開始使用 **Google Cloud**

Cloud Volumes ONTAP

NetApp
February 26, 2026

目錄

開始使用 Google Cloud

Google Cloud 中的Cloud Volumes ONTAP快速入門

只需幾個步驟即可在 Google Cloud 中開始使用Cloud Volumes ONTAP 。

1 建立控制台代理

如果你沒有 "控制台代理"但是，你需要創建一個。 "了解如何在 Google Cloud 中建立控制台代理"

請注意，如果您想在沒有網路存取的子網路中部署Cloud Volumes ONTAP ，則需要手動安裝控制台代理程式並存取在該控制台代理程式上執行的NetApp Console。 "了解如何在沒有網路存取的地方手動安裝控制台代理"

2 規劃您的配置

控制台提供符合您的工作負載要求的預先配置包，或者您可以建立自己的配置。如果您選擇自己的配置，您應該了解可用的選項。

"了解有關規劃配置的更多信息" 。

3 設定網路

1. 確保您的 VPC 和子網路將支援控制台代理和Cloud Volumes ONTAP之間的連線。
2. 如果您打算啟用資料分層， "為私有 Google 存取權設定Cloud Volumes ONTAP子網路" 。
3. 如果您正在部署 HA 對，請確保您有四個 VPC，每個 VPC 都有自己的子網路。
4. 如果您使用共用 VPC，請向控制台代理服務帳戶提供_計算網路使用者_角色。
5. 為NetApp AutoSupport啟用從目標 VPC 的出站網際網路存取。

   如果您在沒有網路存取的位置部署Cloud Volumes ONTAP，則不需要執行此步驟。

"了解有關網絡要求的更多信息" 。

4 設定服務帳戶

Cloud Volumes ONTAP需要 Google Cloud 服務帳戶來實現兩個目的。第一個是當你啟用"資料分層"將冷資料分層到 Google Cloud 中的低成本物件儲存。第二個是當你啟用 "NetApp Backup and Recovery"將磁碟區備份到低成本的物件儲存。

您可以設定一個服務帳戶並將其用於兩種用途。服務帳戶必須具有*儲存管理員*角色。

"閱讀逐步說明" 。

5 啟用 **Google Cloud API**

"在您的專案中啟用 Google Cloud API". "這些 API"，您可能已經在建立 Console 代理時啟用了它們，這些是在 Google Cloud 中部署 Cloud Volumes ONTAP 所必需的。

6 使用控制台啟動**Cloud Volumes ONTAP**

按一下“新增系統”，選擇您想要部署的系統類型，然後完成精靈中的步驟。"閱讀逐步說明" 。

相關連結

- "建立控制台代理"
- "在 Linux 主機上安裝控制台代理軟體"
- "控制台代理的 Google Cloud 權限"

在 Google Cloud 中規劃您的Cloud Volumes ONTAP配置

在 Google Cloud 中部署Cloud Volumes ONTAP時，您可以選擇符合您的工作負載需求的預先設定係統，也可以建立自己的設定。如果您選擇自己的配置，您應該了解可用的選項。

選擇**Cloud Volumes ONTAP**許可證

Cloud Volumes ONTAP有多種授權選項。每個選項都可以讓您選擇符合您需求的消費模式。

- "了解Cloud Volumes ONTAP的授權選項"
- "了解如何設定許可"

選擇支援的區域

大多數 Google Cloud 區域支援Cloud Volumes ONTAP 。 "查看支援區域的完整列表" 。

選擇支援的機器類型

Cloud Volumes ONTAP支援多種機器類型，具體取決於您選擇的授權類型。

"Google Cloud 中 Cloud Volumes ONTAP 支援的組態"

了解儲存限制

Cloud Volumes ONTAP系統的原始容量限制與許可證相關。額外的限制會影響聚合和磁碟區的大小。在規劃配置時您應該注意這些限制。

"Google Cloud 中 Cloud Volumes ONTAP 的儲存限制"

在 **Google Cloud** 中調整系統大小

調整Cloud Volumes ONTAP系統的大小可以幫助您滿足效能和容量要求。在選擇機器類型、磁碟類型和磁碟大小時，您應該注意幾個關鍵點：

機器類型

請查看支援的機器類型。 "Cloud Volumes ONTAP發行說明"然後查看谷歌提供的關於每種受支援機器類型的詳細資訊。將您的工作負載需求與機器類型的 vCPU 和記憶體數量相符。請注意，每個 CPU 核心都會提高網路效能。

請參閱以下內容以了解更多詳細資訊：

- "Google Cloud 文件：N1 標準機器類型"
- "Google Cloud 文件：效能"

磁碟類型

為Cloud Volumes ONTAP建立磁碟區時，您需要選擇Cloud Volumes ONTAP用於磁碟的底層雲端儲存。磁碟類型可以是以下任一種：

- 區域 *SSD* 持久性磁碟：SSD 持久性磁碟最適合需要高隨機 IOPS 率的工作負載。
- 區域平衡持久性磁碟：這些 SSD 透過提供每 GB 較低的 IOPS 來平衡效能和成本。
- 區域標準持久磁碟：標準持久磁碟經濟實惠，可處理順序讀取/寫入作業。

  如欲了解更多詳情，請參閱 "Google Cloud 文件：區域持久性磁碟（標準和 SSD）"。

磁碟大小

部署Cloud Volumes ONTAP系統時，您需要選擇初始磁碟大小。之後，您可以讓NetApp Console為您管理系統的容量，但如果您想自行建立聚合，請注意以下事項：

- 聚合中的所有磁碟必須具有相同的大小。
- 確定所需的空間，同時考慮性能。
- 持久磁碟的效能會隨著磁碟大小和系統可用的 vCPU 數量自動擴展。

  請參閱以下內容以了解更多詳細資訊：

  - "Google Cloud 文件：區域持久性磁碟（標準和 SSD）"
  - "Google Cloud 文件：最佳化持久磁碟和本機 SSD 效能"

查看預設系統磁碟

除了用戶資料的儲存之外，控制台還購買了Cloud Volumes ONTAP系統資料（啟動資料、根資料、核心資料和NVRAM）的雲端儲存。出於規劃目的，在部署Cloud Volumes ONTAP之前查看這些詳細資訊可能會有所幫助。

- "查看 Google Cloud 中Cloud Volumes ONTAP系統資料的預設磁碟"。
- "Google Cloud 文件：雲端配額概述"

  Google Cloud Compute Engine 對資源使用實施配額，因此您應確保在部署Cloud Volumes ONTAP之前尚未達到限制。

控制台代理還需要係統磁碟。 "查看控制台代理預設配置的詳細信息"。

收集網路資訊

在 Google Cloud 中部署 Cloud Volumes ONTAP 時，您需要指定虛擬網路的詳細資訊。您可以使用工作表從管理員收集這些資訊。

單節點系統的網路資訊

Google Cloud 資訊	你的價值
地區	
區	
VPC 網路	
子網	
防火牆策略（如果使用您自己的）	

多個區域中 **HA** 對的網路資訊

Google Cloud 資訊	你的價值
地區	
節點 1 的區域	
節點 2 的區域	
調解員區域	
VPC-0 和子網	
VPC-1 和子網	
VPC-2 和子網	
VPC-3 和子網	
防火牆策略（如果使用您自己的）	

單一區域中 **HA** 對的網路資訊

Google Cloud 資訊	你的價值
地區	
區	
VPC-0 和子網	
VPC-1 和子網	
VPC-2 和子網	
VPC-3 和子網	
防火牆策略（如果使用您自己的）	

選擇寫入速度

控制台可讓您選擇Cloud Volumes ONTAP的寫入速度設置，但 Google Cloud 中的高可用性 (HA) 對除外。在選擇寫入速度之前，您應該了解正常設定和高設定之間的差異以及使用高寫入速度時的風險和建議。"了解有關寫入速度的更多信息" 。

選擇卷使用情況設定檔

ONTAP包含多種儲存效率功能，可減少您所需的總儲存量。在控制台中建立磁碟區時，您可以選擇啟用這些功能的設定檔或停用這些功能的設定檔。您應該了解有關這些功能的更多信息，以幫助您決定使用哪個配置文件。

NetApp儲存效率功能有以下優勢：

精簡配置

向主機或使用者提供比實體儲存池中實際擁有的更多的邏輯儲存。不是預先分配儲存空間，而是在寫入資料時動態地將儲存空間分配給每個磁碟區。

重複資料刪除

透過定位相同的資料塊並將其替換為對單一共享區塊的引用來提高效率。該技術透過消除駐留在同一磁碟區中的冗餘資料區塊來減少儲存容量需求。

壓縮

透過壓縮主儲存、輔助儲存和歸檔儲存磁碟區內的資料來減少儲存資料所需的實體容量。

為Cloud Volumes ONTAP設定 Google Cloud 網路

NetApp Console負責設定Cloud Volumes ONTAP的網路元件，例如 IP 位址、網路遮罩和路由。您需要確保可以存取外部網路、有足夠的私人 IP 位址、有正確的連線等等。

如果你想部署 HA 對，你應該"了解 HA 對在 Google Cloud 中的工作原理"。

Cloud Volumes ONTAP的要求

Google Cloud 必須滿足以下要求。

單節點系統的特定要求

如果要部署單節點系統、請確保您的網路符合下列要求。

一個 VPC

單節點系統需要一個虛擬私有雲（VPC）。

私人 IP 位址

對於 Google Cloud 中的單節點系統，Console 會將私人 IP 位址指派給下列各項：

- 節點
- 簇

- 儲存虛擬機
- 數據 NAS LIF
- 資料 iSCSI LIF

如果您使用 API 部署Cloud Volumes ONTAP並指定下列標誌，則可以跳過建立儲存虛擬機器 (SVM) 管理 LIF：

```
skipSvmManagementLif: true
```

LIF 是與實體連接埠關聯的 IP 位址。 SnapCenter等管理工具需要儲存虛擬機器 (SVM) 來管理 LIF。

HA 對的特定要求

如果要部署 HA 對，請確保您的網路符合以下要求。

一個或多個區域

您可以透過在多個區域或單一區域中部署 HA 配置來確保資料的高可用性。建立 HA 對時，控制台會提示您選擇多個區域或單一區域。

- 多區域（建議）

  跨三個區域部署 HA 配置可確保當一個區域內發生故障時資料仍然可用。請注意，與使用單一區域相比，寫入效能略低，但差異很小。

- 單區

  在單一區域中部署時， Cloud Volumes ONTAP HA 配置使用分散放置策略。此策略可確保 HA 配置免受區域內單點故障的影響，而無需使用單獨的區域來實現故障隔離。

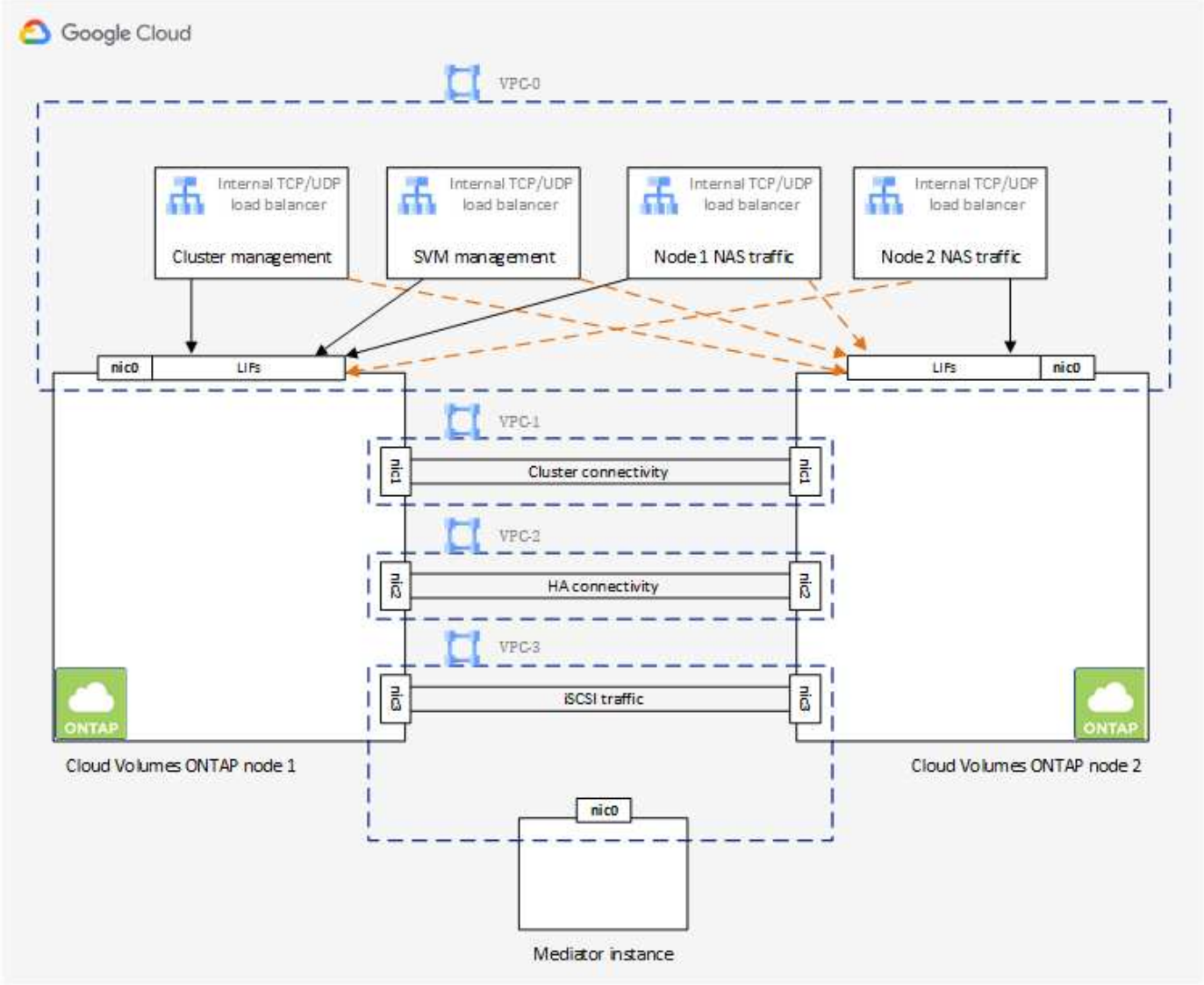
  這種部署模型確實降低了您的成本，因為區域之間沒有資料流出費用。

四個虛擬私有雲

HA 配置需要四個虛擬私有雲 (VPC)。需要四個 VPC，因為 Google Cloud 要求每個網路介面位於單獨的 VPC 網路中。

建立 HA 對時，控制台會提示您選擇四個 VPC：

- VPC-0 用於資料和節點的入站連接
- VPC-1、VPC-2 和 VPC-3 用於節點和 HA 中介之間的內部通信



子網

每個 VPC 都需要一個私有子網路。

如果將控制台代理程式放置在 VPC-0 中，則需要在子網路上啟用私人 Google 存取權限以存取 API 並啟用資料分層。

這些 VPC 中的子網路必須具有不同的 CIDR 範圍。它們不能有重疊的 CIDR 範圍。

私人 **IP** 位址

控制台會自動為 Google Cloud 中的Cloud Volumes ONTAP指派所需數量的私有 IP 位址。您需要確保您的網路有足夠的可用私有位址。

分配給 Cloud Volumes ONTAP 的 LIF 數量取決於您部署的是單節點系統還是 HA 配對。LIF 是與實體連接埠相關聯的 IP 位址。管理工具（例如 SnapCenter）需要 SVM 管理 LIF。

- 單節點 Console 會為單節點系統指派 4 個 IP 位址：
  - 節點管理 LIF

- 集群管理 LIF
- iSCSI 資料 LIF

  iSCSI LIF 透過 iSCSI 協定提供用戶端訪問，並被系統用於其他重要的網路工作流程。這些 LIF 是必需的，不應刪除。

- NAS LIF

  如果您使用 API 部署Cloud Volumes ONTAP並指定下列標誌，則可以跳過建立儲存虛擬機器 (SVM) 管理 LIF：

```
skipSvmManagementLif: true
```

- **HA** 對 控制台為 HA 對分配 12-13 個 IP 位址：
  - 2 個節點管理 LIF (e0a)
  - 1 集群管理 LIF (e0a)
  - 2 個 iSCSI LIF (e0a)

    iSCSI LIF 透過 iSCSI 協定提供用戶端訪問，並被系統用於其他重要的網路工作流程。這些 LIF 是必需的，不應刪除。

  - 1 或 2 個 NAS LIF (e0a)
  - 2 個集群 LIF (e0b)
  - 2 個 HA 互連 IP 位址 (e0c)
  - 2 個 RSM iSCSI IP 位址（e0d）

    如果您使用 API 部署Cloud Volumes ONTAP並指定下列標誌，則可以跳過建立儲存虛擬機器 (SVM) 管理 LIF：

```
skipSvmManagementLif: true
```

內部負載平衡器

控制台建立四個 Google Cloud 內部負載平衡器（TCP/UDP），用於管理傳入Cloud Volumes ONTAP HA 對的流量。您無需進行任何設定。我們將其列為一項要求只是為了告知您網路流量並減輕任何安全問題。

一個負載平衡器用於叢集管理，一個用於儲存虛擬機器 (SVM) 管理，一個用於到節點 1 的 NAS 流量，最後一個用於到節點 2 的 NAS 流量。

每個負載平衡器的設定如下：

- 一個共享的私人 IP 位址
- 一次全球健康檢查

  預設情況下，健康檢查使用的連接埠為63001、63002、63003。

- 一個區域 TCP 後端服務
- 一個區域 UDP 後端服務
- 一條 TCP 轉送規則
- 一條 UDP 轉送規則
- 全域存取已禁用

  儘管預設情況下會停用全域訪問，但支援在部署後啟用它。我們禁用它是因為跨區域流量會有明顯更高的延遲。我們希望確保您不會因為意外的跨區域坐騎而產生負面體驗。啟用此選項是為了滿足您的業務需求。

共享 **VPC**

Google Cloud 共享 VPC 和獨立 VPC 皆支援Cloud Volumes ONTAP和控制台代理。

對於單節點系統，VPC 可以是共用 VPC 或獨立 VPC。

對於 HA 對，需要四個 VPC。每個 VPC 可以是共享的，也可以是獨立的。例如，VPC-0 可以是共用 VPC，而 VPC-1、VPC-2 和 VPC-3 可以是獨立 VPC。

共用 VPC 可讓您跨多個專案配置和集中管理虛擬網路。您可以在_主機專案_中設定共用 VPC 網絡，並在_服務項目_中部署控制台代理程式和Cloud Volumes ONTAP虛擬機器實例。

"Google Cloud 文件：共享 VPC 概覽" 。

"查看控制台代理部署中涵蓋的所需共用 VPC 權限"

VPC 中的資料包鏡像

"資料包鏡像"必須在部署Cloud Volumes ONTAP的 Google Cloud 子網路中停用。

出站互聯網訪問

Cloud Volumes ONTAP系統需要出站網際網路存取才能存取外部端點以實現各種功能。如果這些端點在具有嚴格安全要求的環境中被阻止， Cloud Volumes ONTAP將無法正常運作。

控制台代理也會聯絡多個端點以進行日常操作。有關端點的信息，請參閱 "查看從控制台代理聯繫的端點"和 "準備好使用控制台的網絡"。

Cloud Volumes ONTAP端點

Cloud Volumes ONTAP使用這些端點與各種服務進行通訊。

端點	適用於	目的	部署模式	端點不可用時的影響
\ https://netapp-cloud-account.auth0.com	驗證	用於控制台中的身份驗證。	標準和限制模式。	用戶身份驗證失敗，以下服務仍然不可用： • Cloud Volumes ONTAP服務 • ONTAP服務 • 協定和代理服務
\ https://api.bluexp.netapp.com/tenancy	租賃	用於從控制台檢索Cloud Volumes ONTAP資源以授權資源和使用者。	標準和限制模式。	Cloud Volumes ONTAP資源和使用者未獲得授權。
\ https://mysupport.netapp.com/aods/asupmessage \ https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	用於將AutoSupport遙測資料傳送給NetApp支援。	標準和限制模式。	AutoSupport資訊仍未送達。

端點	適用於	目的	部署模式	端點不可用時的影響
https://cloudbuild.googleapis.com/v1（僅適用於私有模式部署）https://cloudkms.googleapis.com/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://compute.googleapis.com/compute/v1 https://www.googleapis.com/compute/beta https://www.googleapis.com/compute/v1/projects/ https://www.googleapis.com/deploymentmanager/v2/projects https://www.googleapis.com/storage/v1 https://www.googleapis.com/upload/storage/v1 https://config.googleapis.com/v1 https://iam.googleapis.com/v1 https://storage.googleapis.com/storage/v1	Google Cloud（商業用途）。	與 Google Cloud 服務通訊。	標準、受限和私人模式。	Cloud Volumes ONTAP無法與 Google Cloud 服務通訊以對 Google Cloud 中的控制台執行特定操作。

與其他網路中的**ONTAP**系統的連接

要在 Google Cloud 中的Cloud Volumes ONTAP系統和其他網路中的ONTAP系統之間複製數據，您必須在 VPC 和其他網路（例如您的公司網路）之間建立 VPN 連線。

"Google Cloud 文件：Cloud VPN 概覽" 。

防火牆規則

控制台建立 Google Cloud 防火牆規則，其中包含Cloud Volumes ONTAP成功運作所需的入站和出站規則。您可能希望參考連接埠以進行測試，或者您喜歡使用自己的防火牆規則。

Cloud Volumes ONTAP的防火牆規則需要入站和出站規則。如果您正在部署 HA 配置，這些是 VPC-0 中Cloud Volumes ONTAP的防火牆規則。

請注意，HA 配置需要兩組防火牆規則：

- 針對 VPC-0 中的 HA 組件的一組規則。這些規則允許對Cloud Volumes ONTAP進行資料存取。
- 針對 VPC-1、VPC-2 和 VPC-3 中的 HA 組件的另一組規則。這些規則對於 HA 組件之間的入站和出站通訊開放。了解更多 。

正在尋找有關控制台代理的資訊？ "查看控制台代理的防火牆規則"

入站規則

新增Cloud Volumes ONTAP系統時，您可以在部署期間選擇預先定義防火牆策略的來源篩選器：

- 僅限選定的 **VPC**：入站流量的來源過濾器是Cloud Volumes ONTAP系統的 VPC 子網路範圍和控制台代理程式所在的 VPC 子網路範圍。這是推薦的選項。
- 所有 **VPC**：入站流量的來源過濾器是 0.0.0.0/0 IP 範圍。

如果您使用自己的防火牆策略，請確保新增所有需要與Cloud Volumes ONTAP通訊的網絡，同時也要確保新增兩個位址範圍以允許內部 Google 負載平衡器正常運作。這些位址是 130.211.0.0/22 和 35.191.0.0/16。欲了解更多信息，請參閱 "Google Cloud 文件：負載平衡器防火牆規則"。

協定	港口	目的
所有 ICMP	全部	對執行個體執行 ping 操作
HTTP	80	使用叢集管理 LIF 的 IP 位址透過 HTTP 存取ONTAP System Manager Web 控制台
HTTPS	443	使用叢集管理 LIF 的 IP 位址與控制台代理程式建立連線並透過 HTTPS 存取ONTAP System Manager Web 控制台
SSH	22	透過 SSH 存取叢集管理 LIF 或節點管理 LIF 的 IP 位址
TCP	111	NFS 的遠端過程調用
TCP	139	CIFS 的 NetBIOS 服務會話
TCP	161-162	簡單網路管理協議
TCP	445	使用 NetBIOS 框架的 TCP 上的 Microsoft SMB/CIFS
TCP	635	NFS 掛載
TCP	749	Kerberos
TCP	2049	NFS 伺服器守護程式
TCP	3260	透過 iSCSI 資料 LIF 進行 iSCSI 訪問
TCP	4045	NFS 鎖守護程式
TCP	4046	NFS 網路狀態監視器
TCP	10000	使用 NDMP 備份
TCP	11104	SnapMirror群集間通訊會話的管理
TCP	11105	使用集群間 LIF 進行SnapMirror資料傳輸
TCP	63001-63050	負載平衡探測端口以確定哪個節點是健康的（僅 HA 對需要）

協定	港口	目的
UDP	111	NFS 的遠端過程調用
UDP	161-162	簡單網路管理協議
UDP	635	NFS 掛載
UDP	2049	NFS 伺服器守護程式
UDP	4045	NFS 鎖守護程式
UDP	4046	NFS 網路狀態監視器
UDP	4049	NFS rquotad 協議

出站規則

Cloud Volumes ONTAP的預設安全群組開啟所有出站流量。如果可以接受，請遵循基本的出站規則。如果您需要更嚴格的規則，請使用進階出站規則。

基本出站規則

Cloud Volumes ONTAP的預設安全群組包括以下出站規則。

協定	港口	目的
所有 ICMP	全部	所有出站流量
所有 TCP	全部	所有出站流量
所有 UDP	全部	所有出站流量

高級出站規則

如果您需要對出站流量製定嚴格的規則，則可以使用下列資訊僅開啟Cloud Volumes ONTAP出站通訊所需的連接埠。 Cloud Volumes ONTAP叢集使用下列連接埠來調節節點流量。

來源是Cloud Volumes ONTAP系統的介面（IP 位址）。

服務	協定	港口	來源	目的地	目的
活動目錄	TCP	88	節點管理 LIF	Active Directory 林	Kerberos V 驗證
	UDP	137	節點管理 LIF	Active Directory 林	NetBIOS 名稱服務
	UDP	138	節點管理 LIF	Active Directory 林	NetBIOS 資料封包服務
	TCP	139	節點管理 LIF	Active Directory 林	NetBIOS 服務會話
	TCP 和 UDP	389	節點管理 LIF	Active Directory 林	LDAP
	TCP	445	節點管理 LIF	Active Directory 林	使用 NetBIOS 框架的 TCP 上的 Microsoft SMB/CIFS
	TCP	464	節點管理 LIF	Active Directory 林	Kerberos V 更改和設定密碼（SET_CHANGE）
	UDP	464	節點管理 LIF	Active Directory 林	Kerberos 金鑰管理
	TCP	749	節點管理 LIF	Active Directory 林	Kerberos V 更改和設定密碼（RPCSEC_GSS）
	TCP	88	資料 LIF（NFS、CIFS、iSCSI）	Active Directory 林	Kerberos V 驗證
	UDP	137	資料 LIF（NFS、CIFS）	Active Directory 林	NetBIOS 名稱服務
	UDP	138	資料 LIF（NFS、CIFS）	Active Directory 林	NetBIOS 資料封包服務
	TCP	139	資料 LIF（NFS、CIFS）	Active Directory 林	NetBIOS 服務會話
	TCP 和 UDP	389	資料 LIF（NFS、CIFS）	Active Directory 林	LDAP
	TCP	445	資料 LIF（NFS、CIFS）	Active Directory 林	使用 NetBIOS 框架的 TCP 上的 Microsoft SMB/CIFS
	TCP	464	資料 LIF（NFS、CIFS）	Active Directory 林	Kerberos V 更改和設定密碼（SET_CHANGE）
	UDP	464	資料 LIF（NFS、CIFS）	Active Directory 林	Kerberos 金鑰管理
	TCP	749	資料 LIF（NFS、CIFS）	Active Directory 林	Kerberos V 更改和設定密碼（RPCSEC_GSS）
AutoSupport	HTTPS	443	節點管理 LIF	mysupport.netapp.com	AutoSupport （預設為 HTTPS）
	HTTP	80	節點管理 LIF	mysupport.netapp.com	AutoSupport （僅當傳輸協定從 HTTPS 變更為 HTTP 時）
	TCP	3128	節點管理 LIF	控制台代理	如果出站網路連線不可用，則透過控制台代理上的代理伺服器傳送AutoSupport訊息

服務	協定	港口	來源	目的地	目的
配置備份	HTTP	80	節點管理 LIF	http://<控制台代理 IP 位址>/occm/offboxconfig	將配置備份傳送到控制台代理程式。"ONTAP文檔"
DHCP	UDP	68	節點管理 LIF	DHCP	DHCP 用戶端首次設定
DHCP服務	UDP	67	節點管理 LIF	DHCP	DHCP 伺服器
DNS	UDP	53	節點管理 LIF 和資料 LIF（NFS、CIFS）	DNS	DNS
NDMP	TCP	18600–18699	節點管理 LIF	目標伺服器	NDMP 拷貝
SMTP	TCP	25	節點管理 LIF	郵件伺服器	SMTP 警報，可用於AutoSupport
SNMP	TCP	161	節點管理 LIF	監控伺服器	透過 SNMP 陷阱進行監控
	UDP	161	節點管理 LIF	監控伺服器	透過 SNMP 陷阱進行監控
	TCP	162	節點管理 LIF	監控伺服器	透過 SNMP 陷阱進行監控
	UDP	162	節點管理 LIF	監控伺服器	透過 SNMP 陷阱進行監控
SnapMirror	TCP	11104	集群間 LIF	ONTAP叢集間 LIF	SnapMirror群集間通訊會話的管理
	TCP	11105	集群間 LIF	ONTAP叢集間 LIF	SnapMirror資料傳輸
系統日誌	UDP	514	節點管理 LIF	Syslog伺服器	Syslog 轉送訊息

VPC-1、**VPC-2** 和 **VPC-3** 的規則

在 Google Cloud 中，HA 配置部署在四個 VPC 中。 VPC-0 中的 HA 設定所需的防火牆規則是以上所列的Cloud Volumes ONTAP。

同時，為 VPC-1、VPC-2 和 VPC-3 中的執行個體所建立的預定義防火牆規則支援透過所有協定和連接埠進行入站通訊。這些規則支援 HA 節點之間的通訊。

從 HA 節點到 HA 中介的通訊透過連接埠 3260（iSCSI）進行。

> 為了讓新的 Google Cloud HA 對部署實現較高的寫入速度，VPC-1、VPC-2 和 VPC-3 需要至少 8,896 位元組的最大傳輸單元 (MTU)。如果您選擇將現有的 VPC-1、VPC-2 和 VPC-3 升級到 8,896 位元組的 MTU，則必須在設定過程中關閉使用這些 VPC 的所有現有 HA 系統。

私有模式部署的 **Infrastructure Manager** 組態

如果您想要以私有模式部署 Cloud Volumes ONTAP 9.16.1 或更高版本，則需要進行一些設定變更，以便 Cloud Volumes ONTAP 可以使用 Google Cloud Infrastructure Manager 作為部署服務，而不是 Google 最終將棄用的 Deployment Manager。

開始之前

- 請確保您的 Cloud Volumes ONTAP 系統版本為 9.16.1 或更高版本。如果不是，請升級您的系統。有關說明，請參閱 "升級Cloud Volumes ONTAP"。
- 請確保已啟用 Google Cloud API。請參閱 "啟用 Google Cloud API"。
- 請確保已啟用 Cloud Build API。請參閱 "在此處啟用 Cloud Build API"。
- 確認 Console 代理程式的服務帳戶擁有所有標準權限。此外，請確保該服務帳戶擁有 `cloudbuild.workerpools.get`和 `cloudbuild.workerpools.list`權限。請參閱 "控制台代理的 Google Cloud 權限"。

步驟

1. 使用此配置在與 Cloud Volumes ONTAP 部署相同的區域中建立私有工作池。有關建立私有工作池的資訊，請參閱 "Google Cloud 文件：建立和管理私有資源池"和 "Google Cloud Build 定價"。

   工作池必須具有以下配置：

   - 機器類型：e2-medium
   - 磁碟大小：100 GB
   - 指派外部 IP：False
   - 網路：預設或專用網路。
   - 已配置子網路以存取 "Google API"。請執行以下步驟以確保子網路可以存取 Google API：
     i. 請確保已為子網路啟用「Private Google Access」。
     ii. 前往 **VPC Network** 層級 **> Private Service Access** 標籤 **> Allocated IP ranges for services**。
     iii. 選擇 **Allocate IP range** 並為與 Google Compute Service 的私有連線分配內部 IP 範圍。
     iv. 在 **Private connection to services** 中，選擇 **Create Connection**。
     v. 選擇 **Connected service producer = Google Cloud Platform**。
     vi. 為上一個步驟中建立的私人連線 IP 範圍指派配置。
2. 部署此工作池並保持其運行，以進行 Cloud Volumes ONTAP 管理。Google Cloud 使用此工作池在隔離環境中執行所有 Terraform 操作。
3. 以私有模式部署 Cloud Volumes ONTAP 時，請在 **GCP Worker Pool** 欄位中選擇此工作池的名稱。請參閱 "在 Google Cloud 啟動Cloud Volumes ONTAP" 以取得相關說明。

控制台代理的要求

如果您尚未建立控制台代理，則應查看網路需求。

- "查看控制台代理程式的網路要求"
- "Google Cloud 中的防火牆規則"

支援控制台代理的網路配置

您可以使用為控制台代理程式設定的代理伺服器來啟用來自Cloud Volumes ONTAP存取。控制台支援兩種類型的代理：

- 明確代理：來自Cloud Volumes ONTAP 的出站流量使用控制台代理代理程式設定期間指定的代理伺服器的

HTTP 位址。控制台代理管理員可能還配置了使用者憑證和根 CA 憑證以進行額外的驗證。Cloud Volumes ONTAP顯式代理程式有可用的根 CA 證書，請確保使用 "ONTAP CLI：安全性憑證安裝"命令。

- 透明代理：網路配置為透過控制台代理代理程式自動路由來自Cloud Volumes ONTAP 的出站流量。設定透明代理程式時，控制台代理程式管理員僅需要提供用於從Cloud Volumes ONTAP進行連接的根 CA 證書，而不是代理伺服器的 HTTP 位址。確保使用以下方式取得相同的根 CA 憑證並將其上傳到您的Cloud Volumes ONTAP系統 "ONTAP CLI：安全性憑證安裝"命令。

有關為控制台代理程式配置代理伺服器的信息，請參閱 "配置控制台代理以使用代理伺服器"。

在 **Google Cloud** 中為**Cloud Volumes ONTAP**設定網路標籤

在控制台代理程式的透明代理程式配置期間，管理員會為 Google Cloud 新增網路標籤。您需要取得並手動新增Cloud Volumes ONTAP配置的相同網路標籤。此標籤對於代理伺服器正常運作是必要的。

1. 在 Google Cloud Console 中、找到您的 Cloud Volumes ONTAP 系統。
2. 前往*詳細資料>網路>網路標籤*。
3. 新增用於控制台代理的標籤並儲存配置。

相關主題

- "驗證Cloud Volumes ONTAP 的AutoSupport設置"
- "了解ONTAP內部端口" 。

設定 VPC 服務控制以在 Google Cloud 中部署Cloud Volumes ONTAP

當選擇使用 VPC 服務控制鎖定您的 Google Cloud 環境時，您應該了解NetApp Console和Cloud Volumes ONTAP如何與 Google Cloud API 交互，以及如何配置您的服務邊界以部署控制台和Cloud Volumes ONTAP。

VPC 服務控制使您能夠控制對受信任邊界之外的 Google 管理服務的訪問，阻止來自不受信任位置的資料訪問，並降低未經授權的資料傳輸風險。 "詳細了解 Google Cloud VPC 服務控制" 。

NetApp服務如何與 VPC 服務控制進行通訊

控制台直接與 Google Cloud API 通訊。這可以從 Google Cloud 外部的外部 IP 位址觸發（例如，來自 api.services.cloud.netapp.com），也可以從 Google Cloud 內部指派給控制台代理程式的內部位址觸發。

根據控制台代理程式的部署方式，您的服務邊界可能需要做出某些例外。

圖片

Cloud Volumes ONTAP 和 Console 都使用來自 Google Cloud 內由 NetApp 管理的專案中的映像。如果您的組織有政策阻止使用非組織內部託管的映像，這可能會影響 Console 代理程式和 Cloud Volumes ONTAP 的部署。

您可以使用手動安裝方法手動部署控制台代理，但Cloud Volumes ONTAP也需要從NetApp專案中擷取映像。您必須提供允許清單才能部署控制台代理程式和Cloud Volumes ONTAP。

部署控制台代理

部署控制台代理程式的使用者需要能夠引用 projectId 為 *netapp-cloudmanager* 且專案編號為 *14190056516* 中所託管的映像。

部署**Cloud Volumes ONTAP**

- 控制台服務帳戶需要引用服務項目中託管在 projectId *netapp-cloudmanager* 中的映像和項目編號 *14190056516*。
- 預設 Google API 服務代理程式的服務帳戶需要引用服務項目中 projectId *netapp-cloudmanager* 和項目編號 *14190056516* 中託管的圖片。

下面定義了使用 VPC 服務控制拉取這些影像所需的規則範例。

VPC 服務控制邊界策略

策略允許對 VPC Service Controls 規則集設定例外。有關策略的更多資訊，請造訪 "Google Cloud VPC Service Controls 政策文件"。

若要設定控制台所需的策略，請導覽至您組織內的 VPC 服務控制邊界並新增下列策略。這些欄位應與 VPC 服務控制策略頁面中給出的選項相符。也要注意，*所有*規則都是必需的，並且規則集中應該使用*OR*參數。

入口規則

```
From:
    Identities:
        [User Email Address]
    Source > All sources allowed
To:
    Projects =
        [Service Project]
    Services =
        Service name: iam.googleapis.com
          Service methods: All actions
        Service name: compute.googleapis.com
          Service methods:All actions
```

或者

```
From:
    Identities:
        [User Email Address]
    Source > All sources allowed
To:
    Projects =
        [Host Project]
    Services =
        Service name: compute.googleapis.com
          Service methods: All actions
```

或者

```
From:
    Identities:
        [Service Project Number]@cloudservices.gserviceaccount.com
    Source > All sources allowed
To:
    Projects =
        [Service Project]
        [Host Project]
    Services =
        Service name: compute.googleapis.com
        Service methods: All actions
```

出口規則

```
From:
    Identities:
        [Service Project Number]@cloudservices.gserviceaccount.com
To:
    Projects =
        14190056516
    Service =
        Service name: compute.googleapis.com
        Service methods: All actions
```

上面列出的項目編號是NetApp用於儲存控制台代理程式和Cloud Volumes ONTAP 的圖像的專案 *netapp-cloudmanager*。

為Cloud Volumes ONTAP建立 Google Cloud 服務帳號

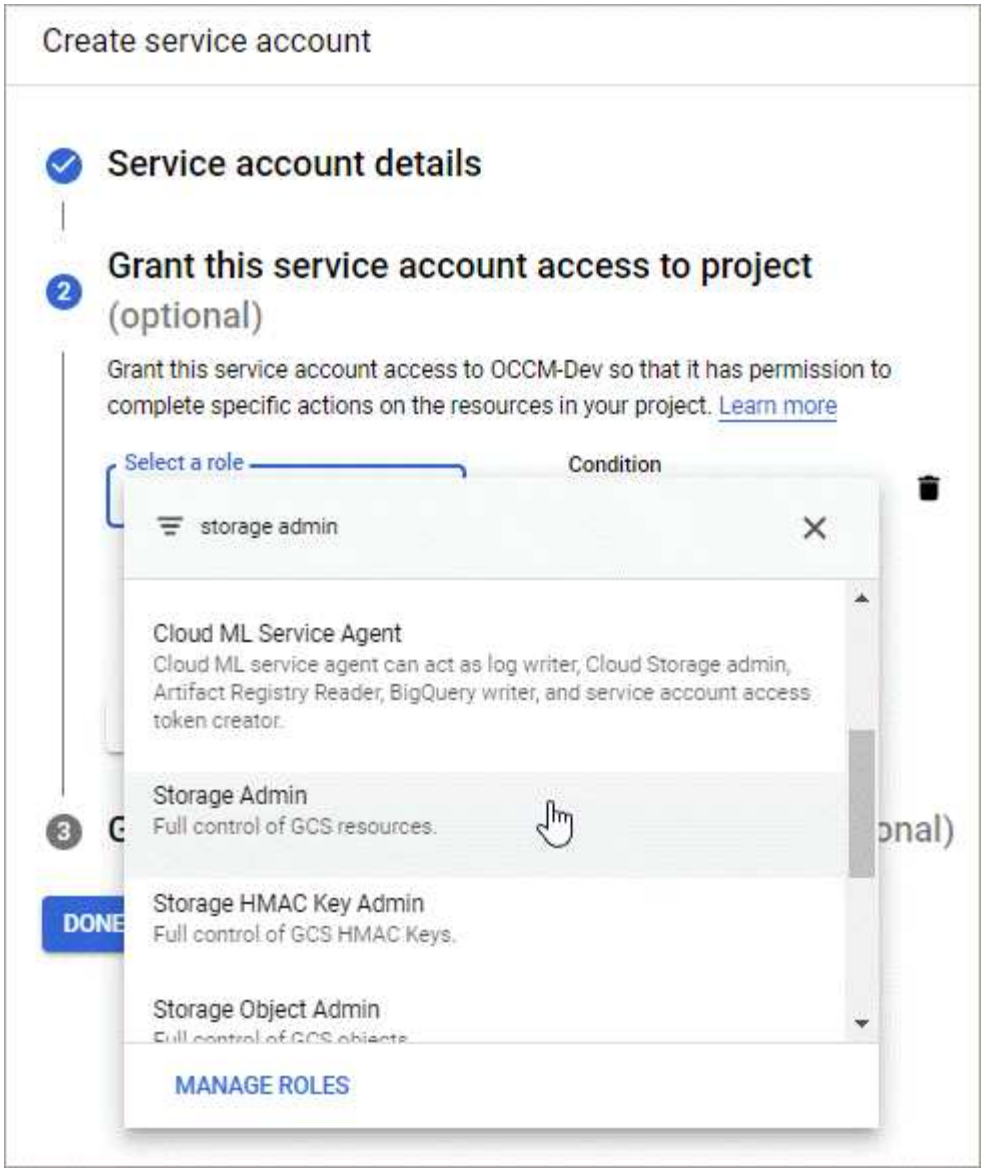
Cloud Volumes ONTAP需要 Google Cloud 服務帳戶來實現兩個目的。第一個是當你啟用"資料分層"將冷資料分層到 Google Cloud 中的低成本物件儲存。第二個是當你啟用"NetApp Backup and Recovery"將磁碟區備份到低成本的物件儲存。

Cloud Volumes ONTAP使用服務帳戶來存取和管理一個用於分層資料的儲存桶以及另一個用於備份的儲存桶。

您可以設定一個服務帳戶並將其用於兩種用途。服務帳戶必須具有*儲存管理員*角色。

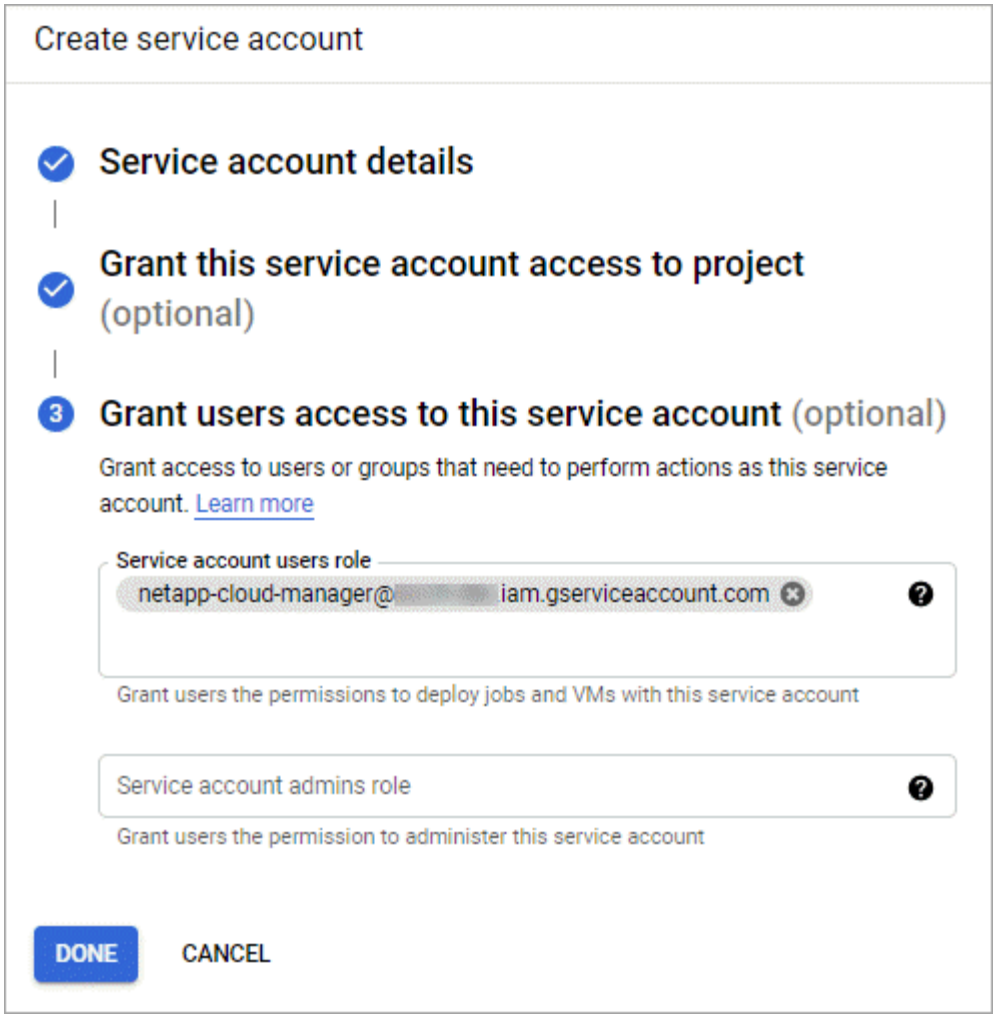
步驟

1. 在 Google Cloud Console 中 "前往服務帳戶頁面"。
2. 選擇您的項目。
3. 點擊*建立服務帳戶*並提供所需資訊。
    a. 服務帳戶詳細資料：輸入名稱和描述。
    b. 授予此服務帳戶存取項目的權限：選擇*儲存管理員*角色。



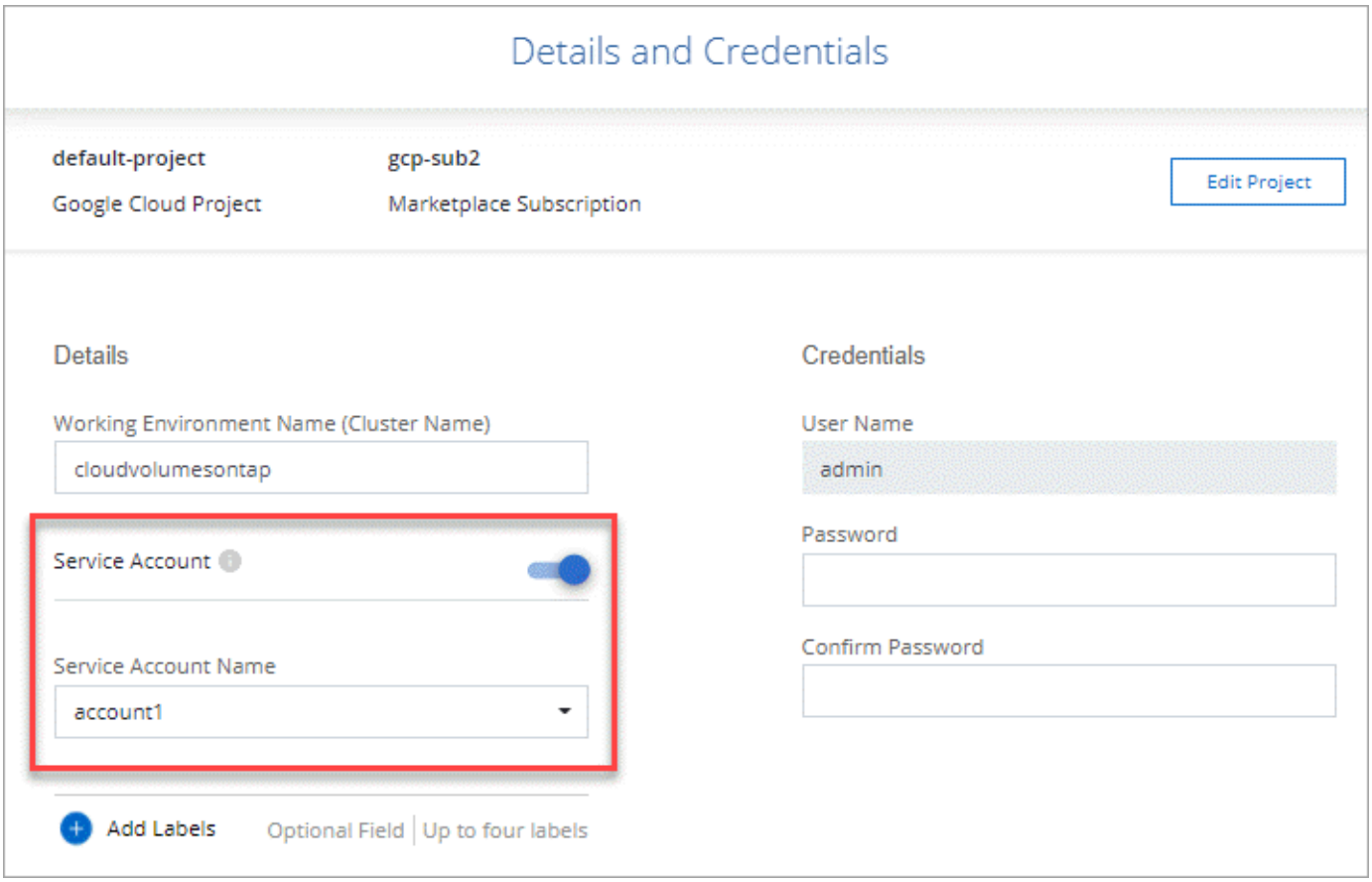
c. 授予使用者存取此服務帳戶的權限：將控制台代理服務帳戶作為_服務帳戶使用者_新增至此新服務帳戶。

此步驟僅對於資料分層是必需的。備份和還原不需要它。



下一步是什麼？

稍後建立Cloud Volumes ONTAP系統時，您需要選擇服務帳戶。



將客戶管理的加密金鑰與Cloud Volumes ONTAP結合使用

雖然 Google Cloud Storage 總是會在將資料寫入磁碟之前加密，但您可以使用 API 建立使用_客戶管理加密金鑰_的Cloud Volumes ONTAP系統。這些是您使用雲端金鑰管理服務在 GCP 中產生和管理的金鑰。

步驟

1. 確保控制台代理服務帳戶在儲存金鑰的項目中具有專案層級的正確權限。

   權限已在以下文件中提供： "預設的服務帳戶權限"但如果您使用其他項目來管理雲端金鑰服務，則可能無法套用此功能。

   權限如下：

   ```
   - cloudkms.cryptoKeyVersions.useToEncrypt
   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.list
   ```

2. 確保 "Google Compute Engine 服務代理"對金鑰具有 Cloud KMS 加密器/解密器權限。

   服務帳戶的名稱使用以下格式：「service-[service_project_number]@compute-system.iam.gserviceaccount.com」。

"Google Cloud 文件：將 IAM 與 Cloud KMS 結合使用 - 授予資源角色"

3. 透過呼叫 get 指令來取得金鑰的“id” `/gcp/vsa/metadata/gcp-encryption-keys` API 呼叫或透過在 GCP 控制台中的鍵上選擇「複製資源名稱」。
4. 如果使用客戶管理的加密金鑰並將資料分層到物件存儲， NetApp Console會嘗試使用用於加密持久磁碟的相同金鑰。但您首先需要啟用 Google Cloud Storage 儲存桶才能使用金鑰：

   a. 請依照下列步驟尋找 Google Cloud Storage 服務代理 "Google Cloud 文件：取得雲端儲存服務代理"。

   b. 導覽至加密金鑰並為 Google Cloud Storage 服務代理程式指派 Cloud KMS Encrypter/Decrypter 權限。

   有關詳細信息，請參閱 "Google Cloud 文件：使用客戶管理的加密金鑰"

5. 建立系統時，請在 API 請求中使用「gcpEncryption」參數。

   例子

```
"gcpEncryptionParameters": {
    "key": "projects/project-1/locations/us-east4/keyRings/keyring-
1/cryptoKeys/generatedkey1"
  }
```

請參閱 "NetApp Console自動化文檔"有關使用“GcpEncryption”參數的更多詳細資訊。

在 Google Cloud 中設定Cloud Volumes ONTAP許可

在您決定要與Cloud Volumes ONTAP一起使用哪種授權選項後，需要執行幾個步驟才能在建立新系統時選擇該授權選項。

免費增值

選擇免費加值服務，免費使用Cloud Volumes ONTAP，最高可提供 500 GiB 的設定容量。"了解有關免費增值服務的更多信息" 。

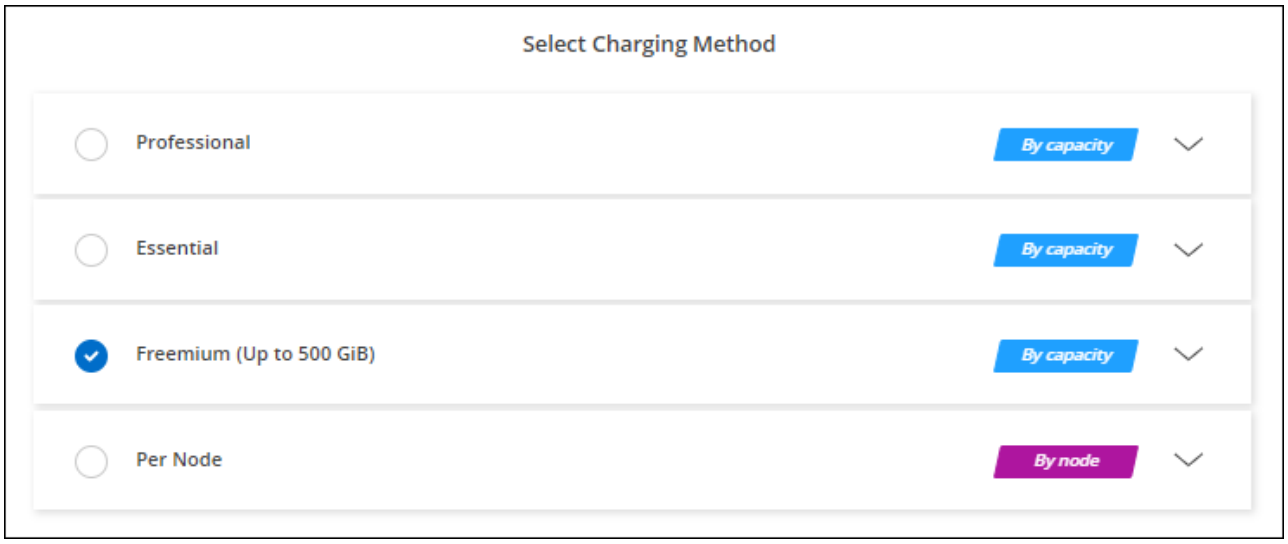
步驟

1. 從左側導覽功能表中，選擇“儲存”>“管理”。
2. 在「系統」頁面上，按一下「新增系統」並依照NetApp Console中的步驟進行操作。

   a. 在*詳細資訊和憑證*頁面上，按一下*編輯憑證>新增訂閱*，然後依照指示訂閱 Google Cloud Marketplace 中的即用即付產品。

      除非您超過 500 GiB 的預配置容量，否則您無需透過市場訂閱付費，此時系統將自動轉換為"基本套餐"。

   b. 返回控制台後，到達收費方式頁面時選擇「免費增值」。



"查看在 Google Cloud 中啟動Cloud Volumes ONTAP 的逐步說明" 。

基於容量的許可證

基於容量的許可使您能夠按 TiB 容量支付Cloud Volumes ONTAP費用。基於容量的許可以_包_的形式提供：Essentials 或 Professional 包。

Essentials 和 Professional 套餐提供以下幾種消費模式或購買選項：

- 從NetApp購買的授權（自帶授權 (BYOL)）
- Google Cloud Marketplace 的按小時付費 (PAYGO) 訂閱
- 年度合約

"了解有關基於容量的許可的更多信息" 。

以下部分介紹如何開始使用每種消費模型。

BYOL

透過從NetApp購買授權 (BYOL) 進行預付款，以便在任何雲端供應商部署Cloud Volumes ONTAP系統。

已限制 BYOL 授權的購買、延期和續約。有關更多信息，請參閱 "Cloud Volumes ONTAP的 BYOL 授權可用性受限" 。

步驟

1. "聯絡NetApp銷售人員以取得許可證"
2. "將您的NetApp支援網站帳號新增至NetApp Console"

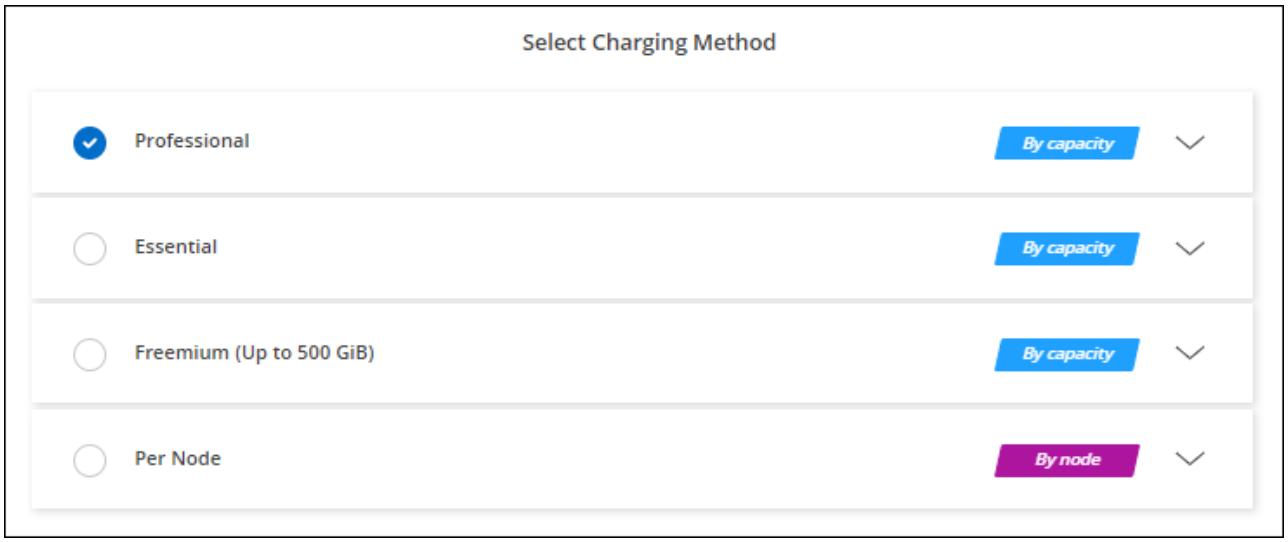
   控制台會自動查詢 NetApp 的授權服務，以取得與您的NetApp支援網站帳戶相關的授權的詳細資訊。如果沒有錯誤，控制台將新增許可證。

   您必須先從控制台取得許可證，然後才能與Cloud Volumes ONTAP一起使用。如果需要的話，你可以"手動將許可證新增至控制台"。

3. 在*系統*頁面上，按一下*新增系統*並依照步驟操作。
   a. 在*詳細資訊和憑證*頁面上，按一下*編輯憑證>新增訂閱*，然後依照指示訂閱 Google Cloud Marketplace 中的即用即付產品。

      總是會先向您從NetApp購買的許可證收費，但如果您超出許可容量或許可證期限到期，則會按照市場上的小時費率向您收費。

   b. 返回控制台後，在到達收費方式頁面時選擇基於容量的套餐。



"查看在 Google Cloud 中啟動Cloud Volumes ONTAP 的逐步說明" 。

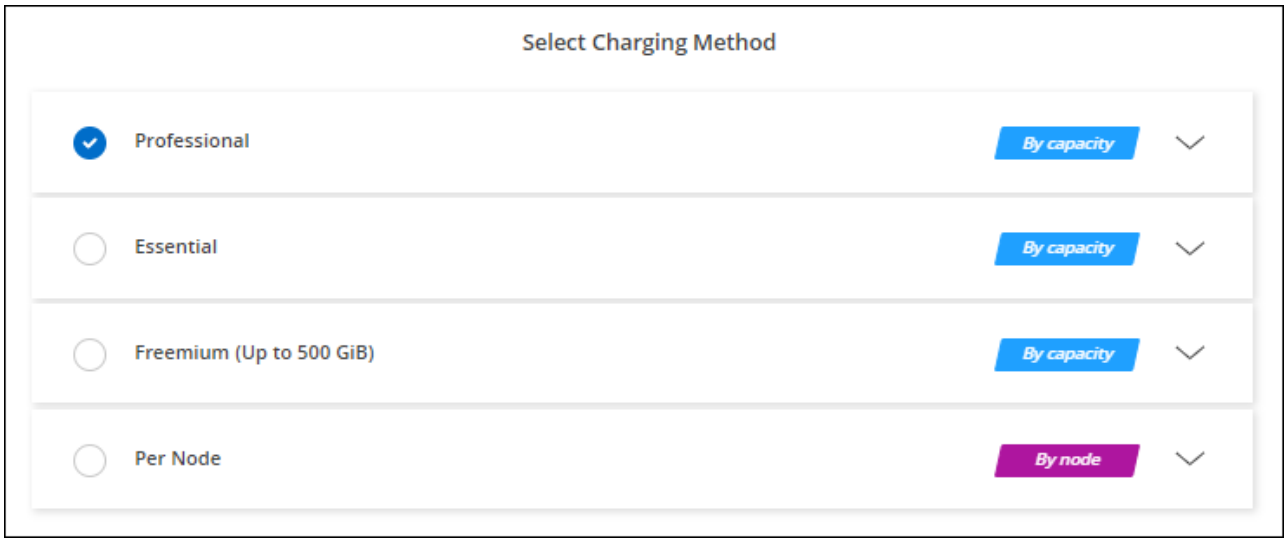
PAYGO 訂閱

透過訂閱雲端供應商市場提供的服務按小時付費。

當您建立Cloud Volumes ONTAP系統時，控制台會提示您訂閱 Google Cloud Marketplace 中提供的協定。然後將該訂閱與系統關聯以進行收費。您可以將同一訂閱用於其他系統。

步驟

1. 從左側導覽功能表中，選擇“儲存”>“管理”。
2. 在*系統*頁面上，按一下*新增系統*並依照步驟操作。
   a. 在*詳細資訊和憑證*頁面上，按一下*編輯憑證>新增訂閱*，然後依照指示訂閱 Google Cloud Marketplace 中的即用即付產品。
   b. 返回控制台後，在到達收費方式頁面時選擇基於容量的套餐。



"查看在 Google Cloud 中啟動Cloud Volumes ONTAP 的逐步說明" 。

您可以從「設定」>「憑證」頁面管理與您的帳戶相關的 Google Cloud Marketplace 訂閱。 "了解如何管理您的 Google Cloud 憑證和訂閱"

年度合約

透過購買年度合約每年支付Cloud Volumes ONTAP 的費用。

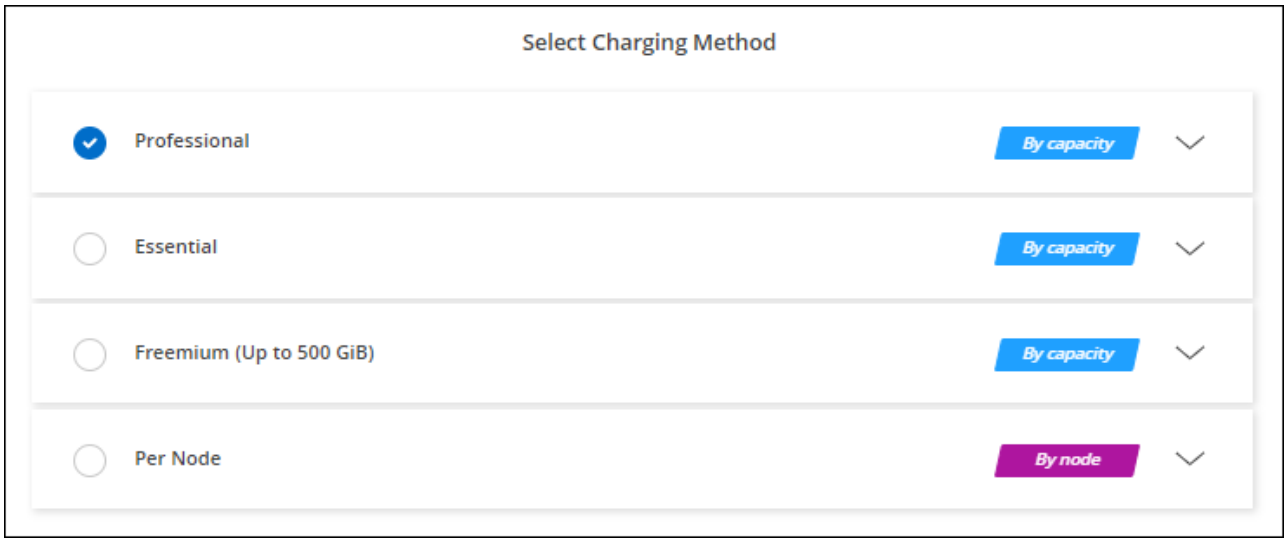
步驟

1. 聯絡您的NetApp銷售代表購買年度合約。

   該合約在 Google Cloud Marketplace 中以私人優惠形式提供。

   NetApp與您分享私人優惠後，您可以在系統建立期間從 Google Cloud Marketplace 訂閱時選擇年度方案。

2. 在*系統*頁面上，按一下*新增系統*並依照步驟操作。
   a. 在*詳細資訊和憑證*頁面上，按一下*編輯憑證>新增訂閱*，然後依照指示在 Google Cloud Marketplace 中訂閱年度方案。
   b. 在 Google Cloud 中，選擇與您的帳戶共享的年度計劃，然後按一下*訂閱*。
   c. 返回控制台後，在到達收費方式頁面時選擇基於容量的套餐。



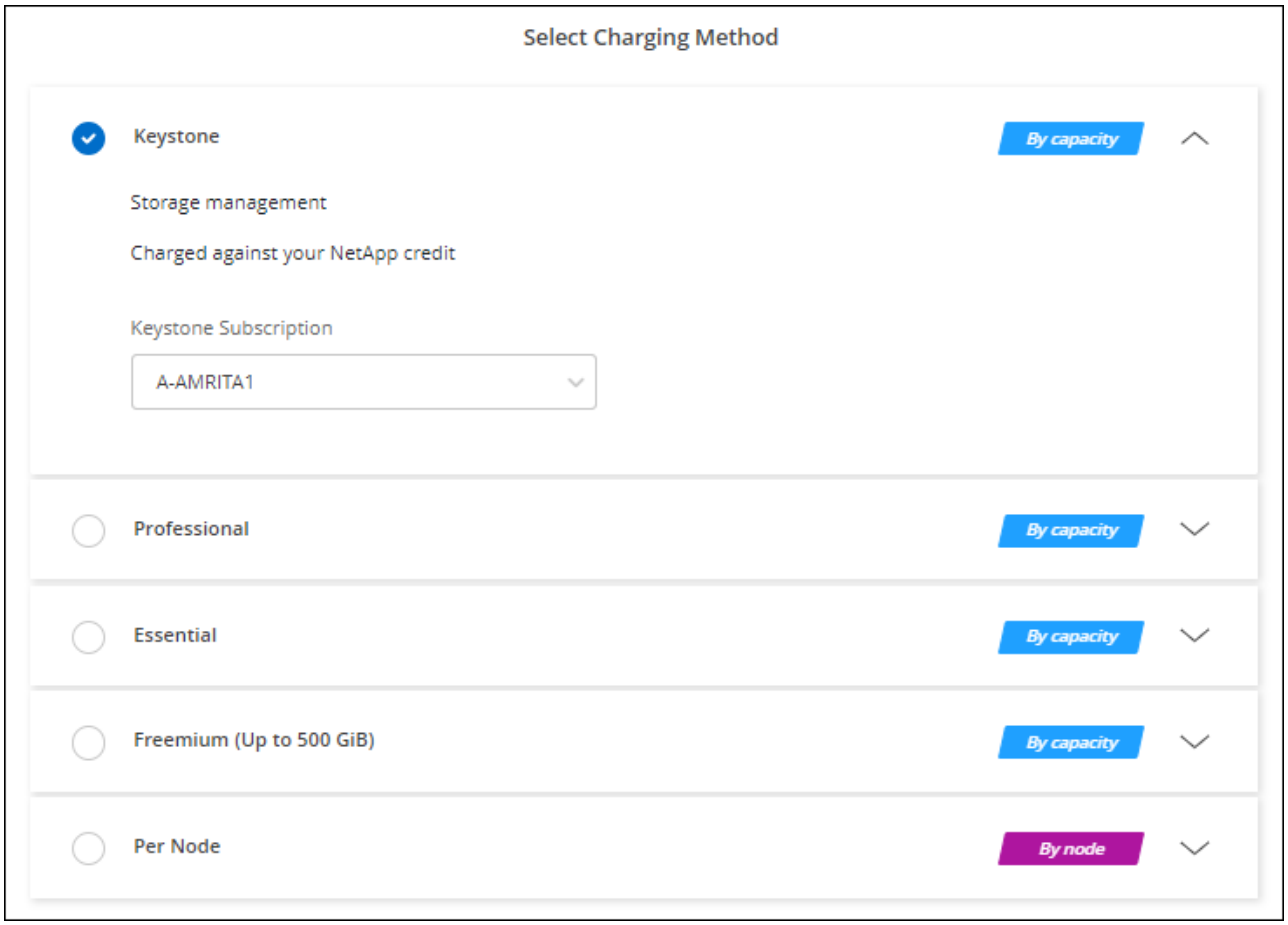
"查看在 Google Cloud 中啟動Cloud Volumes ONTAP 的逐步說明" 。

Keystone訂閱

Keystone訂閱是一種按需付費的訂閱式服務。"了解有關NetApp Keystone訂閱的更多信息" 。

步驟

1. 如果您尚未訂閱， "聯絡NetApp"
2. 聯絡NetApp 授權您的控制台使用者帳號擁有一個或多個Keystone訂閱。
3. NetApp授權您的帳戶後，"連結您的訂閱以用於Cloud Volumes ONTAP" 。
4. 在*系統*頁面上，按一下*新增系統*並依照步驟操作。
    a. 當提示選擇充電方式時，選擇Keystone Subscription 充電方式。



"查看在 Google Cloud 中啟動Cloud Volumes ONTAP 的逐步說明" 。

基於節點的許可證

基於節點的許可證是Cloud Volumes ONTAP的上一代許可證。基於節點的授權可以從NetApp (BYOL) 購買，並且僅在特定情況下才可以續訂授權。有關信息，請參閱：

- "基於節點的許可證的可用性終止"
- "基於節點的許可證的可用性終止"
- "將基於節點的許可證轉換為基於容量的許可證"

在 Google Cloud 啟動Cloud Volumes ONTAP

您可以在單一節點設定中啟動Cloud Volumes ONTAP ，也可以在 Google Cloud 中以 HA 對的形式啟動 Cloud Volumes ONTAP。

開始之前

開始之前您需要以下內容。

- 已啟動並執行的 NetApp Console 代理程式。
  - 你應該有一個 "與您的系統關聯的控制台代理" 。

- "您應該準備好讓控制台代理程式始終處於運行狀態" 。
- 與控制台代理程式關聯的服務帳戶 "應該具有所需的權限"

- 了解您想要使用的配置。

  您應該已經做好準備，選擇配置並從管理員處獲取 Google Cloud 網路資訊。有關詳細信息，請參閱"規劃您的Cloud Volumes ONTAP配置"。

- 了解設定Cloud Volumes ONTAP許可所需的條件。

  "了解如何設定許可" 。

- Google Cloud API 應該 "在您的專案中啟用"：
  - 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

在 Google Cloud 啟動單節點系統

在NetApp Console中建立一個系統以在 Google Cloud 中啟動Cloud Volumes ONTAP 。

步驟

1. 從左側導覽功能表中，選擇“儲存”>“管理”。
2. 在*系統*頁面上，點擊*新增系統*並依照指示操作。
3. 選擇位置：選擇*Google Cloud*和* Cloud Volumes ONTAP*。
4. 如果出現提示， "建立控制台代理" 。
5. 詳細資料和憑證：選擇一個項目，指定一個群集名稱，可選地選擇一個服務帳戶，可選地新增標籤，然後指定憑證。

   下表描述了您可能需要指導的欄位：

場地	描述
系統名稱	控制台使用系統名稱來命名Cloud Volumes ONTAP系統和 Google Cloud VM 執行個體。如果您選擇該選項，它也會使用該名稱作為預先定義安全性群組的前綴。
服務帳戶名稱	如果你打算使用"資料分層"或者 "NetApp Backup and Recovery"使用Cloud Volumes ONTAP，則需要啟用*服務帳戶*並選擇具有預先定義儲存管理員角色的服務帳戶。"了解如何建立服務帳號" 。
添加標籤	標籤是您的 Google Cloud 資源的元資料。控制台將標籤新增至Cloud Volumes ONTAP系統以及與該系統關聯的 Google Cloud 資源。建立系統時，您可以從使用者介面新增多達四個標籤，然後可以在建立系統後新增更多標籤。請注意，在建立系統時，API 不會將您限制為四個標籤。有關標籤的信息，請參閱 "Google Cloud 文件：標記資源"。

場地	描述
使用者名稱和密碼	這些是Cloud Volumes ONTAP叢集管理員帳戶的憑證。您可以使用這些憑證透過ONTAP System Manager 或ONTAP CLI 連線到Cloud Volumes ONTAP 。保留預設的_admin_使用者名稱或將其變更為自訂使用者名稱。
編輯項目	選擇您希望Cloud Volumes ONTAP駐留的項目。預設項目是控制台所在的項目。 如果下拉清單中沒有顯示其他專案，則表示您尚未將服務帳戶與其他專案建立關聯。請前往 Google Cloud Console，開啟 IAM 服務，然後選擇專案。將服務帳戶與您用於 Console 的角色新增至該專案。您需要為每個專案重複此步驟。 這是您為控制台設定的服務帳戶，"如本頁所述" 。 按一下「新增訂閱」將選定的憑證與訂閱關聯。 若要建立按使用量付費的Cloud Volumes ONTAP系統，您需要從 Google Cloud 市場選擇與Cloud Volumes ONTAP訂閱相關聯的 Google Cloud 專案。參考 "將市場訂閱與 Google Cloud 憑證關聯"。

6. 服務：選擇您想要在此系統上使用的服務。為了選擇備份和恢復，或使用NetApp Cloud Tiering，您必須在步驟 3 中指定服務帳戶。

   如果您想使用 WORM 和資料分層，則必須停用備份和還原並部署版本 9.8 或更高版本的Cloud Volumes ONTAP系統。

7. 位置與連線：選擇系統所在的 Google Cloud 區域和區域、選擇防火牆原則，並確認與 Google Cloud 儲存設備的網路連線以進行資料分層。

   下表描述了您可能需要指導的欄位：

場地	描述
連線驗證	若要將冷資料分層至 Google Cloud Storage 儲存桶，必須為Cloud Volumes ONTAP所在的子網路設定私人 Google Access。有關說明，請參閱 "Google Cloud 文件：配置私有 Google 存取權限"。
產生的防火牆策略	如果您讓控制台為您產生防火牆策略，則需要選擇如何允許流量： • 如果您選擇*僅限選定的 VPC*，則入站流量的來源過濾器是選定 VPC 的子網路範圍和控制台代理程式所在 VPC 的子網路範圍。這是推薦的選項。 • 如果您選擇*所有 VPC*，則入站流量的來源過濾器是 0.0.0.0/0 IP 範圍。
使用現有的防火牆策略	如果您使用現有的防火牆策略，請確保它包含所需的規則："了解Cloud Volumes ONTAP的防火牆規則"

8. 收費方式與 **NSS** 帳戶：指定您想要在此系統中使用的收費選項，然後指定NetApp支援網站帳號：
   - "了解Cloud Volumes ONTAP的授權選項"
   - "了解如何設定許可"

9. 預先配置套件：選擇其中一個套件以快速部署 Cloud Volumes ONTAP 系統，或按一下*建立我自己的組態*。預先配置套件會因所選的 Cloud Volumes ONTAP 版本而異。例如，對於 Cloud Volumes ONTAP 9.18.1 及更新版本，NetApp Console 會顯示包含 C3 VM 的套件，包括 Hyperdisk Balanced 磁碟。您可以根據工作負載需求修改組態，例如 IOPS 和處理量參數。

   如果您選擇其中一個套餐，您只需指定一個卷，然後審核並批准配置。

10. 許可：根據需要變更Cloud Volumes ONTAP版本並選擇機器類型。

    如果所選版本有較新的候選版本、通用版本或修補程式版本，則控制台在建立系統時會將其更新至該版本。例如，如果您選擇Cloud Volumes ONTAP 9.13.1 且 9.13.1 P4 可用，則會發生更新。更新不會從一個版本發生到另一個版本 — 例如，從 9.13 到 9.14。

11. 底層儲存資源：選擇初始聚合的設定：磁碟類型和每個磁碟的大小。

    磁碟類型適用於初始磁碟區。您可以為後續磁碟區選擇不同的磁碟類型。

    磁碟大小適用於初始聚合中的所有磁碟以及使用簡單配置選項時控制台建立的任何其他聚合。您可以使用進階分配選項建立使用不同磁碟大小的聚合。

    有關選擇磁碟類型和大小的協助，請參閱"在 Google Cloud 中調整系統大小"。

12. 快閃記憶體快取、寫入速度和 **WORM**：

    a. 如有需要，請啟用 **Flash Cache** 或選擇 **Normal** 或 **High** 寫入速度。

       了解更多關於 "快閃記憶體"和"寫入速度"的信息。

       透過*高*寫入速度選項可實現高寫入速度和更高的 8,896 位元組最大傳輸單元 (MTU)。此外，8,896 的更高 MTU 要求選擇 VPC-1、VPC-2 和 VPC-3 進行部署。有關 VPC-1、VPC-2 和 VPC-3 的更多信息，請參閱 "VPC-1、VPC-2 和 VPC-3 的規則"。

    b. 如果需要，請啟動一次寫入、多次讀取 (WORM) 儲存。

       如果為Cloud Volumes ONTAP 9.7 及更低版本啟用了資料分層，則無法啟用 WORM。啟用 WORM 和分層後，恢復或降級到Cloud Volumes ONTAP 9.8 的操作將被阻止。

    "了解有關 WORM 存儲的更多信息" 。

    a. 如果您啟動 WORM 存儲，請選擇保留期限。

13. **Google Cloud Platform** 中的資料分層：選擇是否在初始聚合上啟用資料分層，為分層資料選擇儲存類，然後選擇具有預先定義儲存管理員角色的服務帳戶（ Cloud Volumes ONTAP 9.7 或更高版本所需），或選擇 Google Cloud 帳戶（ Cloud Volumes ONTAP 9.6 所需）。

    請注意以下事項：

    - 控制台在Cloud Volumes ONTAP實例上設定服務帳戶。此服務帳戶提供將資料分層至 Google Cloud Storage 儲存桶的權限。請確保將控制台代理服務帳戶新增為分層服務帳戶的用戶，否則，您無法從控制台中選擇它。
    - 如需新增 Google Cloud 帳戶的協助，請參閱 "使用 9.6 設定和新增 Google Cloud 帳戶以進行資料分層"。

- 您可以在建立或編輯磁碟區時選擇特定的磁碟區分層策略。
- 如果停用資料分層、則可以在後續 Aggregate 上啟用、但您需要關閉系統、並從 Google Cloud Console 新增服務帳戶。

  "了解有關數據分層的更多信息" 。

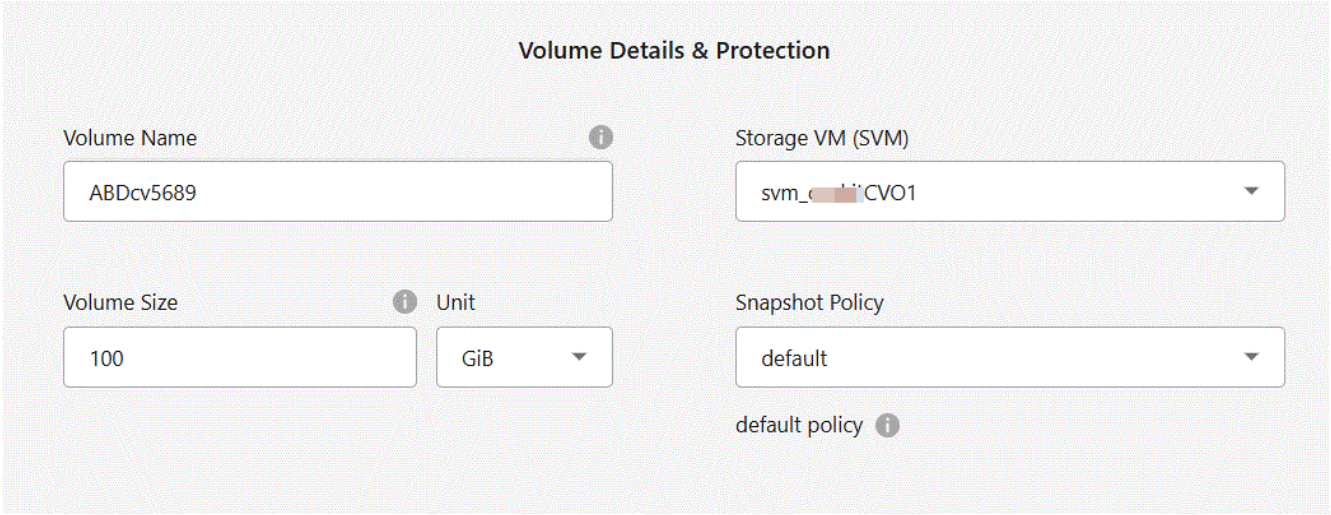
14. 建立磁碟區：輸入新磁碟區的詳細資料或點選*跳過*。

    "了解支援的客戶端協定和版本" 。

    此頁面中的某些欄位是不言自明的。下表描述了您可能需要指導的欄位：

場地	描述
尺寸	您可以輸入的最大大小很大程度上取決於您是否啟用精簡配置，這使您能夠建立比目前可用的實體儲存更大的磁碟區。
存取控制（僅適用於 NFS）	導出策略定義了子網路中可以存取磁碟區的用戶端。預設情況下，控制台輸入一個提供對子網路中所有實例的存取權限的值。
權限和使用者/群組（僅適用於 CIFS）	這些欄位可讓您控制使用者和群組對共用的存取等級（也稱為存取控制清單或 ACL）。您可以指定本機或網域 Windows 使用者或群組，或 UNIX 使用者或群組。如果指定網域 Windows 使用者名，則必須使用網域\使用者名稱格式包含使用者的網域。
快照策略	Snapshot 副本策略指定自動建立的NetApp Snapshot 副本的頻率和數量。NetApp Snapshot 副本是時間點檔案系統映像，它不會影響效能並且只需要最少的儲存空間。您可以選擇預設策略或無策略。對於瞬態數據，您可能會選擇無：例如，對於 Microsoft SQL Server，請選擇 tempdb。
進階選項（僅適用於 NFS）	為磁碟區選擇一個 NFS 版本：NFSv3 或 NFSv4。
啟動器群組和 IQN（僅適用於 iSCSI）	iSCSI 儲存目標稱為 LUN（邏輯單元），並以標準區塊裝置呈現給主機。啟動器群組是 iSCSI 主機節點名稱表，用於控制哪些啟動器可以存取哪些 LUN。iSCSI 目標透過標準乙太網路網路適配器 (NIC)、具有軟體啟動器的 TCP 卸載引擎 (TOE) 卡、融合網路適配器 (CNA) 或專用主機匯流排適配器 (HBA) 連接到網絡，並透過 iSCSI 限定名稱 (IQN) 進行識別。當您建立 iSCSI 磁碟區時，控制台會自動為您建立 LUN。我們透過為每個磁碟區建立一個 LUN 來簡化操作，因此無需進行任何管理。建立磁碟區後，"使用 IQN 從主機連線到 LUN" 。

    下圖顯示了磁碟區建立精靈的第一頁：



15. **CIFS** 設定：如果您選擇 CIFS 協議，請設定 CIFS 伺服器。

場地	描述
DNS 主 IP 位址和輔助 IP 位址	為 CIFS 伺服器提供名稱解析的 DNS 伺服器的 IP 位址。所列的 DNS 伺服器必須包含定位 CIFS 伺服器將加入的網域的 Active Directory LDAP 伺服器和網域控制站所需的服務位置記錄 (SRV)。如果您正在設定 Google 管理的 Active Directory，則預設可以使用 169.254.169.254 IP 位址存取 AD。
要加入的 Active Directory 網域	您希望 CIFS 伺服器加入的 Active Directory (AD) 網域的 FQDN。
授權加入網域的憑證	具有足夠權限將電腦新增至 AD 網域內指定組織單位 (OU) 的 Windows 帳戶的名稱和密碼。
CIFS 伺服器 NetBIOS 名稱	AD 網域中唯一的 CIFS 伺服器名稱。
組織單位	AD 網域內與 CIFS 伺服器關聯的組織單位。預設值為 CN=Computers。若要將 Google Managed Microsoft AD 設定為Cloud Volumes ONTAP的 AD 伺服器，請在此欄位中輸入 **OU=Computers,OU=Cloud** 。https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Google Cloud 文件：Google Managed Microsoft AD 中的組織單位"^]
DNS 網域	Cloud Volumes ONTAP儲存虛擬機器 (SVM) 的 DNS 網域。大多數情況下，該域與 AD 域相同。
NTP 伺服器	選擇「使用 Active Directory 網域」以使用 Active Directory DNS 設定 NTP 伺服器。如果您需要使用不同的位址來設定 NTP 伺服器，那麼您應該使用 API。欲了解更多信息，請參閱 "NetApp Console自動化文檔"了解詳情。請注意，只有在建立 CIFS 伺服器時才能設定 NTP 伺服器。建立 CIFS 伺服器後，它不可配置。

16. 使用情況設定檔、磁碟類型和分層策略：選擇是否要啟用儲存效率功能並變更磁碟區分層策略（如果需要）。

    更多信息，請參閱"選擇卷使用情況設定檔"，"資料分層概述" ， 和 "KB：CVO 支援哪些內嵌儲存效率功能？"

17. 審核並批准：審核並確認您的選擇。

a. 查看有關配置的詳細資訊。

b. 點擊*更多資訊*查看有關支援和控制台將購買的 Google Cloud 資源的詳細資訊。

c. 選取*我明白…*複選框。

d. 按一下“開始”。

結果

控制台部署Cloud Volumes ONTAP系統。您可以在*審核*頁面上追蹤進度。

如果您在部署Cloud Volumes ONTAP系統時遇到任何問題，請查看失敗訊息。您也可以選擇系統並點擊*重新建立環境*。

如需更多協助，請訪問 "NetApp Cloud Volumes ONTAP支持"。

完成後

- 如果您配置了 CIFS 共享，請授予使用者或群組對檔案和資料夾的權限，並驗證這些使用者是否可以存取共用並建立檔案。
- 如果要將配額套用於卷，請使用ONTAP系統管理員或ONTAP CLI。

  配額可讓您限製或追蹤使用者、群組或 qtree 使用的磁碟空間和檔案數量。

部署程序完成後，請勿在 Google Cloud 入口網站中修改系統產生的 Cloud Volumes ONTAP 配置，例如系統標記和 Google Cloud 資源中設定的標籤。對這些配置進行任何更改都可能導致意外行為或資料遺失。

在 Google Cloud 中啟動 HA 對

在控制台中建立一個系統以在 Google Cloud 中啟動Cloud Volumes ONTAP 。

步驟

1. 從左側導覽功能表中，選擇“儲存”>“管理”。
2. 在*系統*頁面上，按一下*儲存>系統*並按照提示進行操作。
3. 選擇位置：選擇*Google Cloud*和* Cloud Volumes ONTAP HA*。
4. 詳細資料和憑證：選擇一個項目，指定一個群集名稱，可選地選擇一個服務帳戶，可選地新增標籤，然後指定憑證。

   下表描述了您可能需要指導的欄位：

場地	描述
系統名稱	控制台使用系統名稱來命名Cloud Volumes ONTAP系統和 Google Cloud VM 執行個體。如果您選擇該選項，它也會使用該名稱作為預先定義安全性群組的前綴。
服務帳戶名稱	如果您打算使用"NetApp Cloud Tiering"或者 "備份和復原"服務，您需要啟用*服務帳戶*開關，然後選擇具有預先定義儲存管理員角色的服務帳戶。

場地	描述
添加標籤	標籤是您的 Google Cloud 資源的元資料。控制台將標籤新增至Cloud Volumes ONTAP系統以及與該系統關聯的 Google Cloud 資源。建立系統時，您可以從使用者介面新增多達四個標籤，然後可以在建立系統後新增更多標籤。請注意，在建立系統時，API 不會將您限制為四個標籤。有關標籤的信息，請參閱 "Google Cloud 文件：標記資源"。
使用者名稱和密碼	這些是Cloud Volumes ONTAP叢集管理員帳戶的憑證。您可以使用這些憑證透過ONTAP System Manager 或ONTAP CLI 連線到Cloud Volumes ONTAP 。保留預設的_admin_使用者名稱或將其變更為自訂使用者名稱。
編輯項目	選擇您希望 Cloud Volumes ONTAP 所在的專案。 如果下拉清單中沒有顯示其他專案，則表示您尚未將服務帳戶與其他專案建立關聯。請前往 Google Cloud Console，開啟 IAM 服務，然後選擇專案。將服務帳戶與您用於 Console 的角色新增至該專案。您需要為每個專案重複此步驟。 這是您為控制台設定的服務帳戶，"如本頁所述" 。 按一下「新增訂閱」將選定的憑證與訂閱關聯。 若要建立按使用量付費的Cloud Volumes ONTAP系統，您需要從 Google Cloud Marketplace 中選擇與Cloud Volumes ONTAP訂閱相關聯的 Google Cloud 專案。參考 "將市場訂閱與 Google Cloud 憑證關聯"。

5. 服務：選擇您想要在此系統上使用的服務。若要選擇備份和恢復，或使用NetApp Cloud Tiering，您必須在步驟 3 中指定服務帳戶。

   如果您想使用 WORM 和資料分層，則必須停用備份和還原並部署版本 9.8 或更高版本的Cloud Volumes ONTAP系統。

6. **HA** 部署模型：為 HA 配置選擇多個區域（建議）或單一區域。然後選擇區域和分區。

   "了解有關 HA 部署模型的更多信息" 。

7. 連線性：為 HA 設定選擇四個不同的 VPC，每個 VPC 中選擇一個子網，然後選擇一個防火牆策略。

   "了解有關網絡要求的更多信息" 。

   下表描述了您可能需要指導的欄位：

場地	描述
產生的策略	如果您讓控制台為您產生防火牆策略，則需要選擇如何允許流量： • 如果您選擇*僅限選定的 VPC*，則入站流量的來源過濾器是選定 VPC 的子網路範圍和控制台代理程式所在 VPC 的子網路範圍。這是推薦的選項。 • 如果您選擇*所有 VPC*，則入站流量的來源過濾器是 0.0.0.0/0 IP 範圍。

場地	描述
使用現有的	如果您使用現有的防火牆策略，請確保它包含所需的規則。"了解Cloud Volumes ONTAP的防火牆規則" 。

8. 收費方式和 **NSS** 帳戶：指定您想要在此系統中使用的收費選項，然後指定NetApp支援網站帳戶。
   - "了解Cloud Volumes ONTAP的授權選項" 。
   - "了解如何設定許可" 。
9. 預先配置套件：選擇其中一個套件來快速部署Cloud Volumes ONTAP系統，或點擊*建立我自己的設定*。

   如果您選擇其中一個套餐，您只需指定一個卷，然後審核並批准配置。
10. 許可：根據需要變更Cloud Volumes ONTAP版本並選擇機器類型。

    如果所選版本有較新的候選版本、通用版本或修補程式版本，則控制台在建立系統時會將其更新至該版本。例如，如果您選擇Cloud Volumes ONTAP 9.13.1 且 9.13.1 P4 可用，則會發生更新。更新不會從一個版本發生到另一個版本 - 例如，從 9.13 到 9.14。
11. 底層儲存資源：選擇初始聚合的設定：磁碟類型和每個磁碟的大小。

    磁碟類型適用於初始磁碟區。您可以為後續磁碟區選擇不同的磁碟類型。

    磁碟大小適用於初始聚合中的所有磁碟以及使用簡單配置選項時控制台建立的任何其他聚合。您可以使用進階分配選項建立使用不同磁碟大小的聚合。

    有關選擇磁碟類型和大小的協助，請參閱"在 Google Cloud 中調整系統大小"。
12. 快閃記憶體快取、寫入速度和 **WORM**：
    a. 如有需要，請啟用 **Flash Cache** 或選擇 **Normal** 或 **High** 寫入速度。

       了解更多關於 "快閃記憶體"和"寫入速度"的信息。

       透過 n2-standard-16、n2-standard-32、n2-standard-48 和 n2-standard-64 實例類型的高 寫入速度選項，可以獲得高寫入速度和更高的 8,896 位元組的最大傳輸單元 (MTU)。此外，8,896 的更高 MTU 要求選擇 VPC-1、VPC-2 和 VPC-3 進行部署。高寫入速度和 8,896 的 MTU 取決於功能，無法在配置的實例中單獨停用。有關 VPC-1、VPC-2 和 VPC-3 的更多信息，請參閱 "VPC-1、VPC-2 和 VPC-3 的規則"。

    b. 如果需要，請啟動一次寫入、多次讀取 (WORM) 儲存。

       如果為Cloud Volumes ONTAP 9.7 及更低版本啟用了資料分層，則無法啟用 WORM。啟用 WORM 和分層後，恢復或降級到Cloud Volumes ONTAP 9.8 的操作將被阻止。

    "了解有關 WORM 存儲的更多信息" 。

    a. 如果您啟動 WORM 存儲，請選擇保留期限。
13. **Google Cloud** 中的資料分層：選擇是否在初始聚合上啟用資料分層，為分層資料選擇儲存類，然後選擇具有預先定義儲存管理員角色的服務帳戶。

請注意以下事項：

- 控制台在Cloud Volumes ONTAP實例上設定服務帳戶。此服務帳戶提供將資料分層至 Google Cloud Storage 儲存桶的權限。請確保將控制台代理服務帳戶新增為分層服務帳戶的用戶，否則，您無法從控制台中選擇它。
- 您可以在建立或編輯磁碟區時選擇特定的磁碟區分層策略。
- 如果停用資料分層、則可以在後續 Aggregate 上啟用、但您需要關閉系統、並從 Google Cloud Console 新增服務帳戶。

  "了解有關數據分層的更多信息" 。

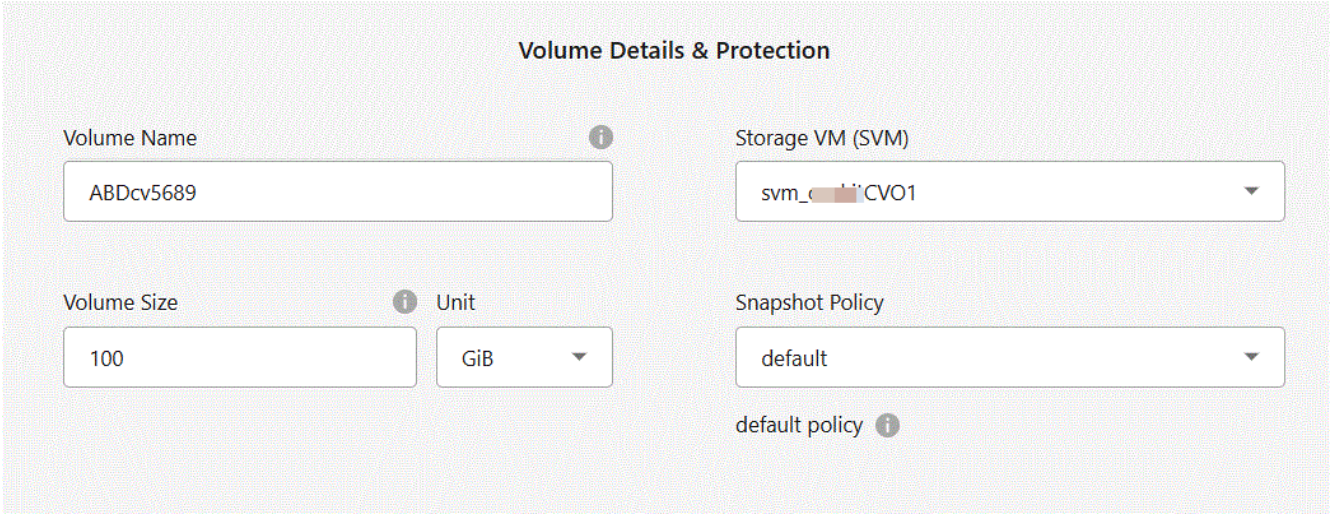
14. 建立磁碟區：輸入新磁碟區的詳細資料或點選*跳過*。

    "了解支援的客戶端協定和版本" 。

    此頁面中的某些欄位是不言自明的。下表描述了您可能需要指導的欄位：

場地	描述
尺寸	您可以輸入的最大大小很大程度上取決於您是否啟用精簡配置，這使您能夠建立比目前可用的實體儲存更大的磁碟區。
存取控制（僅適用於 NFS）	導出策略定義了子網路中可以存取磁碟區的用戶端。預設情況下，控制台輸入一個提供對子網路中所有實例的存取權限的值。
權限和使用者/群組（僅適用於 CIFS）	這些欄位可讓您控制使用者和群組對共用的存取等級（也稱為存取控制清單或 ACL）。您可以指定本機或網域 Windows 使用者或群組，或 UNIX 使用者或群組。如果指定網域 Windows 使用者名，則必須使用網域\使用者名稱格式包含使用者的網域。
快照策略	Snapshot 副本策略指定自動建立的NetApp Snapshot 副本的頻率和數量。NetApp Snapshot 副本是時間點檔案系統映像，它不會影響效能並且只需要最少的儲存空間。您可以選擇預設策略或無策略。對於瞬態數據，您可能會選擇無：例如，對於 Microsoft SQL Server，請選擇 tempdb。
進階選項（僅適用於 NFS）	為磁碟區選擇一個 NFS 版本：NFSv3 或 NFSv4。
啟動器群組和 IQN（僅適用於 iSCSI）	iSCSI 儲存目標稱為 LUN（邏輯單元），並以標準區塊裝置呈現給主機。啟動器群組是 iSCSI 主機節點名稱表，用於控制哪些啟動器可以存取哪些 LUN。iSCSI 目標透過標準乙太網路網路適配器 (NIC)、具有軟體啟動器的 TCP 卸載引擎 (TOE) 卡、融合網路適配器 (CNA) 或專用主機匯流排適配器 (HBA) 連接到網絡，並透過 iSCSI 限定名稱 (IQN) 進行識別。當您建立 iSCSI 磁碟區時，控制台會自動為您建立 LUN。我們透過為每個磁碟區建立一個 LUN 來簡化操作，因此無需進行任何管理。建立磁碟區後，"使用 IQN 從主機連線到 LUN" 。

    下圖顯示了磁碟區建立精靈的第一頁：



15. **CIFS** 設定：如果您選擇 CIFS 協議，請設定 CIFS 伺服器。

場地	描述
DNS 主 IP 位址和輔助 IP 位址	為 CIFS 伺服器提供名稱解析的 DNS 伺服器的 IP 位址。所列的 DNS 伺服器必須包含定位 CIFS 伺服器將加入的網域的 Active Directory LDAP 伺服器和網域控制站所需的服務位置記錄 (SRV)。如果您正在設定 Google 管理的 Active Directory，則預設可以使用 169.254.169.254 IP 位址存取 AD。
要加入的 Active Directory 網域	您希望 CIFS 伺服器加入的 Active Directory (AD) 網域的 FQDN。
授權加入網域的憑證	具有足夠權限將電腦新增至 AD 網域內指定組織單位 (OU) 的 Windows 帳戶的名稱和密碼。
CIFS 伺服器 NetBIOS 名稱	AD 網域中唯一的 CIFS 伺服器名稱。
組織單位	AD 網域內與 CIFS 伺服器關聯的組織單位。預設值為 CN=Computers。若要將 Google Managed Microsoft AD 設定為Cloud Volumes ONTAP的 AD 伺服器，請在此欄位中輸入 **OU=Computers,OU=Cloud** 。https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Google Cloud 文件：Google Managed Microsoft AD 中的組織單位"^]
DNS 網域	Cloud Volumes ONTAP儲存虛擬機器 (SVM) 的 DNS 網域。大多數情況下，該域與 AD 域相同。
NTP 伺服器	選擇「使用 Active Directory 網域」以使用 Active Directory DNS 設定 NTP 伺服器。如果您需要使用不同的位址來設定 NTP 伺服器，那麼您應該使用 API。請參閱 "NetApp Console自動化文檔"了解詳情。請注意，只有在建立 CIFS 伺服器時才能設定 NTP 伺服器。建立 CIFS 伺服器後，它不可配置。

16. 使用情況設定檔、磁碟類型和分層策略：選擇是否要啟用儲存效率功能並變更磁碟區分層策略（如果需要）。

    更多信息，請參閱"選擇卷使用情況設定檔"，"資料分層概述" ， 和 "KB：CVO 支援哪些內嵌儲存效率功能？"

17. 審核並批准：審核並確認您的選擇。

a. 查看有關配置的詳細資訊。
b. 點擊*更多資訊*查看有關支援和控制台將購買的 Google Cloud 資源的詳細資訊。
c. 選取*我明白…*複選框。
d. 按一下“開始”。

結果

控制台部署Cloud Volumes ONTAP系統。您可以在*審核*頁面上追蹤進度。

如果您在部署Cloud Volumes ONTAP系統時遇到任何問題，請查看失敗訊息。您也可以選擇系統並點擊*重新建立環境*。

如需更多協助，請訪問 "NetApp Cloud Volumes ONTAP支持"。

完成後

- 如果您配置了 CIFS 共享，請授予使用者或群組對檔案和資料夾的權限，並驗證這些使用者是否可以存取共用並建立檔案。
- 如果要將配額套用於卷，請使用ONTAP系統管理員或ONTAP CLI。

  配額可讓您限製或追蹤使用者、群組或 qtree 使用的磁碟空間和檔案數量。

部署程序完成後，請勿在 Google Cloud 入口網站中修改系統產生的 Cloud Volumes ONTAP 配置，例如系統標記和 Google Cloud 資源中設定的標籤。對這些配置進行任何更改都可能導致意外行為或資料遺失。

相關連結

- "在 Google Cloud 規劃Cloud Volumes ONTAP配置"

Google Cloud Platform 圖像驗證

了解如何在Cloud Volumes ONTAP中驗證 Google Cloud 映像

Google Cloud 映像驗證符合增強的NetApp安全要求。已經對生成圖像的腳本進行了更改，以便使用專門為此任務生成的私鑰對圖像進行簽署。您可以使用 Google Cloud 的簽章摘要和公用憑證來驗證 Google Cloud 映像的完整性，該憑證可透過以下方式下載 "國家安全局"針對特定版本。

Cloud Volumes ONTAP軟體版本 9.13.0 或更高版本支援 Google Cloud 映像驗證。

將 Google Cloud 映像轉換為Cloud Volumes ONTAP 的原始格式

用於部署新實例、升級或在現有映像中使用的映像將透過以下方式與客戶端共用 "NetApp 支援站點 (NSS)"。已簽署的摘要和憑證可透過 NSS 入口網站下載。確保您下載的摘要和憑證與NetApp支援共享的影像對應的正確版本。例如，9.13.0 影像將具有 9.13.0 簽名摘要和 NSS 上可用的憑證。

為什麼需要這一步？

無法直接下載 Google Cloud 的圖片。為了根據簽署的摘要和證書驗證圖像，您需要有一個機制來比較兩個檔案並下載圖像。為此，您必須將圖像匯出/轉換為 disk.raw 格式，並將結果保存在 Google Cloud 的儲存桶中。在此過程中，disk.raw 檔案被壓縮並壓縮。

使用者/服務帳戶需要權限才能執行以下操作：

- 存取 Google 儲存桶
- 寫入 Google 儲存桶
- 建立雲端建置作業（在匯出過程中使用）
- 存取所需圖像
- 建立匯出影像任務

若要驗證映像，必須將其轉換為 disk.raw 格式，然後下載。

使用 **Google Cloud** 命令列匯出 **Google Cloud** 鏡像

將影像匯出到雲端儲存的首選方法是使用 "gcloud compute images export 指令"。此命令獲取提供的圖像並將其轉換為 disk.raw 文件，該文件會被 tarred 和 gzip 壓縮。產生的檔案保存在目標URL，然後可以下載進行驗證。

使用者/帳戶必須具有存取和寫入所需儲存桶、匯出映像和雲端建置（Google 用於匯出映像）的權限才能執行此操作。

使用 **gcloud** 匯出 **Google Cloud** 鏡像

點擊顯示

```
$ gcloud compute images export \
    --destination-uri DESTINATION_URI \
    --image IMAGE_NAME

# For our example:
$ gcloud compute images export \
    --destination-uri gs://vsa-dev-bucket1/example-user-exportimage-
gcp-demo \
    --image example-user-20230120115139


## DEMO ##
# Step 1 - Optional: Checking access and listing objects in the
destination bucket
$ gsutil ls gs://example-user-export-image-bucket/

# Step 2 - Exporting the desired image to the bucket
$ gcloud compute images export --image example-user-export-image-demo
--destination-uri gs://example-user-export-image-bucket/export-
demo.tar.gz
Created [https://cloudbuild.googleapis.com/v1/projects/example-demo-
project/locations/us-central1/builds/xxxxxxxxxxxx].
Logs are available at [https://console.cloud.google.com/cloud-
build/builds;region=us-central1/xxxxxxxxxxxx?project=xxxxxxxxxxxx].
[image-export]: 2023-01-25T18:13:48Z Fetching image "example-user-
export-image-demo" from project "example-demo-project".
[image-export]: 2023-01-25T18:13:49Z Validating workflow
[image-export]: 2023-01-25T18:13:49Z Validating step "setup-disks"
[image-export]: 2023-01-25T18:13:49Z Validating step "image-export-
export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "setup-disks"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "run-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "wait-for-inst-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "copy-image-object"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "delete-inst"
[image-export]: 2023-01-25T18:13:51Z Validation Complete
[image-export]: 2023-01-25T18:13:51Z Workflow Project: example-demo-
project
[image-export]: 2023-01-25T18:13:51Z Workflow Zone: us-central1-c
```

```
[image-export]: 2023-01-25T18:13:51Z Workflow GCSPath: gs://example-
demo-project-example-bkt-us/
[image-export]: 2023-01-25T18:13:51Z Example scratch path:
https://console.cloud.google.com/storage/browser/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px
[image-export]: 2023-01-25T18:13:51Z Uploading sources
[image-export]: 2023-01-25T18:13:51Z Running workflow
[image-export]: 2023-01-25T18:13:51Z Running step "setup-disks"
(CreateDisks)
[image-export.setup-disks]: 2023-01-25T18:13:51Z CreateDisks: Creating
disk "disk-image-export-image-export-r88px".
[image-export]: 2023-01-25T18:14:02Z Step "setup-disks" (CreateDisks)
successfully finished.
[image-export]: 2023-01-25T18:14:02Z Running step "image-export-export-
disk" (IncludeWorkflow)
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "setup-disks" (CreateDisks)
[image-export.image-export-export-disk.setup-disks]: 2023-01-
25T18:14:02Z CreateDisks: Creating disk "disk-image-export-export-disk-
image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Step
"setup-disks" (CreateDisks) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "run-image-export-export-disk" (CreateInstances)
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:02Z CreateInstances: Creating instance "inst-image-
export-export-disk-image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Step
"run-image-export-export-disk" (CreateInstances) successfully finished.
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:08Z CreateInstances: Streaming instance "inst-image-
export-export-disk-image-export-image-export--r88px" serial port 1
output to https://storage.cloud.google.com/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px/logs/inst-
image-export-export-disk-image-export-image-export--r88px-serial-
port1.log
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Running
step "wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:08Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
watching serial port 1, SuccessMatch: "ExportSuccess", FailureMatch:
["ExportFailed:"] (this is not an error), StatusMatch: "GCEExport:".
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
```

```
StatusMatch found: "GCEExport: <serial-output key:'source-size-gb'
value:'10'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Running export tool."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Disk /dev/sdb is 10 GiB, compressed size
will most likely be much smaller."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Beginning export process..."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Copying \"/dev/sdb\" to gs://example-
demo-project-example-bkt-us/example-image-export-20230125-18:13:49-
r88px/outs/image-export-export-disk.tar.gz."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Using \"/root/upload\" as the buffer
prefix, 1.0 GiB as the buffer size, and 4 as the number of workers."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Creating gzipped image of \"/dev/sdb\"."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 1.0 GiB of 10 GiB (212 MiB/sec),
total written size: 992 MiB (198 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:59Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 8.0 GiB of 10 GiB (237 MiB/sec),
total written size: 1.5 GiB (17 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Finished creating gzipped image of
\"/dev/sdb\" in 48.956433327s [213 MiB/s] with a compression ratio of
6."
```

```
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Finished export in  48.957347731s"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: <serial-output key:'target-size-gb'
value:'2'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
SuccessMatch found "ExportSuccess"
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step
"wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running
step "copy-image-object" (CopyGCSObjects)
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running
step "delete-inst" (DeleteResources)
[image-export.image-export-export-disk.delete-inst]: 2023-01-
25T18:15:19Z DeleteResources: Deleting instance "inst-image-export-
export-disk".
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step
"copy-image-object" (CopyGCSObjects) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:34Z Step
"delete-inst" (DeleteResources) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Step "image-export-export-disk"
(IncludeWorkflow) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> source-
size-gb:10
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> target-
size-gb:2
[image-export]: 2023-01-25T18:15:34Z Workflow "image-export" cleaning
up (this may take up to 2 minutes).
[image-export]: 2023-01-25T18:15:35Z Workflow "image-export" finished
cleanup.

# Step 3 - Validating the image was successfully exported
$ gsutil ls gs://example-user-export-image-bucket/
gs://example-user-export-image-bucket/export-demo.tar.gz


# Step 4 - Download the exported image
$ gcloud storage cp gs://BUCKET_NAME/OBJECT_NAME SAVE_TO_LOCATION
```

```
$ gcloud storage cp gs://example-user-export-image-bucket/export-
demo.tar.gz CVO_GCP_Signed_Digest.tar.gz
Copying gs://example-user-export-image-bucket/export-demo.tar.gz to
file://CVO_GCP_Signed_Digest.tar.gz
  Completed files 1/1 | 1.5GiB/1.5GiB | 185.0MiB/s

Average throughput: 213.3MiB/s
$ ls -l
total 1565036
-rw-r--r-- 1 example-user example-user 1602589949 Jan 25 18:44
CVO_GCP_Signed_Digest.tar.gz
```

解壓縮壓縮檔

```
# Extracting files from the digest
$ tar -xf CVO_GCP_Signed_Digest.tar.gz
```

有關如何透過 Google Cloud 匯出圖像的更多信息，請參閱 "Google Cloud 文件：匯出影像"。

影像簽名驗證

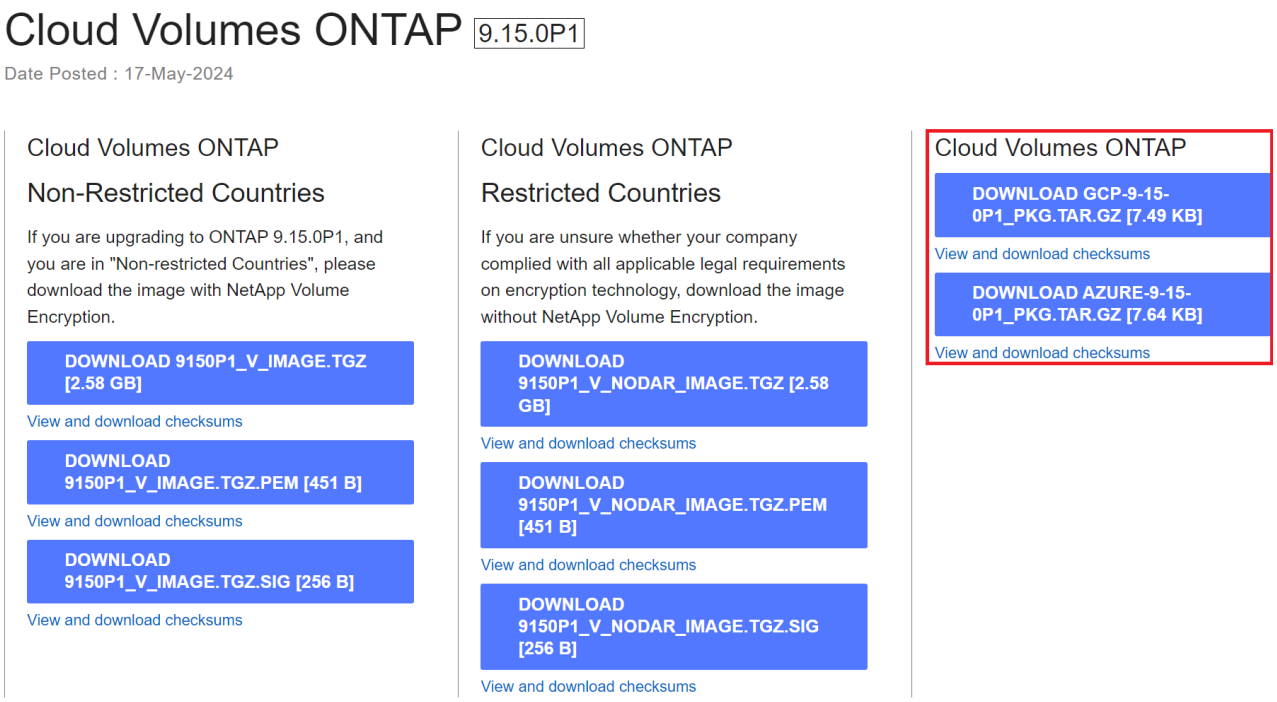
Cloud Volumes ONTAP的 Google Cloud 映像簽章驗證

若要驗證匯出的 Google Cloud 簽章映像，您必須從 NSS 下載映像摘要檔案以驗證 disk.raw 檔案和摘要檔案內容。

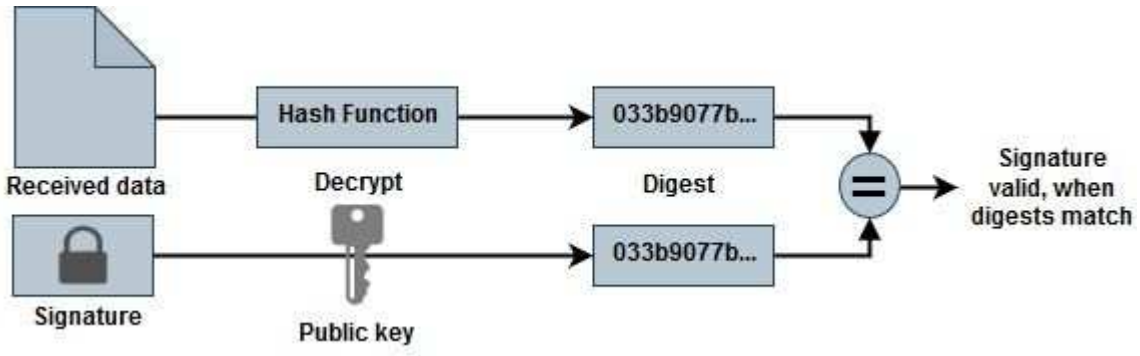
簽名影像驗證工作流程摘要

以下是 Google Cloud 簽名影像驗證工作流程的概述。

- 從 "國家安全局"，下載包含以下文件的 Google Cloud 檔案：
  - 簽名摘要（.sig）
  - 包含公鑰的憑證（.pem）
  - 憑證鏈（.pem）



- 下載轉換後的 disk.raw 文件
- 使用證書鏈驗證證書
- 使用包含公鑰的憑證驗證簽署的摘要
  - 使用公鑰解密簽署的摘要，以提取映像檔的摘要
  - 建立下載的 disk.raw 檔案的摘要
  - 比較兩個摘要文件進行驗證



使用 **OpenSSL** 驗證**Cloud Volumes ONTAP**的 **Google Cloud** 映像 **disk.raw** 文件

您可以透過以下方式驗證 Google Cloud 下載的 disk.raw 檔案與摘要檔案內容 "國家安全局"使用 OpenSSL。

用於驗證映像的 OpenSSL 命令與 Linux、macOS 和 Windows 機器相容。

步驟

1. 使用 OpenSSL 驗證憑證。

點擊顯示

```
# Step 1 - Optional, but recommended: Verify the certificate using
OpenSSL

# Step 1.1 - Copy the Certificate and certificate chain to a
directory
$ openssl version
LibreSSL 3.3.6
$ ls -l
total 48
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem

# Step 1.2 - Get the OSCP URL
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in <Certificate-
Chain.pem>)
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem)
$ echo $oscp_url
http://ocsp.entrust.net

# Step 1.3 - Generate an OCSP request for the certificate
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -reqout <request.der>
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem -reqout req.der

# Step 1.4 - Optional: Check the new file "req.der" has been
generated
$ ls -l
total 56
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der

# Step 1.5 - Connect to the OCSP Manager using openssl to send the
OCSP request
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -url ${ocsp_url} -resp_text
-respout <response.der>
```

```
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem  -url ${ocsp_url} -resp_text
-respout resp.der
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: C = US, O = "Entrust, Inc.", CN = Entrust Extended
Validation Code Signing CA - EVCS2
    Produced At: Jan 19 15:14:00 2023 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: 69FA640329AB84E27220FE0927647B8194B91F2A
      Issuer Key Hash: CE894F8251AA15A28462CA312361D261FBF8FE78
      Serial Number: 5994B3D01D26D594BD1D0FA7098C6FF5
    Cert Status: good
    This Update: Jan 19 15:00:00 2023 GMT
    Next Update: Jan 26 14:59:59 2023 GMT

    Signature Algorithm: sha512WithRSAEncryption
         0b:b6:61:e4:03:5f:98:6f:10:1c:9a:f7:5f:6f:c7:e3:f4:72:
         f2:30:f4:86:88:9a:b9:ba:1e:d6:f6:47:af:dc:ea:e4:cd:31:
         af:e3:7a:20:35:9e:60:db:28:9c:7f:2e:17:7b:a5:11:40:4f:
         1e:72:f7:f8:ef:e3:23:43:1b:bb:28:1a:6f:c6:9c:c5:0c:14:
         d3:5d:bd:9b:6b:28:fb:94:5e:8a:ef:40:20:72:a4:41:df:55:
         cf:f3:db:1b:39:e0:30:63:c9:c7:1f:38:7e:7f:ec:f4:25:7b:
         1e:95:4c:70:6c:83:17:c3:db:b2:47:e1:38:53:ee:0a:55:c0:
         15:6a:82:20:b2:ea:59:eb:9c:ea:7e:97:aa:50:d7:bc:28:60:
         8c:d4:21:92:1c:13:19:b4:e0:66:cb:59:ed:2e:f8:dc:7b:49:
         e3:40:f2:b6:dc:d7:2d:2e:dd:21:82:07:bb:3a:55:99:f7:59:
         5d:4a:4d:ca:e7:8f:1c:d3:9a:3f:17:7b:7a:c4:57:b2:57:a8:
         b4:c0:a5:02:bd:59:9c:50:32:ff:16:b1:65:3a:9c:8c:70:3b:
         9e:be:bc:4f:f9:86:97:b1:62:3c:b2:a9:46:08:be:6b:1b:3c:
         24:14:59:28:c6:ae:e8:d5:64:b2:f8:cc:28:24:5c:b2:c8:d8:
         5a:af:9d:55:48:96:f6:3e:c6:bf:a6:0c:a4:c0:ab:d6:57:03:
         2b:72:43:b0:6a:9f:52:ef:43:bb:14:6a:ce:66:cc:6c:4e:66:
         17:20:a3:64:e0:c6:d1:82:0a:d7:41:8a:cc:17:fd:21:b5:c6:
         d2:3a:af:55:2e:2a:b8:c7:21:41:69:e1:44:ab:a1:dd:df:6d:
         15:99:90:cc:a0:74:1e:e5:2e:07:3f:50:e6:72:a6:b9:ae:fc:
         44:15:eb:81:3d:1a:f8:17:b6:0b:ff:05:76:9d:30:06:40:72:
         cf:d5:c4:6f:8b:c9:14:76:09:6b:3d:6a:70:2c:5a:c4:51:92:
         e5:cd:84:b6:f9:d9:d5:bc:8d:72:b7:7c:13:9c:41:89:a8:97:
         6f:4a:11:5f:8f:b6:c9:b5:df:00:7e:97:20:e7:29:2e:2b:12:
         77:dc:e2:63:48:87:42:49:1d:fc:d0:94:a8:8d:18:f9:07:85:
```

```
          e4:d0:3e:9a:4a:d7:d5:d0:02:51:c3:51:1c:73:12:96:2d:75:
          22:83:a6:70:5a:4a:2b:f2:98:d9:ae:1b:57:53:3d:3b:58:82:
          38:fc:fa:cb:57:43:3f:3e:7e:e0:6d:5b:d6:fc:67:7e:07:7e:
          fb:a3:76:43:26:8f:d1:42:d6:a6:33:4e:9e:e0:a0:51:b4:c4:
          bc:e3:10:0d:bf:23:6c:4b
WARNING: no nonce in response
Response Verify OK
Certificate-GCP-CVO-20230119-0XXXXX.pem: good
    This Update: Jan 19 15:00:00 2023 GMT
    Next Update: Jan 26 14:59:59 2023 GMT

# Step 1.5 - Optional: Check the response file "response.der" has
been generated. Verify its contents.
$ ls -l
total 64
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der
-rw-r--r--  1 example-user  engr   806 Jan 19 16:51 resp.der

# Step 1.6 - Verify the chain of trust and expiration dates against
the local host
$ openssl version -d
OPENSSLDIR: "/private/etc/ssl"
$ OPENSSLDIR=$(openssl version -d | cut -d '"' -f2)
$ echo $OPENSSLDIR
/private/etc/ssl

$ openssl verify -untrusted <Certificate-Chain.pem> -CApath <OpenSSL
dir> <Certificate.pem>
$ openssl verify -untrusted Certificate-Chain-GCP-CVO-20230119-
0XXXXX.pem -CApath ${OPENSSLDIR} Certificate-GCP-CVO-20230119-
0XXXXX.pem
Certificate-GCP-CVO-20230119-0XXXXX.pem: OK
```

2. 將下載的 disk.raw 檔案、簽名和憑證放在一個目錄中。
3. 使用 OpenSSL 從憑證中提取公鑰。
4. 使用提取的公鑰解密簽名並驗證下載的 disk.raw 檔案的內容。

點擊顯示

```
# Step 1 - Place the downloaded disk.raw, the signature and the
certificates in a directory
$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 2 - Extract the public key from the certificate
$ openssl x509 -pubkey -noout -in (certificate.pem) >
(public_key.pem)
$ openssl x509 -pubkey -noout -in Certificate-GCP-CVO-20230119-
0XXXXX.pem > CVO-GCP-pubkey.pem

$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 17:02 CVO-GCP-pubkey.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 3 - Decrypt the signature using the extracted public key and
verify the contents of the downloaded disk.raw
$ openssl dgst -verify (public_key) -keyform PEM -sha256 -signature
(signed digest) -binary (downloaded or obtained disk.raw)
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary disk.raw
Verified OK

# A failed response would look like this
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary
../sample_file.txt
Verification Failure
```