開始使用Google Cloud

Cloud Volumes ONTAP

NetApp
June 27, 2024

目錄

開始使用Google Cloud

在Google Cloud中快速入門Cloud Volumes ONTAP

只要幾個步驟、就能開始使用Cloud Volumes ONTAP 適用於Google Cloud的解決方案。

1 建立連接器

如果您沒有 "連接器" 然而、帳戶管理員需要建立一個帳戶。 "瞭解如何在Google Cloud中建立Connector"

請注意、如果您想要在Cloud Volumes ONTAP 無法存取網際網路的子網路中部署支援、則必須手動安裝Connector、並存取在該Connector上執行的BlueXP使用者介面。 "瞭解如何在無法存取網際網路的位置手動安裝Connector"

2 規劃您的組態

BlueXP提供符合工作負載需求的預先設定套件、或者您也可以建立自己的組態。如果您選擇自己的組態、應該瞭解可用的選項。

"深入瞭解規劃組態"。

3 設定您的網路

1. 確保您的 VPC 和子網路支援連接器與 Cloud Volumes ONTAP 支援之間的連線。
2. 如果您打算啟用資料分層、 "設定Cloud Volumes ONTAP 私有Google Access的子網路"。
3. 如果您要部署 HA 配對、請確定您有四個 VPC 、每個 VPC 都有自己的子網路。
4. 如果您使用的是共享VPC、請將_Compute Network User_角色提供給Connector服務帳戶。
5. 啟用從目標VPC for NetApp AutoSupport 的傳出網際網路存取功能。

   如果您在Cloud Volumes ONTAP 無法存取網際網路的位置部署支援、則不需要執行此步驟。

"深入瞭解網路需求"。

4 設定服務帳戶

下列兩種用途需要Google Cloud服務帳戶：Cloud Volumes ONTAP第一個是啟用時 "資料分層" 將冷資料分層至Google Cloud中的低成本物件儲存設備。第二個是啟用時 "BlueXP 備份與還原" 將磁碟區備份至低成本的物件儲存設備。

您可以設定一個服務帳戶、並將其用於這兩種用途。服務帳戶必須具有*儲存設備管理*角色。

"閱讀逐步指示"。

5 啟用 **Google Cloud API**

"在專案中啟用下列 Google Cloud API"。這些 API 是部署連接器和 Cloud Volumes ONTAP 功能不全的必備條件。

- Cloud Deployment Manager V2 API
- 雲端記錄 API
- Cloud Resource Manager API
- 運算引擎 API
- 身分識別與存取管理（ IAM ） API

6 使用**BlueXP**啟動**Cloud Volumes ONTAP**

按一下「 * 新增工作環境 * 」、選取您要部署的系統類型、然後完成精靈中的步驟。 "閱讀逐步指示"。

相關連結

- "從BlueXP建立連接器"
- "在 Linux 主機上安裝 Connector 軟體"
- "BlueXP使用Google Cloud權限的功能"

在Cloud Volumes ONTAP Google Cloud規劃您的不一樣組態

在 Cloud Volumes ONTAP Google Cloud 中部署時、您可以選擇符合工作負載需求的預先設定系統、或是建立自己的組態。如果您選擇自己的組態、應該瞭解可用的選項。

選擇**Cloud Volumes ONTAP** 一個不含功能的授權

有多種授權選項可供Cloud Volumes ONTAP 選擇。每個選項都能讓您選擇符合需求的消費模式。

- "深入瞭Cloud Volumes ONTAP 解適用於此功能的授權選項"
- "瞭解如何設定授權"

選擇支援的地區

支援大部分Google Cloud地區的支援。Cloud Volumes ONTAP "檢視支援區域的完整清單"。

選擇支援的機器類型

根據您選擇的授權類型、支援多種機器類型。 Cloud Volumes ONTAP

"支援的GCP組態Cloud Volumes ONTAP"

瞭解儲存限制

一個不含資源的系統的原始容量上限 Cloud Volumes ONTAP 與授權有關。其他限制會影響集合體和磁碟區的大小。在規劃組態時、您應該注意這些限制。

"適用於GCP的儲存限制Cloud Volumes ONTAP"

在 GCP 中調整系統大小

調整 Cloud Volumes ONTAP 您的支援規模、有助於滿足效能與容量的需求。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

請查看中支援的機器類型 "發行說明 Cloud Volumes ONTAP" 然後檢視 Google 提供的每種受支援機器類型的詳細資料。將工作負載需求與機器類型的 vCPU 和記憶體數量配對。請注意、每個 CPU 核心都能提升網路效能。

如需詳細資料、請參閱下列內容：

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

GCP 磁碟類型

當您建立 Cloud Volumes ONTAP 用於資料的 Volume 時、您需要選擇 Cloud Volumes ONTAP 基礎雲端儲存設備、以便將其用於磁碟。磁碟類型可以是下列任一種：

- *Zonal SSD*持續式磁碟：SSD持續式磁碟最適合需要高隨機IOPS速率的工作負載。
- 分區平衡的持續磁碟：這些SSD可提供較低的每GB IOPS、以平衡效能與成本。
- *Zonal Standard*持續式磁碟：標準持續式磁碟經濟實惠、可處理連續讀寫作業。

  如需詳細資料、請參閱 "Google Cloud 文件：分區持續磁碟（標準和 SSD ）"。

GCP 磁碟大小

部署 Cloud Volumes ONTAP 一套系統時、您需要選擇初始磁碟大小。之後、您可以讓BlueXP為您管理系統容量、但如果您想自行建置集合體、請注意下列事項：

- 集合體中的所有磁碟大小必須相同。
- 判斷您需要的空間、同時考量效能。
- 持續性磁碟的效能會隨著磁碟大小和系統可用的 vCPU 數目而自動擴充。

  如需詳細資料、請參閱下列內容：

  - "Google Cloud 文件：分區持續磁碟（標準和 SSD ）"
  - "Google Cloud 文件：最佳化持續磁碟和本機 SSD 效能"

檢視預設系統磁碟

除了儲存使用者資料之外、BlueXP也購買雲端儲存設備來儲存Cloud Volumes ONTAP 作業系統資料（開機資料、根資料、核心資料和NVRAM）。為了規劃目的、在部署Cloud Volumes ONTAP 完更新之前、您可能需要先檢閱這些詳細資料。

- "在Cloud Volumes ONTAP Google Cloud中檢視系統資料的預設磁碟"。
- "Google Cloud文件：資源配額"

  Google Cloud Compute Engine會強制執行資源使用量配額、因此您應該在部署Cloud Volumes ONTAP 時確保未達到上限。

連接器也需要系統磁碟。 "檢視Connector預設組態的詳細資料"。

收集網路資訊

在 Cloud Volumes ONTAP GCP 中部署時、您需要指定虛擬網路的詳細資料。您可以使用工作表向系統管理員收集資訊。

- 單節點系統的網路資訊 *

GCP 資訊	您的價值
區域	
區域	
VPC 網路	
子網路	
防火牆原則（如果使用您自己的）	

- 多個區域中 HA 配對的網路資訊 *

GCP 資訊	您的價值
區域	
節點 1 的區域	
節點 2 的區域	
中介人區域	
VPC-0 和子網路	
VPC-1 和子網路	
VPC-2 和子網路	
VPC-3 和子網路	
防火牆原則（如果使用您自己的）	

- 單一區域中 HA 配對的網路資訊 *

GCP 資訊	您的價值
區域	
區域	
VPC-0 和子網路	
VPC-1 和子網路	
VPC-2 和子網路	
VPC-3 和子網路	
防火牆原則（如果使用您自己的）	

選擇寫入速度

BlueXP可讓您選擇Cloud Volumes ONTAP 適合的寫入速度設定、但Google Cloud中的高可用度（HA）配對除外。在您選擇寫入速度之前、您應該先瞭解一般與高設定之間的差異、以及使用高速寫入速度時的風險與建議。"深入瞭解寫入速度"。

選擇Volume使用設定檔

包含多項儲存效率功能、可減少您所需的總儲存容量。 ONTAP在BlueXP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。您應該深入瞭解這些功能、以協助您決定要使用的設定檔。

NetApp 儲存效率功能提供下列效益：

資源隨需配置

為主機或使用者提供比實體儲存資源池實際擁有更多的邏輯儲存設備。儲存空間不會預先配置儲存空間、而是會在寫入資料時動態分配給每個磁碟區。

重複資料刪除

找出相同的資料區塊、並以單一共用區塊的參考資料取代這些區塊、藉此提升效率。這項技術可消除位於同一個磁碟區的備援資料區塊、進而降低儲存容量需求。

壓縮

藉由壓縮主儲存設備、次儲存設備和歸檔儲存設備上磁碟區內的資料、來減少儲存資料所需的實體容量。

Google Cloud中的功能需求Cloud Volumes ONTAP

設定您的Google Cloud網路功能、Cloud Volumes ONTAP 讓各個系統都能正常運作。

如果您想要部署 HA 配對、應該這樣做 "瞭解HA配對如何在Google Cloud中運作"。

需求 Cloud Volumes ONTAP

Google Cloud必須符合下列要求。

單一節點系統的特定需求

如果您要部署單一節點系統、請確定您的網路符合下列需求。

一個**VPC**

單一節點系統需要一個虛擬私有雲（VPC）。

私有**IP**位址

BlueXP會將3或4個私有IP位址分配給Google Cloud中的單一節點系統。

如果Cloud Volumes ONTAP 您使用API部署了Sf2並指定下列旗標、則可以跳過儲存VM（SVM）管理LIF的建立：

```
skipSvmManagementLif: true
```

LIF 是與實體連接埠相關聯的 IP 位址。諸如VMware等管理工具需要儲存VM（SVM）管理LIF SnapCenter 。

HA配對的特定需求

如果您要部署HA配對、請確定您的網路符合下列需求。

一個或多個區域

您可以跨多個區域或單一區域部署HA組態、確保資料的高可用度。建立HA配對時、BlueXP會提示您選擇多個區域或單一區域。

- 多個區域（建議）

  跨三個區域部署 HA 組態、可確保在區域內發生故障時、仍能持續提供資料。請注意、與使用單一區域相比、寫入效能略低、但卻是最低的。

- 單一區域

  當部署在單一區域時、 Cloud Volumes ONTAP 使用分散配置原則的即可實現不受限制的 HA 組態。此原則可確保 HA 組態不會在區域內發生單點故障、而無需使用個別區域來實現故障隔離。

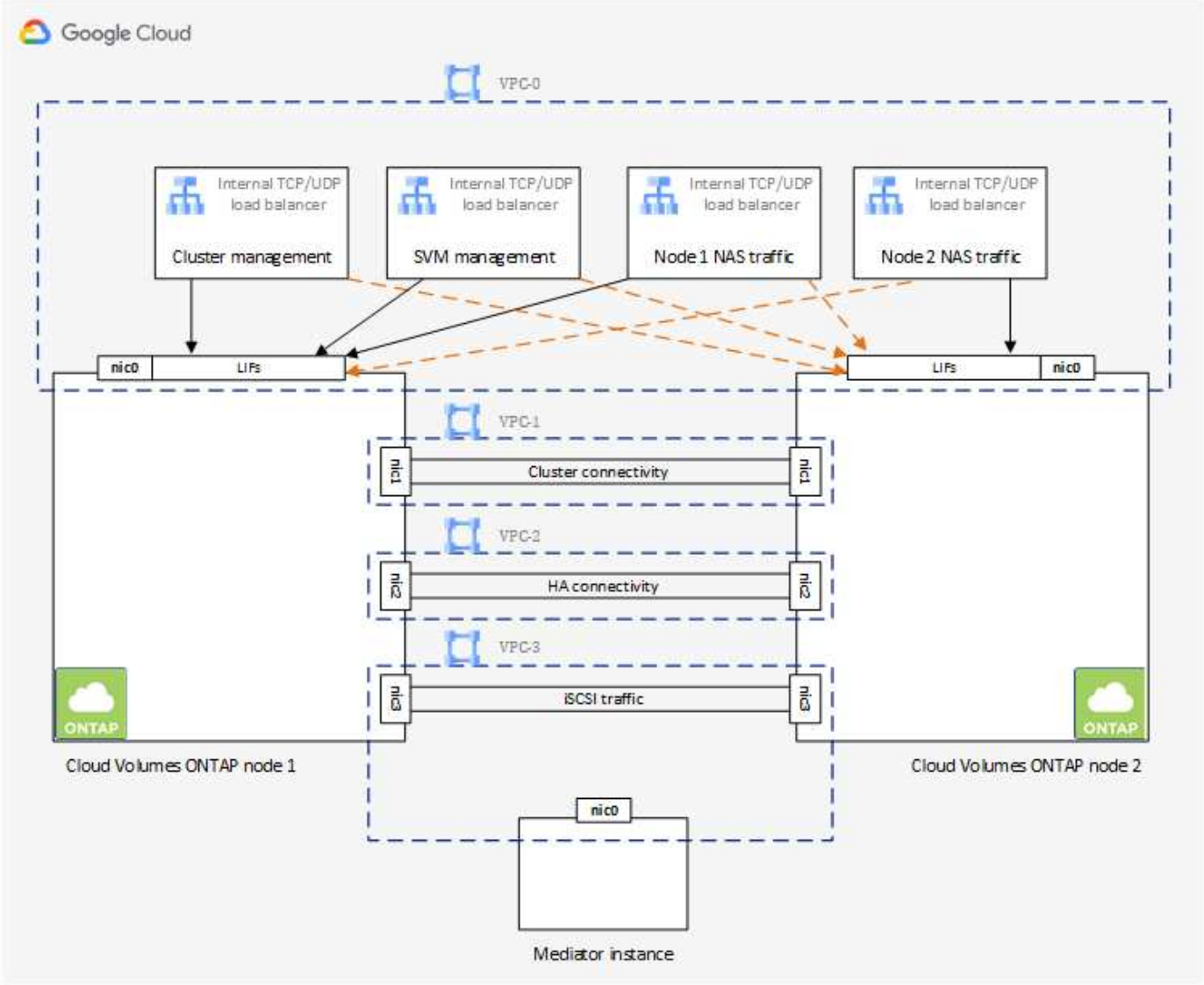
  此部署模式可降低成本、因為各區域之間不需支付任何資料出口費用。

四個虛擬私有雲端

HA組態需要四個虛擬私有雲端（VPC）。由於Google Cloud要求每個網路介面都位於獨立的VPC網路、因此需要四個VPC。

在建立HA配對時、BlueXP會提示您選擇四個VPC：

- VPC-0 用於資料和節點的傳入連線
- VPC-1 、 VPC-2 和 VPC-3 用於節點與 HA 中介器之間的內部通訊



子網路

每個VPC都需要私有子網路。

如果您將Connector放在VPC-0中、則必須在子網路上啟用私有Google Access、才能存取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。

私有**IP**位址

在Cloud Volumes ONTAP Google Cloud中、BlueXP會自動分配所需數量的私有IP位址給功能。您必須確定網路有足夠的私有位址可供使用。

BlueXP分配Cloud Volumes ONTAP 給功能的生命量取決於您是部署單一節點系統或HA配對。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 。

- 單一節點
  BlueXP 會將 4 個 IP 位址分配給單一節點系統：
  - 節點管理 LIF

- 叢集管理LIF
- iSCSI資料LIF

  > iSCSI LIF可透過iSCSI傳輸協定提供用戶端存取、並供系統用於其他重要的網路工作流程。這些生命是必要的、不應刪除。

- NAS LIF

  如果Cloud Volumes ONTAP 您使用API部署了Sf2並指定下列旗標、則可以跳過儲存VM（SVM）管理LIF的建立：

```
skipSvmManagementLif: true
```

- * HA 配對 *
  BlueXP 會將 12-13 個 IP 位址分配給 HA 配對：
  - 2個節點管理生命里數（e0a）
  - 1叢集管理LIF（e0a）
  - 2個iSCSI LIF（e0a）

    > iSCSI LIF可透過iSCSI傳輸協定提供用戶端存取、並供系統用於其他重要的網路工作流程。這些生命是必要的、不應刪除。

  - 1或2個NAS lifs（e0a）
  - 2個叢集LIF（e0b）
  - 2個HA互連IP位址（e0c）
  - 2個RSMiSCSI IP位址（e0d）

    如果Cloud Volumes ONTAP 您使用API部署了Sf2並指定下列旗標、則可以跳過儲存VM（SVM）管理LIF的建立：

```
skipSvmManagementLif: true
```

內部負載平衡器

BlueXP會自動建立四個Google Cloud內部負載平衡器（TCP/IP）、以管理Cloud Volumes ONTAP 傳入至該HA配對的流量。您不需要在結束時進行任何設定我們將此列為一項要求、只是告知您網路流量、並減輕任何安全顧慮。

其中一個負載平衡器用於叢集管理、一個用於儲存VM（SVM）管理、一個用於連接節點1的NAS流量、最後一個用於連接節點2的NAS流量。

每個負載平衡器的設定如下：

- 一個共享的私有IP位址
- 一次全域健全狀況檢查

  根據預設、狀況檢查所使用的連接埠為63001、63002和63003。

- 一個區域TCP後端服務
- 一個區域性的udp後端服務
- 一個TCP轉送規則
- 一個udp轉送規則
- 全域存取已停用

  即使預設停用全域存取、仍支援在部署後啟用IT。我們停用此功能、因為跨區域流量的延遲時間會大幅增加。我們希望確保您不會因為意外的跨區域裝載而有負面體驗。啟用此選項是專為您的業務需求所打造。

共享**VPC**

支援的對象包括 Google Cloud 共享 VPC 和獨立 VPC 。 Cloud Volumes ONTAP

對於單一節點系統、VPC可以是共享VPC或獨立VPC。

HA配對需要四個VPC。每個VPC都可以是共享的或獨立的。例如、VPC-0可以是共享VPC、VPC-1、VPC-2和VPC-3則可以是獨立式VPC。

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 _ 中部署連接器與支援虛擬機器執行個體。 "Google Cloud 文件：共享 VPC 總覽"。

"檢閱Connector部署所涵蓋的必要共享VPC權限"

VPC中的封包鏡射

"封包鏡射" 必須在部署Cloud Volumes ONTAP 了下列項目的Google Cloud VPC中停用。啟用封包鏡射時、無法正常運作。Cloud Volumes ONTAP

傳出網際網路存取

NetApp支援需要外傳網際網路存取功能、才能主動監控系統健全狀況、並將訊息傳送給NetApp技術支援部門。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

如果傳出的網際網路連線無法傳送AutoSupport 功能性訊息、則BlueXP會自動將Cloud Volumes ONTAP 您的功能性更新系統設定為使用Connector做為Proxy伺服器。唯一的需求是確保連接器的防火牆允許連接埠3128上的傳入連線。部署Connector之後、您需要開啟此連接埠。

如果您定義了Cloud Volumes ONTAP 嚴格的出站規則以供支援、那麼您也必須確保Cloud Volumes ONTAP 透過連接埠3128建立的支援_出站_連線。

在您確認可以存取傳出網際網路之後、您可以測試AutoSupport 以確保能夠傳送訊息。如需相關指示、請參閱 "文件：設定檔ONTAP AutoSupport"。

如果您使用 HA 配對、 HA 中介器不需要傳出網際網路存取。

如果BlueXP通知您AutoSupport 無法傳送資訊、 "疑難排解AutoSupport 您的VMware組態"。

防火牆規則

您不需要建立防火牆規則、因為BlueXP會為您執行這些規則。如果您需要使用自己的防火牆、請參閱下列防火牆規則。

請注意、 HA 組態需要兩組防火牆規則：

- VPC-0 中 HA 元件的一組規則。這些規則可讓您存取 Cloud Volumes ONTAP 資料以存取資料。 深入瞭解。
- VPC-1 、 VPC-2 和 VPC-3 中的另一組 HA 元件規則。這些規則可用於 HA 元件之間的傳入和傳出通訊。 深入瞭解。

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 （如果您使用 HA 配對、則此子網路位於 VPC-0 ）。如需相關指示、請參閱 "Google Cloud 文件：設定私有 Google Access"。

如需在BlueXP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 Google Cloud中的某個支援中心系統與ONTAP 其他網路中的支援中心系統之間複寫資料、您必須在VPC與其他網路（例如公司網路）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"。

防火牆規則

BlueXP會建立Google Cloud防火牆規則、其中包括Cloud Volumes ONTAP 需要順利運作的傳入和傳出規則。您可能需要參照連接埠進行測試、或是偏好使用自己的防火牆規則。

適用於此功能的防火牆規則 Cloud Volumes ONTAP 需要傳入和傳出規則。如果您要部署 HA 組態、 Cloud Volumes ONTAP 以下是 VPC-0 中的防火牆規則。

請注意、 HA 組態需要兩組防火牆規則：

- VPC-0 中 HA 元件的一組規則。這些規則可讓您存取 Cloud Volumes ONTAP 資料以存取資料。
- VPC-1 、 VPC-2 和 VPC-3 中的另一組 HA 元件規則。這些規則可用於 HA 元件之間的傳入和傳出通訊。 深入瞭解。

正在尋找Connector的相關資訊？ "檢視Connector的防火牆規則"

傳入規則

建立工作環境時、您可以在部署期間選擇預先定義防火牆原則的來源篩選器：

- *限選定VPC *：傳入流量的來源篩選器為VPC的子網路範圍、Cloud Volumes ONTAP 適用於該系統、以及連接器所在VPC的子網路範圍。這是建議的選項。

- 所有**VPC**：傳入流量的來源篩選器為0.00.0.0/0 IP範圍。

如果您使用自己的防火牆原則、請確定您新增了所有需要與Cloud Volumes ONTAP 之通訊的網路、但同時也請務必新增這兩個位址範圍、以讓內部Google負載平衡器正常運作。這些位址分別為130.211.0.0/22和35.191.0/16。如需詳細資訊、請參閱 "Google Cloud文件：負載平衡器防火牆規則"。

傳輸協定	連接埠	目的
所有ICMP	全部	Ping 執行個體
HTTP	80	使用叢集管理 LIF 的 IP 位址、以 HTTP 存取 System Manager Web 主控台
HTTPS	443..	使用叢集管理LIF的IP位址、連線到Connector和HTTPS、存取System Manager Web主控台
SSH	22.	SSH 存取叢集管理 LIF 的 IP 位址或節點管理 LIF
TCP	111.	遠端程序需要 NFS
TCP	139.	CIFS 的 NetBios 服務工作階段
TCP	161-162-163.	簡單的網路管理傳輸協定
TCP	445	Microsoft SMB/CIFS over TCP 搭配 NetBios 架構
TCP	635	NFS 掛載
TCP	749	Kerberos
TCP	2049	NFS 伺服器精靈
TCP	3260	透過 iSCSI 資料 LIF 存取 iSCSI
TCP	4045	NFS 鎖定精靈
TCP	4046	NFS 的網路狀態監控
TCP	10000	使用 NDMP 備份
TCP	11104.	管理 SnapMirror 的叢集間通訊工作階段
TCP	11105.	使用叢集間生命體進行 SnapMirror 資料傳輸
TCP	63001-63050	負載平衡探針連接埠、判斷哪個節點正常（僅 HA 配對需要）
UDP	111.	遠端程序需要 NFS
UDP	161-162-163.	簡單的網路管理傳輸協定
UDP	635	NFS 掛載
UDP	2049	NFS 伺服器精靈
UDP	4045	NFS 鎖定精靈
UDP	4046	NFS 的網路狀態監控
UDP	4049	NFS rquotad 傳輸協定

預先定義 Cloud Volumes ONTAP 的 Security Group for the 旅行團會開啟所有的傳出流量。如果可以接受、請遵循基本的傳出規則。如果您需要更嚴格的規則、請使用進階的傳出規則。

基本傳出規則

適用於此功能的預先定義安全性群組 Cloud Volumes ONTAP 包括下列傳出規則。

傳輸協定	連接埠	目的
所有 ICMP	全部	所有傳出流量
所有 TCP	全部	所有傳出流量
所有的 udp	全部	所有傳出流量

進階傳出規則

如果您需要嚴格的傳出流量規則、可以使用下列資訊、僅開啟 Cloud Volumes ONTAP 那些由真人進行傳出通訊所需的連接埠。

來源是 Cloud Volumes ONTAP 指在整個系統上的介面（ IP 位址）。

服務	傳輸協定	連接埠	來源	目的地	目的
Active Directory	TCP	88	節點管理 LIF	Active Directory 樹系	Kerberos V 驗證
	UDP	137.	節點管理 LIF	Active Directory 樹系	NetBios 名稱服務
	UDP	138	節點管理 LIF	Active Directory 樹系	NetBios 資料報服務
	TCP	139.	節點管理 LIF	Active Directory 樹系	NetBios 服務工作階段
	TCP 與 UDP	389..	節點管理 LIF	Active Directory 樹系	LDAP
	TCP	445	節點管理 LIF	Active Directory 樹系	Microsoft SMB/CIFS over TCP 搭配 NetBios 架構
	TCP	464. 64	節點管理 LIF	Active Directory 樹系	Kerberos V 變更及設定密碼（ Set_change ）
	UDP	464. 64	節點管理 LIF	Active Directory 樹系	Kerberos 金鑰管理
	TCP	749	節點管理 LIF	Active Directory 樹系	Kerberos V 變更與設定密碼（ RPCSEC_GSS ）
	TCP	88	資料 LIF （ NFS 、 CIFS 、 iSCSI ）	Active Directory 樹系	Kerberos V 驗證
	UDP	137.	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	NetBios 名稱服務
	UDP	138	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	NetBios 資料報服務
	TCP	139.	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	NetBios 服務工作階段
	TCP 與 UDP	389..	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	LDAP
	TCP	445	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	Microsoft SMB/CIFS over TCP 搭配 NetBios 架構
	TCP	464. 64	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	Kerberos V 變更及設定密碼（ Set_change ）
	UDP	464. 64	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	Kerberos 金鑰管理
	TCP	749	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	Kerberos V 變更及設定密碼（ RPCSEC_GSS ）
AutoSupport	HTTPS	443..	節點管理 LIF	support.netapp.com	支援（預設為HTTPS）AutoSupport
	HTTP	80	節點管理 LIF	support.netapp.com	僅當傳輸傳輸傳輸傳輸傳輸傳輸協定從HTTPS變更為HTTP 時、AutoSupport
	TCP	3128	節點管理 LIF	連接器	如果無法使用傳出的網際網路連線、請透過Connector上的Proxy伺服器傳送AutoSupport 功能介紹訊息

服務	傳輸協定	連接埠	來源	目的地	目的
叢集	所有流量	所有流量	一個節點上的所有 LIF	其他節點上的所有 LIF	叢集間通訊（ Cloud Volumes ONTAP 僅限不含 HA ）
組態備份	HTTP	80	節點管理 LIF	\http ： //// <connector-IP-address> occm/offboxconfig	將組態備份傳送至Connector。 "深入瞭解組態備份檔案"。
DHCP	UDP	68	節點管理 LIF	DHCP	第一次設定的 DHCP 用戶端
DHCPS	UDP	67	節點管理 LIF	DHCP	DHCP 伺服器
DNS	UDP	53.	節點管理 LIF 與資料 LIF （ NFS 、 CIFS ）	DNS	DNS
NDMP	TCP	18600 – 18699	節點管理 LIF	目的地伺服器	NDMP 複本
SMTP	TCP	25.	節點管理 LIF	郵件伺服器	可以使用 SMTP 警示 AutoSupport 來執行功能
SNMP	TCP	161.	節點管理 LIF	監控伺服器	透過 SNMP 設陷進行監控
	UDP	161.	節點管理 LIF	監控伺服器	透過 SNMP 設陷進行監控
	TCP	162-1662	節點管理 LIF	監控伺服器	透過 SNMP 設陷進行監控
	UDP	162-1662	節點管理 LIF	監控伺服器	透過 SNMP 設陷進行監控
SnapMirror	TCP	11104.	叢集間 LIF	叢集間 LIF ONTAP	管理 SnapMirror 的叢集間通訊工作階段
	TCP	11105.	叢集間 LIF	叢集間 LIF ONTAP	SnapMirror 資料傳輸
系統記錄	UDP	514	節點管理 LIF	系統記錄伺服器	系統記錄轉送訊息

VPC-1、**VPC-2**和**VPC-3**的規則

在Google Cloud中、HA組態部署於四個VPC上。VPC-0 中 HA 組態所需的防火牆規則為 以上所列 Cloud Volumes ONTAP 的 for 列舉。

同時、BlueXP針對VPC-1、VPC-2和VPC-3中的執行個體所建立的預先定義防火牆規則、可透過_all_傳輸協定和連接埠進行入侵通訊。這些規則可在HA節點之間進行通訊。

HA節點與HA中介器之間的通訊會透過連接埠3260（iSCSI）進行。

若要為新的Google Cloud HA配對部署啟用高速寫入速度、VPC-1、VPC-2和VPC-3至少需要8、896位元組的最大傳輸單元（MTU）。如果您選擇將現有VPC-1、VPC-2和VPC-3升級為8、896位元組的MTU、則必須在組態程序期間使用這些VPC關閉所有現有的HA系統。

連接器需求

如果您尚未建立連接器、也應該檢閱連接器的網路需求。

- "檢視連接器的網路需求"
- "Google Cloud中的防火牆規則"

在GCP中規劃VPC服務控制

選擇使用VPC服務控制來鎖定Google Cloud環境時、您應該瞭解BlueXP和Cloud Volumes ONTAP Isa如何與Google Cloud API互動、以及如何設定服務邊界以部署BlueXP和Cloud Volumes ONTAP Isa。

VPC服務控管可讓您控制在信任邊界之外存取Google管理的服務、封鎖來自不信任位置的資料存取、並降低未獲授權的資料傳輸風險。 "深入瞭解Google Cloud VPC服務控制"。

NetApp服務如何與VPC服務控制通訊

BlueXP直接與Google Cloud API通訊。這可能是從Google Cloud外部的外部IP位址觸發（例如從api.services.cloud.netapp.com）、或從指派給BlueXP Connector的內部位址觸發。

視連接器的部署風格而定、您可能需要針對服務邊界進行某些例外。

映像

支援使用NetApp管理的GCP專案影像。Cloud Volumes ONTAP如果Cloud Volumes ONTAP 您的組織有封鎖使用組織內未託管之映像的原則、這可能會影響到BlueXP Connector和功能的部署。

您可以使用手動安裝方法手動部署Connector、Cloud Volumes ONTAP 但也需要從NetApp專案中擷取影像。您必須提供允許的清單、才能部署連接器和Cloud Volumes ONTAP 功能表。

部署**Connector**

部署Connector的使用者必須能夠參考專案ID *NetApp-cloudmanag__*中裝載的映像、以及專案編號*_14190056516*。

部署**Cloud Volumes ONTAP** 功能

- BlueXP服務帳戶需要參考專案ID *NetApp-cloudmanager-_*中的映像、以及服務專案中的專案編號*_14190056516*。
- 預設Google API服務代理程式的服務帳戶必須參考專案ID *NetApp-cloudmanag__*中所裝載的映像、以及服務專案中的專案編號*_14190056516*。

以下是使用VPC服務控制擷取這些影像所需的規則範例。

VPC服務控制周邊原則

原則允許VPC服務控制規則集例外。如需原則的詳細資訊、請參閱 "GCP VPC服務控制原則文件"。

若要設定BlueXP所需的原則、請瀏覽至組織內部的VPC服務控制周邊、然後新增下列原則。這些欄位應符合VPC服務控制原則頁面中提供的選項。另請注意、* all *規則是必要的、且*或*參數應用於規則集中。

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

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

或

```
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
```

上述專案編號是NetApp用來儲存Connector和Cloud Volumes ONTAP for the SURO影像的專案_NetApp-cloudmanag__。

建立資料分層與備份的服務帳戶

下列兩種用途需要Google Cloud服務帳戶：Cloud Volumes ONTAP第一個是啟用時 "資料分層" 將冷資料分層至Google Cloud中的低成本物件儲存設備。第二個是啟用時 "BlueXP 備份與還原" 將磁碟區備份至低成本的物件儲存設備。

使用服務帳戶存取及管理階層資料的儲存庫、以及另一個儲存庫進行備份。Cloud Volumes ONTAP

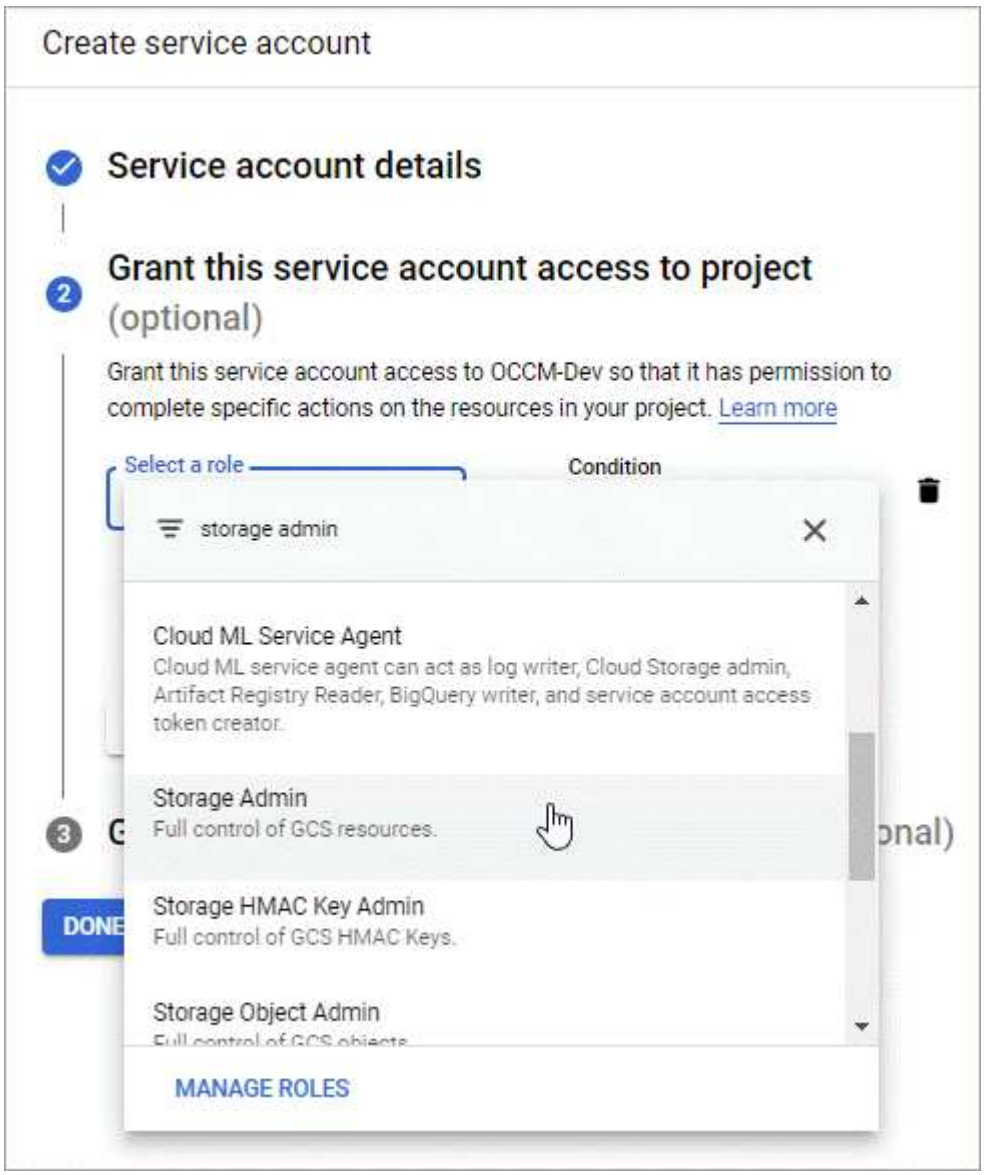
您可以設定一個服務帳戶、並將其用於這兩種用途。服務帳戶必須具有*儲存設備管理*角色。

步驟

1. 在Google Cloud主控台中、 "前往「服務帳戶」頁面"。
2. 選取您的專案。
3. 按一下「建立服務帳戶」、並提供必要資訊。

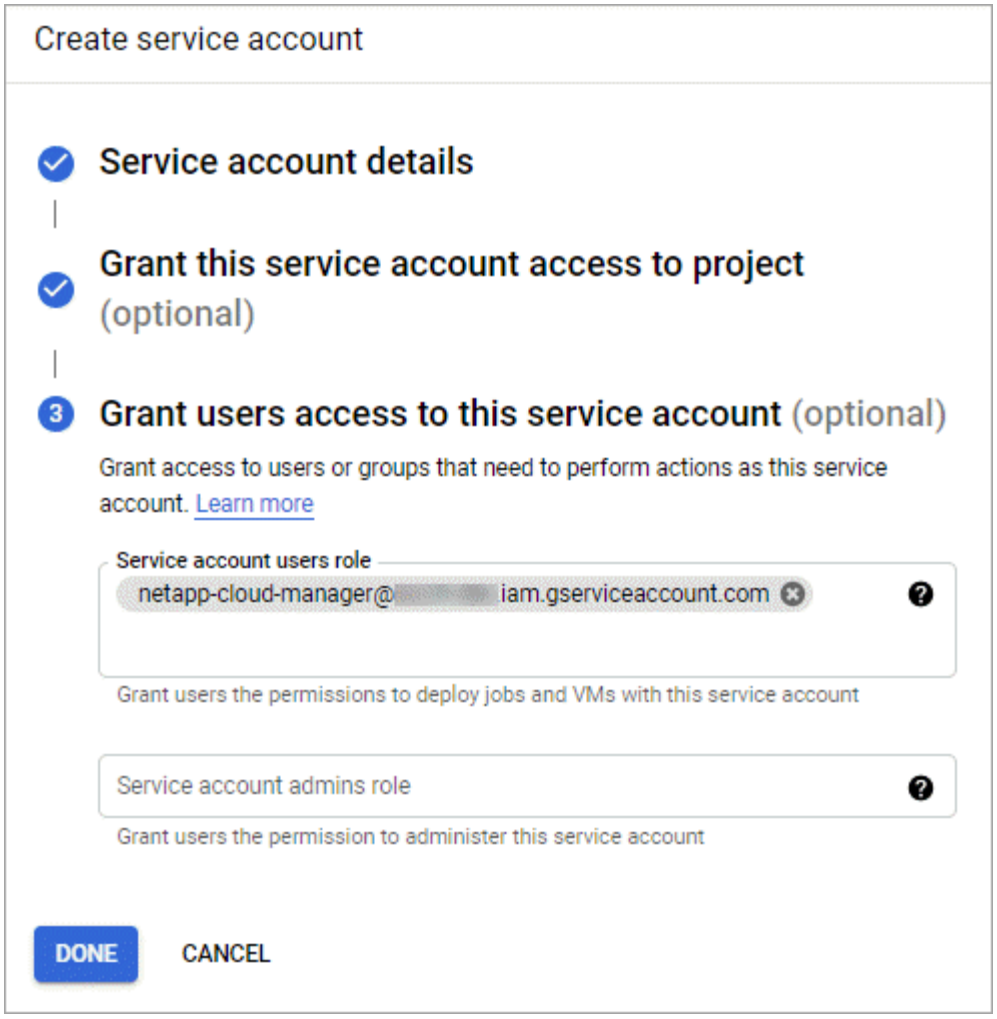
    a. 服務帳戶詳細資料：輸入名稱和說明。

b. 授予此服務帳戶專案存取權：選取*儲存管理員*角色。



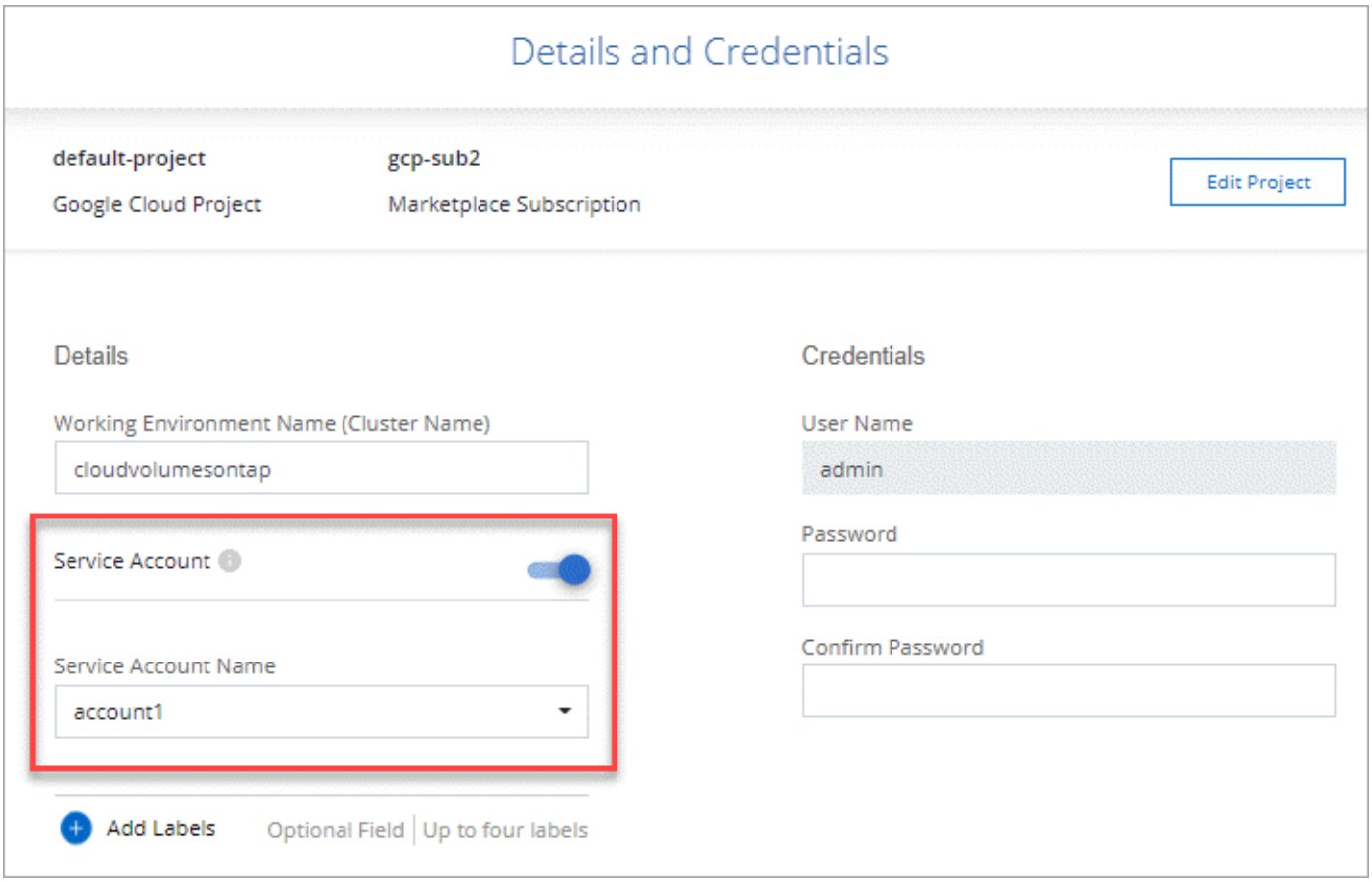
c. 授予使用者此服務帳戶的存取權：將Connector服務帳戶新增為_Service Account User_至此新的服務帳戶。

此步驟僅適用於資料分層。BlueXP 備份與還原不需要此功能。



接下來呢？

建立Cloud Volumes ONTAP 一套運作環境時、您稍後需要選擇服務帳戶。



搭配 Cloud Volumes ONTAP 使用客戶管理的加密金鑰

雖然Google Cloud Storage會在資料寫入磁碟之前先加密資料、但您可以使用BlueXP API來建立Cloud Volumes ONTAP 使用_客戶管理的加密金鑰_的支援系統。這些是您使用Cloud Key Management Service 在 GCP 中產生及管理的金鑰。

步驟

1. 確認BlueXP Connector服務帳戶在專案層級（儲存金鑰的專案）擁有正確的權限。

   權限會在中提供 "連接器服務帳戶權限依預設"、但如果您使用雲端金鑰管理服務的替代專案、則可能無法套用。

   權限如下：

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

2. 確認的服務帳戶 "Google Compute Engine服務代理程式" 具有金鑰的Cloud KMS Encrypter/Dec供 解密權限。

   服務帳戶名稱使用下列格式：「service-[service_project _number]@ compute-

system.iam.gserviceaccount.com」。

"Google Cloud文件：使用IAM搭配Cloud KMS使用-授予資源角色"

3. 請叫用的取得命令、以取得金鑰的「 id 」 `/gcp/vsa/metadata/gcp-encryption-keys` API 呼叫或在 GCP 主控台的金鑰上選擇「複製資源名稱」。
4. 如果使用客戶管理的加密金鑰和分層資料來物件儲存設備、則BlueXP會嘗試使用相同的金鑰來加密持續磁碟。但您必須先啟用Google Cloud Storage儲存桶、才能使用這些金鑰：

   a. 請依照下列步驟尋找Google Cloud Storage服務代理程式 "Google Cloud文件：取得Cloud Storage服務代理程式"。

   b. 瀏覽至加密金鑰、並指派具有Cloud KMS Encrypter/Decypter權限的Google Cloud Storage服務代理程式。

   如需詳細資訊、請參閱 "Google Cloud文件：使用客戶管理的加密金鑰"

5. 建立工作環境時、請將「 GcpEncryption 」參數搭配 API 要求使用。

   。範例 *

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

請參閱 "藍圖XP自動化文件" 如需使用「 GcpEncryption 」參數的詳細資訊、

在Cloud Volumes ONTAP Google Cloud中設定適用於此技術的授權

決定Cloud Volumes ONTAP 要搭配使用哪種授權選項之後、您必須先執行幾個步驟、才能在建立新的工作環境時選擇授權選項。

Freemium

選擇Freemium產品、即可免費使用Cloud Volumes ONTAP 多達500 GiB的配置容量。 "深入瞭解Freemium產品"。

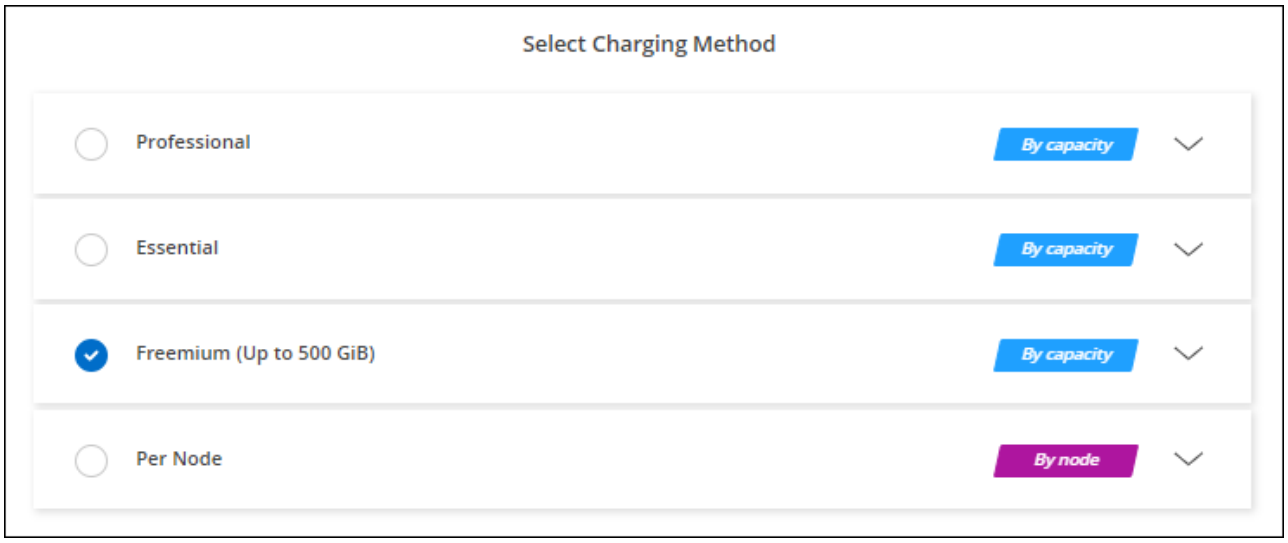
步驟

1. 從左側導覽功能表中、選取*儲存設備> Canvas*。
2. 在「畫版」頁面上、按一下「新增工作環境」、然後依照BlueXP中的步驟進行。

   a. 在*詳細資料與認證*頁面上、按一下*編輯認證>新增訂閱*、然後依照提示訂閱Google Cloud Marketplace中的隨用隨付方案。

   除非您超過500 GiB的已配置容量、系統會自動轉換為、否則不會透過市場訂閱付費 "Essentials套件"。

   b. 返回BluetXP之後、當您到達「充電方法」頁面時、請選取* Freemium *。



"請參閱逐步指示Cloud Volumes ONTAP 、在Google Cloud中啟動「功能不全」"。

容量型授權

容量型授權可讓您針對Cloud Volumes ONTAP 容量的每個TiB付費。容量型授權的形式為_package_：Essentials套件或Professional套件。

Essentials和Professional套件可搭配下列消費模式使用：

- 向NetApp購買的授權（BYOL）
- 從Google Cloud Marketplace訂閱時數小時隨付（PAYGO）
- 年度合約

"深入瞭解容量型授權"。

下列各節將說明如何開始使用這些消費模式。

BYOL

事先向NetApp購買授權（BYOL）、即可在Cloud Volumes ONTAP 任何雲端供應商部署支援系統。

步驟

1. "請聯絡NetApp銷售人員以取得授權"
2. "將NetApp 支援網站 您的不更新帳戶新增至藍圖XP"

   BlueXP會自動查詢NetApp的授權服務、以取得NetApp 支援網站 與您的還原帳戶相關之授權的詳細資料。如果沒有錯誤、 BlueXP 會自動將授權新增至數位錢包。

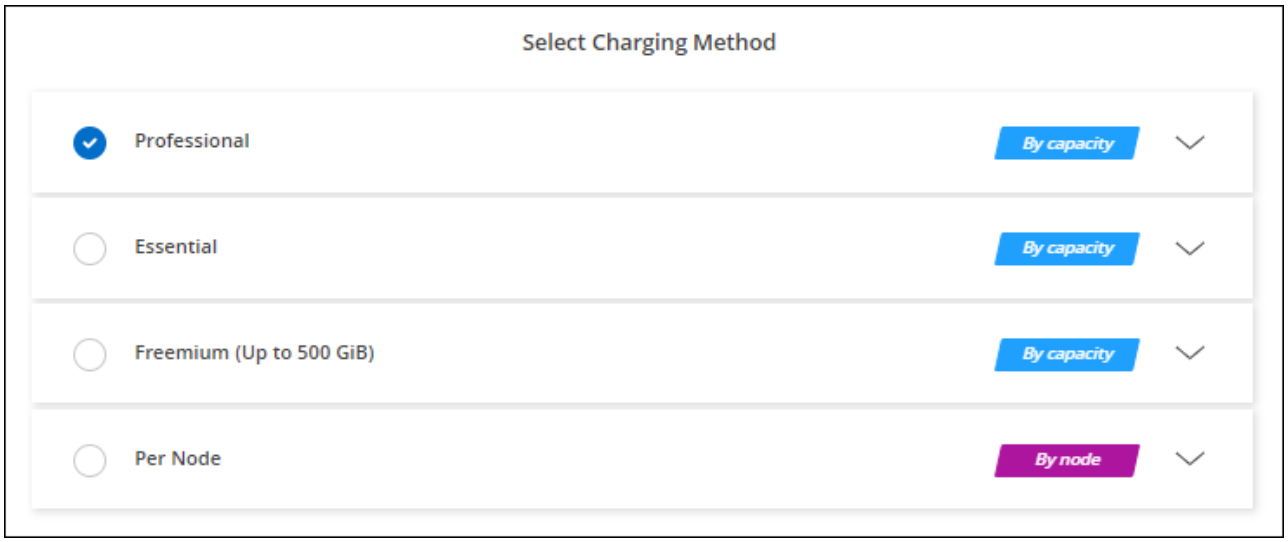
   您必須先從 BlueXP 數位錢包取得授權、才能搭配 Cloud Volumes ONTAP 使用。如有需要、您可以 "手動將授權新增至 BlueXP 數位錢包"。

3. 在「畫版」頁面上、按一下「新增工作環境」、然後依照BlueXP中的步驟進行。
   a. 在*詳細資料與認證*頁面上、按一下*編輯認證>新增訂閱*、然後依照提示訂閱Google Cloud

Marketplace中的隨用隨付方案。

您向NetApp購買的授權一律會先收取費用、但如果您超過授權容量或授權到期、則會從市場的每小時費率中收取費用。

b. 返回BlueXP之後、當您到達「充電方法」頁面時、請選取容量型套件。



"請參閱逐步指示Cloud Volumes ONTAP 、在Google Cloud中啟動「功能不全」"。

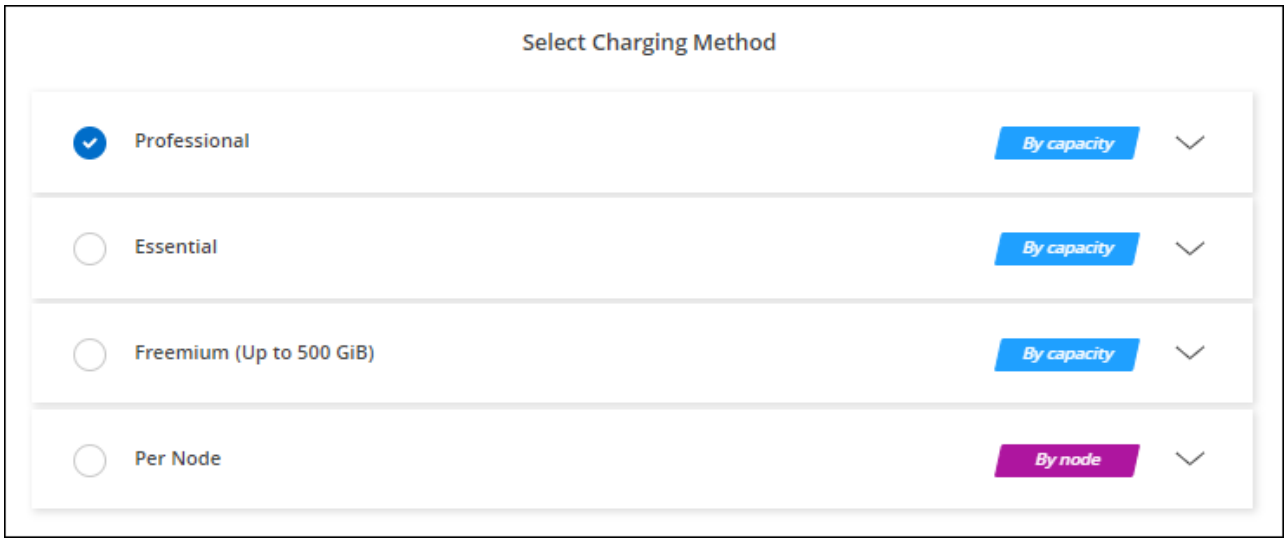
PAYGO訂閱

從雲端供應商的市場訂閱優惠、每小時支付一次。

當您建立Cloud Volumes ONTAP 一個運作環境時、BlueXP會提示您訂閱Google Cloud Marketplace提供的合約。該訂閱之後會與工作環境建立關聯、以便進行充電。您可以在其他工作環境中使用相同的訂閱。

步驟

1. 從左側導覽功能表中、選取*儲存設備> Canvas*。
2. 在「畫版」頁面上、按一下「新增工作環境」、然後依照BlueXP中的步驟進行。
   a. 在*詳細資料與認證*頁面上、按一下*編輯認證>新增訂閱*、然後依照提示訂閱Google Cloud Marketplace中的隨用隨付方案。
   b. 返回BlueXP之後、當您到達「充電方法」頁面時、請選取容量型套件。



"請參閱逐步指示Cloud Volumes ONTAP 、在Google Cloud中啟動「功能不全」"。

您可以從「設定」>「認證」頁面管理與您帳戶相關的Google Cloud Marketplace訂閱。 "瞭解如何管理您的Google Cloud認證與訂閱"

年度合約

購買年度合約、每年支付Cloud Volumes ONTAP 一份銷售費。

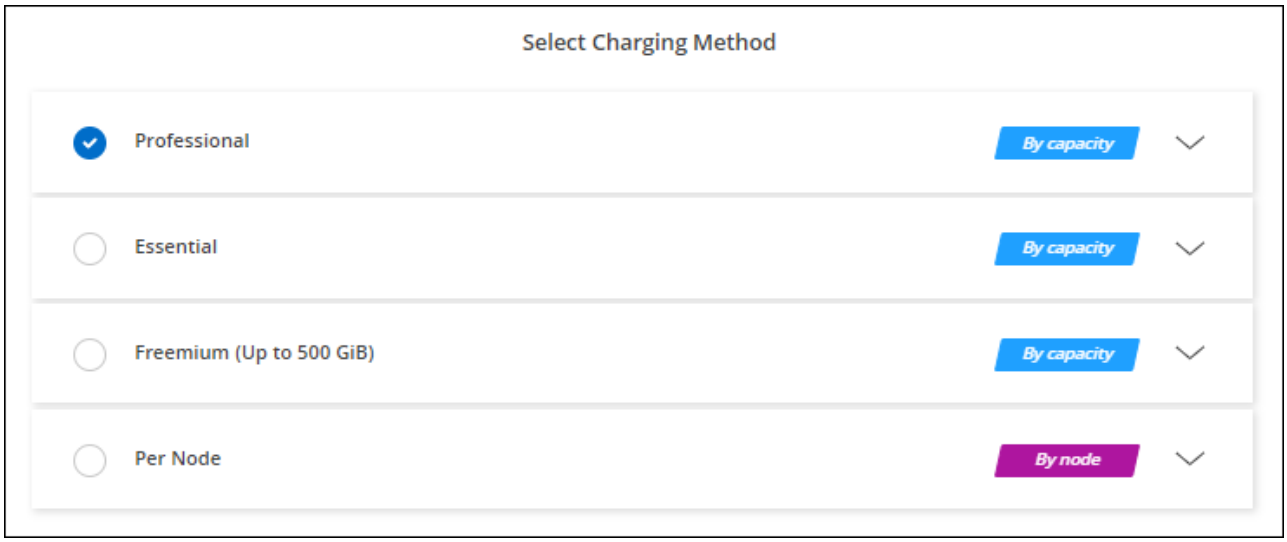
步驟

1. 請聯絡您的NetApp銷售代表以購買年度合約。

   合約可在Google Cloud Marketplace以_Private _優惠形式提供。

   在NetApp與您分享私人優惠之後、您可以在工作環境建立期間、從Google Cloud Marketplace訂閱年度方案。

2. 在「畫版」頁面上、按一下「新增工作環境」、然後依照BlueXP中的步驟進行。
   a. 在*詳細資料與認證*頁面上、按一下*編輯認證>新增訂閱*、然後依照提示在Google Cloud Marketplace訂閱年度計畫。
   b. 在Google Cloud中、選取與您的帳戶共享的年度計畫、然後按一下*訂閱*。
   c. 返回BlueXP之後、當您到達「充電方法」頁面時、請選取容量型套件。



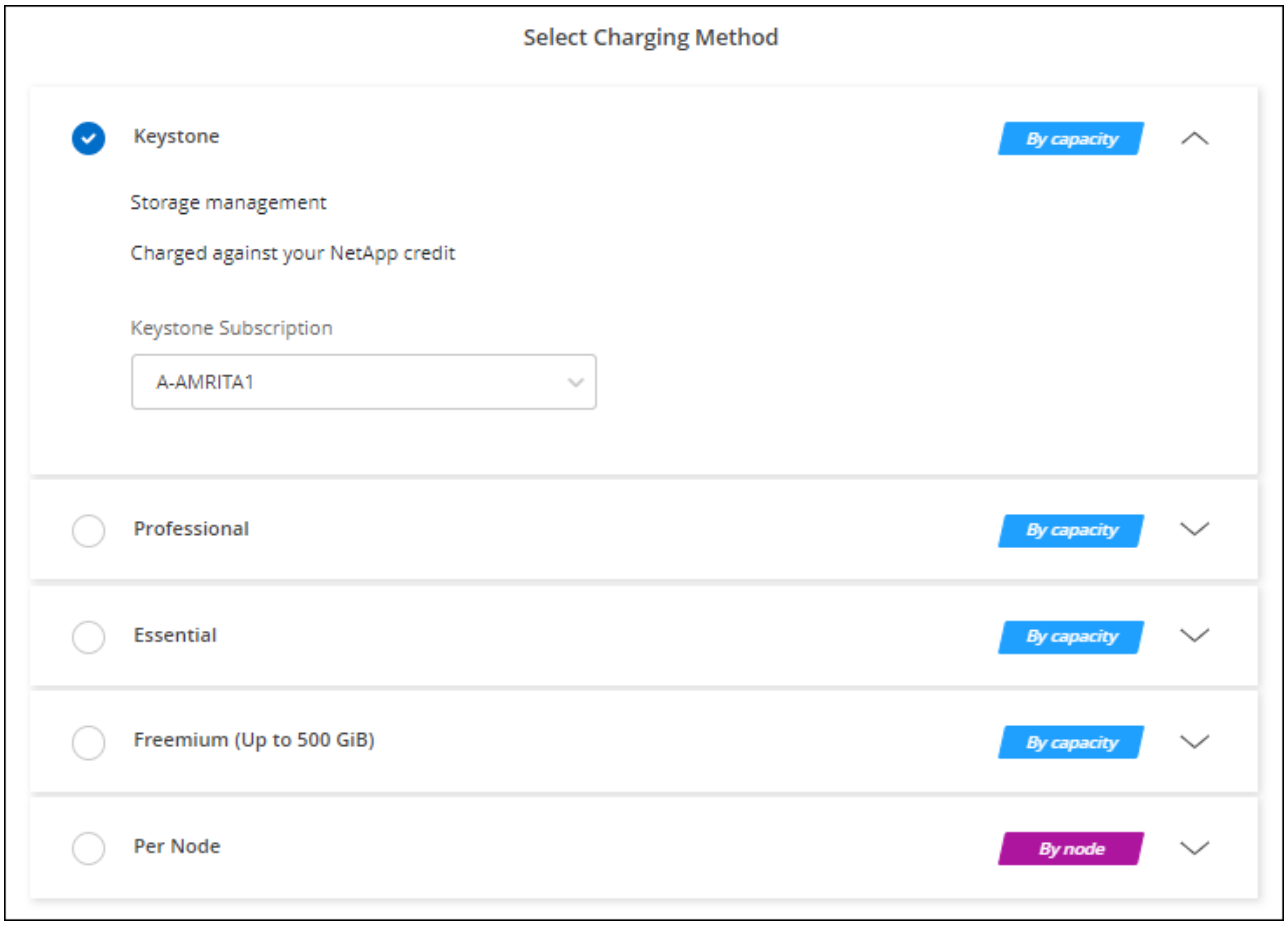
"請參閱逐步指示Cloud Volumes ONTAP 、在Google Cloud中啟動「功能不全」"。

Keystone訂閱

Keystone 訂閱是一項隨成長付費訂閱服務。 "深入瞭解 NetApp Keystone 訂閱"。

步驟

1. 如果您尚未訂閱、 "請聯絡NetApp"
2. mailto ： ng-keystone-success@netapp.com [聯絡 NetApp] 以使用一或多個 Keystone 訂閱來授權您的 BlueXP 使用者帳戶。
3. NetApp授權您的帳戶之後、 "連結您的訂閱內容以供Cloud Volumes ONTAP 搭配使用"。
4. 在「畫版」頁面上、按一下「新增工作環境」、然後依照BlueXP中的步驟進行。
    a. 當系統提示您選擇充電方法時、請選取 Keystone Subscription 充電方法。



"請參閱逐步指示Cloud Volumes ONTAP 、在Google Cloud中啟動「功能不全」"。

在Cloud Volumes ONTAP Google Cloud上啟動

您可以Cloud Volumes ONTAP 在單一節點組態中或在Google Cloud中以HA配對的形式啟動功能。

開始之前

您需要下列項目才能建立工作環境。

- 已啟動並執行的連接器。
  - 您應該擁有 "與工作區相關的連接器"。
  - "您應該隨時準備好讓 Connector 保持運作"。
  - 與 Connector 相關的服務帳戶 "應具備所需的權限"
- 瞭解您要使用的組態。

  您應該已做好準備、選擇組態、並向系統管理員取得Google Cloud網路資訊。如需詳細資訊、請參閱 "規劃 Cloud Volumes ONTAP 您的需求組態"。

- 瞭解設定Cloud Volumes ONTAP 驗證功能所需的條件。

"瞭解如何設定授權"。

- Google Cloud API應該是 "在您的專案中啟用"：
  - Cloud Deployment Manager V2 API
  - 雲端記錄 API
  - Cloud Resource Manager API
  - 運算引擎 API
  - 身分識別與存取管理（ IAM ） API

在Google Cloud中啟動單一節點系統

在BlueXP中建立工作環境、在Cloud Volumes ONTAP Google Cloud中推出功能更新。

步驟

1. 從左側導覽功能表中、選取*儲存設備> Canvas*。
2. [[訂閱]在「畫版」頁面上、按一下「新增工作環境」、然後依照提示進行。
3. * 選擇位置 * ：選擇 * Google Cloud * 和 * Cloud Volumes ONTAP
4. 如果出現提示、 "建立連接器"。
5. 詳細資料與認證：選取專案、指定叢集名稱、選擇性地選取服務帳戶、選擇性地新增標籤、然後指定認證資料。

   下表說明您可能需要指導的欄位：

欄位	說明
工作環境名稱	BlueXP使用工作環境名稱來命名Cloud Volumes ONTAP 支援系統和Google Cloud VM執行個體。如果您選取該選項、它也會使用名稱做為預先定義安全性群組的前置詞。
服務帳戶名稱	如果您打算使用 "資料分層" 或 "BlueXP 備份與還原" 有了這個功能、您就需要啟用*服務帳戶*、並選取具有預先定義儲存管理員角色的服務帳戶。Cloud Volumes ONTAP "瞭解如何建立服務帳戶"。
新增標籤	標籤是Google Cloud資源的中繼資料。BlueXP會將標籤新增Cloud Volumes ONTAP 至與系統相關的支援系統和Google Cloud資源。 建立工作環境時、您最多可以從使用者介面新增四個標籤、然後在建立之後新增更多標籤。請注意、在建立工作環境時、 API 不會限制您使用四個標籤。 如需標籤的相關資訊、請參閱 "Google Cloud 文件：標示資源"。
使用者名稱和密碼	這些是Cloud Volumes ONTAP 適用於整個叢集管理員帳戶的認證資料。您可以使用這些認證資料、 Cloud Volumes ONTAP 透過 System Manager 或其 CLI 連線至功能驗證。保留預設的_admin_使用者名稱、或將其變更為自訂使用者名稱。

欄位	說明
編輯專案	選取 Cloud Volumes ONTAP 您要駐留的專案。預設專案是BlueXP所在的專案。 如果在下拉式清單中沒有看到任何其他專案、表示您尚未將BlueXP服務帳戶與其他專案建立關聯。前往 Google Cloud 主控台、開啟 IAM 服務、然後選取專案。將具有BlueXP角色的服務帳戶新增至該專案。您必須針對每個專案重複此步驟。 這是您為BlueXP設定的服務帳戶、 "如本頁所述"。 按一下 * 「新增訂閱」 * 、將選取的認證資料與訂閱建立關聯。 若要建立隨用隨付Cloud Volumes ONTAP 功能的功能性支援系統、您需要從Cloud Volumes ONTAP Google Cloud Marketplace選擇與訂閱功能相關的Google Cloud專案。

下列影片說明如何將隨用隨付服務市場訂閱關聯至Google Cloud專案。或者、請依照中的步驟訂閱 "將Marketplace訂閱與Google Cloud認證建立關聯" 區段。

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

6. * 服務 * ：選取您要在此系統上使用的服務。若要選取 BlueXP 備份與還原、或使用 BlueXP 分層、您必須在步驟 3 中指定服務帳戶。

   如果您想要使用 WORM 和資料分層功能、您必須停用 BlueXP 備份與還原、並部署 9.8 版或更新版本的 Cloud Volumes ONTAP 工作環境。

7. 位置與連線：選擇位置、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。

   下表說明您可能需要指導的欄位：

欄位	說明
連線驗證	若要將冷資料分層至Google Cloud Storage儲存庫、Cloud Volumes ONTAP 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"。
產生的防火牆原則	如果讓BlueXP為您產生防火牆原則、您必須選擇允許流量的方式： • 如果您選擇*選取的VPC only（僅VPC）*、則傳入流量的來源篩選器為所選VPC的子網路範圍、以及連接器所在VPC的子網路範圍。這是建議的選項。 • 如果您選擇*所有VPC*、傳入流量的來源篩選器為0.00.0.0/0 IP範圍。
使用現有的防火牆原則	如果您使用現有的防火牆原則、請確定其中包含必要的規則。連結： Learn 關於 Cloud Volumes ONTAP 的防火牆規則 。

8. 收費方法與 **NSS** 帳戶：指定您要搭配此系統使用的收費選項，然後指定 NetApp 支援網站帳戶。

- "深入瞭Cloud Volumes ONTAP 解適用於此功能的授權選項"。
- "瞭解如何設定授權"。

9. * 預先設定的套件 * ：選取其中一個套件以快速部署 Cloud Volumes ONTAP 某個作業系統、或按一下 * 建立我自己的組態 * 。

   如果您選擇其中一個套件、則只需指定一個 Volume 、然後檢閱並核准組態。

10. 授權：視Cloud Volumes ONTAP 需要變更此版本、然後選取機器類型。

    如果所選版本有較新的發行候選版本、一般可用度或修補程式版本、則在建立工作環境時、BlueXP會將系統更新至該版本。例如、如果您選擇Cloud Volumes ONTAP 了「更新」功能、就會進行更新。更新不會從一個版本發生到另一個版本、例如從 9.6 到 9.7 。

11. * 基礎儲存資源 * ：選擇初始 Aggregate 的設定：每個磁碟的磁碟類型和大小。

    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Aggregate中的所有磁碟、以及使用Simple Provisioning選項時、BlueXP所建立的任何其他Aggregate。您可以使用進階配置選項、建立使用不同磁碟大小的集合體。

    如需選擇磁碟類型和大小的說明、請參閱 "在 Google Cloud 中調整系統規模"。

12. * Flash Cache 、寫入速度與 WORM * ：

    a. 如有需要、請啟用 * Flash Cache* 。

       從 Cloud Volumes ONTAP 9.13.1 開始、 n2-Standard-32 、 n2-Standard-48 和 n2-Standard-64 執行個體類型支援 _Flash Caches 。您無法在部署後停用 Flash Cache 。

    b. 如果需要、請選擇*正常*或*高速*寫入速度。

       "深入瞭解寫入速度"。

       高寫入速度和高傳輸單位（ MTU ） 8 、 896 位元組可透過 * 高 * 寫入速度選項取得。此外、較高的MTU為8、896、需要選擇VPC-1、VPC-2和VPC-3來進行部署。如需VPC-1、VPC-2和VPC-3的詳細資訊、請參閱 "VPC-1、VPC-2和VPC-3的規則"。

    c. 視需要啟動一次寫入、多次讀取（WORM）儲存設備。

       如果啟用Cloud Volumes ONTAP 資料分層功能、無法啟用WORM 9.7版及更低版本。啟用WORM和分層後、將Cloud Volumes ONTAP 會封鎖還原或降級至物件9.8。

    "深入瞭解 WORM 儲存設備"。

    a. 如果您啟動WORM儲存設備、請選取保留期間。

13. * Google Cloud Platform中的資料分層*：選擇是否要在初始Aggregate上啟用資料分層、選擇階層式資料的儲存類別、然後選擇具有預先定義儲存管理角色的服務帳戶（Cloud Volumes ONTAP 適用於更新版本的更新版本）、或是選擇Google Cloud帳戶（Cloud Volumes ONTAP 不支援支援支援功能9.6）。

    請注意下列事項：

- BlueXP會在Cloud Volumes ONTAP 整個過程中設定服務帳戶。此服務帳戶提供資料分層至 Google Cloud Storage 儲存庫的權限。請務必將Connector服務帳戶新增為分層服務帳戶的使用者、否則您無法從BlueXP中選取該帳戶
- 如需新增Google Cloud帳戶的說明、請參閱 "設定及新增Google Cloud帳戶、以便使用9.6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原則。
- 如果停用資料分層、您可以在後續的Aggregate上啟用、但您需要關閉系統、並從Google Cloud主控台新增服務帳戶。

  "深入瞭解資料分層"。

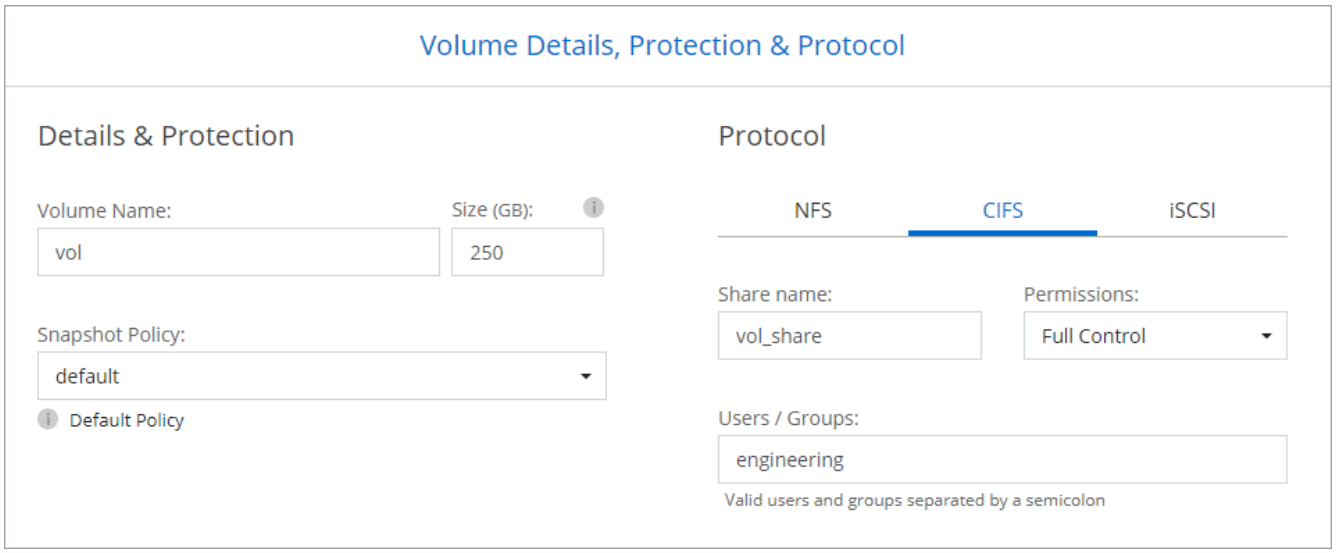
14. * 建立 Volume * ：輸入新磁碟區的詳細資料、或按一下 * 跳過 * 。

    "瞭解支援的用戶端傳輸協定和版本"。

    本頁中的部分欄位是不知自明的。下表說明您可能需要指導的欄位：

欄位	說明
尺寸	您可以輸入的最大大小、主要取決於您是否啟用精簡配置、這可讓您建立比目前可用實體儲存容量更大的磁碟區。
存取控制（僅適用於 NFS ）	匯出原則會定義子網路中可存取磁碟區的用戶端。根據預設、BlueXP會輸入一個值、以供存取子網路中的所有執行個體。
權限與使用者 / 群組（僅限 CIFS ）	這些欄位可讓您控制使用者和群組（也稱為存取控制清單或 ACL ）的共用存取層級。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。如果您指定網域 Windows 使用者名稱、則必須使用網域 \ 使用者名稱格式來包含使用者的網域。
Snapshot 原則	Snapshot 複製原則會指定自動建立的 NetApp Snapshot 複本的頻率和數量。NetApp Snapshot 複本是一種不影響效能的時間點檔案系統映像、需要最少的儲存容量。您可以選擇預設原則或無。您可以針對暫時性資料選擇「無」：例如、 Microsoft SQL Server 的 Tempdb 。
進階選項（僅適用於 NFS ）	為磁碟區選取 NFS 版本： NFSv3 或 NFSv3 。
啟動器群組和 IQN （僅適用於 iSCSI ）	iSCSI 儲存目標稱為 LUN （邏輯單元）、以標準區塊裝置的形式呈現給主機。 啟動器群組是 iSCSI 主機節點名稱的表格、可控制哪些啟動器可存取哪些 LUN 。 iSCSI 目標可透過標準乙太網路介面卡（ NIC ）、 TCP 卸載引擎（ TOE ）卡（含軟體啟動器）、整合式網路介面卡（ CNA ）或專用主機匯流排介面卡（ HBA ）連線至網路、並由 iSCSI 合格名稱（ IQN ）識別。 建立iSCSI磁碟區時、BlueXP會自動為您建立LUN。我們只要在每個磁碟區建立一個 LUN 、就能輕鬆完成工作、因此不需要管理。建立磁碟區之後、 "使用 IQN 從主機連線至 LUN"。

    下圖顯示 CIFS 傳輸協定的「 Volume 」（磁碟區）頁面：



15. * CIFS 設定 * ：如果您選擇 CIFS 傳輸協定、請設定 CIFS 伺服器。

欄位	說明
DNS 主要和次要 IP 位址	提供 CIFS 伺服器名稱解析的 DNS 伺服器 IP 位址。 列出的 DNS 伺服器必須包含所需的服務位置記錄（ SRV), 才能找到 CIFS 伺服器要加入之網域的 Active Directory LDAP 伺服器和網域控制器。 如果您要設定Google Managed Active Directory、AD預設可透過169.254.169.254 IP位址存取。
要加入的 Active Directory 網域	您要 CIFS 伺服器加入之 Active Directory （ AD ）網域的 FQDN 。
授權加入網域的認證資料	具有足夠權限的 Windows 帳戶名稱和密碼、可將電腦新增至 AD 網域內的指定組織單位（ OU ）。
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 網域中與 CIFS 伺服器相關聯的組織單位。預設值為「 CN= 電腦」。 若要將Google託管Microsoft AD設定為Cloud Volumes ONTAP AD伺服器以供使用、請在此欄位中輸入* OU=computers,OU=Cloud *。 "Google Cloud文件：Google託管Microsoft AD的組織單位"
DNS 網域	適用於整個儲存虛擬 Cloud Volumes ONTAP 機器（ SVM ）的 DNS 網域。在大多數情況下、網域與 AD 網域相同。
NTP 伺服器	選擇 * 使用 Active Directory 網域 * 來使用 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、則應該使用 API 。請參閱 "藍圖XP自動化文件" 以取得詳細資料。 請注意、您只能在建立CIFS伺服器時設定NTP伺服器。您建立CIFS伺服器之後、就無法進行設定。

16. * 使用率設定檔、磁碟類型及分層原則 * ：視需要選擇是否要啟用儲存效率功能、並變更磁碟區分層原則。

如需詳細資訊、請參閱 "選擇Volume使用設定檔" 和 "資料分層總覽"。

17. * 審查與核准 * ：檢閱並確認您的選擇。
    a. 檢閱組態的詳細資料。
    b. 按一下*更多資訊*以檢閱有關支援與BlueXP將購買的Google Cloud資源的詳細資料。
    c. 選取「 * 我瞭解 … * 」核取方塊。
    d. 按一下「 * 執行 * 」。

結果

BlueXP部署Cloud Volumes ONTAP 了這個功能完善的系統。您可以追蹤時間表的進度。

如果您在部署 Cloud Volumes ONTAP 此系統時遇到任何問題、請檢閱故障訊息。您也可以選取工作環境、然後按一下 * 重新建立環境 * 。

如需其他協助、請前往 "NetApp Cloud Volumes ONTAP 支援"。

完成後

- 如果您已配置 CIFS 共用區、請授予使用者或群組檔案和資料夾的權限、並確認這些使用者可以存取共用區並建立檔案。
- 如果您要將配額套用至磁碟區、請使用 System Manager 或 CLI 。

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

在Google Cloud上啟動HA配對

在BlueXP中建立工作環境、在Cloud Volumes ONTAP Google Cloud中推出功能更新。

步驟

1. 從左側導覽功能表中、選取*儲存設備> Canvas*。
2. 在「畫版」頁面上、按一下「 * 新增工作環境 * 」、然後依照提示進行。
3. * 選擇位置 * ：選擇 * Google Cloud * 和 * Cloud Volumes ONTAP 《 * 》 HA * 。
4. * 詳細資料與認證 * ：選取專案、指定叢集名稱、選擇性地選取服務帳戶、選擇性地新增標籤、然後指定認證資料。

   下表說明您可能需要指導的欄位：

欄位	說明
工作環境名稱	BlueXP使用工作環境名稱來命名Cloud Volumes ONTAP 支援系統和Google Cloud VM執行個體。如果您選取該選項、它也會使用名稱做為預先定義安全性群組的前置詞。
服務帳戶名稱	如果您打算使用 "BlueXP 分層" 或 "BlueXP 備份與還原" 服務、您必須啟用 * 服務帳戶 * 交換器、然後選取具有預先定義儲存管理角色的服務帳戶。

欄位	說明
新增標籤	標籤是Google Cloud資源的中繼資料。BlueXP會將標籤新增Cloud Volumes ONTAP 至與系統相關的支援系統和Google Cloud資源。 建立工作環境時、您最多可以從使用者介面新增四個標籤、然後在建立之後新增更多標籤。請注意、在建立工作環境時、 API 不會限制您使用四個標籤。 如需標籤的相關資訊、請參閱 "Google Cloud 文件：標示資源"。
使用者名稱和密碼	這些是Cloud Volumes ONTAP 適用於整個叢集管理員帳戶的認證資料。您可以使用這些認證資料、 Cloud Volumes ONTAP 透過 System Manager 或其 CLI 連線至功能驗證。保留預設的_admin_使用者名稱、或將其變更為自訂使用者名稱。
編輯專案	選取 Cloud Volumes ONTAP 您要駐留的專案。預設專案是BlueXP所在的專案。 如果在下拉式清單中沒有看到任何其他專案、表示您尚未將BlueXP服務帳戶與其他專案建立關聯。前往 Google Cloud 主控台、開啟 IAM 服務、然後選取專案。將具有BlueXP角色的服務帳戶新增至該專案。您必須針對每個專案重複此步驟。 這是您為BlueXP設定的服務帳戶、 "如本頁所述"。 按一下 * 「新增訂閱」 * 、將選取的認證資料與訂閱建立關聯。 若要建立隨用隨付Cloud Volumes ONTAP 功能的功能性支援系統、您需要從Cloud Volumes ONTAP Google Cloud Marketplace選擇與訂閱功能相關的Google Cloud專案。

下列影片說明如何將隨用隨付服務市場訂閱關聯至Google Cloud專案。 或者、請依照中的步驟訂閱 "將Marketplace訂閱與Google Cloud認證建立關聯" 區段。

▶ https://docs.netapp.com/zh-tw/test//media/video_subscribing_gcp.mp4 *(video)*

5. * 服務 * ：選取您要在此系統上使用的服務。若要選取 BlueXP 備份與還原、或使用 BlueXP 分層、您必須在步驟 3 中指定服務帳戶。

   如果您想要使用 WORM 和資料分層功能、您必須停用 BlueXP 備份與還原、並部署 9.8 版或更新版本的 Cloud Volumes ONTAP 工作環境。

6. * HA 部署模式 * ：選擇多個區域（建議）或單一區域進行 HA 組態。然後選取區域和區域。

   "深入瞭解 HA 部署模式"。

7. * 連線能力 * ：為 HA 組態選取四個不同的 VPC 、在每個 VPC 中選取一個子網路、然後選擇防火牆原則。

   "深入瞭解網路需求"。

   下表說明您可能需要指導的欄位：

欄位	說明
產生的原則	如果讓BlueXP為您產生防火牆原則、您必須選擇允許流量的方式： • 如果您選擇*選取的VPC only（僅VPC）*、則傳入流量的來源篩選器為所選VPC的子網路範圍、以及連接器所在VPC的子網路範圍。這是建議的選項。 • 如果您選擇*所有VPC*、傳入流量的來源篩選器為0.00.0.0/0 IP範圍。
使用現有的	如果您使用現有的防火牆原則、請確定其中包含必要的規則。 "深入瞭Cloud Volumes ONTAP 解適用於此功能的防火牆規則"。

8. 收費方法與 **NSS** 帳戶：指定您要搭配此系統使用的收費選項，然後指定 NetApp 支援網站帳戶。
   - "深入瞭Cloud Volumes ONTAP 解適用於此功能的授權選項"。
   - "瞭解如何設定授權"。
9. * 預先設定的套件 * ：選取其中一個套件以快速部署 Cloud Volumes ONTAP 某個作業系統、或按一下 * 建立我自己的組態 * 。

   如果您選擇其中一個套件、則只需指定一個 Volume 、然後檢閱並核准組態。
10. 授權：視Cloud Volumes ONTAP 需要變更此版本、然後選取機器類型。

    如果所選版本有較新的發行候選版本、一般可用度或修補程式版本、則在建立工作環境時、BlueXP會將系統更新至該版本。例如、如果您選擇Cloud Volumes ONTAP 了「更新」功能、就會進行更新。更新不會從一個版本發生到另一個版本、例如從 9.6 到 9.7 。
11. * 基礎儲存資源 * ：選擇初始 Aggregate 的設定：每個磁碟的磁碟類型和大小。

    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Aggregate中的所有磁碟、以及使用Simple Provisioning選項時、BlueXP所建立的任何其他Aggregate。您可以使用進階配置選項、建立使用不同磁碟大小的集合體。

    如需選擇磁碟類型和大小的說明、請參閱 "在 Google Cloud 中調整系統規模"。
12. * Flash Cache 、寫入速度與 WORM * ：
    a. 如有需要、請啟用 * Flash Cache* 。

       從 Cloud Volumes ONTAP 9.13.1 開始、 n2-Standard-32 、 n2-Standard-48 和 n2-Standard-64 執行個體類型支援 _Flash Caches 。您無法在部署後停用 Flash Cache 。
    b. 如果需要、請選擇*正常*或*高速*寫入速度。

       "深入瞭解寫入速度"。

透過使用 n2-Standard-16 、 n2-Standard-32 、 n2-Standard-48 及 n2-Standard-64 執行個體類型的 * High * 寫入速度選項、可獲得高寫入速度及高傳輸單位（ MTU ） 8 、 896 位元組。此外、較高的MTU為8、896、需要選擇VPC-1、VPC-2和VPC-3來進行部署。高寫入速度和 8 、 896 的 MTU 與功能有關、無法在設定的執行個體中個別停用。如需VPC-1、VPC-2和VPC-3的詳細資訊、請參閱 "VPC-1、VPC-2和VPC-3的規則"。

c. 視需要啟動一次寫入、多次讀取（WORM）儲存設備。

如果啟用Cloud Volumes ONTAP 資料分層功能、無法啟用WORM 9.7版及更低版本。啟用WORM和分層後、將Cloud Volumes ONTAP 會封鎖還原或降級至物件9.8。

"深入瞭解 WORM 儲存設備"。

a. 如果您啟動WORM儲存設備、請選取保留期間。

13. * Google Cloud中的資料分層*：選擇是否要在初始Aggregate上啟用資料分層、選擇階層式資料的儲存類別、然後選取具有預先定義儲存管理角色的服務帳戶。

請注意下列事項：

- BlueXP會在Cloud Volumes ONTAP 整個過程中設定服務帳戶。此服務帳戶提供資料分層至 Google Cloud Storage 儲存庫的權限。請務必將Connector服務帳戶新增為分層服務帳戶的使用者、否則您無法從BlueXP中選取該帳戶。
- 您可以在建立或編輯磁碟區時、選擇特定的磁碟區分層原則。
- 如果停用資料分層、您可以在後續的Aggregate上啟用、但您需要關閉系統、並從Google Cloud主控台新增服務帳戶。

"深入瞭解資料分層"。

14. * 建立 Volume * ：輸入新磁碟區的詳細資料、或按一下 * 跳過 * 。

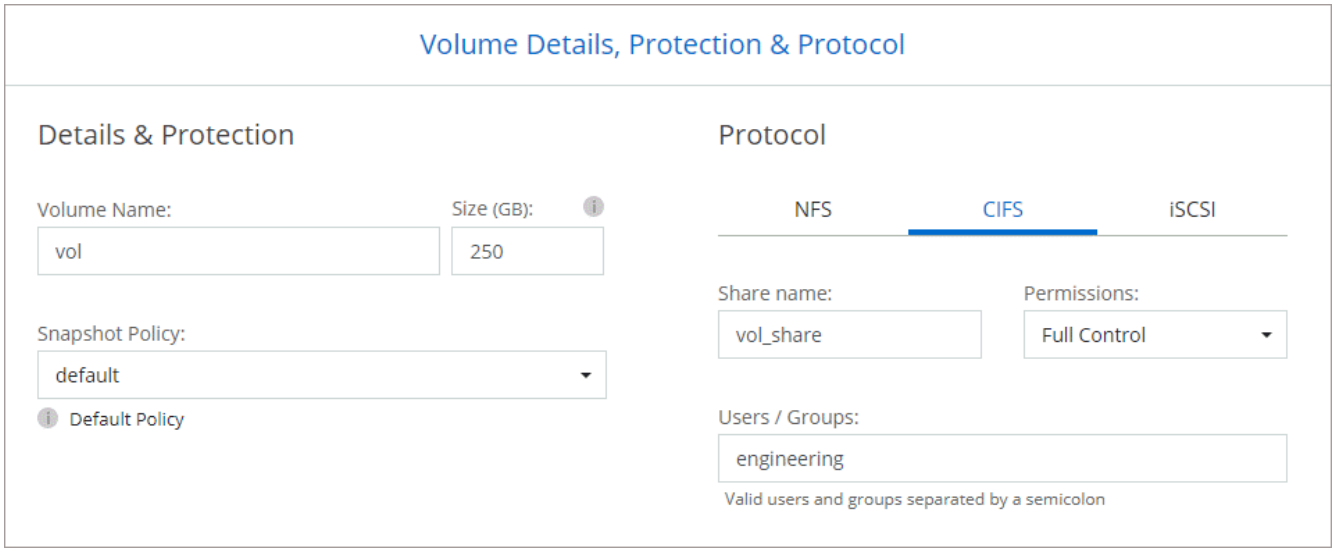
"瞭解支援的用戶端傳輸協定和版本"。

本頁中的部分欄位是不知自明的。下表說明您可能需要指導的欄位：

欄位	說明
尺寸	您可以輸入的最大大小、主要取決於您是否啟用精簡配置、這可讓您建立比目前可用實體儲存容量更大的磁碟區。
存取控制（僅適用於 NFS ）	匯出原則會定義子網路中可存取磁碟區的用戶端。根據預設、BlueXP會輸入一個值、以供存取子網路中的所有執行個體。
權限與使用者 / 群組（僅限 CIFS ）	這些欄位可讓您控制使用者和群組（也稱為存取控制清單或 ACL ）的共用存取層級。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。如果您指定網域 Windows 使用者名稱、則必須使用網域 \ 使用者名稱格式來包含使用者的網域。
Snapshot 原則	Snapshot 複製原則會指定自動建立的 NetApp Snapshot 複本的頻率和數量。NetApp Snapshot 複本是一種不影響效能的時間點檔案系統映像、需要最少的儲存容量。您可以選擇預設原則或無。您可以針對暫時性資料選擇「無」：例如、 Microsoft SQL Server 的 Tempdb 。

欄位	說明
進階選項（僅適用於 NFS ）	為磁碟區選取 NFS 版本： NFSv3 或 NFSv3 。
啟動器群組和 IQN （僅適用於 iSCSI ）	iSCSI 儲存目標稱為 LUN （邏輯單元）、以標準區塊裝置的形式呈現給主機。 啟動器群組是 iSCSI 主機節點名稱的表格、可控制哪些啟動器可存取哪些 LUN 。 iSCSI 目標可透過標準乙太網路介面卡（ NIC ）、 TCP 卸載引擎（ TOE ）卡（含軟體啟動器）、整合式網路介面卡（ CNA ）或專用主機匯流排介面卡（ HBA ）連線至網路、並由 iSCSI 合格名稱（ IQN ）識別。 建立iSCSI磁碟區時、BlueXP會自動為您建立LUN。我們只要在每個磁碟區建立一個 LUN 、就能輕鬆完成工作、因此不需要管理。建立磁碟區之後、 "使用 IQN 從主機連線至 LUN"。

下圖顯示 CIFS 傳輸協定的「 Volume 」（磁碟區）頁面：



15. * CIFS 設定 * ：如果您選擇 CIFS 傳輸協定、請設定 CIFS 伺服器。

欄位	說明
DNS 主要和次要 IP 位址	提供 CIFS 伺服器名稱解析的 DNS 伺服器 IP 位址。 列出的 DNS 伺服器必須包含所需的服務位置記錄（ SRV), 才能找到 CIFS 伺服器要加入之網域的 Active Directory LDAP 伺服器和網域控制器。 如果您要設定Google Managed Active Directory、AD預設可透過169.254.169.254 IP位址存取。
要加入的 Active Directory 網域	您要 CIFS 伺服器加入之 Active Directory （ AD ）網域的 FQDN 。
授權加入網域的認證資料	具有足夠權限的 Windows 帳戶名稱和密碼、可將電腦新增至 AD 網域內的指定組織單位（ OU ）。
CIFS 伺服器 NetBios 名稱	AD 網域中唯一的 CIFS 伺服器名稱。

欄位	說明
組織單位	AD 網域中與 CIFS 伺服器相關聯的組織單位。預設值為「 CN= 電腦」 。 若要將Google託管Microsoft AD設定為Cloud Volumes ONTAP AD伺服器以供使用、請在此欄位中輸入* OU=computers,OU=Cloud *。 "Google Cloud文件：Google託管Microsoft AD的組織單位"
DNS 網域	適用於整個儲存虛擬 Cloud Volumes ONTAP 機器（ SVM ）的 DNS 網域。在大多數情況下、網域與 AD 網域相同。
NTP 伺服器	選擇 * 使用 Active Directory 網域 * 來使用 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、則應該使用 API 。請參閱 "藍圖XP自動化文件" 以取得詳細資料。 請注意、您只能在建立CIFS伺服器時設定NTP伺服器。您建立CIFS伺服器之後、就無法進行設定。

16. * 使用率設定檔、磁碟類型及分層原則 * ：視需要選擇是否要啟用儲存效率功能、並變更磁碟區分層原則。

    如需詳細資訊、請參閱 "選擇Volume使用設定檔" 和 "資料分層總覽"。

17. * 審查與核准 * ：檢閱並確認您的選擇。
    a. 檢閱組態的詳細資料。
    b. 按一下*更多資訊*以檢閱有關支援與BlueXP將購買的Google Cloud資源的詳細資料。
    c. 選取「 * 我瞭解 … * 」核取方塊。
    d. 按一下「 * 執行 * 」 。

結果

BlueXP部署Cloud Volumes ONTAP 了這個功能完善的系統。您可以追蹤時間表的進度。

如果您在部署 Cloud Volumes ONTAP 此系統時遇到任何問題、請檢閱故障訊息。您也可以選取工作環境、然後按一下 * 重新建立環境 * 。

如需其他協助、請前往 "NetApp Cloud Volumes ONTAP 支援"。

完成後

- 如果您已配置 CIFS 共用區、請授予使用者或群組檔案和資料夾的權限、並確認這些使用者可以存取共用區並建立檔案。
- 如果您要將配額套用至磁碟區、請使用 System Manager 或 CLI 。

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

Google Cloud Platform映像驗證

Google Cloud映像驗證總覽

Google Cloud映像驗證符合增強的NetApp安全要求。已對產生映像的指令碼進行變更、以

便在過程中使用專為此工作所產生的私密金鑰來簽署映像。您可以使用已簽署的Google Cloud摘要與公開憑證來驗證GCP映像的完整性、此憑證可透過下載 "NSS" 以取得特定版本。

支援Google Cloud映像驗證Cloud Volumes ONTAP 功能的更新版本為9.13.0或更新版本。

將Google Cloud上的影像轉換成原始格式

用於部署新執行個體、升級或用於現有映像的映像、將透過與用戶端共用 "The》（NSS）NetApp 支援網站"。已簽署的摘要及憑證將可透過NSS入口網站下載。請確定您下載的摘要和憑證是與NetApp支援部門共用的映像相對應的適當版本。例如、9.13.0映像會有9.13.0簽署的摘要和證書、可在NSS上取得。

為何需要此步驟？

無法直接從Google Cloud下載影像。若要根據簽署的摘要和憑證來驗證映像、您需要有機制來比較這兩個檔案並下載映像。若要這麼做、您必須將映像匯出/轉換成磁碟.RAW格式、並將結果儲存在Google Cloud的儲存庫中。磁碟.RAW檔案會在處理過程中產生損及壓縮。

使用者/服務帳戶需要權限才能執行下列作業：

- 存取Google儲存庫
- 寫入Google Storage儲存區
- 建立雲端建置工作（在匯出程序期間使用）
- 存取所需的映像
- 建立匯出映像工作

若要驗證映像、必須先將其轉換成磁碟.RAW格式、然後再下載。

使用Google Cloud命令列匯出Google Cloud映像

將映像匯出至雲端儲存設備的首選方法是使用 "gCloud運算映像匯出命令"。此命令會取得所提供的映像、並將其轉換成磁碟.原始 檔案、並取得tar和gzipped。產生的檔案會儲存在目的地URL、然後下載以供驗證。

使用者/帳戶必須擁有存取及寫入所需儲存區、匯出映像及雲端建置（Google用於匯出映像）的權限、才能執行此作業。

使用gCloud匯出Google Cloud映像

按一下以顯示指令碼

```
$ 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
```

解壓縮檔案

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

請參閱 "匯出影像的Google Cloud文件" 如需如何透過Google Cloud匯出影像的詳細資訊、

影像簽名驗證

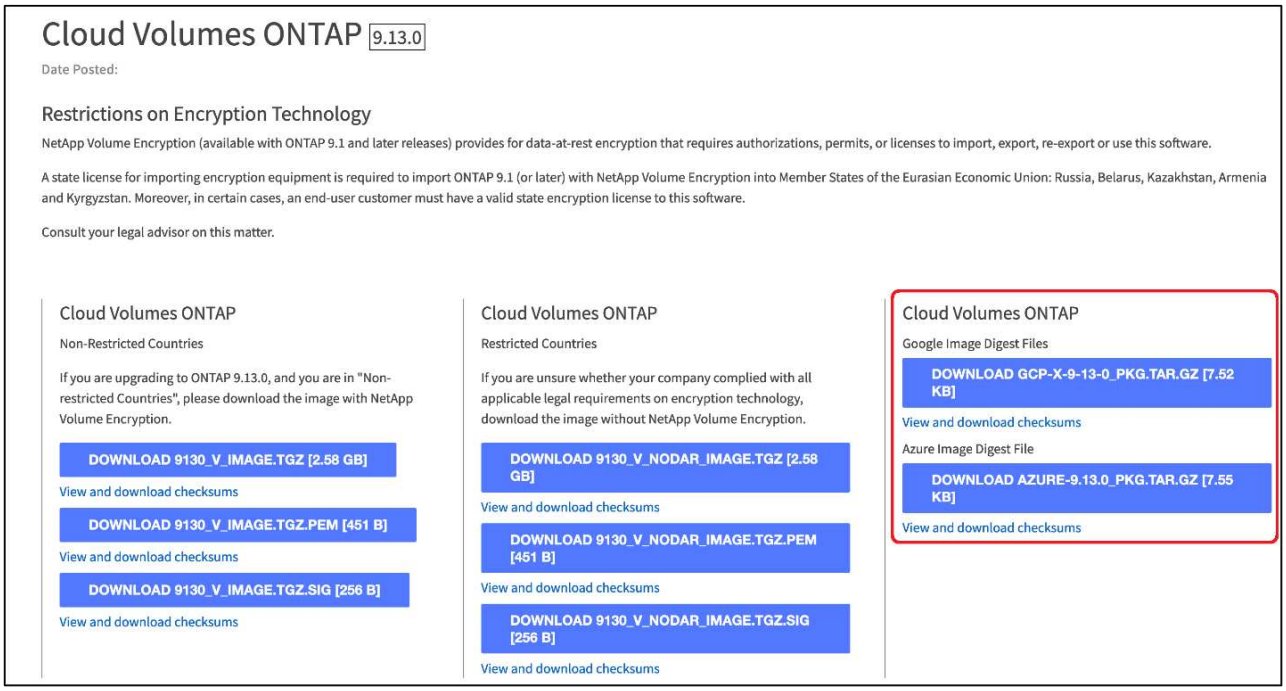
驗證**Google Cloud**簽署的映像

若要驗證匯出的Google Cloud簽署映像、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。

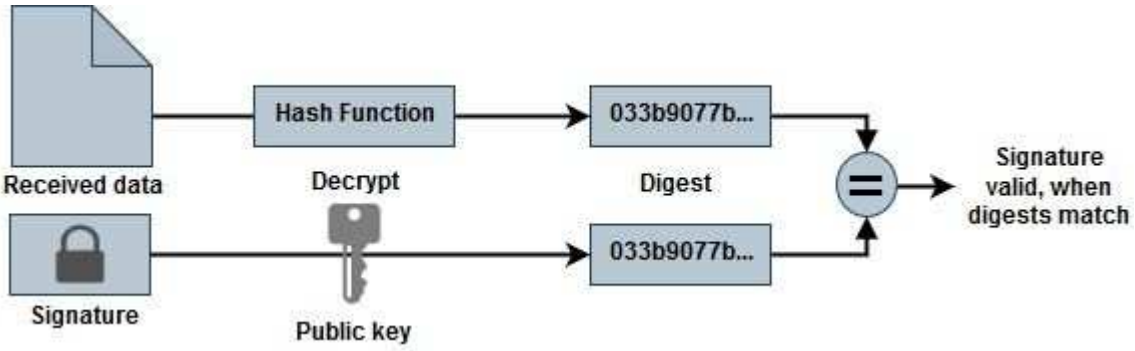
簽署映像驗證工作流程摘要

以下是Google Cloud簽署映像驗證工作流程的總覽。

- 從 "NSS"下載內含下列檔案的Google Cloud歸檔：
  - 簽名摘要（.sig）
  - 包含公開金鑰（.pem）的憑證
  - 憑證鏈結（.pem）



- 下載轉換後的disk.原始 檔案
- 使用憑證鏈結驗證憑證
- 使用含有公開金鑰的憑證來驗證已簽署的摘要
  - 使用公開金鑰解密已簽署的摘要、以擷取映像檔摘要
  - 建立已下載磁碟.原始 檔案的摘要
  - 比較兩個摘要檔案以進行驗證



使用**OpenSSL**驗證磁碟**.RAW**檔案和摘要檔案內容

您可以根據可透過取得的摘要檔案內容、驗證Google Cloud下載的disk.RAW檔案 "NSS" 使用OpenSSL。

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

步驟

1. 使用OpenSSL驗證憑證。

按一下以顯示指令碼

```
# 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.原始 檔案、簽名及憑證放在目錄中。
3. 使用OpenSSL從憑證擷取公開金鑰。
4. 使用擷取的公開金鑰解密簽名、並驗證下載的disk.原始 檔案內容。

按一下以顯示指令碼

```
# 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
```