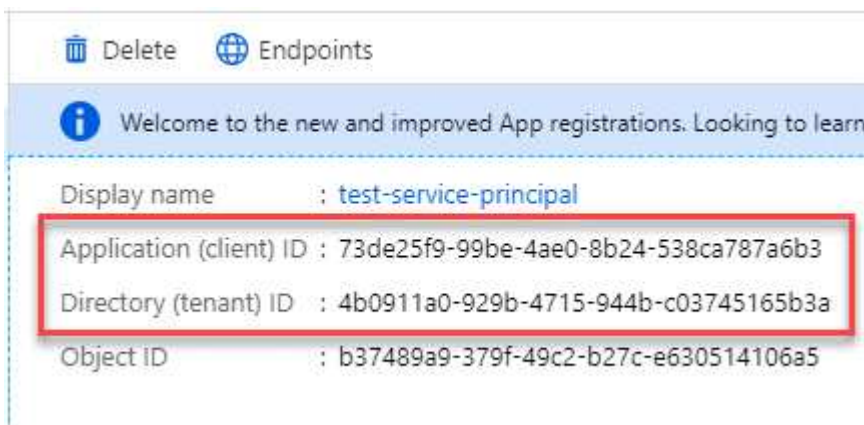


user_impersonation

Access Azure Service Management as organization users (preview)

取得應用程式的應用程式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。

Client secrets

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

[+ New client secret](#)

DESCRIPTION	EXPIRES	VALUE	Copy to clipboard
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA	

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

- 選擇“管理 > 代理”。
- 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：設定網路

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。

連接到目標網路

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.blueexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.blueexp.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。

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。

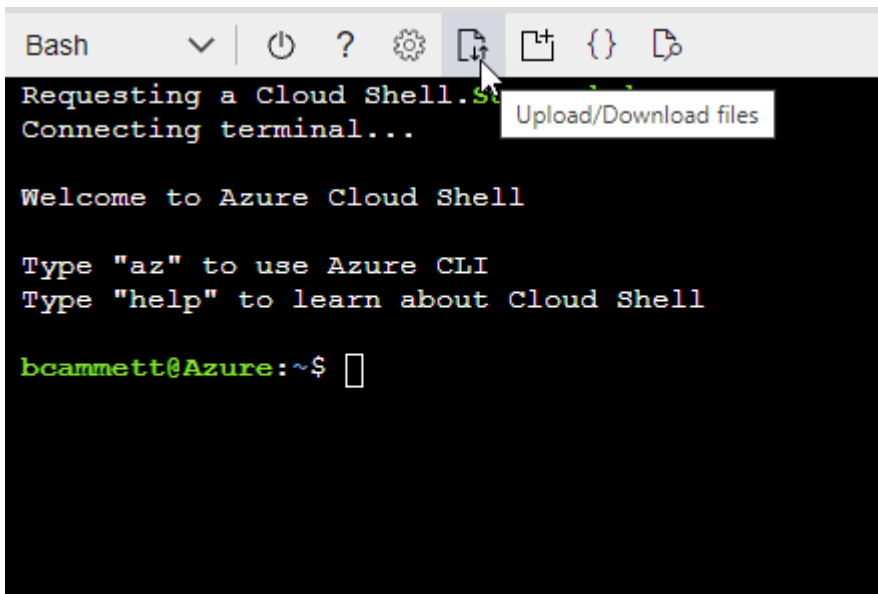
例子

```
"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

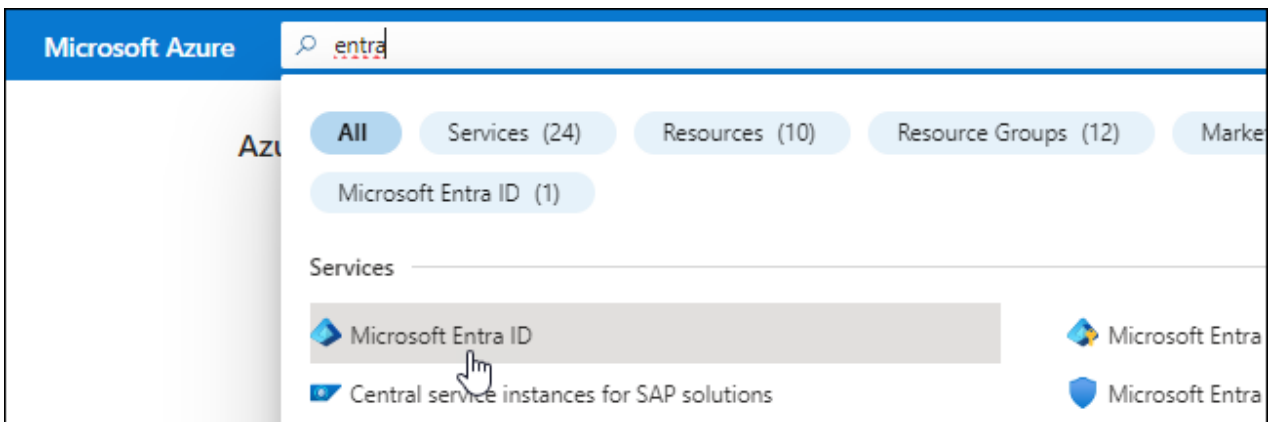
在 Microsoft Entra ID 中建立並設定服務主體，並取得控制台所需的 Azure 憑證。

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。

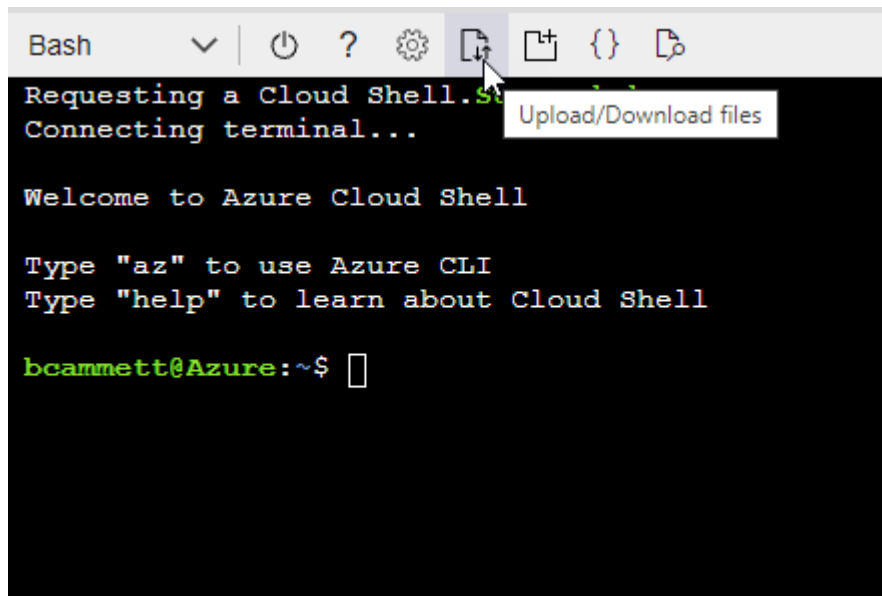
例子

```
"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
```

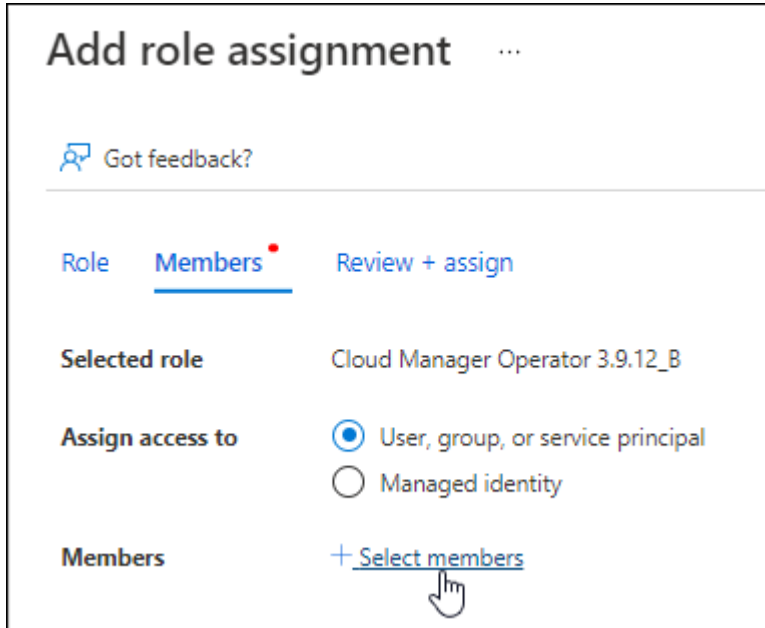
現在您應該有一個名為「控制台操作員」的自訂角色，可以將其指派給控制台代理虛擬機器。

2. 將應用程式指派給角色：

- 從 Azure 入口網站開啟 **Subscriptions** 服務。
- 選擇訂閱。
- 選擇“存取控制 (IAM)”>“新增”>“新增角色分配”。
- 在*角色*標籤中，選擇*控制台操作員*角色並選擇*下一步*。

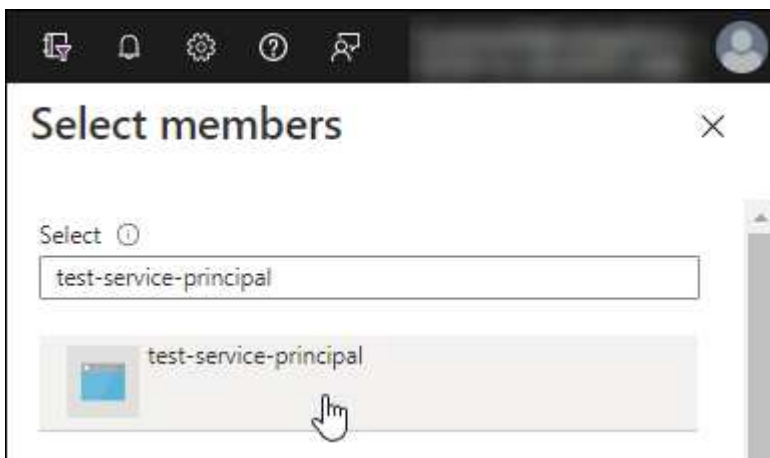
e. 在「成員」標籤中，完成以下步驟：

- 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」。

Request API permissions

Select an API

Microsoft APIs **APIs my organization uses** My APIs

Commonly used Microsoft APIs

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

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

4. 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*。

Request API permissions

[< All APIs](#)



Azure Service Management

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

What type of permissions does your application require?

Delegated permissions

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

Application permissions

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

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED

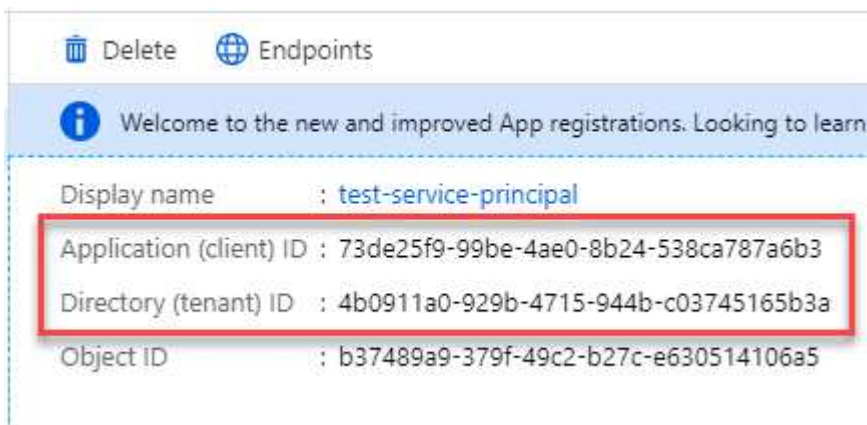


user_impersonation

Access Azure Service Management as organization users (preview)

取得應用程式的應用程式ID和目錄ID

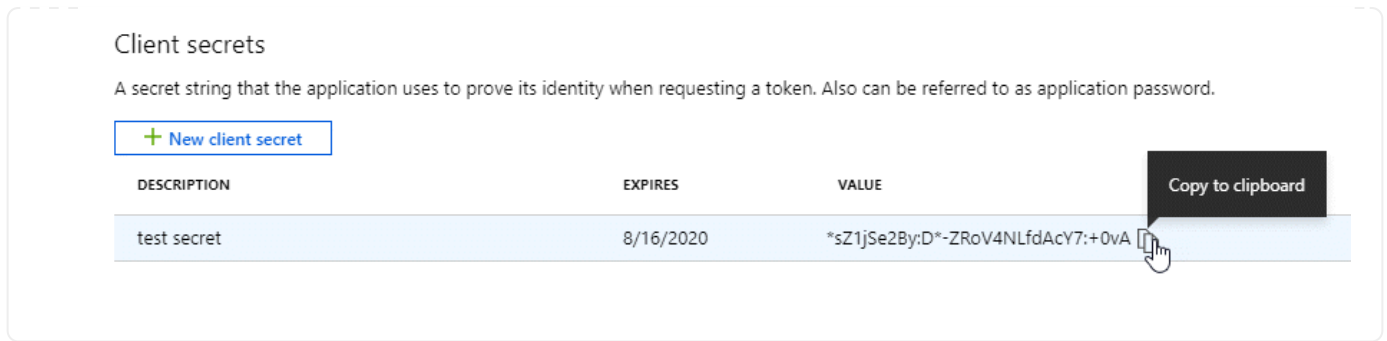
1. 在*Microsoft Entra ID*服務中，選擇*App Registrations*並選擇應用程式。
2. 複製*應用程式（客戶端）ID*和*目錄（租用戶）ID*。



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

步驟 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.blueexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.blueexp.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。

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。

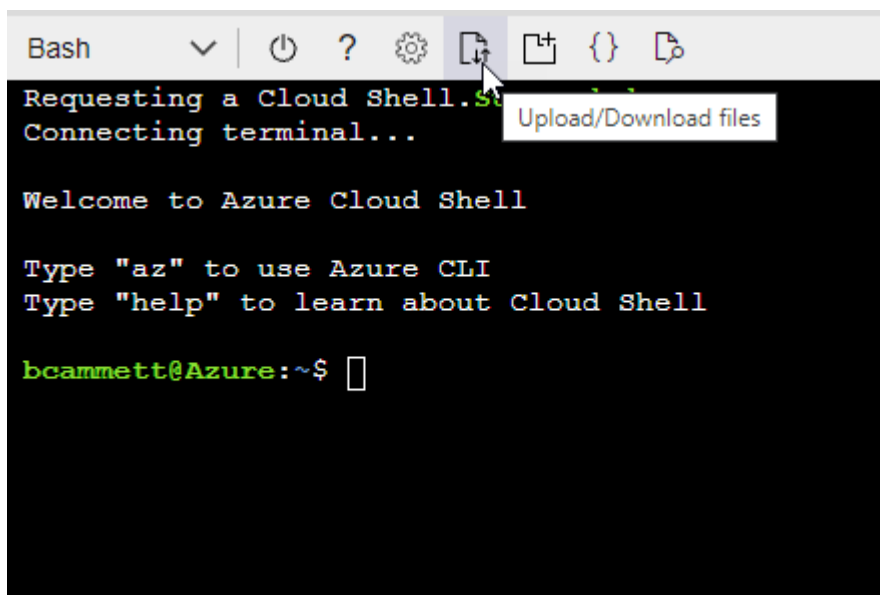
例子

```
"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

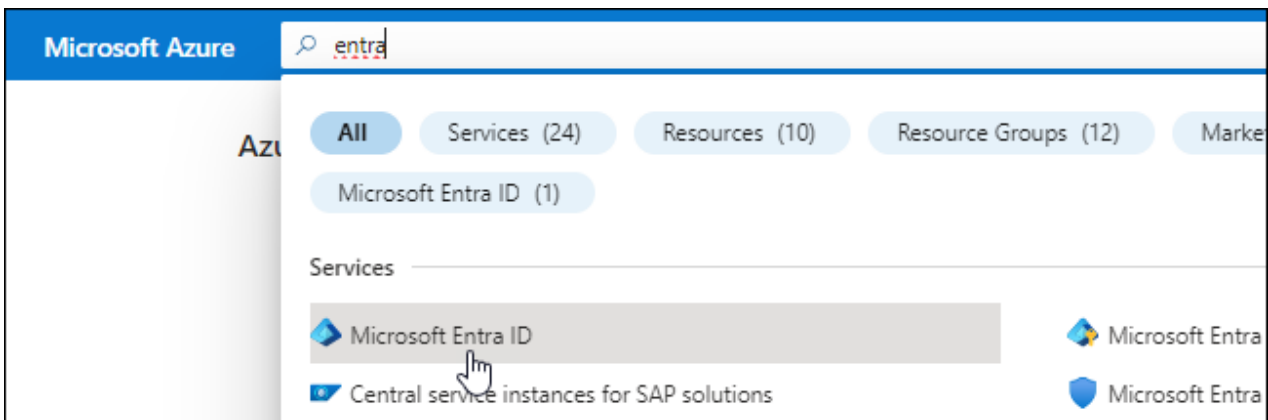
在 Microsoft Entra ID 中建立並設定服務主體，並取得控制台代理程式所需的 Azure 憑證。

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。

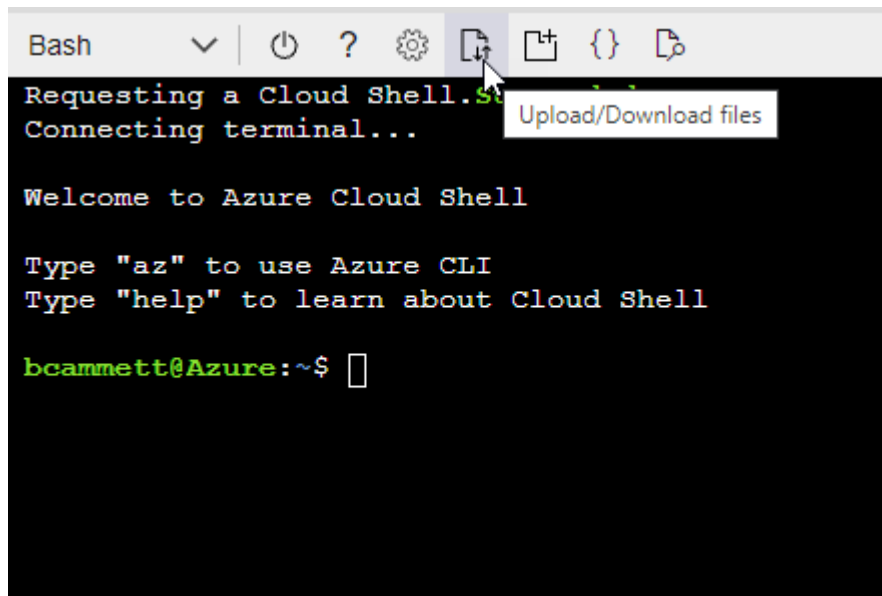
例子

```
"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
```

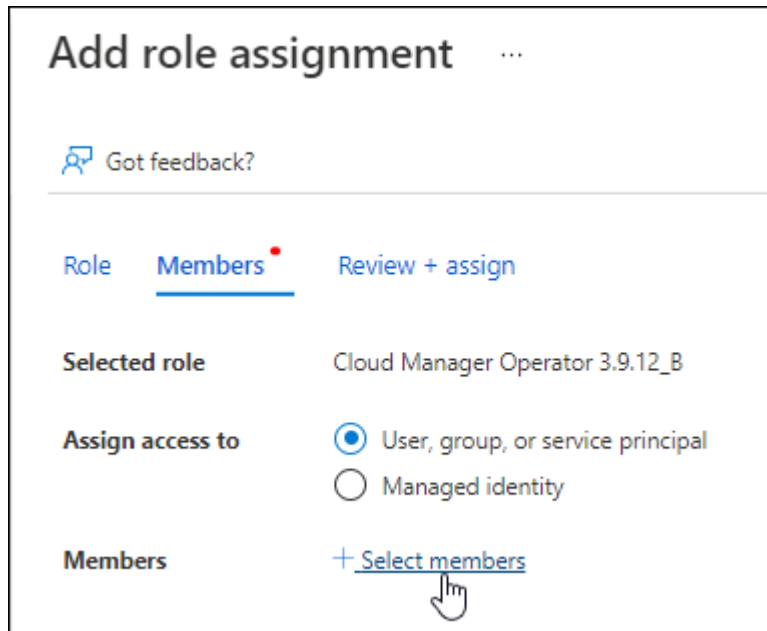
現在您應該有一個名為「控制台操作員」的自訂角色，可以將其指派給控制台代理虛擬機器。

2. 將應用程式指派給角色：

- 從 Azure 入口網站開啟 **Subscriptions** 服務。
- 選擇訂閱。
- 選擇“存取控制 (IAM)”>“新增”>“新增角色分配”。
- 在*角色*標籤中，選擇*控制台操作員*角色並選擇*下一步*。

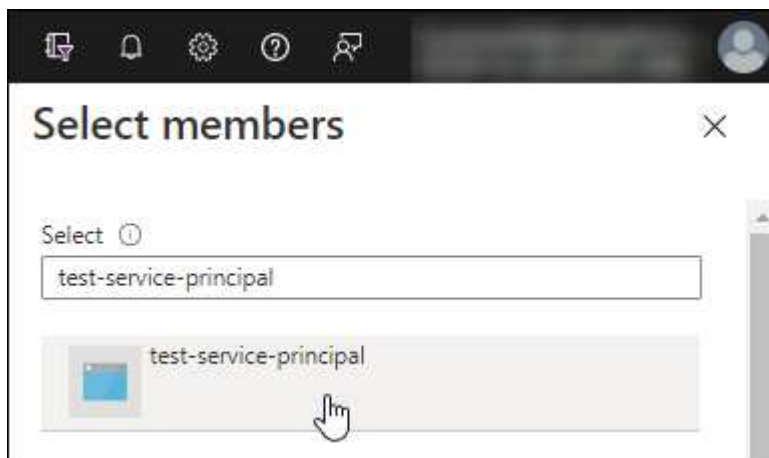
e. 在「成員」標籤中，完成以下步驟：

- 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」。

Request API permissions

Select an API

Microsoft APIs **APIs my organization uses** My APIs

Commonly used Microsoft APIs

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



**Azure Batch**
Schedule large-scale parallel and HPC applications in the cloud

**Azure Data Catalog**
Programmatic access to Data Catalog resources to register, annotate and search data assets

**Azure Data Explorer**
Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

**Azure Data Lake**
Access to storage and compute for big data analytic scenarios

**Azure DevOps**
Integrate with Azure DevOps and Azure DevOps server

**Azure Import/Export**
Programmatic control of import/export jobs

**Azure Key Vault**
Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

**Azure Rights Management Services**
Allow validated users to read and write protected content

**Azure Service Management**
Programmatic access to much of the functionality available through the Azure portal

**Azure Storage**
Secure, massively scalable object and data lake storage for unstructured and semi-structured data

**Customer Insights**
Create profile and interaction models for your products

**Data Export Service for Microsoft Dynamics 365**
Export data from Microsoft Dynamics CRM organization to an external destination

4. 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*。

Request API permissions

[< All APIs](#)



Azure Service Management

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

What type of permissions does your application require?

Delegated permissions

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

Application permissions

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

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED

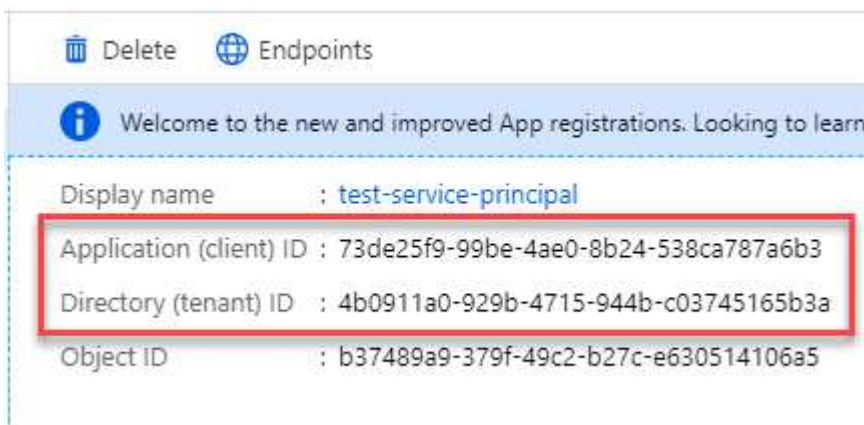


user_impersonation

Access Azure Service Management as organization users (preview)

取得應用程式的應用程式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。

Client secrets

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

[+ New client secret](#)

DESCRIPTION	EXPIRES	VALUE	Copy to clipboard
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA	

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：設定網路

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。

連接到目標網路

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。 - 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。

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：

- 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](#)"。
- 從 Google Cloud 啟動雲殼。
- 上傳包含所需權限的 YAML 檔案。
- 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：

- 從 IAM 和管理服務中，選擇 服務帳戶 > 建立服務帳戶。
- 輸入服務帳戶詳細資料並選擇*建立並繼續*。
- 選擇您剛剛建立的角色。
- 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。

- 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。
- 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 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：
 - 雲端基礎架構管理器 API
 - 雲端部署管理器 V2 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
- 雲端金鑰管理服務 (KMS) API

(僅當您打算將NetApp Backup and Recovery與客戶管理加密金鑰 (CMEK) 結合使用時才需要)

"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：設定網路

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。

連接到目標網路

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。 - 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。

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.preview.get
- config.preview.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 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：

- 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。
- 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。
- 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

- 在您的專案中啟用以下 Google Cloud API：
 - 雲端基礎架構管理器 API
 - 雲端部署管理器 V2 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
- 雲端金鑰管理服務 (KMS) API

(僅當您打算將NetApp Backup and Recovery與客戶管理加密金鑰 (CMEK) 結合使用時才需要)

"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 • 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

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://bluepinfraprod.eastus2.data.azurecr.io \ https://bluepinfraprod.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。

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：

- 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](#)"。
- 從 Google Cloud 啟動雲殼。
- 上傳包含所需權限的 YAML 檔案。
- 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：

- 從 IAM 和管理服務中，選擇 服務帳戶 > 建立服務帳戶。
- 輸入服務帳戶詳細資料並選擇*建立並繼續*。
- 選擇您剛剛建立的角色。
- 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。

- 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。
- 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 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：
 - 雲端基礎架構管理器 API
 - 雲端部署管理器 V2 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
- 雲端金鑰管理服務 (KMS) API

(僅當您打算將NetApp Backup and Recovery與客戶管理加密金鑰 (CMEK) 結合使用時才需要)

"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 • 僅限英文版本。 • 主機必須在 Red Hat 訂閱管理中註冊。如果未註冊，主機將無法在代理安裝期間存取儲存庫來更新所需的第三方軟體。	4.0.0 或更高版本，控制台處於標準模式或受限模式	Podman 版本 5.4.0，podman-compose 版本 1.5.0。 查看 Podman 設定要求 。
在強制模式或寬容模式下受支持		9.1 至 9.4 • 僅限英文版本。 • 主機必須在 Red Hat 訂閱管理中註冊。如果未註冊，主機將無法在代理安裝期間存取儲存庫來更新所需的第三方軟體。	3.9.50 或更高版本，控制台處於標準模式或受限模式	Podman 版本 4.9.4，podman-compose 版本 1.5.0。 查看 Podman 設定要求 。

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 • 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

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。

連接到目標網路

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 控制台準備網路"](#)。

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) : • 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。
\ 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.blueexp.netapp.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.blueexp.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

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。 - 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。

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

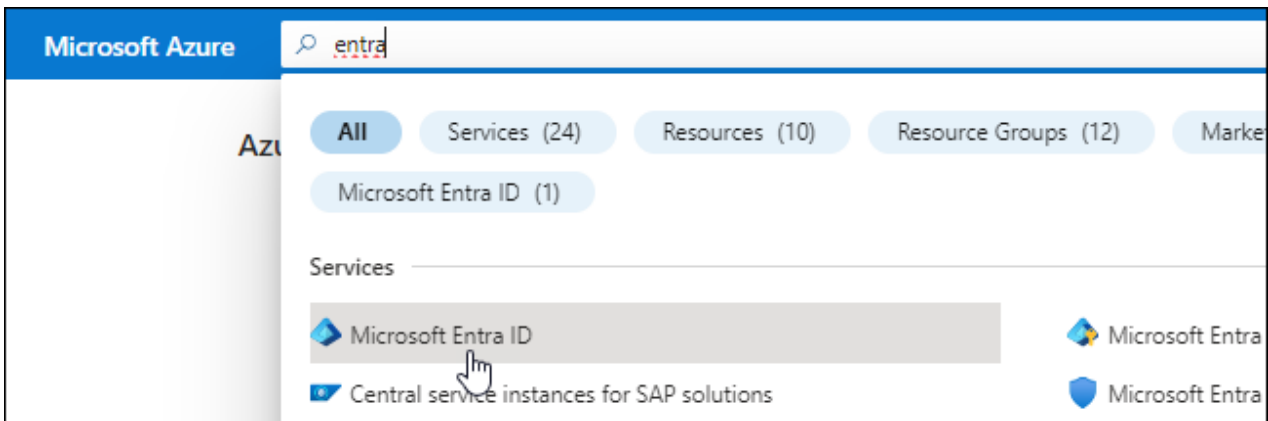
當控制台代理程式安裝在本機時，您需要透過在 Microsoft Entra ID 中設定服務主體並取得控制台代理程式所需的 Azure 憑證來為控制台代理程式提供 Azure 權限。

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。

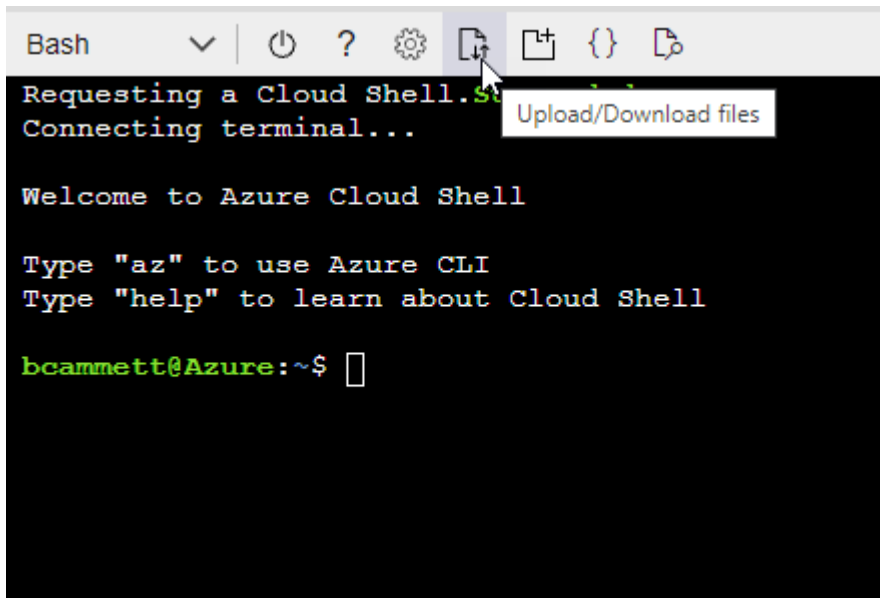
例子

```
"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。



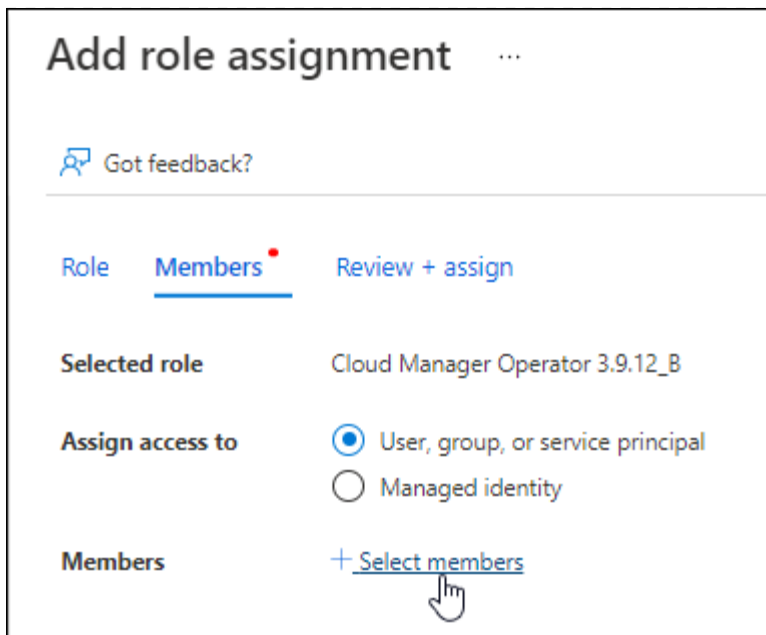
- 使用 Azure CLI 建立自訂角色：

```
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。

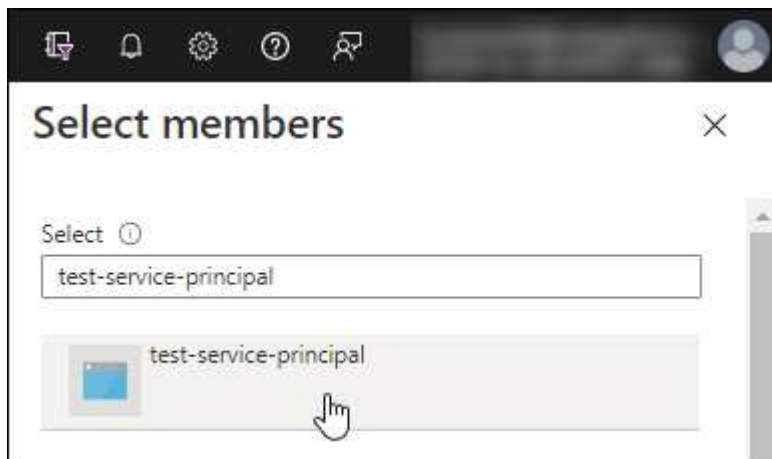
2. 將應用程式指派給角色：

- 從 Azure 入口網站開啟 **Subscriptions** 服務。
- 選擇訂閱。
- 選擇“存取控制 (IAM)”>“新增”>“新增角色分配”。
- 在*角色*標籤中，選擇*控制台操作員*角色並選擇*下一步*。
- 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」。

Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

Microsoft Graph

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



Azure Batch

Schedule large-scale parallel and HPC applications in the cloud

Azure Data Catalog

Programmatic access to Data Catalog resources to register, annotate and search data assets

Azure Data Explorer

Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

Azure Data Lake

Access to storage and compute for big data analytic scenarios

Azure DevOps

Integrate with Azure DevOps and Azure DevOps server

Azure Import/Export

Programmatic control of import/export jobs

Azure Key Vault

Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

Azure Rights Management Services

Allow validated users to read and write protected content

Azure Service Management

Programmatic access to much of the functionality available through the Azure portal

Azure Storage

Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Customer Insights

Create profile and interaction models for your products

Data Export Service for Microsoft Dynamics 365

Export data from Microsoft Dynamics CRM organization to an external destination

4. 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*。

Request API permissions

[← All APIs](#)



Azure Service Management

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

What type of permissions does your application require?

Delegated permissions

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

Application permissions

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

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED

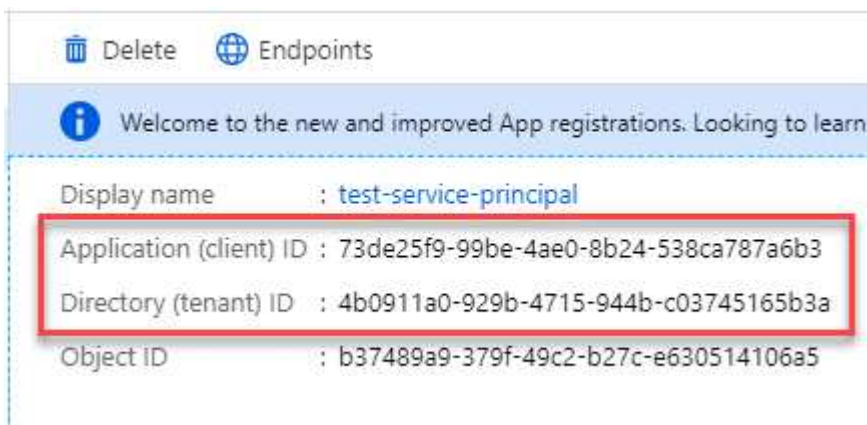


user_impersonation

Access Azure Service Management as organization users (preview)

取得應用程式的應用程式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。

Client secrets

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

[+ New client secret](#)

DESCRIPTION	EXPIRES	VALUE	
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA	

Copy to clipboard

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。

連接到目標網路

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 控制台準備網路"](#)。

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) : • 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。
\ 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.blueexp.netapp.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.blueexp.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

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。 - 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。

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。

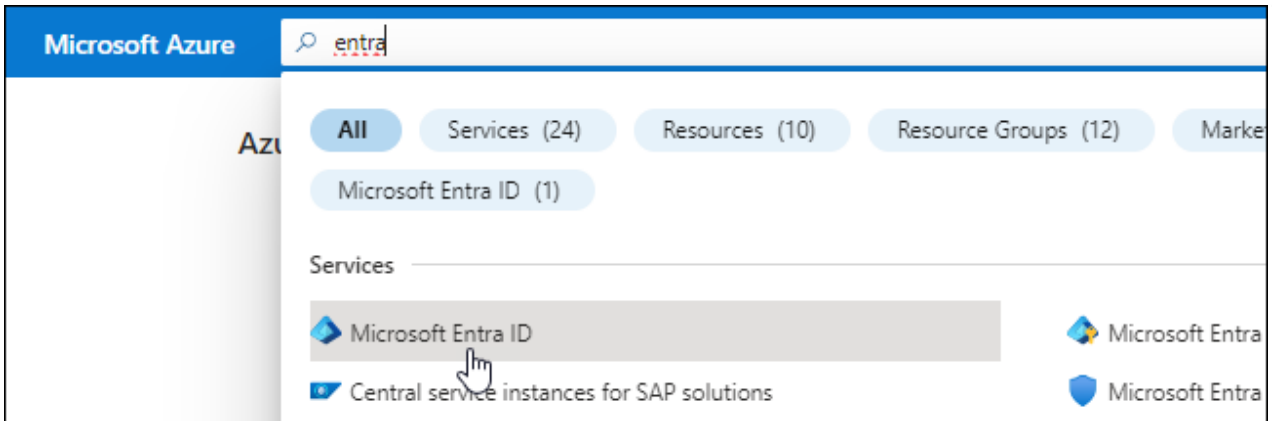
Azure

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。

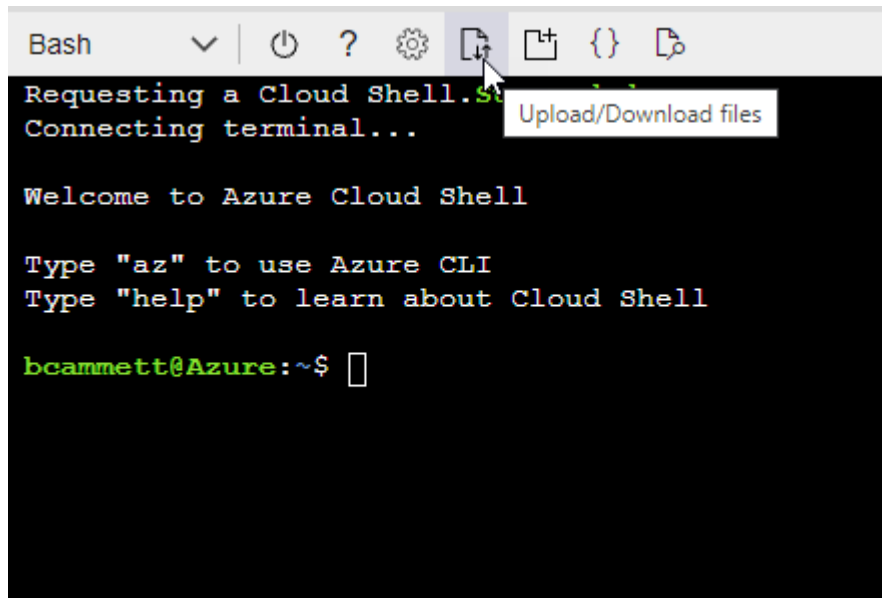
例子

```
"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。



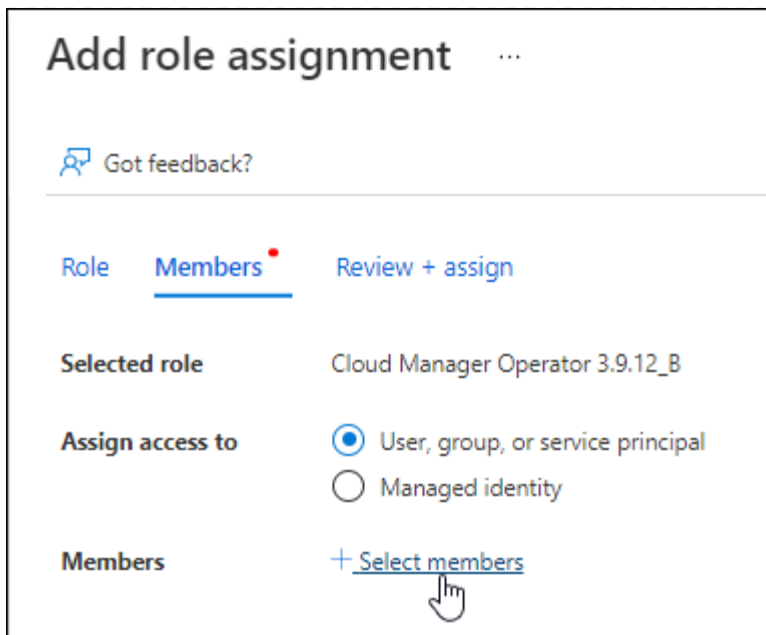
- 使用 Azure CLI 建立自訂角色：

```
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。

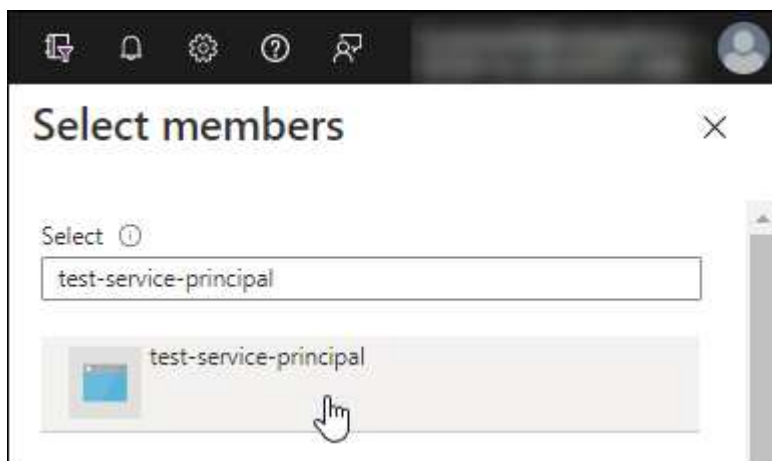
2. 將應用程式指派給角色：

- 從 Azure 入口網站開啟 **Subscriptions** 服務。
- 選擇訂閱。
- 選擇“存取控制 (IAM)”>“新增”>“新增角色分配”。
- 在*角色*標籤中，選擇*控制台操作員*角色並選擇*下一步*。
- 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」。

Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

Microsoft Graph

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



Azure Batch

Schedule large-scale parallel and HPC applications in the cloud

Azure Data Catalog

Programmatic access to Data Catalog resources to register, annotate and search data assets

Azure Data Explorer

Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

Azure Data Lake

Access to storage and compute for big data analytic scenarios

Azure DevOps

Integrate with Azure DevOps and Azure DevOps server

Azure Import/Export

Programmatic control of import/export jobs

Azure Key Vault

Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

Azure Rights Management Services

Allow validated users to read and write protected content

Azure Service Management

Programmatic access to much of the functionality available through the Azure portal

Azure Storage

Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Customer Insights

Create profile and interaction models for your products

Data Export Service for Microsoft Dynamics 365

Export data from Microsoft Dynamics CRM organization to an external destination

4. 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*。

Request API permissions

[← All APIs](#)



Azure Service Management

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

What type of permissions does your application require?

Delegated permissions

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

Application permissions

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

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED

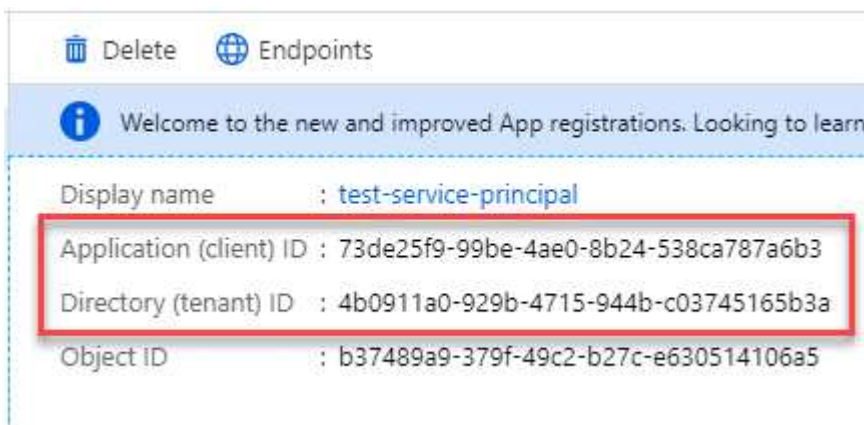


user_impersonation

Access Azure Service Management as organization users (preview)

取得應用程式的應用程式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。

Client secrets

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

[+ New client secret](#)

DESCRIPTION	EXPIRES	VALUE	Copy to clipboard
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA	

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 • 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。 控制台顯示憑證簽署要求。 b. 使用 CSR 向 CA 提交 SSL 憑證請求。 憑證必須使用隱私增強郵件 (PEM) Base-64 編碼的 X.509 格式。 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*。 b. 載入憑證檔案和私鑰，然後選擇*安裝*。 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：

HTTPS Certificate

Change Certificate

✔ HTTPS Setup is active

Expiration: Aug 15, 2029 10:09:01 am

Issuer: C=IL, ST=Israel, L=Tel Aviv, O=NetApp, OU=Dev, CN= Localhost, E=Admin@netapp.com

Subject: C=IL, ST=Israel, L=Tel Aviv, O=NetApp, OU=Dev, CN= Localhost, E=Admin@netapp.com

Certificate:

View CSR

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。 • 驗證所有容器是否正在運作。 • 確保您的防火牆允許存取連接埠 8888 的服務。 • 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。 • 驗證 Service Manager 服務 • 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。 • 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。

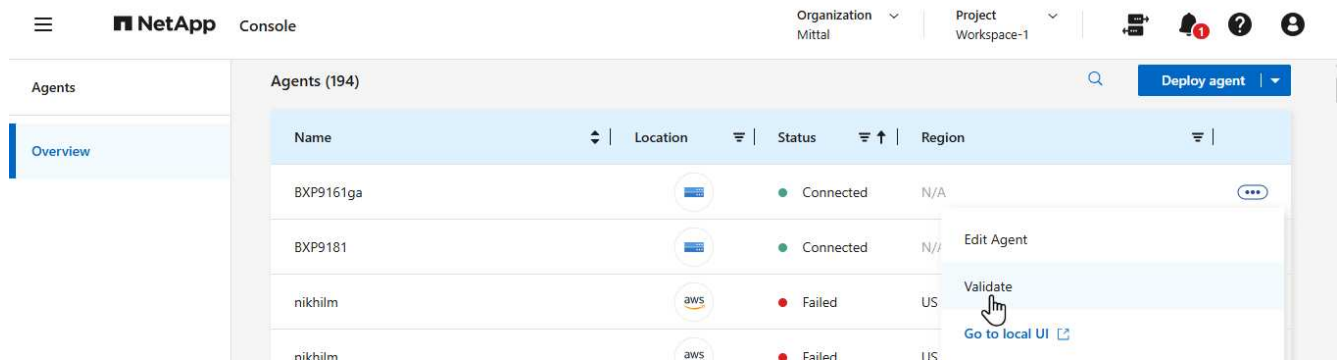
您也可以使用代理維護控制台執行設定檢查。["了解更多關於使用 config-checker validate 命令的資訊。"](#)



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

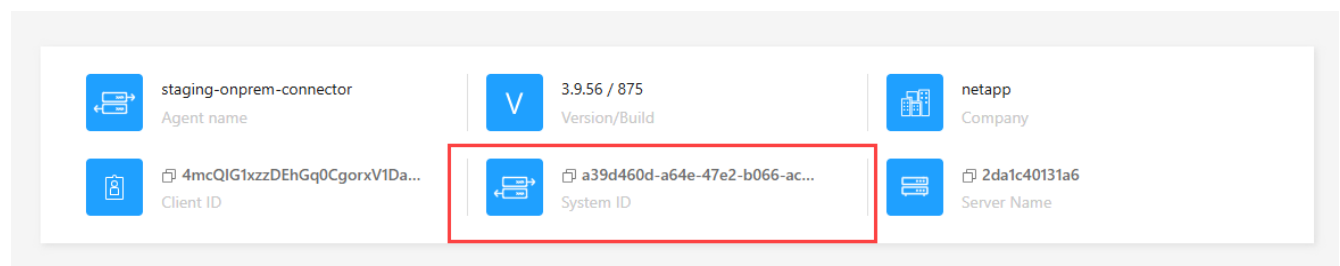
為了幫助您入門，您可能需要控制台代理的系統 ID。此 ID 通常用於許可和故障排除目的。

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

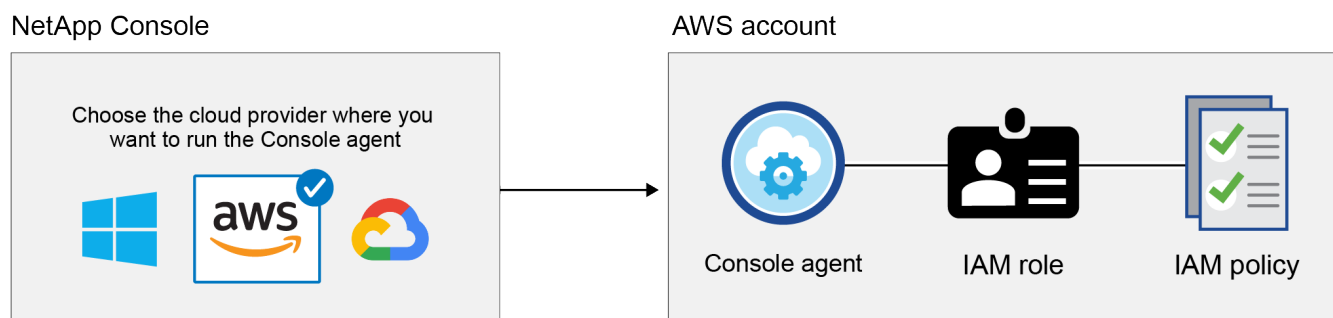
了解NetApp Console中的 **AWS** 憑證和權限

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。

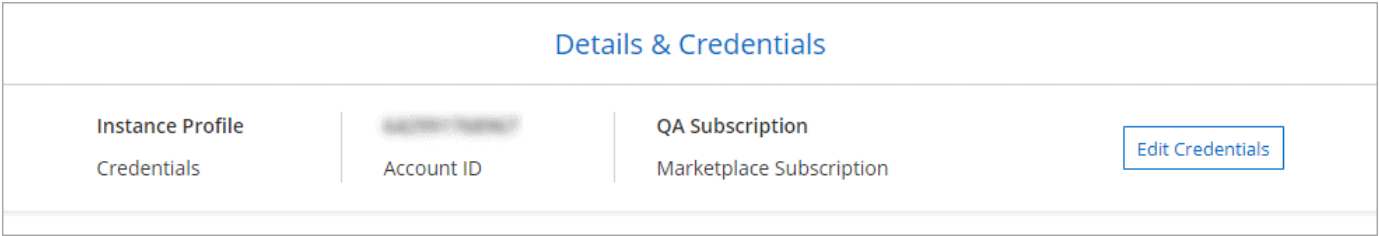
初始 AWS 憑證

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

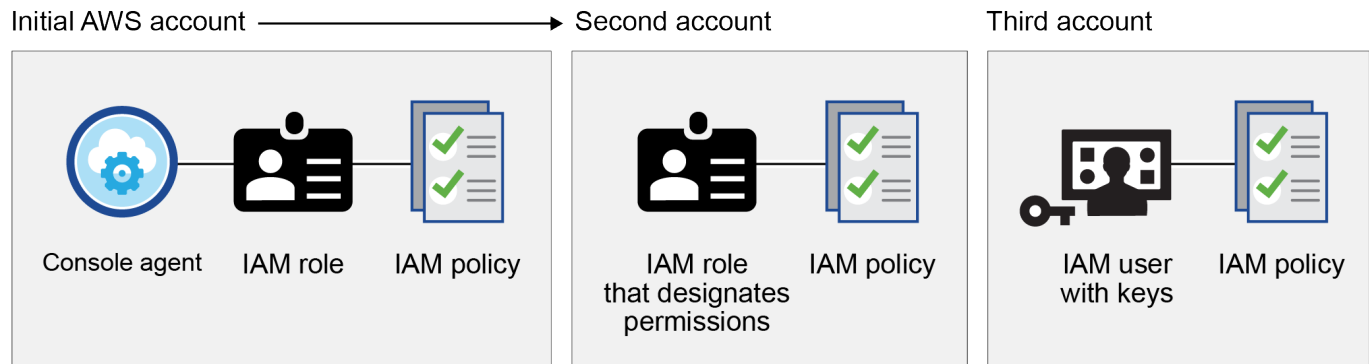
在下列情況下，您可能會為控制台新增其他 AWS 憑證：

- 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：

Edit Credentials & Add Subscription

Associate Subscription to Credentials ⓘ

Credentials

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

+ Add Subscription

Apply Cancel

["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”。

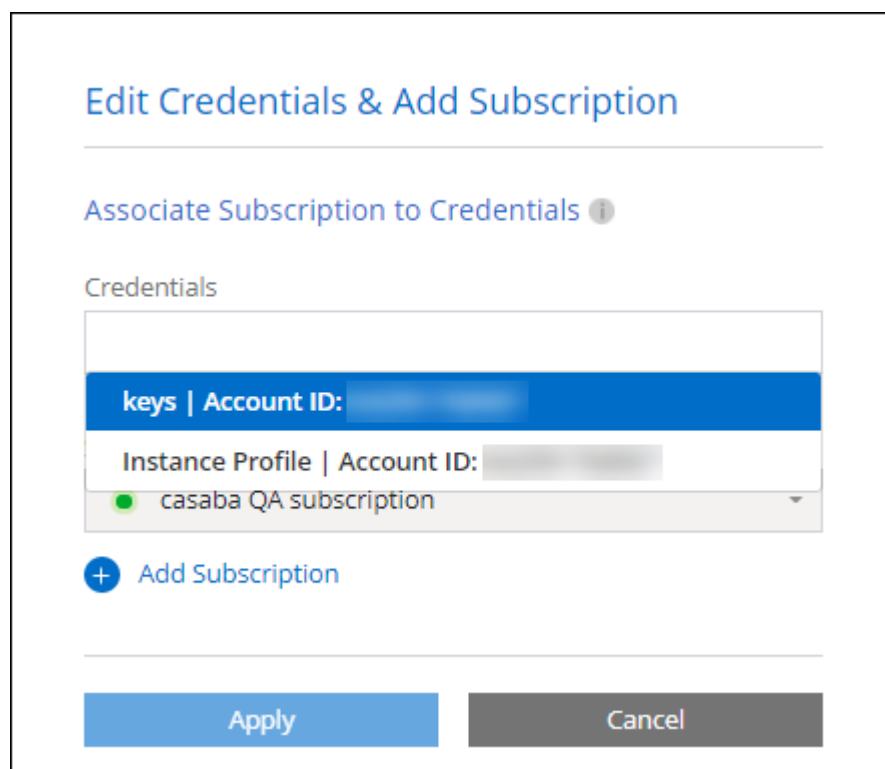
3. 在*組織憑證*頁面上，選擇*新增憑證*並按照精靈中的步驟進行操作。
 - a. 憑證位置：選擇*Amazon Web Services > 代理*。
 - b. 定義憑證：提供受信任的 IAM 角色的 ARN（Amazon 資源名稱），或輸入 AWS 存取金鑰和金鑰。
 - c. 市場訂閱：透過立即訂閱或選擇現有訂閱將市場訂閱與這些憑證關聯。

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。



The screenshot shows a modal window titled "Edit Credentials & Add Subscription". Inside, there's a section "Associate Subscription to Credentials" with a help icon. Below that, a table lists credentials. The first row is highlighted in blue and shows "keys | Account ID: [redacted]". The second row shows "Instance Profile | Account ID: [redacted]". Below the table is a dropdown menu with "casaba QA subscription" selected. At the bottom left is a "+ Add Subscription" button, and at the bottom right are "Apply" and "Cancel" buttons.

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。

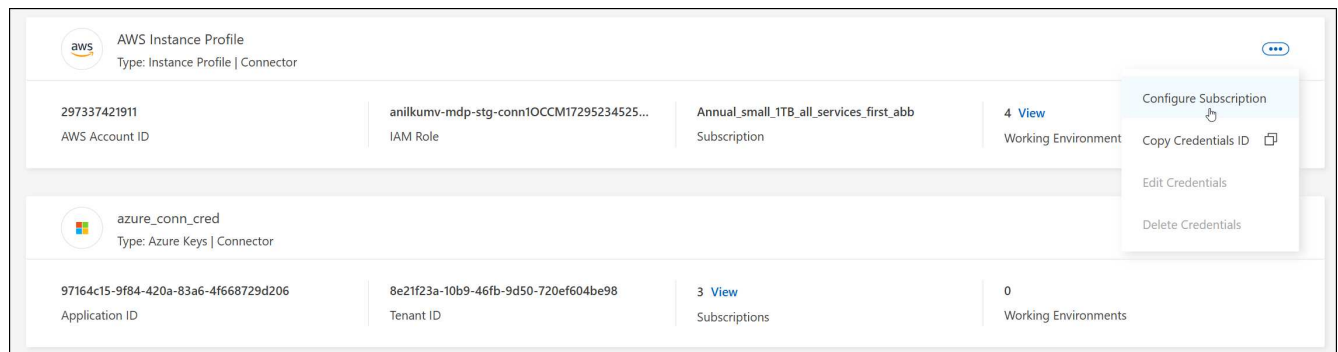
開始之前

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"](#)

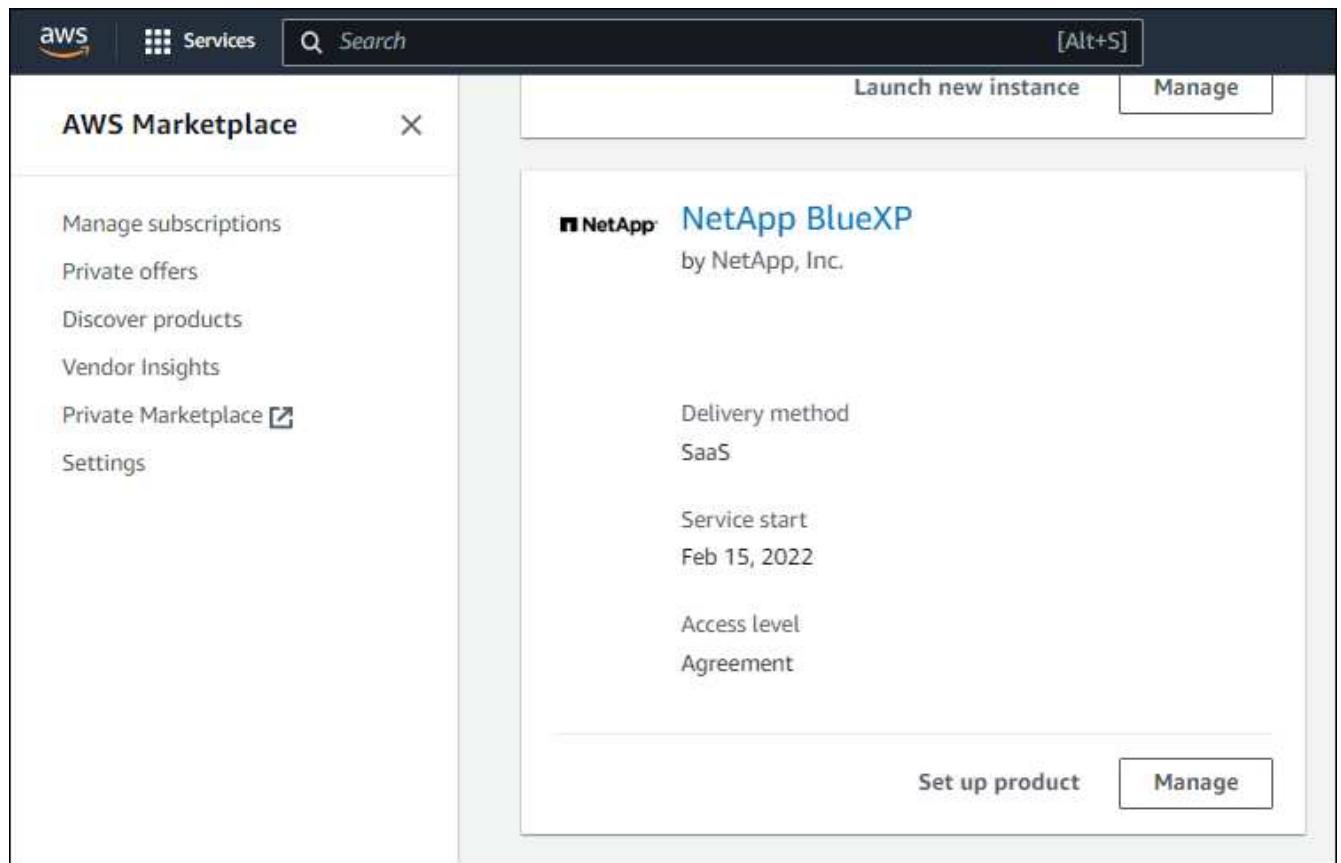
如果您從 AWS Marketplace 訂閱了NetApp Intelligent Services，但錯過了將訂閱與您的帳戶關聯的步驟，請按照以下步驟操作。

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。

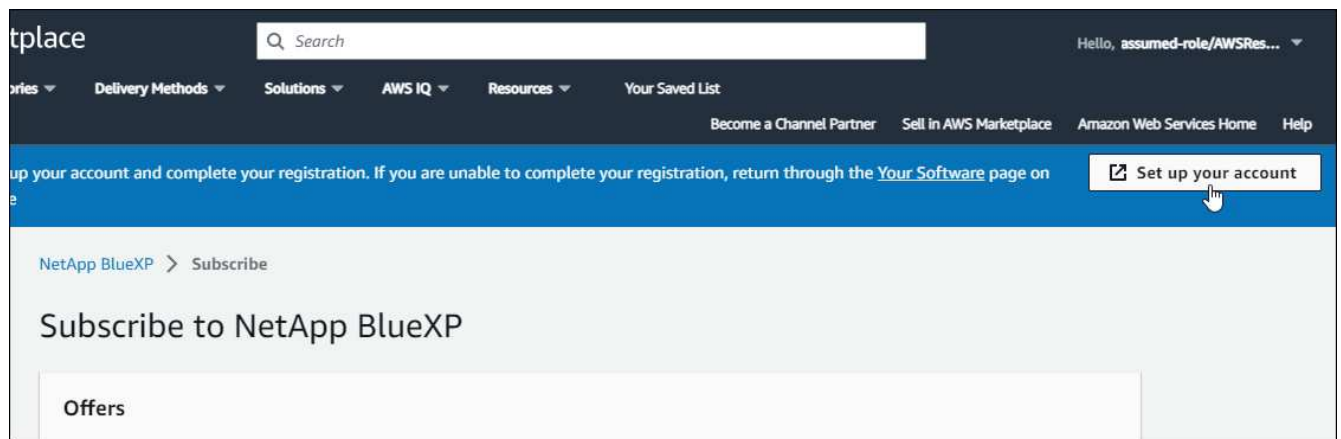
2. 登入 AWS 主控台並導覽至 **AWS Marketplace** 訂閱。
3. 尋找訂閱。



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。

Subscription Assignment [X]

✓ Your subscription to BlueXP / Cloud Volumes ONTAP from the AWS Marketplace was created successfully.

Subscription name i
PayAsYouGo

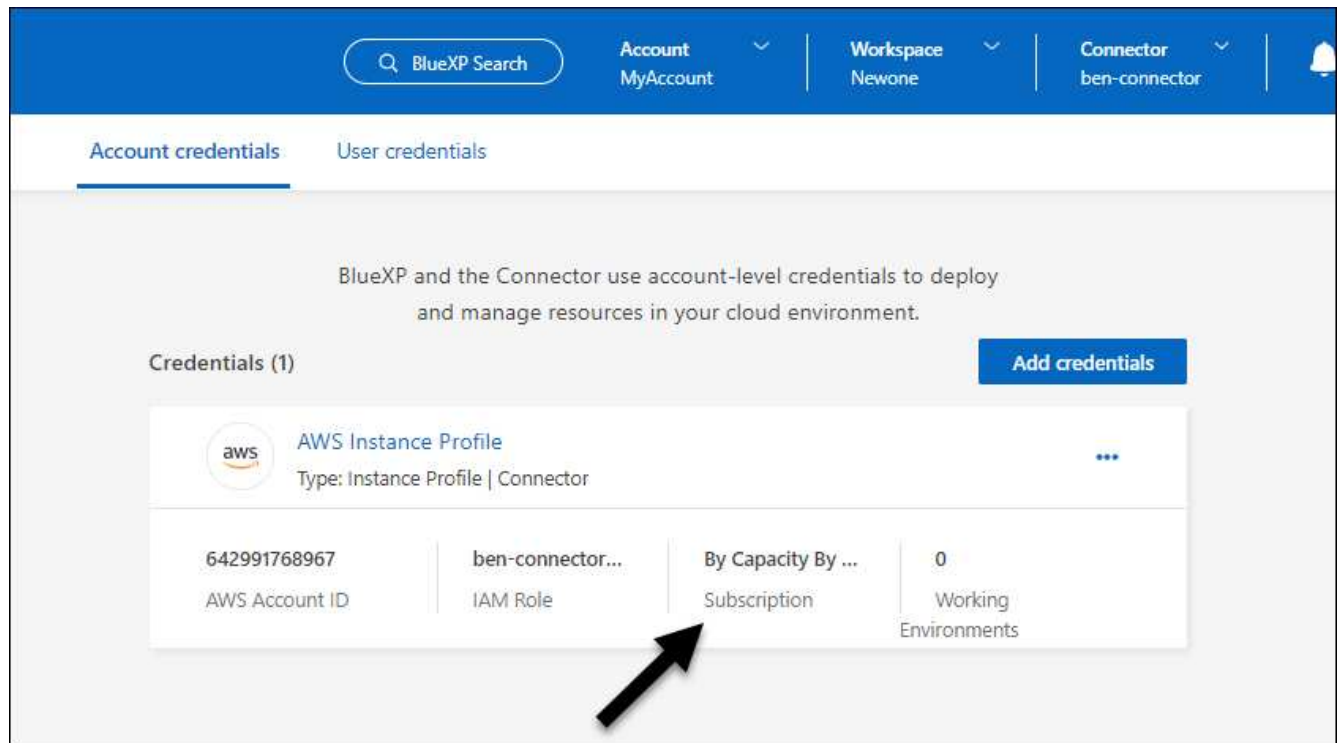
Select the NetApp accounts that you'd like to associate this subscription with. i
You can automatically replace the existing subscription for one account with this new subscription.

NetApp account	Replace existing subscription
☒ cloudTiering_undefined	☐
☒ CS-HhewH	☐
☒ benAccount	☒

Save

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

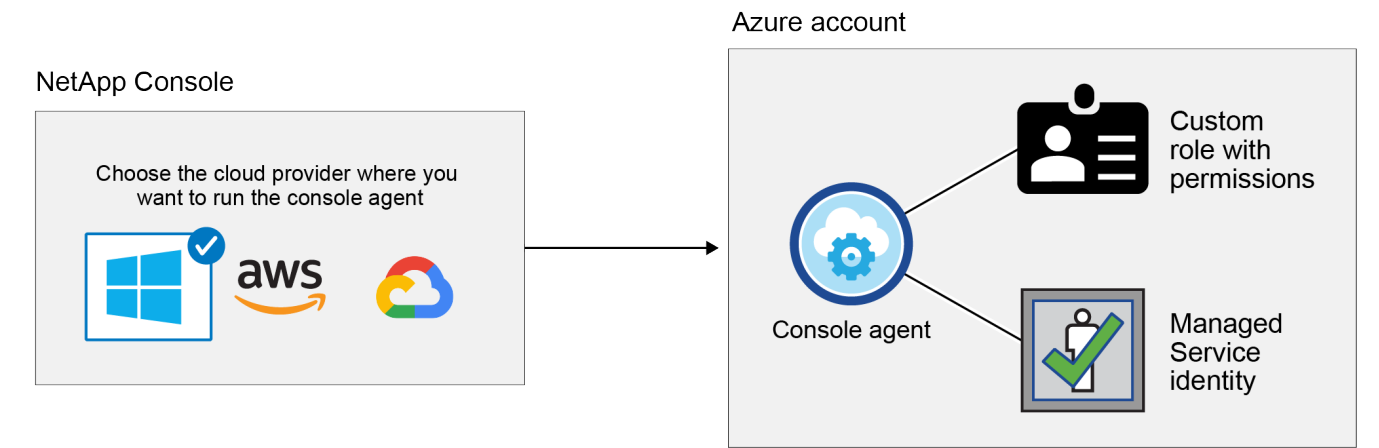
了解NetApp Console中的 Azure 憑證和權限

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：

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

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。

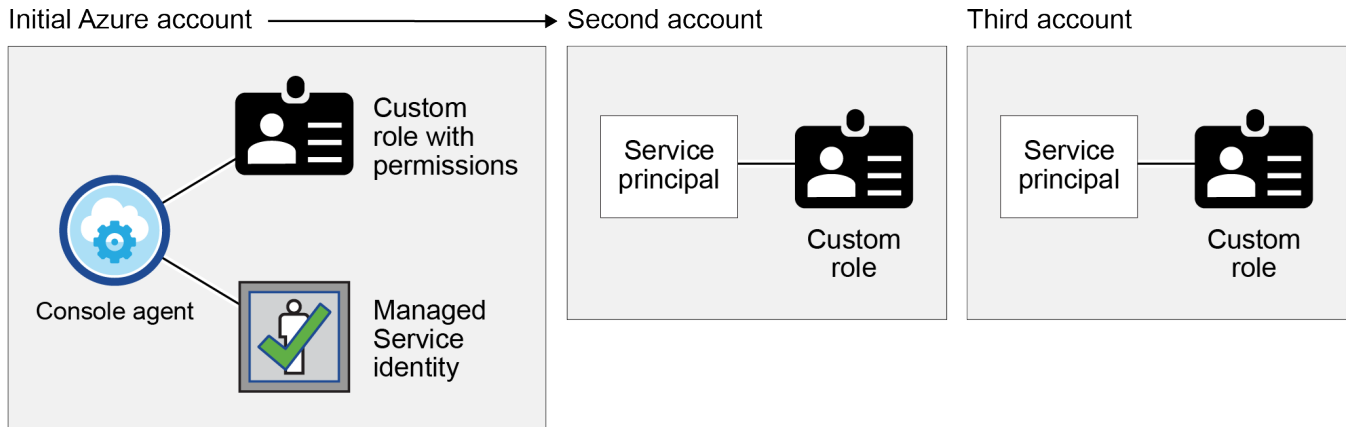
託管識別碼的其他 Azure 訂閱

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

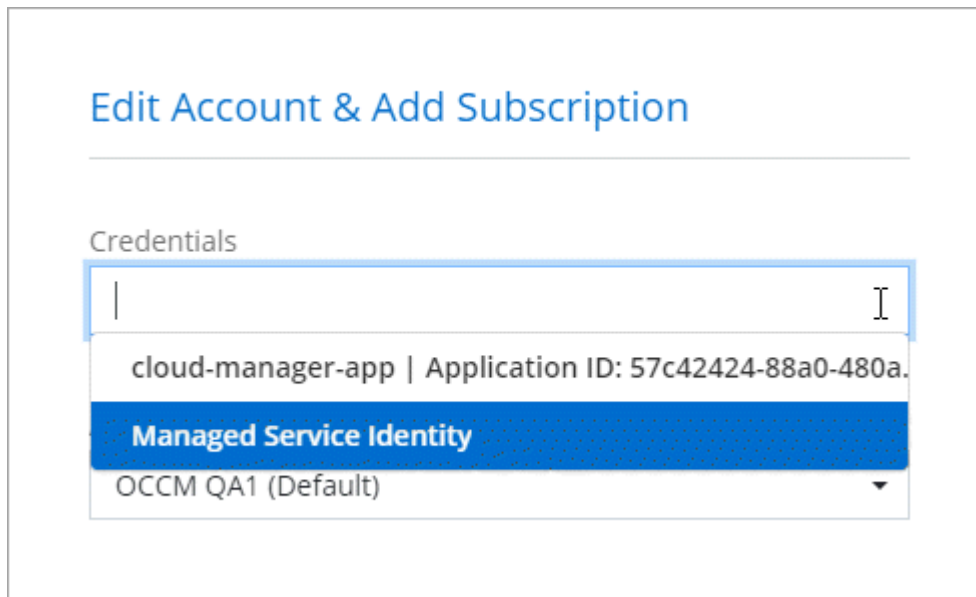
如果要在控制台中使用不同的 Azure 憑證，則必須透過以下方式授予所需的權限"在 Microsoft Entra ID 中建立和

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。



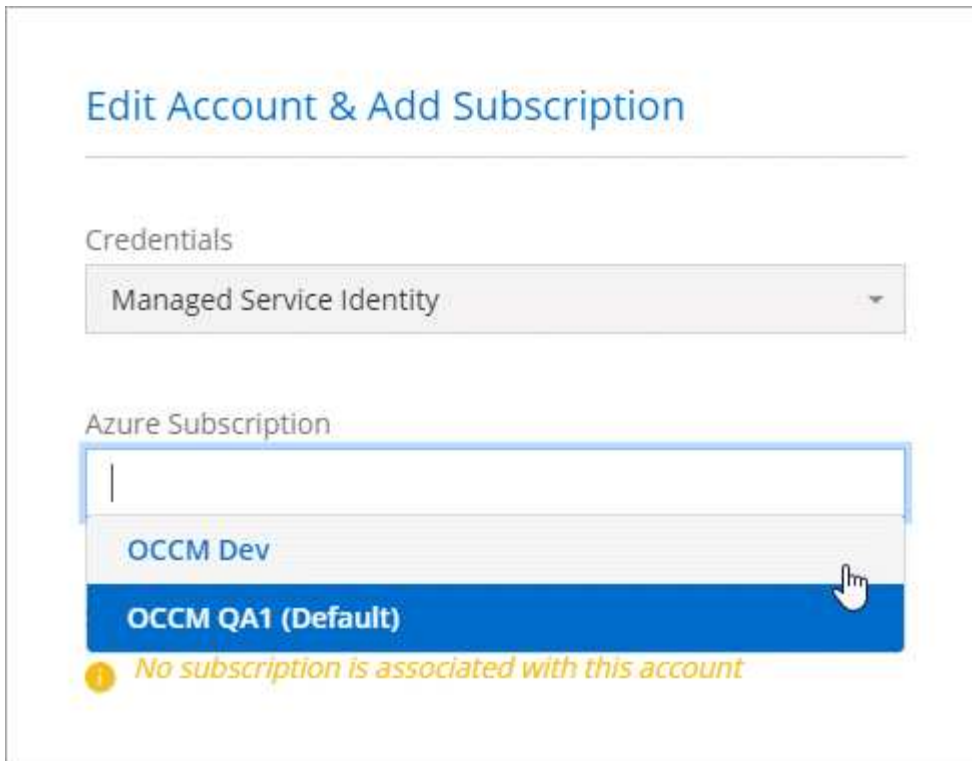
控制台操作員是控制台代理程式策略中提供的預設名稱。如果您為角色選擇了不同的名稱，請選擇該名稱。

- 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"](#)。

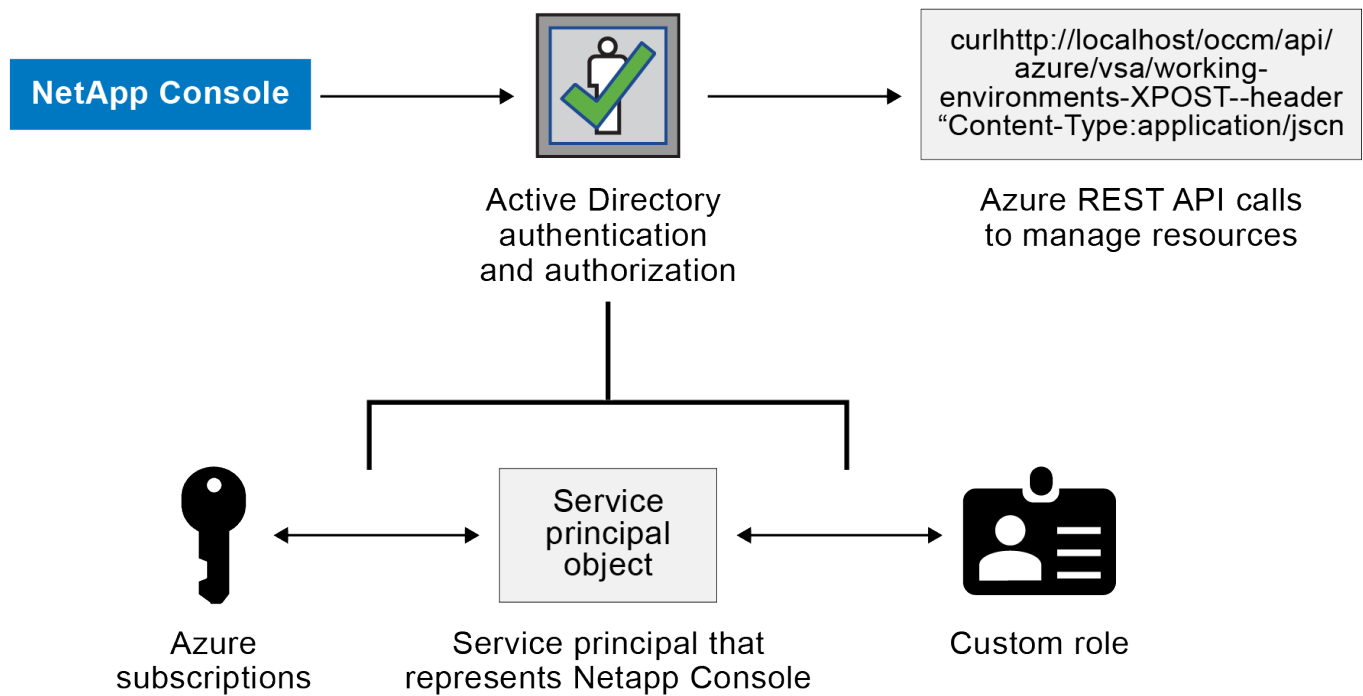
如果您想要使用不同的 Azure 憑證部署Cloud Volumes ONTAP，則必須透過在 Microsoft Entra ID 中為每個 Azure 帳戶建立和設定服務主體來授予所需的權限。然後，您可以將新憑證新增至控制台。

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

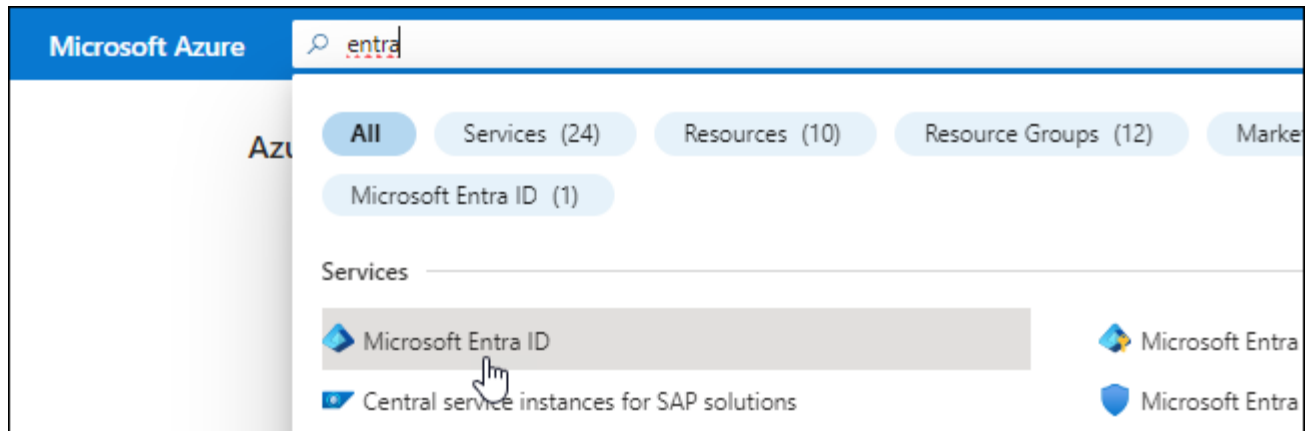
建立控制台可用於基於角色的存取控制的 Microsoft Entra 應用程式和服務主體。

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。

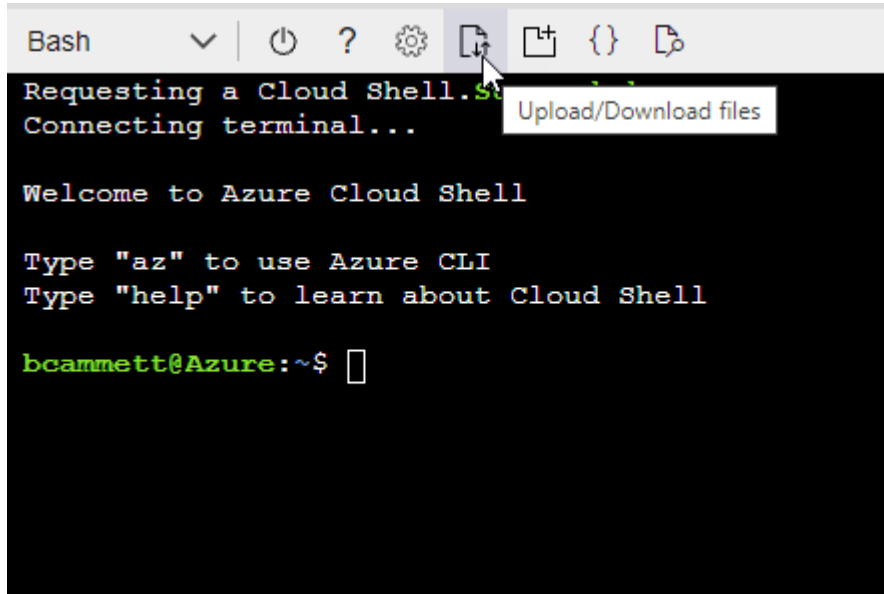
例子

```
"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。



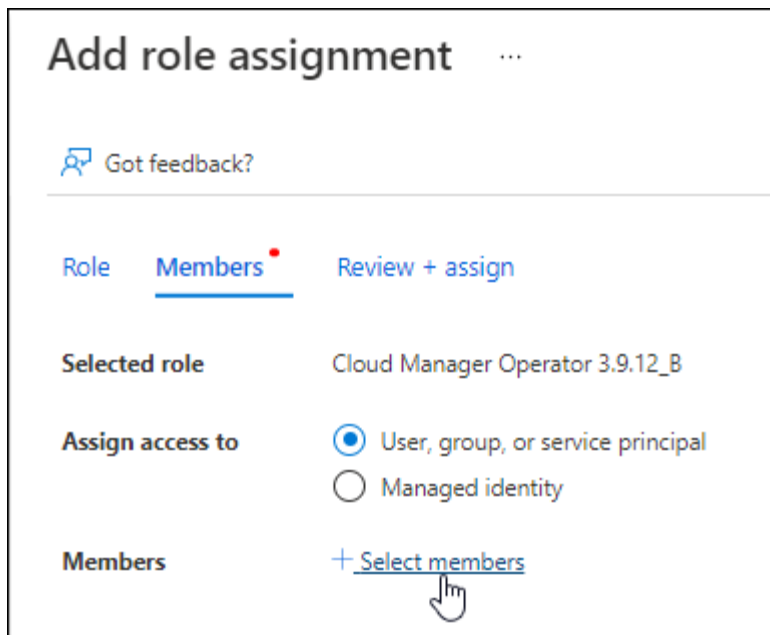
- 使用 Azure CLI 建立自訂角色：

```
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。

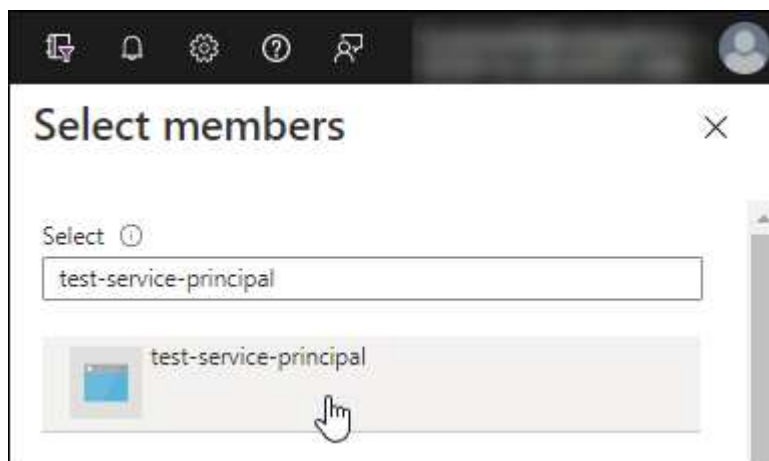
2. 將應用程式指派給角色：

- 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」。

Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

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

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

4. 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*。

Request API permissions

< All APIs



Azure Service Management

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

What type of permissions does your application require?

Delegated permissions

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

Application permissions

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

Select permissions

[expand all](#)

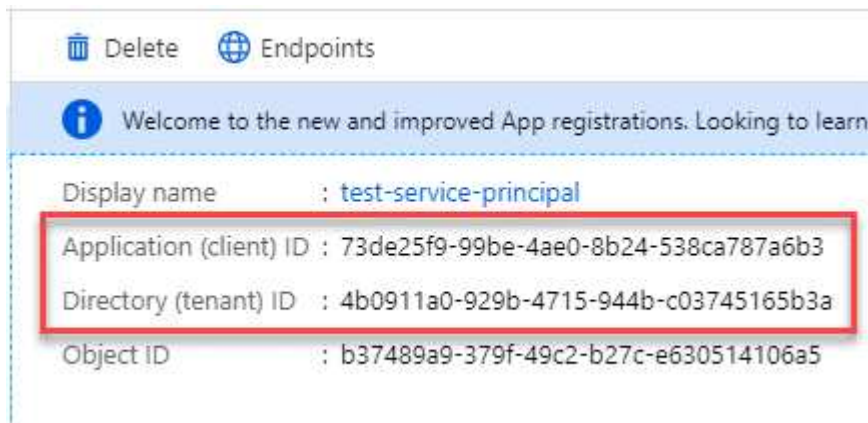
Type to search	
PERMISSION	ADMIN CONSENT REQUIRED
☒ user_impersonation Access Azure Service Management as organization users (preview) ⓘ	-

取得應用程式ID和目錄ID

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。

Client secrets

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

+ New client secret		
DESCRIPTION	EXPIRES	VALUE
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA

Copy to clipboard

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

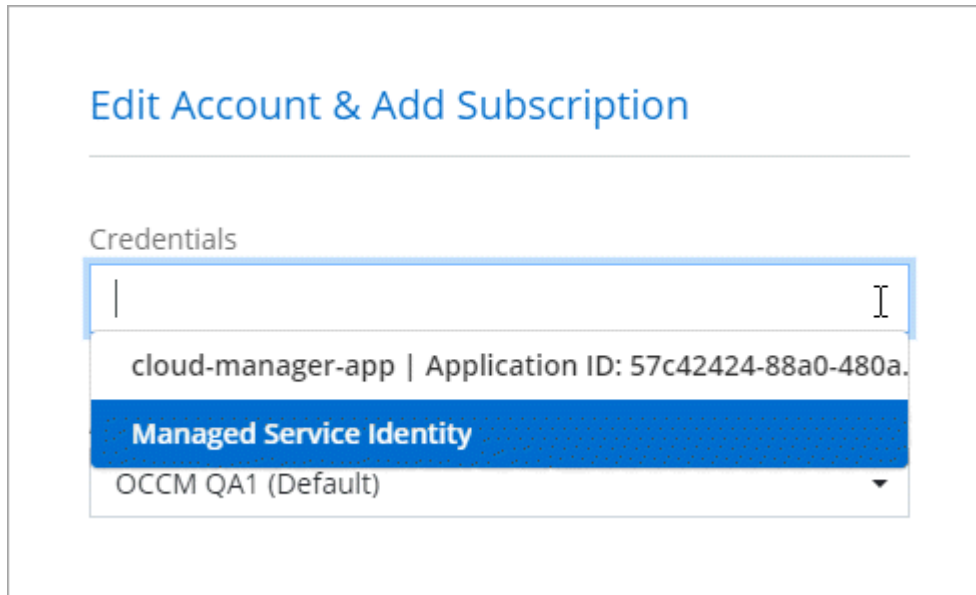
您需要先建立控制台代理，然後才能變更控制台設定。["了解如何建立控制台代理"](#)。

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

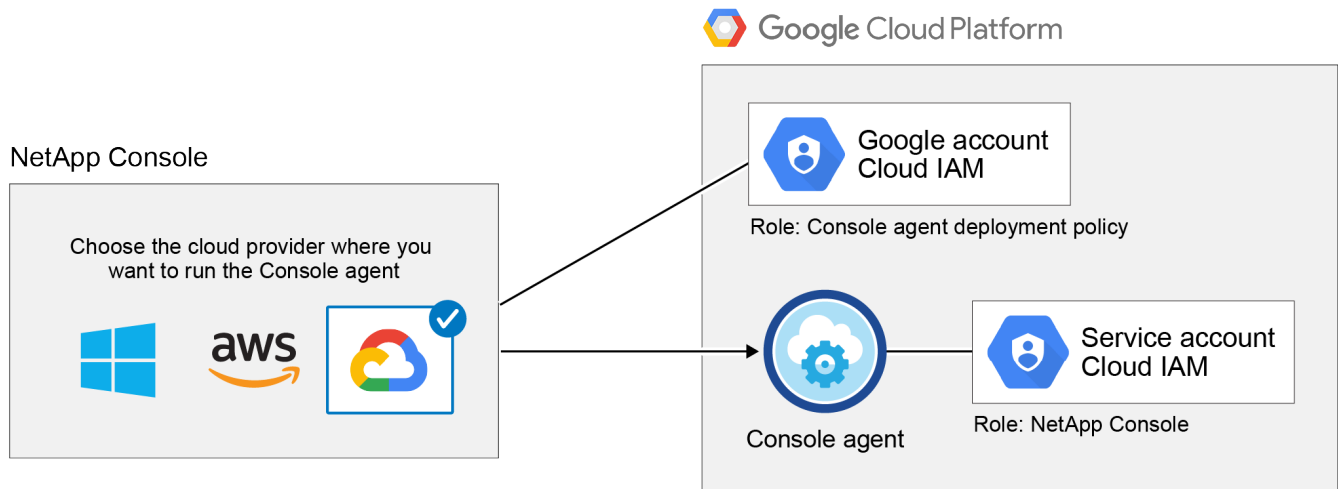
您必須先部署控制台代理，然後才能使用控制台管理 Google Cloud 專案中的資源。代理程式不能在您的場所或

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 服務帳戶建立一組預設憑證。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** 部署的控制台代理權限

NetApp有時會在將控制台代理部署到 Google Cloud 時更新用於該代理程式的服務帳戶所需的權限。

["核實所需的 Google 權限列表"](#)。

使用 Google Cloud 控制台更新指派給服務帳號的 IAM 角色，使其與新的權限集相符。

["Google Cloud 文件：編輯自訂角色"](#)

版權資訊

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

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

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

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

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

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

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

商標資訊

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