開始使用
Cloud Manager 3.7

NetApp
March 25, 2024

目錄

開始使用

部署總覽

在開始之前、您可能想要更深入瞭解部署Cloud Manager和Cloud Volumes ONTAP 解決方案的選項。

Cloud Manager安裝

需要Cloud Manager軟體來部署和管理Cloud Volumes ONTAP 功能。您可以在下列任一位置部署Cloud Manager：

- Amazon Web Services（AWS）
- Microsoft Azure
- Google Cloud Platform

  在Cloud Volumes ONTAP GCP中部署時、Cloud Manager必須位於Google Cloud Platform中。

- IBM Cloud
- 在您自己的網路中

部署Cloud Manager的方式取決於您選擇的位置：

Cloud Manager的位置	如何部署**Cloud Manager**
AWS	1. "從NetApp Cloud Central部署Cloud Manager" （建議） 2. "從AWS Marketplace部署" 3. "在Linux主機上下載並安裝軟體"
AWS C2S	"從AWS Intelligence Community Marketplace部署Cloud Manager"
Azure一般適用地區	1. "從NetApp Cloud Central部署Cloud Manager" （建議） 2. "從Azure Marketplace部署" 3. "在Linux主機上下載並安裝軟體"
Azure政府	"從Azure美國政府市場部署Cloud Manager"
Azure德國	"在Linux主機上下載並安裝軟體"
Google Cloud Platform	1. "從NetApp Cloud Central部署Cloud Manager" （建議） 2. "在Linux主機上下載並安裝軟體" 您無法從GCP Marketplace在Google Cloud中部署Cloud Manager
IBM Cloud	"在Linux主機上下載並安裝軟體"

Cloud Manager的位置	如何部署Cloud Manager
內部部署網路	"在Linux主機上下載並安裝軟體"

Cloud Manager設定

您可能想在安裝Cloud Manager之後執行其他設定、例如新增其他雲端供應商帳戶、安裝HTTPS憑證等。

- "設定Cloud Central帳戶"
- "將AWS帳戶新增至Cloud Manager"
- "將Azure帳戶新增至Cloud Manager"
- "安裝 HTTPS 憑證"
- "設定 AWS KMS"

部署Cloud Volumes ONTAP

在Cloud Manager啟動並開始運作之後、您可以開始在Cloud Volumes ONTAP 雲端供應商部署功能。

"AWS快速入門"、 "Azure入門"和 "GCP入門" 提供快速Cloud Volumes ONTAP 執行和升級的指示。如需其他說明、請參閱下列內容：

- "支援Cloud Volumes ONTAP AWS中的支援的支援組態"
- "Azure支援的支援功能組態Cloud Volumes ONTAP"
- "支援的GCP中的VMWare 9.7組態Cloud Volumes ONTAP"
- "規劃組態"
- "在 Cloud Volumes ONTAP AWS 中啟動"
- "在 Cloud Volumes ONTAP Azure 中啟動"
- "在 Cloud Volumes ONTAP GCP 中啟動"

開始使用Cloud Volumes ONTAP AWS的功能

設定AWS、Cloud Volumes ONTAP 然後從NetApp Cloud Central啟動Cloud Manager軟體、即可開始使用此功能。您Cloud Volumes ONTAP 在AWS中啟動的第一個版本為免費試用30天。

1 設定您的網路

1. 啟用從目標VPC的傳出網際網路存取、讓Cloud Manager和Cloud Volumes ONTAP 支援中心能夠連絡多個端點。

   這個步驟很重要、因為Cloud Manager Cloud Volumes ONTAP 無法在沒有外傳網際網路存取的情況下部署不穩定功能。如果您需要限制傳出連線、請參閱的端點清單 "Cloud Manager" 和 "Cloud Volumes ONTAP"。

2. 設定 S3 服務的 VPC 端點。

   如果您想要將冷資料從 Cloud Volumes ONTAP 不願儲存到低成本物件儲存設備、則需要 VPC 端點。

2 提供必要的**AWS**權限

當您從NetApp Cloud Central部署Cloud Manager時、您需要使用具有部署執行個體權限的AWS帳戶。

1. 前往AWS IAM主控台、然後複製並貼上的內容來建立原則 "適用於AWS的NetApp Cloud Central原則"。
2. 將原則附加至IAM使用者。

3 從**AWS Marketplace**訂閱

"從AWS Marketplace訂閱Cloud Manager" 確保在免費試用Cloud Volumes ONTAP 完VMware後、服務不會中斷。您將會從這項訂閱中、針對Cloud Volumes ONTAP 您所建立的每個功能、以及您啟用的每個附加功能、收取費用。

如果您是Cloud Volumes ONTAP 透過自帶授權（BYOL）來啟動 "然後您需要在AWS Marketplace訂閱該產品項目"。

4 從**NetApp Cloud Central**啟動**Cloud Manager**

需要Cloud Manager軟體來部署和管理Cloud Volumes ONTAP 功能。從啟動Cloud Manager執行個體只需幾分鐘的時間 "Cloud Central"。

5 使用 **Cloud Manager** 啟動 **Cloud Volumes ONTAP**

Cloud Manager準備好之後、只要按一下「Create（建立）」、選取您要啟動的系統類型、然後完成精靈中的步驟。25分鐘後、您的第一個Cloud Volumes ONTAP 作業系統應該會啟動並開始運作。

觀看下列影片、瞭解這些步驟：

► https://docs.netapp.com/zh-tw/occm37//media/video_getting_started_aws.mp4 *(video)*

相關連結

- "評估"
- "Cloud Manager的網路需求"
- "AWS 的網路需求 Cloud Volumes ONTAP"
- "AWS 的安全群組規則"
- "將AWS帳戶新增至Cloud Manager"
- "Cloud Manager 使用 AWS 權限的功能"
- "在 Cloud Volumes ONTAP AWS 中啟動"

- "從AWS Marketplace啟動Cloud Manager"

Azure版的功能入門Cloud Volumes ONTAP

設定Azure、Cloud Volumes ONTAP 然後從NetApp Cloud Central部署Cloud Manager軟體、即可開始使用此功能。可在中部署Cloud Manager的個別指示 "Azure美國政府區域" 和 "Azure德國地區"。

1 設定您的網路

啟用從目標vnet的傳出網際網路存取、讓Cloud Manager和Cloud Volumes ONTAP 支援中心能夠連絡多個端點。

這個步驟很重要、因為Cloud Manager Cloud Volumes ONTAP 無法在沒有外傳網際網路存取的情況下部署不穩定功能。如果您需要限制傳出連線、請參閱的端點清單 "Cloud Manager" 和 "Cloud Volumes ONTAP"。

2 提供必要的**Azure**權限

從NetApp Cloud Central部署Cloud Manager時、您需要使用具備部署Cloud Manager虛擬機器權限的Azure帳戶。

1. 下載 "適用於Azure的NetApp Cloud Central原則"。
2. 若要修改Json檔案、請將Azure訂閱ID新增至「AscignableScopes」欄位。
3. 使用Json檔案在Azure中建立自訂角色、名稱為_Azure Setup AsService_。

   範例：* AZ角色定義建立-角色定義C：\Policy_for_SETUP_as_Service_Azure .json*

4. 從Azure入口網站、將自訂角色指派給將從Cloud Central部署Cloud Manager的使用者。

3 從**NetApp Cloud Central**啟動**Cloud Manager**

需要Cloud Manager軟體來部署和管理Cloud Volumes ONTAP 功能。從啟動Cloud Manager執行個體只需幾分鐘的時間 "Cloud Central"。

4 使用 **Cloud Manager** 啟動 **Cloud Volumes ONTAP**

Cloud Manager準備好之後、只要按一下「Create（建立）」、選取您要部署的系統類型、然後完成精靈中的步驟即可。25分鐘後、您的第一個Cloud Volumes ONTAP 作業系統應該會啟動並開始運作。

相關連結

- "評估"
- "Cloud Manager的網路需求"
- "Azure 的網路需求 Cloud Volumes ONTAP"

- "Azure的安全性群組規則"
- "將Azure帳戶新增至Cloud Manager"
- "Cloud Manager 具備 Azure 權限的功能"
- "在 Cloud Volumes ONTAP Azure 中啟動"
- "從Azure Marketplace啟動Cloud Manager"

在 Google Cloud Platform 中開始 Cloud Volumes ONTAP 使用功能

設定GCP、Cloud Volumes ONTAP 然後從NetApp Cloud Central部署Cloud Manager軟體、即可開始使用此功能。

Cloud Manager必須安裝在Google Cloud Platform中、才能在Cloud Volumes ONTAP GCP中部署。

1 設定您的網路

啟用從目標VPC的傳出網際網路存取、讓Cloud Manager和Cloud Volumes ONTAP 支援中心能夠連絡多個端點。

這個步驟很重要、因為Cloud Manager Cloud Volumes ONTAP 無法在沒有外傳網際網路存取的情況下部署不穩定功能。如果您需要限制傳出連線、請參閱的端點清單 "Cloud Manager" 和 "Cloud Volumes ONTAP"。

2 設定**GCP**權限和專案

確定已設置兩組權限：

1. 確保從 NetApp Cloud Central 部署 Cloud Manager 的 GCP 使用者擁有中的權限 "適用於GCP的Cloud Central原則"。

   "您可以使用 Yaml 檔案建立自訂角色" 然後附加到使用者。您需要使用 gCloud 命令列來建立角色。

2. 設定具有 Cloud Manager 所需權限的服務帳戶、以便在 Cloud Volumes ONTAP 專案中建立及管理各種系統。

   您將在步驟6中、將此服務帳戶與Cloud Manager VM建立關聯。

   - "在 GCP 中建立角色" 這包括在中定義的權限 "GCP 的 Cloud Manager 原則"。同樣地、您需要使用 gCloud 命令列。

     此Y反 洗錢檔案所含的權限與步驟2a中的權限不同。

   - "建立 GCP 服務帳戶、並套用您剛建立的自訂角色"。
   - 如果您想要在 Cloud Volumes ONTAP 其他專案中部署 "將具有 Cloud Manager 角色的服務帳戶新增至該專案、以授予存取權"。您必須針對每個專案重複此步驟。

3 設定GCP以進行資料分層

必須滿足兩項要求、才能將冷資料從Cloud Volumes ONTAP NetApp 9.7分層到低成本物件儲存（Google Cloud Storage儲存庫）：

1. "建立服務帳戶" 其使用者為預先定義的Storage Admin角色和Cloud Manager服務帳戶。

   您稍後在建立Cloud Volumes ONTAP 運作環境時、需要選擇此服務帳戶。此服務帳戶與您在步驟2中建立的服務帳戶不同。

2. "設定 Cloud Volumes ONTAP 私有 Google Access 的子網路"。

如果您想使用Cloud Volumes ONTAP 資料分層功能搭配使用 "然後依照下列步驟操作"。

4 啟用 Google Cloud API

"在專案中啟用下列 Google Cloud API"。部署Cloud Manager和Cloud Volumes ONTAP 功能完善的應用程式需要這些API。

- Cloud Deployment Manager V2 API
- Cloud Resource Manager API
- 運算引擎 API
- StackdrivER記錄API

5 從GCP Marketplace訂閱

"從Cloud Volumes ONTAP GCP Marketplace訂閱" 確保在免費試用結束後不會中斷服務。您所Cloud Volumes ONTAP 建立的每個功能不只是功能不全的功能不全、您將會從訂閱中收取費用。

6 從NetApp Cloud Central啟動Cloud Manager

需要Cloud Manager軟體來部署和管理Cloud Volumes ONTAP 功能。從GCP啟動Cloud Manager執行個體只需幾分鐘的時間 "Cloud Central"。

當您選擇GCP做為雲端供應商時、Google會提示您登入您的帳戶並授予權限。按一下「允許」可授予部署Cloud Manager所需的運算API存取權限。

7 使用 Cloud Manager 啟動 Cloud Volumes ONTAP

Cloud Manager準備好之後、只要按一下「Create（建立）」、選取您要部署的系統類型、然後完成精靈中的步驟即可。25分鐘後、您的第一個Cloud Volumes ONTAP 作業系統應該會啟動並開始運作。

相關連結

- "評估"
- "Cloud Manager的網路需求"
- "GCP 中的功能需求 Cloud Volumes ONTAP"
- "GCP的防火牆規則"
- "Cloud Manager 具備 GCP 權限的功能"
- "在 Cloud Volumes ONTAP GCP 中啟動"
- "下載並安裝Linux主機上的Cloud Manager軟體"

設定Cloud Manager

在 **Cloud Central** 帳戶中設定工作區和使用者

每個Cloud Manager系統都會與_NetApp Cloud Central帳戶建立關聯。設定與Cloud Manager系統相關的Cloud Central帳戶、讓使用者能夠存取Cloud Manager、Cloud Volumes ONTAP 並在工作空間中部署整套系統。只要新增使用者或新增多個使用者和工作區即可。

此帳戶會保留在Cloud Central中、因此您所做的任何變更都可用於其他Cloud Manager系統和其他NetApp雲端資料服務。 "深入瞭解 Cloud Central 帳戶的運作方式"。

新增工作區

在 Cloud Manager 中、工作區可讓您將一組工作環境與其他工作環境和其他使用者隔離。例如、您可以建立兩個工作區、並將個別使用者與工作區建立關聯。

步驟

1. 按一下*帳戶設定*。

2. 按一下 * 工作區 * 。
3. 按一下「 * 新增工作區 * 」。
4. 輸入工作區名稱、然後按一下 * 「 Add* （新增 * ）」。

完成後

您現在可以將使用者和服務連接器與工作區建立關聯。

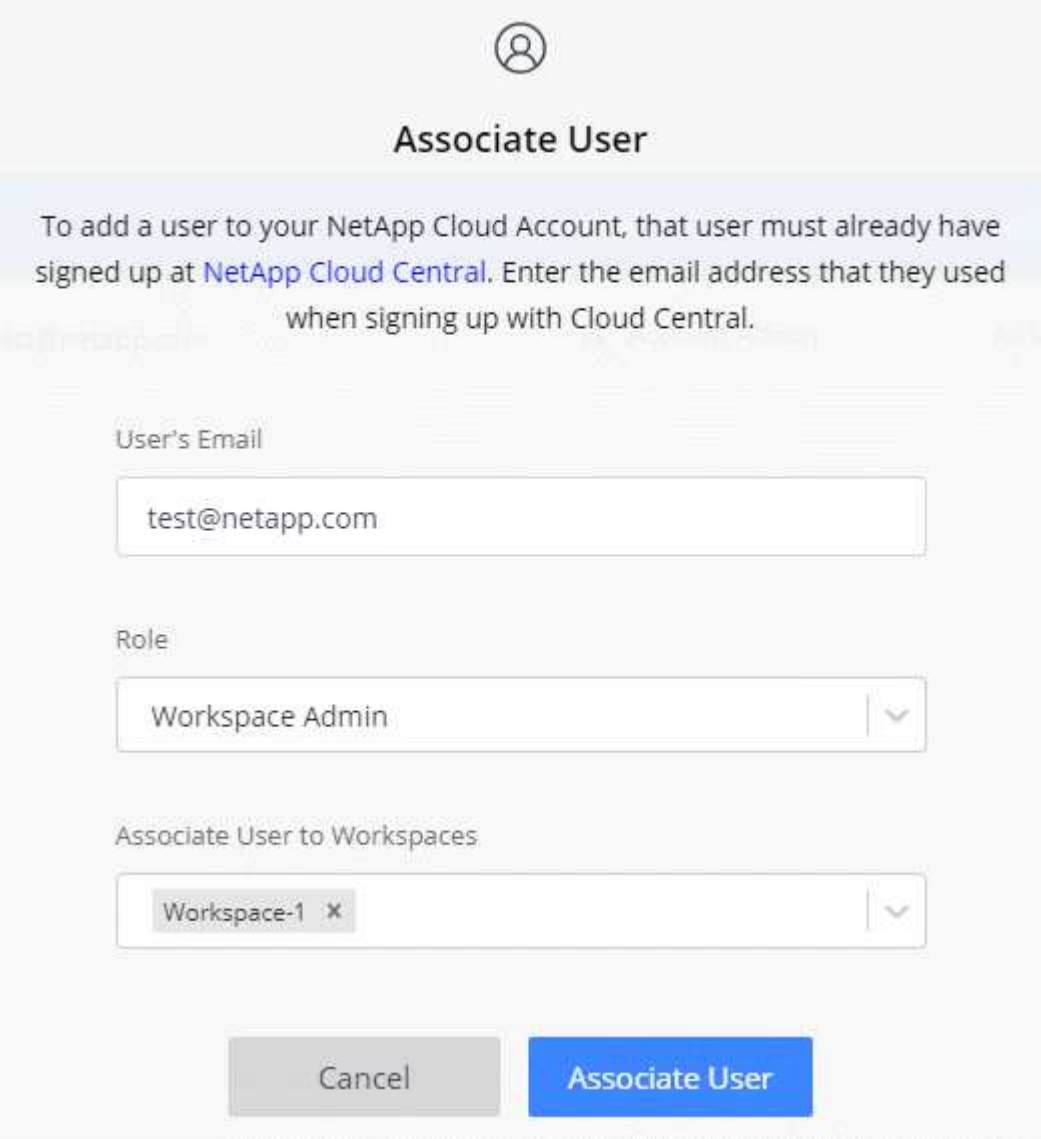
新增使用者

將 Cloud Central 使用者與 Cloud Central 帳戶建立關聯、讓這些使用者可以在 Cloud Manager 中建立及管理工

作環境。

步驟

1. 如果使用者尚未這麼做、請要求使用者前往 "NetApp Cloud Central" 並建立帳戶。
2. 在Cloud Manager中、按一下*帳戶設定*。
3. 在「使用者」索引標籤中、按一下「建立使用者關聯」。
4. 輸入使用者的電子郵件地址、然後為使用者選取角色：
   - * 客戶管理 * ：可在 Cloud Manager 中執行任何動作。
   - * 工作區管理 * ：可在指派的工作區中建立及管理資源。
5. 如果您選取「工作區管理」、請選取一個或多個工作區以與該使用者建立關聯。



6. 按一下「 * 建立使用者關聯 * 」。

結果

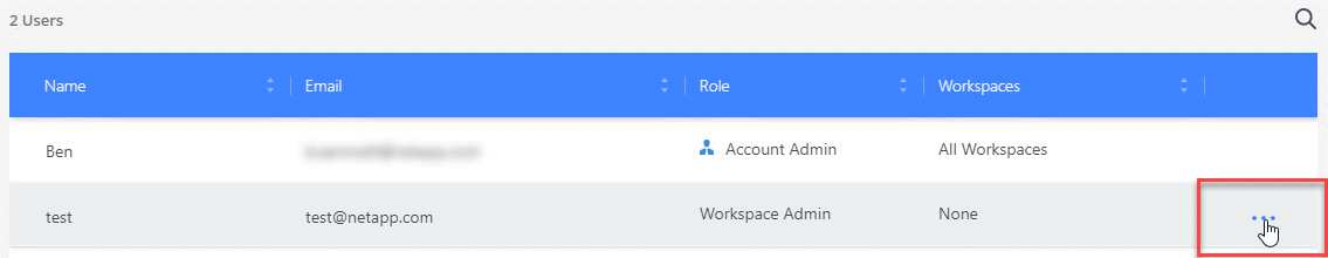
使用者應收到 NetApp Cloud Central 寄送的電子郵件、標題為「 Account Association （客戶關聯）」。 電子郵件中包含存取 Cloud Manager 所需的資訊。

將 **Workspace Admins** 與工作區建立關聯

您可以隨時將 Workspace Admins 與其他工作區建立關聯。建立使用者關聯可讓他們在該工作區中建立及檢視工作環境。

步驟

1. 按一下*帳戶設定*。
2. 按一下對應使用者列中的動作功能表。



3. 按一下 * 管理工作區 * 。
4. 選取一或多個工作區、然後按一下「 * 套用 * 」。

結果

只要服務連接器也與工作區相關聯、使用者就能從Cloud Manager存取這些工作區。

將服務連接器與工作區建立關聯

服務連接器是Cloud Manager系統的一部分。它可在部署於雲端供應商的虛擬機器執行個體上執行、或是在您設定的內部部署主機上執行。您需要將此服務連接器與工作區建立關聯、以便Workspace Admins可從Cloud Manager存取這些工作區。

如果您只有帳戶管理員、則不需要將服務連接器與工作區建立關聯。根據預設、 Account Admins 可存取 Cloud Manager 中的所有工作區。

"深入瞭解使用者、工作區和服務連接器"。

步驟

1. 按一下*帳戶設定*。
2. 按一下「服務連接器」。
3. 按一下*管理工作區*以取得您要關聯的服務連接器。
4. 選取一或多個工作區、然後按一下「 * 套用 * 」。

結果

只要使用者也與工作區相關聯、Workspace Admins現在即可存取相關的工作區。

設定**AWS**帳戶並將其新增至**Cloud Manager**

如果您想要在Cloud Volumes ONTAP 不同的AWS帳戶中部署功能、則需要提供必要的權限、並將詳細資料新增至Cloud Manager。您提供權限的方式取決於您是要為 Cloud

Manager 提供 AWS 金鑰、還是要為信任帳戶中的角色提供 ARN 。

> 當您從Cloud Central部署Cloud Manager時、Cloud Manager會自動新增AWS帳戶、讓您在其中部署Cloud Manager。如果您在現有系統上手動安裝Cloud Manager軟體、則不會新增初始帳戶。 "深入瞭解AWS帳戶和權限"。

- 選項 *
- 提供 AWS 金鑰來授予權限
- 在其他帳戶中假設 IAM 角色來授予權限

提供 **AWS** 金鑰來授予權限

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

步驟

1. 請從下載 Cloud Manager IAM 原則 "Cloud Manager 原則頁面"。
2. 從 IAM 主控台複製並貼上 Cloud Manager IAM 原則中的文字、以建立您自己的原則。

   "AWS 文件：建立 IAM 原則"

3. 將原則附加至 IAM 角色或 IAM 使用者。
   - "AWS 文件：建立 IAM 角色"
   - "AWS 文件：新增和移除 IAM 原則"

結果

帳戶現在擁有必要的權限。 您現在可以將它新增至 Cloud Manager。

在其他帳戶中假設 **IAM** 角色來授予權限

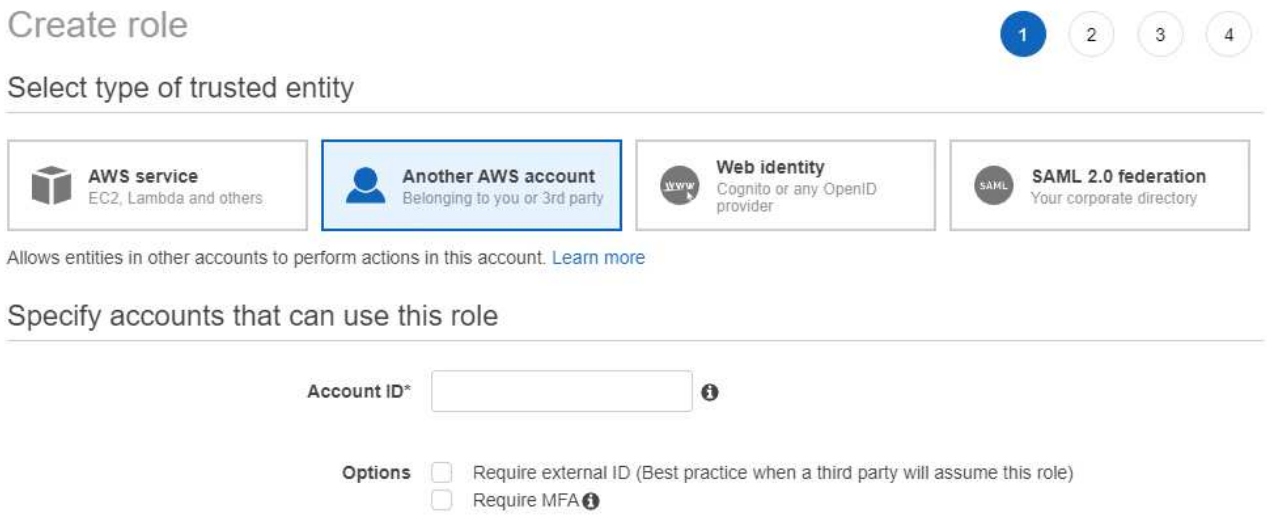
您可以使用IAM角色、在部署Cloud Manager執行個體的來源AWS帳戶與其他AWS帳戶之間建立信任關係。接著、您將從信任的帳戶中、為 Cloud Manager 提供 IAM 角色的 ARN 。

步驟

1. 前往您要部署 Cloud Volumes ONTAP 的目標帳戶、並選取 * 其他 AWS 帳戶 * 來建立 IAM 角色。

   請務必執行下列動作：

   - 輸入Cloud Manager執行個體所在帳戶的ID。
   - 附加 Cloud Manager IAM 原則、可從取得 "Cloud Manager 原則頁面"。



2. 前往Cloud Manager執行個體所在的來源帳戶、然後選取附加至執行個體的IAM角色。
   a. 按一下*信任關係>編輯信任關係*。
   b. 新增「STS:AssumeRole」動作和您在目標帳戶中建立之角色的ARN。
      - 範例 *

```
{
 "Version": "2012-10-17",
 "Statement": {
   "Effect": "Allow",
   "Action": "sts:AssumeRole",
   "Resource": "arn:aws:iam::ACCOUNT-B-ID:role/ACCOUNT-B-ROLENAME"
}
}
```

結果

帳戶現在擁有必要的權限。 您現在可以將它新增至 Cloud Manager。

將AWS帳戶新增至Cloud Manager

在您提供具備所需權限的AWS帳戶之後、您可以將帳戶新增至Cloud Manager。如此一來、您就能在 Cloud Volumes ONTAP 該帳戶中啟動支援系統。

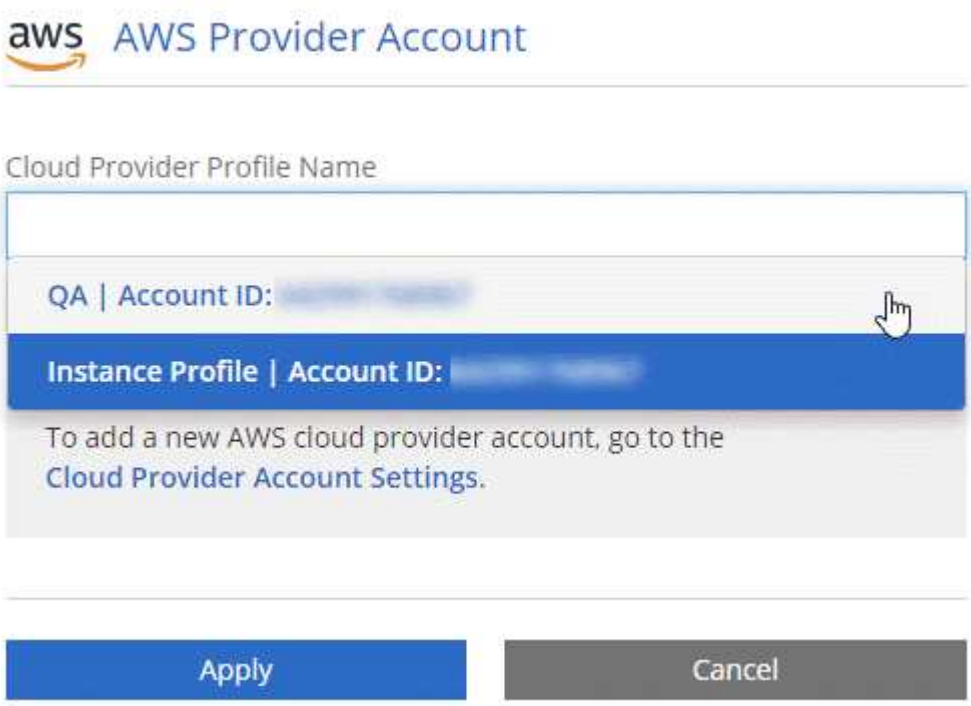
步驟

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

2. 按一下「新增帳戶」、然後選取「* AWS *」。
3. 選擇您要提供AWS金鑰或信任IAM角色的ARN。
4. 確認已符合原則需求、然後按一下「 * 建立帳戶 * 」。

結果

您現在可以在建立新的工作環境時、從「詳細資料與認證」頁面切換至其他帳戶：



設定Azure帳戶並新增至Cloud Manager

如果您想要在Cloud Volumes ONTAP 不同的Azure帳戶中部署功能、則必須提供這些帳戶所需的權限、然後將帳戶的詳細資料新增至Cloud Manager。

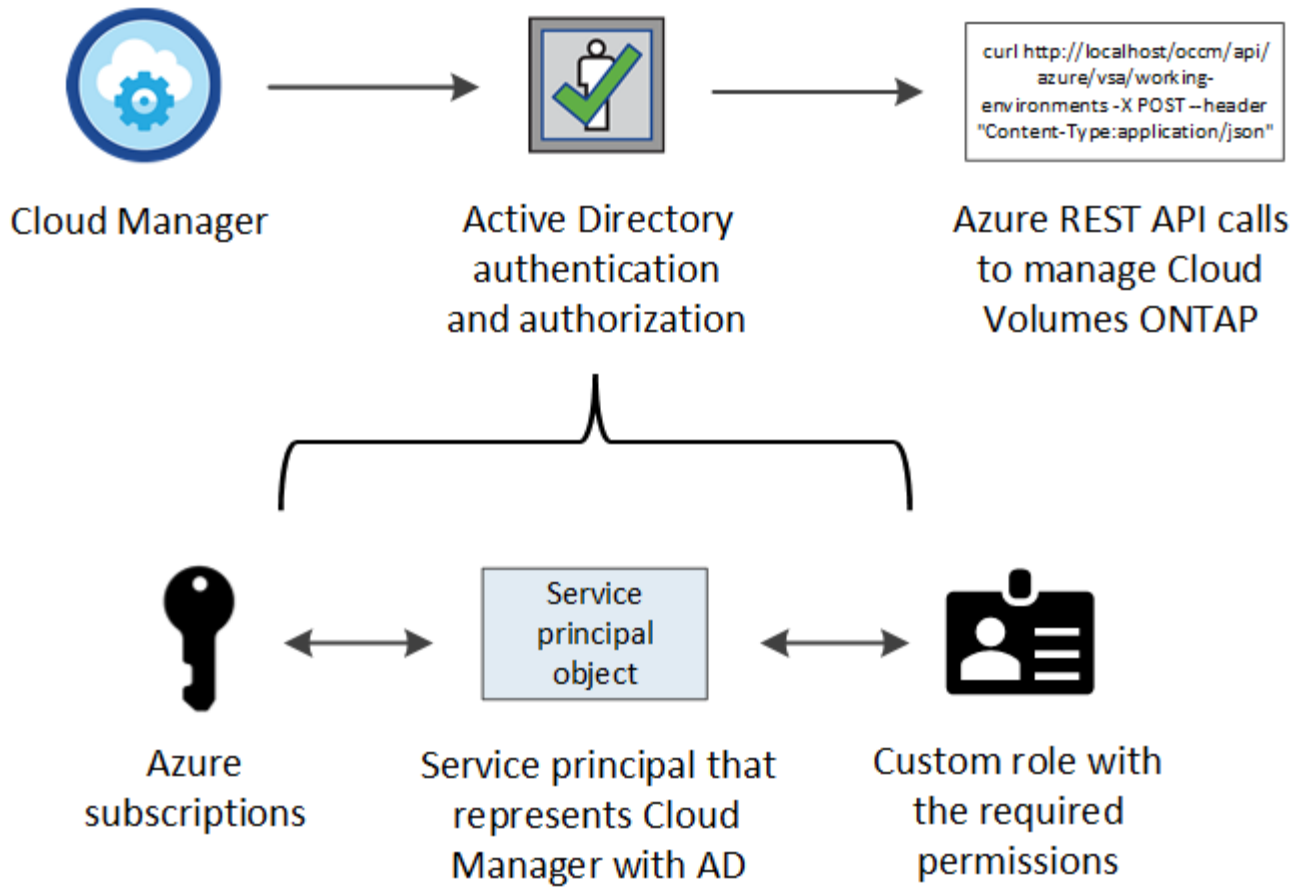
> 當您從Cloud Central部署Cloud Manager時、Cloud Manager會自動新增Azure帳戶、讓您部署Cloud Manager。如果您在現有系統上手動安裝Cloud Manager軟體、則不會新增初始帳戶。 "瞭解 Azure 帳戶與權限"。

使用服務主體授予 Azure 權限

Cloud Manager 需要權限才能在 Azure 中執行動作。您可以在 Azure Active Directory 中建立及設定服務主體、並取得 Cloud Manager 所需的 Azure 認證資料、將必要的權限授予 Azure 帳戶。

關於這項工作

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



步驟

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

建立 **Azure Active Directory** 應用程式

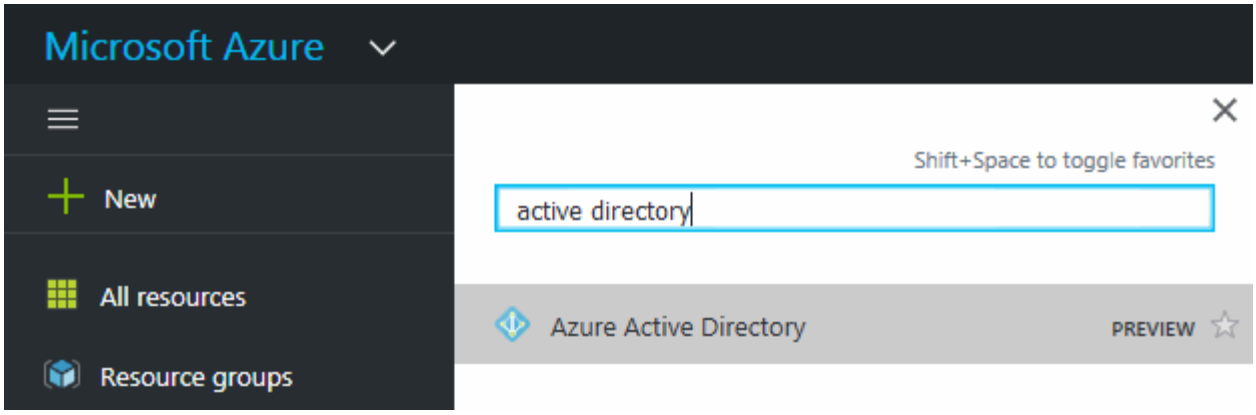
建立 Azure Active Directory （AD）應用程式與服務主體、讓 Cloud Manager 可用於角色型存取控制。

開始之前

您必須在 Azure 中擁有適當權限、才能建立 Active Directory 應用程式、並將應用程式指派給角色。如需詳細資訊、請參閱 "Microsoft Azure 說明文件：必要權限"。

步驟

1. 從 Azure 入口網站開啟 * Azure Active Directory * 服務。



2. 在功能表中、按一下 * 應用程式註冊 * 。
3. 按一下「 * 新登錄 * 」。
4. 指定應用程式的詳細資料：
   - * 名稱 * ：輸入應用程式的名稱。
   - * 帳戶類型 * ：選取帳戶類型（任何帳戶類型都可與 Cloud Manager 搭配使用）。
   - * 重新導向 URI* ：選取 * Web* 、然後輸入任何 URL 、例如： https://url
5. 按一下 * 註冊 * 。

結果

您已建立 AD 應用程式和服務主體。

將應用程式指派給角色

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

步驟

1. 建立自訂角色：
   a. 下載 "Cloud Manager Azure 原則"。
   b. 將 Azure 訂閱 ID 新增至可指派的範圍、以修改 Json 檔案。

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

      - 範例 *

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

   c. 使用 Json 檔案在 Azure 中建立自訂角色。

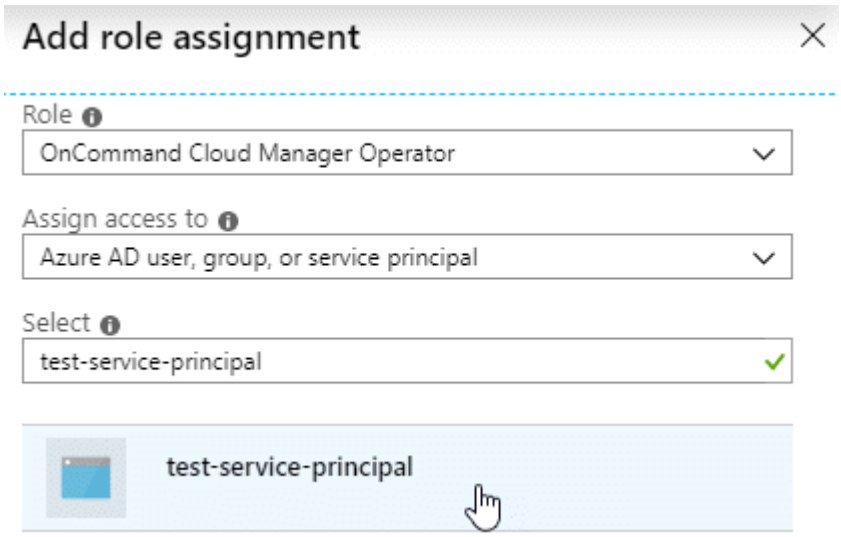
      下列範例說明如何使用 Azure CLI 2.0 建立自訂角色：

- AZ角色定義建立：-role定義C：\Policy_for_cove_Manager_Azure _3.7.4.json*

您現在應該擁有名為_EstratCloud OnCommand Manager operator_的自訂角色。

2. 將應用程式指派給角色：

   a. 從 Azure 入口網站開啟 * 訂閱 * 服務。
   b. 選取訂閱。
   c. 按一下 * 存取控制（ IAM ） > 新增 > 新增角色指派 * 。
   d. 選擇* OnCommand 《Cloud Manager operator*》角色。
   e. 保留 * Azure AD 使用者、群組或服務主體 * 的選取狀態。
   f. 搜尋應用程式名稱（您無法透過捲動在清單中找到）。



   g. 選取應用程式、然後按一下 * 「 Save （儲存）」 * 。

      Cloud Manager 的服務主體現在擁有該訂閱所需的 Azure 權限。

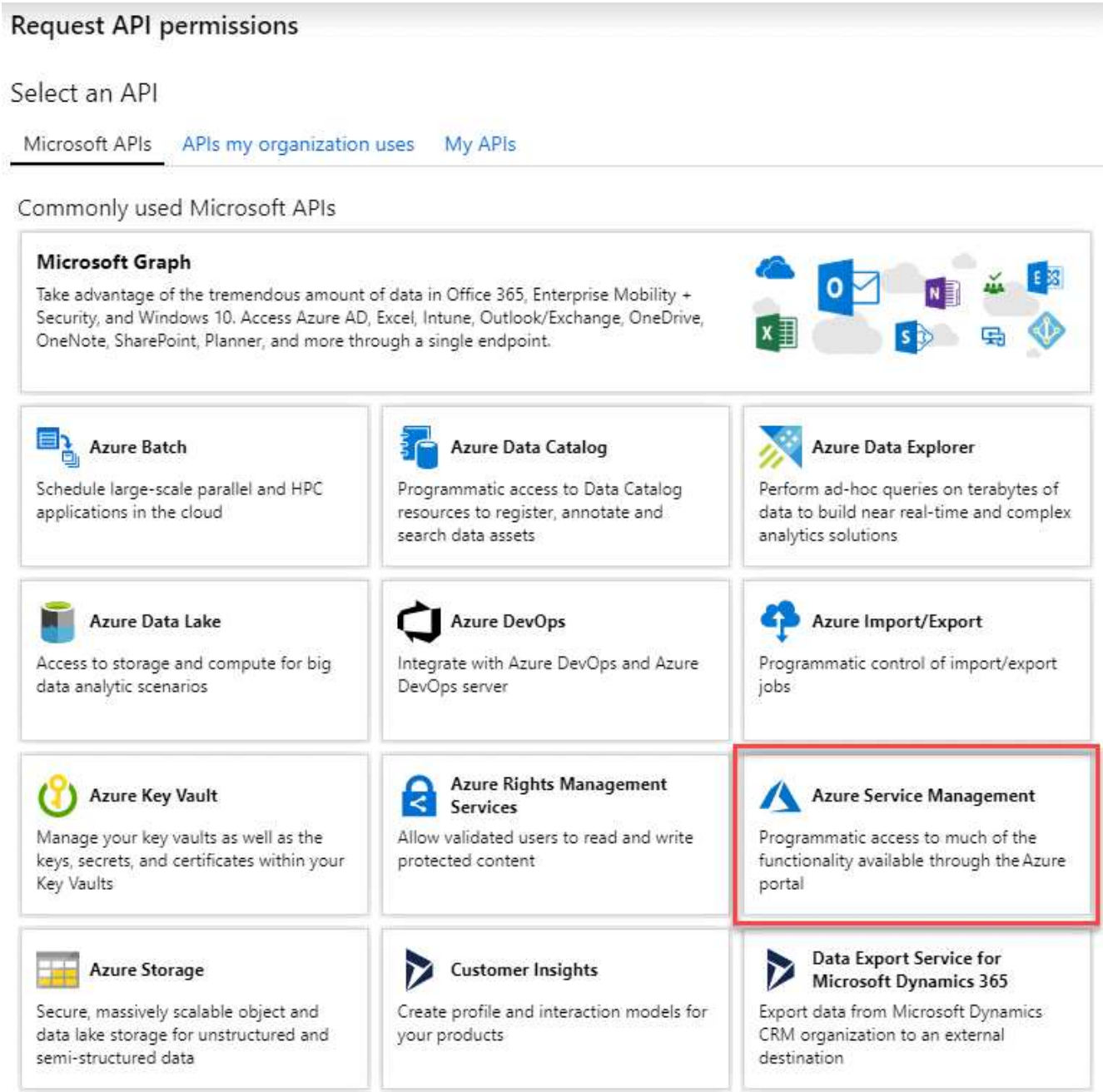
如果您想要從 Cloud Volumes ONTAP 多個 Azure 訂閱中部署支援功能、則必須將服務授權對象繫結至每個訂閱項目。Cloud Manager 可讓您選擇部署 Cloud Volumes ONTAP 時要使用的訂閱。

新增 **Windows Azure Service Management API** 權限

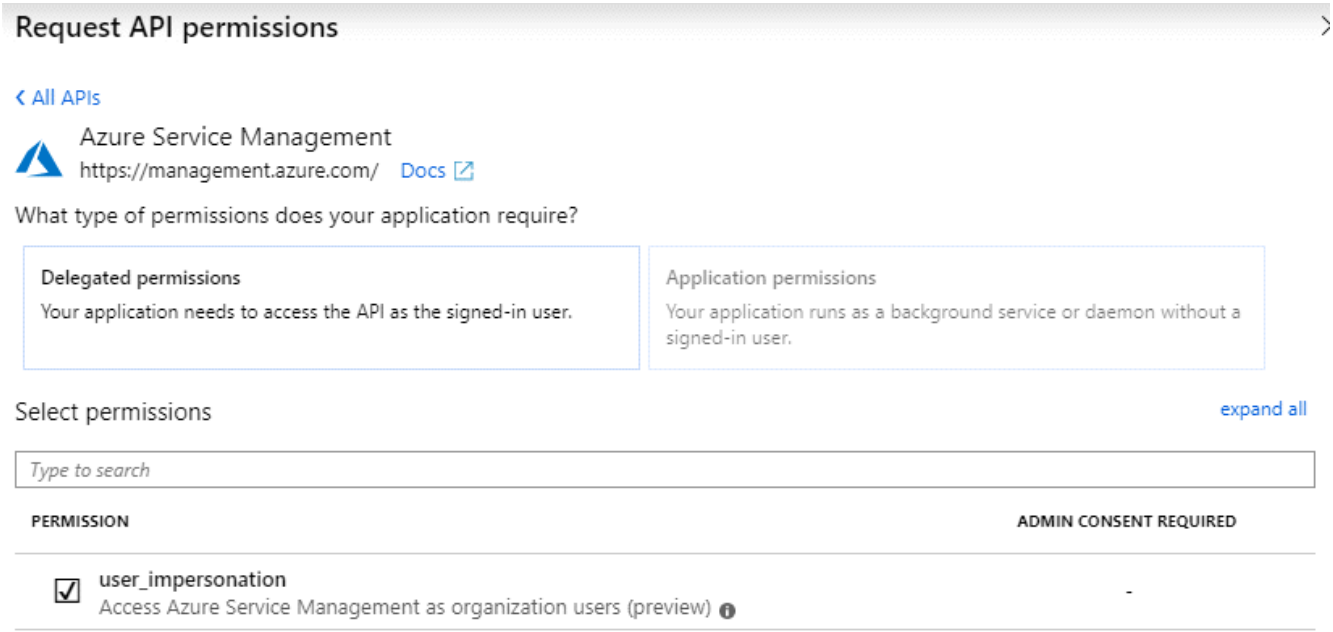
服務主體必須具有「 Windows Azure Service Management API 」權限。

步驟

1. 在 * Azure Active Directory * 服務中、按一下 * 應用程式註冊 * 、然後選取應用程式。
2. 按一下「 * API 權限 > 新增權限 * 」。
3. 在「 * Microsoft API* 」下、選取「 * Azure 服務管理 * 」。



4. 按一下「 * 以組織使用者身分存取 Azure 服務管理 * 」、然後按一下「 * 新增權限 * 」。

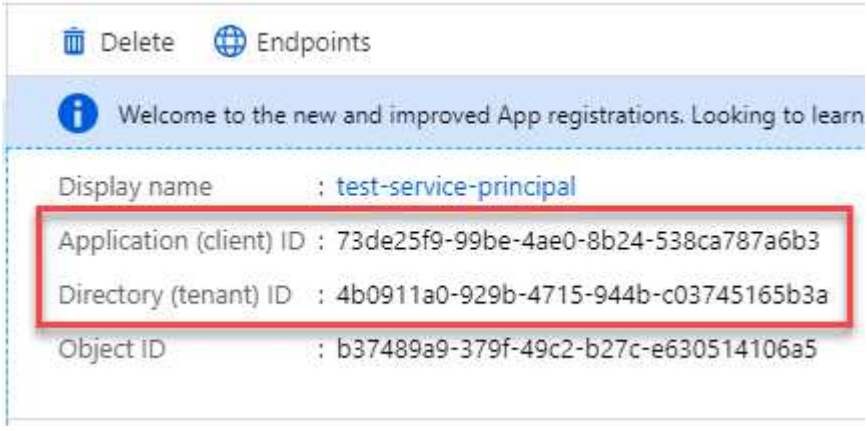


取得應用程式 **ID** 和目錄 **ID**

將 Azure 帳戶新增至 Cloud Manager 時、您必須提供應用程式的應用程式（用戶端） ID 和目錄（租戶） ID 。Cloud Manager 會使用 ID 以程式設計方式登入。

步驟

1. 在 * Azure Active Directory * 服務中、按一下 * 應用程式註冊 * 、然後選取應用程式。
2. 複製 * 應用程式（用戶端） ID* 和 * 目錄（租戶） ID* 。



建立用戶端機密

您需要建立用戶端機密、然後為 Cloud Manager 提供機密的價值、以便 Cloud Manager 使用它來驗證 Azure AD 。

> 將帳戶新增至 Cloud Manager 時、 Cloud Manager 會將用戶端機密稱為應用程式金鑰。

步驟

1. 開啟 * Azure Active Directory * 服務。
2. 按一下 * 應用程式註冊 * 、然後選取您的應用程式。
3. 按一下 * 「憑證與機密」 > 「新用戶端機密」 * 。
4. 提供機密與持續時間的說明。
5. 按一下「 * 新增 * 」。
6. 複製用戶端機密的值。

結果

您的服務主體現在已設定完成、您應該已經複製應用程式（用戶端） ID 、目錄（租戶） ID 、以及用戶端機密的值。新增 Azure 帳戶時、您必須在 Cloud Manager 中輸入此資訊。

將**Azure**帳戶新增至**Cloud Manager**

在您提供Azure帳戶所需的權限之後、即可將帳戶新增至Cloud Manager。如此一來、您就能在 Cloud Volumes ONTAP 該帳戶中啟動支援系統。

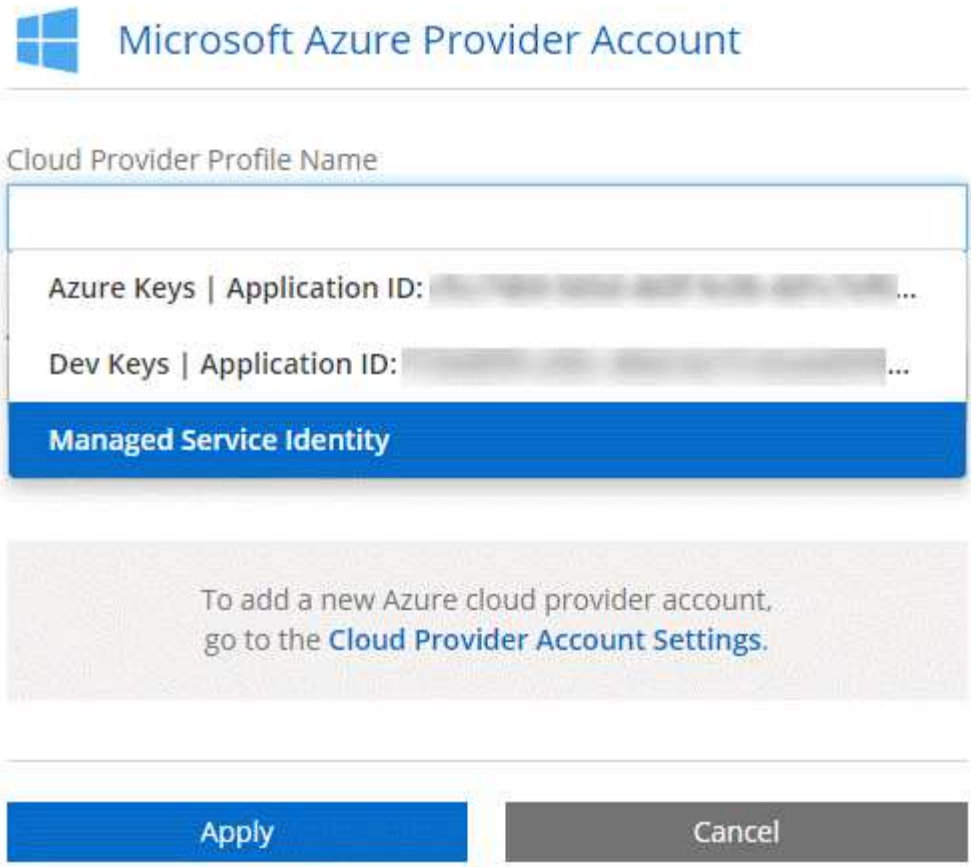
步驟

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

2. 按一下*「Add New Account*（新增帳戶）」、然後選取「Microsoft Azure *（Microsoft Azure
3. 輸入 Azure Active Directory 服務主體的相關資訊、以授予必要的權限：
   - 應用程式ID：請參閱 取得應用程式 ID 和目錄 ID。
   - 租戶ID（或目錄ID）：請參閱 取得應用程式 ID 和目錄 ID。
   - 應用程式金鑰（用戶端機密）：請參閱 [建立用戶端機密]。
4. 確認已符合原則需求、然後按一下「 * 建立帳戶 * 」。

結果

您現在可以在建立新的工作環境時、從「詳細資料與認證」頁面切換至其他帳戶：



將額外的 **Azure** 訂閱與託管身分識別建立關聯

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

關於這項工作

託管身分識別是 "初始 Azure 帳戶" 當您從NetApp Cloud Central部署Cloud Manager時、當您部署Cloud Manager時、Cloud Central建立OnCommand 了「不再只是做為運算子的解決方案」角色、並將其指派給Cloud Manager虛擬機器。

步驟

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

        中提供的預設名稱為「Cloud Manager操作員」OnCommand "Cloud Manager 原則"。如果您為角色選擇不同的名稱、請改為選取該名稱。

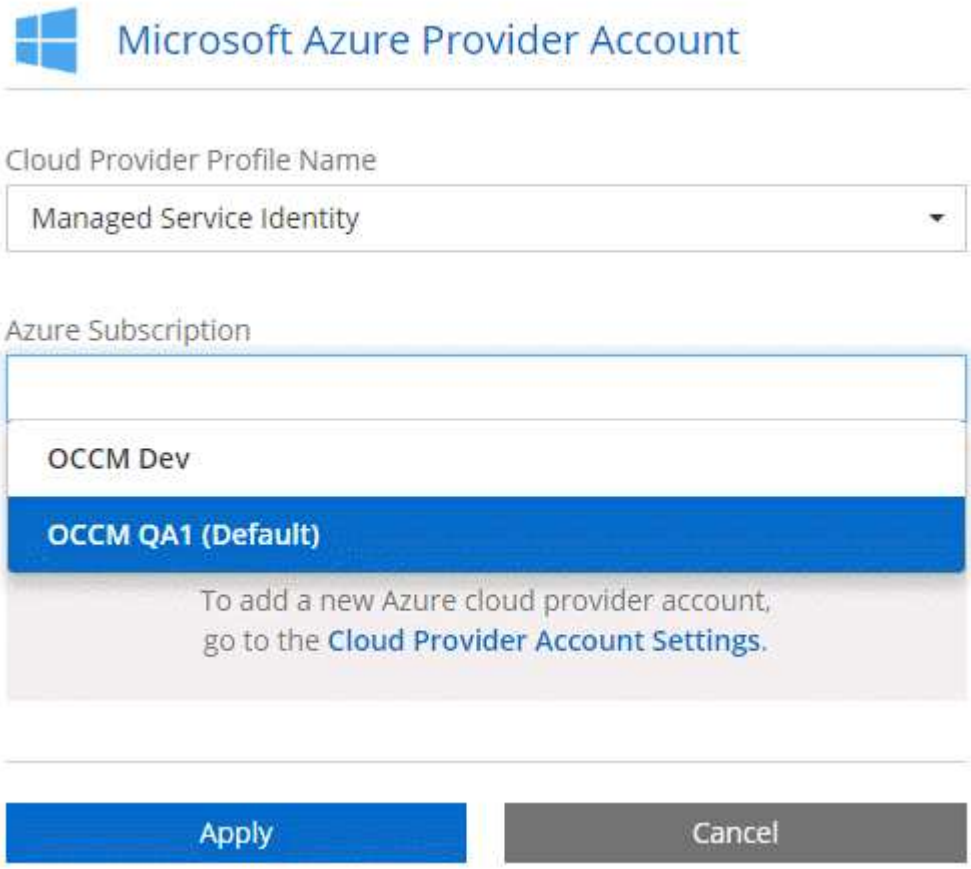
      - 指派 * 虛擬機器 * 的存取權。
      - 選取建立Cloud Manager虛擬機器的訂閱。

- 選取Cloud Manager虛擬機器。
- 按一下「 * 儲存 * 」。

4. 請重複這些步驟以取得額外訂閱內容。

結果

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



設定GCP帳戶並將其新增至Cloud Manager

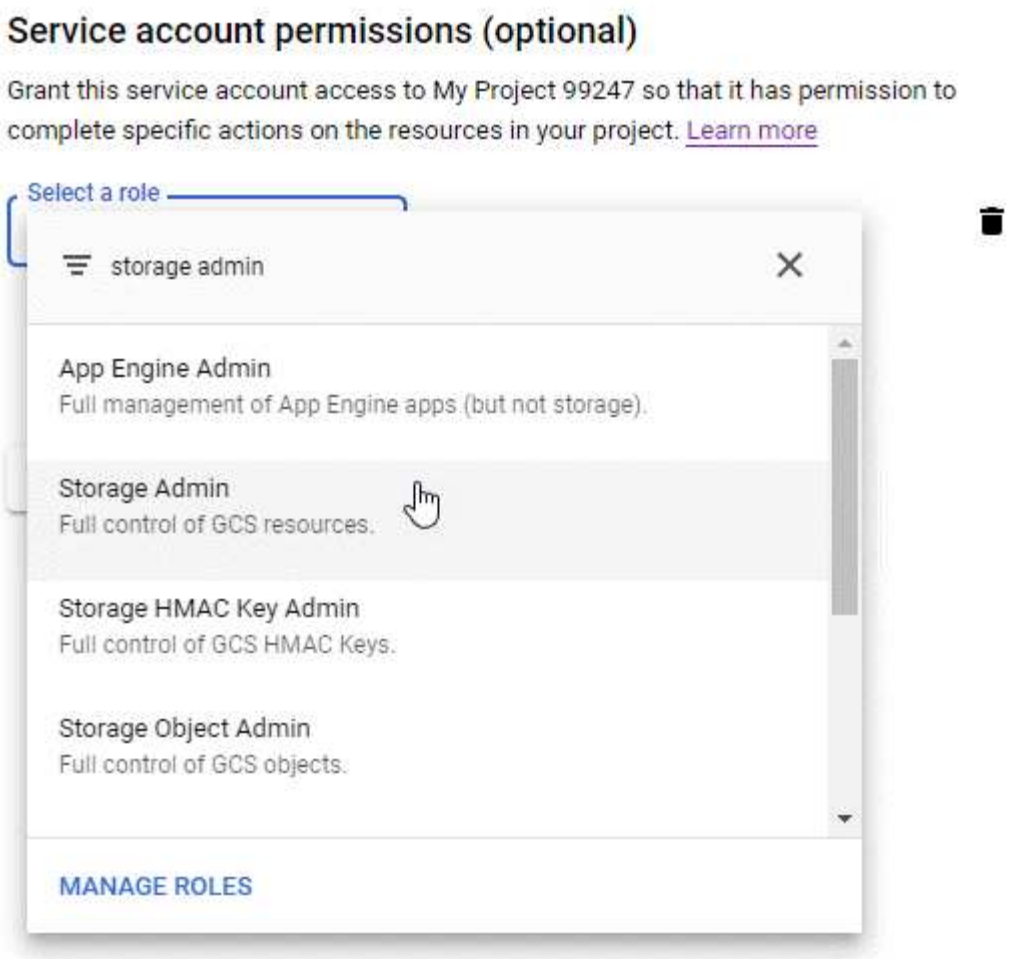
如果您要啟用 "資料分層" 在這個系統上、您需要為具有Storage Admin權限的服務帳戶、提供Cloud Manager儲存存取金鑰。Cloud Volumes ONTAPCloud Manager 使用存取金鑰來設定及管理雲端儲存庫、以利資料分層。

設定 **Google Cloud Storage** 的服務帳戶和存取金鑰

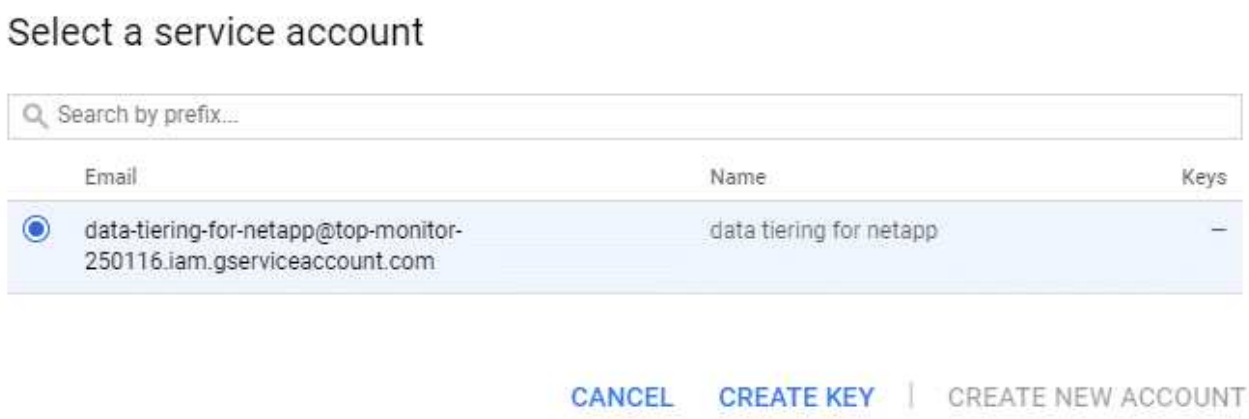
服務帳戶可讓 Cloud Manager 驗證及存取用於資料分層的雲端儲存桶。這些金鑰是必要的、以便 Google Cloud Storage 知道誰在提出要求。

步驟

1. 開啟 GCP IAM 主控台和 "建立具有 Storage Admin 角色的服務帳戶"。



2. 前往 "GCP 儲存設定"。
3. 如果出現提示、請選取專案。
4. 按一下「 * 互通性 * 」索引標籤。
5. 如果您尚未啟用、請按一下 * 「啟用互通性存取」 * 。
6. 在 * 服務帳戶的存取金鑰 * 下、按一下 * 建立服務帳戶的金鑰 * 。
7. 選取您在步驟 1 中建立的服務帳戶。



8. 按一下「 * 建立金鑰 * 」。
9. 複製存取金鑰和密碼。

   新增 GCP 帳戶以進行資料分層時、您必須在 Cloud Manager 中輸入此資訊。

將 GCP 帳戶新增至 Cloud Manager

現在您已擁有服務帳戶的存取金鑰、可以將其新增至 Cloud Manager 。

步驟

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

2. 按一下「新增帳戶」並選取「* GCP*」。
3. 輸入服務帳戶的存取金鑰和密碼。

   這些關鍵功能可讓 Cloud Manager 設定雲端儲存庫、以利資料分層。

4. 確認已符合原則需求、然後按一下「 * 建立帳戶 * 」。

接下來呢？

現在、您可以在建立、修改或複寫個別磁碟區時、在這些磁碟區上啟用資料分層功能。如需詳細資訊、請參閱 "將非作用中資料分層至低成本物件儲存設備"。

但在您之前、請確定 Cloud Volumes ONTAP 駐留的子網路已設定為私有 Google Access 。如需相關指示、請參閱 "Google Cloud 文件：設定私有 Google Access"。

新增 NetApp 支援網站帳戶至 Cloud Manager

若要部署 BYOL 系統、必須將 NetApp Support Site 帳戶新增至 Cloud Manager 。此外、您也必須註冊隨用付費系統、並升級 ONTAP 各種版本的軟件。

觀看下列影片、瞭解如何將 NetApp 支援網站帳戶新增至 Cloud Manager 。或向下捲動以閱讀步驟。

[] | *https://img.youtube.com/vi/V2fLTyztqYQ/maxresdefault.jpg*

步驟

1. 如果您還沒有 NetApp 支援網站帳戶、 "註冊一項"。
2. 在Cloud Manager主控台右上角、按一下「設定」圖示、然後選取「* Cloud Provider & Support Account*」。

3. 單擊* Add New Account*（添加新帳戶）並選擇* NetApp Support Site"（* NetApp支持站點*）。
4. 指定帳戶名稱、然後輸入使用者名稱和密碼。
   - 帳戶必須是客戶層級的帳戶（不是來賓帳戶或臨時帳戶）。
   - 如果您打算部署 BYOL 系統：
     - 帳戶必須獲得授權、才能存取 BYOL 系統的序號。
     - 如果您購買安全的 BYOL 訂閱、則需要安全的 NSS 帳戶。
5. 按一下「 * 建立帳戶 * 」

接下來呢？

使用者現在可以在建立新 Cloud Volumes ONTAP 的功能表系統和註冊現有系統時、選擇帳戶。

- "在 Cloud Volumes ONTAP AWS 中啟動"
- "在 Cloud Volumes ONTAP Azure 中啟動"
- "註冊隨用隨付系統"
- "瞭解 Cloud Manager 如何管理授權檔案"

安裝HTTPS憑證以確保安全存取

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

步驟

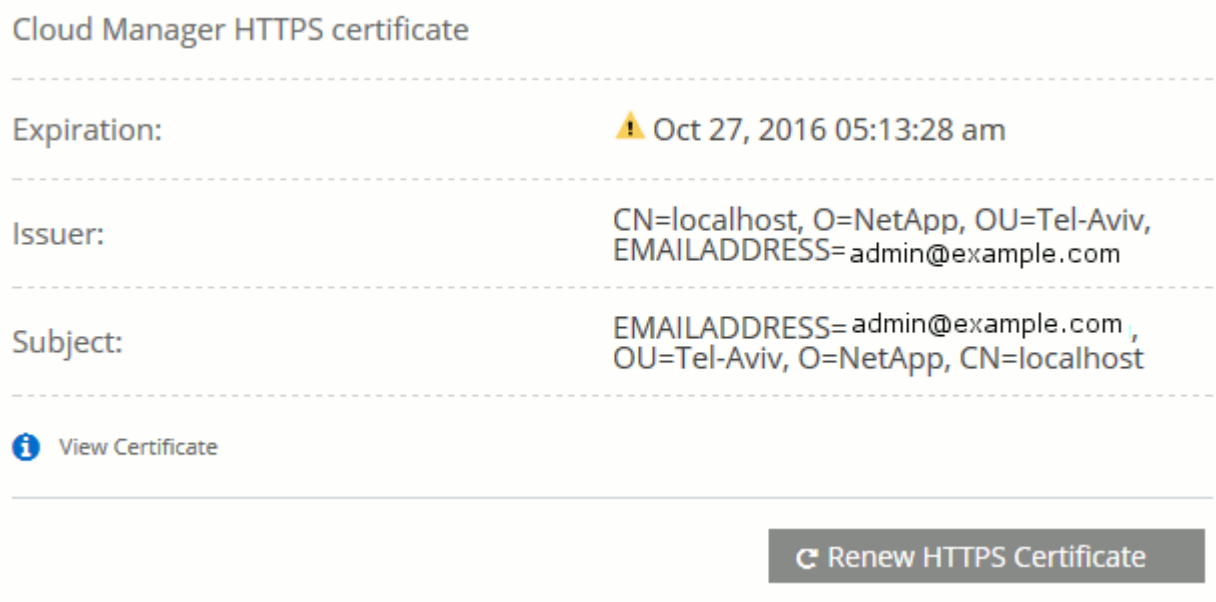
1. 在 Cloud Manager 主控台右上角、按一下「設定」圖示、然後選取「 * HTTPS 設定 * 」。

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

選項	說明
產生 CSR	a. 輸入Cloud Manager主機的主機名稱或DNS（其一般名稱）、然後按一下* 產生CSR *。 Cloud Manager 會顯示憑證簽署要求。 b. 使用 CSR 將 SSL 憑證要求提交給 CA 。 憑證必須使用隱私增強型郵件（ PEF ） Base - 64 編碼的 X · 509 格式。 c. 複製簽署的憑證內容、貼到「憑證」欄位、然後按一下「 * 安裝 * 」。
安裝您自己的 CA 簽署憑證	a. 選擇 * 安裝 CA 簽署的憑證 * 。 b. 同時載入憑證檔案和私密金鑰、然後按一下「 * 安裝 * 」。 憑證必須使用隱私增強型郵件（ PEF ） Base - 64 編碼的 X · 509 格式。

結果

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



設定 **AWS KMS**

如果您想搭配 Cloud Volumes ONTAP 使用 Amazon 加密搭配使用、則需要設定 AWS 金鑰管理服務（ KMS ）。

步驟

1. 確認存在作用中的客戶主金鑰（ CMK ）。

CMK 可以是 AWS 託管的 CMK 、也可以是客戶託管的 CMK 。它可以與 Cloud Manager 及 Cloud Volumes ONTAP 其他 AWS 帳戶位於相同的 AWS 帳戶中、也可以位於不同的 AWS 帳戶中。

"AWS 文件：客戶主要金鑰（CMK）"

2. 將 IAM 角色新增為 Cloud Manager 提供權限、做為 _key 使用者 _ 、以修改每個 CMK 的金鑰原則。

   將 IAM 角色新增為主要使用者、可讓 Cloud Manager 有權搭配 Cloud Volumes ONTAP 使用 CMK 。

   "AWS 文件：編輯金鑰"

3. 如果 CMK 位於不同的 AWS 帳戶、請完成下列步驟：

   a. 從 CMK 所在的帳戶移至 KMS 主控台。

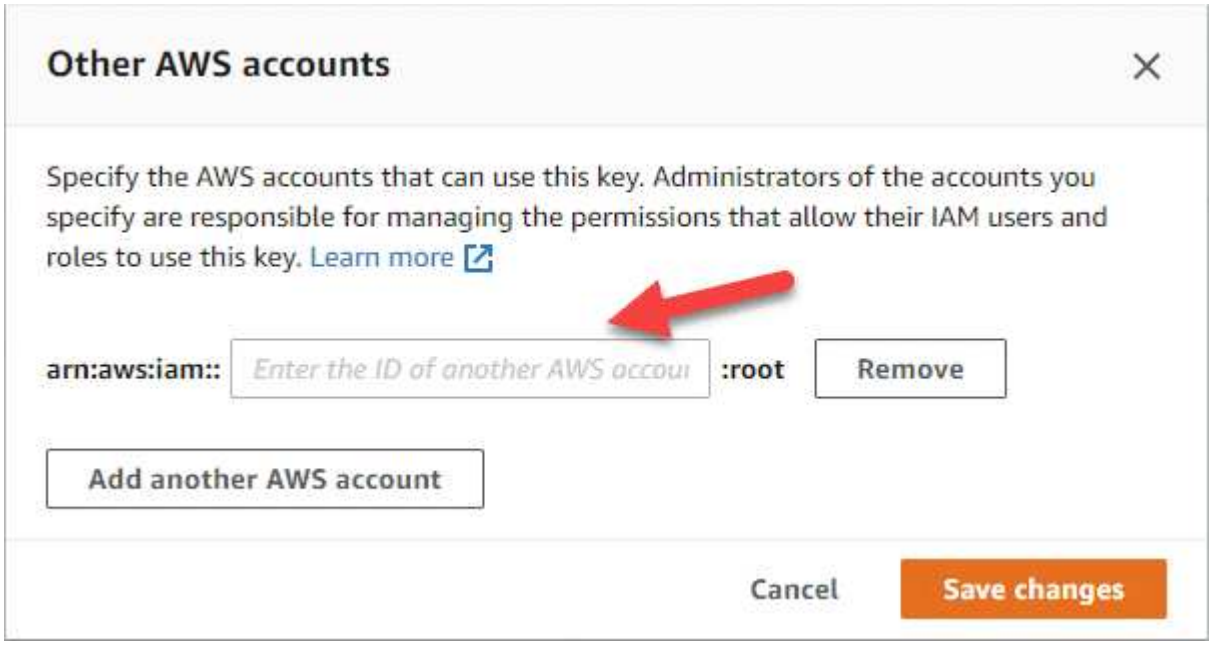
   b. 選取金鑰。

   c. 在「* 一般組態 *」窗格中、複製金鑰的 ARN 。

      建立 Cloud Volumes ONTAP 一套系統時、您必須提供 ARN 給 Cloud Manager 。

   d. 在 * 其他 AWS 帳戶 * 窗格中、新增提供 Cloud Manager 權限的 AWS 帳戶。

      在大多數情況下、這是 Cloud Manager 所在的帳戶。如果 AWS 中未安裝 Cloud Manager 、則您會將 AWS 存取金鑰提供給 Cloud Manager 。



e. 現在請切換至 AWS 帳戶、該帳戶可為 Cloud Manager 提供權限、並開啟 IAM 主控台。

f. 建立包含下列權限的 IAM 原則。

g. 將原則附加至提供 Cloud Manager 權限的 IAM 角色或 IAM 使用者。

下列原則提供 Cloud Manager 從外部 AWS 帳戶使用 CMK 所需的權限。請務必修改「資源」區段中的區域和帳戶 ID 。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowUseOfTheKey",
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalkeyid"
            ]
        },
        {
            "Sid": "AllowAttachmentOfPersistentResources",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalaccountid"
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

+
如需此程序的其他詳細資料、請參閱 "AWS 文件：允許外部 AWS 帳戶存取 CMK"。

網路需求

Cloud Manager的網路需求

設定您的網路、讓Cloud Manager能夠在Cloud Volumes ONTAP AWS、Microsoft Azure或Google Cloud Platform中部署不支援的系統。最重要的步驟是確保從網際網路存取各種端點。

> 如果您的網路使用Proxy伺服器來進行所有與網際網路的通訊、Cloud Manager會在設定期間提示您指定Proxy。您也可以從「設定」頁面指定Proxy伺服器。請參閱 "設定Cloud Manager使用Proxy伺服器"。

連線至目標網路

Cloud Manager需要網路連線至您要部署Cloud Volumes ONTAP 的VPC和VNets。

例如、如果您在公司網路中安裝Cloud Manager、則必須設定VPN連線至VPC或vnet、以便在其中啟動Cloud Volumes ONTAP 更新。

傳出網際網路存取

Cloud Manager需要存取外部網際網路、才能部署Cloud Volumes ONTAP 及管理功能。從網頁瀏覽器存取Cloud Manager時、以及在Linux主機上執行Cloud Manager安裝程式時、也需要外傳網際網路存取。

下列各節將說明特定的端點。

端點以管理Cloud Volumes ONTAP AWS中的功能

Cloud Manager在Cloud Volumes ONTAP AWS中部署及管理功能時、需要透過外傳網際網路連絡下列端點：

端點	目的
AWS 服務（amazonaws.com): • CloudForation • 彈性運算雲端（EC2） • 金鑰管理服務（KMS） • 安全性權杖服務（STOS） • 簡易儲存服務（S3） 確切的端點取決於您部署 Cloud Volumes ONTAP 的區域。 "如需詳細資料、請參閱 AWS 文件。"	讓Cloud Manager能夠在Cloud Volumes ONTAP AWS中部署及管理功能。

端點	目的
https://api.services.cloud.netapp.com:443	API 要求 NetApp Cloud Central 。
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	提供軟體映像、資訊清單和範本的存取權限。
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com	讓Cloud Manager能夠存取及下載資訊清單、範本及Cloud Volumes ONTAP 升級影像。
https://kinesis.us-east-1.amazonaws.com	讓 NetApp 能夠從稽核記錄串流資料。
https://cloudmanager.cloud.netapp.com	與 Cloud Manager 服務（包括 Cloud Central 帳戶）進行通訊。
https://netapp-cloud-account.auth0.com	與 NetApp Cloud Central 通訊、以進行集中式使用者驗證。
https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist	用於將AWS帳戶ID新增至允許備份至S3的使用者清單。
https://support.netapp.com/aods/asupmessage https://support.netapp.com/asupprod/post/1.0/postAsup	與 NetApp AutoSupport 通訊
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement	與 NetApp 溝通以取得系統授權與支援登錄。
https://ipa-signer.cloudmanager.netapp.com	讓 Cloud Manager 能夠產生授權（例如 FlexCache 、針對 Cloud Volumes ONTAP 功能不全的
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	需要將Cloud Volumes ONTAP 支援的系統與Kubernetes叢集連線。端點可安裝NetApp Trident。
各種協力廠商位置、例如： • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org 第三方據點可能會有所變更。	在升級期間、 Cloud Manager 會針對協力廠商相依性下載最新的套件。

在**Cloud Volumes ONTAP Azure**中管理功能的端點

在Cloud Volumes ONTAP Microsoft Azure中部署及管理功能時、Cloud Manager需要透過外傳網際網路連絡下列端點：

端點	目的
https://management.azure.com https://login.microsoftonline.com	讓 Cloud Manager 能夠在 Cloud Volumes ONTAP 大多數 Azure 地區部署及管理功能。

端點	目的
https://management.microsoftazure.de https://login.microsoftonline.de	讓 Cloud Manager 能夠在 Cloud Volumes ONTAP Azure Germany 地區部署及管理功能。
https://management.usgovcloudapi.net https://login.microsoftonline.com	讓 Cloud Manager 能夠在 Cloud Volumes ONTAP Azure US Gov 地區部署及管理功能。
https://api.services.cloud.netapp.com:443	API 要求 NetApp Cloud Central 。
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	提供軟體映像、資訊清單和範本的存取權限。
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com	讓Cloud Manager能夠存取及下載資訊清單、範本及Cloud Volumes ONTAP 升級影像。
https://kinesis.us-east-1.amazonaws.com	讓 NetApp 能夠從稽核記錄串流資料。
https://cloudmanager.cloud.netapp.com	與 Cloud Manager 服務（包括 Cloud Central 帳戶）進行通訊。
https://netapp-cloud-account.auth0.com	與 NetApp Cloud Central 通訊、以進行集中式使用者驗證。
https://mysupport.netapp.com	與 NetApp AutoSupport 通訊
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement	與 NetApp 溝通以取得系統授權與支援登錄。
https://ipa-signer.cloudmanager.netapp.com	讓 Cloud Manager 能夠產生授權（例如 FlexCache 、針對 Cloud Volumes ONTAP 功能不全的
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	需要將Cloud Volumes ONTAP 支援的系統與Kubernetes叢集連線。端點可安裝NetApp Trident。
各種協力廠商位置、例如： • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org 第三方據點可能會有所變更。	在升級期間、 Cloud Manager 會針對協力廠商相依性下載最新的套件。

端點以管理**Cloud Volumes ONTAP GCP**中的功能

Cloud Manager在Cloud Volumes ONTAP GCP中部署及管理功能時、需要透過外傳網際網路連絡下列端點：

端點	目的
https://www.googleapis.com	讓Cloud Manager能夠聯絡Google API、以便在Cloud Volumes ONTAP GCP中部署及管理功能。
https://api.services.cloud.netapp.com:443	API 要求 NetApp Cloud Central 。

端點	目的
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	提供軟體映像、資訊清單和範本的存取權限。
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com	讓Cloud Manager能夠存取及下載資訊清單、範本及Cloud Volumes ONTAP 升級影像。
https://kinesis.us-east-1.amazonaws.com	讓 NetApp 能夠從稽核記錄串流資料。
https://cloudmanager.cloud.netapp.com	與 Cloud Manager 服務（包括 Cloud Central 帳戶）進行通訊。
https://netapp-cloud-account.auth0.com	與 NetApp Cloud Central 通訊、以進行集中式使用者驗證。
https://mysupport.netapp.com	與 NetApp AutoSupport 通訊
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement	與 NetApp 溝通以取得系統授權與支援登錄。
https://ipa-signer.cloudmanager.netapp.com	讓 Cloud Manager 能夠產生授權（例如 FlexCache 、針對 Cloud Volumes ONTAP 功能不全的
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	需要將Cloud Volumes ONTAP 支援的系統與Kubernetes叢集連線。端點可安裝NetApp Trident。
各種協力廠商位置、例如： • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org 第三方據點可能會有所變更。	在升級期間、 Cloud Manager 會針對協力廠商相依性下載最新的套件。

從網頁瀏覽器存取端點

使用者必須從網頁瀏覽器存取 Cloud Manager 。執行 Web 瀏覽器的機器必須連線至下列端點：

端點	目的
Cloud Manager主機	您必須從網頁瀏覽器輸入主機的 IP 位址、才能載入 Cloud Manager 主控台。 視您與雲端供應商的連線能力而定、您可以使用指派給主機的私有 IP 或公有 IP ： • 如果您有 VPN 並直接連線至虛擬網路、則私有 IP 可正常運作 • 公有 IP 適用於任何網路情境 無論如何、您應該確保安全群組規則僅允許從授權的 IP 或子網路存取、以確保網路存取安全。
https://auth0.com https://cdn.auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com	您的網頁瀏覽器會連線至這些端點、以便透過 NetApp Cloud Central 進行集中式使用者驗證。
https://widget.intercom.io	產品內對談可讓您與 NetApp 雲端專家交談。

端點以在**Linux**主機上安裝**Cloud Manager**

Cloud Manager安裝程式必須在安裝過程中存取下列URL：

- http://dev.mysql.com/get/mysql-community-release-el7-5.noarch.rpm
- https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
- https://s3.amazonaws.com/aws-cli/awscli-bundle.zip

連接埠和安全性群組

- 如果您從Cloud Central或市場映像部署Cloud Manager、請參閱下列內容：
  - "AWS中Cloud Manager的安全群組規則"
  - "Azure中Cloud Manager的安全群組規則"
  - "GCP中Cloud Manager的防火牆規則"
- 如果您在現有的Linux主機上安裝Cloud Manager、請參閱 "Cloud Manager主機需求"。

AWS 的網路需求 Cloud Volumes ONTAP

設定 AWS 網路功能、 Cloud Volumes ONTAP 讓各個系統正常運作。

一般**AWS**網路需求**Cloud Volumes ONTAP**

AWS 必須符合下列要求。

對節點的輸出網際網路存取 **Cloud Volumes ONTAP**

支援不需透過外部網際網路存取、即可將訊息傳送至 NetApp 解決方案、以主動監控儲存設備的健全狀況。Cloud Volumes ONTAP AutoSupport

路由和防火牆原則必須允許 AWS HTTP / HTTPS 流量傳輸至下列端點、 Cloud Volumes ONTAP 才能讓下列端點傳送 AutoSupport 動態訊息：

- https://support.netapp.com/aods/asupmessage
- https://support.netapp.com/asupprod/post/1.0/postAsup

如果您有 NAT 執行個體、則必須定義傳入安全性群組規則、以允許 HTTPS 流量從私有子網路傳入網際網路。

HA 中介器的傳出網際網路存取

HA 中介執行個體必須具有 AWS EC2 服務的傳出連線、才能協助進行儲存容錯移轉。若要提供連線、您可以新增公用 IP 位址、指定 Proxy 伺服器或使用手動選項。

手動選項可以是從目標子網路到 AWS EC2 服務的 NAT 閘道或介面 VPC 端點。如需 VPC 端點的詳細資訊、請參閱 "AWS 文件：介面 VPC 端點（AWS Private Link）"。

IP 位址數

Cloud Manager 會在 Cloud Volumes ONTAP AWS 中配置下列數量的 IP 位址給功能不全：

- 單一節點： 6 個 IP 位址
- HA 配對單一 AZs ： 15 個位址
- 多個 AZs 中的 HA 配對： 15 或 16 個 IP 位址

請注意、 Cloud Manager 會在單一節點系統上建立 SVM 管理 LIF 、但不會在單一 AZ 的 HA 配對上建立。您可以選擇是否在多個 AZs 的 HA 配對上建立 SVM 管理 LIF 。

> LIF 是與實體連接埠相關聯的 IP 位址。諸如 VMware 的管理工具需要 SVM 管理 LIF SnapCenter 。

安全性群組

您不需要建立安全性群組、因為 Cloud Manager 會為您建立安全性群組。如果您需要使用自己的、請參閱 "安全性群組規則"。

從 **Cloud Volumes ONTAP** 支援資料分層的功能、從功能鏈接至 **AWS S3**

如果您想要將 EBS 當作效能層、將 AWS S3 當作容量層、您必須確保 Cloud Volumes ONTAP 將該連接到 S3 。提供此連線的最佳方法是建立 VPC 端點至 S3 服務。如需相關指示、請參閱 "AWS 文件：建立閘道端點"。

當您建立 VPC 端點時、請務必選取與 Cloud Volumes ONTAP 該實例相對應的區域、 VPC 和路由表。您也必須修改安全性群組、以新增允許流量到 S3 端點的傳出 HTTPS 規則。否則 Cloud Volumes ONTAP 、無法連線至 S3 服務。

如果您遇到任何問題、請參閱 "AWS 支援知識中心：為什麼我無法使用閘道 VPC 端點連線至 S3 儲存區？"

連線 **ONTAP** 至其他網路中的不二系統

若要在 Cloud Volumes ONTAP AWS 系統和 ONTAP 其他網路中的更新系統之間複寫資料、您必須在 AWS VPC 和其他網路之間建立 VPN 連線、例如 Azure vnet 或公司網路。如需相關指示、請參閱 "AWS 文件：設定 AWS VPN 連線"。

適用於 **CIFS** 的 **DNS** 和 **Active Directory**

如果您想要配置 CIFS 儲存設備、則必須在 AWS 中設定 DNS 和 Active Directory 、或將內部部署設定延伸至 AWS 。

DNS 伺服器必須為 Active Directory 環境提供名稱解析服務。您可以將 DHCP 選項集設定為使用預設 EC2 DNS 伺服器、此伺服器不得是 Active Directory 環境所使用的 DNS 伺服器。

如需相關指示、請參閱 "AWS 文件： AWS Cloud 上的 Active Directory 網域服務：快速入門參考部署"。

AWS 在 **Cloud Volumes ONTAP** 多個 **AZs** 中的功能需求

其他 AWS 網路需求適用於 Cloud Volumes ONTAP 使用多個可用區域（ AZs ）的 SestHA 組態。在啟動 HA 配對之前、您應該先檢閱這些需求、因為您必須在 Cloud Manager 中輸入網路詳細資料。

若要瞭解 HA 配對的運作方式、請參閱 "高可用度配對"。

可用度區域

此 HA 部署模式使用多個 AZs 來確保資料的高可用度。您應該使用專屬的 AZ 來處理每 Cloud Volumes ONTAP 個實例、並使用中介執行個體、以提供 HA 配對之間的通訊通道。

用於 **NAS** 資料和叢集 **/ SVM** 管理的浮動 **IP** 位址

多個 AZs 中的 HA 組態會使用浮動 IP 位址、在發生故障時在節點之間移轉。除非您的選擇、否則無法從 VPC 外部原生存取 "設定 AWS 傳輸閘道"。

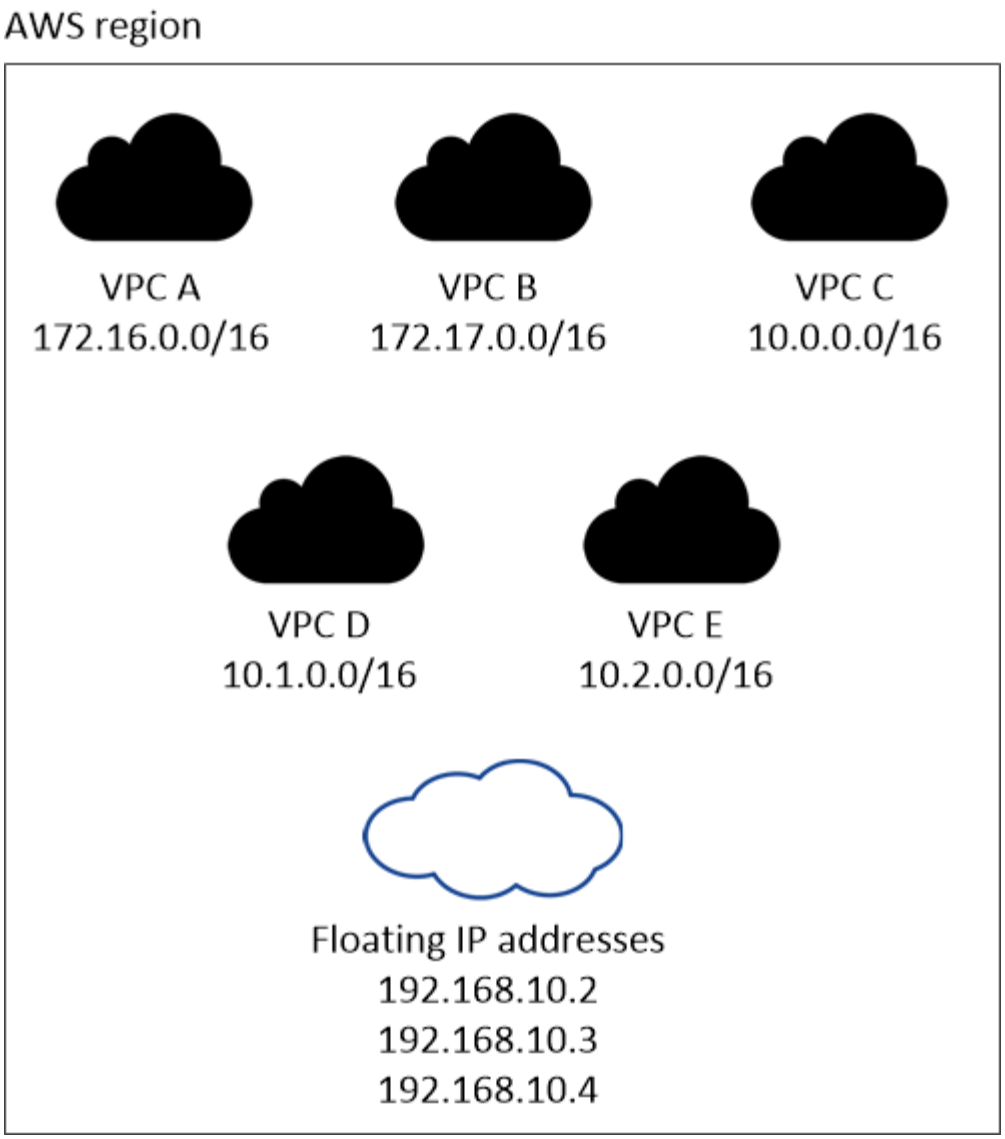
一個浮動 IP 位址是用於叢集管理、一個用於節點 1 上的 NFS/CIFS 資料、另一個用於節點 2 上的 NFS/CIFS 資料。SVM 管理的第四個浮動 IP 位址為選用項目。

> 如果您使用 SnapDrive 適用於 Windows 的 SHIP 或 SnapCenter 搭配 HA 配對的 SHIP 、則 SVM 管理 LIF 需要一個浮動 IP 位址。如果您在部署系統時未指定 IP 位址、您可以稍後建立 LIF 。如需詳細資訊、請參閱 "設定 Cloud Volumes ONTAP 功能"。

當您建立 Cloud Volumes ONTAP 一個發揮作用的環境時、需要在 Cloud Manager 中輸入浮動 IP 位址。Cloud Manager 會在 HA 配對啟動系統時、將 IP 位址分配給 HA 配對。

在部署 HA 組態的 AWS 區域中、所有 VPC 的浮動 IP 位址都必須位於 CIDR 區塊之外。將浮動 IP 位址視為位於您所在地區 VPC 外部的邏輯子網路。

下列範例顯示 AWS 區域中浮動 IP 位址與 VPC 之間的關係。雖然浮動 IP 位址位於所有 VPC 的 CIDR 區塊之外、但仍可透過路由表路由傳送至子網路。



Cloud Manager 會自動建立靜態 IP 位址、以供 iSCSI 存取及從 VPC 外部用戶端存取 NAS 。您不需要滿足這些類型 IP 位址的任何需求。

傳輸閘道、可從 **VPC** 外部啟用浮動 **IP** 存取

"設定 AWS 傳輸閘道" 可從 HA 配對所在的 VPC 外部存取 HA 配對的浮動 IP 位址。

路由表

在 Cloud Manager 中指定浮動 IP 位址之後、您必須選取路由表、其中應包含通往浮動 IP 位址的路由。這可讓用戶端存取 HA 配對。

如果 VPC 中只有一個子網路路由表（主路由表）、 Cloud Manager 會自動將浮動 IP 位址新增至該路由表。如果您有多個路由表、在啟動 HA 配對時、請務必選取正確的路由表。否則、部分用戶端可能無法存取 Cloud Volumes ONTAP 功能不完全。

例如、您可能有兩個子網路與不同的路由表相關聯。如果您選取路由表 A 而非路由表 B 、則與路由表 A 相關聯的子網路中的用戶端可以存取 HA 配對、但與路由表 B 相關的子網路中的用戶端則無法存取。

如需路由表的詳細資訊、請參閱 "AWS 文件：路由表"。

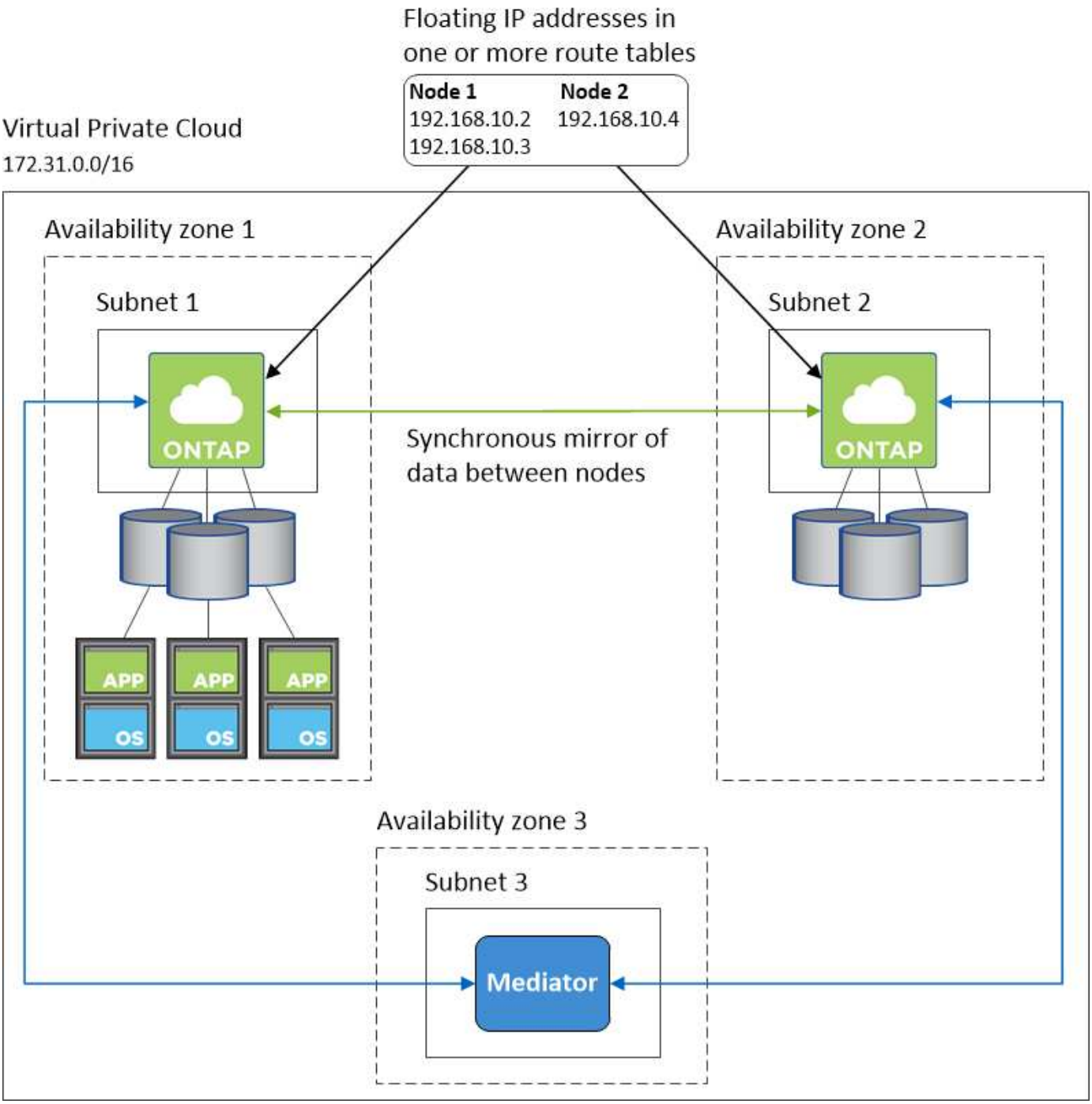
連線至 **NetApp** 管理工具

若要將 NetApp 管理工具搭配多個 AZs 中的 HA 組態使用、您有兩種連線選項：

1. 在不同的 VPC 和中部署 NetApp 管理工具 "設定 AWS 傳輸閘道"。閘道可讓您從 VPC 外部存取叢集管理介面的浮動 IP 位址。
2. 在與 NAS 用戶端相同的 VPC 中部署 NetApp 管理工具、其路由組態與 NAS 用戶端相似。

組態範例

下圖顯示 AWS 以主動 - 被動式組態運作時的最佳 HA 組態：



VPC組態範例

若要更深入瞭Cloud Volumes ONTAP 解如何在AWS中部署Cloud Manager和功能、您應該檢閱最常見的VPC組態。

- 具有公有和私有子網路及NAT裝置的VPC
- 具有私有子網路和VPN連線的VPC、可連線至您的網路

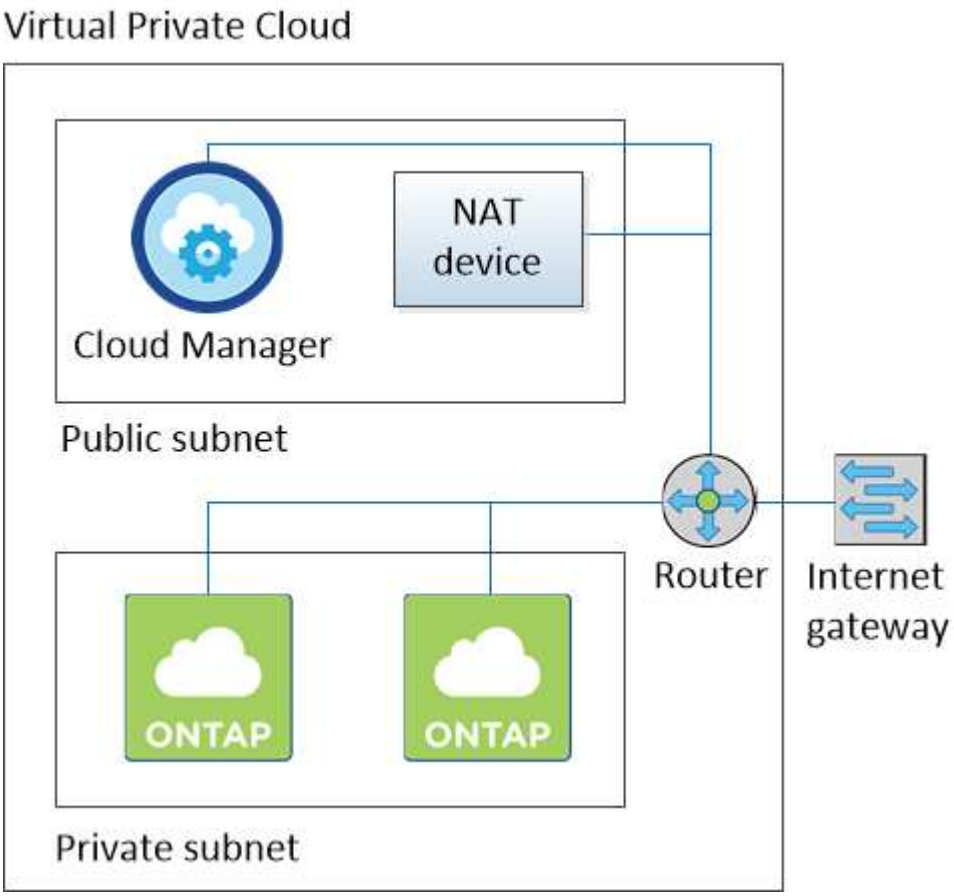
具有公有和私有子網路及**NAT**裝置的**VPC**

此VPC組態包括公有和私有子網路、將VPC連接至網際網路的網際網路閘道、以及在公有子網路中啟用傳出網際網路流量的NAT閘道或NAT執行個體。在此組態中、您可以在公有子網路或私有子網路中執行Cloud Manager、但建議使用公有子網路、因為它允許從VPC以外的主機存取。然後、您可以在Cloud Volumes ONTAP 私有子網路中啟動執行個體。

> 您可以使用HTTP Proxy來提供網際網路連線功能、而非使用NAT裝置。

如需此案例的詳細資訊、請參閱 "AWS文件：情境2：VPC搭配公有和私有子網路（NAT）"。

下圖顯示在公有子網路中執行的Cloud Manager、以及在私有子網路中執行的單一節點系統：



具有私有子網路和**VPN**連線的**VPC**、可連線至您的網路

這種VPC組態是混合雲組態、Cloud Volumes ONTAP 其中的功能是將效能提升到私有環境的延伸。此組態包括私有子網路和虛擬私有閘道、並可透過VPN連線至您的網路。透過VPN通道路由可讓EC2執行個體透過網路和防火牆存取網際網路。您可以在私有子網路或資料中心執行Cloud Manager。接著您會在Cloud Volumes ONTAP

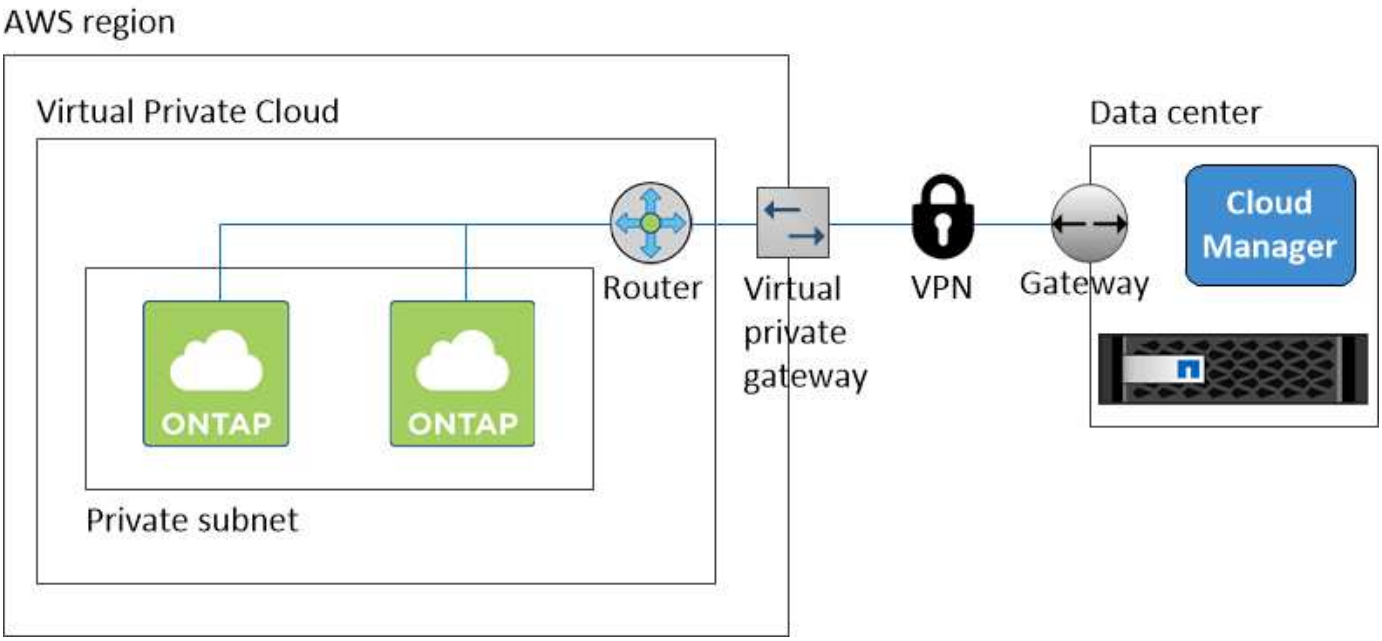
私有子網路中啟動效能不均。

> 您也可以在此組態中使用Proxy伺服器來允許網際網路存取。Proxy伺服器可以位於您的資料中心或AWS中。

如果您想要在FAS 資料中心的支援系統和Cloud Volumes ONTAP AWS的支援系統之間複寫資料、您應該使用VPN連線、以確保連結安全無虞。

如需此案例的詳細資訊、請參閱 "AWS文件：案例4：VPC僅含私有子網路和AWS託管VPN存取"。

下圖顯示在資料中心執行的Cloud Manager、以及在私有子網路中執行的單一節點系統：



在多個 **AZs** 中設定 **HA** 配對的 **AWS** 傳輸閘道

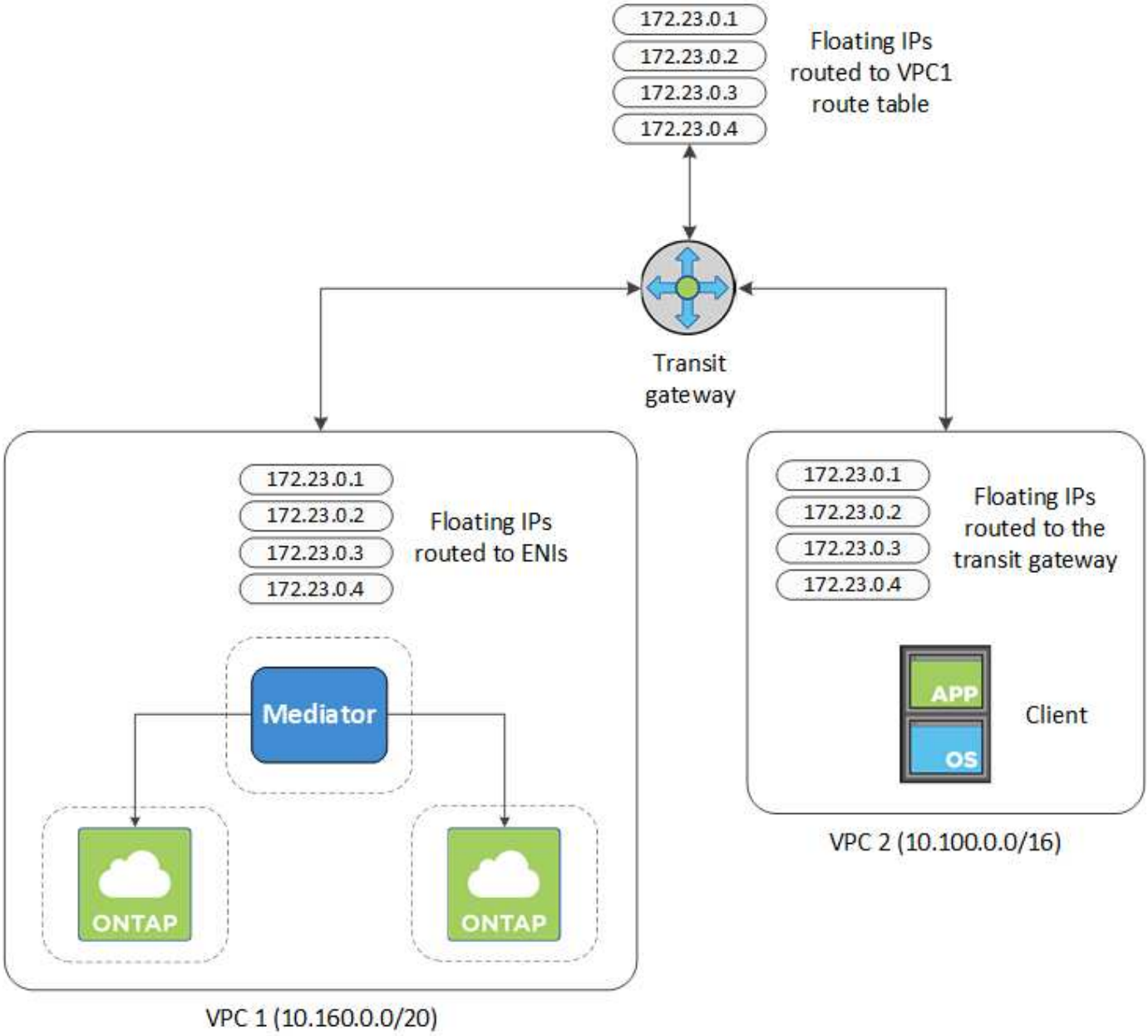
設定AWS傳輸閘道、以便從HA配對所在的VPC外部存取HA配對的浮動IP位址。

當某個靜態 HA 組態分佈於多個 AWS 可用區域時、從 VPC 內部存取 NAS 資料時、需要使用浮動 IP 位址。Cloud Volumes ONTAP當發生故障時、這些浮動 IP 位址可在節點之間移轉、但無法從 VPC 外部原生存取。獨立的私有 IP 位址可從 VPC 外部存取資料、但無法提供自動容錯移轉功能。

叢集管理介面和選用的 SVM 管理 LIF 也需要浮動 IP 位址。

如果您設定 AWS 傳輸閘道、就能從 HA 配對所在的 VPC 外部存取浮動 IP 位址。這表示 VPC 以外的 NAS 用戶端和 NetApp 管理工具可以存取浮動 IP 。

以下範例顯示兩個透過傳輸閘道連線的 VPC 。HA 系統位於一個 VPC 、而用戶端位於另一個 VPC 。然後、您可以使用浮動 IP 位址、在用戶端上掛載 NAS Volume 。

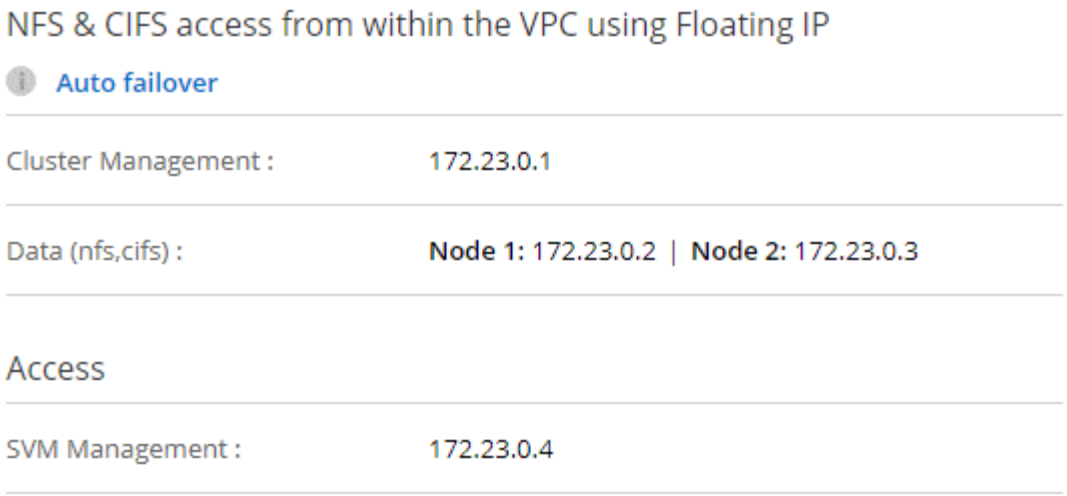


下列步驟說明如何設定類似的組態。

步驟

1. "建立傳輸閘道、並將 VPC 附加至閘道"。
2. 指定 HA 配對的浮動 IP 位址、在傳輸閘道的路由表中建立路由。

   您可以在 Cloud Manager 的「工作環境資訊」頁面找到浮動 IP 位址。範例如下：



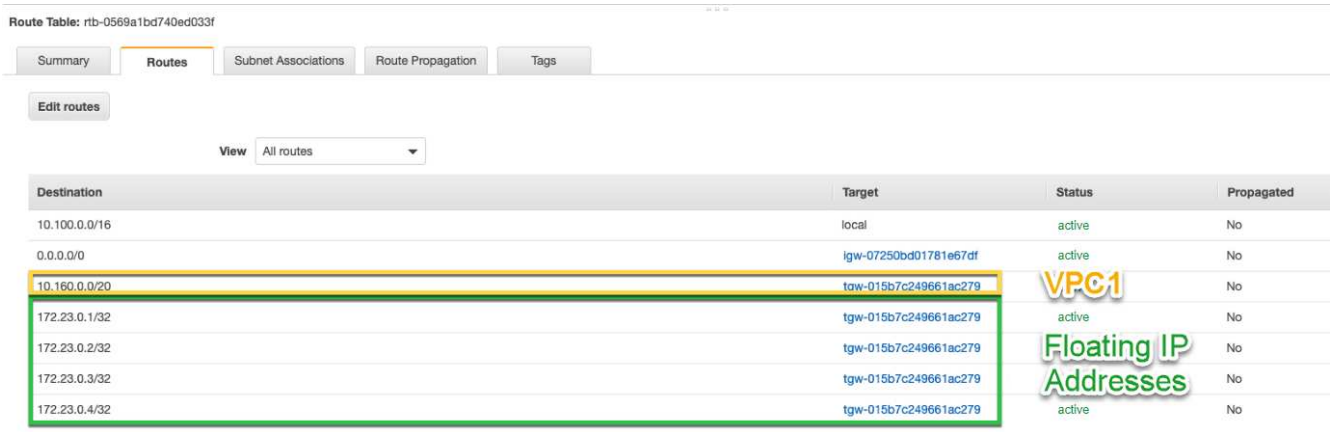
下列範例影像顯示傳輸閘道的路由表。其中包括兩部 VPC 的 CIDR 區塊路由、 Cloud Volumes ONTAP 以及由 R1 使用的四個浮動 IP 位址。

3. 修改需要存取浮動 IP 位址的 VPC 路由表。

   a. 新增路由項目至浮動 IP 位址。

   b. 將路由項目新增至 HA 配對所在 VPC 的 CIDR 區塊。

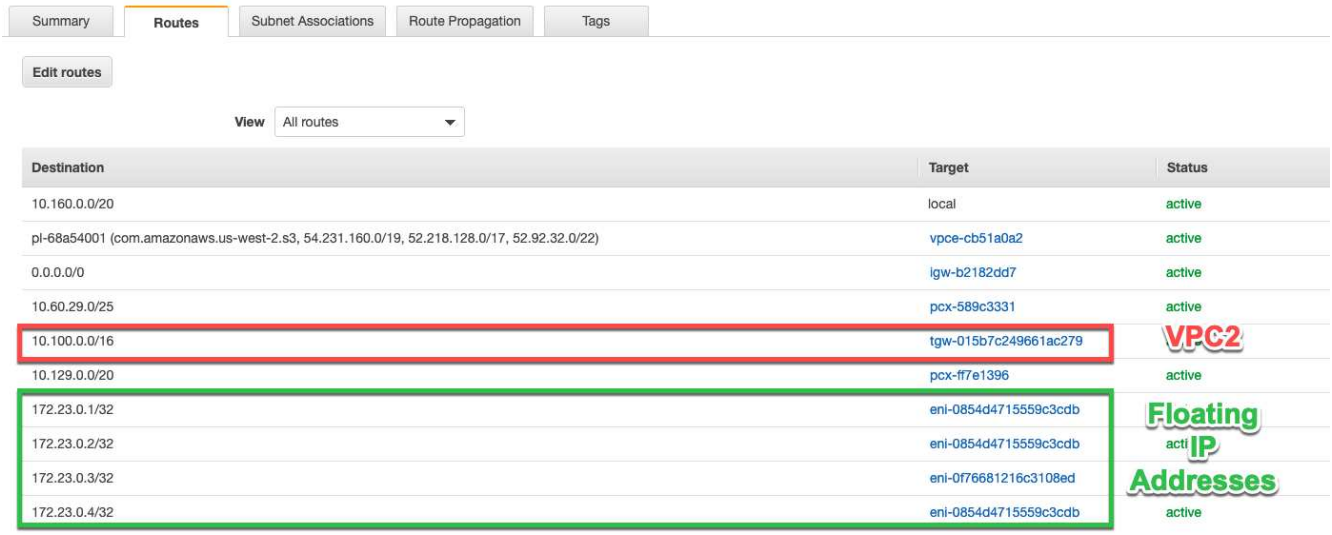
      下列範例影像顯示 VPC 2 的路由表、其中包括通往 VPC 1 的路由和浮動 IP 位址。



4. 將需要存取浮動 IP 位址的路由新增至 VPC 、以修改 HA 配對 VPC 的路由表。

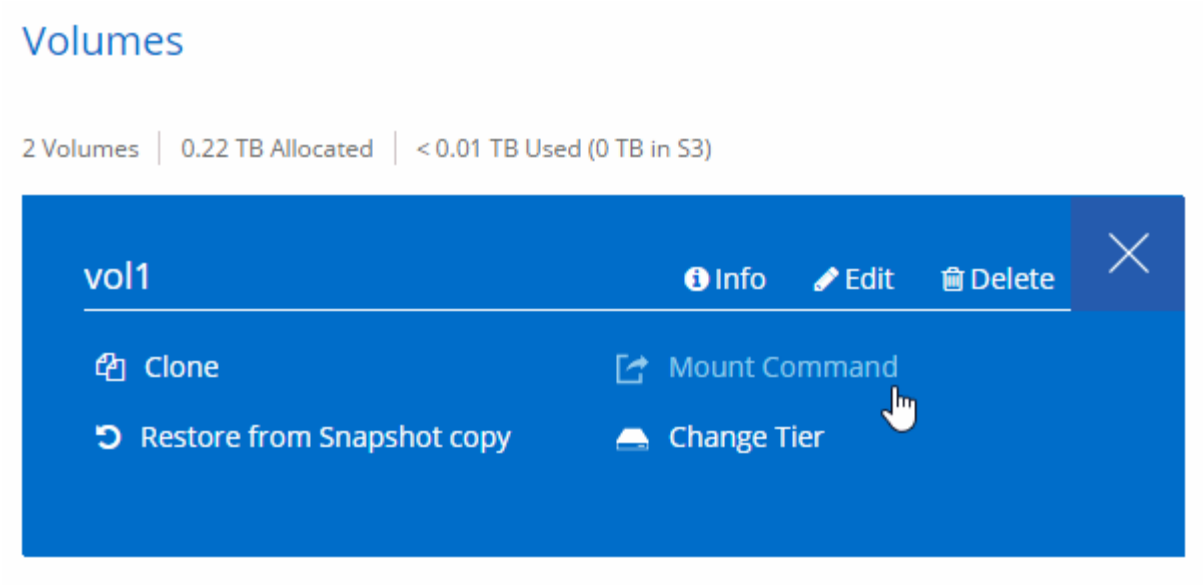
   此步驟非常重要、因為它會完成 VPC 之間的路由。

   下列範例影像顯示 VPC 1 的路由表。其中包括通往浮動 IP 位址和 VPC 2 的路由、而 VPC 2 是用戶端所在的位置。Cloud Manager 會在部署 HA 配對時、自動將浮動 IP 新增至路由表。



5. 使用浮動 IP 位址將磁碟區掛載到用戶端。

   您可以在 Cloud Manager 中找到正確的 IP 位址、方法是選取磁碟區、然後按一下 * Mount Command* 。



- 相關連結 *
- "AWS 中的高可用度配對"
- "AWS 的網路需求 Cloud Volumes ONTAP"

Azure 的網路需求 Cloud Volumes ONTAP

設定您的 Azure 網路、 Cloud Volumes ONTAP 使其能夠正常運作。

輸出網際網路存取 **Cloud Volumes ONTAP** 功能

支援向 NetApp 支援部門傳送訊息、以便主動監控儲存設備的健全狀況。 Cloud Volumes ONTAP AutoSupport

路由和防火牆原則必須允許將 HTTP / HTTPS 流量傳送至下列端點、 Cloud Volumes ONTAP 才能讓下列端點傳送 AutoSupport 動態訊息：

- https://support.netapp.com/aods/asupmessage
- https://support.netapp.com/asupprod/post/1.0/postAsup

安全性群組

您不需要建立安全性群組、因為 Cloud Manager 會為您建立安全性群組。如果您需要使用自己的、請參閱 "安全性群組規則"。

IP 位址數

Cloud Manager 會將下列 IP 位址分配給 Cloud Volumes ONTAP Azure 中的功能：

- 單一節點： 5 個 IP 位址
- HA 配對： 16 個 IP 位址

  請注意、 Cloud Manager 會在 HA 配對上建立 SVM 管理 LIF 、但不會在 Azure 中的單一節點系統上建立。

LIF 是與實體連接埠相關聯的 IP 位址。諸如 VMware 的管理工具需要 SVM 管理 LIF SnapCenter 。

從邊到 **Azure Blob** 儲存設備的連線 **Cloud Volumes ONTAP** 、可用於資料分層

如果您想要將冷資料分層至 Azure Blob 儲存設備、只要 Cloud Manager 具備必要的權限、就不需要在效能層與容量層之間建立連線。如果 Cloud Manager 原則具有下列權限、 Cloud Manager 可為您啟用 vnet 服務端點：

```
"Microsoft.Network/virtualNetworks/subnets/write",
"Microsoft.Network/routeTables/join/action",
```

這些權限包含在最新版本中 "Cloud Manager 原則"。

如需設定資料分層的詳細資訊、請參閱 "將冷資料分層至低成本物件儲存設備"。

連線 **ONTAP** 至其他網路中的不二系統

若要在 Cloud Volumes ONTAP Azure 中的某個更新系統與 ONTAP 其他網路中的其他更新系統之間複寫資料、您必須在 Azure vnet 與其他網路（例如 AWS VPC 或公司網路）之間建立 VPN 連線。

如需相關指示、請參閱 "Microsoft Azure 文件：在 Azure 入口網站中建立站台對站台連線"。

GCP 中的功能需求 Cloud Volumes ONTAP

設定您的 Google Cloud Platform 網路功能、 Cloud Volumes ONTAP 讓支援的系統能夠正常運作。

共享**VPC**

Cloud Manager與Cloud Volumes ONTAP 功能不受Google Cloud Platform共享VPC支援。

共享 VPC 可讓您設定及集中管理多個專案中的虛擬網路。您可以在_主機專案_中設定共享VPC網路、並在Cloud Volumes ONTAP _服務專案_中部署Cloud Manager與支援虛擬機器執行個體。 "Google Cloud 文件：共享 VPC 總覽"。

唯一的要求是在共享VPC主機專案中、為Cloud Manager服務帳戶提供下列權限：

compute。防火牆。* compute.networks.* compute。子網路。*

Cloud Manager 需要這些權限、才能查詢主機專案中的防火牆、 VPC 和子網路。

輸出網際網路存取 **Cloud Volumes ONTAP** 功能

支援向 NetApp 支援部門傳送訊息、以便主動監控儲存設備的健全狀況。 Cloud Volumes ONTAP AutoSupport

路由和防火牆原則必須允許將 HTTP / HTTPS 流量傳送至下列端點、 Cloud Volumes ONTAP 才能讓下列端點傳送 AutoSupport 動態訊息：

- https://support.netapp.com/aods/asupmessage

- https://support.netapp.com/asupprod/post/1.0/postAsup

IP 位址數

Cloud Manager會在Cloud Volumes ONTAP GCP中分配5個IP位址給功能不全的人。

請注意、Cloud Manager不會在Cloud Volumes ONTAP GCP中建立SVM管理LIF以供使用。

> LIF 是與實體連接埠相關聯的 IP 位址。諸如 VMware 的管理工具需要 SVM 管理 LIF SnapCenter 。

防火牆規則

您不需要建立防火牆規則、因為 Cloud Manager 能為您做到這一點。如果您需要使用自己的、請參閱 "GCP 防火牆規則"。

從 **Cloud Volumes ONTAP** 功能區連接到 **Google Cloud Storage** 、以利資料分層

如果您想要將冷資料分層至 Google Cloud Storage 資源桶、 Cloud Volumes ONTAP 則必須將駐留的子網路設定為私有 Google Access 。如需相關指示、請參閱 "Google Cloud 文件：設定私有 Google Access"。

如需在 Cloud Manager 中設定資料分層所需的其他步驟、請參閱 "將冷資料分層至低成本物件儲存設備"。

連線 **ONTAP** 至其他網路中的不二系統

若要在 Cloud Volumes ONTAP GCP 中的某個系統與 ONTAP 其他網路中的某個系統之間複寫資料、您必須在 VPC 與另一個網路（例如您的公司網路）之間建立 VPN 連線。

如需相關指示、請參閱 "Google Cloud 文件：雲端 VPN 概述"。

其他部署選項

Cloud Manager主機需求

如果您在自己的主機上安裝Cloud Manager、則必須驗證組態的支援、包括作業系統需求、連接埠需求等。

> 您可以在GCP的主機上安裝Cloud Manager、但不能安裝在內部部署網路中。Cloud Manager必須安裝在GCP中、才能在Cloud Volumes ONTAP GCP中部署。

需要專用主機

與其他應用程式共用的主機不支援Cloud Manager。主機必須是專屬主機。

支援的**AWS EC2**執行個體類型

- T2.medium
- T3.medium（建議）
- M4.Large
- M5.xLarge
- m5.2xLarge
- M5.4xLarge

- M5.8xLarge

支援的**Azure VM**大小

A2、D2 v2或D2 v3（視可用度而定）

支援的**GCP**機器類型

一種至少有2個vCPU和4 GB記憶體的機器類型。

支援的作業系統

- CentOS 7.2
- CentOS 7.3.
- CentOS 7.4.
- CentOS 7.5
- Red Hat Enterprise Linux 7.2
- Red Hat Enterprise Linux 7.3
- Red Hat Enterprise Linux 7.4
- Red Hat Enterprise Linux 7.5

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

  這些作業系統的英文版本支援Cloud Manager。

Hypervisor

通過認證可執行 CentOS 或 Red Hat Enterprise Linux 的裸機或託管Hypervisorhttps://access.redhat.com/certified-hypervisors["Red Hat 解決方案：哪些 Hypervisor 已通過認證、可執行 Red Hat Enterprise Linux ？"^]

CPU

2.27 GHz或更高、含兩個核心

RAM

4 GB

可用磁碟空間

50 GB

傳出網際網路存取

安裝Cloud Manager及使用Cloud Manager部署Cloud Volumes ONTAP 時、需要外傳網際網路存取功能。如需端點清單、請參閱 "Cloud Manager的網路需求"。

連接埠

下列連接埠必須可用：

- 80 （用於 HTTP 存取）
- 用於 HTTPS 存取的 443

- 適用於 Cloud Manager 資料庫的 3306
- 8080 for the Cloud Manager API Proxy

  如果其他服務使用這些連接埠、Cloud Manager安裝將會失敗。

  > 連接埠3306可能發生衝突。如果主機上正在執行另一個MySQL執行個體、則預設會使用連接埠3306。您必須變更現有MySQL執行個體使用的連接埠。

  安裝Cloud Manager時、您可以變更預設的HTTP和HTTPS連接埠。您無法變更MySQL資料庫的預設連接埠。如果您變更HTTP和HTTPS連接埠、則必須確保使用者能從遠端主機存取Cloud Manager Web主控台：

  - 修改安全性群組、允許透過連接埠進行傳入連線。
  - 輸入Cloud Manager網路主控台的URL時、請指定連接埠。

在現有的Linux主機上安裝Cloud Manager

部署Cloud Manager最常見的方法是從Cloud Central或雲端供應商的市場部署。但您可以選擇在網路或雲端的現有Linux主機上下載並安裝Cloud Manager軟體。

> 您可以在GCP的主機上安裝Cloud Manager、但不能安裝在內部部署網路中。Cloud Manager必須安裝在GCP中、才能在Cloud Volumes ONTAP GCP中部署。

開始之前

- Red Hat Enterprise Linux 系統必須在 Red Hat 訂購管理中註冊。如果尚未註冊、系統將無法在Cloud Manager安裝期間存取儲存庫來更新所需的協力廠商軟體。
- Cloud Manager安裝程式會在安裝程序期間存取多個URL。您必須確保允許這些端點存取傳出網際網路。請參閱 "Cloud Manager的網路需求"。

關於這項工作

- 安裝Cloud Manager不需要root權限。
- Cloud Manager會安裝AWS命令列工具（awscli）、以啟用NetApp支援的還原程序。

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

- NetApp 支援網站上提供的安裝程式可能是較早的版本。安裝完成後、Cloud Manager會在有新版本可用時自動更新。

步驟

1. 檢閱網路需求：
   - "Cloud Manager的網路需求"
   - "AWS 的網路需求 Cloud Volumes ONTAP"
   - "Azure 的網路需求 Cloud Volumes ONTAP"
   - "GCP 中的功能需求 Cloud Volumes ONTAP"
2. 檢閱 "Cloud Manager主機需求"。

3. 從下載軟體 "NetApp 支援網站"，然後將其複製到 Linux 主機。

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

4. 指派執行指令碼的權限。

   - 範例 *

```
 chmod +x OnCommandCloudManager-V3.7.0.sh
. 執行安裝指令碼：
```

```
./OnCommandCloudManager-V3.7.0.sh [silent] [proxy=ipaddress]
[proxyport=port] [proxyuser=user_name] [proxypwd=password]
```

   silon 在不提示您提供資訊的情況下執行安裝。

   如果Cloud Manager主機位於Proxy伺服器後方、則需要_proxy_。

   proxyport 是 Proxy 伺服器的連接埠。

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

proxyypwd 是您指定之使用者名稱的密碼。

5. 除非您指定無聲參數、否則請輸入 * Y* 繼續指令碼、然後在出現提示時輸入 HTTP 和 HTTPS 連接埠。

   如果您變更HTTP和HTTPS連接埠、則必須確保使用者能從遠端主機存取Cloud Manager Web主控台：

   - 修改安全性群組、允許透過連接埠進行傳入連線。
   - 輸入Cloud Manager網路主控台的URL時、請指定連接埠。

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

6. 開啟網頁瀏覽器並輸入下列 URL ：

   https://ipaddress:port

   _ipaddress_可以是localhost、私有IP位址或公有IP位址、視Cloud Manager主機的組態而定。例如、如果Cloud Manager位於沒有公有IP位址的公有雲中、您必須輸入與Cloud Manager主機連線的主機私有IP位址。

   如果您變更預設的 HTTP （ 80 ）或 HTTPS （ 443 ）連接埠、則必須使用 port 。例如、如果 HTTPS 連接埠變更為 8443 、您可以輸入 https://ipaddress:8443

7. 請在 NetApp Cloud Central 註冊或登入。

8. 登入之後、請設定 Cloud Manager ：
   a. 指定要與此Cloud Manager系統建立關聯的Cloud Central帳戶。

      "深入瞭解 Cloud Central 帳戶"。

   b. 輸入系統名稱。

完成後

設定權限、讓Cloud Manager能夠在Cloud Volumes ONTAP 雲端供應商中部署支援功能：

- AWS ： "設定 AWS 帳戶、然後將其新增至 Cloud Manager"。
- Azure ： "設定 Azure 帳戶、然後將其新增至 Cloud Manager"。
- GCP ：設定具有 Cloud Manager 所需權限的服務帳戶、以便在 Cloud Volumes ONTAP 專案中建立及管理各種系統。
  a. "在 GCP 中建立角色" 這包括在中定義的權限 "GCP 的 Cloud Manager 原則"。
  b. "建立 GCP 服務帳戶、並套用您剛建立的自訂角色"。
  c. "將此服務帳戶與Cloud Manager VM建立關聯"。
  d. 如果您想要在 Cloud Volumes ONTAP 其他專案中部署 "將具有 Cloud Manager 角色的服務帳戶新增至該專案、以授予存取權"。您必須針對每個專案重複此步驟。

從AWS Marketplace啟動Cloud Manager

最好使用AWS啟動Cloud Manager "NetApp Cloud Central"、但您可以視需要從AWS Marketplace啟動。

> 如果您從AWS Marketplace啟動Cloud Manager、Cloud Manager仍會與NetApp Cloud Central整合。 "深入瞭解整合"。

關於這項工作

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

步驟

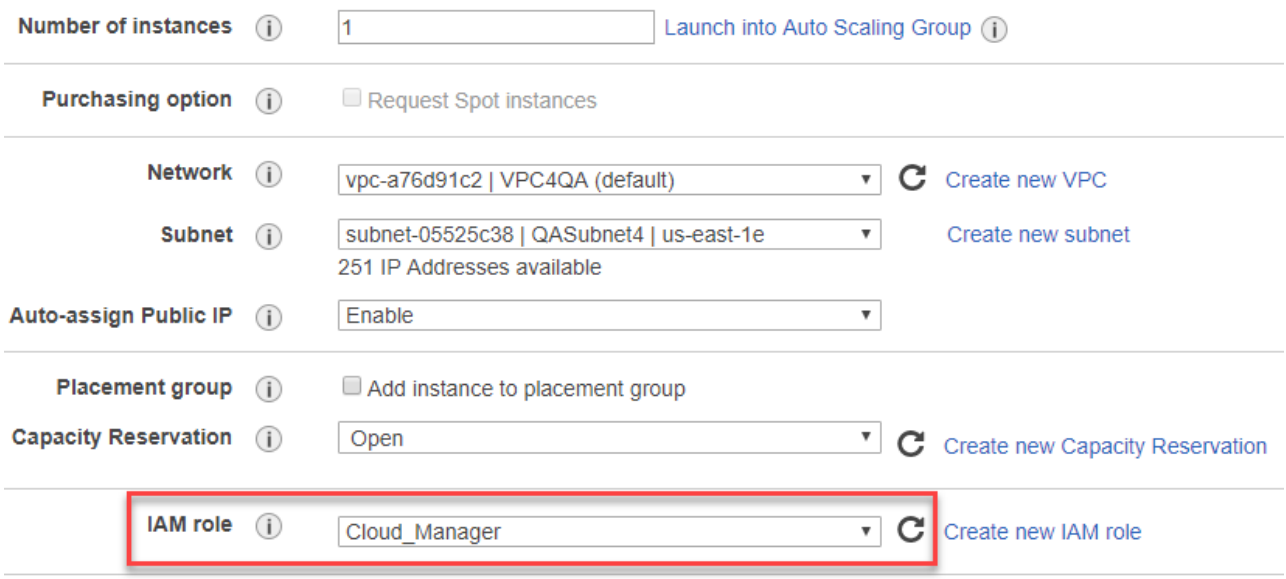
1. 為 EC2 執行個體建立 IAM 原則和角色：
   a. 請從下列位置下載 Cloud Manager IAM 原則：

      "NetApp Cloud Manager ： AWS 、 Azure 和 GCP 原則"

   b. 從 IAM 主控台複製並貼上 Cloud Manager IAM 原則中的文字、以建立您自己的原則。
   c. 建立角色類型為 Amazon EC2 的 IAM 角色、並將您在上一步建立的原則附加至角色。
2. "從AWS Marketplace訂閱" 確保在免費試用Cloud Volumes ONTAP 完VMware後、服務不會中斷。此訂閱將會針對 Cloud Volumes ONTAP 您所建立的每個更新版的 PAYGO 系統、以及您啟用的每個附加功能、向您收取費用。
3. 現在請前往 "AWS Marketplace 上的 Cloud Manager 頁面" 從 AMI 部署 Cloud Manager 。
4. 在 Marketplace 頁面上、按一下 * 繼續訂閱 * 、然後按一下 * 繼續進行組態 * 。
5. 變更任何預設選項、然後按一下 * 繼續啟動 * 。
6. 在「 * 選擇行動 * 」下、選取「 * 透過 EC2* 啟動」、然後按一下「 * 啟動 * 」。
7. 依照提示設定及部署執行個體：
   - 選擇執行個體類型：視地區可用度而定、請選擇其中一種支援的執行個體類型（建議使用T3.medium）。

     "檢閱支援的執行個體類型清單"。

   - 設定執行個體：選取VPC和子網路、您在步驟1中建立的IAM角色、以及符合您需求的其他組態選項。



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

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

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

   http://ipaddress:80

9. 登入之後、請設定 Cloud Manager ：
   a. 指定要與此Cloud Manager系統建立關聯的Cloud Central帳戶。

      "深入瞭解 Cloud Central 帳戶"。

   b. 輸入系統名稱。

結果

雲端管理程式現已安裝並設定完成。

從Azure Marketplace部署Cloud Manager

最好使用在Azure中部署Cloud Manager "NetApp Cloud Central"但您可以視需要從Azure Marketplace部署。

可在中部署Cloud Manager的個別指示 "Azure美國政府區域" 和 "Azure德國地區"。

> 如果您從Azure Marketplace部署Cloud Manager、Cloud Manager仍會與NetApp Cloud Central整合。 "深入瞭解整合"。

在Azure中部署Cloud Manager

您必須安裝並設定Cloud Manager、才能在Cloud Volumes ONTAP Azure中使用Cloud Manager來啟動功能。

步驟

1. "前往 Azure Marketplace for Cloud Manager 頁面"。
2. 按一下「 * 立即取得 * 」、然後按一下「 * 繼續 * 」。
3. 從 Azure 入口網站按一下 * 「 Create 」（建立） * 、然後依照步驟設定虛擬機器。

設定 VM 時請注意下列事項：

- Cloud Manager 可搭配 HDD 或 SSD 磁碟以最佳方式執行。
- 選擇建議的虛擬機器大小之一：A2、D2 v2或D2 v3（視可用度而定）。
- 對於網路安全群組、Cloud Manager需要使用SSH、HTTP和HTTPS的傳入連線。

  "深入瞭解Cloud Manager的安全群組規則"。

- 在「管理」下、選取「開啟」來啟用*系統指派的Cloud Manager託管身分識別*。

  這項設定非常重要、因為託管身分識別可讓Cloud Manager虛擬機器在Azure Active Directory中識別自己、而無需提供任何認證資料。 "深入瞭解 Azure 資源的託管身分識別"。

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

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

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

   http://ipaddress:80

6. 登入之後、請設定 Cloud Manager ：
   a. 指定要與此Cloud Manager系統建立關聯的Cloud Central帳戶。

      "深入瞭解 Cloud Central 帳戶"。

   b. 輸入系統名稱。

結果

雲端管理程式現已安裝並設定完成。您必須先授予 Azure 權限、使用者才能在 Cloud Volumes ONTAP Azure 中部署不必要的功能。

將Azure權限授予Cloud Manager

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

步驟

1. 使用 Cloud Manager 原則建立自訂角色：

   a. 下載 "Cloud Manager Azure 原則"。

   b. 將 Azure 訂閱 ID 新增至可指派的範圍、以修改 Json 檔案。

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

      - 範例 *

      「AssignableScopes」：[「/unorder/d333af45-0d07-4154-943d-c25fbzzzz」、「/unorder/54b91999-b3e6-4599-908e-416e0zzzz」、「/unuses/398e471c-3bzzz-4bez-4bez-4bez-4bz-4bz-4bz-4bz-4bz-4bz-4bz-4bz-4bz-4bz-4bz-4bez-

c. 使用 Json 檔案在 Azure 中建立自訂角色。

下列範例說明如何使用 Azure CLI 2.0 建立自訂角色：

- AZ角色定義建立：-role定義C：\Policy_for_cove_Manager_Azure _3.7.4.json*

現在您應該要有名為OnCommand 「Cloud Manager操作員」的自訂角色、可以指派給Cloud Manager虛擬機器。

2. 將角色指派給Cloud Manager虛擬機器以進行一或多項訂閱：
   a. 開啟 * 「訂閱」 * 服務、然後選取您要在其中部署 Cloud Volumes ONTAP 的訂閱。
   b. 按一下 * 存取控制（ IAM ） * 。
   c. 按一下「 * 新增 * > * 新增角色指派 * 」、然後新增權限：
      - 選擇* OnCommand 《Cloud Manager operator*》角色。

        中提供的預設名稱為「Cloud Manager操作員」OnCommand "Cloud Manager 原則"。如果您為角色選擇不同的名稱、請改為選取該名稱。

      - 指派 * 虛擬機器 * 的存取權。
      - 選取建立Cloud Manager虛擬機器的訂閱。
      - 選取Cloud Manager虛擬機器。
      - 按一下「 * 儲存 * 」。
   d. 如果您想要從 Cloud Volumes ONTAP 其他訂閱中部署、請切換至該訂閱、然後重複這些步驟。

結果

Cloud Manager現在擁有在Cloud Volumes ONTAP Azure中部署及管理功能所需的權限。

在Azure美國政府區域部署Cloud Manager

若要讓Cloud Manager在美國政府區域內正常運作、請先從Azure政府Marketplace部署Cloud Manager。然後提供Cloud Manager部署和管理Cloud Volumes ONTAP 功能所需的權限。

如需受支援Azure美國政府區域的清單、請參閱 "Cloud Volumes全球區域"。

從Azure美國政府市場部署Cloud Manager

Cloud Manager可在Azure US Government Marketplace中以映像形式提供。

步驟

1. 請確認您的訂閱已啟用Azure政府Marketplace：
   a. 以企業管理員身分登入入口網站。
   b. 瀏覽至*管理*。
   c. 在「註冊詳細資料」下、按一下「* Azure Marketplace *」旁邊的鉛筆圖示。

d. 選擇*已啟用*。

e. 按一下「 * 儲存 * 」。

"Microsoft Azure文件：Azure政府市場"

2. 在OnCommand Azure US政府入口網站中搜尋《解決方案與解決方案：

3. 按一下「建立」、然後依照步驟設定虛擬機器。

設定虛擬機器時請注意下列事項：

- Cloud Manager 可搭配 HDD 或 SSD 磁碟以最佳方式執行。
- 您應該選擇建議的虛擬機器大小之一：A2、D2 v2或D2 v3（視可用度而定）。
- 對於網路安全性群組、最好選擇*進階*。

  「進階」選項會建立新的安全性群組、其中包含Cloud Manager所需的傳入規則。如果您選擇「基本」、請參閱 "安全性群組規則" 以取得必要規則清單。

4. 在摘要頁面上、檢閱您的選擇、然後按一下「建立」開始部署。

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

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

http://ipaddress:80

6. 登入之後、請設定 Cloud Manager ：

a. 指定要與此Cloud Manager系統建立關聯的Cloud Central帳戶。

"深入瞭解 Cloud Central 帳戶"。

b. 輸入系統名稱。

結果

雲端管理程式現已安裝並設定完成。您必須先授予 Azure 權限、使用者才能在 Cloud Volumes ONTAP Azure 中部署不必要的功能。

使用託管身分識別、將**Azure**權限授予**Cloud Manager**

提供權限的最簡單方法是啟用 "託管身分識別" 在Cloud Manager虛擬機器上、然後將所需權限指派給虛擬機器。如有需要、另一種方法是 "使用服務主體授予Azure權限"。

步驟

1. 在Cloud Manager虛擬機器上啟用託管身分識別：
   a. 瀏覽至Cloud Manager虛擬機器、然後選取* Identity *。
   b. 按一下「系統指派」下的「開啟」、然後按一下「儲存」。
2. 使用 Cloud Manager 原則建立自訂角色：
   a. 下載 "Cloud Manager Azure 原則"。
   b. 將 Azure 訂閱 ID 新增至可指派的範圍、以修改 Json 檔案。

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

      - 範例 *

「 AssignableScopes 」：[「 /unorder/d333af45-0d07-4154-943d-c25fbzzzz 」、「 /unorder/54b91999-b3e6-4599-908e-416e0zzzz 」、「 /unuses/398e471c-3bzzz-4bez-4bez-4bez-4bz-4bz-4bz-4bz-4bz-4bz-4bz-4bz-4bz-4bz-4bz-4bez-

c. 使用 Json 檔案在 Azure 中建立自訂角色。

下列範例說明如何使用 Azure CLI 2.0 建立自訂角色：

- AZ角色定義建立：-role定義C：\Policy_for_cove_Manager_Azure _3.7.4.json*

現在您應該要有名為OnCommand 「Cloud Manager操作員」的自訂角色、可以指派給Cloud Manager虛擬機器。

3. 將角色指派給Cloud Manager虛擬機器以進行一或多項訂閱：

a. 開啟 * 「訂閱」 * 服務、然後選取您要在其中部署 Cloud Volumes ONTAP 的訂閱。

b. 按一下 * 存取控制（ IAM ） * 。

c. 按一下「新增」、按一下「新增角色指派」、然後新增權限：

- 選擇* OnCommand 《Cloud Manager operator*》角色。

> 中提供的預設名稱為「Cloud Manager操作員」OnCommand "Cloud Manager 原則"。如果您為角色選擇不同的名稱、請改為選取該名稱。

- 指派 * 虛擬機器 * 的存取權。
- 選取建立Cloud Manager虛擬機器的訂閱。
- 輸入虛擬機器的名稱、然後加以選取。
- 按一下「 * 儲存 * 」。

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

結果

Cloud Manager現在擁有在Cloud Volumes ONTAP Azure中部署及管理功能所需的權限。

在Azure Germany地區安裝Cloud Manager

Azure Marketplace不適用於Azure Germany地區、因此您必須從NetApp支援網站下載Cloud Manager安裝程式、並將其安裝在該地區現有的Linux主機上。

步驟

1. "檢閱Azure的網路需求"。
2. "檢閱Cloud Manager主機需求"。
3. "下載並安裝Cloud Manager"。
4. "使用服務主體將Azure權限授予Cloud Manager"。

完成後

Cloud Manager現在已準備好在Cloud Volumes ONTAP Azure Germany地區部署支援、就像其他地區一樣。不過、您可能需要先執行其他設定。

讓Cloud Manager保持正常運作

Cloud Manager應隨時保持執行狀態。

Cloud Manager是Cloud Volumes ONTAP 健全狀況和向客戶收費的關鍵要素。如果Cloud Manager關機、Cloud Volumes ONTAP 則在與Cloud Manager失去通訊超過4天之後、將會關閉此功能。